
GAZİ ÜNİVERSİTESİ
Gazi
1926

BİLGİ GÜVENLİĞİ EĞİTİMİNE YÖNELİK UYARLANABİLİR ÖĞRENME ORTAMININ GELİŞTİRİLMESİ

Onur Ceran

DOKTORA TEZİ

BİLGİSAYAR VE ÖĞRETİM TEKNOLOJİLERİ EĞİTİMİ ANABİLİM DALI

GAZİ ÜNİVERSİTESİ

EĞİTİM BİLİMLERİ ENSTİTÜSÜ

MART, 2021

TELİF HAKKI VE TEZ FOTOKOPİ İZİN FORMU

YAZARIN

Adı : Onur

Soyadı : CERAN

Bölümü : Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü

İmza :

Teslim tarihi : …/…/2021

TEZİN

Türkçe Adı : Bilgi Güvenliği Eğitimine Yönelik Uyarlanabilir Öğrenme Ortamının Geliştirilmesi

İngilizce Adı : Development of an Adaptive Learning System about Information Security Education

ETİK İLKELERE UYGUNLUK BEYANI

Tez yazma sürecinde bilimsel ve etik ilkelere uyduğumu, yararlandığım tüm kaynakları kaynak gösterme ilkelerine uygun olarak kaynakçada belirttiğimi ve bu bölümler dışındaki tüm ifadelerin şahsıma ait olduğunu beyan ederim.

Yazar Adı Soyadı: Onur CERAN

İmza: ……

JÜRİ ONAY SAYFASI

Onur CERAN tarafından hazırlanan "Bilgi Güvenliği Eğitimine Yönelik Uyarlanabilir Öğrenme Ortamının Geliştirilmesi" adlı tez çalışması aşağıdaki jüri tarafından oy birliği ile Gazi Üniversitesi Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı'nda Doktora tezi olarak kabul edilmiştir.

Danışman: Prof. Dr. Serçin KARATAŞ .....
Bilgisayar ve Öğretim Teknolojileri Eğitimi, Gazi Üniversitesi
Başkan: Prof. Dr. Halil YURDUGÜL .....
Bilgisayar ve Öğretim Teknolojileri Eğitimi, Hacettepe Üniversitesi
Üye: Prof. Dr. Tolga GÜYER .....
Bilgisayar ve Öğretim Teknolojileri Eğitimi, Gazi Üniversitesi
Üye: Doç. Dr. Mutlu Tahsin ÜSTÜNDAĞ .....
Bilgisayar ve Öğretim Teknolojileri Eğitimi, Gazi Üniversitesi
Üye: Doç. Dr. Erhan GÜNEŞ .....
Bilgisayar ve Öğretim Teknolojileri Eğitimi, Ahi Evran Üniversitesi

Tez Savunma Tarihi: 12/02/2021
Bu tezin Bilgisayar ve Öğretim Teknolojileri Eğitimi Ana Bilim Dalında Doktora tezi olması için şartları yerine getirdiğini onaylıyorum.

Prof. Dr. Yücel GELİŞLİ
Eğitim Bilimleri Enstitüsü Müdürü ……..

“Ben doktor oldum” diyemediğim canım Anneme..

TEŞEKKÜR

Evlat olarak kendisini mutlu etmek ve onurlandırmak için çabaladığım, bana bu çabamın milyonlarca katını veren, yürümeden yemek yemeye, edepli olmaktan matematiğe, güzel söz söylemekten ahlaklı olmaya, yemek yapmaktan hak yememeye, yazı yazmaktan resim yapmaya ve bu çalışmadan daha uzun sürecek daha birçok şeyi ve hatta herşeyi bana öğreten, başım sıkıştığında hep orada olan, tatlı dili, güler yüzü ile karşılıksız sevmenin ne olduğunu yaşatan, şu an neysem onun sayesinde olan, yokluğuna alışamadığım ve alışamayacağım gül yüzlü, cennet kokulu, güzel annem ben senden razı idim Allah da senden razı olsun..

Dersime ilk girdiğinde henüz araştırma görevlisi iken bu çalışmayı tamamladığımda Prof. Dr. ünvanı olan, bana azim ve çalışma konusunda en güzel örneği oluşturan, gece, gündüz, tatil, bayram demeden her türlü soruma bıkmadan cevap veren, hayata dair sıkıntılarımı bile usanmadan dinleyen ve yol gösteren, bana danışman bir hoca gibi değil de evin küçük oğlunu ders çalıştıran bir abla gibi davranan çok kıymetli danışmanın Prof. Dr. Serçin KARATAŞ'a, tez izleme komitemde bulunan, bilgisine lisans eğitimimden bu yana büyük saygı duyduğum, verdiği küçük yönlendirmelerin her zaman büyük sorunlarımı çözdüğü Prof. Dr. Tolga GUYER'e, bu çalışma sebebiyle tanıştığım ve keşke kendisinden ders alabilmiş olsaydım dediğim, çalışmamı yaptığı yapıcı yorum ve eleştirilerle ileri taşıyan Prof. Dr. Halil YURDUGÜL'e sonsuz şükranlarımı sunarım. "İşte ülkenin böyle hocalara ihtiyacı var" cümlesinin karşılıklarından biri olduğuna inandığım Doç.Dr. Mutlu Tahsin ÜSTÜNDAĞ'a ve tez jürimde sunduğu katkılardan dolayı Doç.Dr. Erhan GÜNEŞ'e çok teşekkür ederim.

Hayata tutunma sebebim, ne yapıyorsam onun için yapıyor olduğum, en kötü zamanlarımda yüzüne bakınca enerji topladığım, “babammmm” demesiyle dünyamı değiştiren, çalışma boyunca ara sıra ihmal etmek zorunda kaldığım, ömrüm yettiğince bildiğim herşeyi ona öğretmek için çabalayacağım canım oğlum Bozlak Deniz CERAN’a kucak dolusu öpücükler..

Kendisine rağmen bu çalışmayı sonuçlandırdığım, “başlayacağım senin tezine” söylemini kendisinden her işitişim sonrasında “çalışmaya” olan hevesimi artıran, bilim dostu biricik eşim Sıla CERAN’a öyle ya da böyle bu duruma katlandığı için sonsuz şükranlarımı sunarım.

Beni bu günlere kadar yetiştiren, ilimden önce irfan öğreten, tek direğimiz babam Ahmet CERAN’a ve varlığını her daim yanımda hissettiğim abim, arkadaşım, yoldaşım Mustafa Ömür CERAN’a teşekkürü borç bilirim.

İstatistik gurusu kardeşim Ömer Faruk GÖKÇEK’e, teknik bilgi ve birikimleri ile hep kendilerinden fikir aldığım Furkan YILMAZ’a, Talip Can YALÇIN’a, Sefa ERÇEK’e, Murat AVŞAR’a, Mustafa MAŞA’ya çok teşekkür ederim.

Çalışma boyunca yetişemediğim işlemler için benim kadar koşturan İsa DEMİR’e, Ahmet ÇALTI’ya, Mehmet EROĞLU’na çok teşekkür ederim.

Çalışmama var gücüyle destek olan Junior Ahmet CERAN’a, Sevil KÜPELİ’ye, Işıl Küpeli’ye, Damla Küpeli’ye, Sarp DEMİRHAN’a ve ismini sayamadığım tüm arkdaşlarıma şükranlarımı sunarım.

Üniversitedeki her işlemim için “Alo Yardım” hattı gibi destek veren eski ve kadim dostlarım Mustafa TANRIVERDİ’ye ve Mevlüt UYSAL’a çok teşekkür ederim.

Bu zorlu süreç yaşanırken “liyakatsizlik” sebebi ile bir üst rütbeye terfimi uygun görmeyen onurlu teşkilatım Emniyet Genel Müdürlüğü’nün terfi kurullarına ayrıca teşekkürü borç bilirim..

Onur CERAN

Ankara, 2021

BİLGİ GÜVENLİĞİ EĞİTİMİNE YÖNELİK UYARLANABİLİR ÖĞRENME ORTAMININ GELİŞTİRİLMESİ

(Doktora Tezi)

Onur Ceran

GAZİ ÜNİVERSİTESİ

EĞİTİM BİLİMLERİ ENSTİTÜSÜ

MART 2021

ÖZ

Bu çalışmanın amacı, bireyleri birbirinden ayıran demografik, sosyo-demografik, kişilik özellikleri, tehlike algıları ve suça maruziyet durumları ile bilgi güvenliğine yönelik korumacı ve riskli davranışlarına ilişkin dillendirdikleri ve hayata geçirdikleri davranışlar arasındaki ilişkiyi inceleyerek bilgi güvenliği eğitimi için uyarlanabilir öğrenme ortamı geliştirilmesidir. Alan yazın ve gerçek hayat uygulamaları incelendiğinde bilgi güvenliğine yönelik tehditlerin genel olarak teknik bir takım yöntemlerle önüne geçilmeye çalışıldığı ancak bu çabaların yüzde yüz bir başarı sağlamadığı görülmüştür. Zincirin en zayıf halkası olarak bilişim sistemleri kullanıcılarının konu üzerindeki farkındalıkları büyük önem arz etmektedir. Yine alan yazındaki çalışmalar göstermektedir ki bireyler bireysel farklılıkları dolayısıyla bilgi güvenliğine dair farklı davranışlar sergilemekte, bu da farklı tehditlere maruz kalmalarına neden olmaktadır. Tasarım tabanlı araştırma yöntemi kullanılan bu çalışmada, bu kapsamda öncelikle gönüllü 619

katılımcıdan demografik, sosyo-demografik ve kişilik özellikleri, tehlike algıları, suça maruziyet durumları ile bilgi güvenliğine dair riskli ve korumacı davranışları kendi beyanatlarına dayalı (self-reported) olarak, Bilgi Güvenliği Farkındalık Ölçeği kullanılarak toplanmıştır. Daha sonra aynı katılımcıların daha önce kendi beyanatlarına göre cevap verdikleri riskli ve korumacı davranışlardan, bir web sitesi kullanılarak ölçülebilecek olan, alınan uzman görüşü sonrası belirlenen 11 tanesini uygulamalı olarak göstermeleri sağlanmıştır. 619 katılımcıdan 301'inin dâhil olduğu web uygulamasında kullanıcıların bir web sitesinin kullanılabilirliğini test ediyor oldukları izlenimi verilmiştir. Toplanan veriler ışığında, katılımcıların bilgi güvenliği konusunda korumacı ve riskli davranış söylemlerindeki değişimleri bağımsız demografik, sosyo-demografik, kişilik testi puanları değişkenleri ile açıklamak için basit doğrusal regresyon istatistik analiz yöntemi kullanılmıştır. Katılımcıların hangi bireysel özelliklerinin söylemlerini ve davranışlarını ne derece etkilediği ve buna bağlı olarak da belli bir bilgi güvenliği konu başlığı üzerinde ne şekilde bir davranış gösterebileceği hususunda tahminde bulunmak için farklı karar ağacı algoritmaları denenmiş, veri kümesi üzerinde en iyi sonucu veren C5.0 karar ağacı algoritması kullanılmıştır. Gerçekleştirilen bu analizler sonucunda kullanıcıya bu doğrultuda kişiselleştirilmiş bir çevrimiçi eğitim içeriği sunulmuştur. Hızlı prototipleme yöntemi kullanılarak hazırlanan uyarlanabilir çevrimiçi öğrenme ortamı üzerinde tasarım ve içerik konularında uzman görüşlerine sunularak düzenlemeler yapılmıştır. Hayata geçirilen çevrimiçi uyarlanabilir öğrenme ortamı bilgi güvenliğine dair gerçek davranışı ölçerek modellenmesi, çevrimiçi yapıda olması ile büyük kitleleri ulaşabilmesi, kişiselleştirilmiş eğitim içeriği sağlaması ile fazla bilgi yüklemesi ve yönlendirme problemlerinin önüne geçmesi açısından alanyazına ve gerçek hayat uygulamalarına katkı sağlamıştır.

Anahtar kelimeler : bilgi güvenliği, uyarlanabilir çevrimiçi eğitim, veri madenciliği, makine öğrenmesi, bireysel farklılıklar

Sayfa adedi : xxiii + 356

Danışman : Prof. Dr. Serçin KARATAŞ

DEVELOPMENT OF AN ADAPTIVE LEARNING SYSTEM ABOUT INFORMATION SECURITY EDUCATION

(Ph.D Thesis)

Onur Ceran

GAZİ UNIVERSITY

GRADUATE SCHOOL OF EDUCATIONAL SCIENCES

MARCH 2021

ABSTRACT

The aim of this study is development of an adaptive web based learning system about information security education by investigating relationship between users' actual behaviors and their intentions on risky and conservative behaviors about information security considering individual differences which are demographics, socio-demographics, internet usage routines, personality, risk perception and exposure to offense. According to literature and real life practices, some kind of technical solutions are applied in order to provide information security in which attempts still cannot stop information systems' to be compromised. As being the weakest link, human behavior and awareness on information security needs to be considered and studied. The literature also shows that end users show different information security behaviors because of individual differences which causes to be compromised with different threats. Developmental research method is used in this study. At the first stage of this study, demographic, socio-demographic, internet usage routines, personality, risk perception and exposure to offense attributes, risky and conservative behaviors are collected through self-reported "Information Security Awareness Scale" with the attendance of 619 volunteer end-

user. After that, these volunteers were asked to show 11 of the risky and conservative behaviors which can be measured through a web site and defined with the expert opinions. Then 301 of this 619 users' actual behaviors related with their answers to scales are examined through a web application. This web application pretends for users to evaluate a web application's usability in order to prevent Hawthorne effect. In order to explain the differences between the intensions and actual behaviors of the participants about risky and conservative behaviors with independent variables of demographic, socio-demographic and personality test scores, simple lineer regression model was used. Different decision tree algorithms have been tried to predict which individual characteristics of the participants affect their intension and behavior, and how they may act on a particular information security topic. C5.0 decision tree algorithm, which gaved the best result on the data set, has been used. As a result of these analyzes, a personalized online learning content was presented to the user in this direction. Arrangements were made on the adaptable web based learning system prepared using the rapid prototyping method by presenting expert opinions on design and content. Adaptable web based learning system that has been implemented has contributed to the literature and real life applications in terms of modeling and modeling the real behavior regarding information security, reaching large audiences with its online structure, providing personalized educational content and preventing over-information and orientation problems.

Keywords : information security, adaptable web based learning, data mining, machine learning, individual differences

Page number : xxiii + 356

Supervisor : Prof. Dr. Serçin KARATAŞ

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

BÖLÜM I

GİRİŞ

Bu bölümde araştırmanın problemi, amacı, önemi ve sınırlılıkları verilerek, araştırma raporunda kullanılan temel kavramlar açıklanmaktadır.

Problem Durumu ve Gerekçesi

İnternet ve mobil teknolojilerin gelişimi zaman ve mekân kavramlarını ortadan kaldırmış, yapılan işlemler tek bir tuşa basmakla sınırları aşarak farklı kıtalarda sonuçların alınabilmesini sağlamıştır. "We are Social" uluslararası dijital raporu (Kemp, 2019), dünya nüfusunun, geçen yıla oranla %9,1 artışla, %57'lik kısmının internet kullanıcısı olduğu ve geçen yıla oranla %2'lik bir artışla %67'lik kısmının tekil mobil cihaz kullanıcısı olduğunu belirtmektedir. Aynı raporda dünya nüfusunun %69'unun finans birimlerinde hesabı olduğunu, bu rakamın %29'unun çevrimiçi alışveriş yaptığını veya fatura ödediğini açıklamaktadır. 2018-2019 yılları arasında e-ticaret marketinde dünya çapında 1.768 trilyon dolar harcanmıştır. 2019 yılında Çin'in Wuhan kentinden başlayarak yayılan koronavirüs sonrası yaşanan pandemiden dolayı dünya öğrenci nüfusunun %68'inin okullarına fiziki olarak erişimleri kısıtlanmış (Unesco, 2020) okulların büyük bir çoğunluğunda çevrimiçi öğretim sistemlerinden yararlanarak eğitime devam edilmiştir. Kolay erişilebilir teknolojiler bir taraftan hayatımızı kolaylaştırırken diğer taraftan siber-kriminal sorunların oluşmasına da neden olmaktadır (Sarre vd., 2018). (Jagatic, Johnson, Jakobsson ve Menczer, 2007) fikri mülkiyet ve finansal kayıplara neden olan en yaygın beş siber tehdidi dağıtık servis engelleme (DDoS), zararlı yazılımlar, şifre atakları, sızdırma ve oltalama atakları olarak sıralamışlardır. Oltalama saldırısı bir sosyal mühendislik formu olup,

kendilerini güvenilir kişiler olarak kabul ettirip kişilerden hassas bilgileri almaya çalışmak olarak tanımlanabilir (Jagatic vd., 2007). Krombholz vd., (2015) oltalama saldırısını, bilişim sistemlerine teknik olarak saldırmaktansa, saldırganların bu sistemlere yasadışı olarak girmelerini sağlayacak kişisel veya gizli bilgileri insanları manipüle ederek elde etme işlemi olarak tanımlamışlardır. İnsanları bilişim sistemlerine girmeye yetkili şifrelerini vermek için manipüle etmek daha kolay olduğu için, saldırganlar eforlarını sosyal mühendislik saldırılarını kullanmak için harcamaktadırlar (Abraham ve Chengalur-Smith, 2010). Bir bireyi başka birinden ayırt etmek için kendi başına kullanılan veya başka bir bilgi ile birleştirilerek bu ayırt etme işlemi yapılabilen herhangi bir bilgiye "kişisel olarak tanımlanabilir bilgi" (PII, Personally Identifiable Information) denilmektedir (Krishnamurthy ve Wills, 2009). Milyarlarca üyesi bulunan sosyal medya platformları, saldırganların, sosyal mühendislik saldırıları gerçekleştirebilmesi için çok değerli olan kişisel olarak tanımlanabilir bilgilere kolaylıkla erişebileceği mecralar konumundandır (K. Thomas vd., 2015). Mitnick ve Simon (2009), en üst seviye güvenlik teknolojilerinin kullanıldığı organizasyonların ağ veya bilgisayar sistemlerinin, saldırı için sosyal mühendislik taktiklerini uygulayan saldırganlardan korunamayabileceğini vurgulamışlardır.

SANS Bilişim Teknolojileri Güvenlik harcamaları raporuna göre (Filkins, 2016) organizasyonlar, kaynaklarını, en çok erişim ve kimlik doğrulama, gelişmiş zararlı yazılım önleme, uç nokta güvenliği, kablosuz ağ güvenliği ve veri koruma/şifreleme teknolojilerine harcamaktadırlar. Gartner Bilgi Güvenliği Harcama Raporu (Moore ve Keen, 2018) ise 2017 yılı içerisinde bilgi güvenliği yazılım ve servislerine dünya genelinde 101.544 milyar dolar harcandığını bildirmektedir. Fakat Avustralya, Kanada, Almanya, Hollanda, İsveç, İngiltere ve Amerika gibi gelişmiş ülkelerdeki polis kayıtlarına göre siber suç eğilimlerini araştıran Levi (2017) çalışmasında çevrimiçi dolandırıcılık vakalarının önemli ölçüde artış gösterdiğini ortaya koymuştur. Federal Soruşturma Bürosu (FBI, Federal Bureau of Investigation) İnternet Suç Raporuna göre (FBI, 2018); 2017 yılında yapılan 301.580 şikâyet kaydı sonucu 1 milyar 418,7 milyon Dolar, 2018 yılında yapılan 351.937 şikâyet kaydı sonucu 2 milyar 706,4 milyon Dolar kayıp yaşanmıştır.

İstatistikler ve raporlar incelendiğinde bilgi güvenliği konusunda alınmaya çalışılan tedbirler genel olarak teknoloji tabanlı çözümlerle veya kural tabanlı politikalarla sağlanmaya çalışılmaktadır. Ancak sadece bilişim sistemi teknolojileri üzerine yapılan yatırımların insanların bilgi güvenliği suçuna maruz kalma sayısında veya kaybedilen para miktarında bir azalmayı sağlamadığı çok açıktır. Organizasyonların bilgi teknolojileri bütçelerinin büyük bir kısmını yüksek teknoloji ürünü araçlara harcıyor olmasına rağmen saldırganların genellikle eğitimsiz, bilgisiz ve izlenmeyen kullanıcıları hedef aldığının altını çizen Lineberry (2007) bilgi güvenliği farkındalık eğitiminin önemini vurgulamaktadır. Benzer bir şekilde Ghafir vd. (2018) bilgisayar sistemleri yüksek teknoloji ürünlerle korunan askeriye, sağlık, finans ve eğitim gibi birçok kritik altyapının bilgisayar uzmanı olmayan kişilerce işletildiğini ve bu durumun sosyal mühendislik gibi siber saldırılara hedef oluşturacağını belirtmişlerdir. Flores ve Ekstedt (2016) ise dışarıdan gelebilecek bilgi güvenliği tehditlerine karşı en zayıf halkanın davranışlarından ötürü çalışanlar olduğunu vurgulamaktadır. Morgan (2019) başarı ile sonuçlanan siber saldırı girişimlerinin %90'ının, oltalama saldırı ile başlatıldığını ortaya koymuş, Trček vd. (2007), insan davranışları gibi teknik olmayan konuların da göz önüne alınması gerektiğini vurgulamışlardır. Herath ve Rao (2009) çalışmalarında bilgi güvenliği farkındalığı konusunun son kullanıcılar üzerinde çalışılması gerektiğini vurgulamış, alanda yapılan çalışmaların çoğunlukla bilgi güvenliği uzmanlarına yönelik olmasını eleştirmişlerdir. Eminağaoğlu gerek Türkiye'de gerekse diğer ülkelerde alınan teknolojik, yönetimsel ve hukuksal önlemlerin artan zarar ve sorunları önlemekte yetersiz kaldığını belirtmişlerdir. Bu sebeple bilgi güvenliği konusunda teknik konuda harcamalardan önce son kullanıcı olan insanların farkındalıklarının artırılmasının önemini vurgulamışlardır. Bilgi güvenliğinin sağlanması hususuna teknoloji alanındaki çalışmalar tüm çabaların merkezinde yer alıyor olmasına rağmen, en zayıf halka olarak tabir edilen son kullanıcı bu konuda yer edinmeye başlamıştır. Bu durum son kullanıcı davranışlarının incelenmesindeki önemi ortaya koymaktadır.

Alan yazında farklı yönleriyle bireysel bilgi güvenliğine konusunda gerçekleştirilen çalışmalar bulunmaktadır (McCormac, Zwaans, Parsons, Calic ve Butavicius, 2017; Parsons vd., 2017; Öğütçü, 2010). Ancak bu çalışmalarda genellikle katılımcılardan alınan bilgiler "kişinin kendi beyanına dayalı" (self-reported) olarak adlandırılan ölçekler yardımı ile elde edilmektedir. Bu çalışmalarda katılımcılar tarafından verilen cevaplar genel olarak bilgi güvenliği konusunda

yeterli bilgilerinin olduğunu, doğru şekilde işlem yaptıklarını gösterir nitelikte sonuçlara ulaşıldığı görülmektedir. Ancak bilgi güvenliği suçlarına dair yayınlanan devlet raporları, bilgi güvenliği firmalarının yayınlamış olduğu analiz raporları ve akademik yayınlar bu çalışmaların yine aksi yönünde bulguları işaret etmektedir. Avrupa Ağ ve Bilgi Güvenliği Ajansı (Hogben ve Dekker, 2010) yayınlamış olduğu raporda, zararlı yazılımların son kullanıcıların bilgisi ve farkındalığı olmadan akıllı telefonlarına yüklenebildiklerini belirtmiş, güvenlik seçeneklerinin telefon ayarları üzerinde düzenlenebilir olmasına karşın çoğu son kullanıcının bu durumdan habersiz olduğunu vurgulamıştır. Bu sebeple son kullanıcıların dikkatsiz davranışlarının ve farkındalık eksikliklerinin en büyük risk kaynağını oluşturduğunu belirtmiştir. Jeon, Kim, Lee ve Won (2011) akıllı telefonlar ve bilgi güvenliği konulu çalışma gerçekleştirmişlerdir. Çalışma sonucunda son kullanıcıların onaylanmamış kaynaklar üzerinden yüklenen uygulamaların içerdiği riskler ve oluşabilecek zararlar konusunda farkındalıklarının olmadığı belirtilmiştir. İngiltere, Amerika, Kanada, Avustralya, Estonya, Japonya, Fransa, Finlandiya, Hollanda ve Rusya gibi gelişmiş ülkelerin bilgi güvenliği yaklaşımlarını düzenlemeye çalıştıkları, bu hususta son kullanıcıların farkındalıklarını artırma veya farkındalık oluşturma gayesi içinde oldukları belirtilmiştir (Franke ve Brynielsson, 2014). Bu durum, insanların bilgi güvenliği konusunda bilişsel olarak sahip oldukları bilgilerini, davranışa dönüştür(e)medikleri sonucunu doğurmaktadır.

Benzer bir şekilde alanyazında yapılan birçok çalışma insanların demografik, sosyo-kültürel durum, kuşak farklılıkları ve kişilik özelliklerinin, genelde bilgi teknolojileri kullanım alışkanlıkları özelde bilgi güvenliği davranış şekilleri konusunda, farklılık gösterdiğini ortaya koymaktadır. Whitty, Doodson, Creese ve Hodges (2015) kişilerin şifrelerini paylaşma konusunda bireysel farklılıkları araştırdıkları çalışmalarında kendilerini azimli olarak tanımlayan kişilerin şifrelerini paylaşmada daha açık olduklarını, kendini denetleyen genç bireylerin yaşlılara göre şifrelerini başkalarıyla paylaşmaya daha açık olduklarını vurgulamışlardır. Gratian vd. (2018), bilgi güvenliği davranış niyetleri ile birey özellikleri arasındaki bağlantıyı araştırdıkları çalışmalarında, finansal risk alma, rasyonel karar alma ve cinsiyet değişkenlerinin bilgi güvenliğine dair iyi davranış niyetlerinin önemli belirleyicilerinden oldukları sonucuna varmışlardır. McCormac vd. (2017), bilgi güvenliği farkındalığı ile bireysel farklılıkları arasındaki ilişkiyi araştırdıkları çalışmalarında genç yaş

grubunda bulunan kişilerin daha yaşlılara göre, erkeklerin ise kadınlara göre daha düşük bilgi güvenliği farkındalığı olduğunu belirlemişlerdir. Hamburger ve Ben-Artzi (2000) yüksek nevrotizm kişilik özelliği gösteren kadınların çevrimiçi uygulamalarda daha çok vakit geçirme ve fazlaca bilgisini ifşa etme eğiliminde olduğunu; Sumner, Byers ve Shearing (2011) yüksek dışa dönüklük ve uyumluluk gösteren bireylerin çevrimiçi gizliliğe daha çok önem verme ve yüksek nevrotizm ve deneyime açıklık gösteren bireylerin kendileri hakkında daha çok bilgi paylaşma eğiliminde olduğunu çalışmalarında vurgulamışlardır. Sayıca ve görece az da olsa bilgi güvenliğini etkileyen bireysel faktörleri davranış olarak ölçen araştırmalar da alanyazında mevcuttur. Butavicius vd. (2017) şüpheli epostaları belirlemede yaş, cinsiyet, kişilik özelliği, bilişsel dürtüsellik ve bilgi güvenliği farkındalık düzeyleri arasındaki ilişkiyi katılımcıların üç farklı eposta içeriğinden onların oltalama epostası olup olmadığını belirlemeleri yöntemiyle yaptıkları çalışmalarında, bireysellik özelliği öne çıkan ve bilgi güvenliği farkındalık düzeyi yüksek olan katılımcıların daha yüksek skorlar aldığını belirlemişlerdir. Al-Saggaf (2017), 269 kadın katılımcının Facebook sosyal paylaşım sitesi üzerindeki gerçek paylaşımlarını analiz ederek yaptığı çalışmasında ilişki durumunu yalnız olarak belirten katılımcıların hassas veya hassas olmayan kişisel verilerini daha çok paylaştığını belirlemiştir. Bu çalışmalar bireysel bilgi güvenliği konusunda farklı kişisel, sosyo-kültürel, demografik vb. özelliklere haiz bireylerin farklı davranışlar içerisinde bulunmasının bu konuda yapılacak olan çalışmalarda göz ardı edilmemesi gerekliliğini vurgulamaktadır.

Bireysel bilgi güvenliği konusunun sadece bu alandaki teknik uzmanların müdahil olması ve mücadele etmesinin gerek ve yeterli olmadığı yapılan akademik ve kurumsal çalışmalardan anlaşılmaktadır. Sadece akıllı telefon kullanıcısı olan ve gündelik iş ve işlemlerini bu cihaz vasıtasıyla yapan herhangi bir bireyin bile özellikle sosyal mühendislik saldırılarına maruz kalabileceği görülmektedir. Konuya getirilmeye çalışılan teknik çözümler yüzde yüz çare olmadığından bireysel bilgi güvenliği farkındalık eğitimlerinin önemi ve gerekliliği ortaya çıkmaktadır.

Eğitim müfredatları incelendiğinde bireysel bilgi güvenliğine yönelik kapsamlı bir eğitim içeriğinden bahsedilememektedir. Üniversite bünyesinde bilişim ve iletişim konularında uzmanlaşan bölümlerde (bilgisayar mühendisliği, bilişim sitemleri vb.) bilgi güvenliğinin bir

ders olarak işlendiği ancak ders içeriklerinin de güvenli kodlama, ağ güvenliği, kriptoloji vb. gibi uzmanlaşma alanlarına yönelik olduğu görülmüştür. Üniversite resmi web siteleri basın bültenlerinde, bireysel bilgi güvenliği farkındalığı için genel olarak seminerler vasıtası ile bilgilendirmelerin gerçekleştirildiğine dair video ve doküman paylaşımı yapıldığı görülmektedir.

Farkındalığının artırılması gereken kitle ve eğitimi verilecek olan konuların özelliği göz önüne alındığında çevrimiçi öğretim sistemlerinin bu konuda en başarılı araç olabileceği düşünülmektedir. Çevrimiçi öğretim sistemlerinin bireysel bilgi güvenliği farkındalık eğitimi konusunda kullanımına yönelik çalışmalar incelendiğinde, bazı üniversitelerde (örn: Cleveland State Üniversitesi, Colorado Üniversitesi vb.) bireysel bilgi güvenliği farkındalık eğitimlerinin çevrimiçi olarak verildiği ancak düşülen dipnotlarda eğitimin "güvenlik liderliği ve yönetimi" yapan kişiler için olduğu veya "iş yeri faaliyetleri" için özelleştirildiği belirtilmiştir. Bu konuda bazı devlet kuruluşlarının ve bilgi güvenliği firmalarının çevrimiçi olarak sundukları bireysel bilgi güvenliği öğretim programları, bilgi ve iletişim teknolojilerinin kullanımı esnasında dikkat edilmesinin önemli olduğunu belirtir ipuçları sayfaları bulunmaktadır. İngiltere Güvenlik Bakanlığı (NCA) tarafından hazırlanan bilgi güvenliği çevrimiçi sistemde (www.getsafeonline.org, 2020) 7 başlık altında 166 konu yer almaktadır. Aynı şekilde Amerikan Güvenlik Bakanlığı bünyesinde FBI (Federal Bureau of Investigation) tarafından hazırlanan web sitesinde (https://www.us-cert.gov/ncas/tips) 9 başlık altında 73 ipucu bulunmaktadır. Amerikan çevrimiçi eğitim platformu sağlayıcısı Coursera (www.coursera.org, 2020) üzerinde "information security + awareness", "cyber security + awareness" anahtar kelimeleri ile arama yapıldığında toplam 151 eğitim içeriğine rastlanmış ancak sadece bir tanesinin bireysel bilgi güvenliği farkındalığına yönelik olarak hazırlandığı görülmüştür. Eit Digital isimli firma tarafından hazırlanan bu eğitim içeriğini 4 ayrı konudan ibaret toplam 92 dakikalık video kaydı oluşturmaktadır. TÜBİTAK Bilgem Siber Güvenlik Enstitüsü tarafından hazırlanan "Bilgimi Koruyorum" çevrimiçi eğitim sistemi (http://www.bilgimikoruyorum.org.tr/, 2020) incelendiğinde eğitimin 4 konu başlığı altında 13 konudan oluştuğu görülmüştür. Eğitim sistemi öneriler bölümünde katılımcıların kendi planlarını kendi ihtiyaçlarına göre düzenlemeleri ve eğitim içeriği üzerinde bu plana göre

ilerlemeleri bildirilmiştir. Eğitim başlıklarından oluşturulan kelime bulutu Şekil 1 üzerinde gösterilmiştir.

Şekil 1. Bilgi güvenliğine yönelik Eğitim başlıklarından oluşturulan kelime bulutu

Örnekleri verilen ve muadilleri bulunabilecek olan çevrimiçi eğitim sistemleri, biri hepsine uyar mantığı ile hazırlanmış olup; son kullanıcının bireysel olarak neye ihtiyacı olabileceğini hesaba katmadan oluşturulan sistemler olarak karşımıza çıkmaktadır. Öğretim teknolojisi, insan performansını artırmak ve öğretme işlemini daha kolay, etkili ve verimli hale getirmek için kaynakların ve süreçlerin oluşturulması ve kullanılması ile ilgilenen bir alandır. Bu alan bir problemin çözümü konusunda geliştirilen ve kullanılan yöntem, teknik ve araçları kapsayan "teknolojiler, öğrenmeyi açıklamaya çalışan "öğrenme yaklaşımları" ve bu yaklaşımlara uygun öğretim ortamları tasarlamayı amaçlayan "öğretim sistemleri geliştirme" bileşenleri ile ilgilenmektedir (Çakır, Çebi ve Özcan, 2013). Öğretim teknolojileri alanı kavramsal ve içerik olarak değişim ve gelişmeler göstermiştir. Paralel bir şekilde zaman içerisinde alan üzerinde çeşitli eleştiriler yapılmıştır ve yapılmaktadır. Öğretim teknolojilerine yapılan eleştirilerden biri alanda pratiğe dökülen sonuç odaklı araştırmaların az olması konularında gözlenmektedir. Schwier, Campbell ve Kenny (2004) öğretim tasarımı kuramsal modellerini tanımlayan birçok çalışmanın öğretim teknologlarının yapmış olduğu pratiğe dökülmüş işlemlerden

kaynaklanmadığını bu sebeple öğretim tasarımı teorilerinin pratikte zemini olmadığını vurgulamışlardır. Reeves (2000), çoğu öğretim teknoloğunun bir bilimsel alanın temellerinin daha iyi anlaşılması için yapılan "temel" araştırma çalışmalarını, bireylerin, grupların karşı karşıya kaldıkları problemleri çözmek için yapılan "uygulamalı" araştırma çalışmalarına tercih ettiklerini belirtmiştir. Ayrıca bazı öğretim teknologlarının pratikte bir değeri olup olmadığına bakmaksızın temel araştırma çalışmaları yapmakta ısrar ettiklerini, buldukları sonuçları da başkalarının uygulayacağını düşündükleri şeklinde iğneleyici bir eleştiride bulunmuştur. Dillon ve Gabbard (1998), ERIC ve PsycLIT veri tabanından eriştikleri 1990 ve 1996 yılları arasında yayınlanan öğrenme çıktıları üzerinde hiper medya ve öğrenme konulu 500 çalışma üzerinde yaptıkları çalışmada sadece 118 çalışmanın hiper medyanın eğitim üzerindeki etkisini araştıran nicel çalışma olduğu ve bunlardan sadece 30 tanesinin yayınlandığını belirtmişlerdir. Teknolojinin yenilikçi bir yaklaşımla sınıflarda kullanılması alanındaki çalışmaların avantajlar sunacağı ancak bu tarza çalışmaların bulunmadığı şeklinde eleştirilerde bulunmuşlardır.

Richard ve Stephen (1998), öğrenenlerin sahip olduğu farklı kişilik özellikleri, öğrenme biçimleri, bilgiyi işleme biçimleri ve bilgiyi elde etme konusunda yaptıkları farklı tercihlerin, aynı öğrenme ortamını kullanırken farklı öğrenme gereksinimlerinin oluşmasına sebep olduğunu vurgulamışlardır. Eklund ve Brusilovsky (1999), çevrimiçi öğrenme uygulamaları ile ilgili olarak yapılan eleştirilerin başında, sistemlerin, öğrenenlerin kişisel ihtiyaçlarına uyarlanabilme yeteneklerinin olmamasını göstermişlerdir. Uyarlanabilir öğretim sistemleri; "öğrenenlerin tercihleri, bilgi, ilgi ve hedefleri göz önüne alınarak bir modelinin oluşturulması ile öğretim ortamının bu modele göre yapılandırılması ve her bir öğrenen için öğretimin kişiselleştirilmesi ile ortaya çıkan; öğrenenin tarama alanını sınırlayıp ona en uygun bağlantıları önererek, yararlanabileceği farklı ve özel bilgi parçalarına erişmesini sağlayarak destekleyen hiper ortam" olarak tanımlanabilir (Brusilovsky, 1996). Alanyazında vurgulanan bireysel bilgi güvenliğine yönelik olarak farklı bireysel özelliklere sahip olan kişilerin farklı davranışlar sergilemesi onlara verilecek eğitimin de uyarlanabilir olmasının önemini açığa çıkarmaktadır.

Bilgisayar ve iletişim teknolojilerinde yaşanan gelişmelerle insanların hatta belirtilen teknolojilerin bizzat kendilerinin her zaman her yerde mantığıyla veri üretme kapasitelerini yükseltmesi ile oluşturulan veri miktarını ve veriyi işleme kapasitesini artması ile veri

madenciliği işlemleri, veriden bilgi keşfi amacıyla astronomiden biyolojiye, finanstan pazarlamaya, sigortadan tıbba birçok alanda uygulanmaya başlamıştır. Çevrimiçi öğrenmede uygun öğretim yönteminin seçilmesi, farklı öğretim programlarının formüle edilmesi için, öğrencilerin bireysel karakterleri, farklı altyapıları, öğrenme kabiliyetleri ve bilgi düzeylerine uygulanabilecek veri madenciliği çalışmaları geliştirilmektedir (Gao ve Zhang, 2018). He (2013) yapmış olduğu çalışmasında ders içerisindeki etkileşimlerinin kayıt altına alındığı çevrimiçi öğretim sistemi üzerinde öğrenen ve öğreten arasında geçen yazışmaları veri madenciliği işlemlerine tabi tutmuş, öğrenenlerin öğretene ve kendi aralarında sordukları soruları sınıflandırmış ve oluşan sınıfların öğrenenlerin sınav notları ile ilişkilerini tespit etmiştir. Machado, Lima, Maciel ve Rodrigues (2016) çalışmalarında, katılımcıların tartışma forumunda yapmış olduğu etkileşimleri veri madenciliği işlemleri ile kümelendirilmiş, her bir kümenin dersi planlamak ve farklı öğrenci özelliklerinin öğrenme süreçlerini anlamlandırmak için kullanılabileceği belirtilmiştir. Preidys ve Sakalauskas (2010), çevrimiçi öğrenme sisteminde öğrenciler tarafından oluşturulan iz kayıtları üzerinde veri madenciliği işlemleri uygulayarak öğrencilere kişiselleştirilmiş öğrenme etkinlikleri ve materyalleri sunumu konusunda karar alma imkânı sunmuşlardır. Algarni (2016) eğitim amaçlı veri madenciliğinin riskli grupta yer alan öğrenenlerin belirlenmesi, farklı öğrenen kümelerinin öğrenme ihtiyaçlarındaki önceliklerin belirlenmesi, kurumsal performans göstergelerinin değerlendirilmesi, eğitim kurumu kaynaklarının etkili bir şekilde kullanılması ve müfredat geliştirilmesi gibi birçok alanda kullanımının faydalı olacağını belirtmiştir. Bireysel bilgi güvenliği konusunda yapılan çalışmaların genellikle katılımcılardan alınan "kişinin kendi beyanatına dayalı" bilgilerden oluşması probleminin davranışa yönelik olarak bilgi toplamanın zorluğundan kaynaklanması ile birlikte, hem öğrenen davranışı hakkında yanlış bir değerlendirme yapılmasına sebep olacak hem de bu yönde oluşturulacak uyarlanabilir öğrenme ortamının etkinliğini azaltacaktır. Naqvi (2015) eğitsel içerikteki verilerde saklı olan örüntülerin keşfedilmesi ile öğrencilerin öğrenme davranışlarının analiz edilmesi, gelecekteki durumlarının tahmin edilmesi konusunda sağladığı katkıyı vurguladığı üzere, öğrenen davranışlarının tahmin edilerek kendisine uyarlanabilir bir çevrimiçi öğrenme içeriği sunmak için veri madenciliği işlemlerinin işe koşulmasının faydalı olacağı değerlendirilmektedir. Bu çalışmada bilgi güvenliği konusunda, bireylerin korumacı ve riskli davranışlarına ilişkin dillendirdikleri ve

hayata geçirdikleri davranışların farklı olmasına sebep olan, bireyleri birbirinden ayıran bireysel özelliklerine göre uyarlanabilir çevrimiçi öğrenme ortamı nasıl geliştirilmelidir? sorusu araştırmanın temel problemini oluşturmaktadır.

Çalışmanın Amacı

Bu çalışmada, bireyleri birbirinden ayıran demografik, sosyo-demografik, kişilik özellikleri, tehlike algıları ve suça maruziyet durumları ile bilgi güvenliğine yönelik korumacı ve riskli davranışlarına ilişkin dillendirdikleri ve hayata geçirdikleri davranışlar arasındaki ilişki incelenerek uyarlanabilir öğrenme ortamı geliştirilmesi amaçlanmıştır. Bu amaç doğrultusunda aşağıdaki araştırma sorularına cevap aranmıştır.

1- Bilgi güvenliği konusunda bireysel özellikler, niyetler ve davranışlar arasında nasıl bir ilişki vardır?
   a. Bilgi güvenliği konusunda demografik özellikler niyetleri nasıl etkilemektedir?
   b. Bilgi güvenliği konusunda kişilik özellikleri niyetleri nasıl etkilemektedir?
   c. Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin demografik özellikleri arasında anlamlı bir ilişki var mıdır?
   d. Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin sosyo-demografik özellikleri arasında anlamlı bir ilişki var mıdır?
   e. Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin kişilik özellikleri arasında anlamlı bir fark var mıdır?
   f. Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin tehlike algıları, suça maruz kalma durumları, riskli davranış özellikleri ve korumacı davranış özellikleri arasında anlamlı bir fark var mıdır?
   g. Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin yazma hızları ve dikkatleri arasında anlamlı bir fark var mıdır?
2- Bilgi güvenliği eğitimine yönelik olarak geliştirilen uyarlanabilir çevrimiçi öğrenme ortamı nasıl olmalıdır?

a. Uyarlama nasıl gerçekleştirilmelidir?
b. Öğrenen modellemesi nasıl yapılmalıdır?

3- Bilgi güvenliği eğitimine yönelik olarak geliştirilen uyarlanabilir öğrenme ortamı hakkında konu alanı uzmanlarının görüşleri nelerdir?

Çalışmanın Önemi

Bilgi güvenliği konusunda sistemleri istismar eden unsurlar arasında virüsler, zararlı yazılımlar, spam epostalar, tuş kaydediciler vb. tehditler sıralanabilir. Ancak sosyal mühendislik saldırıları insanların zafiyetlerinden faydalanarak gerçekleştirilen semantik Kumaraguru (2009) saldırılardır. Alanyazında ve pratik yaşantıda üzerinde çalışılan teknik düzeydeki önlemlerin yüzde yüz korunma sağlayamadığı görülmektedir. Akıllı telefon kullanıcısı olup da günlük işlemlerini bu cihazlar üzerindeki internet bağlantısını kullanarak gerçekleştiren tüm bireyler sosyal mühendislik saldırılarına maruz kalmaya adaydırlar. Bu sebeple son kullanıcıların konu üzerindeki farkındalıkları çok önemlidir.

Genel olarak ilgili kamu kurum ve kuruluşları ve üniversiteler tarafından yapılan farkındalık eğitimleri, seminerleri, konferanslar, kamu spotları ve dağıtılan el broşürleri ile bireylerde farkındalık oluşturulmaya çalışılmaktadır. Ulaşılabilecek kitlenin büyüklüğü, zamandan ve mekândan bağımsız erişim, gelişen teknoloji ile paralel olarak değişen tehditlere karşı anında yapılabilen içerik güncellemeleri avantajları ile bu çalışmalardan çevrimiçi öğretim sistemleri aracılığı ile gerçekleştirilen çabalar önem arz etmektedir. Ancak konu hakkında yayında bulunan çevrimiçi ortamların "tek beden hepsine uyar" mantığıyla hazırlanmış olması çevrimiçi öğretim ortamlarının geneli için geçerli olan problemleri de beraberinde getirmektedir. Bu kapsamda uyarlanabilir çevrimiçi öğretim sistemleri öğrenene özgü çözümler sunmaktadırlar. Bilgi güvenliği eğitimi kapsamında gerçekleştirilen mevcut çalışma; öğrenenlerin farklı bireysel özellikleri doğrultusunda çalışan uyarlanabilir yapısı ile zaten yapısı itibarı ile de bilgi güvenliğine karşı oluşan tehditlere bireysel farklı özellikleri sebebiyle maruz kalan veya kalma ihtimali olan bireylere çevrimiçi bir öğrenme platformu sunmaktadır.

Alanyazında sonuçlarının kişiselleştirilmiş, uyarlanabilir öğretim sistemleri konusunda kullanılabileceğini belirtilen, bilgi güvenliği konusunda çalışmalar bulunmaktadır (Parsons vd.

(2017); McCormac vd. (2017); Öğütçü (2010); Egelman ve Peer (2015) vb.). Ancak belirtilen çalışmalar "kişinin kendi beyanına dayalı" olarak adlandırılan ölçekler yardımıyla yapılıyor olmasından dolayı birey davranışlarının söylemleriyle aynı doğrultuda olup olmayacağı konusunda bilgi verememektedir. Dolayısıyla bu temel üzerine kurulacak uyarlama çalışmaları da ancak temel kadar sağlam olabilecektir. Mevcut çalışma ile bireyin bilgi güvenliği hakkındaki söylemleri, gösterdiği davranışları ve bireysel özellikleri veri madenciliği ve makine öğrenmesi işlemlerine tabi tutularak, belli bir bilgi güvenliği konu başlığı üzerinde ne şekilde bir davranış gösterebileceği konusunda tahminde bulunulmuş ve kendisine bu doğrultuda kişiselleştirilmiş bir çevrimiçi eğitim içeriği sunulmuştur. Alanyazında bireysel bilgi güvenliği üzerinde yapılmış tek örneği oluşturmasının yanında, mevcut çalışmanın çevrimiçi öğretim sistemleri üzerinde yapılacak olan veri madenciliği ve makine öğrenmesi uygulamaları açısından rehber niteliğinde olacağı düşünülmektedir. Ayrıca çalışma yöntemi farklı konu alanlarında tekrarlanarak benzer uygulamaların geliştirilmesine yardımcı olacağı gibi çalışmanın sonuçları ise benzer uygulamaların geliştirmesine ön olacaktır.

Kuram ve uygulamanın eş zamanlı olarak yürütüldüğü bu çalışmada hem alanyazında hem de uygulamada eksikliği düşünülen sıralı durumların tamamlanacağı veya tamamlanmasına ön olacağı müşahede edilmektedir. Bu kapsamda;

- Bilgi güvenliğine yönelik, insan faktörünün merkeze alındığı çözümlerin sayıca az olması,
- Bilgi güvenliğine yönelik, insan faktörünün merkeze alındığı çalışmaların "kişinin kendi beyanatına dayalı" olarak adlandırılan ölçekler yardımıyla yapılıyor olmasından dolayı birey davranışlarının söylemleriyle aynı doğrultuda olup olmayacağının belirlenememesi,
- Bilgi güvenliği konusunda incelenen çevrimiçi öğrenme ortamlarının herhangi bir kullanıcı kaydı alıyor olmasına bakılmaksızın, kişisel ihtiyaçları göz ardı ederek var olan tüm konuları öğrenene sunuyor olmasından dolayı çalışmanın gerçekleştirilmesi gereklilik oluşturmuştur.

Varsayımlar

Bu çalışmada aşağıdaki varsayımlar temel alınmıştır;

- Katılımcıların anketteki cevapları kişisel bilgi, görüş ve eğilimlerini yansıtmaktadır.

- Katılımcıların uygulama üzerindeki davranışları kendi bireysel yetkinliklerini yansıtmaktadır.
- Uygulama üzerinde geçen sürede kontrol altına alınamayan değişkenler katılımcıları benzer şekilde etkilemiştir.

Sınırlılıklar

Mevcut çalışmada aşağıdaki sınırlılıklar yaşanmıştır;

- İki aşamadan oluşan çalışma her iki aşamaya da dâhil olan katılımcı verileri ile gerçekleştirilmiştir.
- Çalışma kapsamında kullanılan bilgi güvenliğine dair korumacı ve riskli davranış ölçekleri toplam 40 maddeden oluşmaktadır. Katılımcıların bilgi güvenliğine dair söylemleri ve gerçek davranışlarının incelendiği çalışmada, alınan uzman görüşleri sonrasında bir web sitesinin kullanımıyla, davranış olarak ölçülebilecek ölçek maddeleri belirlenmiştir. Makine öğrenme algoritmaları sadece belirlenen bu 11 madde üzerinde gerçekleştirilmiştir.
- Çalışma kapsamında yapılan analizlerde demografik özelliklerden olan eğitim düzeyi bir girdi olarak kullanılmıştır. Veri toplama aşamasına katkı sağlayan katılımcıların %48,3'ü lisans eğitim düzeyinde iken %1,9'u ilköğretim mezunu, %4'ü ise doktora eğitim düzeyindedir. Çalışma başlangıcında amaçlanan, her eğitim düzeyinden homojen olarak dağılmış katılımcı sayısına ulaşılamamıştır.
- Çalışma kapsamında kullanılan, toplam 40 maddeden oluşan bilgi güvenliğine dair korumacı ve riskli davranışlar sınıflandırılarak, bir web sitesi kullanımıyla ölçülemeyecek olan davranışların da tahmin edilebilmesi amaçlanmıştır. Ancak görüşüne başvurulan uzmanlar sınıflandırma konusunda bir mutabakata varamamışlardır. Bu sebeple çevrimiçi öğretim içeriği, bir web sitesinin kullanımıyla, davranış olarak ölçülebilecek 11 ölçek maddesi hakkında oluşturulmuştur.
- Oluşturulan öğretim içeriği bilgilendirici niteliktedir. Konu kapsamında bir senaryo, animasyon vb. oluşturulmamıştır.
- Prototip olarak hayata geçirilen öğrenme ortamında kullanılan eğitim içerikleri açık kaynaklardan derlenerek hazırlanmıştır. Bu sebeple, özellikle video içerikleri açık

kaynaklardan derlenirken ses, görüntü kalitesi, uzunluk vb. konularında uyumluluk sağlanamamıştır.

- Çalışma kapsamında prototip olarak hayata geçirilen öğrenme ortamı büyük ekranlı sistemlerde (dizüstü veya masaüstü bilgisayarlar vb.) kullanılmak üzere tasarlanmıştır. Çalışma sonucunda farklı ekran büyüklüğüne sahip cihazlar üzerinde denemeler yapıldığında içeriğin okunmasında zorluklar, yapılan tasarımda kaymalar oluşabildiği fark edilmiştir.
- Çalışma kapsamında toplanan veriler ışığında makine öğrenmesi algoritması çalıştırılarak modelleme yapılmış ve süreç tamamlanmıştır. Oluşturulan kurallar alınacak yeni verilerle yeniden güncellenmemektedir.

Tanımlar

a. **Uyarlanabilir Öğrenme Ortamı:** Öğrenenlerin ilgi, hedef ve tercihlerini bir model oluşturmak için kullanan, oluşturulan bu model ile öğrenme ortamını her farklı öğrenci için kişiselleştiren öğrenme sistemleridir (Brusilovsky, 1998).

b. **İçeriğin Uyarlanması:** Öğrenme ortamında sayfaların içeriklerinin, sunum şeklinin öğrenenin farklı özellikleri göz önüne alınarak oluşturulmasıdır (Brusilovsky ve Pesin, 1994)

c. **Makine Öğrenmesi:** Var olan bir problemi, o probleme ait olan verileri kullanarak modelleyen algoritmaların genel adlandırılmasıdır (Atalay ve Çelik, 2017).

d. **Algoritma:** Kendisine verilen talimatları ve görevleri hızlı bir şekilde gerçekleştirebilen bilgisayarların uyguladıkları, açık bir şekilde tanımlanan ve birbirini takip eden işlem adımlarıdır (Aytekin, Çakır, Yücel ve Kulaözü, 2018).

e. **Protokol:** Yazılım veya donanım arasında gerçekleştirilen iletişim sürecinde verilerin alınıp verilmesinin bir düzen içerisinde yapılmasını sağlayan kurallar dizisidir.

f. **Web Uygulaması:** Lokal olarak bilgisayarda tutulmak yerine uzak sunucular üzerinde çalışan yazılımlardır (Jazayeri, 2007).

g. **URL:** Bir ağ üzerinde bulunan web kaynağına erişmek için kullanılan referans metindir. (Wikipedia, 2020)

h. **SSL:** Ağ üzerinden yapılan iletişim için güvenlik sağlama amaçlı hazırlanmış bir iletişim protokolüdür (Thomas, 2000).

i. **Geçici İnternet Dosyası:** Bir kullanıcının bir web sitesini tekrar ziyaret ettiğinde, web sitesinin daha kolay görüntülenmesini sağlayan tarayıcı belleğine kaydedilmiş web sitesine ait dosyalardır (Park, Jang ve James, 2017).

BÖLÜM II

KAVRAMSAL ÇERÇEVE

Bu aşamada bilgi güvenliğinin alan yazında geçen tanımı, bilgi güvenliğine yönelik tehditler, bilgi güvenliğinin nasıl sağlandığı ve yönetiminin nasıl yapıldığı, konu üzerinde verilen eğitimler açıklanmıştır. Ayrıca bilgi güvenliğine yönelik yapılan çalışmalarda kullanılan farkındalık ölçekleri ve bireylerin bilgi güvenliğine yönelik davranışlarını etkileyen bireysel farklılıklar da ele alınmıştır.

Bilgi Güvenliği

Teknoloji alanında yaşanan gelişimler sonucu oluşan tehditler bireyleri, kurum ve kuruluşları hatta devletleri derinden etkilemiş (Çintiriz ve Durak, 2014) ve bu tehditlere karşı alınabilecek önlemleri de kapsayan siber güvenlik veya bilgi güvenliği kavramları önemini artırmıştır. Bilgi güvenliği, bir varlık olarak verilerin veya bilgilerin, elektronik ortamlarda saklanması veya taşınması sırasında bütünlüklerinin muhafaza edilip, yetkisiz erişimlerden korunarak işlenebilecek halde tutulmaları çabalarının tümü olarak tanımlanmıştır (Canbek ve Sağıroğlu, 2006). Bilgisayar ağlarını, bilgisayarları, bilgisayar uygulamalarını ve verilerini G-B-E (Gizlilik – Bütünlük – Erişilebilirlik) (CIA: confidentiality, integrity, accessibility) üçlemesi doğrultusunda korumak için uyguladığımız tüm işlemler ve uygulamalar olarak da tanımlanmaktadır (Carstens, Malone, DeMara ve McCauley-Bell, 2004). Türkiye 2016-2019 Ulusal Siber Güvenlik Stratejisi Eylem Planında ise bilgi güvenliği "siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunması, bu ortamda işlenen bilgi/verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınması, saldırıların ve siber güvenlik olaylarının tespit

edilmesi, bu tespitlere karşı tepki mekanizmalarının devreye alınması ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi" olarak tanımlanmıştır. Tanımlardan da görüleceği üzere bilgi güvenliği kavramı daha çok bilişim sistemlerinin ana ögesi olan bilgi üzerinden gerçekleştirilmektedir. G-B-E modeli bilgi güvenliği konusunda genel üç bileşen olarak kabul görmüştür (Başaran, 2016). Goncalves vd. (2013) bilgi güvenliği için ülkelerin ve işletmelerin verilerin gizliliği, bütünlüğü ve erişilebilirliğini garanti altına almak için standartlar, araçlar ve kılavuzlar oluşturduğunu belirtmiş; gizliliği yetkisiz kişilerin bilgiye hiçbir zaman erişememesi veya eriştiği bilgiyi anlamlandıramaması, erişilebilirliği yetkili kişilerin bilgi için istekte bulunduklarında kurallardan veya herhangi bir hatadan dolayı reddedilmemesi, bütünlüğü bilginin herhangi bir şekilde bozulmaması veya değiştirilmemesi olarak tanımlamışlardır. G-B-E modelinin özellikleri ISO (International Organization of Standardization, Uluslararası Standartlar Teşkilatı) 17799'da da açıklanmıştır (Reid ve Gilbert, 2010).

Bilgi Güvenliğine Yönelik Tehditler

Budapeşte - Sanal Ortamda İşlenen Suçlar Sözleşmesi'nin (TBMM, 2014) "Bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik suçlar" başlığı ile siber ve bilgi güvenliği tanımlamalarının paralellik gösterdiği açıktır. İlgili sözleşmenin bahsi geçen başlığı altında tanımlanan;

- Yasa dışı erişim (…bir bilgisayar sisteminin tamamına veya bir kısmına haksız yere gerçekleştirilen erişim…) maddesi bilgi güvenliğinin gizlilik bileşenine
- Verilere müdahale (...bilgisayar verilerine haksız yere zarar verilmesi, silinmesi, tahrip edilmesi, değiştirilmesi...) maddesi bütünlük bileşenine
- Sisteme müdahale (…bir bilgisayar sisteminin işleyişinin haksız yere engellenmesi…) maddesi erişilebilirlik bileşenine karşı gerçekleştirilen tehditler olarak görülmektedir.

Jouini, Rabai ve Aissa (2014) bilgi güvenliğine dair her tehdidin sadece bir kategoride yer aldığı, tüm olasılıkları içeren, kesin, çalışmacıdan bağımsız tekrarlanabilir, akla ve mantığa uygun, çoğunluk tarafından kolayca kabul görebilecek ve kullanışlı olarak nitelendirdikleri tasniflemede, sistem üzerinde zarar verici etkisine göre şu ayrımı kullanmışlardır:

- Bilgilerin yok edilmesi
- Bilgilerin bozulması
- Bilgilerin açığa vurulması
- Bilgilerin kullanımının engellenmesi
- Kullanıcı ayrıcalıklarının yükseltilmesi
- İllegal kullanım olarak genel bir sınıflandırma yapmışlardır.

Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı tarafından oluşturulan "Tehdit Durum Raporu" (European Union ve Agency for Network and Information Security, 2019) ise bilgi güvenliğine yönelik tehditleri açık kaynak ve ticari sağlayıcılardan elde ettiği bilgiler üzerinden yaptığı analiz ile en dikkat çekici olaylara göre yapılan tasniflemeyi şu başlıklar altında incelemiştir:

- Zararlı Yazılım (Malware) : Rapor edilen veri ihlali olaylarının %30'luk bir kısmında dahli olan tehdit, çalıştırılabilir bir dosya olarak veya çalıştırılamayan bir dosya üzerinde betik işlemlerle bulunduğu sisteme çeşitli şekillerde zarar veren yazılımlardır.
- Web-tabanlı Ataklar (Web-Based Attacks) : Kurbanı veya hedefi tuzağa düşürmek için tarayıcı, web servisi enjeksiyonu gibi web sistem ve servislerini ana satıh olarak kullanan tehditlerdir.
- Web Uygulaması Atakları (Web Application Attacks): Ortak kullanılan servisler dolayısıyla web-tabanlı ataklarla bazen örtüşen web uygulaması atakları, web üzerinde bulunan uygulamaların programlama ara yüzlerini, çalışma zamanı ortamlarını veya hizmetlerini kötüye kullanarak zayıflıklarını direk veya dolaylı olarak sömürme çabalarıdır.
- Oltalama Saldırıları (Phishing): Alıcının cezbedilmesi ve "yemi alması" için sosyal mühendislik tekniklerini kullanan mesajların hazırlama mekanizması olarak tanımlanmıştır. Saldırı alıcılara gönderilen epostalar veya mesajlar ile zararlı bir ekin açılması, güvenli olmayan bir web adresinin tıklanması, yasal gibi görünen bir web sayfasına banka vb. bilgilerinin yollanması sonuçlarını sağlamaya çalışmaktadır.
- Dağıtık Servis dışı Bırakma Saldırıları (Distributed Denial of Service: Hemen her işletmeyi veya organizasyonu hedef alan, ağ veya altyapı üzerinde sistemin cevap veremez hale gelmesini sağlayan saldırılardır.

- İstenmeyen Eposta (Spam): Kullanıcılara talep etmedikleri mesajları göndermek sürekli göndermek için eposta ve mesajlaşma teknolojilerinin kötüye kullanılmasıdır.
- Zombi Ağı (Botnet) : Çeşitli şekillerde enfekte edilmiş bilgisayarlardan oluşan ağdır. Ağdaki bilgisayarlar genel olarak zararlı yazılım veya istenmeyen eposta dağıtımı veya DDOS atakları oluşturmak için kullanılırlar.
- Veri İhlalleri (Data Breaches) : Siber tehdit alanında kendi başına bir tehdit olarak algılanmayan ancak kişisel, medikal vb. bilgilerin başarılı bir şüpheli girişim sonunda yitirilmesi sonucunu doğuran girişimlerdir.
- İçeriden Tehdit (Insider Threat): Bir şirkette veya organizasyonda organizasyonun dijital altyapısına erişimi veya konuda bilgisi olan, halen çalışıyor veya daha önce çalışmış bir görevli, iş ortağı veya tarafın bilerek veya bilmeyerek bu bilgisini veya erişimini kötüye kullanmasıdır.
- Fiziki Zarar/Çalınma/Kayıp (Physical Damage/Theft/Loss): Her ne kadar gerçek siber tehditler olmasa da veri kaybına sebep olan; hassas verileri içeren cihazların zarar görmesi, çalınması veya kaybolması ile sonuçlanan durumdur.
- Bilgi Sızdırma (Information Leakage): Bilgi teknolojileri altyapısında muhafaza edilen bilgilerin genellikle teknik bir hata veya yanlış bir yapılandırma sonrasında istemsizce açığa çıkmasıdır.
- Kimlik Hırsızlığı (Identity Theft): Bireylerin doğru bir şekilde tam profillerinin çıkarılarak onlar adına işlem yapılabilmesi için banka hesabı, bağlantıları gibi yasal veya kişisel kayıtlarının çalınması işlemidir.
- Gizli Kripto Para Madenciliği (Cyrptojacking): Kurbanın haberi ve izni olmadan, işlemci gücünün kripto para madenciliği işlemlerinde kullanılmasına yönelik bir ataktır.
- Fidye Yazılım (Ransomware): Bu atağı yapan kişinin bir dosyanın veya cihazın esas sahibi tarafından erişilmesini engelleyerek, sahipliği geri vermek için fidye talep etmesiyle sonuçlanan atak türüdür.
- Siber Espiyonaj (Cyber Espionage) : Genellikle kritik ve stratejik altyapıları hedef alan bu atak ile gizli ticari, jeopolitik, istihbarat vb. bilgilerin çalınması ile sonuçlandırılan atak türüdür.

Berger ve Jones (2016) ise bireyleri, kurum ve kuruluşları, devletleri etkileyen en yaygın tehditleri pratikte şu başlıklar altında incelenmiştir:

- DDOS Saldırıları: Zombi adı verilen bilgisayarlar tarafından bir web sitesi/ web sunucusuna sistemin cevap veremeyeceği kadar istek göndererek servisin çalışmasını engellemeye yönelik saldırı tipidir.
- Zararlı Yazılımlar: Genellikle eposta üzerinden ek olarak veya bir bağlantı adresi olarak son kullanıcıya gönderilen ve sistemin çalışmasını engelleyecek, bozacak veya izinsiz erişim yetkisi sağlayacak şekilde kodlanmış yazılımlardır.
- Şifre Saldırıları: Kullanıcının herhangi bir sisteme erişim için kullandığı şifrenin hazır bir kütüphane kullanılarak veya kişisel bilgilerinden yararlanıp tahmin etme yoluyla kırılmaya çalışıldığı saldırıdır.
- Oltalama Saldırıları: Genellikle eposta veya mesajlaşma uygulamaları üzerinden gönderilen bir bağlantı adresi ile erişilen, banka, sosyal medya hesaplarına ait web sitelerinin birebir taklit edilmiş tasarımlarını içeren ve kullanıcının hesap şifresini, bankacılık bilgilerini vb. çalmayı amaçlayan saldırıdır.
- Sosyal mühendislik: Bazı kaynaklarda saldırı başlığı altında tanımlanırken bazı kaynaklarda ise yukarıda bahsi geçen tehditlerin mümkün hale getirilmesi için bir yöntem olarak tanımlanmıştır. Mills (2009) sosyal mühendisliği kişisel bir etkileşimin merkezde yer aldığı, saldırganın telefon görüşmesi, müşteri kılığına girme, kurbanla bağlantısı olabilecek bir kişi gibi davranma şeklinde sosyal durumları kullandığı, bilgi güvenliğine karşı yapılan saldırılar olarak tanımlamıştır. Rössling ve Müller (2009) ise yaptıkları çalışmalarında sosyal mühendisliği yetkili kişinin haberi olmadan kritik olarak tanımlanan bir veriye erişmek için kullanılan bir yöntem olarak belirtmişlerdir. Dimkov, Van Cleeff ve Hartel (2010), amacı bir kurumdaki belirli bilgileri ele geçirme veya değiştirme olan sızma testini yapan uzmanların sosyal mühendisliği testin yapıldığı kurum çalışanları ile onları aldatmaya yönelik olarak iletişime geçtikleri bir yöntem olarak tasvir etmişlerdir.

İster bir siber tehdit olarak isterse de siber saldırıları gerçekleştirmek için bir yöntem olarak algılansın sosyal mühendislik son kullanıcıların en çok karşılaştıkları unsur olarak karşımıza

çıkmaktadır. Teknolojilerin güvenlik üzerine çalışmaları arttıkça olası teknik zafiyetlerin kullanılması veya sömürülmesi zorlaşacağından saldırganların insanın zayıflıklarını kullanarak faydalanma eğilimleri artmıştır (Şahinaslan, Kantürk, Şahinaslan ve Borandağ, 2009) Dimensional Research (2011) altı farklı ülkede gerçekleştirdiği araştırmada katılımcıların %43'ünün en az bir kere sosyal mühendislik saldırılarına maruz kaldıklarını ve bu saldırıların %48'inin her birinde yaklaşık 25.000 dolar değerinde zarar açıklandığını bildirmiştir. Sosyal mühendislik saldırıları daha az çabayla çok daha başarılı sonuçlar elde edilmesine olanak sağlar bir durumdadır. Güvenlik programlarında en zayıf halkanın insan olması ile saldırganlar sistemin açığını bulmak yerine insanların açığını aramaktadırlar. Verizon (2012), Veri İhlali Araştırma Raporuna göre yapılan tüm ihlallerin %7'lik bir kısmı sosyal mühendislik içermektedir ve bu oran sadece büyük organizasyonlar için %22'dir. Verizon (2016) Veri İhlali Araştırma Raporuna göre ise korsanlık (hacking) etkinliklerinin 2011 yılı sayıları ile benzer olduğu ancak sosyal tehditler kategorisinin yükselen bir trend olduğu belirtilmiştir.

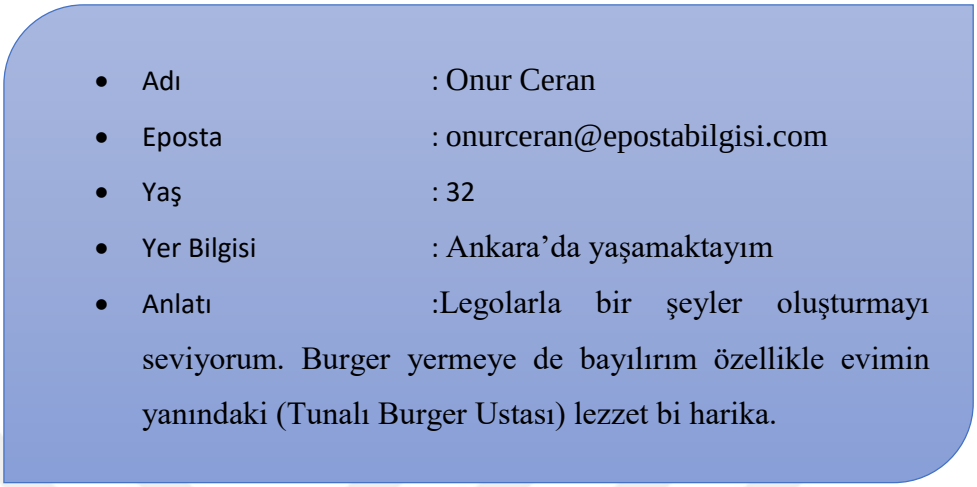
Akıllı telefonların yüksek seviyede bilgi işleme kapasiteleri, günlük yaşantımızın bir parçası haline gelmesini sağlamış; eposta, çevrimiçi alışveriş, bankacılık, fatura ödeme gibi işlemleri bu cihazlar üzerinden yapar duruma gelmemizi sağlamıştır fakat bu durum güvenlik tehlikelerini de aynı derecede artırmıştır (Omar ve Dawson, 2013). Türkiye İstatistik Kurumunun (TUİK, 2016) hazırlamış olduğu Hane Halkı Bilişim Teknolojileri Kullanım Araştırması'na göre Türkiye'de internet kullanan bireylerin %61,2 olduğu, yaklaşık olarak her 10 haneden 8 inde internet erişimi bulunduğu, hanelerin %96,9'luk kısmında cep telefonu olduğu, internet kullanım amaçları arasında ise %82,4'lük bir oranla sosyal medyanın ilk sırada yer aldığı bildirilmiştir. Dijital pazarlama ajansı We are Social'ın (2016) küresel internet ve sosyal medya kullanıcıları istatistikleri raporuna göre dünya nüfusunun %46'lık kısmının internet kullanıcısı olduğu, %31'lik bir kısmının sosyal medya kullanıcısı olduğu, %51'lik bir kısmının tekil akıllı telefon kullanıcısı olduğu, %27'lik kısmın ise akıllı telefon üzerinden sosyal medyayı kullandığı belirtilmiştir.

Sosyal medya platformları insanların gerçek veya hayali birer kimlik oluşturarak arkadaşları veya hiç tanımadıkları kişilerle arkadaşlık kurabildikleri, mesajlaşabildikleri, her konudan içerik oluşturarak seslerini duyurabildikleri araçlardır. Günümüzde Twitter, Facebook gibi sosyal

medya platformları tüm dünyada, yüksek sayıda kullanıcı tarafından kullanılmaktadır. Global olarak insanlar günün ortalama 2 saat 24 dakikası sosyal medya platformlarının kullanımı il geçirmektedir (Broadbandsearch, 2020). İnternetin ve mobil teknolojilerin bu denli erişilebilir hale gelmesi ve yaygınlaşması, sosyal medya araçlarının kullanım oranını da artırmıştır ki bu da sosyal medya platformları üzerinden sosyal mühendislik saldırılarına maruz kalma durumunu da artırmıştır. Bu durum "Kişisel olarak tanımlanabilir bilgiler" kavramının oluşmasını sağlamıştır. Kişisel olarak tanımlanabilir bilgiler gizlilik düzenlemelerinin merkezinde yer alıyor olup sosyal güvenlik numarası, ehliyet numarası, kredi kartı bilgileri, telefon numarası, eposta adresi, isim ve soy isim gibi bilgilerden oluşmaktadır. Örneğin, Şekil 2'de gösterildiği üzere bir birey hakkında verilen bilgiler anonim olabilir:

Şekil 2. Anonim bilgi örneği

Normal hayatta diğer veri kaynakları olmadığı durumlarda bu bilgiler anonim olarak kalabilir. Ancak günümüz dünyasında birçok başka veri kaynağı bulunmaktadır. Şekil 3 üzerinde gösterildiği üzere bu bilgiler bir Facebook sosyal medya hesabı üzerinden:



Şekil 3. Anonim olmayan bilgiler örneği

paylaşılabilir. Kişisel olarak tanımlanabilir bu bilgiler anonimlikten uzaklaşır (Schwartz ve Solove, 2011). K. Thomas vd. (2015), saldırganlar için sosyal ağların değerli birer veri kaynağı olduğunu, 2010 yılında bir milyonun üzerinde sahte Facebook ve Twitter hesabı üzerinden gereksiz eposta (spam) gönderildiği belirtmiştir.

Bilgi Güvenliği Yönetimi

Bireyleri, kurum ve kuruluşları, devletleri etkileyen bu tehditler karşısında çeşitli teknolojiler kullanılarak önlemler alınmaya çalışılmaktadır. Bilgiyi oluşturmaya, işlemeye, dağıtmaya ve depolamaya yarayan bilgi sistemleri, donanım ve yazılımlar ihtiva etmektedir ve bu sistemleri saldırılara karşı korumak, saldırıyı tespit etmek, incelemesini yapmak ve verileri kurtarmak için sistemler geliştirilmektedir. Denning (2003) bu önlemleri kimlik doğrulama sistemleri (şifreler, biyometrik veriler, akıllı kartlar vb.), şifreleme sistemleri (veri ve ağ iletişimi korumak için), erişim kontrol sistemleri, ateş duvarları, zafiyet tarayıcılar ve güvenlik yönetim sistemleri, denetleme ve ihlal tanımlama sistemleri, anti-virüs sistemleri, bal kovanı sistemleri, bilgisayar ve ağ inceleme sistemleri ve geri kurtarma sistemleri olarak sıralamıştır. Bıçakçı (2014) ise bilgi güvenliğini sağlamak için kurumların personelin hiyerarşik bir yapıda bilgilere erişebildiği, her kullanıcının her bilgiye istediği şekilde ulaşamayacağı, böylece sistem ve güvenliği hakkında bilgi sahibi olmayan personelin sistemin tamamını tehlikeye atamayacağı bir güvenlik politikasından söz etmiştir.

Bilgi güvenliğine dair alınan önlemleri bu alanda yapılan harcamaları inceleyerek sınıflandırmak mümkün olacaktır. Bilgi güvenliği eğitimi ve güvenlik sertifikasyonu enstitüsü SANS'ın (Filkins, 2016) yayınlamış olduğu 2016 Bilgi Teknolojileri Harcama Trendleri raporuna göre şirketler toplam bilgi teknolojileri bütçelerinin %7-%9'unu oluşturan güvenlik harcamalarını sıralanan (harcama boyutuna göre) sebepler/amaçlar dolayısıyla gerçekleştirmektedirler:

- Hassas verinin korunması
- Mevzuata uygunluk
- İhlal hadiselerinin azaltılması
- Fikri mülkiyetin korunması
- Organizasyonel stratejik planlamaya uyum
- Marka itibarını koruma
- Saldırı alanını azaltma
- Güvenlik operasyonlarının görünürlüğünü artırma
- Son kullanıcı eğitim ve farkındalığı
- Müdahale kabiliyetinin artırılması

Aynı raporun harcama yapılan araç ve teknolojiler başlığı (harcama boyutuna göre) şu şekilde sıralanmıştır:

- Erişim kontrolü ve kimlik doğrulama: Bilgi güvenliği kapsamında erişim kontrolü, kimin veya neyin bir tarafın kaynaklarını görüntüleyebileceği veya kullanabileceği hakkında izinleri belirtirken; kimlik doğrulama erişim kontrolünün bir ön koşulu olup kullanıcı-sistem-işlem üçlüsü arasında gerçekleşen, bir tarafın diğer tarafa kimliğini onaylattığı ve en yaygın kullanım tekniğinin "şifre" olduğu mekanizmadır (Sandhu ve Samarati, 1996). Eposta hizmetlerinden bankacılık işlemlerine kadar hemen her bilgi işleme ortamında yer alan erişim kontrolü ve kimlik doğrulama mekanizması, bulut teknolojilerinde (Ruj, 2012); nesnelerin interneti alanında (Liu, Xiao ve Chen, 2012) üzerinde sıklıkla çalışılan konuların başında gelmektedir.
- Gelişmiş, zararlı yazılım engelleme: Genellikle büyük ölçekli işletmelerde ve kamusal alanda kullanılmaktadırlar. Çok katmanlı savunma sistemi olarak da adlandırılan bu sistemler kütük

kayıtları (Log) gibi çok çeşitli bilgileri ağ bileşenlerinden veya sunucu ve istemcilere yüklenen ajanlar sayesinde toplayıp işleyerek savunma reaksiyonu göstermektedirler (Moon, Im, Lee ve Park, 2014). Bütünleşik güvenlik cihazı (Unified Threat Management- UTM) ismi ile bilgi güvenliği marketinde bulunan sistemler standart güvenlik duvarı fonksiyonları, uzaktan erişim, uçtan-uca sanal özel ağ (virtual private network-VPN), zararlı yazılım önleme, standart kaynak konumlayıcı (Uniform Resource Locator-URL) ve içerik filtreleme gibi özellikleri tek bir ortamda toplamaktadırlar (Kurpjuhn, 2013). Belirtilen cihazlardan beklenen minimum fonksiyon gereksinimlerinden en önemlisi saldırı önleme mekanizması (Intrusion Prevention System-IPS) olarak göze çarpmaktadır. Saldırı önleme mekanizması yukarıda sıralanan bileşenleri tekrar konfigüre ederek gelecek atakları engelleme, şüpheli paketleri ağ dışında bırakma gibi işlemleri yürüten yazılım veya donanım parçasıdır (Patel, Qassim ve Wills, 2010)

- Uç nokta güvenliği: Uç nokta bir IP (Internet Protocol Address-İnternet protokol adresi) adresi olan, bir başka cihaza veri transfer edebilen, bilgiyi işleyen veya sunan veya bir ağa veya bilgi işleme altyapısına bağlanan donanım veya yazılıma verilen addır. Uç nokta masaüstü, dizüstü, sunucu bilgisayar veya akıllı telefonlar olabileceği gibi radyo dalgası cihazları, yönlendiriciler, dağıtıcılar, ağa bağlı depolamalar veya VOIP cihazlar da olabilir (Rai ve Chukwuma, 2010). Ağa bağlı bu noktaları riskli etkinliklerden ve/veya saldırılardan koruyan sistemlere uç nokta güvenlik sistemleri adı verilmektedir. Bağımsız olarak bulunan cihazların bir ağa bağlanma kabiliyeti kazanması veya nesnelerin internetinde olduğu gibi ağda olmasıyla var olan cihazlardaki artış ciddi tehditlerin oluşma olasılığını artırmıştır (Jinnai, Inomata, Arai ve Fujikawa, 2017). Uç nokta güvenliği konusunda en büyük tehditlerden birini USB Evrensel Seri Veriyolu (Universal Serial Bus-Evrensel Seri Veriyolu) oluşturmaktadır. USB tak kullan mantığıyla çalışan, veri depolamadan kullanıcıların bilgisayarla etkileşime girebilmesini sağlayan ara yüze kadar birçok fonksiyonu olan ve fakat uç nokta sistemlerde güvenlik riski oluşturan teknoloji olarak karşımıza çıkmaktadır (Clark, Leblanc ve Knight, 2011).
- Kablosuz ağ güvenliği: Kablosuz ağ teknolojileri üretkenliği ve bilgiye erişilebilirliği artırması ile muazzam avantajlar sunuyor olmasının yanında kullanılan zayıf algoritmalar ve saldırganlara daha erişilebilir bir ortam sunması sebebiyle kablolu ağlarda bulunan tehditleri

de içinde barındıran ek tehditlere oldukça açık konumdadır (Choi, Robles, Hong ve Kim, 2008). Çevrimiçi bankacılık, kişisel eposta gibi servislerin, akıllı telefonların gün ve gün daha fazla son kullanıcı tarafından kullanılıyor olması hücresel ve wi-fi ağların kullanımını da doğal olarak artırmaktadır. Bu sebeple kablosuz ağ güvenliği konusu önemini de aynı oranda artırmaktadır (Zou, Zhu, Wang ve Hanzo, 2016).

- Veri koruma / Şifreleme: Veri sızdırma/kayıp önleme sistemleri (Data Loss Prevention-DLP) hassas verilerin sızdırılması riskini tanımlama, izleme, koruma ve azaltmaya yardımcı olan çözümlerdir. Yetkisiz kullanıcıların hassas veriye erişmelerini belirleme ve önleme gibi işlevlerinin yanı sıra özel bilgilerin kazara paylaşılmasının da önüne geçmek için kullanılmaktadır (Costante vd., 2016). Veri sızdırma/kayıp önleme sistemleri veriyi kullanımda iken (son kullanıcı hareketleri), hareket halinde iken (ağ trafiği) veya dinlenme durumunda iken (veri depolama) gözlemleyerek kayba sebep olabilecek potansiyel durumların belirlenmesi için tasarlanmış, riskleri adresleyen bir mekanizmadır (Tahboub ve Saleh, 2014). Şifreleme bu işlem için düz bir metnin girdi olarak alındığı ve yapılan matematiksel işlem sonucunda üçüncü kişilerin okusa da anlamlandıramayacağı şekilde şifreli metnin çıktı olarak verildiği çevirme işlemidir. Şifre çözme ise şifreli bir metnin anlamlandırılacak bir şekilde tekrar düz metine çevrilme işlemidir (Saxena, Kaushik ve Kaushik, 2018) Şifrelemenin, ağ teknolojilerinin gelişmesi ile birlikte bankacılık, sağlık, güvenlik gibi verinin sıklıkla hareket halinde olduğu işlemlerde kullanımı büyük önem arz etmektedir.
- Sürekli izleme: Ulusal Standartlar ve Teknoloji Enstitüsü sürekli izleme kavramını organizasyonların risk yönetimi üzerine kararlar almasını desteklemek için bilgi güvenliği, tehditler ve açıklar konusunda devam eden farkındalığının düzenlenmesi olarak açıklamaktadır (Kott ve Arnold, 2013). Tehdit alanlarının dinamik olarak artması ile meydana gelebilecek potansiyel ve yıkıcı tehdit şablonlarının belirlenmesi ve bunlara uygun tedbirlerin alınması için bilgi-işleme altyapılarının devamlı olarak izlenmesi ve risk skorlaması yapılmasını sağlayan mekanizmalardır (Awan, Burnap, Rawa ve Javed, 2015).
- Kütük kayıtları (log) yönetimi: Kütük kaydı bir sistem veya ağ üzerinde anti-zararlı yazılım, ateş duvarı, saldırı tespit ve önleme gibi güvenlik yazılım ve donanımları, sunucu, istemci veya ağ ekipmanları üzerinde koşan işletim sistemleri veya uygulamalar tarafından

oluşturulan olay kayıtlarıdır (Kent ve Murugiah, 2006). Birçok cihaz tarafından oluşturulan büyük miktardaki kütük kaydının birleştirilip dinamik bir şekilde işlenmesini kütük kayıt yönetim sistemleri gerçekleştirmektedir (Anastopoulos ve Katsikas, 2018). Tehdit yönetimi ve olay müdahalesi de yine kütük kayıtlarının analizi sayesinde mümkün olmaktadır (Madani, Reyazi ve Gaharaee, 2011). Bu konudaki en büyük zorluklardan biri organizasyonların kütük kayıtlarının doğru bir şekilde oluşturulması, toplanması, analiz edilmesi ve anlamlı bir değer oluşturulmasının yönetilebilmesidir (Jayathilake, 2012).

- Ağ görünürlüğü: Ağdan geçen trafiğin yakalaması, çoğaltması, toplaması, iletmesi ve analiz edilmesi olarak tanımlanabilir. Port aynalama/SPAN gibi geleneksel yöntemlerin kullanıldığı gibi (Rehman, Song ve Kang, 2014) imza tabanlı veya makine öğrenmesi sınıflayıcı yöntemleri kullanan araçlar da bulunmaktadır (Baskaran vd., 2019). Ağ güvenliği geleneksel olarak ağ paketlerinin analiz edilmesiyle gerçekleştirilmektedir.
- Güvenlik açığı yönetimi: Güvenlik açığı bilgisayar sistemi tasarımı, uygulaması, bakımı ve işletiminden kaynaklı güvenlik kusurudur (Wang ve Guo, 2009). Güvenlik açığı yönetimi istismar edilmesi potansiyeli olan güvenlik açıkları risklerinin en aza indirilmesiyle ilgilenen, bilgi güvenliği yönetiminin bir parçası olarak tanımlanmaktadır (Nyanchama, 2005). Güvenlik açığı yönetimi bir risk değerlendirme süreci olup, tarama sonucunda gerçekleşebilecek potansiyel bir saldırı yüzeyi hakkında bilgi verir. Bilgiler pasif, aktif veya her iki tekniğin karışımı bir yöntemle sistemden toplanarak analiz edilir (Haber ve Hibbert, 2018).
- Analitik: Bilgi güvenliğine yönelik büyük veri analizi IP adresi, epostalar, kütük kayıtları gibi yüksek miktardaki verinin analiz edilerek anlamlı bilgi oluşturulması süreci olarak tanımlanabilir. Bu bilgiler anormallikleri, tehditleri, uyarıları ve güvenlik olaylarını anlamlandırmak için organizasyonlar tarafından sıklıkla kullanılmaktadır (Dev Mishra ve Beer Singh, 2016). Toplanan ve analiz edilen bilgiler ayrıca güvenlik amaçlı öngörülerin oluşturulması, yönetim planının güncellenmesi, uygulamaya yönelik kararların verilmesi konularında da fayda sağlamaktadır (Naseer, Shanks, Ahmad ve Maynard, 2017). Etkileşimli grafiksel veri sunumu yöntemlerinin kullanıldığı görsel analiz teknikleri ise organizasyonlarda istemcilerin güvenlik seviyesi analizi, organizasyon içi tehditlerin gerçek

zamanlı belirlenmesi, güvenlik politikalarının belirlenmesi gibi pek çok sorunun çözümü için işe koşulmaktadır (Novikova, Bekeneva ve Shorov, 2017).

Bilgi güvenliği konusunda 2014 yılı harcamaları ile karşılaştırıldığında 2015 yılında belirgin bir artış olduğu belirtilmiştir. Gartner (Moore ve Keen, 2018) raporunda ise bilgi güvenliği ürünlerine ve servislerine dünya çapında yapılacak olan harcamaların 2015 yılı ile karşılaştırıldığında %7,9'luk bir artışla ulaşacağı, 2018 yılı itibariyle güvenlik duvarlarına olacak talebin artmasıyla fiyatlarının %2 veya %3 lük bir artış olacağına vurgu yapmıştır. Statista (Holst, 2020) bilgi güvenliği harcama raporunda, dünya çapında 2017 yılında yaklaşık 52 milyar dolar harcama yapıldığı, 2019 yılında ise bu miktarın yaklaşık 64 milyar dolar olduğu vurgulanmıştır. Yapılan harcamalar bilgi güvenliği yönetimi konusunda işe koşulan çabaların yukarıda sayılan teknik çözümlerden öteye gitmediğini göstermektedir.

Bilgi Güvenliği Eğitimi

Kurum ve kuruluşlar tarafından yayınlanan istatistikler ve raporlar incelendiğinde bilgi güvenliği konusunda alınmaya çalışılan tedbirlerin genel olarak teknoloji tabanlı çözümler veya kural tabanlı politikalar olduğu anlaşılmaktadır. Ancak sadece bilgi teknolojileri üzerine yapılan yatırımların insanların bilgi güvenliği suçuna maruz kalma sayısında veya kaybedilen para miktarında bir azalmayı sağlamadığı aynı istatistik ve raporlarda belirtilmektedir. Kurum ve kuruluşlar bilgi teknolojileri bütçelerinin oransal olarak yüksek bir bölümünü teknoloji ürünü araçlara harcamaktadırlar. Buna karşın bilgi güvenliğine yönelik saldırıların genel olarak bilgisiz ve izlenmeyen kullanıcıları hedef alması, bilgi güvenliği eğitiminin ne derece önemli olduğunu göstermektedir.

"Education" ve "training" kelimeleri Türkçe dilinde "eğitim" olarak karşılık bulmaktadır. Ancak bu iki kelimenin alanyazında bilgi güvenliği eğitimi için farklı kullanımları bulunmaktadır. Amankwa, Loock ve Kritzinger (2014) bilgi güvenliği konusunda oluşan farkı şu şekilde açıklamıştır:

1- Bilgi Güvenliği Eğitimi-BGE (Information Security Education-ISE): Bilgi güvenliği eğitimi (ISE) teknik ve yönetimsel parçalardan oluşmaktadır. Bilgi sistemlerinin gizlilik, bütünlük,

takip edilebilirlik ve erişilebilirliklerini kesintisiz sağlamayı amaçlamaktadır. Eğitim, güvenlik konusunda uzman kariyeri oluşturmak bireylere veya hali hazırda bilgi güvenliği profesyonellerine uygun olarak düzenlenmektedir.

2- Bilgi Güvenliği Eğitimi (Information Security Training-IST): Bir kurum veya kuruluşta çalışanların görev ve sorumluluklarına yönelik bilgi güvenliği becerileri ve bilgisi kazanması için gerçekleştirilen eğitimlerdir.
3- Bilgi Güvenliği Eğitimi (Information Security Awareness-ISA): Son kullanıcıların bilgi güvenliği konusundaki riskleri benimseyip, alınabilecek önlemlere uyum sağlayarak ona göre davranış sergilemelerini amaçlayan çabalar setidir.

Bu çalışma kapsamında bireysel farkındalık ön planda tutulmuş, profesyonellik ve organizasyonla ilişkili herhangi bir çaba ortaya konulmamıştır.

Arama motorları üzerinden ("bilgi güvenliği eğitimi", "information security education", "information security training", "information security awareness") + ("içerik", "müfredat", syllabus") anahtar kelimeleri ve kombinasyonları ile yapılan araştırma ve akabinde yapılan incelemelerde bireysel bilgi güvenliğine yönelik kapsamlı eğitim içeriğine rastlanmamıştır. Özellikle üniversitelerin bilgisayar ve yazılım mühendisliği, bilişim sistemleri gibi bilgi teknolojileri ve iletişim konularında uzman birey yetiştirmeyi amaçlayan bölümlerinde "bilgi güvenliğinin" BGE tanımına uygun müfredatların olduğu görülmektedir. Rowe, Lunt ve Ekstorm (2011) bilgi güvenliği eğitimi hususunda önkoşul olan beş ana başlığın programlama becerisi, bilgisayar ağları, veri tabanı uygulamaları, web teknolojileri ve insan bilgisayar etkileşimi olduğunu belirtmişlerdir. Knapp, Maurer ve Plachkinova (2017) yükseköğretim programları özelinde bilgi güvenliği müfredatı için dünya çapında geçerliliği olan sertifika programları (Certified Information Systems Security Professional-CISSP, Certified Information Security Manager-CISM, Certified Information Systems Auditor-CISA, Certified Ethical Hacker-CEH) ile paralel bir içeriğe sahip olacak şekilde bilgi yönetim sistemleri, uygulama geliştirme, bilgi güvenliği temelleri, ağ ve bulut altyapısı, bilgi güvenliği risk yönetimi, ağ güvenliği, fiziksel ve Operasyonel güvenlik konularının dâhil edilmesi gerekliliğini belirtmişlerdir. (Vaughn, Dampier ve Warkentin (2004)Vaughn, Missisipi Devlet Üniversitesi özelinde bilgi güvenliği eğitimi için önerdikleri müfredatta işletim sistemleri kuramları, yazılım

mühendisliği, veri tabanları, ağlar ve yapay zekâ konularının yer bulmasını belirtmişlerdir. Önaçan ve Atan (2016) dünyadaki, ABD'deki ve Türkiye'deki bilgi güvenlik eğitimlerini incelediği çalışmasında bilgi güvenliğine yönelik tehdit ve saldırıların gün geçtikçe artmasından kaynaklı olarak alanda uzman profesyonellere duyulan ihtiyacın da arttığını ülkemizde de dünyaya paralel bir şekilde bu ihtiyacı karşılamak üzere bilgi güvenliği eğitimlerinin üniversitelerin ilgili bölümlerinde verilmeye başladığını vurgulamışlardır. Dünyanın en köklü bilişim kuruluşlarından biri olan Bilgisayar Makineleri Derneği (Association for Computing Machinery-ACM) (2017) hazırlamış olduğu "Bilgi Güvenliği Eğitim ve Öğretimi için Müfredat Kılavuzu'nda" müfredatın ana konu alanlarını şu şekilde sıralamıştır;

- Veri güvenliği
- Yazılım güvenliği
- Bileşen güvenliği
- Bağlantı güvenliği
- Sistem güvenliği
- İnsan güvenliği
- Organizasyonel güvenlik

Woodard, Imboden ve Martin (2013) ise yukarıda yapılan çalışmaları; 2000'li yıllardan itibaren lisans ve lisansüstü programlar için bilgi güvenliğine yönelik müfredat geliştirilmeye ve ders programına eklenmeye çalışıldığı, bu doğrultudaki yaklaşımların ise bir bilgi teknolojisi içeriğinin üzerine "güvenlik" eklenerek gerçekleştirildiği şeklinde özetlemişlerdir.

Bilgi güvenliği eğitiminde farkındalığın ön planda olduğu (ISA) bireylerin dikkatini bilgi güvenliği konularına yönlendirerek, konudaki endişeleri fark edip önlemlere uyum sağlayarak o yönde davranış sergilemelerini sağlamak için gösterilen çabalar incelendiğinde üç farklı durum olduğu görülmektedir. Bunlardan ilki üniversite, kamu kurum ve kuruluşları, ilgili dernekler vb. oluşumların kendi paydaş topluluklarının veya katılım açık olarak düzenledikleri genel seminerler vasıtası ile katılımcıların bilgilendirildiği seçenektir. Bu seminerler belirli bir kitleyi hedefleyen ve dar bir kapsam için düzenlenmiş olabileceği gibi (örn. ailede teknoloji kullanımı ve bilgi güvenliği), herhangi bir çalışanın veya basit kullanıcının gündelik teknoloji kullanım alışkanlıklarında yapılabilecek ufak değişiklerle bireysel veya kurumsal güvenlik

seviyelerinin artırılmasına yönelik düzenlenebilmektedir. İkinci durum ise ülke çapında bilgi teknolojileri ve telekomünikasyon sektörünü düzenleyip denetleyen bakanlık, kurum veya bağlı kuruluşların veya bu kapsamdaki suçlarla mücadele eden kolluk kuvvetlerinin el broşürü, televizyon reklamı, duvar ilanları gibi elektronik veya konvansiyonel duyuru araçlarının kullanıldığı farkındalık çalışmalarından oluşmaktadır. Türkiye özelinde bilgi teknolojileri ve telekomünikasyon sektörünü düzenleme ve denetleme yetkisi Ulaştırma ve Altyapı Bakanlığı altında hizmet veren Bilgi Teknolojileri ve İletişim Kurumu iken bu kapsamdaki suçlarla mücadeleyi İçişleri Bakanlığı hiyerarşisinde faaliyet gösteren Siber Suçlarla Mücadele Daire Başkanlığı ve şube müdürlükleri sürdürmektedir. Bilgi Teknolojileri Kurumu tarafından hazırlanan hane içerisinde kullanılan internet hizmeti için çocuk profili ve yetişkin profili seçenekleri konusunda ve Siber Suçlarla Mücadele Daire Başkanlığı tarafından hazırlanan sanal klavye ve güvenli eposta kullanımına yönelik (EK 1) farkındalık oluşturulmaya çalışılan el broşürleri hazırlanmış ve vatandaşa sunulmuştur. Bu kapsamda mevcut üçüncü durumu ise ilgili kamu kurum ve kuruluşları, alanda hizmet veren dernekler, bilgi güvenliği alanında hizmet veya ürün satışı yapan özel firmalar, alanda çalışmaları bulunan eğitmenler veya gönüllüler vb. tarafından, profesyonel veya amatör bir bilinçle oluşturulmuş çevrimiçi öğretim sistemler veya materyaller oluşturmaktadır. Bu konu "Çevrimiçi Bilgi Güvenliği Öğrenme Ortamları" başlığı altında incelenecektir.

Bilgi Güvenliği Farkındalık Ölçme Çalışmaları

Bireysel bilgi güvenliğini farkındalık boyutunda incelemeye yönelik olarak alanyazında konunun farklı yönleriyle ele alındığı çalışmalar bulunmaktadır. Bu çalışmaların büyük bir kısmı sadece tek bir konu alanda bilgi güvenliği farkındalığını ölçmeye yöneliktir. Teknolojinin gelişmesi ve daha önemlisi belirli bir teknolojik ürün veya servisin yaygın hale gelmesi o konuya özgü bilimsel çalışmaların fazla sayıda olmasını açıklar niteliktedir. Örneğin; mobil ağ teknolojilerinin ve akıllı telefonların yaygınlaşması ile mobil bankacılık hizmetinin sunulmaya başlanması bu konuya özel farkındalık çalışmalarının yapılmasına sebebiyet vermiştir.

Organizasyonlarda bilgi güvenliğini sağlamanın çalışanların farkındalıkları ile bağlantılı olduğunu vurgulayan Stanton, Stam, Mastrangelo ve Jolton (2005), bir organizasyon dâhilinde

bilgi güvenliği farkındalık konusunu şifre davranışları üzerinden inceledikleri bir çalışma yürütmüşlerdir. Bu çalışmalarını güçlü şifre oluşturma, şifrenin değiştirilme sıklığı, şifrenin not olarak bir yere yazılması ve şifrenin paylaşılması (çalışma arkadaşları, organizasyon içi paydaş veya organizasyon dışı herhangi kişi ile) başlıklarını katılımcıların kendi beyanatına dayalı olan anket uygulaması ile irdeleyerek gerçekleştirmişlerdir. (Clarke, Symes, Saevanee ve Furnell, (2016) çalışmalarında insanların teknoloji ve internet ile bağlarını tamamen değiştirdiğini vurguladıkları akıllı telefonların güvenliği konusunda kullanıcıların tutum ve görüşlerini incelemişlerdir. Çalışmalarını kullanıcıların akıllı cihazlara olan erişim kontrolleri tercihleri ve zararlı yazılım kullanımı başlıkları altında anket çalışması ile gerçekleştirmişlerdir. Sosyal ağların organizasyonların bilgi güvenliği politikalarının, bilgilerin paylaşımı ile zedelendiğini belirten Sari ve Prasetio (2017) bilgi güvenliği farkındalık çalışmalarını sosyal ağlar alanında yapmış, bilginin bir başkasına sunumundaki amaç ve sunulan kişi veya topluluğun katılımcı ile bağı konularının araştırmasını çevrimiçi bir anket çalışması ile gerçekleştirmişlerdir. Talib, Clarke ve Furnell (2010) ev ve işyeri içerisinde bilgi güvenliği farkındalığını güvenlik tehditleri hakkında sahip olunan bilgi, bilgi güvenliğine dair pratikler, güvenlik kontrolü uygulamaları (zararlı yazılım önleme, güvenlik duvarı vb.) kullanımı ve bu alanlarda alının eğitimle ilişkisini bir anket çalışması ile gerçekleştirmişlerdir. Oltalama saldırılarının önlenebilmesi için son kullanıcıların muhakkak bir eğitim almasının gerekliliğini savunan Arachchilage ve Love (2014), öncelikle bilgisayar kullanıcılarının bu alandaki farkındalığının ölçülmesi gerekliliğini belirtmiş, eğitime ön olacak verileri; "kişilerin öz yeterliliği, kaçınma motivasyonları, kaçınma davranışları ve prosedürle ilgili bilgileri" başlıkları altında katılımcılara uyguladıkları anket uygulaması ile toplamışlardır.

Alanyazında, yukarıda sıralanan örnekleri çoğaltılabilecek sadece tek bir konu alanında bilgi güvenliği farkındalığını ölçmeye yönelik çok sayıda çalışma bulunmaktadır. Ancak sayıca az olmasına karşın tüm bilgi teknolojileri ürün ve hizmetlerinin kullanımı konularını kapsayacak/kapsamayı amaçlayan bilgi güvenliği farkındalığı çalışmaları da alanyazında yer almaktadır.

Egelman ve Peer (2015) son kullanıcı güvenlik davranışlarını ölçmek için standart bir araç geliştirmeyi amaçladıkları çalışmalarında, son kullanıcılara bilgi güvenliğine yönelik olarak

verilen tavsiyelerden yola çıkarak, genel geçer kabul edilen, çekirdek yapıda bilgi güvenliği davranışlarından oluşan bir ölçek ortaya koymuşlardır. SeBIS ismini verdikleri bu ölçekte 4 davranış çatısı altında;

- Cihaz güvenliği
- Şifre kullanımı
- Proaktif farkındalık (Sıkıntıların önceden farkında olunması)
- Güncelleme

16 çekirdek davranış belirlenmiştir. Araştırmacılar oluşturulan ölçeğin farkındalık belirlenmesi, eğitsel müdahalelerin tanımlanması, kişilerin farklı güvenlik tedbirlerine karşı tutumları, gerçek dünyada karşılaşılabilecek sorunlara karşı gösterilebilecek tepkilerin tahmini vb. durumlar için kullanılabileceğini vurgulamışlardır.

Parsons vd. (2017) bilgi güveliği ihlallerinin büyük kaynağının bile isteye veya kazara yanlış davranışlarda bulunan insan olduğunu vurgulayarak, bilgi güvenliği farkındalığını ölçecek etkili bir araç oluşturmak amacıyla gerçekleştirdikleri çalışmalarında BTD (bilgi-tutum-davranış) modelini kullanan bir ölçek geliştirmişlerdir. Ölçek aynı konu ve alt başlığı için katılımcının hem bilgisini hem tutumunu hem de davranışını belirlemeyi amaçlamıştır. HAIS-Q (The Human Aspects of Information Security Questionnaire- Bilgi Güvenliğinin İnsani Boyut Ölçeği) ismini verdikleri bu ölçek çatısı altında;

- Şifre yönetimi
- Eposta kullanımı
- İnternet kullanımı
- Sosyal medya kullanımı
- Akıllı cihaz kullanımı
- Bilgi yönetimi
- Olay bildirimi

21 belli başlık altında 63 madde belirlenmiştir. Teknolojik gelişmelere paralel olarak güncellenmesinin öneminin vurgulandığı çalışmanın, organizasyon ve çalışanlar tarafından

güçlü ve zayıf yönlerinin belirlenebilmesi ve bu sayede bilgi güvenliği eğitimi ihtiyaçlarının belirlenebileceği vurgulanmıştır.

İnternet kullanıcılarının farkındalık, bilgi ve davranışlarından büyük oranda etkilenen bilgi güvenliği için çözümler üretmeden önce kullanıcıların farkındalıklarının ölçülmesi gerektiğini vurgulayan Velki, Solic ve Ocevcic (2014) bu amaca hizmet eden USIAQ (Users' Information Security Awareness Questionnaire – Kullanıcı Bilgi Güvenliği Farkındalığı Ölçeği) isimli bir ölçek geliştirmişlerdir. 4 bölümden oluşan bu anket 37 sorudan ibaret olup;

- 1. Bölüm kullanıcıların riskli davranışlarını
- 2. Bölüm kullanıcıların bilgi güvenliği farkındalıklarını
- 3. Bölüm kullanıcıların bilgi güvenliği hakkında inançlarını
- 4. Bölüm kullanıcıların şifre kalitelerini ve güvenilirliğini

ölçmek için tasarlanmıştır. Ölçek çalışması ile kullanıcıların bilgi güvenliğine dair riskli davranışları hakkında genel bir sonuca varılabileceği, güvenliği göz ardı eden kullanıcı betimlemesinin yapılabileceği vurgulanmıştır.

Keser ve Güldüren (2015) görece daha dar bir kapsamı olan, yükseköğretim kurumlarında çalışan öğretim görevlilerinin bilgi güvenliği farkındalık seviyelerini belirlemek için geliştirdikleri BGFÖ ismini verdikleri ölçek çalışması 34 maddeden oluşmaktadır. Ölçeğin alt boyutlarını;

- Genel güvenlik
- Saldırı ve tehditler
- Eposta ve iletişim
- Mobil cihazlar
- Mahremiyet
- Güvenli gezinme
- Yazılım ve uygulamalar

oluşturmaktadır.

Öğütçü (2010) bilgi güvenliği farkındalığı kazandırmaya yönelik, çevrimiçi bir öğretim ortamı geliştirmeyi amaçladığı tez çalışması kapsamında geliştirdiği ölçek, bu çalışma kapsamında kullanılmış olup ayrıntılı bilgi veri toplama araçları başlığında detaylı olarak açıklanmıştır.

Alanyazında bilgi güvenliği farkındalığını ölçmeye yönelik çalışmaların örnekleri çoğaltılabilecek durumdadır. Bu çalışmaların ortak özelliği "kişinin kendi beyanatına dayalı" olmasıdır. Hemen her çalışmanın sınırlılıklar veya varsayımlar bölümünde "kişisel bilgi, görüş ve eğilimlerini yansıtmaktadır" ibaresine rastlanılmaktadır. Babbie (2016) anket çalışmalarının zayıf yönlerini sıralarken, katılımcının sosyal yaşantısındaki davranışlar yerine söylediği bilgilere dayalı olmasını, katılımcıların araştırmacının kendilerini pozitif bir algı ile görmelerini sağlayacağı şekilde cevaplar sunmasını vurgulamıştır. Ajzen, Brown ve Carvajal (2004) insanların davranış şekli olarak iddia ettikleri niyetleri ile aynı doğrultuda davranış gösterememesinin yaygın olarak gözlendiğini belirtmişlerdir. Bagozzi (2007) de benzer şekilde insanların niyetleri ile gerçek davranışları arasındaki bulunan bağın zayıflığının deneysel çalışmalarla kanıtlandığını vurgulamıştır. Alanyazında benzer çalışmalar niyetlerin gerçek davranışları doğurmadığından dolayı davranışlardansa niyetlerin ölçülmesinin sıkıntılı durumlar çıkaracağını ortaya koymuştur (Crossler vd., 2013; Anderson ve Agarwal, 2010; Mahmood vd., 2010).

Bilgi Güvenliği ve Bireysel Farklılıklar

Bilgi ve iletişim sistemlerinin güvenlik gereksinimine karşı yapılarını her geçen gün daha karmaşık ve daha aşılmaz şekilde güncelleniyor olmalarına karşın, siber suçlular da kendilerini bu güncellemeye ayak uyduracak şekilde geliştirmekte ve bu sitemler üzerinde zarar oluşturmak için yeni ve farklı yöntemler denemektedirler (Neghina ve Scarlat, 2013). Ancak bu durumda güncellemesi daha yavaş olan veya hiç güncellenmeyen, bu sistemleri veya verdiği hizmetleri kullanan insan faktörü en zayıf halka olarak karşımıza çıkmaktadır. Ayyagari (2012) birbirinden bağımsız olarak gerçekleşen 2633 bilgi güvenliği ihlali olayını analiz ettiği çalışmasında teknik olarak korsan faaliyet girişimlerinde azalma gözlenirken insan faktörü üzerinden gerçekleştirilen saldırılarda artış olduğunu göstermiştir. Zhang, Reithel ve Li (2009) bilgi

güvenliği açısından özellikle bireysel farkındalığın anahtar rolde olduğunu vurgulamış ve hem akademik hem de endüstri çevresinde çalışılması gerekli bir alan olarak belirtmişlerdir.

Özellikle, saldırganların temel hedeflerinin bireylerin zafiyetlerini ikna etme, kandırma vb. yöntemlerle kullanarak onlardan birtakım bilgileri çalıp amaçları doğrultusunda kullanmak olduğu sosyal mühendislik saldırıları yaşam döngüsünde; hedefin belirlendikten sonra ilgili bilgilerin toplanarak zafiyetlerinin tespit edildiği ve ona göre saldırıların gerçekleştirildiği; bu konuda ise bireylerin hangi teknolojiyi nasıl kullandığının ve farkındalığının büyük önem arz ettiği vurgulanmaktadır (Irmak ve Reis, 2018). Bireysel farklılıklar bilgi güvenliği konusunda insan davranışlarının da farklılaşmasına sebep olmuş ve bu durum alanyazında sıklıkla çalışılmıştır. Bireylerin psikolojik farklılıklarının bilgi güvenliği konusunda davranışlarını etkileyebileceğini düşünen Egelman ve Peer (2015) yapmış oldukları çalışmada, bireylerin risk alma konusundaki farklılıklarını, karar verme stillerini, bilişsel ihtiyaçlarını, dikkat dürtülerini ve davranışlarının uzun dönem sonuçlarının tercihlerine etkisi arasındaki farklılıklarını incelemişlerdir. Çalışmanın sonuçları sağlık ve güvenlik konusunda risk almaya yatkın bireylerin yazılımlarını güncelleme eğiliminde olduklarını, karar alma konusunda bağımlı olmayan bireylerin bilgi güvenliği konusunda proaktif davranış sergilediğini göstermiştir. Hadlington ve Chivers (2018) bireylerin bilgi güvenliği ihlallerine maruz kalmaları ve bilgi güvenliği farkındalıkları ile kişilik özellikleri arasındaki ilişkiyi inceledikleri çalışmalarında; 40 yaş altındaki bireylerin bilgi güvenliği ihlallerine maruz kalmakta daha riskli olduğu, ani kararlar vermeyen, "hayır" demekten korkmayan, sosyal medyayı nadiren kullanan katılımcıların şifre yönetimi ve güvenli eposta kullanımı konusunda daha iyi davranışlar gösterdiği, teknoloji ile çokça haşır neşir olmayan, 50-64 yaş aralığında, düşük gelir düzeyinde kazancı olan ve eğitim seviyesi görece daha düşük atılımcıların bilgi güvenliği konusunda en güvensiz davranışları sergiledikleri sonucunu bildirmişlerdir. Belirtilen araştırmadan sadece bu çalışma kapsamını ilgilendiren bulgulara yer verilmiştir. McCormac vd. (2017) gerçekleştirmiş oldukları çalışmalarında bireylerin bilgi güvenliği özelinde bilgi, tutum ve davranışları ile bireysel farklılıkları olan yaş, cinsiyet, kişilik, risk alma eğilimi ve organizasyonel faktörleri arasındaki ilişkiyi incelemişlerdir. Genç bireylerin yaşlılara göre daha düşük bilgi güvenliği farkındalık puanları aldıkları ve ayrıca kişilik özelliklerinden olan yumuşak başlılık, dışa dönüklük ve özdenetim puanları yüksek olan bireylerin görece daha iyi bilgi güvenliği

farkındalıklarının olduğu vurgulanmıştır. Hadlington vd. (2019) gerçekleştirdikleri çalışmalarında bir organizasyon çatısı altındaki bireyin iş yerindeki algılanan kontrolü, mevcut iş kimliğine olan bağlılığı ve iş yerine verdiği çalışma taahhüdünü ne ölçüde yeniden değerlendirdiği bireysel değişkenlerin bilgi güvenliğine olan etkilerini incelemişlerdir. Çalışmanın sonuçları dışsal olan, işyeri ortamları üzerinde algılanan sınırlı denetime sahip olan bireylerin daha zayıf bilgi güvenliği farkındalığı olduğu, mevcut iş kimliğine bağlı olan bireylerin ise görece daha yüksek bilgi güvenliği farkındalığı olduğunu vurgulamıştır. Dodel ve Mesch (2017) zararlı yazılım önleme yazılımlarının kullanımını etkileyen bireysel farklılıkları inceledikleri çalışmalarında yaş, cinsiyet, eğitim seviyesi ve internet kullanım sıklığı değişkenlerinin bu yöndeki davranışı etkiledikleri sonucuna varmışlardır. Gratian vd. (2018) çalışmalarında bireylerin risk alma yetkinlikleri, karar verme stilleri, demografik ve kişilik özellikleri ile bilgi güvenliğine özgü şifre yönetimi, güncelleme, proaktif farkındalık ve araç güvenliği arasındaki ilişkiyi incelemişlerdir. Demografik özellikler açısından yaş, cinsiyet, üniversitedeki rolü (öğrenci, akademik ve idari personel) ve çalışma süreleri çalışmada irdelenmiştir. Çalışmanın sonucunda finansal risk alma, akılcı karar verme, dışadönüklük ve cinsiyet değişkenlerinin daha iyi bilgi güvenliği davranışları gösterme konusunda önemli belirleyiciler olduğu vurgulanmıştır. Shropshire, Warkentin ve Sharma (2015), son kullanıcı güvenlik yazılımları kullanma davranışı ile kişilik, organizasyonel destek, kullanılabilirlik ve yararlılık algıları arasındaki ilişkiyi incelemişlerdir. Özdenetim ve yumuşak başlılık kişisel özelliklerinin güvenlik yazılımı kullanma niyeti ile gerçekten kullanımını belirleyen en önemli bireysel farklılıklar olarak vurgulanırken, kullanılabilirlik konusundaki algının yararlılık konusundaki algıyı onun da güvenlik yazılımı kullanmayı etkilediğini belirtmişlerdir. Wiley, McCormac ve Calic (2020), çalışmalarında dâhil olma, fark yaratma, öğrenme, stratejik amaçlara yön verme, koordinasyon, bütünleşme, kapasite artırma gibi birçok alt başlığı olan organizasyonel kültür ve güvenlik kültürü bireysel farklılıklarına ait değişkenler ile bilgi güvenliği farkındalığı arasındaki ilişkiyi incelemişlerdir. Çalışmanın sonuçları her iki bireysel farklılığın bilgi güvenliği farkındalığı ile pozitif ilişkisi olduğunu ortaya koysa da yazarlar güvenlik kültürünün organizasyonların daha çok üzerinde durması gereken değişken olduğunu vurgulamışlardır. McGill ve Thompson (2018) bireylerin demografik farklılıklarından olan cinsiyetin bilgi güvenliği ile olan ilişkisini incelemişlerdir. Çalışmalarında güvenlik

tehditlerinin sonuçlarının nasıl algılandığı, koruyucu güvenlik almada yeterlilikler, güvenlik önlemlerine karşı bakış açıları gibi bireylerin bilgi güvenliği farkındalıklarının alt konuları araştırılmıştır. Çalışma sonucunda kadın katılımcıların erkek katılımcılara oranla daha düşük seviyede güvenli davranış içerisinde oldukları belirtilmiştir. Halevi, Lewis ve Memon (2013) ise bireylerin kişilik özellikleri ile oltalama saldırılarına karşına düşme ve kişisel bilgilerini paylaşama eğilimleri arasındaki ilişkiyi inceledikleri çalışmalarında, yeni deneyimlere açık olan bireylerin çevrimiçi bilgi paylaşma konusunda daha açık davranışlar sergilerken sosyal medya platformları güvenlik ayarlarını daha az koruyucu olarak düzenlediklerini belirtmişlerdir.

Alanyazında bireylerin bilgi güvenliği kurallarına uymasını veya ihlal etmesine neden olabilecek birçok bireysel faktör çalışılmıştır (Dhillon ve Backhouse, 2000). İncelenen çalışmalarda bireysel farklılıklardan demografik özelliklerle kişilik özelliklerinin ortak olarak veya daha sıklıkla incelendiği gözlemlenmiştir. Demografik özelliklerin anket uygulaması ile katılımcıların duygularını katmadan alınabilecek en doğru bilgi olması ve kolay ulaşılabilir olması sebebi ile incelendiği değerlendirilmektedir. Kişilik özellikleri ise birey için hayat boyu görece sabit kalacak bir değişken olarak (Warkentin, McBride, Carter ve Johnston, 2012) nitelendirildiğinden çalışmalara sıkça dâhil edildiği düşünülmektedir.

Çevrimiçi Öğrenme Ortamları

Yıllardır süren araştırmalara rağmen öğrenenleri odaklandıracak ve öğrenme sürecini geliştirecek uygun ve ilgi çekici içerikte yaşanan eksiklikten dolayı, araştırmacılar içinde bulundukları zamana, dünyanın gerçeklerine ve olanaklarına uygun olacak yeni yöntemler konusunda arayışlara girmişlerdir (Pivec, Dziabenko ve Schinnerl, 2003). Bu arayışlar tarih boyunca sürmüş psikolojik, sosyolojik, ekonomik ve bilhassa teknolojik gelişmeler arayışlara ve yöntemlerin gelişimine etki etmiştir.

1592-1670 yılları arasında yaşamış olan Çek eğitimci ve bilim adamı Jan Amos Comenius kendisini öğretme'nin geliştirilmesine adamış ve bilinenden bilinmeyene doğru ilerleyen bir sistemi benimseyerek öğretimin 9 evrensel prensibini ortaya koymuştur (Schwarz ve Martin, 2012). Comenius Latince kelimelerin yanında özetleyici görsel öğeleri kullanan resimli bir kitap geliştiren ilk kişi olarak (Mandl ve Levin, 1989) verimliliğin artırılmasını sağlamıştır.

İnsan gücü ile gerçekleştirilen üretim tarzından yoğunlukla makine gücünün hâkim olduğu üretim şekline geçiş olarak tanımlanan (Aston, 1948 akt. Küçükkalay, 1997) Sanayi Devrimi'nin etkisi ile az zamanda çok fazla sayıda insana öğretilmesi ihtiyacı doğmuştur. Üretim sisteminde insan gücü yanında makinelerin kullanılmaya başlanması sonrası fabrika üretim sistemine doğru bir geçiş dikkati çekmekte olup, süreç giderek okula dayalı bir mesleki eğitim anlayışını gündeme getirmeye başlamıştır (Taşpınar, 2014). Lawrence Stone okuryazarlık oranının 1775'te %56'ya, 1800'de %65'e, 1840'ta ise %66'ya çıktığını bunun sebebinin ise endüstrileşen toplumdaki eğitilmiş işçi gücündeki talepten kaynaklandığını belirtmiştir (Sanderson, 2007). Bu durum, fazla sayıda insanın etkili ve verimli bir şekilde öğretim alması adına bir öncül olmuştur.

2. Dünya Savaşı sırasında Sanayi Devrimi sonrasındaki benzer bir durumda çok fazla sayıda askerin eğitimi için 400 film çekilmiş ve 4 milyon kez gösterim yapılmış, aynı şekilde sivillerin endüstride çalışma eğitimleri için de aynı yol izlenmiştir. Bu durum çok sayıda insanın verimli bir şekilde eğitilmesi konusunda görsel-işitsel materyallerin okullarda kullanımına olan bakış açısını değiştirmiştir (Reiser, 2001).

Öğretim teknolojisi olarak sonuçlandırılabilecek bu arayışların özünde eğitimin daha çok sayıda bireye hitap etmesi ve yaygınlaştırılması gereksinimi olduğu aşikârdır. Yazılı ve elektronik iletişim araçları kullanılarak, planlanmış olan ders programı bağlamında öğrenen ve öğretenin zaman ve mekândan bağımsız olduğu ve öğrenmenin sağlanması için yapılan her türlü düzenleme olarak (Verduin ve Clark, 1991) nitelendirilen uzaktan eğitim, tarih boyunca mektup, basılı malzemeler, radyo, televizyon gibi iletişim araçları kullanılarak gerçekleştirilmiş (İşman, 2011) ve eğitimin yaygınlaşması konusunda büyük bir etki yaratmıştır.

Tarih boyunca gerçekleştirilen bu çabaların bilginin daha kolay çoğaltılması, iletilmesi ve erişilebilir olması konusunda etkisi açıkça ortadadır. Bilgi ve iletişim teknolojilerinde gerçekleşen gelişmeler çevrimiçi öğretim konusunda da paralel bir gelişmeye olanak sağlamış, alanda yapılan çalışmalar yeni gelişen ihtiyaçlar ve sorunlar bağlamında şekillenmiştir. Alanyazında çevrimiçi öğretimle ilgili farklı bir özelliğini ön plana çıkaran tanımlamalar olmasının yanı sıra ortak bileşenin kullanılan teknoloji olduğu göze çarpmaktadır. Ally (2004) eğitsel içeriğe ve ilgili materyale erişim sağlamak, öğreten ve diğer öğrenenlerle etkileşim

sağlamak, bilgiyi oluşturma, anlamlandırma ve paylaşma konusunda internet teknolojilerinin kullanılması olarak açıklamıştır. Means vd. (2009) ise basılı-materyal, radyo veya televizyon yayını, video konferans, videokaset, eğitsel uygulama gibi internet-temelli öğretimsel bir bileşeni olmayan teknolojileri dışarıda bırakarak, öğretimin kısmen veya tamamen internet üzerinden gerçekleştirilmesi olarak açıklamışlardır. Ko ve Rossen de (2017) bir dersin sunulduğu teknolojiden bağımsız olarak internet üzerinden işlenmesi olarak tanımlamışlardır.

Web teknolojilerinin hemen her disiplin için getirdiği yenilikler ve sağladığı faydalar çevrimiçi öğretim sistemleri için de benzer olanaklar sağlamaktadır. Kaynaklara erişimde yer ve zaman merfumunun olmaması, daha az maliyet ile daha kaliteli eğitim materyaline erişilebilmesi ve bu materyalden eş zamanlı olarak çok daha fazla sayıda öğrenenin istifade edebiliyor olması (Panigrahi, Srivastava ve Sharma, 2018), diğer öğrenenlerle konuşma konusunda korkusu olanlar için tartışma forumlarının bu bariyeri yıkması, öğrenene kendi ayarlayabileceği süre ve şekilde öğrenme ortam sağlaması (Arkorful ve Abaidoo, 2015) çevrimiçi öğretimin sağladığı avantajlardan önemli bir kısmı olarak sıralanabilir.

İnternet hızında yaşanan gelişmeler, işlemci hızlarının artması, görüntüleme sistemlerinin daha çok kabiliyet kazanması ve tüm bu gelişmelerin akıllı cihazlar üzerinde de erişilebilir olması çevrimiçi öğrenme ortamlarının daha çok bireye ulaşmasını sağlaması ve alana olan ilgiyi artırmasının yanında beraberinde getirdiği sorunlar da alan yazının konusu olmuştur. Panigrahi vd. (2018) çevrimiçi öğrenme konusunda yaşanan sıkıntılar, bu sıkıntıların kaynağı ve getirilmeye çalışılan çözümler kapsamında alan yazında yapılan çalışmalar üzerinden durumu teknoloji adaptasyonu, teknoloji devamlılığı ve öğrenme çıktıları şeklinde üç başlık altında kategorize etmişlerdir. Çalışmaya göre; teknoloji adaptasyonu için kullanılabilirlik, kullanışlılık ve etkileşim algısı, bilişsel olgunluk ve kazanım, sosyallik, ulus kültürü, çevresel faktörler, kullanıcı direnci gibi konular çalışılırken; öğrenenin çevrimiçi öğrenmeye devam etmesi başlığında memnuniyet, alışkanlıklar, deneyimleme, kendini gerçekleştirme, bilişim sisteminin kalitesi, psikolojik olarak güvenlik, cevaplanabilirlik konuları çalışılmıştır. En kritik üst başlık olarak tanımlanan öğrenme çıktıları açısından ise bağlılık, öğrenen motivasyonu, odaklanma, tasarım, birlikte çalışma, içerik yönetimi alan yazında çalışılan konular olarak sınıflandırılmıştır.

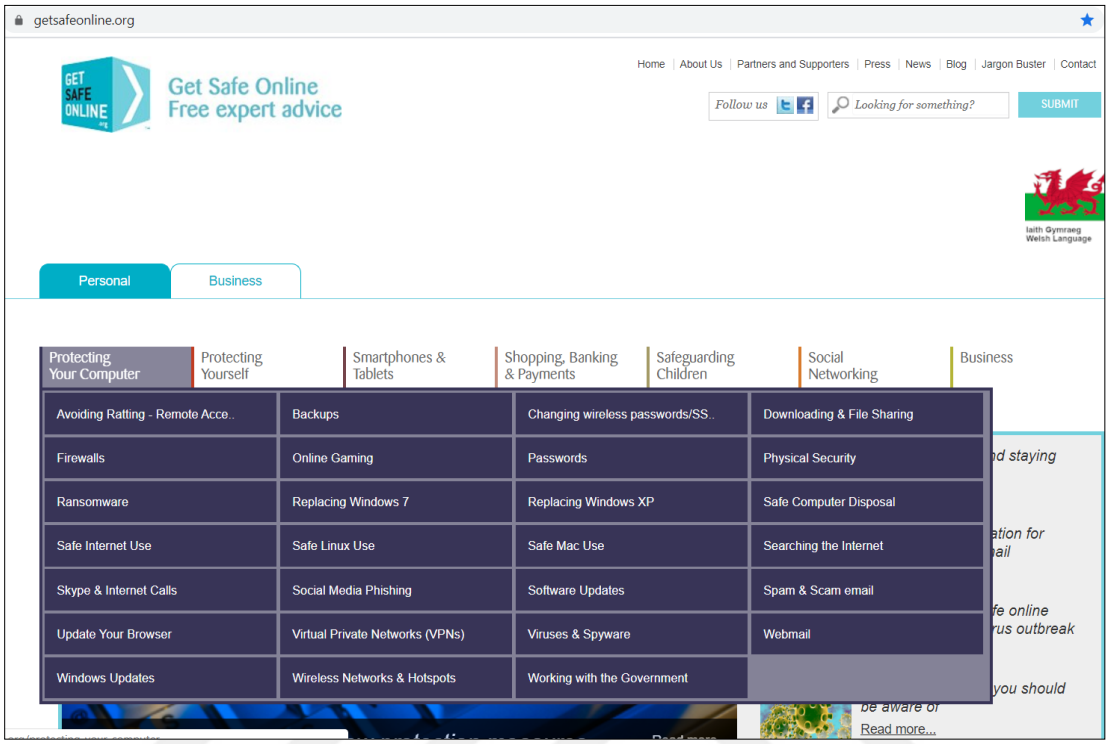
Çevrimiçi öğrenme ortamlarının öğrenene kendi ayarlayabileceği süre ve şekilde öğrenme ortam sağlaması, doğrusal olmayan bir sıralamada, belli bir sırayı takip etmesi gerekmeden, özgürce gezinme imkânı tanıyor olmasından kaynaklanmaktadır. Ancak sistemin kullanılabilirliği ile ilgili sorunlar yine web teknolojilerinin sağladığı avantajlardan kaynaklanmaktadır. Şöyle ki içeriğin ve bağlantı sayısının sınırsız olabilmesi, öğrenenin aradığı bilgiyi bulamamasına ya da hangi bilgiye ihtiyacının olduğunu belirleyememesine sebep olmaktadır (Micarelli ve Sciarrone, 1996; Otter ve Johnson 2000). Bu durum gezinme ile ilgili en büyük problemlerden biri olan kaybolmayı oluşturmakla; öğrenenlerin, topolojisinden dolayı doğrusal bir sıralaması olmayan hiper belgelerde nerede olduğunu ve nereye ilerleyeceğini belirleyememesi, kaybetmesi eğilimi olarak açıklanabilir (Conklin, 1987). Hiper ortamda, genelde olduğu gibi alan yeterince genişse kullanıcının ağ boyunca düğümler arasında aşağı veya yukarı sezgisel olarak hareket ediyor olması onun bu ortamda kaybolmasına sebep olabilir (Pérez, Gutiérrez ve Lopistéguy, 1995). Bir hiper metinde farklı rota seçeneklerinin olması kullanıcıya planlama ve karar verme gibi ekstra bilişsel yük getirebilmekle, bu durum doğrusal rota formatında yaşanmamaktadır. Kötü tasarlanmış hiper metin yüksek sayıda kullanıcının kaybolmasına sebebiyet vermektedir (Jones ve Burnett, 2007). Kaybolmayı etkileyen üç ana faktörün kullanıcının "bir sonraki gideceği yerin neresi olduğunu bilmemesi", "oraya nasıl gideceğini bilmemesi" ve "tüm yapı içerisinde nerede olduğunu bilmemesi" olarak sıralanmıştır (Elm ve Woods, 1985; akt. Chen, 2002). Bu durum için hiper ortamda bulunan içeriğin hiyerarşik veya alfabetik bir indeksinin sağlanması, tipo grafik belirleyicilerin belgenin kendi içinde sunulması, tüm içerik yapısının grafikse olarak sunulması, kullanıcının hiper ortamdaki ayak izlerinin gösterilmesi, menü ve harita ara yüzlerinin, kılavuzların kullanılması (Simpson, 1990; Dias ve Sousa, 1997) önerileri getirilmiş ve uygulanmaktadır. Brusilovsky (1996) ise hiper ortamlardaki kaybolma probleminin, akıllı rehberlik imkânı sunan uyarlanabilir sistemlerle çözümlenebileceğini savunmuştur.

Bilgi Güvenliği Konusunda Çevrimiçi Öğrenme Ortamları

Bireylerin dikkatini bilgi güvenliği konularına yönlendirmek ve bu konudaki endişeleri fark edip önlemlere uyum sağlayarak o yönde davranış sergilemelerini sağlamak için gösterilen çabalar

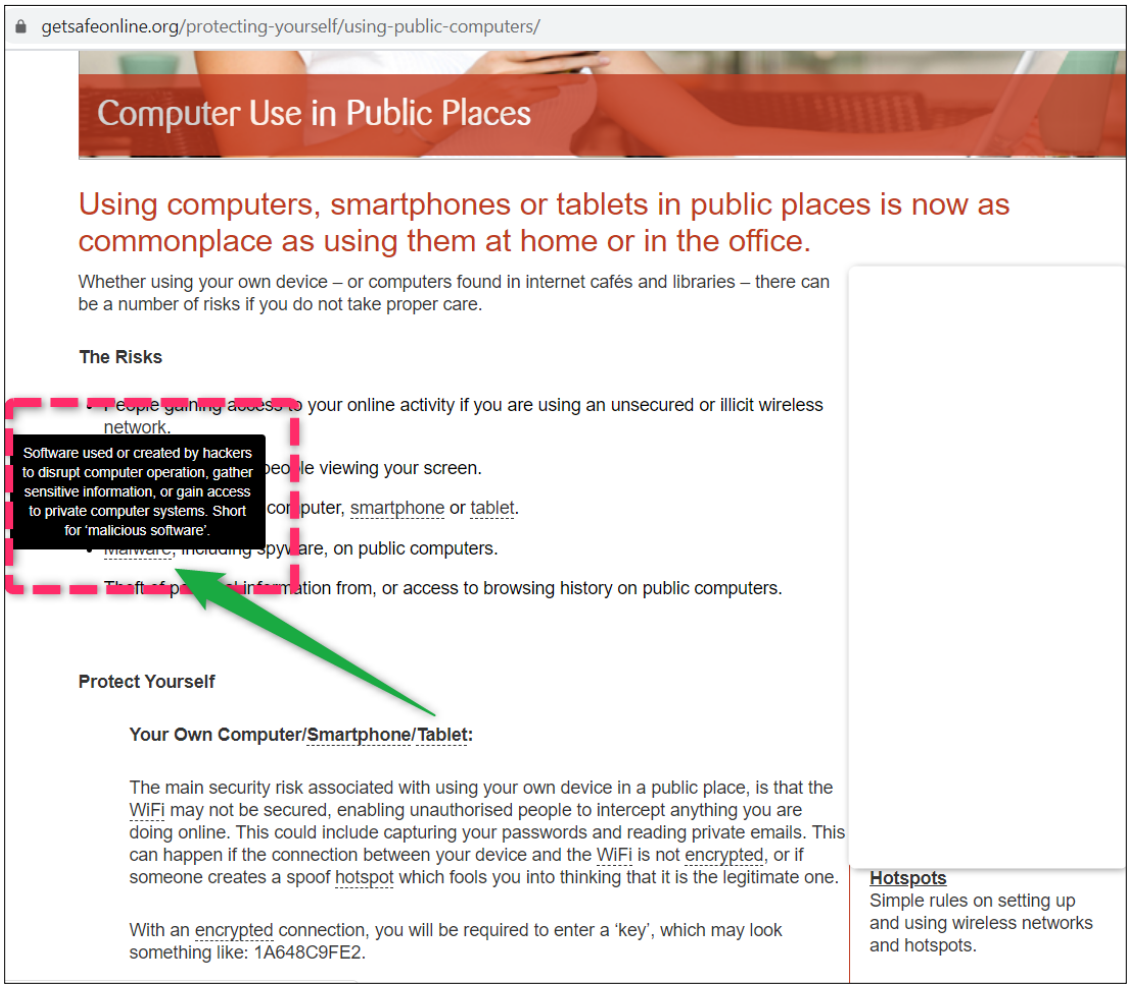
bütünü olarak tanımlanan bilgi güvenliği eğitimi (Information Security Awareness-ISA) konusu akıllı telefon kullanıcısı olan, internet üzerinden fatura ödeyen, alışveriş yapan, iletişim için epostayı araç olarak kullanan, başka bir ifadeyle 7'den 77'ye tüm toplumu ilgilendirmektedir. Alanyazında konu üzerinde birçok çalışma mevcut olmasına karşın gerçek yaşantıda veya endüstride genellikle ücretsiz olarak sunulan, kamu kurumu, alanda hizmet gösteren dernek vb. veya eğitim kurumları tarafından sağlanan içerikler olarak karşımıza çıkmaktadır. Bazı üniversitelerin ilgili bölümlerinde ilgili dersin bir konusu olarak işlenen örnekler olsa da hedef kitlesi derse katılım gösteren öğrenenlerle sınırlıdır. Dünyada ve Türkiye'de örnekleri bulunan, konu ile ilgili karar alma, faaliyetleri düzenleme veya önleme faaliyetlerinde bulunan kurumlar tarafından çevrimiçi öğretim sistemleri yayın yapmaktadır. Aşağıda tanıtımı ve değerlendirmesi yapılan çevrimiçi sistemlerin ortak özelliğini belirtilen ilgili kurum ve kuruluşlar tarafından tasarlanıyor olmalarının yanı sıra öğrenene herhangi bir uyarlanabilir içerik sunuyor olamamalarıdır.

1- www.getsafeonline.org: Web sitesi Birleşik Krallık hükümeti tarafından desteklenen, kolluk kuvvetleri birimleri ile etkinlikler konusunda birlikte çalışan ayrıca ülke çapında bankacılık, tedarik hizmetleri ve internet güvenliği sektörü ile ortak çalışmaları bulunan çevrimiçi öğretim sistemi hizmetidir. Web sitesi ücretsiz olarak hizmet vermekte olup dünya çapında meydana gelen olaylar ve haberlerle de kendini güncelleyen, erişim sağlayan kullanıcılara kendilerini nasıl koruyacaklarını anlatan pratik tavsiyeler sunmaktadır. Şekil 4'te görüldüğü üzere "bilgisayarınızı koruma", "kendinizi koruma", "akıllı cihaz ve tabletler", "alışveriş, bankacılık ve ödemeler", "çocukları koruma", "sosyal ağlar" ve "iş" olmak üzere 7 başlık altında tavsiyeler içermektedir.



Şekil 4. www.getsafeonline.org Web sitesi tavsiye başlıkları

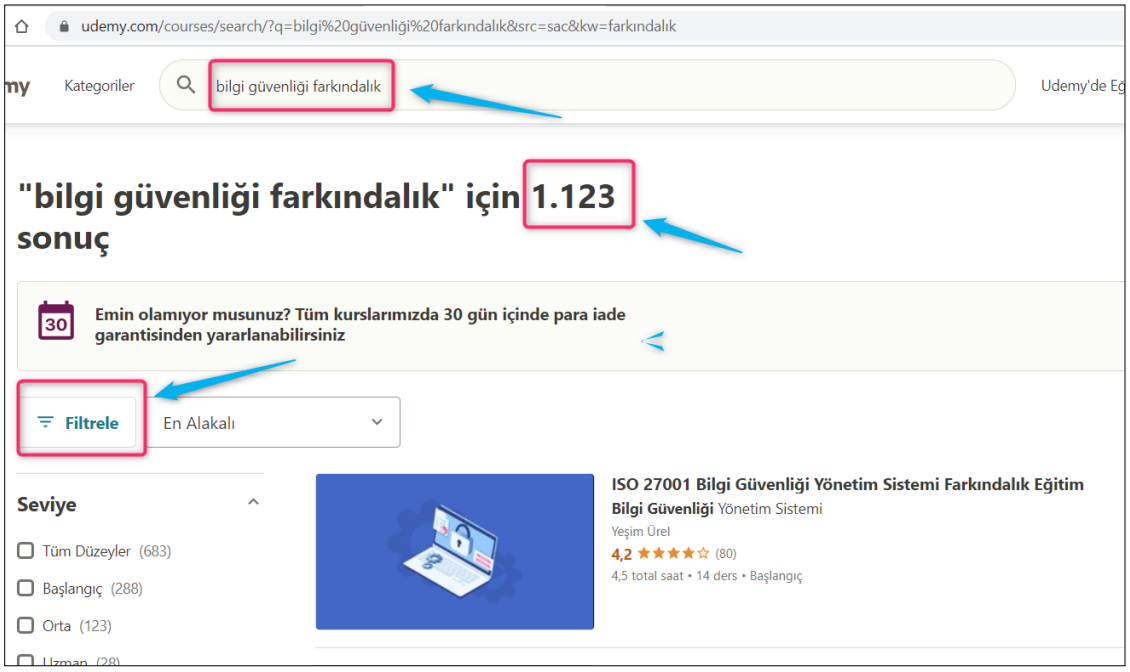
Bilgisayarınızı koruma üst başlığında "güvenlik duvarı", "yedekleme", "kablosuz modem şifresi değiştirme" gibi 27 alt başlık (Şekil 4), toplamda ise 157 alt başlık altında pratik tavsiyeler bulunmaktadır. Belirtilen alt başlıklardan örnek olarak "halka açık yerlerde bilgisayar kullanımı" alt başlığı incelendiğinde, kullanıcının ilgili konuda hangi tür risklerle karşı karşıya gelebileceği bilgisi verilerek içeriğin aktarılmaya başlandığı görülmektedir. Daha sonra ise kullanıcının bu risklere karşı kendini nasıl koruyabileceğine karşın, günlük hayatta uygulanabilir, pratik tavsiyeler aktarılmaktadır. Şekil 5 üzerinde görülebileceği üzere kullanıcının aşina olmadığı terimler altı çizili olarak sunulmakta, fare üzerine geldiği zaman açılır kutu şeklinde ek bilgi sunulmaktadır. Örnekte belirtildiği üzere "malware" terimi üzerine fare işaretçisi getirildiğinde "zararlı ve yazılım kelimelerinin birleşiminin kısaltması olan, bilgisayar işlemlerini bozmak, hassas bilgileri çalmak veya özel bilgisayar sistemlerine erişim yetkisi sağlamak için oluşturulmuş yazılımlardır" şeklinde ek bilgi verildiği görülmektedir. Hazırlanan çevrimiçi sistem çok yoğun ve pratik uygulamaları olan bilgileri içermesine karşın kullanıcının nereden başlayacağını kestiremediği, hangi alt başlıktaki bilginin ne kadarına ihtiyaç duyduğunu belirleyemeyeceği, kişiselleştirilmemiş bir yapıda olduğu görülmektedir.



Şekil 5. Aşina olunmayan terimler için ek açıklama gösterimi

2- www.udemy.com: Udemy 2010 yılında kurulmuş çevrimiçi öğretim platformudur. Bünyesinde 57 bin eğitmen, 150 bin ders, 295 milyon ders kaydı, 33 milyon dakika video ders içeriği barındırmaktadır (18.05.2020). Platform eğitmenlere seçtiği bir konu başlığı altında çevrimiçi bir ders hazırlama ve sunma imkânı getirmekle birlikte video, sunum dosyası, taşınabilir doküman, sıkıştırılmış dosya yükleme özellikleri mevcuttur. Sanattan tarihe, yabancı dilden teknolojiye kadar konularda, kelime işlemci programların kullanımından fotoğraf çekmeye kadar pratik çok çeşitli ders içerikleri barındırmaktadır. Eğitmenin seçimine göre eğitimler ücret karşılığı veya ücretsiz olarak kullanıcılara sunulmaktadır.

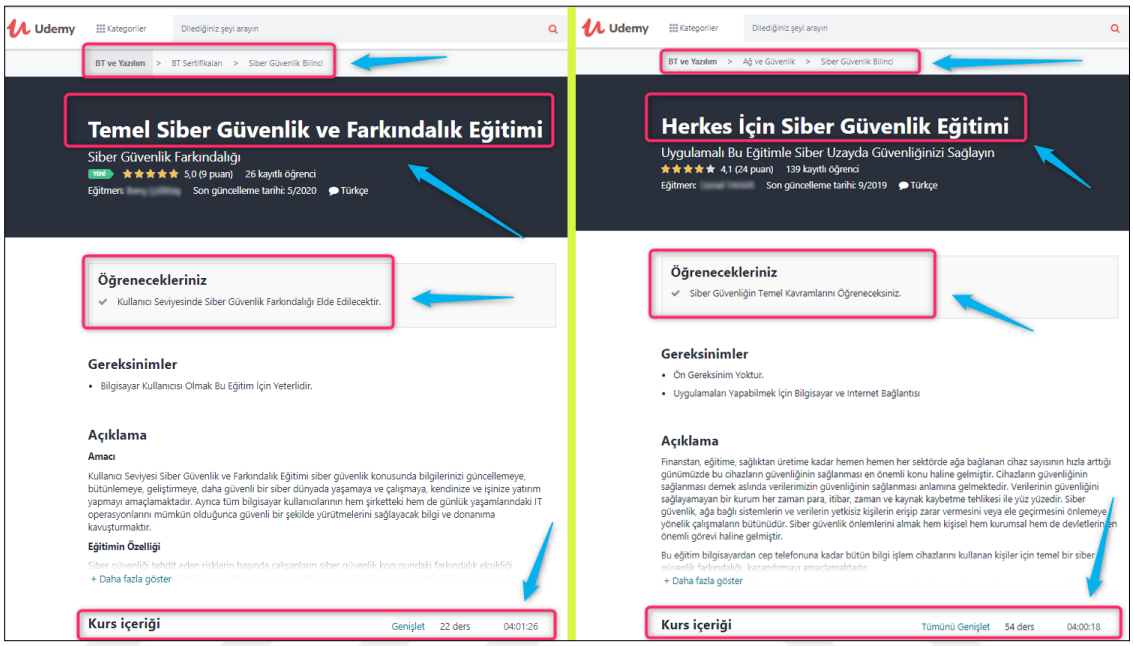
Çevrimiçi öğretim sistemi kullanıcılara kategorik olarak ders seçebilme imkânı sunmakla birlikte, sistem içerisinde kullanıcının belirleyeceği anahtar kelimeler ile de arama yapma olanağı tanımaktadır. Şekil 6 üzerinde belirtildiği üzere "bilgi güvenliği farkındalık" anahtar kelimeleri ile sistem üzerinde yapılan arama sonucunda 1.123 farklı eğitim başlığı sunulmaktadır. Çıkan sonuçlar, eğitmenlerin belirlemiş olduğu bilgi düzeyi, öğretim dili, kullanıcı puanları, video süreleri ve altyazı seçenekleri bağlamında filtre edilebilmektedir.



Şekil 6. www.udemy.com Sistemi üzerinde anahtar kelimelerle yapılan arama sonucu

Sunmuş olduğu bu zengin içeriğe rağmen, bu durumun kullanıcı için hangi dersi seçeceği konusunda belirsizlikler yaşamasına sebep olacağı değerlendirilmektedir. Sonuç ekranında çıkan ve benzer başlıklara sahip iki eğitim tanıtımı yan yana olacak şekilde Şekil 7 üzerinde gösterilmiştir. Buna göre her iki eğitim de "siber güvenlik bilinci" kategorisi altında yer almaktadır. Her iki eğitim içeriğinde "öğrenilecekleriniz" açıklamalarının temel düzeyde olduğu anlaşılmaktadır. Eğitime başlamak için her iki ders için de ön gereksinim ise "bilgisayar kullanıcısı" olmaktır. Ancak ders içerikleri ayrıntılı olarak incelendiğinde birinci eğitimin 22 dersten oluşurken ikinci eğitimin 54 dersten oluştuğu görülmektedir. Toplam eğitim sürelerinin neredeyse aynı olduğu bu iki içerik konusunda bile öğrenenin bireysel

olarak kendisi ile bağlantılı bir tercih yapması konusunda belirsizlik yaşayabileceği değerlendirilmektedir.



Şekil 7. Anahtar kelimeye göre seçilen 2 eğitim içeriğinin karşılaştırılması

3- www.bilgimikoruyorum.org.tr: Bilgimi Koruyorum çevrimiçi öğretim sistemi, Türkiye Cumhuriyeti Sanayi ve Teknoloji Bakanlığı altında teşkilatlanmış olan Türkiye Bilimsel ve Teknolojik Araştırma Kurumu, Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü tarafından gerçekleştirilmiş olan bir projedir. Projenin amacı bilgisayar ve internet kullanıcılarının bilgi güvenliği ile ilgili doğru ve güncel bilgilere hızlı ve etkin bir şekilde erişmesinin sağlanması olarak açıklanmıştır.

Çevrimiçi eğitim sistemi "bilgi güvenliği", "bilgisayar ve erişim güvenliği", "tehditler ve korunma yöntemleri", "internet ve ağ güvenliği" şeklinde 4 bölüm altında 13 konudan oluşmaktadır. Eğitim içeriği incelendiğinde, konu başlarında günlük yaşantıda bireylerin karşılaşabilecekleri günlük olaylara benzerlikler kurulan hikâyelere yer verildiği, konu içeriklerinde ise kuramsal ve pratik bilgiler sunduğu gözlenmiştir. Şekil 8 üzerinde gösterimi yapıldığı üzere sistem üzerinde kaybolma probleminin önüne geçilebilmesi için, kullanıcının o an hangi bölümde bulunduğu gösterilmekle birlikte bir menü ara yüzü sunulmuştur.

Şekil 8. Bilgimi koruyorum çevrimiçi öğretim sistemi ara yüzü

Öğretim sistemi üzerinde yapılan açıklamalarda, öğrenenin öğrenme sürecini kendisinin ihtiyaçlarına göre planlaması gerektiği, konu bazlı olarak sıralı bir şekilde ilerlemelerinin önerildiği belirtilmiştir. Güncel bilgilerle beslenen çevrimiçi öğretim sistemi her konu sonunda öğrenenin kendisini sınamasına olanak sağlıyor olsa da, öğrenenle alakalı herhangi bir modelleme doğrultusunda uyarlanabilirlikten bahsetmek mümkün değildir. Sisteme giriş yapan her kullanıcı sistem içerisinde gezinerek kendine uygun olduğunu düşündüğü eğitim konularını kendisi seçmek zorundadır.

Çevrimiçi Öğrenme Ortamlarında Veri Madenciliği

Bu bölümde iletişim teknolojileri, öğretim teknolojileri ve veri madenciliği uygulamaları tarihsel gelişimleri ile birlikte değerlendirilerek aktarılmıştır.

Öğretim Teknolojileri Bağlamında Bilgi ve İletişim Teknolojilerindeki Gelişmeler

Bu bölümde bilgi ve iletişim teknolojileri alanında yaşanan gelişmeler ve bu bağlamda öğretim teknolojilerine olan yansımaları incelenmiştir. Yeni gelişmelerin yeni ihtiyaçları ve yeni ihtiyaçların ise yeni gelişmeleri takip ettiği durumlar kronolojik olarak ele alınmıştır.

- 1960'lı yıllar: 1960-1967 yılları arasında PLATO (Programmed Logic for Automatic Teaching Operations - Merkezi Ders Kütüphanesine Bağlı Eğitim Ağı) ismi verilen bilgisayar temelli, bireysel öğrenmenin otomatikleştirilebilirliğini görmeyi amaçlayan bir öğretim sistemi geliştirilmiş olup, sorgulama yapabilen, daha önceden öğrenilmiş bilgiler üzerinde pratik yapıp geri dönüt alınabilen modüller sunulmuştur (Lyman, 1972). Bu gelişmenin öncesinde, 1959'da işlemciler için basit devre elemanı olarak hizmet eden transistorun yeterince güvenli ve ucuz hale gelmesi, 1957'de IBM firmasının model 704 bilgisayarı ile okuması ve işlemesi kolay Fortran programını piyasaya sürmesi; aynı programın birbirinden farklı firmalar tarafından geliştirilen farklı bilgisayarlarda çalıştırılabilmesine imkân tanıyan, standardize edilmiş ilk programlama dili olan COBOL'un (Common Business Oriented Language) ve Avrupa'daki alternatifi olan ALGOL'un (Ceruzzi, 2003) ortaya çıkmış olması göz önüne alınmalıdır. 1960'lı yılları veri saklama yöntem ve teknolojileri bakımından incelendiğinde; bilgisayar teknolojisinin gelişimine paralel olarak kaset tipi kayıt cihazlarına sadece geçmişi işlemekten, doğrudan erişimli depo olarak tanımlanan veri tabanları üzerinde etkileşimli olarak işlem yapılmaya geçildiği yıllar olarak göze çarpmaktadır (Berg, Seymour ve Goel, 2013).
- 1970'li ve 1980'li yıllar: Yarı iletken firmalarının arza hazır, ucuz çipleri piyasaya sağlamasının ardından 1970'li yılların ortalarına doğru 100'ün üzerinde yeni firma genellikle büyük organizasyonlar tarafından kritik uygulamalar için kullanılan ana bilgisayarlar (mainframe) kullanımını bırakarak entegre devre, paketleme ve işlemci mimarisi avantajları olan mini bilgisayarları temin etmeye başlamışlardır. 1980 yılında Xerox firması ethernet ismi verilen ağ şemasını icat ederek kullanıcılara sunmuş, 1984'te Apple firması pencere, ikon, fare ve açılır menü kavramlarını seri üretim pazarına sokmuştur (Ceruzzi, 2003).

1970'li yıllar içerik tabanlı arama yapma imkânı sağlayan ilişkisel veri tabanı kavramının ortaya çıktığı ve yoğunlukla kullanıldığı dönem olmuşken, 1980'li yıllar kalıtım ve çok biçimlilik (inheritance, polymorphism) işlemlerinin kolaylıkla üstesinden gelinebildiği, nesne yönelimli veri tabanı sistemlerinin ortaya çıktığı dönem olmuştur (Berg, Seymour ve Goel, 2013). Bu durum bilgisayar teknolojilerindeki gelişme ve yaygınlaşma ile doğru orantılı olup veri miktarının artması ve işlenmesi ihtiyacından kaynaklanmaktadır. Bu dönemde internet teknolojilerinde yaşanan gelişmeler incelenecek olursa; 1970 yılında Ağ Çalışma Grubu (Network Working Group) NCP (Network Control Protocol) ismi verilen istemci-istemci protokolünü tanımlamıştır. 1972 yılında eposta sistemi ilk defa tanıtılmış olup, 1983 yılında ise ARPANET istemci protokolü olan NCP'den, tüm istemcilerin eş zamanlı olarak iletişim kurabileceği TCP (Transmission Control Protocol) protokolüne geçilmiş; böylelikle 1985 yılında internet, araştırmacı ve geliştiricilerden oluşan geniş bir topluluğa hizmet eden bir teknoloji olarak hayata geçmiştir (Leiner vd., 2009). 1980'li yıllar birbirinden kopuk ve yeni olmayan bilgilerin öğrenenlere aktarımının yapıldığı eğitim düzeninden problem çözme ve kendi kendine öğrenme düzenine geçişi yaşamış (Facione, 1990), 1984 yılında Apple firmasının kişisel Macintosh bilgisayarlarını piyasaya sürmüş ve devamında öğretimsel materyaller analog medyadan dijital medyaya dönmüştür (Molenda, 2008). 1982 yılı Western Davranış Bilimleri Enstitüsü (WBSI) bilgisayarın araç olarak kullanıldığı, işlerinden dolayı eğitime katılma olanağı bulamayan dünyanın çeşitli yerlerinden uzmanların yaklaşık 10 yıl boyunca çevrimiçi eğitimlere katıldıkları hizmeti ilk defa sunmuş, ancak teknolojinin yaygın olmamasından dolayı uzmanların öncelikle belirlenmiş bir yerde bilgisayar eğitimi almalarının getirdiği mali yük, eğitimden sonra evine dönen uzmanın bilgisayar ve ağ teknolojileri konusunda yaşadığı teknik sıkıntılara çözüm bulamayışı sorunları baş göstermiştir (Feenberg, 1993). Sun, Finger ve Liu (2014) çevrimiçi öğrenme konusunda yapmış oldukları eğilim analizi çalışmalarında da 1977-1991 tarihleri arasında yayınlanan ilgili makalelerin 1981 yılına kadar olan aralığında bilgisayarın öğretim amaçlı kullanılabilirliği konusunda yoğunlaştığını belirtirken, kalan yıllarda hala bilgisayar destekli eğitim konusunun çok yoğun işlendiğini ancak tasarım konularının da ön plana çıkmaya başladığını vurgulamışlardır.

- 1990'lı yıllar: 1980'li yılların sonu 1990'lı yılların başı teknoloji ile birlikte hayatın hemen her alanını değişime itecek olan gelişime sahne olmuştur. Tim Berners-Lee CERN araştırma laboratuvarında internet üzerinde hipermedya uygulamalarının gerçekleştirilmesi ve bilgi paylaşımı konusunda standart haline gelecek olan World Wide Web'i (www) hayata geçirmiştir. İstemci-sunucu mimarisi üzerine kurulmuş olan www'de kaynak konumlayıcısı (URL) olarak adlandırılan bağlantıları takip ederek sunucuda tutulan her hiper-dokümana, ağa katılmış olan bir istemci bilgisayar üzerinden erişim imkanı sağlanmış bulunmaktadır (Berners-Lee vd., 1994). Önceki döneme kıyasla kişisel bilgisayarlara erişim imkânının artması, ağ teknolojilerinde yaşanan gelişmeler, hazırlanan ve paylaşıma açılan veri miktarını da artırmış bu durum ise veri tabanı sistemlerinin de gelişimine ön olmuştur. 1990'lı yıllar kişisel bilgisayarlarda veri tabanı uygulamalarının geliştirilmesi, internet firmalarının web/veri tabanı bağlantılarını yapabilecekleri sistemler ve genişletilebilir işaretleme dili (XML) olarak isimlendirilen ve internet üzerinde farklı veri tabanlarında bulunan verilerin başka bir platforma uygun bir şekilde taşınıp kullanılmasına imkan sağlayan dilin veri tabanlarına entegre edilmesi uğraşlarına sahne olmuştur (Berg, Seymour ve Goel, 2013). Bu durum bilginin üretilmesinin yanında geniş kitlelerin erişimi için paylaşılması konusunda yaşanan gelişmeleri göstermektedir. Bu dönem çevrimiçi öğretim teknolojileri ve araştırmaları özelinde incelendiğinde 1990-2000 yılları arasında eğilimin web temelli öğrenme, zeki öğrenme sistemleri, öğrenme toplulukları, birlikte öğrenme konuları üzerine yoğunlaştığı görülmektedir (Sun vd., 2014).
- 2000'li yıllar ve günümüz: 2000 yılına gelindiğinde ".com" ve ".net" alan adları eğitim kurumları için kullanılan ".edu" alan adını sayı olarak katlamış (Mowery ve Simcoe, 2002), 2001 yılında ise internet işletmeleri için oldukça popüler hale gelen "nokta com" (dot-com) balonunun patlamasıyla (O'reilly, 2007) web 1.0'dan web 2.0'a geçiş bilgi ve iletişim çevrelerinde bir devrim olarak nitelendirilmiştir. Web 1.0, web teknolojilerinin ilk jenerasyonu olarak kabul edilmektedir. Salt-okunur (read-only web) web olarak tabir edilen web 1.0, ticaret ve hizmet sektörü dünyasının insanlara bilgilerini paylaştıkları, kullanıcıların içeriğe katkısının hemen hem hiç olmadığı, sadece istediği bilgiye dair arama yapıp ona eriştiği teknoloji iken; 2004 yılında resmi olarak duyurusu yapılan ve bilge-web (wisdom-web) olarak da isimlendirilen web 2.0, kullanıcıların daha fazla etkileşime girebildiği,

içeriğin kullanıcılarla birlikte oluşturulduğu teknoloji olarak nitelendirilmiştir (Aghaei, Nematbakhsh ve Farsani, 2012). Youtube, Twitter, Facebook, Wikipedia gibi web siteleri web 2.0 teknolojisinin en önemli örneklerini oluşturmuşlardır. Web 2.0 teknolojisini kullanan herhangi bir web sitesine kullanıcıların içerik olarak katkıda bulunulabilmesi oluşturulan veri miktarını büyük miktarda artırmıştır. 2005 yılında Apple firmasının cep telefonu pazarına yeni nesil ürününü sürmesi ile akıllı telefon kavramı yaygın olarak kullanılmaya başlanmış ve bu sektör en hızlı büyüyen sektörlerden biri haline gelmiştir (Gülpınar ve Atıcı, 2014). İvmeli bir hızla yayılan internet bağlantısı ile birlikte web 2.0 teknolojilerinin akıllı telefon kullanıcılarının hizmetine sunulur hale gelmesi oluşturulan veri miktarının katlanmasına yol açmıştır. Anlamsal web (semantic web) olarak da adlandırılan web 3.0'ın alanyazına girmesini tetikleyen gelişmeler; internet hızının ve erişilebilirliğinin artması, kendi kendine veri üretebilen veya bir başka sistemin veri üretilmesine aracı olan akıllı cihazların işlemci hızları, bağlantı kapasiteleri ve yine erişilebilirliklerinin artması olmuştur. Dünya çapında bir veri tabanı olarak da nitelendirilmekte olan web 3.0; kullanıcıların karmaşık sorgulamalarını, onları manalandırarak erişilmesini veya başka bir bilgiye bağlanmasını sağlayan sistemdir (Choudhury, 2014). Naik ve Shivalingaiah (2008) web 3.0'ın interneti bir veri tabanına dönüştürdüğünü, oluşturulan içeriğin farklı uygulamalar, cihazlar veya kullanıcıların erişimine açan evrim niteliğinde bir gelişme olduğunu vurgulamışlardır. Web 3.0 veriye bağımlı olan veri madenciliği, makine öğrenmesi, doğal dil işleme ve yapay zeka gibi kavramların da daha sık kullanılmaya başlanmasını sağlamıştır (Dwivedi vd., 2011). Depolanabilen verinin hacminde oluşan artış, depolanma şekli ve veri yapısı öncelikli olmak üzere, veri üzerinde yapılabilecek işlemlerin ve analizlerin seyrini değiştirmiş bu da veri tabanı sistemlerinin değişimini sağlamıştır. Hacim olarak büyük veri üzerinde güncelleme ve arama işlemlerinde yaşanan yavaşlıklar, büyük ölçekte veri depolama ve veri işleme için tasarlanmış dağınık, ilişkisel olmayan veri tabanları olarak adlandırılan NoSQL (Not only SQL [Structured Query Language]-Yalnız Yapılandırılmış Sorgu Dili olmayan) (Moniruzzaman ve Hossain, 2013) kavramının oluşmasına ön olmuştur. Han, Haihong, Le ve Du (2011) NoSQL'in ortaya koymuş olduğu avantajları; büyük miktardaki verinin okunması ve yazılması konusundaki hızı, genişletilmesinin kolay ve az maliyetli olması olarak sıralamışlardır. 2000'li yıllardan

başlayarak bilgi ve iletişim teknolojilerinde yaşanan bu gelişmeler çevrimiçi öğretim olgusunu evirerek daha kapsamlı bir hale getirmiş, "büyük veri" kavramının alanyazında artan bir sıklıkta kullanılmaya başlanmasını sağlamış; genelde öğretim teknolojileri özelde çevrimiçi öğrenme konusunda yapılan çalışmaların yönünü değiştirmiştir.

Büyük Veri ve Veri Madenciliği

İnsanoğlu var olduğundan beri bir ihtiyaca karşılık verebilmek adına vuku bulan iş ve işlemlerle ilgili verileri kaydede gelmiştir. Bir doğa olayı olan güneşin hareketlerini kaydederek takvimin bulunduğu antik Mısır'da da, bir sonraki ay tahsil edilmek için veresiye defterine borç işlenen mahalle bakkalında da, faturalandırılmak için milyarlarca görüşmenin veri tabanlarına kaydedildiği telekomünikasyon şirketlerinde de ortak özneyi kaydedilen veri oluşturmaktadır. Gelişen teknoloji ile birlikte kayıt altına alınan verinin yapısında ve miktarında büyük değişiklikler yaşanmıştır. Bulunduğumuz tarihten otuz yıl öncesinde bireysel bir taşıtla ilgili şase numarası, alıcısı, satıcısı, sigortası gibi kâğıt dosyalarda tutulan bilgilerden, aracın hangi parçasının hangi ülkede hangi tarihte üretildiği ve araca monte edildiğinden, aracın trafiğe çıktığı andan itibaren hangi yoldan kaç defa hangi hızda ve yönde geçtiğine, kaç kilometre yol yaptıktan sonra rutin bakıma girdiği ve hangi marka yağın hangi tarihte ne miktarda değiştirildiğine kadar veriler oluşturulmakta ve kaydedilmektedir. Web teknolojilerinin ilk versiyonu web 1.0'ın sadece oluşturulan içerikle ilgili arama ve okuma işlemlerinin yapılmasına olanak tanıyan yapısı, o dönem kayıt altına alınabilecek veriyi web sitesi sahibinin oluşturduğu içerik, web sitesine erişilen tarih, saat ve IP adresi ile sınırlamıştır. Ancak web 2.0'ın kullanıcıların içeriğe katkı yapabilmesini sağlayan ve web 3.0'ın kullanıcı katkısına gerek duymadan kendi kendine içerik üreten yapısı kaydedilen veri yapısının çeşitlenmesine ve hacminin artmasına sebep olmuştur. Tüm dünyada 2003 yılına kadar üretildiği değerlendirilen veri miktarı 5 exaByte (1 exaByte = 1 milyon gigaByte) olarak belirtilirken (Hammad, Fakharaldien, Zain ve Majid, 2015); 2025 yılında üretilecek dijital veri miktarının 175 zettaByte (1 zettaByte = 1000 exaByte) olması öngörülmektedir (Coughlin, 2018). Web 1.0 teknolojisi üzerine kurgulanmış çevrimiçi öğretim sistemleri üzerinde oluşturulan ve kaydedilen veri yapısındaki çeşitlilik ve veri miktarındaki hacim ile web 3.0 teknolojisi üzerine kurgulanan

çevrimiçi öğretim sistemleri üzerinde oluşturulan ve kaydedilen veri yapısındaki çeşitlilik ve veri miktarındaki hacim arasındaki fark açıklanan değişimle paralellik gösterecektir. 2018 yılı verilerine göre kitlesel çevrimiçi ders ortamlarında yaklaşık 900 üniversitede yaklaşık 100 milyon katılımcıya yaklaşık 12 bin ders verildiği belirtilmiştir (Shah, 2019).

Alanyazında büyük veri kavramı üzerinde özünde benzer olmakla birlikte farklı tanımlamalara rastlamak mümkündür. Madden (2012) büyük veriyi, mevcut olan araçlarla işlemesinin zor olduğu, hızın işlemdeki çabuklukla ilgili olması gerekirken miktarındaki büyümeyi tarif ettiği, birçok kaynaktan toplanarak bir araya gelen yüksek miktardaki veri olarak tanımlamıştır. Storey ve Song (2017) ise yapılandırılmış veya yapılandırılmamış, analiz edildiklerinde kararlar almaya yardımcı olan yüksek miktardaki veriyi büyük veri olarak tanımlamışlardır. Tech Amerika Vakfı Federal Büyük Veri Komisyonu (S. Mills vd., 2012) ise büyük veriyi, elde edilmesi, kaydedilmesi, dağıtılması, yönetilmesi ve analiz edilmesi için gelişmiş teknik ve teknolojilere ihtiyacın duyulduğu, yüksek hızda büyüyen, karmaşık ve yüksek hacimdeki veriyi büyük veri olarak tanımlamıştır. Alanyazında büyük verinin karakteristik özelliklerini beş ana başlıkta inceleyen çalışmalar bulunmakla birlikte (Örn:Demchenko vd. (2014): Hacim, çeşitlilik, hız, gerçeklik, değer) genel olarak üç karakteristik özelliğinden bahsedilmektedir. Gandomi ve Haider (2015) bu özellikleri şu şekilde sıralamıştır:

- Hacim: Verinin büyüklüğü ile ilgili karakteristik özeliğidir. Büyük veriler genel olarak terebaytlar veya petabaytlarla ifade edilmektedir. Ancak hacim zamana ve verinin tipine göre göreceli bir özellik olarak değerlendirilmektedir. Çünkü bugün büyük olarak sınıflandırılan veri gelecekte bu sınırın altında kalabilir. Benzer şekilde aynı büyüklükte olan video veri seti büyük veri olarak tanımlanamazken metin veri seti büyük veri olarak tanımlanabilir.
- Çeşitlilik: Veri setindeki yapısal heterojenlik ile tarif edilmektedir. İlişkisel veri tabanlarında bulunan yapılandırılmış, analizler için organize edilmesi gereken metin, resim, ses, video gibi yapılandırılmamış, XML gibi oluşturucusu tarafından tanımlanmış etiketleri bulunan yarı yapılandırılmış tipte bulunabilirler.
- Hız: Verinin üretilme ve analiz edilebilme sürati ile tanımlanmaktadır. Gelişen teknoloji ile özellikle akıllı cihazların veri üretme kapasiteleri artmış bu da öngörülemeyen miktarda

verinin çok çabuk bir şekilde ortaya çıkmasını sağlamıştır. Bu durum ise gerçek zamanlı analizlerin yapılması ihtiyacını da doğurmuştur.

Alanyazında bahsi geçen gerçeklik özelliği belirtilen yüksek hacimli veri kümelerinde %100 doğru veriye erişimin mümkün olamayacağı, kaydedilen verinin kalitesinin değişiklik gösterebileceği ve bu sebeple veri üzerinde yapılan analiz işleminin kalitesinin de veride bulunan kirlilikle orantılı olacağı ile ilgilidir. Değer özelliği ise büyük verinin potansiyelinin yüksek olması ancak kaydedilen yüksek miktardaki verinin analiz edilerek bir değer katılmadığı takdirde kullanışsız olması ile tarif edilmektedir (Anuradha, 2015).

Büyük verinin kavramsallaştırılmasına benzer bir şekilde alanyazında veri madenciliği kavramı üzerinde de özünde birbirine benzer ancak farklı tanımlamalar yapılmıştır. Hand (2007) veri madenciliğini büyük veri setleri içerisinden ilginç, beklenmeyen ve değerli yapıların keşfedilmesi olarak açıklamıştır. Larose ve Larose (2014) de benzer bir şekilde büyük veri setleri üzerinde kullanışlı şablonlar ve akımlar keşfetme işlemini veri madenciliği olarak tanımlamışlardır. Aronson, Liang ve Turban (2007), matematiksel, istatistiksel, makine öğrenmesi gibi yöntem ve tekniklerin kullanılmasıyla yüksek hacimli veri setleri üzerinden kullanışlı bilgileri açığa çıkarma ve manalandırma olarak tanımlamışlardır. Alanyazında örnekleri çoğaltılabilecek tanımlar incelendiğinde veri madenciliği ile veriden bilgi keşfi (Knowledge Discovery from Data) kavramlarının birbiri yerine kullanıldığı veya karıştırıldığı müşahede edilmektedir. Ancak veri madenciliği, veriden bilgi keşfi sürecinin sadece bir basamağını oluşturmakta ve bu durum Şekil 9 üzerinde gösterilmektedir (Han, Pei ve Kamber, 2011). Otomatik ve araştırmacı bir analiz ve modelleme işlemi olan veriden bilgi keşfi, büyük ve karmaşık yapıdaki veri setlerinden geçerli, yeni, kullanışlı ve anlamlı örüntüler tanımlama işlemi olarak tanımlanırken; bu işlemin çekirdeğinde yer alan ver madenciliği ise veriyi araştıran algoritmaları ve daha önceden bilinmeyen örüntülerin modellenmesi işlemlerini içerir (Maimon ve Rokach, 2010).

Şekil 9. Veriden bilgi keşfetme süreci

Veriden Bilgi Keşfetme Süreci

Veriden bilgi keşfetme süreci 7 aşamadan meydana gelmektedir. Bu süreç aşağıda belirtildiği şekilde incelenmektedir.

1- Verinin Temizlenmesi: Anuradha (2015) yüksek miktarlardaki verinin kalitesinin düşük olma ihtimalinin yüksek olduğunu, yapılacak analizlerin kalitesinin de verinin kalitesine bağlı olduğunu vurgulamıştır. Veri temizleme işlemi ise elde bulunan veri setinde analizin de kalitesini düşürecek olan değişkenlerin ortaya çıkarılarak veri setinin görece daha kaliteli duruma getirilmesidir (Salem ve Abdo, 2016). Van Hulse ve Khoshgoftaar (2009) veri kalitesini etiketleme hataları, verinin özelliği veya eksik değerler gibi etmenlerin etkileyebileceğini vurgulamışlardır. Sivogolovko ve Novikov (2012) analiz edilecek verilerin kalitesini dört değişken üzerinden incelemenin uygun olacağını bildirmişlerdir:

- Doğruluk: Kaydedilen veri ile gerçek veri arasındaki uyuşma derecesini göstermektedir. Örneğin; veri tabanında ders geçme notunun 50 puan olarak kabul edildiği bir sınavda 55 puan alan öğrencinin, aldığı nota rağmen "kaldı" olarak kayıt edilmesi veri setinin kalitesini düşürmektedir.
- Tamamlılık: iki göstergesi bulunmaktadır. İlk göstergesi veri setinin tüm verilerin ne kadarını kaydettiği ile ölçülürken ikinci gösterge veri setinde var olmayan girdilerden ne kadar az barındırdığı ile ilgilidir. Örneğin: Derse devam kayıtlarının alındığı bir sistemde,

sisteme girdisi yapılmayan bazı devamsızlıklar yapılacak olan analizin sonuçlarını etkileyecektir.

- Tutarlılık: Farklı veri setleri üzerinde aynı veri için bağdaşmazlık olmaması ile ilgilenen verinin formatı ve tanımında tekdüzeliğin sağlanması ile açıklanabilen değişkendir. Örneğin; bir veri setinde cinsiyeti erkek olarak belirlenmiş bir öğrencinin farklı bir veri setinde kadın olarak kaydedilmesi tutarsızlık oluşturacaktır.
- Vakitlilik: Veri setinde değeri zamana bağlı olarak değişebilecek veriler için önemlidir. Gerçek hayatta verinin meydana gelmesi ile verinin veri setine kaydedilmesi arasında geçen zamanla ilgilidir. Bir araştırmacı veri setini kullanmak istediği zaman verinin güncel olup olmaması analiz kalitesini düşürecektir. Örneğin; ders sürelerinin 40 dakikadan 45 dakikaya çıkarılmış olması vaktinde işlenmediği takdirde, bağlı analizler hatalı sonuçlar ortaya koyacaktır.

Sayılan değişkenlere göre kalitesi düşük olan veri setlerinin temizlenmesi için alanyazında farklı modeller ve yöntemler sunulmuştur. Veri setindeki tüm kayıtların ortalama değer, standart sapma, aralık gibi değerlerinin hesaplanarak bu değerlere uymayan verilerin çıkarılması (istatistiksel); kümeleme algoritmaları kullanılarak küme dışında kalan verilerin çıkarılması (kümeleme); önceden belirlenmiş bir örüntüye uymayan verilerin çıkarılması (örüntü-tabanlı) yöntemleri ile veri setlerindeki aykırı veriler temizlenebilirken (Maletic ve Marcus, 2009), eksik verilerin manuel olarak eklenmesi, genel bir değişkenle (örn: Null) doldurulması, en olası değerin seçilmesi veya sayısal verilerin ortalama değer ile tamamlanması vb. yöntemler kullanılarak veri temizleme işlemleri gerçekleştirilebilmektedir (Jing Han vd., 2011).

2- Verinin Entegrasyonu: Gerçek dünyada yararlı olabilecek ve analiz edilebilecek veriler yüzde yüz kullanılabilir olmamakla birlikte genel olarak birbirinden bağımsız veri tabanlarında, birbirinden farklı sağlayıcılardan elde edilen ve farklı formatlarda (ilişkisel, yapılandırılmış veya yapılandırılmamış) saklanıyor durumdadır (Giannadakis, Rowe, Ghanem ve Guo, 2003). Veri kaynaklarındaki bu heterojen durum aynı verinin farklı gösterimleri sunması veya aynı popülasyondan farklı örnekler alınması gibi sonuçlara da sebebiyet verebilmektedir (Scotney ve McClean, 1999). Belirtilen türde sıkıntıların önüne geçmek ve daha iyi bir analiz sonucuna erişmek için bağımsız veri kaynakları tarafından

sağlanan verilerin tek bir veri tabanında saklanmış gibi davranmalarını sağlama işlemi veri entegrasyonu olarak tanımlanmaktadır (Lim, Srivastava, Prabhakar ve Richardson, 1996). Örneğin bir öğrenci hakkında iki farklı okul verilerinin birleştirilerek analiz edileceği bir durumda, birinci veri tabanında sınav notlarının "Not" alanında tutuyorken ikinci veri tabanında "sınav_sonuc" alanında tutuluyor olması veya birinci veri tabanında "not" alanının öğrenci sınav sonuçlarının kaydedildiği alanken ikinci veri tabanında "not" alanının öğretmenin öğrenci hakkında verdiği görüşleri kaydediyor olması belirli entegrasyon işlemlerinin yapılmasını gerektirmektedir.

3- Verinin Seçilmesi: Alanyazında bazı araştırmacılar tarafından veriden bilgi keşfinin ilk aşamasında incelenmekte de olan verinin seçilmesi, uyulama alanının daha önce elde edilmiş bilgilerle harmanlanması ile ilgili olabilecek veri alanlarının ve alt kümelerinin veri setinden seçilmesi işlemidir (Ristoski ve Paulheim, 2016). Özellikle birbirinden bağımsız veri tabanlarının farklı amaçlar ve tasarımlarla oluşturulduğu göz önüne alındığında yapılacak analize etkisi olmayan, hatta sonuçlarda görülecek performansı düşürebilecek farklı özellikteki verilerin bulunma ihtimali yüksektir. Bu bağlamda veri setinden veri alanlarının ve alt kümelerinin seçilesi için Witten, Frank ve Hall (2011) iki farklı yöntem ortaya koymuşlardır. Verinin karakteristik özelliklerinin irdelenerek veri setinden ilgili alanın çıkarılmasını sağlayan filtreleme yöntemi diğer yönteme göre görece daha basit ve uygulaması kolaydır. Daha karmaşık ve uygulaması görece zor olan sarmalama yönteminde ise farklı makine öğrenmesi algoritmaları kullanılarak ilgili olan veri alanlarının seçilmesi sağlanmaktadır. Verinin seçilme işlemi örneklendirildiğinde; veri tabanında bir alan olarak bulunan öğrenci numarası sayısal, artan ve tekil bir değer aldığından yapılacak analiz sonucunun hatalı veya kalitece düşük olmasına sebep olacaktır. Bu sebeple alanın analize katılmaması uygun olacaktır.

4- Verinin Dönüştürülmesi: Veriden bilgi keşfetme sürecinin ilk 4 adımı farklı formlarda olan verilerin işlenerek madencilik işlemine hazır hale getirilmesidir. Madencilikten önceki son adım olan verinin dönüştürülmesi işlemi, veri üzerinde bazı operasyonlar gerçekleştirilerek verinin madencilik işlemlerine uygun hale getirilmesidir (Jing Han vd., 2011). Veri madenciliği aşamasında işe koşulacak olan bir algoritmanın belirli bir yapıda veri ile çalışabiliyor olması (örneğin sadece kategorik yapıda) veya ifade ediliş biçimindeki

gereksinimler (örneğin kategorik olan bir değerin sayısal olarak gösterilmesi) veri setinde dönüştürme işleminin yapılmasını mecbur kılmaktadır. Dash vd. (2011) sürekli değişkenlerin kesikli değişken olarak dönüştürülmesini tanımlayan ayrıklaştırma yönteminin madencilik açısından sağladığı avantajları, hafızayı daha az kullanması ve algoritmaların daha doğru ve hızlı çalışması olarak belirtmişlerdir. Verinin dönüştürülmesi işlemi örneklendirildiğinde; sürekli değişken tipinde ve numerik yapıda olan yaş değişkeninin x, y, z kuşağı gibi kategorik yapıya dönüştürülmesi, kullanılacak algoritma sadece sayısal verilerle çalışıyor ise de x=1, y=2, z=3 şeklinde dönüştürme gerçekleştirilmesi uygun olacaktır.

5- Veri Madenciliği: Veriden bilgi keşfetme sürecinin beşinci basamağını oluşturan veri madenciliği ilk dört adımda kendisi için uygun hale getirilen verilerin çeşitli metotlar kullanılarak örüntü çıkarma işleminin hayata geçirildiği basamaktır. Veri üzerinde geçerli, yeni, potansiyel olarak kullanışlı ve yüksek derecede anlaşılabilir örüntülerin tanımlanması işlemi olarak tanımlanabilir (Fayyad, Piatetsky, Shapiro ve Smyth, 1996). Disiplinler arasında yapıda olduğunu vurguladıkları veri madenciliği için Witten vd. (2011) istatistik, yüksek kapasiteli bilgi işleme ve veri tabanı sistemleri, makine öğrenmesi, algoritma gibi birçok farklı disiplinle iç içe olduğunu, her birinde gerçekleştirilen başarılı işlemin madencilik işlemini de etkilediğini vurgulamışlardır. Alanyazında büyük veri analiz yöntemleri için çeşitli sınıflandırmalar yapılmıştır. KS ve Kamath (2017) veri madenciliği uygulama çalışmalarının ya bir şeyi tahmin etme ya da bir şeyi tanımlama amacında olduklarından varsayımla sınıflandırmalarını tanımlayıcı ve tahmin edici yöntemler başlığı altında incelemişlerdir. Sahu, Shrma ve Gondhalakar (2011) ise sınıflandırmalarını alandan bağımsız olarak en yaygın kullanılan işlemlere göre kümeleme, sınıflandırma, regresyon ve birliktelik kuralı başlıkları altında gerçekleştirmişlerdir. Sivarajah vd. (2017) ise "ne oldu?" sorusuna yanıt aradıkları tanımlayıcı, "nasıl oldu?" sorusuna yanıt aradıkları teşhis koyucu, "gelecekte ne olabilir?" sorusuna yanıt aradıkları tahmin edici, "ne yapmalıyım?" sorusuna yanıt aradıkları önleyici, "ne tür önlemler almalıyım?" sorusuna cevap aradıkları önleyici analizler olarak beş kategoride incelemişlerdir. Alanyazında örneklerin artırılabileceği çalışmaların ortak özeliklerini kullanılan algoritmalar ve kullanış amaçları oluşturmaktadır. Sağlıktan, bankacılık uygulamalarına, kamu yönetiminden, eğitime kadar her alanda uygulama örnekleri ve çalışmaları bulunan veri madenciliği işlemleri için Mohamad ve Tasir

(2013), 2004-2012 yılları arasında ver madenciliğinin eğitimsel alanlara uygulandığı son çalışmaları inceledikleri araştırmalarında tahmin, sınıflandırma, kümeleme, birliktelik kuralları ve sıralı örüntü tekniklerinin kullanıldığını belirtmişlerdir. Benzer ve daha ayrıntılı bir şekilde Aldowah vd. (2019) 2000-2017 yılları arasında eğitsel veri madenciliği ve öğrenme analitiği başlıkları altında otoriter veri tabanlarında indekslenen 402 makaleyi inceledikleri çalışmalarında 12 tekniğin kullanıldığını, bunların kullanım sıklığı sırasına göre sınıflandırma, kümeleme, görsel veri madenciliği, istatistik, birliktelik kuralları, regresyon, sıralı örüntü, metin madenciliği, korelasyon madenciliği, aykırılık tespiti, nedensel madencilik ve yoğunluk tahmini olduğunu belirtmişlerdir. Yaygın olarak kullanılan yöntemlerden;

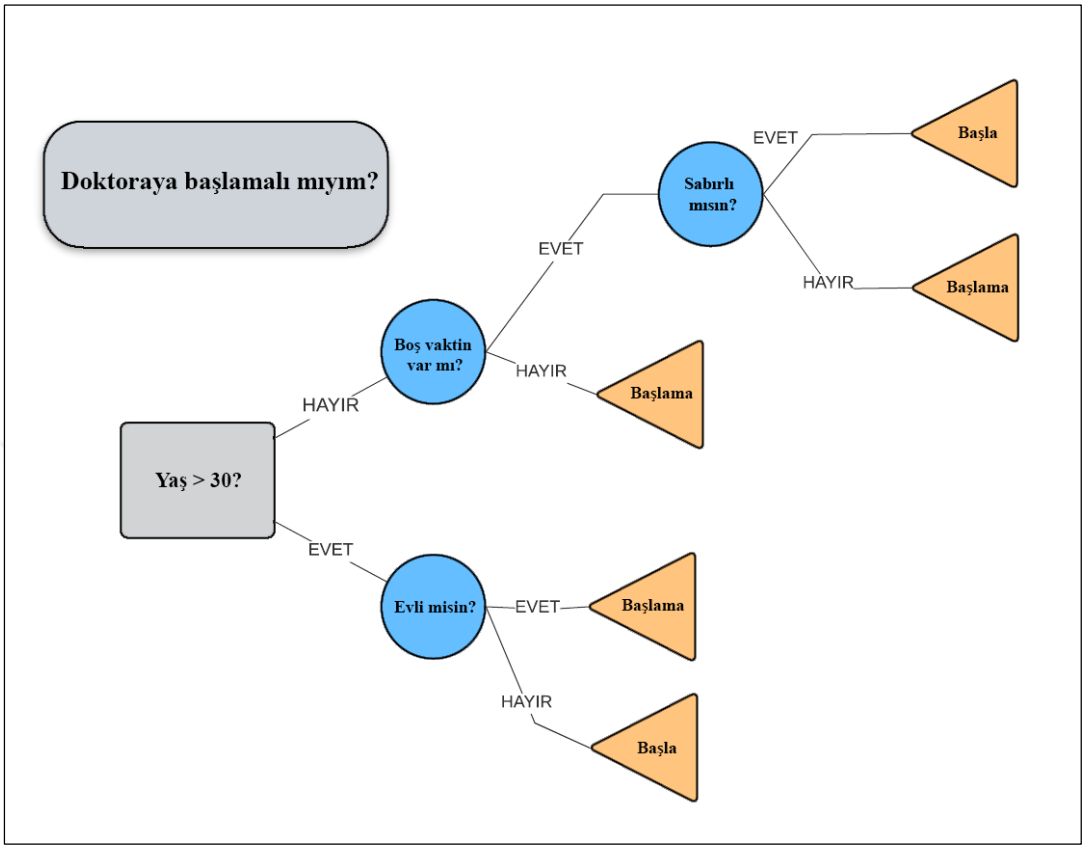
- *Tanımlayıcı Yöntemler:* Tanımlayıcı yöntemler tahmin yapılmayan, eldeki yapının keşfi için odaklanılan ve fakat analiz öncesinde bir etiketleme yapılamadan işlemler yapılan, alanyazında faktör analizi, yapı keşfi gibi yöntemleri bulunsa da en çok kümeleme yönteminin kullanıldığı algoritmalardır.
  - *Kümeleme:* Üzerinde çalışılan veri setinin barındırdığı özellikler ve ilişkiler değerlendirilerek, kendi içerisinde mümkün olduğunca yüksek oranda benzerlik gösterirken kendi dışındakilerle mümkün olduğunca düşük oranda benzerlik göstermesinin beklendiği gruplara bölünmesi işlemidir (Maione vd., 2019). Örneğin Valsamidis vd. (2012), çevrimiçi öğretim sistemi üzerindeki öğrenci hareketlerini kümeleme yöntemi ile analiz etmiş ve 8 ayrı küme elde etmişlerdir. Sekizinci küme üzerinde bulunan öğrencilerin ayrık matematik ve lineer cebir derslerini aldıklarının fark edildiğini belirtmişler, benzer konuları ve ödevleri bulunan bu iki dersin ders takvimi açısından çakışmayacak şekilde düzenlenmesine yardımcı olunabileceğini vurgulamışlardır.
- *İlişkisel Madencilik:* Nedensel madencilik, korelasyon madenciliği, sıralı örüntü çıkarma gibi yöntemleri bulunan ilişkisel madenciliğin birliktelik kuralı en yaygın kullanılan yöntemi olup, veriler arasında bulunan ilişkileri ortaya koymak için koşulan algoritmalardır (Baker ve Inventado, 2014). Örneğin Aher ve Lobo (2012), çalıştıkları kolejde çevrimiçi öğretim sisteminde kaydedilen gerçek veriler üzerinde birliktelik kuralı

algoritmalarını işe koşarak öğrencilerin hangi dersleri birlikte seçebileceklerine yönelik bir destek/öneri sistemi oluşturmuşlardır.

- *Aykırılık Belirleme:* Alanyazında bazı kaynaklarda sınıflandırma ve kümeleme algoritmalarının birlikte veya ayrı olarak kullanıldığı bir teknik olarak bahsedilirken bazı kaynaklarda ise ayrı bir başlık altında tanımlanmaktadır. Aykırı veri belirli bir sınıf veya küme altında gruplanamayan, istisna veya sürpriz veri olarak da adlandırılabilen veridir (Lakshmi ve Raghunandhan, 2011). Örneğin Ueno (2004) yapmış olduğu çalışma ile çevrimiçi öğretim sistemi üzerindeki içeriğe öğrenenlerin verdiği tepki süresi verilerini analiz ederek düzensiz öğrenme süreci yaşayan, aykırı olarak değerlendirilebilecek öğrenenleri tespit edildiğini belirtmiş, bu analiz sonucunda ortaya çıkan sonuçların eğitimciler tarafından öğrencilerle direk iletişim kurmak için kullanılabileceğini ortaya koymuştur.
- *Tahmin Edici Yöntemler:* Tez çalışması kapsamında da kullanılan tahmin edici yöntemler isminden de açık olduğu üzere veri seti üzerindeki veri özellikleri analiz edilecek gelecekte ne olabileceğini tahmin etmeye çalışan yöntemlerdir. Sınıflandırma ve regresyon analizleri en yaygın olarak kullanılan tahmin edici yöntemlerdir.
    - *Sınıflandırma:* Witten vd. (2011) sınıflandırma işlemini basitçe; veri setinde ve daha önce oluşturulmuş sınıflardan hangisinde olduğu belli olan verilerin bir eğitim işlemine tabi tutulması, ardından da bu sınıflardan hangisinde olduğu belli olmayan verilerin bu eğitim sayesinde hangi sınıfa ait olabileceğini belirleme işlemi olarak tarif etmişlerdir. Hatırlanacağı üzere Aldowah vd. (2019) tarafından yapılan çalışmada 2000-2017 yılları arasında eğitim alanında yapılan çalışmalarda en çok kullanılan veri madenciliği yöntemi olarak sınıflandırma göze çarpmaktadır. Veri sınıflandırma işlemi öğrenme ve sınıflandırma olarak iki aşamadan oluşmaktadır. Öğrenme aşamasında eğitilecek veriler, sınıflandırma algoritmaları tarafından analiz edilmekte; sınıflandırma aşamasında ise test verisi sınıflandırma algoritmasının doğru çalışma oranını tahmin etmek için kullanılmaktadır. Eğer doğruluk oranı kabul edilebilir bir seviyede ise algoritma yeni veri setleri üzerinde kullanılabilecektir (Ramageri, 2010). Sınıflandırmada önemli olan tahmin edici yöntemi kurgularken kullanılacak olan veri özelliklerinin doğru seçimidir. Kullanılacak algoritmaya bağlı olarak kullanılacak

özelliklerin korelasyonu incelenmeli, yüksek seviyede korelasyon gösteren özellikler çıkarılmalıdır (Brooks ve Craig, 2017). Naive-Bayes, lojistik regresyon, yapay sinir ağları, K-en yakın komşu, destek vektör makinaları ve bu tez kapsamında kullanılan karar ağaçları en yaygın kullanılan sınıflandırma yöntemleridir.

- *Karar Ağaçları:* Karar ağaçları, "böl ve yönet" stratejisine benzer bir mantıkla çalışan, ağaç benzeri sıralı karar alma yöntemidir. Çoğu karar ağacı algoritmaları tüm karar alma sürecinin, her biri tek bir özelliğe göre ayrılmış, sıralar halindeki daha küçük testlerle (veya kararlarla) halledilebileceği varsayımı ile çalışırlar. Aralarındaki fark ise bu küçük test veya karar parçalarını neye göre ayırdıklarıdır (Sinha ve Zhao, 2008). Bir veriyi belirlenen bir sınıfa atamak için en iyi sıralamayı oluşturmak için çalışan karar ağaçları, yapmış olduğu her bir test/karar ile ağacın dallarını oluşturur. Oluşan her dal ise kendinden sonra (varsa) gelebilecek yeni test/kararın gerçekleşmesini sağlar. Bu sıralama, karar/test işleminin yaprak düğüm adı verilen noktada son bulması ile kökten yaprak düğüme kadar olan "kural" ortaya çıkmış olur (Emel ve Taşkın, 2005) . Örnek bir karar ağacı Şekil 10 üzerinde gösterilmiştir.



Şekil 10. Örnek karar ağacı

Karar ağacı, karar alıcıya karar alırken hangi faktörlerin göz önüne alınması ve her bir faktörün kararın farklı çıktıları ile geçmişte nasıl ilişkili olduğunun belirlenmesi konusunda yardımcı olmaktadır. Karar ağacı algoritmalarında, dallara ayırmak için farklı yöntemler kullanır. Bu yöntemler bilgi kazancı (information gain), gini endeksi (gini index), kazanç oranı (gain ratio), ki-kare istatistikleri (chi-square statistics), DKM kriteri (DKM criterion), uzaklık ölçümü (distance measure), ikili kriter (binary criteria), ortogonal kriter (orthogonal criteria), Kolomograv-Smirnov kriteri (Kolomograv-Smirnov criteria) olarak sıralanabilir (Maimon ve Rokach, 2010). Örneğin bir karar ağacı, bilgi kazancı hesaplaması yapılarak bu değeri yüksek olan özelliğin ağacın en üstüne konumlandırılması ile başlatılır ve her düğüm için bu devam eder. Bilgi kazancı en ayırt edici niteliği belirlemek için (her aşamada) her nitelik için ölçülür. Bu ölçümde ise entropi endeksi kullanılır.

A özelliğinin S örneği için bilgi kazancı;

Kazanç (S,A) = Entropi(S) - ∑Pv Entropi (Pv) olarak hesaplanmaktadır.

(v= A'nın değerleri)

Karar ağaçlarında her özellik için ayrı ayrı bilgi kazancı hesaplanır ve bilgi kazancı en yüksek olanlar kök olarak alınır. Bu işlemler her düğüm için aşağıda sıralı durumlardan biri oluşuncaya kadar devam eder (Dinov, 2018);

1- Örneklerin hepsinin aynı sınıfa ait olması
2- Örnekleri bölecek özellik kalmaması
3- Kalan özelliklerin değerini taşıyan örneğin olmaması

Etkili olduğu kadar keşifçi bilgi araştırmaları için uygun olan karar ağaçlarının alanyazında kullanımının neden bu kadar yaygın olduğunu Gupta vd. (2017) şu şekilde açıklamışlardır:

- Karar ağaçları görselleştirilebilir bir yapıya sahip oldukları için anlaması ve müdahale etmesi kolaydır.
- Diğer yöntemler genellikle veri normalleştirmesi, aptal veri eklenmesi veya boş verilerin çıkarılması gibi ağır veri hazırlama işlemleri gerektirirken, karar ağaçları çok az veri hazırlama işlemine ihtiyaç duyar.
- Karar ağaçları diğer yöntemlerin aksine hem kategorik hem de numerik verirle çalışabilme yetisine sahiptir.
- Karar ağaçları çoklu-çıktı problemlerine de çözüm getirebilir.
- Beyaz kutu modelini kullanır. Genellikle iki tane çıktı (örneğin evet ya da hayır) olacağı için durumun açıklaması boolen mantığıyla kolayca açıklanabilir.

Karar ağaçları yöntemi için kullanılan birçok algoritma bulunmaktadır. Bu algoritmalardan örnekler aşağıdaki gibi açıklanabilir (Anyanwu ve Shiva, 2009; Gupta vd. 2017; Ture, Tokatlı ve Kurt, 2009; Su-lin ve Ji-zhang, 2009; McCarty ve Hastak, 2007):

- *CART Algoritması:* Sınıflandırma ve regresyon ağaçlarının kısaltması olan CART (Classification and Regression Trees) algoritması 1984 yılında Breiman tarafından oluşturulmuştur. İsminden de anlaşılacağı üzere hem sınıflandırma hem de regresyon ağaçları oluşturmaktadır. Ağaç dallarının oluşumu için gini endeksini kullanmaktadır. Veride eksik özellikler olsa da çalışabilen algoritma hem numerik hem kategorik verilerle çalışabilmektedir. Stabil olmayan karar ağaçları oluşturabilmesi ve tek bir değişkene göre dallanması dezavantajları olarak sıralanabilir.
- *CHAID Algoritması:* Ki-kare otomatik etkileşim detektörünün (Chi-square Automatic Interaction Detector) kısaltması olan CHAID algoritması uzun yıllardır veri tabanı segmentasyonu için kullanılan bir yöntemdir. Adından da anlaşılacağı gibi ki-kare tabanlı bir algoritmadır. Tüm veri setini iki veya daha fazla alt noda tekrarlı bir şekilde bölerek çalışır. Herhangi bir noddaki en iyi dallanmayı tahmin edici değişkenlerin izin verilen kategori çiftlerinin hedef değişkenle arasında istatistiki olarak bir fark kalmayana kadar bölünmesi ile belirlenir. Algoritma sadece nominal ve sıralı kategorik tahmin edicilerle çalışabilmektedir. Bu sebeple sürekli değişken tahmin edicilerin sıralı tahmin edicilere dönüştürülmesi gerekmektedir.
- *SLIQ Algoritması:* 1996 yılında Mehta vd. tarafından oluşturulmuştur. Hızlı ve ölçeklendirilebilir bir algoritma olan SLIQ ağaç dallandırma işlemini ön-sıralama tekniği kullanarak gerçekleştirmektedir. Numerik ve kategorik özellikteki veriler üzerinde çalışabilmektedir. Algoritma sınıf listesi veri yapısı ile çalıştığından kaynak tüketimi fazladır ancak dallanmanın sonlanması için kaynak tüketimi az olan MDL tekniğini kullanmaktadır.
- *SPRINT Algoritması:* 1996 yılında Shafer vd. tarafından oluşturulmuştur. Hızlı ve ölçeklendirilebilir bir karar ağacı sınıflandırıcı algoritması olan SPRINT histogram ve özellik listesi olmak üzere iki veri yapısı kullanmaktadır. Bu da hafızaya yük getirmediğinden büyük veri setleri üzerinde kullanılabilirliğini olanaklı kılar. Sıralı ve kategorik özellikteki veriler üzerinde çalışabilmektedir.
- *ID3, C4.5 ve C5.0 Algoritmaları:* ID3 algoritması 1986 yılında Quinlan Ross tarafından geliştirilmiştir. Hunt algoritmasını temel alarak geliştirilen algoritma

ağacının dallanması ve dalların bir süre sonra budanması mantığıyla çalışmaktadır. Dallanma için bilgi kazancı endeksini kullanmaktadır. Tüm ağaç yapısını veri setindeki verilerin kullanılması ile gerçekleştirir. Çok hızlı çalışmaktadır ancak küçük büyüklükteki veri setleri için aşırı-uyum problemi ile karşılaşılabilmektedir ve karar mekanizması tek özellik üzerinden gerçekleştirilmektedir. C4.5 algoritması ise yine Quinlan Ross tarafından 1993 yılında ID3 algoritmasının iyileştirilmiş hali olarak geliştirilmiştir. ID3 algoritmasının özelliklerine sahipken hem sürekli hem kategorik veriler üzerinde çalışabilmektedir. Uygulaması ve müdahale edilmesi kolay olup gürültülü ve eksik değeri olan verilerle çalışabilmektedir. Eğitim veri seti küçük olan durumlarda çok iyi çalışmamaktadır. C5.0 algoritması ise C4.5 algoritmasının gelişmiş versiyonudur.

Quilan Ross tarafından geliştirilen ve C4.5 algoritmasının geliştirilmiş versiyonu olan C5.0 algoritmasının özelliklerini ve artılarını Patidar ve Twari (2013) şu şekilde açıklamıştır:

- Karar ağacı oluştururken hem kategorik hem de sürekli verileri kullanabilmektedir.
- Eksik verilerle başa çıkma kabiliyeti yüksektir.
- Sınıflandırmanın doğruluk oranını artırmak için iyimser budama yöntemini kullanarak gereksiz özellikleri çıkarma yeteneğine sahiptir.
- Çapraz doğrulama ve artırma (boosting) yeteneğine sahiptir.
- Araştırmacılar için büyük kolaylık sağlayan hem dallanmalı büyük karar ağaçları hem de kural setleri oluşturabilmektedir.
- Sınıflandırma için ilişkili olan kadar olmayan özellikleri de tahmin edebilmektedir.
- Karşılaştırma yapıldığında
    - C5.0 algoritması C4.5 algoritmasına göre daha hızlıdır.
    - Kural seti oluşturmada daha az veri kullanır.
    - Kural setlerini daha küçük oluşturabilirken daha fazla doğruluk oranına sahiptir.
    - Daha küçük karar ağaçları oluşturabilmektedir.

- Farklı değişkenlerin ağırlıklandırılmasına olanak tanımaktadır.

Veri madenciliğinin en büyük sorunlarından birini veri setinin dengelenmemiş olmasıdır. Ohsaki vd. (2017) dengelenmemiş veri setini; örneklemlerden oluşan sınıflardan birinin çok fazla sayıda örnek içermesine (çoğunluk) karşın diğer sınıfın görece çok daha az sayıda örnek içermesi (azınlık) olarak açıklamışlardır. Rastgoo vd. (2016) dengelenmemiş veri setinin veri madenciliğinin en önemli 10 problemi arasında olduğunu belirtmişler, H. He ve Garcia (2009) ise veri madenciliği algoritmalarının dengelenmiş veri üzerinde çalışmayı beklediklerini vurgulamışlardır. Bu durum analojik bir yöntemle şu şekilde açıklanabilir. Belirli kriterleri değişken olarak işe koşup bir öğrencinin bir dersten başarılı olup olmayacağını tahmin etmeye çalıştığımızı düşünelim. Veri setimizde eğer %98 oranında başarılı olan öğrenciler varken sadece %2 oranında başarısız olan öğrenciler varsa bu veri seti dengelenmemiş olarak adlandırılmaktadır. Bu durumda işe koşacağımız her hangi veri madenciliği algoritması başarısız olarak adlandırılan %2 oranlı sınıfı göz ardı edecektir. Çünkü algoritmaya dâhil edilen herhangi bir örnek için "başarılı" şeklinde bir sonuç döndürmesi algoritmanın %98 oranında doğru tahmin etmesini sağlayacaktır. Gerçek yaşantı genel olarak doğası gereği dengelenmemiş veri setlerinden oluşmaktadır. Belirli bir tip kanser hastalığı hakkında yapılan çalışmalarda, belirtilen tip kanserli hasta sayısının hasta olmayan birey sayısına oranının çok düşük olması, şüpheli bir ağ trafiğinin belirlenmesi konusunda yapılacak olan çalışmada şüpheli olarak adlandırılabilecek trafiğin tüm ağ trafiğine oranının çok düşük olması veya kredi kartı dolandırıcılığının belirlenmesi için yapılacak bir çalışmada şüpheli kredi kartı işlemlerinin tüm kredi kartı işlemlerine oranın çok düşük olması gerçek hayatta karşılaşılan doğal dengelenmemiş veri seti örnekleridir. Krawczyk (2016) dengelenmemiş veri üzerinde yapılan çalışmaların son yirmi yıldır araştırma konularının hala odağında olduğunu, veri madenciliği çalışmalarının giderek artmasıyla birlikte dengelenmemiş veri üzerinde daha derin araştırmalar yapılmaya başlandığını vurgulamıştır.

Zang vd. (2016) dengelenmemiş verilerin kullanılabilmesi için iki farklı yöntem kullanıldığını bunların veri seviyesinde ve algoritma seviyesinde yöntemler olduğunu belirtmiştir. Veri seviyesinde yapılan işlemlerin azınlıkta bulunan verilerin sentetik veya adaptif bir biçimde çoğaltılması olarak alanyazında karşımıza çıktığını belirtmiştir. Fernández, del Río, Chawla ve

Herrera (2017) ise dengelenmemiş verilerin veri seviyesinde, algoritma seviyesinde ve maliyete duyarlı öğrenme yaklaşımları ile çözülebileceğini belirtmiştir. Benzer bir şekilde Lema^ıtre, Nogueira ve Aridas (2017), son teknolojik gelişmeler ışığında dengelenmemiş verilerin kullanılabilmesi için çoğunluk sınıfın azaltılması, azınlık sınıfın çoğaltılması, azaltma ve çoğaltma işlemlerinin birlikte kullanılması ve topluluk öğrenme yöntemlerinin şeklinde dört grupta işlem yapıldığını belirtmiştir.

Thammasiri, Delen, Meesad ve Kasap (2014) öğrenci yıpranması konusunda yapmış oldukları çalışmada çeşitli makine algoritmaları karşılaştırmışlar, C5.0 algoritmasını dengelenmemiş veri seti üzerinde rastgele azınlık sınıfın çoğaltılması yöntemini kullanarak uygulamışladır. Belirtilen kombinasyonun diğer tüm algoritmalardan daha hassas duyarlılıkta sonuç verdiğini belirtmişlerdir. Wiharto, Kusnanto ve Herianto (2016) koroner kalp krizi konusunda klinik veriler üzerinde yaptıkları çalışmada azınlık sınıfın çoğaltılması metodu ile dengelenmemiş verileri dengeleyerek ve C4.5 algoritmasını kullanarak daha önceki çalışmalarında gelişme kaydettiklerini bildirmişlerdir. Gu vd. (2016) dengelenmemiş veriler üzerinde çalışan en iyi 10 algoritmadan biri olarak tanımladıkları C4.5 algoritması ile 10 ayrı dengelenmemiş veri seti üzerinde yaptıkları çalışmada azınlık sınıfın çoğaltılması yöntemini kullanmışlar ve 9 veri setinde daha iyileştirilmiş sonuç aldıklarını vurgulamışlardır. Alshammari ve Nur Zincir-Heywood (2015) VOIP (Voice over Internet Protocol – İnternet protokolü üzerinden verine ses hizmeti) üzerinde şifrelenmiş trafiğin tanımlanması için C5.0, AdaBoost ve Genetik programlama (GP) algoritmalarını karşılaştırdıkları çalışmalarında C5.0 algoritmasının diğer algoritmalara göre daha iyi sonuç verdiğini belirtmişlerdir.

Fu vd. (2018), 355 hasta verisi üzerinden limpeda durumlarının varlığını sınıflandırmak için C4.5, C5.0, GBM, ANN ve SWM algoritmalarının doğruluk oranlarını karşılaştırdıkları çalışmalarında ANN (Yapay Sinir Ağları) algoritmasının 93.75 doğruluk oranı ile en iyi sonucu verdiğini belirtmişlerdir. Golkarian, Naghibi, Kalantar ve Pradhan (2018) yeraltı sularının potansiyel haritalarını doğrulamak için C5.0, rastgele ormanlar (RF) ve çok değişkenli uyarlanabilir regresyon uzanımları (MARS) algoritmalarını karşılaştırdıkları çalışmalarında ise %84.2 doğruluk oranı ile MARS algoritmasının en iyi sonucu verirken %77.3 doğruluk oranı ile C5.0 algoritmasının görece en kötü sonucu verdiğini belirtmişlerdir. Shirwaikar vd. (2016)

yeni doğan bebeklerin ilk haftalarında meydana gelebilecek apne bölümlerini tahmin etmek için destek vektör makineleri (SVM), C5.0 ve rastgele ormanlar (RF) sınıflandırma algoritmalarını karşılaştırdıkları çalışmalarında %88 doğruluk oranı ile rastgele ormanlar (RF) algoritmasının görece en iyi sonucu ortaya koyduğunu vurgulamışlardır.

Literatürde kullanılan sınıflandırma algoritmalarının kullanılan veri seti, öznitelikler, sınıf sayısı, okunabilirlik, kaynak tüketimi vb. konularında birbirine üstünlük kurduğu durumlar bulunmakla birlikte sıklıkla çalışılmalara konu edilmektedir.

6- Örüntü Değerlendirmesi

Herhangi bir veri seti üzerinde herhangi bir veri madenciliği algoritması işe koşularak bir örüntü ortaya çıkarmak basit bir işlemdir. Aynı veri seti üzerinde farklı parametrelerle farklı algoritmaların işe koşulması ile sayısız örüntü ortaya çıkarılabilir. Ancak bu durumda ortaya çıkan her örüntünün değerli olup olmadığı sorgulanması gerekir. Göreceli bir kavram olan "değer" konusunda Jiawei Han ve Kamber (2006) örüntü değerlendirmesi yaparken hesaba katılabilecek parametreleri:

- Örüntü insanlar tarafından kolay anlaşılabilir mi?
- Örüntü yeni veri seti üzerinde kesinlik açısından belirli bir derecede geçerli mi?
- Örüntünün kullanılabilirlik potansiyeli var mı?
- Örüntü yeni mi?

olarak sıralamışlardır. Bu objektif perspektifin sübjektif tanımlamalarla birleştirilmesi gerektiğini belirten yazarlar; bir marketten devamlı alışveriş yapan bireylerin karakteristik özelliklerini tarif eden bir örüntünün bir veri analisti için genel geçer bir durum olmasına rağmen market sahibi için değerli olacağını belirtmiş, bu durumun göz önüne alınmasının gerekliliğini vurgulamışlardır.

7- Bilginin Gösterimi

Veriden bilgi keşfi sürecinin son aşamasını bilginin gösterimi oluşturmaktadır. Planlama ve bilginin nasıl kullanılacağı işlemlerini kapsar (Cios, Pedrycz ve Swiniarski, 2007). Açığa çıkan bilginin bir sisteme entegre edilmesi, basitçe raporlaştırılması, ilgili paydaşlara iletilmesi ve

potansiyel fikir ayrılıklarının çözüme kavuşturulması bu aşamada gerçekleştirilir (Mariscal, Marbán ve Fernández, 2010)

Uyarlanabilir Çevrimiçi Öğrenme Sistemleri

İnternet teknolojilerindeki gelişmeye paralel olarak çevrimiçi öğrenme sistemleri konusunda da gerek alanyazında gerekse de ticari amaçlarla araştırmalar ve geliştirmeler yapılmış ve yapılmaya devam etmektedir. Belirtilen koşut çalışmalar göz önüne alındığında; web 1.0 teknolojilerinin sunduğu, kullanıcının sadece içeriği okuyabildiği metinlerden, ses, video ve animasyon ile içeriklerin zenginleştirildiği sistemlere; web 2.0 teknolojilerinin yaygınlaşması ile kullanıcının içerikle etkileşime girebildiği öğretim sistemlerine gelişmelerin yaşandığı gözlenmektedir. Web tabanlı öğretim sistemlerinin araştırma ve geliştire açısından yoğun bir alan olduğunu belirten Brusilovsky (1998) birçok çalışmanın hiper metinlerin bir araya geldiği statik bir ağdan öteye gitmediğini, uyarlanabilirliğin web tabanlı öğretim sistemleri için özellikle önemini şu iki sebeple açıklamıştır:

1- Web tabanlı öğretim sistemleri çok çeşitli kullanıcılar için hazırlanmakta olup, bir kullanıcı için uygun olan diğeri için uygun olmayabilir.
2- Birçok durum için kullanıcı, dersi yalnız olarak, bir çalışma arkadaşı veya öğretmenin sınıfta olduğu gibi bireysel yardımları olmadan işlemektedir.

Benzer bir şekilde Riding ve Rayner (1998), öğrenenlerin sahip olduğu farklı kişilik özellikleri, öğrenme biçimleri, bilgiyi işleme biçimleri ve bilgiyi elde etme konusunda yaptıkları farklı tercihlerin, aynı öğrenme ortamını kullanırken farklı öğrenme gereksinimlerinin oluşmasına sebep olduğunu vurgulamışlardır. Uyarlanabilir öğretim sistemleri, öğrenenlerin tercihleri, bilgi, ilgi ve hedefleri göz önüne alınarak bir modelinin oluşturulması ile öğretim ortamının bu modele göre yapılandırılması ve her bir öğrenen için öğretimin kişiselleştirilmesi ile ortaya çıkan; öğrenenin tarama alanını sınırlayıp ona en uygun bağlantıları önererek, yararlanabileceği farklı ve özel bilgi parçalarına erişmesini sağlayarak destekleyen hiper ortam olarak tanımlanabilir (Brusilovsky, 1996).

Hiper ortam; statik grafikler, resimler veya tablolar ihtiva eden düğüm ve bu düğümleri birbirine bağlayan bağlantılardan oluşan hiper metinlere ek olarak dinamik yapıdaki animasyon, diyagram, ses ve vidonun beraber kullanıldığı ortam olarak tanımlanmaktadır (Tolhurst, 1995); De Vries ve De Jong, 1999; akt. Karadeniz, 2006). Hiper metin ve hiper ortamın doğrusal olmayan şekilde okunabilme, içeriklerin ve bağlantıların kolaylıkla değiştirilebilme ve güncellenebilme, içerik üzerinde kolayca arama yapılabilme, kolay erişilebilme avantajları, web tabanlı öğretim sistemleri çalışmalarının var oluşunu sağlamıştır. Brusilovsky (2001) farklı ön bilgi, ihtiyaç ve ilgileri olan öğrenenlerin öğrenme ve bu işlemdeki memnuniyetlerini sağlamak konusunda, tüm kullanıcıları için aynı içeriği ve bağlantıları sunan öğrenme ortamlarının yetersizliğini vurgulamış, uyarlanabilir hiper ortamların geleneksel "tek beden hepsine uyar" yaklaşımına alternatif olabileceğini belirtmiştir. Smith (1999) ise uyarlanabilir öğrenme ortamlarına neden ihtiyaç duyulduğunu şu şekilde açıklamıştır:

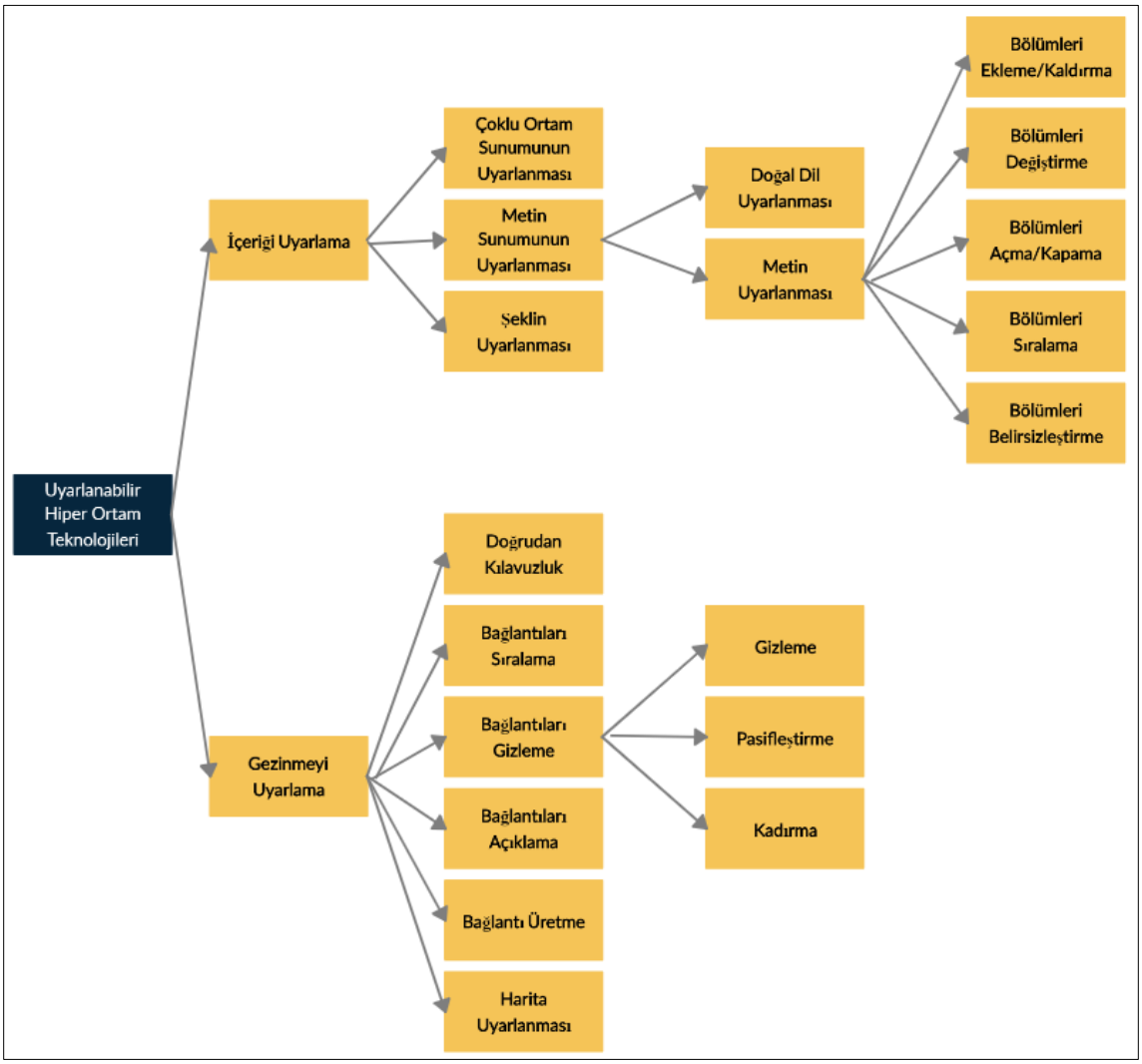
1- Etkili öğretim sistemi öğrenene kendi kabiliyetleri ile örtüşen ve onun önbilgi ve gereksinimlerine uygun olarak bilgiyi oluşturabileceği materyaller sunması gerekmektedir. Ancak geleneksel sistemler bu durumu sağlayamamaktadırlar.
2- Hiper ortamların avantaj olarak görünen özelliklerinin (arama yapılabilmesi, yoğun miktarda bilgi içerebilmesi vb.) öğrenen için fazla bilgi yüklemesi (information overload) ve yönlendirme problemlerine yol açabilmektedir.

Gelişen teknoloji ile birlikte üretilen ve tüketilen bilgi miktarındaki artış hemen her alanda kişiselleştirme kavramının önemini ve çalışma alanını artırmıştır. Çevrimiçi alışveriş yapılabilen web sitelerinde milyonlarca ürün içerisinden kullanıcının ilgi ve ihtiyaçlarına uygun düşenlerin kendisine öneri olarak sunulması, eş anlamlı olan kelime öbekleriyle yapılan web aramalarının kullanıcının ilgi alanına göre olan sonuçları önce döndürmesi oluşan bu veri ve bilgi yoğunluğunun sonucunda ortaya çıkan uyarlanabilir sistemler olarak kaşımıza çıkmaktadır. Çevrimiçi öğretim de aynı düzlemde gelişim göstermektedir. Çevrimiçi öğretim imkânı sunan eğitim kurumlarının, ders sayılarının ve dolayısıyla öğrenen sayısının artmasının benzer ihtiyaçları doğurması hayatın olağan akışıyla da paralellik göstermektedir. Shah'ın (2019) belirttiği ve yukarıda verilen çevrimiçi derslerle ilgili yüksek rakamlar bu durumun göstergesidir.

Her farklı kullanıcı için bir modelin, kullanıcıların amaç, tercih ve bilgi birikimlerinden yararlanılarak meydana getirildiği ve sistem ile kullanıcı arasındaki etkileşimde uyarlamanın gerçekleştirilebilmesi içi bu modelin kullanılması olarak tanımladığı, uyarlanabilir hiper ortam sistemi için Brusilovsky (2001); uyarlamanın özünü oluşturan ve yanıtlanması gereken soruları şu şekilde vurgulamıştır:

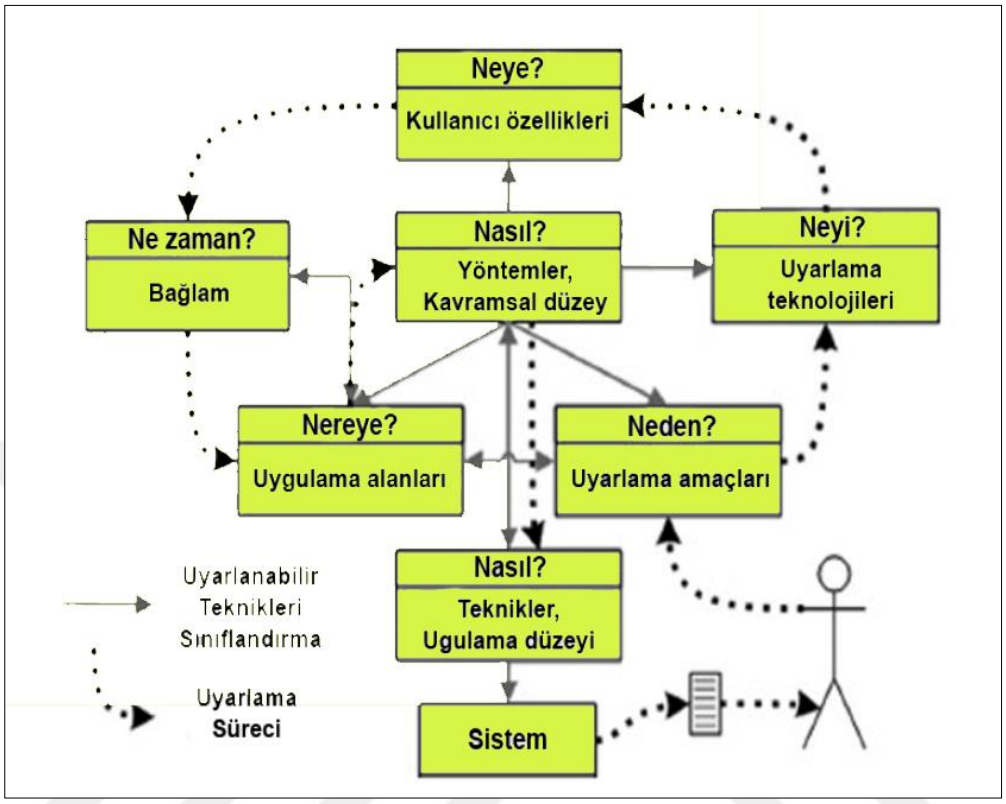
- Neyi uyarlayabiliriz?
- Neye uyarlayabiliriz?
- Neden uyarlamalıyız?
- Nereye uyarlayabiliriz?
- Nasıl uyarlayabiliriz?

Brusilovsky (2001) verdiği cevaplarla gerçekleştirdiği uyarlanabilir hiper ortam uyarlaması yöntem ve tekniklerinin sınıflandırması Şekil 11 üzerinde gösterilmektedir.



Şekil 11. Uyarlanabilir hiper ortam teknolojilerinin taksonomisi. Brusilovsky, P. (2001). Adaptive Hypermedia. *User Modeling and User-Adapted Interaction, 11*, 87-110 kaynağından uyarlanmıştır.

Knutov, De Bra ve Pechenizkiy (2009) ise hiper ortamın uyarlanması yöntem ve tekniklerinin sınıflandırıldığı Brusilovsky (2001) çalışmasından yola çıkarak, "neden uyarlamalıyız?" sorusunun yanıtlanması ile başlattıkları uyarlama yöntem ve tekniklerini süreç olarak modellemişlerdir. Uyarlama süreci Şekil 12 üzerinde gösterilmiştir.



Şekil 12. Uyarlanabilir hiper ortam yöntem ve teknikleri uyarlama süreci. *Knutov, E., De Bra, P., & Pechenizkiy, M. (2009). AH 12 years later: A comprehensive survey of adaptive hypermedia methods and techniques.* New Review of Hypermedia and Multimedia, 15*(1), 5-38* kaynağından uyarlanmıştır.

1- Kullanıcı modelinin oluşturulması

2- Uyarlamanın gerçekleştirilmesi

Uyarlanabilir sistemler kullanıcı modelinin oluşturulmasını onun hakkında öncelikle bilgileri toplayarak sonraki aşamada ise bu bilgileri işlemesiyle gerçekleştirmektedir. Oluşturulan model doğrultusunda sistem üzerinde uyarlamalar gerçekleştirilmektedir. De Bra, Houben ve Wu (1999) uyarlanabilir sistemlerin dört bileşenini şu şekilde açıklamışlardır:

1- Alan Modeli: Bilginin nasıl yapılandırıldığını ve birbirleriyle nasıl bağlantılandırıldığını açıklar.

2- Kullanıcı modeli: Uyarlanabilir bir hiper ortamın kullanıcı hakkında depolanan bilgileri tarif eder ki bu kayıtlı bilgiler kullanıcının kazandığı bilgiyi ve ziyaret ettiği düğümleri içerir.

3- Öğretme modeli: Alan modeli ve kullanıcı modeliyle birleşerek adaptasyonun sağlanması için sunulacak yöntemlerin nasıl olacağını açıklayan pedagojik kurallardır.
4- Uyarlama mekanizması: Her bir farklı kullanıcıya göre içerik ve gezinmenin uyarlandığı esas mekanizmadır.

Çevrimiçi öğretim sistemleri özelinde uyarlanabilirlik göz önüne alındığında modellenecek kullanıcıyı öğrenenler oluştururken, gerçekleştirilecek uyarlama öğretim sistemi üzerinde sunulacak olan içeri ve öğrenenin sistem üzerindeki gezinmesinden oluşmaktadır. Bu durumda Somyürek'in çalışmasına (2008) koşut olarak; öncelikli öğrenci hakkında bilgilerin toplanarak bir modelin oluşturulması daha sonra bu modele göre çevrimiçi öğretim sistemi üzerinde içerik ve gezinmeye yönelik uyarlama işleminin gerçekleştirilmesi gerekmektedir.

Nakic, Granic ve Glavinci (2015) 2001-2013 yılları arasında yayınlanan uyarlanabilir öğretim sistemlerinde kullanıcı modellemenin anatomisini ortaya çıkarmayı hedefledikleri çalışmalarında; demografik özellikler, kişilik özelikleri, işlem hızları, öğrenme stili, bilişsel yetenekler gibi birçok bireysel farklılığı çalışmalara dâhil edildiğini vurgulamışlardır. Ciloglugil ve Inceoglu (2012) ise öğrenen modellemesi için kullanılan bu bilgilerin, alanyazında yapılan çalışmalar incelendiğinde:

- Öğrenci tercihlerinin alınması
- Öğrenci davranışlarının takip edilmesi
- Test sonuçlarının toplanması
- Kullanıcı bildirimleri
- Öğrenme sisteminde geçirilen zaman

gibi girdilerle elde edildiğini belirtmişlerdir. Özyurt ve Özyurt (2015) 2004-2015 yıları arasında yayınlanan uyarlanabilir çevrimiçi öğretim sistemleri konulu çalışmalar üzerinde yaptıkları eğilim analizinde %10,5 payında bilginin sistem kayıtları üzerinden toplanırken, %89,5 payında geri kalan bilginin anket ve görüme kayıtlarından oluşturulduğunu vurgulamışlardır. Aggarwal ve Yu (2000) kişiselleştirme konusunda 2 tür veri toplama yönteminden bahsetmiştir. Buna göre açık toplama (explicit collection) yöntemi kullanıcının kendi ilgi, ihtiyaç vb. durumlarını kendinin bilerek sisteme girmesi yolu ile bilgi edilmesini kapsamaktadır. Üstü kapalı toplama (implicit collection) yöntemi ise kullanıcıların sistem üzerindeki davranışlarının kaydedilmesi

ile bilgi edinilmesini kapsamaktadır. Uyarlanabilir çevrimiçi öğretim sistemleri konusunda alan yazın incelendiğinde bu durumun koşutluk gösterdiği görülmektedir. Öğrenenden bilgi edinme yöntemleri anket, test, form, görüşme gibi yöntemler kullanılarak, öğrenenin kendi beyanatına dayalı (self-reported) olarak alınan veriler doğrudan soru sorma yöntemi ile toplanabilirken; öğrenenin sistem üzerinde oluşturduğu gezinme yolu, sistemde kalma süresi, tıklama sayısı, ekranda izlediği alan vb. öğrenen-sistem etkileşiminin meydana getirdiği çıktılardan oluşan kullanıcının sistemle etkileşimi yöntemi ile toplanabilmektedir.

Öğrenen hakkında bilgiler toplandıktan sonraki adım öğrenenin bu bilgiler ışığında modellenmesidir. Chrysafiadi ve Virvou (2013) ile Tadlaoui, Khaldi ve Carvalho (2016) uyarlanabilir öğretim ortamlarında kullanılan öğrenen modelleme tekniklerini şu şekilde sıralamışlardır:

1- *Örtüşme modeli:* 1976 yılında oluşturulan model birçok sistem tarafından uzun süredir kullanılan en popüler modellerden biridir. Ana varsayımı öğrenenin içerikle alakalı doğru ancak eksik bilgisinin olmasıdır. Bu sebeple konu alan küçük parçalara ayrılır ve model öğrenenin bu küçük araçlar hakkında bilgisi olup olmadığını veya bilme derecesini etiketler.
2- *Kalıp model:* Bir öğrenen sınıfını veya grubunu temsil eder. Arkasında yatan fikir tüm kullanıcıların uyarlanabilir bir sistem içerisinde paylaştıkları ortak karakteristik özelliklere göre bir gruba atılmasıdır. Örneğin, bir veri tabanı modülü acemi, yeni başlayan, ileri ve uzman olarak dört seviyeye ayrılır. Bireylerin bilgi, deneyim ve yetenekleri hakkında toplanan veriler ışığında bir seviyeye atanır ve orada kalır.
3- *Karışıklık modeli:* Örtüşme modelinin bir uzantısıdır ve bu modeldeki öğrenenin doğru bilgilerini işlemesinin yanı sıra yanlış veya hatalı bilgilerini de hesaba katar.
4- *Tanıma Planı:* Öğrenenin performans değerlerini temel alarak yapılan modellemedir. Öğrenen hareketleri olası tüm planların bulunduğu bir kütüphaneye adapte edilir. Öğrenenin hareketlerinin kütüphanede bulunan planlara en çok benzeyen durumu öğrenen modeli olarak seçilir. Kütüphanenin oluşturması çok masraflı ve karmaşık bir işlemdir.
5- *Makine öğrenmesi teknikleri:* Öğrenenin bilgi seviyesi, bilişsel yetenekleri, seçenekleri, yetkinlikleri ve daha birçok özelliğinin hesaba atılarak davranışları hakkında çıkarımlarda bulunma işlemlerini içerir. Öğrenen hakkında yapılan gözlemler eğitim için kullanılacak

gelecekteki hareketlerinin tahmini için kullanılabilir. Bu sebeple öğrenen modellemesi konusunda kullanımı oldukça popülerdir.

Öğrenenin modellenmesinden sona yapılacak son aşama, çevrimiçi öğretim sistemi üzerinde uyarlamanın gerçekleştirilmesi oluşturmaktadır. Uyarlama içeriğin ve gezinmenin uyarlaması olarak iki ana başlıkta gerçekleştirilebilmektedir. Uyarlanabilir gezinme hiper ortamda kullanıcıya rehberlik etmek olarak tanımlanabilirken, uyarlanabilir içerik kullanıcı modeline göre sayfalardaki içerinin çeşitli yönlerde değiştirilmesi olarak tanımlanabilmektedir (Stern ve Woolf, 2000). Somyürek (2008) yapmış olduğu çalışmada içeriğin uyarlanabilmesi için kullanılabilecek yöntem ve teknikleri şu şekilde sıralamıştır:

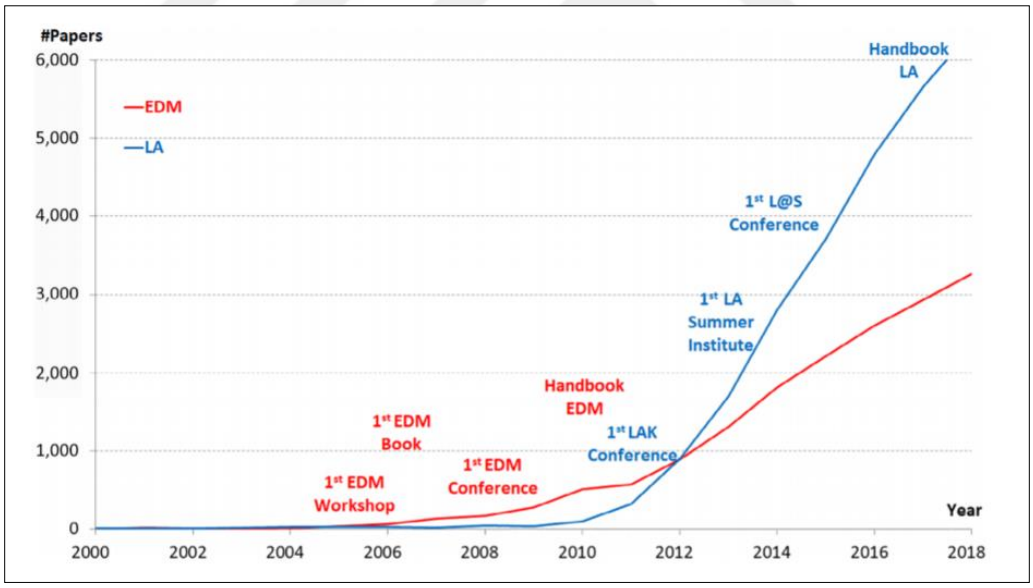
- *Koşula bağlı metin:* Tüm içerik parçalara bölünür ve modellenmeye uygun bir şekilde öğrenene bu parçaların bir kısmı gösterilirken bir kısmı gizlenir. Ön bilgisi yüksek bir öğrenene sınırlı sayıda parçanın sunumu yapılırken ön bilgisi düşük bir öğrenene daha fazla parça veya içeriğin tamamının gösterilmesi örnek olarak gösterilebilir. Parçaların tamamını görmek isteyen bir öğrenen için sınırlılık oluşturabilir.
- *Esnek metin:* Bir konu başlığı ile ilgili ekstra açıklamanın web teknolojilerinin sağlayabileceği herhangi bir yöntemle (açılır pencere, uzayan metin vb.) öğrenene sağlanmasıdır. Öğrenenin kontrolünde gerçekleştirilen bu işlemin niteliği hakkında geribildirim vermemesi sınırlılık oluşturabilir.
- *Farklı bölümler:* Tüm içerik öncelikli olarak bölümlere ayrılır. Her bir bölüm için uygun görülecek şekilde farkı içerikler hazırlanır. Modellemeye göre hangi öğrenenin bölümün hangi içeriğine erişim sağlayacağına karar verilir. Bu işlemin zorluğu her bir bölüm için birbirinden farklı içerikler hazırlamaktır.
- *Farklı sayfalar:* Farklı bölümlere benzer bir yapıda olup her sayfanın farklı içeriklerle modellenen öğrenene göre sunulması olup benzer zorlukları içermektedir.
- *Çerçeve temelli teknik:* Çerçeve şeklinde hazırlanan ve her birinin diğeri ile bağlantısı olan sayfa içerisindeki bölümlerin hangi içerik türünde ve sırasında görüntüleneceği belirlenir. Yeniden sıralanan bölümler doğal akışın dışına çıkabileceği için anlaşılma problemlerine de sebep olabilir.

Houben'in (2004) öğreneni doğru içeriğe erişebilmesi için yönlendirme çalışmaları olarak tanımladığı gezinmenin uyarlanmasına özgü yöntem ve teknikleri Brusilovsky (2007) yaptığı çalışma ile aşağıdaki şekilde sıralamıştır:

- *Doğrudan kılavuzluk:* Uyarlanabilir gezinme yöntemlerinin en basiti olup ihtiyaçları, bilgisi vb. parametrelere göre modellenen öğrenene bir sonraki en iyi içeriğe veya alternatif içeriğe doğrudan yönlendirme yapılmasıdır. Aynı sayfada bulunan bağlantının belirginleştirilmesi şeklinde uygulanabileceği gibi dinamik bir "sonraki" bağlantısı da kullanılabilir. Sistemin önerilerini kullanmak istemeyen öğrenenler için bir sınırlılık oluşturabilir.
- *Bağlantı sıralama:* Öğrenenin belirlemiş olduğu amaçlarını da göz önüne alarak, oluşturulmuş modellemeye göre tüm bağlantıların önceliklendirilerek sunulmasıdır. Stabil bağlantı sıralamasının önem arz etmediği içerikler için kullanılması uygun olmakla birlikte, aksi durumlar için sorunlar yaratabilir.
- *Bağlantı gizleme:* Bu yöntemin amacı öğrenenin amacı ile örtüşmeyen veya henüz anlamakta güçlük çekebileceği materyaller içeren ilgisiz sayfalara yönlenen bağlantıları gizlemek, çıkarmak veya pasif hale getirmektir. Bilişsel yükleme probleminin önüne geçmek için kullanılmaktadır. Bazı çalışmalar daha önce aktif olan bağlantıların daha sonra görünmez veya pasif olmasının öğrenenler üzerinde memnuniyetsizlik yarattığı belirtilmektedir.
- *Bağlantıları açıklama:* Bağlantılar üzerinde yer alan açıklamalar ile erişilecek olan düğümler hakkında öğrenenin daha fazla bilgi edinmesinin amaçlandığı yöntemdir. İkon şeklinde veya fare işaretçisinin bağlantı üzerine gelmesi gibi yöntemlerle uygulanabilmektedir. Bu yöntem bağlantıların sabit sıralamasını koruyarak öğrenenlerin zihinsel haritalar konusunda problem yaşamasını önler.
- *Bağlantı oluşturma:* Sayfada daha önce oluşturulmamış yeni bağlantıların sunulmasıdır. Üç ayrı yöntemle gerçekleştirilirken, o anki öğrenen için öğrendiği içerikle ilgili dinamik bağlantılar önerilmesi uyarlanabilir yöntemi olarak belirtilmektedir. Yeni bağlantının oluşturulması öğrenenin profili ve içerik hesaba katılarak oluşturulmaktadır.

İlgili Araştırmalar

Alanyazında uyarlanabilir çevrimiçi öğretim sistemleri üst başlığında hemen her konuda gerçekleştirilmiş yüksek sayıda çalışma bulunmaktadır. Kaydedilen ve erişilebilen veri miktarındaki ve bu veriyi işleme kapasitesindeki artışın çevrimiçi öğretim sistemi çalışmalarının başlamasından daha sonraki yıllara denk geliyor olması, bu alanda veri madenciliği tekniklerinin uygulandığı çalışma sayısını görece az kılmaktadır. Ancak veri madenciliği yöntemlerinin uyarlanabilir çevrimiçi öğretim sistemleri konusunda işe koşulduğu çalışmalar uzun süreden beri alanyazında ivmeli bir şekilde çalışılan konular arasında yer almaktadır. Romero ve Ventura (2020) yapmış oldukları çalışmada Google Scholars üzerinde 2000-2018 yılları arasında gerçekleştirilen, "eğitsel veri madenciliği" ve "öğrenme analitikleri" anahtar kelimeleri ile yapılan arama sonucunda ortaya çıkan çalışma sayılarını ve yıllara göre artışını belirtmişlerdir (Şekil 13).



Şekil 13. 2000-2018 Yılları arasında yapılan çalışma sayıları *Romero, C., & Ventura, S. (2020). Educational data mining and learning analytics: An updated survey.* WIREs Data Mining and Knowledge Discovery, 10*(3).* kaynağından erişilmiştir.

Wang ve Guo (2009) yapmış oldukları çalışmada İngilizcenin ikinci yabancı dil olarak öğretilmesi konusunda prototip uyarlanabilir çevrimiçi öğretim sistemi geliştirmiştir. Cinsiyet, kişilik, bilişsel stil, öğrenme stili ve daha önceki dönemlerde alınan sınav notlarının Roiger ve Geatz karar ağacı algoritması kullanılarak işlendiği çalışmalarında öğretim içeriği optimize

edilerek, öğrenenlere özgü, kişiselleştirilmiş bir sıralamada gösterilmesi sağlanmıştır. Çalışma gezinmenin uyarlandığı bir sistem olarak nitelendirilmiştir.

Xu, Wang ve Su (2002) yapmış oldukları çalışmada, çevrimiçi olarak sunulan bilişim sistemleri geliştirme yaşam döngüsü dersini uyarlanabilir bir şekilde yeniden tasarlamışlardır. Çalışmalarında uyarlama işlemini daha önceden veri tabanında bulunan önceki sınav puanları gibi statik verileri ve veri tabanına kaydetmeye başladıkları fare hareketlerinin hedefi, zamanlaması gibi dinamik verileri bulanık mantık yöntemi ile işleyerek gerçekleştirmişlerdir. Modellenen öğrenci profili sayesinde her bir farklı öğrenciye farklı öğrenme materyali, test soruları okuma önerileri, uyarılar ve tavsiyeler sunmuşlardır.

Lin, Yeh, Hung ve Chang (2013) yaratıcılığı artırmak için uyarlanabilir çevrimiçi öğretim sistemi geliştirmişlerdir. Yaş, cinsiyet, mezun olunan bölüm gibi demografik ve sosyo-demografik bilgilerin yanı sıra yaratıcılık, öğrenme stili ölçeklerinden ede edilen sonuçları karar ağacı algoritması işe koşularak modellenme gerçekleştirilmiştir. Çalışmada öğrenenlerin problem çözme becerileri, tasarlanan öğretim sistemi ile artırmaya çalışılmış, bu kapsamda geliştirilen üç senaryolu bir oyunda, on farklı problemin çözüm yollarını kişiye özgü olarak uyarlamayı amaçlamışlardır. Gezinmenin uyarlandığı bu sistemde önerilen yolları kullanan öğrenenlerin görece daha yaratıcı beceriler gösterebildikleri vurgulanmıştır.

Huang, Huang ve Chen (2007) yapmış oldukları çalışmada "Java programlama dili" konusunda pilot bir uyarlanabilir çevrimiçi öğretim sistemi tasarlamışlardır. Sistem kapsamında konu başlıklarının sıralanarak, uyarlanabilirlik gerçekleştirilmeye çalışılmıştır. Cinsiyet, yaş, test süresi, uzmanlık seviyesi ve öğrenenin bilgi seviyesi değişkenleri genetik algoritma kullanılarak zorluk derecesi ön testle belirlenmiş ve benzer konu başlıklarının öğrenene kişiselleştirilmiş sırada sunulması sağlanmıştır. Uyarlanabilir çevrimiçi öğretim sistemi, öğrenenin ünite konularını çalıştıktan sonra uyguladığı bir test sonucunda değerlendirilmesi, başarısız olması durumunda kendisine özeleştirilmiş bir sıralama ile aynı konuların yeniden çalışılması ve yeniden test uygulanması şeklinde kurgulanmıştır.

Jovanovic, Vukicevic, Milovanovic ve Minovic (2012) yapmış oldukları çalışma ile prototip bir çevrimiçi öğretim sistemi modülü geliştirmişlerdir. K-ortalama değer algoritmasını kullanarak öğrenenlerin bilişsel stillerini ve Belgrad Üniversitesi çevrimiçi öğretim sistemi üzerinde almış oldukları derslerin performanslarını işleme tabi tutarak öğrenenleri kümelemişlerdir. Hangi

özellikteki öğrenenin hangi ders konusunda başarılı olabileceğini veya zorluk çekebileceğini tahmin etmek için oluşturulan modülün çevrimiçi öğretim sistemi üzerine entegre edilmesiyle, öğrenene özel içerik sunulabileceği gibi öğretene de karar alma konusunda destek olacağı belirtilmiştir.

Wang ve Liao (2011) yapmış oldukları çalışma ile İngilizce'nin ikinci bir yabancı dil olarak öğretildiği uyarlanabilir bir prototip çevrimiçi öğretim sistemi geliştirmişlerdir. Öğrenenlerin demografik ve karakteristik özellikleri olan cinsiyet, kişilik ve anksiyete seviyelerinin ve öğrenme performanslarının yapay sinir ağları algoritması kullanılarak işlendiği çalışmada öğrenenleri sınıflandırmışlardır. Çalışma sonucunda modellenen öğrenenler için farklı seviyelerde kelime bilgisi ve okuma etkinlikleri önerilmiştir.

BÖLÜM III

YÖNTEM

Bu bölümde; araştırma modeli, araştırmanın süreci, çalışma grubu, verilerin toplanması ve verilerin analizine yer verilmektedir.

Araştırmanın Modeli

Bu çalışma ile kullanıcılarının demografik, sosyo-demografik, dikkat, kişilik, bilgi güvenliği konusundaki tehlike algısı, suça maruziyet, riskli ve korumacı davranışlara karşı beyanatları doğrultusunda; aynı konuda gerçek hayattaki gösterecekleri davranışlar veriden bilgi keşfetme süreçleri işletilerek tahmin edilmeye çalışılmıştır. Kullanıcı hakkında yapılan bu tahminler doğrultusunda da kendisine kişiselleştirilmiş bir içerik sunan çevrimiçi öğretim sistemi hazırlanması amaçlanmıştır. Bu amaca ulaşmak için tasarım tabanlı araştırma yöntemi kullanılmıştır. Tasarım tabanlı araştırma yöntemi genel olarak bir ürün veya hizmetin geliştirilmesini hedefleyen, kuram veya eğitim uygulamaları ortaya konulabilen araştırma yöntemidir (Barab ve Squire, 2004). Çalışmada uyarlanabilir öğrenme ortamının ortaya koyulması için ise tasarımın süreç içerisinde şekillendirilerek ürünün süreç sonunda ortaya çıkmış olduğu hızlı prototipleme öğretim tasarımı modeli (Şimşek, 2013) kullanılmıştır.

Tasarım, Türk Dil Kurumu (TDK) (2020) sözlüğünde "*bir araştırma sürecinin çeşitli dönemlerinde izlenecek yol ve işlemleri tasarlayan çerçeve, tasar çizim, dizayn*" olarak tanımlanmaktadır. Tasarım öğretme-öğrenme bağlamında incelendiğinde, geliştirme sürecinin gerçekleştirilebilmesi için gerekli ön işlemler olduğu ve süreç sonucunda yeni bir ortam veya kuramın meydana gelmesi ile sonuçlanacağı görülmektedir. Çalışma kapsamında, çevrimiçi

öğrenme ortamlarının oluşturulmasının tasarım ve geliştirme süreçlerini ihitva etmesinden dolayı, en önemli özelliği yeni bir öğrenme ortamı ya da eğitim uygulaması üretiyor olması (Kuzu, Çankaya ve Mısırlı, 2011) olan tasarım tabanlı araştırma yöntemi tercih edilmiştir.

Wang ve Hannafin (2005) alanyazında tasarımın odak noktası olduğu farklı tanımlamalar atında birçok çalışma olduğunu şu şekilde sıralamıştır:

- Tasarım tabanlı araştırma (Design Based Research, Collective, 2003);
- Tasarım deneyleri (Design experiments, Collins, 1992,1999);
- Tasarım araştırması (Design research, Edelson, 2001);
- Geliştirme araştırması (Development research, Van den Akker, 1999);
- Gelişimsel araştırma (Developmental research, Richey, Klein ve Nelson, 2003);
- Biçimlendirici araştırma (Formative research, Reigeluth ve Frick, 1999)

Bu çalışmaların ortak karakteristik özelliklerini şu şekilde sıralamışlardır:

- Pragmatik: Tasarım tabanlı araştırma hem kuramı hem de uygulamayı geliştirir ki uygulamanın değeri, ilkelerin uygulamayı ne derece geliştirdiği ile değerlendirilir.
- Temeli olan: Tasarım gerçek dünya uygulamaları ile ilgilidir ve süreç tasarım tabanlı araştırmaya bağlı olarak çalışılır
- Etkileşimli, tekrarlayan ve esnek: Fazlaca detaylandırılmamış olan ana başlangıç planının ihtiyaç dâhilinde araştırmacı tarafından değiştirilebildiği işlemler analiz, tasarım, uygulama ve yeniden tasarım basamaklarının tekrarlayan bir yapıda bulunmaktadır.
- Bütünleyici: Karma araştırma yöntemlerinin uygulanabildiği tasarım tabanlı araştırma yöntemlerinde araştırmada yeni ihtiyaçlar oluşması veya araştırma amacının gelişmesi durumlarında çok farklı yöntemler farklı fazlarda kullanılabilirler.
- Bağlamsal: Araştırma süreci, bulgular ve ana plan üzerinde yapılan değişiklikler raporlanır.

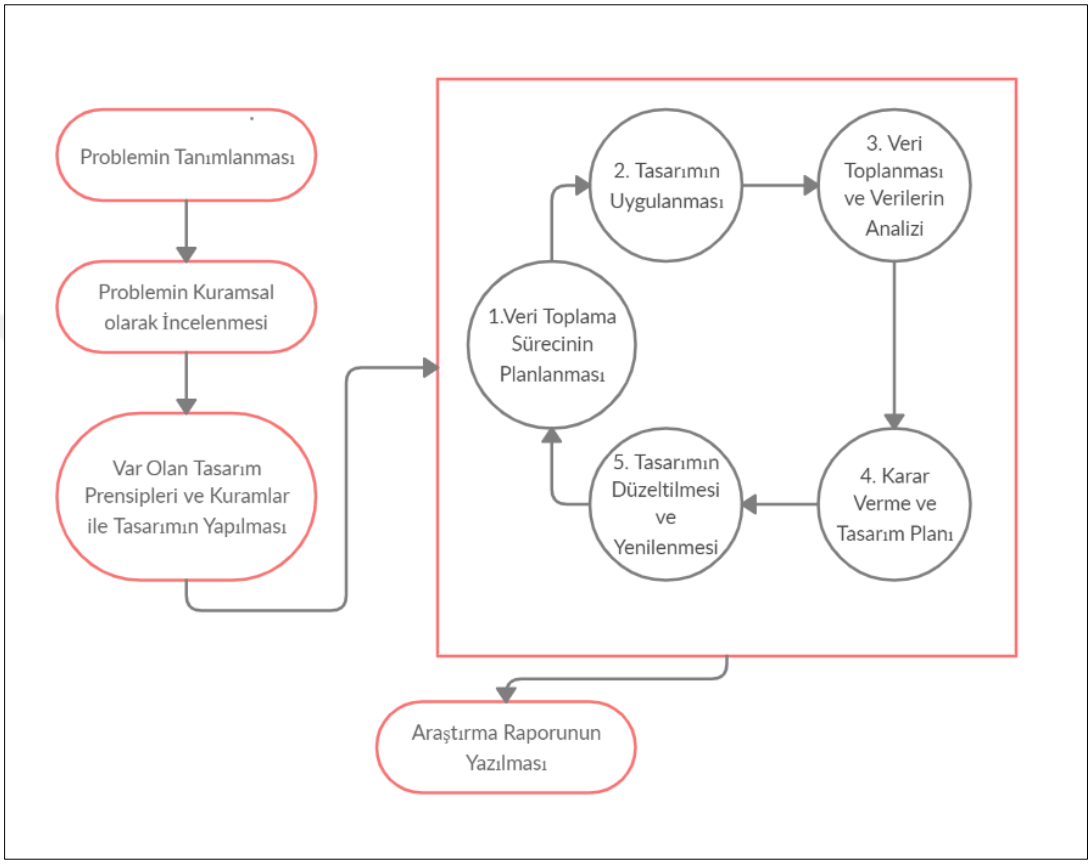
Frick ve Reigeluth (1999) nicel araştırma yöntemlerinin (deneysel, korelasyon analizi vb.) öğretimsel tasarım kuramlarını veya geliştirmeyi iyileştirmek için yeterince yararlı bulmadıklarını, bunun yerine vaka araştırması tarzında yöntemlerin geliştirilmesi gerekliliğini savunmuşlardır. Çoğu eğitim araştırmasının bilgiyi tanımlama ile sonuçlandığını belirtmişler ve tasarım tabanlı yöntemlerin verilen bir duruma göre kuramsal bilginin uygulanması, bu süreçte

sarf edilecek zaman, materyal, ekipman gibi ihtiyaçların göz önüne alınması, öğretimdeki tüm paydaşlar için ne derece tatmin edici olabileceği konularında faydalı olacağını vurgulamışlardır. Benzer bir şekilde Van den Akker (1999) öğretimin dinamik ve karmaşık yapısında kaynaklı olarak gerçek dünya uygulamaları üzerinde geleneksel araştırma yöntemleri kullanılırken araştırmacıların tasarım ve geliştirme problemleri ile karşılaştıklarını, eğitim araştırmalarının tanımlayıcı bilgileri tasarım prensiplerine transfer edebilecek daha değerli pratikler sunması gerektiğini belirtmiş, tasarım tabanlı araştırmaların belirtilen karmaşık yapıdaki geliştirme etkinliklerini destekleyeceğini belirtmiştir. Edelson (2002) ise eğitimsel araştırmaların tarihsel olarak kuramların testi için, tasarımların ise bu kuramları geliştirme ve düzenleme amacında olduğunu ancak tasarım tabanlı araştırmaların belirli derslerin öğrenilebilmesi için fırsatlar sunabileceğini, doğrudan uygulanabilecek pratik ürünler sunabileceğini, araştırmacılara eğitsel uygulamaları doğrudan geliştirebilme imkânı sunabileceğini vurgulamıştır. Eğitim araştırmacıları, kural koyucular ve uygulayıcılar günlük uygulamalarda yaşanan problemlere edebilecek çözümler arayan araştırma yöntemlerine ihtiyaç olduğu konusunda hem fikir olmuş, tasarım tabanlı araştırmaların bu konuda öğrenme ortamlarının geliştirilmesi, yürürlüğe korunması ve sürdürülmesi yardımcı olacağı bildirilmektedir (The Design-Based Research Collective, 2003). Kelly (2013) yaşanan problemin belirli ve standart haline gelmiş bir çözümü ve bu çözümün uygulanması konusunda genel bir düşüncenin hâkim olduğu ve uygulandığında problemin ortaya kalktığında kullanılmasının çok uygun olmadığını belirttiği tasarım tabanlı araştırmaların, belirtilen durumlarda tercih edilmesinin faydasından bahsetmiştir:

- Öğretilecek bilginin yeni veya araştırmacı tarafından yeni keşfediliyor olması
- İçeriğin nasıl öğretileceği konusunun çok açık olmaması
- Öğretimsel materyallerin yetersiz veya hiç olmaması
- Öğreticinin yeteneklerinin ve bilgisinin tatmin edici düzeyde olmaması
- Karmaşık kural veya politik faktörlerin süreci negatif yönde etkilemesi.

Mevcut çalışmanın amacı bir öğretim ortamının tasarlanması ve geliştirilmesi olduğu için, bir ürün ortaya koymaya yönelik olması ve genel öğretim sistemi tasarımı adımlarına benzer şekilde analiz, tasarım ve uygulama adımlarının yinelenen bir şekilde kullanılmasından dolayı tasarım

tabanlı araştırma yöntemi, Şekil 14 üzerinde gösterdiği ve adımları (Kuzu vd., 2011) açıklandığı şekli ile kullanılmıştır.



Şekil 14. Tasarım tabanlı araştırma uygulama adımları. Kuzu, A., Çankaya, S., & Mısırlı, Z. A. (2011). Tasarım Tabanlı Araştırma ve Öğrenme Ortamlarının Tasarımı ve Geliştirilmesinde Kullanımı. *Anadolu Journal of Educational Sciences International, 1*(1), 19-35. Kaynağından uyarlanmıştır.

1. *Problemin Tanımlanması:* Bilgi güvenliğine yönelik çevrimiçi öğretim sistemlerinin uyarlanabilir yapıda olmamasının kullanıcının kaybolmasına, gereksiz zaman ve güç harcamasına sebep olması problem olarak tanımlanmıştır. Bu aşama detaylı olarak "Problem Durumu ve Gerekçesi" başlığı altında detaylı olarak incelenmiştir.
2. *Problemin Kuramsal Olarak İncelenmesi:* 1. aşamada belirlenen problem durumu ve problemin sebepleri ve olası çözümler için alınan reaksiyonlar alan yazın ve gerçek dünya örnekleri üzerinden araştırılarak incelenmiştir. Bu aşama "Kavramsal Çerçeve" başlığı altında detaylı olarak incelenmiştir.

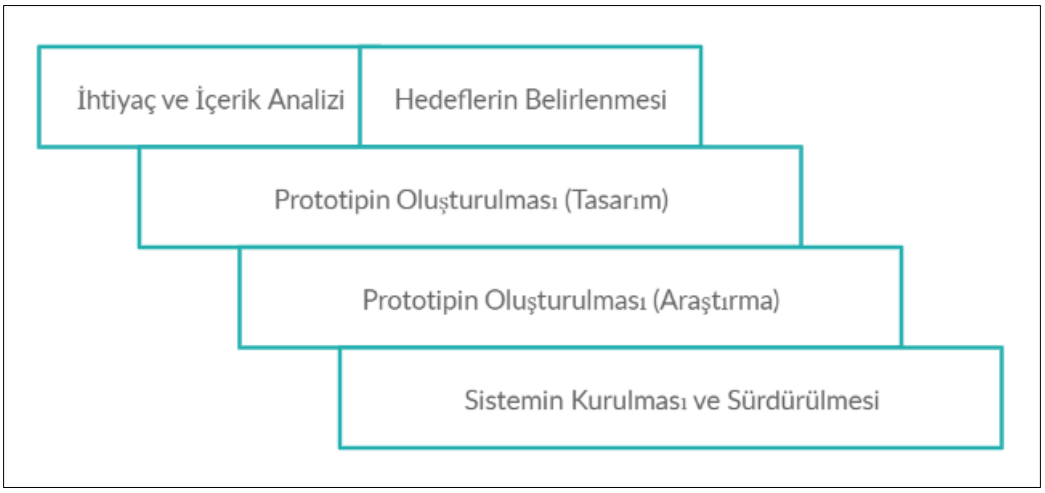
3. *Var Olan Tasarım Prensipleri ve Kuramlar ile Tasarımın Yapılması:* 2. aşamada açığa çıkan bilgiler ışığında uyarlanabilir çevrimiçi öğretim sisteminin tasarımı gerçekleştirilmiştir. Kullanıcıların kendi beyanlarına dayalı olarak bildirdikleri ve gerçek hayatta gösterdikleri davranışların karşılaştırılarak, öğretim ortamına aktarılmasının belirlenmesi bu aşamada gerçekleştirilmiştir.
4. *Döngüsel İşlemler:* 3. aşamada belirlenen genel tasarıma göre, her bir uygulama adımı döngüsel şekilde gerçekleştirilmiş, planlanan veri toplama sürecine göre tasarım uygulanmış, veriler toplanarak analiz edilmiş, ortaya çıkan sonuçlar dâhilinde karar verilerek tasarım yeniden düzenlenmiş veya nihai şeklini almıştır. Bu aşama "Bulgular ve Yorum" başlığı altında detaylı olarak ele alınmıştır.
5. *Araştırma Raporunun Yazılması:* Bu aşama "Bulgular ve Yorum" başlığı altında detaylı olarak ele alınmıştır.

Tasarım tabanlı araştırma yöntemine oluşturulacak uyarlanabilir çevrimiçi öğretim sisteminin nasıl çalışacağına yönelik işlemlerin tamamlanması aşamasında başvurulmuştur. Sistemin öğretimsel tasarımı için hızlı prototipleme modeli kullanılmış böylece süreç içinde şekillenen tasarım süreç nihayetlendiğinde uyarlanabilir çevrimiçi öğretim sisteminin ürün olarak ortaya çıkması sağlanmıştır.

Öğretim bir insanın öğrenmesine yardım etmek için yapılabilecek, öğretimsel tasarım ise bu yardımın kalitesini artırmaya yarayacak her şey olarak ifade edilmektedir (Reigeluth, 1997). Öğretim tasarımı, algı ve öğrenme ile ilgili ilkelerin sistematik bir şekilde öğretim ortamlarına uyarlanması, öğrenme ise genel olarak kişinin bir işin nasıl yapıldığıyla alakalı bilgiyi alarak işi gerçekleştirmesi ve deneyim kazanarak o işin neden yapıldığını kavramlaştırması olarak tanımlanmaktadır (Arı, 2013). Alanyazında farklı alanlardaki eğitim, öğretim, öğrenme ve geliştirme çabalarının bir ürünü olarak birbirine alternatif olabilecek şekilde geliştirilmiş birçok öğretim tasarımı modeli bulunmaktadır. Uygulama sürecini özetleyen ADDIE çekirdek modeli analiz, tasarım, geliştirme, uygulama ve değerlendirme aşamalarından meydana gelmekte olup öğretim tasarımı sürecinin aşamalarını veya bileşenlerini göstermektedir. Alanyazında bulunan bazı modeller ilk basamaktan son basamağa kadar ardışık bir sıra izlerken (doğrusal modeller), bazı modeller basamakların yinelenmesi ile gerçekleştirilmekte (döngüsel modeller), bazıları

tüm basamaklar arasındaki etkileşimi ön plana alırken (etkileşimli modeller), bazıları sistematik yapısının yaratıcılığı engellemesinden dolayı tasarımın verimine odaklanmaktadır (sezgisel modeller) (Şimşek, 2013). Hızlı prototipleme öğretim tasarımı modeli sezgisel modeller içerisinde incelenmektedir.

Yan ve Gu (1996) endüstri için ürün geliştirme konusunda karşılaşılan iki önemli ve zorlayıcı işlemin, ürün geliştirme süresinin hızlıca düşürülmesi ve üretimi yapılacak ürünlerin çeşitli tiplerde ve küçük parti boyutunda üretiminin esnekliğinin artırılması olarak belirtmişlerdir. Hızlı prototipleme yönteminin ise bu zorlayıcı işlemlerin üstesinden gelerek ürün prototiplerinin üretilme süresini hızlıca düşürdüğünü vurgulamışlardır. Hızlı prototipleme öğretimsel konuda yeni bir ürünün çalışan bir modelinin geliştirilmesini kapsar. Prototip ürünün son hali olmamakla birlikte onu betimleyen, işlevlerinin görülmesini sağlayan, son ürünün daha basit ancak çalışan bir modelidir (Jones ve Richey, 2000). Tripp ve Bichelmeyer (1990) hızlı prototipleme modelinin basamaklarını Şekil 15 üzerinde gösterildiği şekilde ifade etmişlerdir. Tasarım, araştırma, oluşturma ve kullanma sıralı işlemlerinin sonucunca ürünle ilgili ihtiyaç, hedef ve içeriklerin tam olarak anlaşılabileceğini belirtmişlerdir.



Şekil 15. Hızlı prototipleme modeli. Tripp, S. D., & Bichelmeyer, B. (1990). Rapid prototyping: An alternative instructional design strategy. *Educational Technology Research and Development, 38*(1), 31-44. Kaynağından uyarlanmıştır.

Reigeluth (1989) araştırma ve tasarımın birbirinden ayrılmasının iyi bir seçenek olmadığını vurgularken, tasarımcının ortaya çıkan ürünü değerlendirebilecek nitelikte ve aşinalıkta olmasının araştırma ve geliştirmenin birlikte yürütülmesinin çok daha etkili olacağını ifade

etmiştir. Hızlı prototipleme modelinin tam bir öğretim programı ortaya koymaktan ziyade ders seviyesindeki öğretimi geliştirmek için kullanılan öğretim tasarımı modeli olmasından dolayı (Şimşek, 2013), bu çalışmada hızlı prototipleme öğretim tasarımı modeli basamakları takip edilmiştir.

Çalışma Grubu

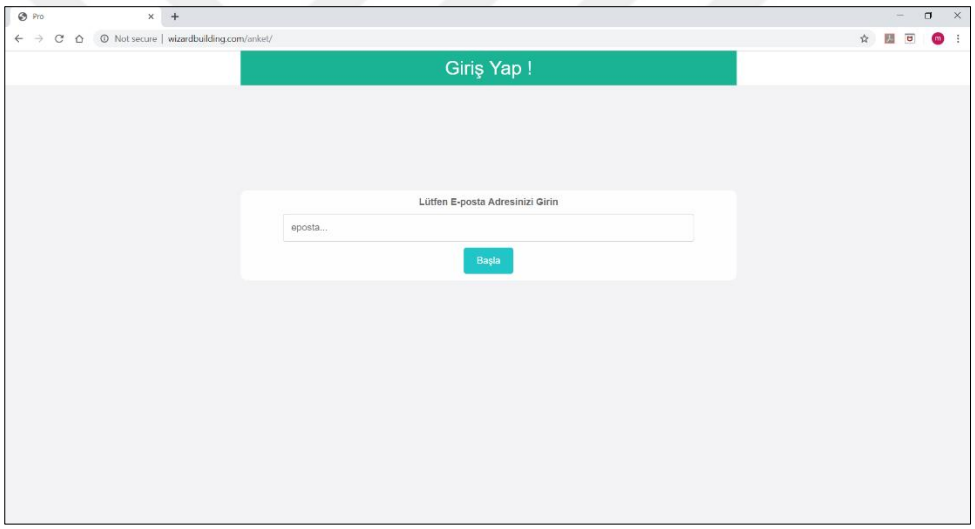
Veri toplama aşaması iki aşamadan oluşan çalışmanın ilk bölümde çalışma grubunu bilgisayar veya akıllı telefon ve internet kullanıcısı olan 619 gönüllü katılımcı oluşturmaktadır. Veri toplama aşamasının ikinci aşaması ise ilk aşamaya katılım gösteren 619 katılımcıdan 301'i gönüllü olarak katılım sağlamışlardır. Bilgisayar veya akıllı telefon kullanarak internet üzerinden herhangi bir işlem yapan 7'den 77'ye her yaşta ve özellikte kullanıcının bilgi güvenliğine yönelik tehditlere maruz kalabileceğinden, belirtilen teknolojilerin kullanımı dışında bir sınırlama getirilmeden çalışma grubu gönüllülük esasına göre oluşturulmuştur. Çalışmanın bir ve ikinci veri toplama aşamaları arasında gözlenen katılımcı farkı sadece ilk aşamaya gönüllü olarak destek veren katılımcıların ikinci aşamaya katılım sağlamak istememelerinden kaynaklanmaktadır.

Çalışma grubunun belirlenmesinde amaçlı örnekleme yöntemlerinden maksimum çeşitlilik yöntemi kullanılmıştır. Büyüköztürk vd. (2014) amaçlı örneklemeyi, temel alınan birimlerin seçilme ihtimallerinin eşit olmadığı seçkisiz örnekleme yönteminin altında değerlendirmekle birlikte araştırmanın derinlemesine gerçekleştirilebilmesi amacı ile çalışmanın bağlamına göre bilgi bakımından zengin durumda olanların seçilmesi olarak ifade etmiş, maksimum çeşitlilik yönteminin ise örneklem üzerinde araştırmaya sebep problemle ilgili kendi içerisinde benzeyen ancak farklı durumlardan oluşması olarak tarif etmişlerdir. Mevcut çalışma göz önüne alındığında, katılımcılar için bilgisayar ve/veya akıllı telefon ve internet kullanıcısı sınırlamasının olması, büyük veri analizi yöntemleri ile araştırmanın derinlemesine gerçekleştirilmesi ve oluşturulacak çevrimiçi öğretim sisteminin uyarlanabilirliğinin kendi içerisinde benzeyen ancak farklı özelliklerde katılımcıların analiz edilmesi ile mümkün olacağından amaçlı örnekleme-maksimum çeşitlilik örnekleme yöntemi en uygun görülen yöntem olmuştur.

Verilerin Toplanması

İki bölümden oluşan veri toplama işlemlerinin birinci aşamasında katılımcıların demografik, sosyo-demografik özellikleri, bilgi güvenliğine yönelik riskli ve korumacı davranışları, risk algıları ve suça maruz kalma durumları ile kişilik özelliklerini belirlemek amacıyla Büyük Beşli Kişilik Envanteri veri toplama aracı olarak kullanılmıştır.

Çalışmanın ve veri toplamanın ikinci aşamasında ise, katılımcıların birinci veri toplama aşamasında ölçülebilir bazı davranışlara verdikleri cevapları davranışa dönüştürüp dönüştürmediklerini belirlemek için bir web sitesi (www.wizardbuilding.com) inşa edilmiştir. Oluşturulan web sitesinin giriş sayfası Şekil 16 üzerinde gösterilmiştir.



Şekil 16. www.wizardbuilding.com veri toplama aracı

Veri toplama birinci aşamasında ankete gönüllü katılım sağlayan 619 katılımcıya, oluşturulan web sitesinin adresi vermiş oldukları eposta adresleri üzerinden gönderilerek çalışmanın ikinci aşamasına da katılım sağlamaları istenmiştir. Katılımcıların kendi davranışlarının ölçüldüğünü düşünmemeleri, doğal davranışlarını sergileyebilmeleri ve böylece deneme etkisini ortadan kaldırmak için oluşturulan web sitesinin kullanılabilirliğinin ölçüldüğü izlenimi verilmiştir.

Her iki veri toplama işlemi için katılımcı sayısını artırabilmek amacıyla ilk yapılan duyuruda; çalışmanın iki aşamadan oluştuğu, her iki aşamaya da katılım sağlayacak gönüllüler arasından, video kaydının eposta üzerinden her katılımcıya gönderilmek üzere yapılacak olan çekilişle bilgi güvenliği firmaları tarafından sağlanan hediyeler gönderileceği vurgulanmıştır. Bu sebeple

iletiyi alan herkesin bunu kendi sosyal medya veya eposta gruplarında paylaşması da teşvik edilmiştir. Çalışma kapsamında ölçekleri kullanılan araştırmacılardan ölçekleri çalışma kapsamında kullanabilmek ile ilgili, Gazi Üniversitesi Etik Kurulu'ndan veri toplama ile ilgili gerekli tüm izinler alınmıştır (EK 2). Çalışma kapsamında cevap aranan araştırma sorularına Tablo 1'de belirtilen veri toplama araçları kullanılarak ulaşılmıştır:

Tablo 1

Veri Toplama Araçları Özet Tablosu

SN	Araştırma Sorusu	Veri Toplama Aracı
1	Bilgi güvenliği konusunda bireysel özellikler, niyetler ve davranışlar arasında nasıl bir ilişki vardır?	
a	Bilgi güvenliği konusunda demografik özellikler niyetleri nasıl etkilemektedir?	Anket
b	Bilgi güvenliği konusunda kişilik özellikleri niyetleri nasıl etkilemektedir?	Anket
c	Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin demografik özellikleri arasında anlamlı bir ilişki var mıdır?	Anket + Araştırmacı tarafından hazırlanan web sitesi
d	Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin sosyo-demografik özellikleri arasında anlamlı bir ilişki var mıdır?	Anket + Araştırmacı tarafından hazırlanan web sitesi
e	Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin kişilik özellikleri arasında anlamlı bir fark var mıdır?	Anket + Araştırmacı tarafından hazırlanan web sitesi
f	Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin tehlike algıları, suça maruz kalma durumları, riskli davranış özellikleri ve korumacı davranış özellikleri arasında anlamlı bir fark var mıdır?	Anket + Araştırmacı tarafından hazırlanan web sitesi
g	Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin yazma hızları ve dikkatleri arasında anlamlı bir fark var mıdır?	Araştırmacı tarafından hazırlanan web sitesi
2	Bilgi güvenliği eğitimine yönelik olarak geliştirilen uyarlanabilir çevrimiçi öğrenme ortamı nasıl olmalıdır?	
a	Uyarlama nasıl gerçekleştirilmelidir?	Yarı yapılandırılmış görüşme
b	Öğrenen modellemesi nasıl yapılmalıdır?	Yarı yapılandırılmış görüşme
3	Bilgi güvenliği eğitimine yönelik olarak geliştirilen uyarlanabilir öğrenme ortamı hakkında konu alanı uzmanlarının görüşleri nelerdir?	Yarı yapılandırılmış görüşme

Demografik Özellikler

Katılımcıların genel demografik özelliklerinin toplandığı anket üzerinde yaş bilgisi doğum tarihi olarak elde edilmiş ve daha sonra veri analizinde kullanılmak üzere kuşak gruplarına çevrilerek kaydedilmiştir. İnsanların algıları, vizyonları, misyonları ve davranışları çevre, önemli olaylar, iş ve hayat tecrübeleri gibi durumlardan etkilendiği için yaş gruplarının, adına kuşak denilen ve bu etki durumlarının bulunduğu periyotlara göre şekillendiği parçalara bölünmesi ile gerçekleştirilmiştir (Bejtkovský, 2016). Bu çalışmada kuşaklar Adıgüzel, Batur ve Ekşili'nin (2014) çalışmalarına göre 5 grup altında incelenmiştir. 1945 yılı ve öncesinde doğanlar "gelenekselciler" grubunu oluştururken, 1946-1964 yılları arasında doğan kişiler "bebek patlaması" grubunu oluşturmaktadır. "X kuşağı" grubunu 1965 ile 1979 yılları arasında doğanlar oluşturmakta iken, 1980 ile 1995 yılları arasında doğanlar "Y kuşağı" grubunu oluşturmaktadır. 1995 sonrasında doğanlar ise "Z kuşağı" olarak nitelendirilmiştir. Katılımcıların cinsiyet değişkeni verileri de alan yazında yapılan çalışmalara uygun olarak "kadın" ve "erkek" şeklinde toplanmıştır.

Sosyo-Demografik Özellikler

Sosyo-demografik bilgiler katılımcının kaç yıldır internet kullanıyor olduğu, günlük kaç saatini internette geçirdiği ve eğitim seviyesi bilgilerinden oluşmaktadır. Eğitim seviyesi Türk eğitim sistemine paralel olarak gerçekleştirilmiştir. Çalışma kapsamında kaydedilen sosyo-demografik değişkenler Tablo 2 üzerinde gösterilmiştir.

Tablo 2

Sosyo-demografik Özellikler

Eğitim Düzeyi	İnternet Kullanım Yılı	Günlük İnternet Kullanım Saati
İlköğretim Mezunu	0-2 Yıl	0-2 Saat
Lise Mezunu	3-6 Yıl	3-5 Saat
Ön lisans Mezunu	7-10 Yıl	6-10 Saat
Lisans Mezunu	11-15 Yıl	11+ Saat
Yüksek Lisans Mezunu	15+ Yıl	
Doktora Mezunu		

Riskli ve Korumacı Davranış Ölçekleri

Riskli ve korumacı davranış ölçekleri Öğütçü (2010) tarafından hazırlanan "E-Dönüşüm Sürecinde Kişisel Bilişim Güvenliği Davranışı ve Farkındalığının Analizi" başlıklı yüksek lisans tezi kapsamında geliştirilmiştir. Riskli davranış ölçeği son kullanıcıların belirli bilişim teknolojileri kullanım alışkanlıklarının veya şekillerinden yola çıkarak kendilerini riske atma derecesini ölçmeyi amaçlamaktadır. Ölçülen davranışlar kısa dönemde kullanıcıya kolaylık sağlasa da uzun dönemde sıkıntı yaşayabileceği davranışlar olarak tanımlanmaktadır. Bu ölçekten alınan puan riskli davranış puanı (RDP) olarak isimlendirilmektedir. Korumacı davranış ölçeği son kullanıcıların bilgilerini güvende tutmak için bilişim teknolojileri üzerinde uyguladıkları belirli davranışlara göre kendilerinin dikkat ve korumacılık seviyesini ölçmeyi amaçlamaktadır. Belirtilen davranışların güvenlik ihlallerinin oluşma riskini azaltacağı ifade edilmektedir. Bu ölçekten alınan puan riskli davranış puanı (KDP) olarak isimlendirilmektedir. Her iki ölçek de 20 sorudan meydana gelmekte olup 5 değerlendirmeli Likert tipi ölçeklerdir (EK 3) . Ölçekler için atanacak değerler 1 (hiç) ve 5 (her zaman) aralığında değişmektedir. Riskli davranış ölçeğinden yüksek puanlar alıyor olmak kişinin bilişim sistemleri ve teknolojilerini kullanırken hayli toleranslı davranışlar sergilediğini gösterirken, korumacı davranış ölçeğinden alınan yüksek puanlar kişinin güvenli ve koruyucu davranışlar sergilediğini göstermektedir. İki ölçek çift kutuplu olmayıp birbirinin karşılığı olarak düşünülemezler.

Tehlike Algısı ve Suça Maruziyet Ölçekleri

Tehlike algısı ve suça maruziyet ölçekleri de Öğütçü (2010) tez çalışması kapsamında geliştirilmiştir. Tehlike algısı ölçeği son kullanıcının belirli bilişim sistemleri ve teknolojileri hakkında algıladıkları riskin seviyesini ölçmeyi amaçlamaktadır. Bu seviye kavram olarak güven duygusu ile ilişkilendirilmektedir. Bu ölçekten alınan puan riskli davranış puanı (TAP) olarak isimlendirilmektedir. Suça maruziyet ölçeği ise son kullanıcının kendi göstermiş olduğu bilinçli veya bilinçsiz bir davranış sonucunda bilgi güvenliğine yönelik bir ihale veya olaya maruz kalma seviyesini ölçmeyi amaçlamaktadır. Bu ölçekten alınan puan suça maruziyet puanı (SMP) olarak isimlendirilmektedir. Ölçek maddeleri Türkiye Bilişim Güvenliği Derneği ve

Emniyet Genel Müdürlüğü Bilişim Suçları Müdürlüğü ile ortak çalışma ile hazırlanmıştır. Tehlike algısı ölçeği 25 sorudan oluşurken suça maruziyet ölçeği 15 soru ihtiva etmektedir (EK 3). Her iki ölçek de değerlendirmeli likert tipinde olup tehlike algısı ölçeği için 1 (fikrim yok) ile 5 (çok tehlikeli) aralığında değer alırken; suça maruziyet ölçeği için 1 (hiçbir zaman) ile 5 (her zaman) aralığında değer almaktadır. 62 katılımcı ile gerçekleştirilen çalışmada tüm ölçekler 0,9345 alfa değeri ile yüksek güvenirlik göstermektedir. Mevcut çalışmada kullanmak üzere araştırmacıdan gerekli izinler alınmış EK 4'te sunulmuştur.

Büyük Beşli Kişilik Envanteri

Büyük Beşli Kişilik Envanteri bireyin kişilik özelliklerini uyumluluk, özdenetim, nevrotizm, gelişime açıklık ve dışa dönüklük bağlamında ölçmek için geliştirilmiştir (Martinez ve John, 1998). 56 farklı ülkeden araştırmacıların kendi ülkelerinde gerçekleştirdikleri çalışmada (Schmitt vd., 2007) Sümer ve Sümer (2005) Büyük Beşli Kişilik Envanterinin Türkçe 'ye uyarlamasını gerçekleştirmişlerdir. Ölçek 44 maddeden oluşmakla birlikte, uyumluluk için 9, özdenetim için 8, nevrotizm için 8, gelişime açıklık için 10 ve dışa dönüklük için 8 soru bulunmaktadır (EK 3). 5 değerlendirmeli Likert tipinde olan ölçek 1 (kesinlikle katılmıyorum) ile 5 (kesinlikle katılıyorum) aralığında değer almaktadır. Beş değişkenli bu modelin en üstün yanı, bilimsel gözleme dayanmasından dolayı farklı ülkelerde veya kültürlerde araştırma konusu edildiğinde benzer sonuçların alınmasıdır (Gültaş ve Tüzüner, 2017).

Nevrotizm duygusal istikrar halinin karşılığı olarak ifade edilmekle birlikte, ölçek sonucu yüksek puan olan bireylerin pesimizim, utanma, suçluluk duyma, duygusal istikrarsızlık gibi olumsuz duyguları yaşama ve barındırma eğiliminde oldukları görülmektedir. Ölçek sonucunda dışadönüklük puanı yüksek olan bireylerin ise sosyal yönlerinin ağır bastığı, diğer bireylerle çalışmaya istekli olup iddialarını belli ettikleri vurgulanmaktadır. Gelişme açıklık puanı yüksek olan bireyler ise aktif olarak tanımlanmakta, hayal gücü yüksek, tercihleri çeşitlilik içeren ve muhakeme yeteneği geniş olarak ifade edilmektedir. Uyumluluk puanı yüksek olan bireylerin ise diğer bireylere karşı hoşgörülü olma, onlara güvenme ve onları kabul etme eğiliminde oldukları vurgulanmaktadır. Ölçek sonucunda özdenetim puanı yüksek olan bireylerin ise kendilerine güvenlerinin tam ve sorumluluk duygularının yüksek olduğu bireyle işaret

edilmekle bu bireyler güçlü, iradeli, görev ve başarı odaklı olarak karakterize edilmektedir (L. Zhang, 2006) Büyük beşli kişilik ölçeğinin Türkçe 'ye uyarlanmış versiyonunun güvenirlik katsayıları 0,66 ile 0,77 arasında değişen değerlerde rapor edilmiştir (Sümer, Lajunen ve Özkan, 2005). Mevcut çalışmada kullanmak üzere araştırmacıdan gerekli izinler alınmıştır (EK 4).

Uygulamanın Web Sitesi

www.wizarduilding.com web sitesi "E-Dönüşüm Sürecinde Kişisel Bilişim Güvenliği Davranışı ve Farkındalığının Analizi" başlıklı çalışması sonucu ortaya çıkan, kişinin beyanatına dayalı 4 ölçek içerisinde davranış olarak ölçülebilen 11 seçeneğin, uzman görüşleri de alınarak kullanıcı girdisine izin verecek şekilde tasarlanması ile hazırlanmıştır. Katılımcıların her bir seçenek için göstermiş olduğu davranış veri tabanına, eposta hesabı birincil anahtar değeri olacak şekilde kaydedilmiştir. Bu sayede veri toplama birinci aşamasında toplanan veriler ile birlikte analiz edilebilme yeteneği kazandırılmıştır.

Verilerin Analizi

Çalışma sırasınca elde edilen veriler SPSS (The Statistical Package for the Social Sciences) istatistik programı kullanılarak çözümlenmiş ve analiz edilmiştir. Katılımcılara ait değişkenlerin gösteriminde denek sayısı, ortalama, standart sapma gibi istatistikler betimleyici istatistiki tablolar kullanılarak aktarılmıştır. Demografik ve sosyo-demografik değişkenleri arasındaki ilişkiler korelasyon analizi ve çapraz tablolar kullanılarak yorumlanmıştır. Katılımcıların KDP, RDP, SMP ve TAP puanlarının demografik ve sosyo-demografik değişkenlere göre farklılaşıp farklılaşmadığını test etmek için tek faktörlü varyans analizi (ANOVA) ve Kruskall-Wallis H testleri kullanılmıştır. KDP ve RDP bağımlı değişkenlerindeki değişimleri bağımsız demografik, sosyo-demografik, kişilik testi puanları değişkenleri ile açıklamak için basit doğrusal regresyon istatistik analiz yöntemi kullanılmıştır. Yöntem doğrusal bir model oluşturup, bu doğrusal modelde bulunan bağımsız değişkenlerdeki bir birimlik değişimin bağımlı değişkende meydana getireceği değişimin tespitinden ibarettir

Basit regresyon modeli şu şekilde ifade edilebilir:

$$Y=a+bX$$

Burada Y bağımlı değişken tahminini ifade ederken, a model sabitini, b katsayıları ise modelde bulunan X bağımsız değişkenlerinin katsayılılarını ifade etmektedir.

Bilgi güvenliği konusunda gözlenen veri toplama aşamasının ikinci bölümünü oluşturan ve ölçülebilecek her bir davranış için, veri toplama aşamasının ilk bölümünü oluşturan ve davranışa ait olarak kendi söylemleri ile birlikte değerlendirilerek sonuçlar dört grup halinde kategorilendirilmiştir. Buna göre ilgili davranışı (korumacı davranışlar için) gerçekleştirdiğini / (riskli davranışlar için) gerçekleştirmediğini;

- "Söyler ve Yapar"
- "Söyler ancak Yapmaz"
- "Söylemez ve Yapmaz"
- "Söylemez ancak Yapar"

şeklinde sınıflandırmıştır.

Bu kapsamda bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin demografik özellikleri arasındaki ilişkinin analiz edilmesi kapsamında, kategorik değişkenler arasındaki ilişkileri araştırmak için Ki-Kare Bağımsızlık testi kullanılmış, güven aralığı %95 olarak analizler yapılmıştır

Aynı kapsamda bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin kişilik özellikleri arasındaki ilişkinin analiz edilmesi için, dört gruptan oluşan davranış durumları normal dağılım göstermediğinden ve gruplar homojen olmadığından analiz için parametrik-olmayan testlerden Kruskal Wallis-H testi, hangi grupların farklılık gösterdiğinin analizi için ise post hoc Tomhane's T2 testi %95 güven aralığında uygulanmıştır.

Aynı kapsamda bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin tehlike algıları, suça maruz kalma durumları, riskli davranış özellikleri ve korumacı davranış özellikleri

arasındaki ilişkinin analiz edilmesi için, dört gruptan oluşan davranış durumları normal dağılım gösteren ve gruplar homojen olan seçeneklerin analizi için MANOVA ve hangi grupların farklılık gösterdiğinin analizi için ise post hoc Tukey testi; normal dağılım göstermeyen ve grupları homojen olmayan seçeneklerin analizi için parametrik olmayan testlerden Kruskal Wallis-H Testi, hangi grupların farklılık gösterdiğinin analizi için ise post hoc Tomhane's T2 testi %95 güven aralığında uygulanmıştır.

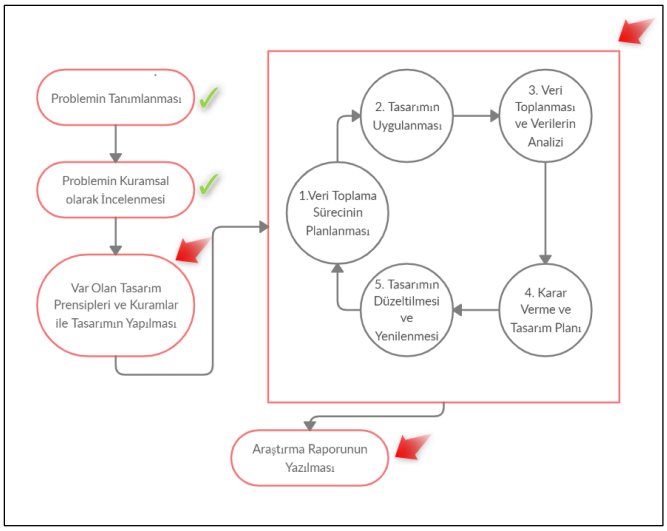
Aynı kapsamda bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin yazma hızları ve dikkatleri arasındaki ilişkinin analiz edilmesi için, dört gruptan oluşan davranış durumları ile sürekli değişken olan yazma hızları arasındaki ilişki analiz edilirken; normal dağılım gösteren ve gruplar homojen olan seçeneklerin analizi için tek-yönlü-ANOVA kullanılmıştır. Hangi grupların farklılık gösterdiğinin analizi için ise post hoc Tukey testi; normal dağılım göstermeyen ve grupları homojen olmayan seçeneklerin analizi parametrik olmayan testlerden Kruskal Wallis-H testi, hangi grupların farklılık gösterdiğinin analizi için ise post hoc Tomhane's T2 testi %95 güven aralığında uygulanmıştır. Kategorik değişkenler arasındaki ilişkileri araştırmak için Ki-Kare Bağımsızlık testi kullanılmış, güven aralığı %95 olarak analizler yapılmıştır. Her bir bilgi güvenliği davranışı için yapılan analizler birlikte verilmiştir.

Tez çalışması kapsamında veri madenciliği ve makine öğrenmesi işlemleri için IBM firması tarafından piyasaya sürülen SPSS Modeler yazılımı kullanılmış olup C5.0 algoritması denemeler için kullanılmıştır. Denemeler sonucunda alan yazınla paralel olarak C5.0 algoritmasının daha yüksek oranda sonuçlar vermesinden ve araştırmacıya üzerinde daha kolay çalışma imkânı tanımasında dolayı kullanıcının modellenmesi ve sınıflandırılan davranışlara göre tahminlerin yapılması için bu algoritma kullanılmıştır.

BÖLÜM IV

BULGULAR VE YORUM

Bu çalışma ile bireylerin bilgi güvenliğine yönelik niyetleri ile gerçek hayattaki davranışları birlikte incelenerek, bilgi güvenliğine yönelik uyarlanabilir bir öğretim sistemi geliştirilmesi amaçlanmıştır. Bu amaç doğrultusunda tasarım tabanlı araştırma yönteminden faydalanılmıştır. Çalışmanın bu bölümüne kadar tasarım tabanlı araştırmanın "problemin tanımlanması", "problemin kuramsal olarak incelenmesi" aşamaları tamamlanmıştır. Bu bölümde "var olan tasarım prensipleri ve kuramlar ile tasarımın yapılması" ile süreçlerin döngüsel olarak ilerlediği "veri toplama sürecinin planlanması", "tasarımın uygulanması", "veri toplanması ve analizi", "karar verme ve tasarım planı" ve "tasarımın düzeltilmesi / yenilenmesi" adımları elde edilen bulgularla birlikte yorumlanarak açıklanmıştır (Şekil 17).

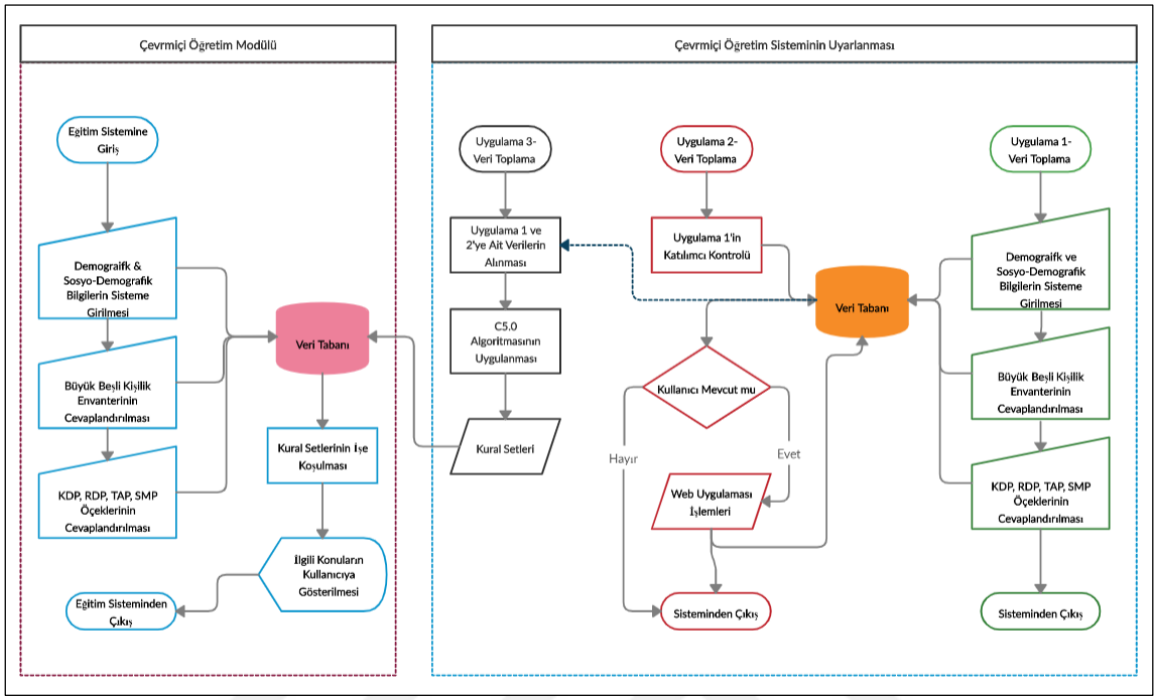


Şekil 17. Tasarım tabanlı araştırma döngüsü – tamamlanan aşamalar

Ayrıca uygun görülen hızlı prototipleme tasarım modelinin gereği olarak öğretim sisteminin prototip modeli ortaya çıkarılmıştır. Her bir uygulama adımında bulgular sunulurken tasarım tabanlı araştırma döngüsel sürecinde bir sonraki uygulama adımına girdi olacak şekilde aktarılmıştır.

Var Olan Tasarım İlkeleri ve Kuramlar ile Tasarımın Yapılması

Tasarlanan çevrimiçi öğretim sistemi ile öncelikli olarak katılımcılardan bilgi güvenliğine yönelik olarak hazırlanan, kişinin kendi beyanatına dayalı Likert tipi ölçekler uygulanıp, daha sonra uzman görüşü alınarak belirtilen ölçeklerde davranış olarak ölçülebilecek maddelerin bir web uygulaması yardımıyla davranışa dönüşüp dönüşmediklerinin belirlenmesi amaçlanmıştır. Alanyazın taraması sonrasında görüldüğü üzere kişi davranışlarını etkileyen kişilik, demografik ve sosyo-demografik özellikler de aynı kullanıcılardan alınarak elde edilen veriler C5.0 karar ağacı algoritması işe koşularak, kişinin kendi beyanatına dayalı olarak verdiği cevaplarla davranışlarının örtüşüp örtüşmediğinin belirlenmesi; bu örtüşme veya örtüşmeme durumuna etken olan sebeplerin ortaya çıkarılması ve buna göre modelleme işleminin yapılması kararına varılmıştır. Bu sayede bilgi güvenliğine yönelik hazırlanacak nihai çevrimiçi öğretim sistemine giriş yapan bir kullanıcının hangi davranış sınıfı için "bilgisi olma ve olmama" ve "davranışı gösterme ve göstermeme" durumunun olabileceğinin koşulan algoritma sayesinde belirlenmesi amaçlanmıştır. Böylece kullanıcının hangi eğitim içeriğine hangi yoğunlukta katılım sağlayacağının otomatik olarak belirlenerek uyarlamanın sağlanması kararına varılmıştır. Oluşturulan tasarıma ilişkin akış şeması Şekil 18'de sunulmuştur.



Şekil 18. Uyarlanabilir eğitim sistemi akış şeması

Birinci Döngü Geliştirme Raporu

Bu aşama, çevrimiçi öğretim sistemin uyarlanabilmesi için yapılan tasarıma göre kişinin kendi beyanatına dayanan ölçekler yardımıyla verilerin toplanması, analizi, bulgu ve yorumları içermektedir. "Bilgi güvenliği konusunda demografik özellikler niyetleri nasıl etkilemektedir?" ve "Bilgi güvenliği konusunda kişilik özellikleri niyetleri nasıl etkilemektedir?" araştırma sorularına bu bölümde cevap verilmiştir. Tasarım tabanlı araştırma yönteminin döngüsel adımlarını takip etmektedir.

Veri Toplama Süreci

Bu aşamada Öğütçü (2010) tarafından hazırlanmış olan "E- Dönüşüm Sürecinde Kişisel Bilişim Güvenliği Davranışı ve Farkındalığının Analizi" başlıklı çalışması sonucu ortaya çıkan, kullanıcının kendi beyanatına dayalı korumacı davranış, riskli davranış, Tehlike Algısı ve Suça Maruziyet Ölçekleri; Sümer ve Sümer (2005) tarafından Türkçe 'ye uyarlanan Büyük Beşli Kişilik Envanterinin çalışma kapsamında kullanılabilmesi için gerekli yazışmalar yapılarak

izinler alınmıştır. Demografik ve sosyo-demografik veriler de çalışma kapsamında veri toplama sürecine bu aşamada dâhil edilmiştir.

Tasarımın Uygulanması

Veri toplama sürecinde planlandığı üzere, veri toplama işlemi web tabanlı anket hizmeti sunan Google Forms üzerinden gerçekleştirilmiştir. Ankete katılım çağrısı sosyal medya platformları ve eposta grupları üzerinden gerçekleştirilmiştir. Çevrimiçi anket 2 ay süre ile yayında kalmıştır.

Verinin Toplanması ve Analizi

Uygulanan veri toplama işlemi sonrasında 640 kullanıcının katılım sağladığı görülmüştür. Birincil anahtar değeri olarak belirlenen eposta adresleri incelendiğinde 21 katılımcının iki defa katılım sağladığı görülmüştür. Anketi katılım tarih ve saatleri incelenerek ilk katılımları analizlere dâhil edilirken, ikinci katılımları silinmiştir. Toplam 619 kullanıcının katılım sağladığı görülmüştür.

Bu aşamada;

- Bilgi güvenliği konusunda demografik özellikler niyetleri nasıl etkilemektedir?
- Bilgi güvenliği konusunda kişilik özellikleri niyetleri nasıl etkilemektedir? Sorularına yanıt aranmış ve analizler gerçekleştirilmiştir.

Çalışmada, ulusal ve uluslararası normlara uygun olarak bağımsız denekler üzerinden toplanmış verilerin analiz edilmesi sonucunda aşağıdaki ilk sonuçlar elde edilmiştir.

Demografik İstatistikler

Çalışmanın ilk aşaması 619 bağımsız birey üzerinden gerçekleştirilmiştir. Bu bireylerden; 240'ı (%38,8) erkek iken 379'ı (%61,2) kadınlardan oluşmaktadır (Tablo 3). Harmanci, Dayıoğlu ve Kırkpınar (2019) sosyal medya bağımlılığı üzerine yaptıkları çalışma kapsamında araştırmaya katılan bireylerin %68,2'sini kadınların, %31,8'ini ise erkeklerin oluşturduğu görülmektedir. Benzer şekilde Dursun ve Özkan'ın (2019) sosyal medya etkisinin ölçüldüğü çalışmalarında araştırmaya katılan bireylerin %72,7'sini kadınların, %28,3'ünü erkeklerin oluşturduğu

görülmektedir. Anket katılım duyurusu sosyal medya üzerinden gerçekleştirildiği için çalışmaya katılan kadın katılımcı sayısının erkek katılımcılara göre fazla olması alan yazınla paralellik göstermektedir.

Tablo 3

Cinsiyet Dağılımı

	Cinsiyet	Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli	Erkek	240	38,8	38,8	38,8
	Kadın	379	61,2	61,2	100,0
	Toplam	619	100,0	100,0	

Katılımcıların 421'i (%60) lisans, yüksek lisans ve doktora mezunlarından oluşurken, 198'i (%40) ilköğretim, lise ve ön lisans mezunlarından oluşmaktadır (Tablo 4). Anket katılım duyurusu erişilen sosyal medya grupları, eposta grupları ve bu grup üyelerinin kendi üye oldukları başka gruplarda katılım çağrısı yapmaları üzerinden gerçekleştirilmiştir. Araştırmacının eğitim düzeyi göz önüne alındığında; katılımcıların eğitim düzeyinin bu şekilde dağılım göstermesinin, benzer sosyo-demografik özellikteki katılımcılara erişilmiş olmasından kaynaklı olabileceği değerlendirilmektedir.

Tablo 4

Eğitim Düzeyi Dağılımı

		Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli	İlköğretim Mezunu	12	1,9	1,9	1,9
	Lise Mezunu	114	18,4	18,4	20,4
	Ön Lisans Mezunu	72	11,6	11,6	32,0
	Lisans Mezunu	299	48,3	48,3	80,3
	Yüksek Lisans Mezunu	97	15,7	15,7	96,0
	Doktora Mezunu	25	4,0	4,0	100,0
	Toplam	619	100,0	100,0	

Katılımcıların yaşları incelendiğinde ise; %64' ünün Y kuşağında bulunduğu görülmektedir. Daha sonra ise en kalabalık yaş grubu olarak %17,9 ile X kuşağı ve %15 ile Z kuşağı gelmektedir. Bebek patlaması ise %3,1'lik oran ile en az katılımcının bulunduğu yaş grubudur. Katılımcılar arasında 1945 ve öncesinde doğan gelenekselciler kuşağından kimse bulunmamaktadır (Tablo 5). We are Social'ın (Kemp, 2019) Türkiye sosyal medya kullanım istatistikleri verilerine göre 65 üzeri yaşında sosyal medya kullanıcı sayısı ülke nüfusunun %2,5'i olarak belirtilmiştir. Bu sebeple gelenekselciler kuşağından katılımcının olmaması hayatın olağan akışına uygunluk göstermektedir.

Tablo 5

Yaş Aralığı Dağılımı

		Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli	X Kuşağı	111	17,9	17,9	17,9
	Y Kuşağı	396	64,0	64,0	81,9
	Z Kuşağı	93	15,0	15,0	96,9
	Bebek Patlaması	19	3,1	3,1	100,0
	Toplam	619	100,0	100,0	

Katılımcıların kaç yıldır internet kullanıcısı olduğu (IKY) incelendiğinde sadece %5,5'inin 3-6 yıl aralığında internet kullanıcısı oldukları, diğerlerinin ise (%94,5) 7 ve üzeri yıl internet kullanıcısı olduğu görülmektedir (Tablo 6). We are Social (Kemp, 2019) Türkiye sosyal medya kullanım istatistikleri verilerine göre X,Y ve Z kuşaklarında bulunan kullanıcı sayısının ülke nüfusunun %91,8'ini oluşturduğu belirtilmiştir. Bu oranın katılımcıların 7 ve üzeri yıl internet kullanıcısı olmaları ile çok yakın olduğu görülmektedir. Belirtilen oranların çalışmaya katılım sağlayan bireylerin sosyal medya üzerinde anket doldurma konusunda deneyim kazanmış olmasının, bu çalışmaya katılım sağlama eğilimini artırdığından kaynaklanıyor olabileceği değerlendirilmiştir.

Tablo 6

İnternet Kullanım Yılı Dağılımı

		Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli	3 - 6 Yıl	34	5,5	5,5	5,5
	7 - 10 Yıl	172	27,8	27,8	33,3
	11 - 15 Yıl	228	36,8	36,8	70,1
	15+ Yıl	185	29,9	29,9	100,0
	Toplam	619	100,0	100,0	

Katılımcıların günlük internet kullanım sürelerine (GİKS) bakıldığında ise katılımcıların %81,1'inin günlük 3 saat ve üzerinde internet kullandıkları görülmektedir (Tablo 7). We are Social (Kemp, 2019) Türkiye sosyal medya kullanım istatistikleri verilerine göre bireyler günün ortalama 7 saat 15 dakikasını internet kullanımı ile geçirmektedir. Çalışma kapsamında toplanan verilerin Türkiye ortalaması ile örtüştüğü görülmektedir.

Tablo 7

Günlük İnternet Kullanım Saati Dağılımı

		Frekans	Yüzde	Geçerli Yüzde	Kümülatif Yüzde
Geçerli	0 - 2 Saat	117	18,9	18,9	18,9
	3 - 5 Saat	275	44,4	44,4	63,3
	6 - 10 Saat	179	28,9	28,9	92,2
	11+ Saat	48	7,8	7,8	100,0
	Toplam	619	100,0	100,0	

Demografik ve Sosyo-Demografik Değişkenler Arasındaki İlişkiler

Demografik değişkenlerin birbirlerine göre gösterdiği değişkenlik ve aralarındaki istatistiksel anlamdaki ilişki seviyelerinin incelenmesi çalışmaya katkı sunan katılımcıların davranışlarının anlamlandırılmasında son derece etkili ve gerekli bir yöntemdir. Bu aşamada değişkenlerin birbirleriyle olan ilişkileri ikili analizler ile gerçekleştirilmiş olup üç ve üzeri etkileşimler göz ardı edilmiştir.

Cinsiyet Değişkeni

Tablo 8 ve Tablo 9 incelendiğinde, erkek katılımcıların yaklaşık %83'ünün X ve Y kuşağında yer aldıkları, kadın katılımcıların ise %81'inin X ve Y kuşağında yer aldıkları görülmektedir. Tablodan da anlaşılacağı üzere yaş aralığı ile cinsiyet değişkenleri arasında anlamlı bir fark bulunmamaktadır.

Tablo 8

Cinsiyet ve Yaş Aralığı Değişkenleri Arasındaki Korelasyon

		Cinsiyet	Yaş Aralığı
Cinsiyet	Pearson Korelasyon	1	,058
	p		,149
	N	619	619
Yaş aralığı	Pearson Korelasyon	,058	1
	p	,149	
	N	619	619

Tablo 9

Cinsiyet ve Yaş Aralığı Değişkenleri Arasındaki Çapraz Tablo

			Yaş Aralığı				
			X Kuşağı	Y Kuşağı	Z Kuşağı	Bebek Patlaması	Toplam
Cinsiyet	Erkek	N	56	144	28	12	240
		% Cinsiyet	23,3%	60,0%	11,7%	5,0%	100,0%
	Kadın	N	55	252	65	7	379
		% Cinsiyet	14,5%	66,5%	17,2%	1,8%	100,0%
Toplam		N	111	396	93	19	619
		% Cinsiyet	17,9%	64,0%	15,0%	3,1%	100,0%

Tablo 10 ve Tablo 11 incelendiğinde, erkek katılımcıların %82,1'inin lise üzeri eğitim aldıkları, kadın katılımcıların ise %78'inin lise üzeri eğitim aldıkları görülmektedir. Tablo 9'dan da anlaşılacağı üzere eğitim durumları ile cinsiyet değişkenleri arasında anlamlı bir fark bulunmamaktadır.

Tablo 10

Cinsiyet ve Eğitim Düzeyi Değişkenleri Arasındaki Korelasyon

		Cinsiyet	Eğitim Düzeyi
Cinsiyet	Pearson Korelasyon	1	-,066
	p		,101
	N	619	619
Eğitim Düzeyi	Pearson Korelasyon	-,066	1
	p	,101	
	N	619	619

Tablo 11

Cinsiyet ve Eğitim Düzeyi Değişkenleri Arasındaki Çapraz Tablo

			Eğitim Düzeyi						
			İlköğretim Mezunu	Lise Mezunu	Ön Lisans Mezunu	Lisans Mezunu	Yüksek Lisans Mezunu	Doktora Mezunu	Toplam
Cinsiyet	Erkek	N	6	37	26	115	45	11	240
		% Cinsiyet	2,5%	15,4%	10,8%	47,9%	18,8%	4,6%	100,0%
	Kadın	N	6	77	46	184	52	14	379
		% Cinsiyet	1,6%	20,3%	12,1%	48,5%	13,7%	3,7%	100,0%
Total		N	12	114	72	299	97	25	619
		% Cinsiyet	1,9%	18,4%	11,6%	48,3%	15,7%	4,0%	100,0%

Tablo 12 ve Tablo 13 incelendiğinde; cinsiyet değişkeni ile İKY değişkeni arasında negatif yönlü kuvvetli bir ilişki olduğu (-0,229**) görülmektedir. Benzer şekilde çapraz tablo incelendiğinde de 7-10 yıl arası internet kullanan erkek katılımcıların oranı %17,5 iken kadın katılımcıların oranının %34,3 olduğu görülmektedir. Benzer şekilde 15 yıl üzeri internet kullanan erkek katılımcı oranı %42,5 iken kadın katılımcı oranının %21,9 olduğu görülmektedir. Çalışmaya katılım sağlayan bireylerden erkek katılımcıların yaygın olarak internet kullanmaya kadın katılımcılardan çok daha önce başladıkları ancak internet kullanımının genel olarak cinsiyetten bağımsız olduğu görülmektedir.

Tablo 12

Cinsiyet ve İnternet Kullanım Yılı Değişkenleri Arasındaki Korelasyon

		Cinsiyet	İnternet Kullanım Yılı
Cinsiyet	Pearson Korelasyon	1	-,229**
	p		,000
	N	619	619
İnternet Kullanım Yılı	Pearson Korelasyon	-,229**	1
	p	,000	
	N	619	619

**. Korelasyon 0.01 düzeyinde anlamlıdır (2-yönlü).

Tablo 13

Cinsiyet ve Eğitim Düzeyi Değişkenleri Arasındaki Çapraz Tablo

			İnternet Kullanım Yılı				
			3 - 6 Yıl	7 - 10 Yıl	11 - 15 Yıl	15+ Yıl	Toplam
Cinsiyet	Erkek	N	10	42	86	102	240
		% Cinsiyet	4,2%	17,5%	35,8%	42,5%	100,0%
	Kadın	N	24	130	142	83	379
		% Cinsiyet	6,3%	34,3%	37,5%	21,9%	100,0%
Total		N		172	228	185	619
		% Cinsiyet		27,8%	36,8%	29,9%	100,0%

Cinsiyet ve GİKS değişkenleri arasındaki korelasyonu gösterir Tablo 14 ile çapraz tablo (Tablo 15) birlikte incelendiğinde; cinsiyet değişkeni ile GİKS değişkeni arasında negatif yönlü kuvvetli bir ilişki olduğu (-0,081**) görülmektedir. Bu iki değişkene ait çapraz tabloyu incelediğimizde ise sırayla, 1-2 saat internet kullanan erkek katılımcı oranı %16,7 iken, kadın katılımcıların oranı %2,3'tür. 3-5 saat internet kullanan erkek katılımcı oranı %41,7 iken, kadın katılımcıların oranı %46,2'dir. 6-10 saat internet kullanan erkek katılımcı oranı %32,5 iken, kadın katılımcıların oranı %26,6'dır. 11 saat üzeri internet kullanan erkek katılımcı oranı %9,2 iken, kadın katılımcıların oranı %6,9 olarak görülmüştür. Tablolardan çıkan sonuç özetle, katılımcılar arasında erkek ve kadınların günlük internet kullanım süreleri arasında bir fark olduğu ancak her ne kadar bu fark anlamlı olsa da süreler bakımından farkın çok büyük düzeylerde olmadığı bildirmektedir.

Tablo 14

Cinsiyet ve Günlük İnternet Kullanım Süresi Değişkenleri Arasındaki Korelasyon

		Cinsiyet	GİKS
Cinsiyet	Pearson Korelasyon	1	-,081*
	p		,044
	N	619	619
GİKS	Pearson Korelasyon	-,081*	1
	p	,044	
	N	619	619

*. Korelasyon 0.05 düzeyinde anlamlıdır (2-yönlü).

Tablo 15

Cinsiyet ve Günlük İnternet Kullanım Saati Değişkenleri Arasındaki Çapraz Tablo

			Günlük İnternet Kullanım Saati				
			0 - 2 Saat	3 - 5 Saat	6 - 10 Saat	11+ Saat	Toplam
Cinsiyet	Erkek	N	40	100	78	22	240
		% Cinsiyet	16,7%	41,7%	32,5%	9,2%	100,0%
	Kadın	N	77	175	101	26	379
		% Cinsiyet	20,3%	46,2%	26,6%	6,9%	100,0%
Total		N	117	275	179	48	619
		% Cinsiyet	18,9%	44,4%	28,9%	7,8%	100,0%

Eğitim Düzeyi Değişkeni

Eğitim düzeyi ve yaş aralığı değişkenleri arasındaki ilişkiyi sezgisel olarak ele aldığımızda aralarında negatif ve güçlü bir ilişki olması beklenmektedir. Bu değerlendirme ışığında yukarıda bulunan iki değişken arasındaki korelasyonu gösterir Tablo 16 ile çapraz tablo (Tablo 17) birlikte incelendiğinde; iki değişken arasında negatif yönlü kuvvetli bir ilişki olduğu (-0,320**) görülmektedir. Katılımcılar arasında yaş aralığı ve eğitim düzeyi arasında ters orantılı bir ilişki söz konusudur.

Tablo 16

Eğitim Düzeyi ve Yaş Aralığı Değişkenleri Arasındaki Korelasyon

		Eğitim Düzeyi	Yaş Aralığı
Eğitim Düzeyi	Pearson Korelasyon	1	-,320**
	p		,000
	N	619	619
Yaş Aralığı	Pearson Korelasyon	-,320**	1
	p	,000	
	N	619	619

**. Korelasyon 0.01 düzeyinde anlamlıdır (2-yönlü).

Tablo 17

Eğitim Düzeyi ve Yaş Aralığı Değişkenleri Arasındaki Çapraz Tablo

			Yaş Aralığı				
			X Kuşağı	Y Kuşağı	Z Kuşağı	Bebek Patlaması	Toplam
Eğitim Düzeyi	İlköğretim Mezunu	N	1	2	9	0	12
		% Eğitim Düzeyi	8,3%	16,7%	75,0%	0,0%	100,0%
	Lise Mezunu	N	16	43	51	4	114
		% Eğitim Düzeyi	14,0%	37,7%	44,7%	3,5%	100,0%
	Ön Lisans Mezunu	N	17	42	7	6	72
		% Eğitim Düzeyi	23,6%	58,3%	9,7%	8,3%	100,0%
	Lisans Mezunu	N	39	228	25	7	299
		% Eğitim Düzeyi	13,0%	76,3%	8,4%	2,3%	100,0%
	Yüksek Lisans Mezunu	N	26	69	1	1	97
		% N Düzeyi	26,8%	71,1%	1,0%	1,0%	100,0%
	Doktora Mezunu	N	12	12	0	1	25
		% Eğitim Düzeyi	48,0%	48,0%	0,0%	4,0%	100,0%
Toplam		N	111	396	93	19	619
		% Eğitim Düzeyi	17,9%	64,0%	15,0%	3,1%	100,0%

Eğitim düzeyi ve İKY değişkenleri arasındaki korelasyonu gösterir Tablo 18 ile çapraz tablo (Tablo 19) birlikte incelendiğinde; eğitim düzeyi değişkeni ile İKY değişkeni arasında pozitif yönlü kuvvetli bir ilişki olduğu (0,412**) görülmektedir. Benzer sonucu iki değişken arasındaki çapraz tablodan da teyit etmek mümkündür. Ayrıca eğitim düzeyi ve yaş aralığı değişkenleri arasındaki ilişki için sezgisel beklentiler bu iki değişken için de geçerlidir. Yaşça küçük olan katılımcıların eğitim düzeyinin düşük olması ve haliyle yaşlarının küçük olması sonucu internet kullanıcısı olma sürelerinin (yıl olarak) de düşük olması beklenilen bir neticedir.

Tablo 18

Eğitim Düzeyi ve İnternet Kullanım Yılı Değişkenleri Arasındaki Korelasyon

		Eğitim Düzeyi	İnternet Kullanım Yılı
Eğitim Düzeyi	Pearson Korelasyon	1	,412**
	p		,000
	N	619	619
İnternet Kullanım Yılı	Pearson Korelasyon	,412**	1
	p	,000	
	N	619	619

**. Korelasyon 0.01 düzeyinde anlamlıdır (2-yönlü).

Tablo 19

Eğitim Düzeyi ve İnternet Kullanım Yılı Değişkenleri Arasındaki Çapraz Tablo

			İnternet Kullanım Yılı				
			3 - 6 Yıl	7 - 10 Yıl	11 - 15 Yıl	15+ Yıl	Toplam
Eğitim Düzeyi	İlköğretim Mezunu	N	3	6	2	1	12
		% Eğitim Düzeyi	25,0%	50,0%	16,7%	8,3%	100,0%
	Lise Mezunu	N	20	45	40	9	114
		% Eğitim Düzeyi	17,5%	39,5%	35,1%	7,9%	100,0%
	Ön Lisans Mezunu	N	2	27	26	17	72
		% Eğitim Düzeyi	2,8%	37,5%	36,1%	23,6%	100,0%
	Lisans Mezunu	N	9	81	121	88	299
		% Eğitim Düzeyi	3,0%	27,1%	40,5%	29,4%	100,0%
	Yüksek Lisans Mezunu	N	0	11	32	54	97
		% Eğitim Düzeyi	0,0%	11,3%	33,0%	55,7%	100,0%
	Doktora Mezunu	N	0	2	7	16	25
		% Eğitim Düzeyi	0,0%	8,0%	28,0%	64,0%	100,0%
Toplam		N	34	172	228	185	619
		% Eğitim Düzeyi	5,5%	27,8%	36,8%	29,9%	100,0%

Eğitim düzeyi ve GİKS değişkenleri arasındaki korelasyonu gösterir Tablo 20 ile çapraz tablo (Tablo 21) birlikte incelendiğinde; eğitim düzeyi değişkeni ile GİKS değişkenleri arasında anlamlı bir ilişki olduğu (0,021) söylenememektedir. Katılımcıların eğitim düzeyleri ile günlük internet kullanım süreleri arasında anlamlandırılabilecek bir ilişki bulunmamaktadır. İki değişken arasındaki çapraz tablo incelendiğinde de herhangi bir ilişkinin bulunmadığı, her eğitim düzeyinde katılımcıların çoğunluğunun günlük 3-5 ila 6-10 saat aralığında internet kullandığı gözlenebilmektedir.

Tablo 20

Eğitim Düzeyi ve Günlük İnternet Kullanım Saati Değişkenleri Arasındaki Korelasyon

		Eğitim Düzeyi	Günlük İnternet Kullanım Saati
Eğitim Düzeyi	Pearson Korelasyon	1	,021
	p		,606
	N	619	619
Günlük İnternet Kullanım Saati	Pearson Korelasyon	,021	1
	p	,606	
	N	619	619

Tablo 21

Eğitim Düzeyi ve Günlük İnternet Kullanım Saati Değişkenleri Arasındaki Çapraz Tablo

			Günlük İnternet Kullanım Saati				
			1 - 2 Saat	3 - 5 Saat	6 - 10 Saat	11+ Saat	Toplam
Eğitim Düzeyi	İlköğretim Mezunu	N	2	8	2	0	12
		% Eğitim Düzeyi	16,7%	66,7%	16,7%	0,0%	100,0%
	Lise Mezunu	N	18	56	32	8	114
		% Eğitim Düzeyi	15,8%	49,1%	28,1%	7,0%	100,0%
	Ön lisans Mezunu	N	13	33	20	6	72
		% Eğitim Düzeyi	18,1%	45,8%	27,8%	8,3%	100,0%
	Lisans Mezunu	N	65	124	84	26	299
		% Eğitim Düzeyi	21,7%	41,5%	28,1%	8,7%	100,0%
	Yüksek Lisans Mezunu	N	14	42	35	6	97
		% Eğitim Düzeyi	14,4%	43,3%	36,1%	6,2%	100,0%
	Doktora Mezunu	N	5	12	6	2	25
		% Eğitim Düzeyi	20,0%	48,0%	24,0%	8,0%	100,0%
Toplam		N	117	275	179	48	619
		% Eğitim Düzeyi	18,9%	44,4%	28,9%	7,8%	100,0%

Yaş Aralığı Değişkeni

Yaş aralığı ile internet kullanım yılı değişkenleri arasındaki korelasyonu gösterir Tablo 22 ile çapraz tablo (Tablo 23) birlikte incelendiğinde; eğitim düzeyi değişkeni ile İKY değişkeni arasında negatif yönlü kuvvetli bir ilişki olduğu (-0,342**) görülmektedir. Benzer sonucu iki değişken arasındaki çapraz tablodan da teyit etmek mümkündür. Daha önce incelenen eğitim düzeyi ve yaş aralığı değişkenleri arasındaki ilişkiye benzer olarak yaş aralığı değişkeni ile İKY değişkeni arasında doğal beklenti olan negatif yönlü kuvvetli ilişki katılımcılardan elde edilen verilerle de desteklenmekte ve çalışmada kullanılan verilerin hayatın normal akışına uyumluluğunu da teyit etmektedir.

Tablo 22

Yaş Aralığı ve İnternet Kullanım Yılı Değişkenleri Arasındaki Korelasyon

		Yaş Aralığı	İnternet Kullanım Yılı
Yaş Aralığı	Pearson Korelasyon	1	-,342**
	p		,000
	N	619	619
İnternet Kullanım Yılı	Pearson Korelasyon	-,342**	1
	p	,000	
	N	619	619

**. Korelasyon 0.01 düzeyinde anlamlıdır (2-yönlü).

Tablo 23

Yaş Aralığı ve İnternet Kullanım Yılı Değişkenleri Arasındaki Çapraz Tablo

			İnternet Kullanım Yılı				
			3 - 6 Yıl	7 - 10 Yıl	11 - 15 Yıl	15+ Yıl	Toplam
Yaş Aralığı	X Kuşağı	N	3	18	28	62	111
		% Yaş Aralığı	2,7%	16,2%	25,2%	55,9%	100,0%
	Y Kuşağı	N	11	99	171	115	396
		% Yaş Aralığı	2,8%	25,0%	43,2%	29,0%	100,0%
	Z Kuşağı	N	17	51	24	1	93
		% Yaş Aralığı	18,3%	54,8%	25,8%	1,1%	100,0%
	Bebek Patlaması	N	3	4	5	7	19
		% Yaş Aralığı	15,8%	21,1%	26,3%	36,8%	100,0%
Toplam		N	34	172	228	185	619
		% Yaş Aralığı	5,5%	27,8%	36,8%	29,9%	100,0%

Yaş aralığı ile GİKS değişkenleri arasındaki korelasyonu gösterir Tablo 24 ile çapraz tablo (Tablo 25) birlikte incelendiğinde; eğitim düzeyi değişkeni ile GİKS değişkeni arasında pozitif yönlü bir ilişki olduğu (0,093*) görülmektedir. İki değişken arasındaki çapraz tablo incelendiğinde ise değişkenler arasındaki korelasyonla benzer olarak Z kuşağının Y kuşağından, Y kuşağının da X kuşağından daha yoğun internet kullandığı gözlemlenebilmektedir.

Tablo 24

Yaş Aralığı ve Günlük İnternet Kullanım Saati Değişkenleri Arasındaki Korelasyon

		Yaş Aralığı	Günlük İnternet Kullanım Saati
Yaş Aralığı	Pearson Korelasyon	1	,093*
	p		,021
	N	619	619
Günlük İnternet Kullanım Saati	Pearson Korelasyon	,093*	1
	p	,021	
	N	619	619

*. Korelasyon 0.05 düzeyinde anlamlıdır (2-yönlü).

Tablo 25

Yaş Aralığı ve Günlük İnternet Kullanım Saati Değişkenleri Arasındaki Çapraz Tablo

			Günlük İnternet Kullanım Saati				Toplam
			0 - 2 Saat	3 - 5 Saat	6 - 10 Saat	11+ Saat	
Yaş Aralığı	X Kuşağı	N	37	47	23	4	111
		% Yaş Aralığı	33,3%	42,3%	20,7%	3,6%	100,0%
	Y Kuşağı	N	65	170	126	35	396
		% Yaş Aralığı	16,4%	42,9%	31,8%	8,8%	100,0%
	Z Kuşağı	N	10	47	28	8	93
		% Yaş Aralığı	10,8%	50,5%	30,1%	8,6%	100,0%
	Bebek Patlaması	N	5	11	2	1	19
		% Yaş Aralığı	26,3%	57,9%	10,5%	5,3%	100,0%
Toplam		N	117	275	179	48	619
		% Yaş Aralığı	18,9%	44,4%	28,9%	7,8%	100,0%

İnternet Kullanım Yılı Değişkeni

İKY ile GİKS değişkenleri arasındaki korelasyonu gösterir Tablo 26 ile çapraz tablo (Tablo 27) birlikte incelendiğinde; aralarında anlamlı bir ilişki olduğu (0,024) söylenememektedir. İki değişken arasındaki çapraz tablo incelendiğinde ise daha uzun yıl internet kullanan katılımcıların günlük internette geçirdikleri sürelerin daha fazla veya daha az olması veya tam tersi bir yorum için geçerli veriler bulunmamaktadır. Sonuç olarak internet kullanım yılının günlük internet kullanım sürelerine bir etkisi bulunmamıştır.

Tablo 26

İnternet Kullanım Yılı ve Günlük İnternet Kullanım Saati Değişkenleri Arasındaki Korelasyon

		İnternet Kullanım Yılı	Günlük İnternet Kullanım Saati
İnternet Kullanım Yılı	Pearson Korelasyon	1	,024
	p		,558
	N	619	619
Günlük İnternet Kullanım Saati	Pearson Korelasyon	,024	1
	p	,558	
	N	619	619

Tablo 27

İnternet Kullanım Yılı ve Günlük İnternet Kullanım Saati Değişkenleri Arasındaki Çapraz Tablo

			Günlük İnternet Kullanım Saati				
			1 - 2 Saat	3 - 5 Saat	6 - 10 Saat	11+ Saat	Toplam
İnternet Kullanım Yılı	3 - 6 Yıl	N	4	16	12	2	34
		% İKY	11,8%	47,1%	35,3%	5,9%	100,0%
	7 - 10 Yıl	N	33	88	39	12	172
		% İKY	19,2%	51,2%	22,7%	7,0%	100,0%
	11 - 15 Yıl	N	42	97	71	18	228
		% İKY	18,4%	42,5%	31,1%	7,9%	100,0%
	15+ Yıl	N	38	74	57	16	185
		% İKY	20,5%	40,0%	30,8%	8,6%	100,0%
Toplam		N	117	275	179	48	619
		% İKY	18,9%	44,4%	28,9%	7,8%	100,0%

Demografik ve Sosyo-Demografik Değişkenler ile KDP, RDP, TAP, SMP Arasındaki İlişkiler

Bu aşamada katılımcıların demografik ve sosyo demografik özellikleri ile korumacı ve riskli davranışları, tehlike algıları ve suça maruziyet durumları arasındaki ilişki incelenmiştir.

Cinsiyet Değişkeni

Cinsiyet değişkeni ile KDP, RDP, SMP ve TAP değişkenleri arasında nasıl bir ilişki olduğunu incelendiğinde aşağıda belirtilen sonuçlar elde edilmiştir.

Tablo 28

Cinsiyet Değişkeni ile KDP, RDP, SMP, TAP Arasındaki Korelasyon

		Cinsiyet	KDP	RDP	SMP	TAP
Cinsiyet	Pearson Korelasyon	1	-,119**	-,012	-,104**	-,053
	p		,003	,773	,009	,187
	N	619	619	619	619	619

**.Korelasyon 0.01 düzeyinde anlamlıdır (2-yönlü).

Cinsiyet değişkeni ile KDP, RDP, SMP ve TAP değişkenleri arasındaki korelasyonlar incelendiğinde (Tablo 28); cinsiyet ile KDP arasında negatif yönlü anlamlı bir ilişki olduğu görülmektedir. Aynı şekilde cinsiyet ile SMP arasında da negatif yönlü anlamlı bir ilişki olduğu

görülmektedir. Ancak cinsiyet değişkeni ile RDP ve TAP değişkenleri arasında anlamlı bir korelasyon olduğu söylenememektedir.

Cinsiyet değişkeni ile KDP, RDP, SMP ve TAP değişkenleri arasında cinsiyet üzerinden gruplar arası anlamlı bir fark olup olmadığı sırası ile ortalamalar tablosu (Tablo 29) ve ANOVA tablosu (Tablo 30) üzerinden incelendiğinde;

Tablo 29

Cinsiyet Değişkeni ile KDP, RDP, SMP, TAP Arasındaki Ortalamalar Tablosu

Cinsiyet		KDP	RDP	SMP	TAP
Erkek	Ortalama	45,00	33,92	5,99	52,72
	N	240	240	240	240
	Std. Sapma	15,030	12,613	7,482	13,470
Kadın	Ortalama	41,23	33,61	4,64	51,08
	N	379	379	379	379
	Std. Sapma	15,663	12,734	5,368	16,004
Total	Ortalama	42,69	33,73	5,16	51,72
	N	619	619	619	619
	Std. Sapma	15,518	12,678	6,302	15,082

Tablo 30

Cinsiyet Değişkeni ile KDP, RDP, SMP, TAP Arasındaki Anova Tablosu

		KT	Sd	KO	F	p
KDP	Gruplar Arası	2091,960	1	2091,960	8,797	,003
	Gruplar İçinde	146720,485	617	237,797		
	Toplam	148812,446	618			
RDP	Gruplar Arası	13,392	1	13,392	,083	,773
	Gruplar İçinde	99318,091	617	160,969		
	Toplam	99331,483	618			
SMP	Gruplar Arası	266,360	1	266,360	6,770	,009
	Gruplar İçinde	24274,160	617	39,342		
	Toplam	24540,520	618			
TAP	Gruplar Arası	396,037	1	396,037	1,743	,187
	Gruplar İçinde	140179,921	617	227,196		
	Toplam	140575,958	618			

Cinsiyet değişkeni ile KDP arasında p=0,003<0,05 olduğundan, gruplar arasında son derece anlamlı bir fark olduğu görülmektedir. Ancak cinsiyet değişkeni ile RDP arasında p=0,773>0,05 olduğundan, gruplar arasında anlamlı bir fark olduğu söylenememektedir. Cinsiyet değişkeni ile SMP arasında p=0,009<0,05 olduğundan, gruplar arasında son derece anlamlı bir fark olduğu görülmektedir. Cinsiyet değişkeni ile TAP arasında p=0,187>0,05 olduğundan, gruplar arasında anlamlı bir fark olduğu söylenememektedir.

Eğitim Düzeyi Değişkeni

Eğitim düzeyi değişkeni ile KDP, RDP, SMP ve TAP değişkenleri arasında nasıl bir ilişki olduğu incelendiğinde aşağıda belirtilen sonuçlar elde edilmiştir.

Tablo 31

Eğitim Düzeyi Değişkeni ile KDP, RDP, SMP, TAP Arasındaki Korelasyon

		Eğitim Düzeyi	KDP	RDP	SMP	TAP
Eğitim Düzeyi	Pearson Korelasyon	1	,081*	,211**	,002	,124**
	p		,043	,000	,969	,002
	N	619	619	619	619	619

*. Korelasyon 0.05 düzeyinde anlamlıdır (2-yönlü).

**. Korelasyon 0.01 düzeyinde anlamlıdır (2-yönlü).

Eğitim düzeyi değişkeni ile KDP, RDP, SMP ve TAP değişkenleri arasındaki korelasyonlar incelendiğinde (Tablo 31); eğitim düzeyi ile KDP arasında pozitif yönlü anlamlı bir ilişki olduğu, RDP ile arasında pozitif yönde kuvvetli bir ilişki olduğu, SMP ile arasında anlamlı bir ilişki bulunmadığı, TAP ile arasında yine pozitif yönde kuvvetli bir ilişki olduğu görülmektedir.

Eğitim düzeyi değişkeni ile KDP, RDP, SMP ve TAP değişkenleri arasında eğitim düzeyi üzerinden gruplar arası anlamlı bir fark olup fark olup olmadığı sırası ile ortalamalar tablosu (Tablo 32) ve Kruskal-Wallis Test tablosu (Tablo 33) üzerinden incelendiğinde;

Tablo 32

Eğitim Düzeyi Değişkeni ile KDP, RDP, SMP, TAP Arasındaki Ortalamalar Tablosu

Eğitim Düzeyi		KDP	RDP	SMP	TAP
İlköğretim Mezunu	Ortalama	42,17	25,33	3,67	48,42
	N	12	12	12	12
	Std. Sapma	19,366	9,109	5,280	17,239
Lise Mezunu	Ortalama	39,56	30,42	5,81	47,42
	N	114	114	114	114
	Std. Sapma	15,704	14,094	6,933	17,209
Ön Lisans Mezunu	Ortalama	43,99	29,94	4,56	50,04
	N	72	72	72	72
	Std. Sapma	16,574	12,362	6,535	15,522
Lisans Mezunu	Ortalama	42,89	34,88	5,00	53,76
	N	299	299	299	299
	Std. Sapma	15,518	12,245	5,698	14,324
Yüksek Lisans Mezunu	Ortalama	44,61	36,71	5,33	51,74
	N	97	97	97	97
	Std. Sapma	13,637	10,255	7,229	12,255
Doktora Mezunu	Ortalama	43,68	38,44	5,96	53,16
	N	25	25	25	25
	Std. Sapma	15,908	15,009	6,295	17,601
Toplam	Ortalama	42,69	33,73	5,16	51,72
	N	619	619	619	619
	Std. Sapma	15,518	12,678	6,302	15,082

Tablo 33

Eğitim Düzeyi Değişkeni ile KDP, RDP, SMP, TAP Arasındaki Hipotez Testi Tablosu

Sıfır Hipotezi	Test	p	Karar
KDP Dağılımı Eğitim Düzeyi Kategorilerinde Aynıdır	Bağımsız- Örnekler Kruskal-Wallis Testi	,230	Sıfır Hipotezi Kabul Edildi
RDP Dağılımı Eğitim Düzeyi Kategorilerinde Aynıdır	Bağımsız- Örnekler Kruskal-Wallis Testi	,000	Sıfır Hipotezi Reddedildi
SMP Dağılımı Eğitim Düzeyi Kategorilerinde Aynıdır	Bağımsız- Örnekler Kruskal-Wallis Testi	,092	Sıfır Hipotezi Kabul Edildi.
TAP Dağılımı Eğitim Düzeyi Kategorilerinde Aynıdır.	Bağımsız- Örnekler Kruskal-Wallis Testi	,003	Sıfır Hipotezi Reddedildi

Anlamlılık düzeyi ,05.

Eğitim düzeyi değişkeni ile KDP arasında gruplar arası anlamlı bir fark olup olmadığına bakıldığında p=0,230>0,05 olduğundan, gruplar arasında anlamlı bir fark olmadığı görülmektedir. Eğitim düzeyi değişkeni ile RDP arasında gruplar arası anlamlı bir fark olup

olmadığına bakıldığında p=0,000<0,05 olduğundan, gruplar arasında son derece anlamlı bir fark olduğu görülmektedir. Eğitim düzeyi değişkeni ile SMP arasında gruplar arası anlamlı bir fark olup olmadığına bakıldığında p=0,092>0,05 olduğundan, gruplar arasında anlamlı bir fark olmadığı görülmektedir. Eğitim düzeyi değişkeni ile TAP arasında gruplar arası anlamlı bir fark olup olmadığına bakıldığında p=0,003<0,05 olduğundan, gruplar arasında son derece anlamlı bir fark olduğu görülmektedir.

Yaş Aralığı Değişkeni

Yaş aralığı değişkeni ile KDP, RDP, SMP ve TAP değişkenleri arasında nasıl bir ilişki olduğu incelendiğinde aşağıda belirtilen sonuçlar elde edilmiştir.

Tablo 34

Yaş Aralığı Değişkeni ile KDP, RDP, SMP, TAP Arasındaki Korelasyon

		Yaş Aralığı	KDP	RDP	SMP	TAP
Yaş Aralığı	Pearson Korelasyon	1	-,132**	,062	,028	-,090*
	p		,001	,126	,484	,025
	N	619	619	619	619	619

*. Korelasyon 0.05 düzeyinde anlamlıdır (2-yönlü).

**. Korelasyon 0.01 düzeyinde anlamlıdır (2-yönlü).

Yaş aralığı değişkeni ile KDP, RDP, SMP ve TAP değişkenleri arasındaki korelasyonlar incelendiğinde (Tablo 34); yaş aralığı değişkeni ile KDP arasında negatif yönlü kuvvetli bir ilişki olduğu, RDP ile arasında anlamlı bir ilişki bulunmadığı, SMP ile arasında anlamlı bir ilişki bulunmadığı, TAP ile arasında yine negatif yönlü anlamlı bir ilişki olduğu görülmektedir.

Yaş aralığı değişkeni ile KDP, RDP, SMP ve TAP değişkenleri arasında yaş aralığı üzerinden gruplar arası anlamlı bir fark olup olmadığı sırası ile ortalamalar tablosu (Tablo 35) ve Kruskal-Wallis Test tablosu (Tablo 36) üzerinden incelendiğinde;

Tablo 35

Yaş Aralığı Değişkeni ile KDP, RDP, SMP, TAP Arasındaki Ortalamalar Tablosu

Yaş Aralığı		KDP	RDP	SMP	TAP
X Kuşağı	Ortalama	43,55	29,51	5,14	54,33
	N	111	111	111	111
	Std. Sapma	15,536	12,656	7,159	15,241
Y Kuşağı	Ortalama	44,03	35,03	4,99	51,69
	N	396	396	396	396
	Std. Sapma	15,248	12,009	6,202	14,849
Z Kuşağı	Ortalama	37,38	34,33	5,95	48,66
	N	93	93	93	93
	Std. Sapma	14,249	13,322	5,944	15,541
Bebek Patlaması	Ortalama	35,79	28,47	5,11	52,00
	N	19	19	19	19
	Std. Sapma	20,305	17,040	4,653	15,055
Toplam	Ortalama	42,69	33,73	5,16	51,72
	N	619	619	619	619
	Std. Sapma	15,518	12,678	6,302	15,082

Tablo 36

Yaş Aralığı Değişkeni ile KDP, RDP, SMP, TAP Arasındaki Hipotez Testi Tablosu

Sıfır Hipotezi	Test	p	Karar
KDP Dağılımı Yaş Aralığı Kategorilerinde Aynıdır	Bağımsız- Örnekler Kruskal-Wallis Testi	,002	Sıfır Hipotezi Reddedildi
RDP Dağılımı Yaş Aralığı Kategorilerinde Aynıdır	Bağımsız- Örnekler Kruskal-Wallis Testi	,000	Sıfır Hipotezi Reddedildi
SMP Dağılımı Yaş Aralığı Kategorilerinde Aynıdır	Bağımsız- Örnekler Kruskal-Wallis Testi	,237	Sıfır Hipotezi Kabul Edildi
TAP Dağılımı Yaş Aralığı Kategorilerinde Aynıdır.	Bağımsız- Örnekler Kruskal-Wallis Testi	,081	Sıfır Hipotezi Kabul Edildi

Anlamlılık düzeyi, 05.

Tablo 36 incelendiğinde yaş aralığı değişkeni ile KDP arasında gruplar arası anlamlı bir fark olup olmadığına bakıldığında p=0,002<0,05 olduğundan, gruplar arasında son derece anlamlı bir fark olduğu görülmektedir. Benzer şekilde; yaş aralığı değişkeni ile RDP arasında p=0,000<0,05 olduğundan gruplar arasında son derece anlamlı bir fark olduğu görülmektedir. Yaş aralığı değişkeni ile SMP arasında p=0,237>0,05 olduğundan gruplar arasında anlamlı bir fark olduğu söylenememektedir. Yaş aralığı değişkeni ile TAP arasında p=0,081>0,05 olduğundan gruplar arasında anlamlı bir fark olduğu söylenememektedir.

İnternet Kullanım Yılı Değişkeni

İnternet kullanım yılı değişkeni ile KDP, RDP, SMP ve TAP değişkenleri arasında nasıl bir ilişki olduğunu incelediğimizde aşağıda belirtilen sonuçlar elde edilmiştir (Tablo 37).

Tablo 37

İKY Değişkeni ile KDP, RDP, SMP, TAP Arasındaki Korelasyon

		İnternet Kullanım Yılı	KDP	RDP	SMP	TAP
İnternet Kullanım Yılı	Pearson Korelasyon	1	,136**	,130**	,022	,149**
	p		,001	,001	,591	,000
	N	619	619	619	619	619

**. Korelasyon 0.01 düzeyinde anlamlıdır (2-yönlü).

İnternet kullanım yılı değişkeni ile KDP, RDP, SMP ve TAP değişkenleri arasındaki korelasyonlar incelendiğinde; internet kullanım yılı değişkeni ile KDP ve RDP arasında pozitif yönlü kuvvetli bir ilişki olduğu, SMP ile arasında anlamlı bir ilişki bulunmadığı, TAP ile arasında yine pozitif yönlü kuvvetli bir ilişki olduğu görülmektedir.

İnternet kullanım yılı değişkeni ile KDP, RDP, SMP ve TAP değişkenleri arasında İnternet kullanım yılı üzerinden gruplar arası anlamlı bir fark olup olmadığı sırası ile ortalamalar tablosu (Tablo 38) ve Kruskal-Wallis Test tablosu (Tablo39) üzerinden incelendiğinde;

Tablo 38

İKY Değişkeni ile KDP, RDP, SMP, TAP Arasındaki Ortalamalar Tablosu

İKY		KDP	RDP	SMP	TAP
3 - 6 Yıl	Ortalama	37,59	23,18	3,94	47,53
	N	34	34	34	34
	Std. Sapma	20,074	13,726	6,353	14,431
7 - 10 Yıl	Ortalama	41,05	33,26	4,92	49,45
	N	172	172	172	172
	Std. Sapma	15,210	13,170	4,735	17,552
11 - 15 Yıl	Ortalama	42,36	35,18	5,74	51,60
	N	228	228	228	228
	Std. Sapma	16,020	11,586	7,412	14,585
15+ Yıl	Ortalama	45,57	34,32	4,90	54,74
	N	185	185	185	185
	Std. Sapma	13,751	12,471	6,059	12,676
Toplam	Ortalama	42,69	33,73	5,16	51,72
	N	619	619	619	619
	Std. Sapma	15,518	12,678	6,302	15,082

Tablo 39

İKY Değişkeni ile KDP, RDP, SMP, TAP Arasındaki Hipotez Testi Tablosu

Sıfır Hipotezi	Test	p	Karar
KDP Dağılımı İKY Kategorilerinde Aynıdır	Bağımsız- Örnekler Kruskal-Wallis Testi	,008	Sıfır Hipotezi Reddedildi
RDP Dağılımı İKY Kategorilerinde Aynıdır	Bağımsız- Örnekler Kruskal-Wallis Testi	,000	Sıfır Hipotezi Reddedildi
SMP Dağılımı İKY Kategorilerinde Aynıdır	Bağımsız- Örnekler Kruskal-Wallis Testi	,032	Sıfır Hipotezi Reddedildi
TAP Dağılımı İKY Kategorilerinde Aynıdır.	Bağımsız- Örnekler Kruskal-Wallis Testi	,003	Sıfır Hipotezi Reddedildi

Anlamlılık düzeyi ,05

Tablo 39 incelendiğinde İKY değişkeni ile KDP arasında p=0,008<0,05 olduğundan, gruplar arasında son derece anlamlı bir fark olduğu görülmektedir. Benzer şekilde; İKY değişkeni ile RDP arasında gruplar arası anlamlı bir fark olup olmadığına bakıldığında p=0,000<0,05 olduğundan gruplar arasında son derece anlamlı bir fark olduğu söylenebilmektedir. İKY değişkeni ile SMP arasında p=0,032<0,05 olduğundan gruplar arasında son derece anlamlı bir fark olduğu görülmektedir. İKY değişkeni ile TAP arasında p=0,003<0,05 olduğundan gruplar arasında son derece anlamlı bir fark olduğu görülmektedir.

Günlük İnternet Kullanım Saati Değişkeni

GİKS değişken i ile KDP, RDP, SMP ve TAP değişkenleri arasında nasıl bir ilişki olduğu incelendiğinde aşağıda belirtilen sonuçlar elde edilmiştir (Tablo 40).

Tablo 40

GİKS Değişkeni ile KDP, RDP, SMP, TAP Arasındaki Korelasyon

		Günlük İnternet Kullanım Saati	KDP	RDP	SMP	TAP
Günlük İnternet Kullanım Saati	Pearson Korelasyon	1	,173**	,261**	,038	,002
	p		,000	,000	,348	,958
	N	619	619	619	619	619

**. Korelasyon 0.01 düzeyinde anlamlıdır (2-yönlü).

GİKS değişkeni ile KDP, RDP, SMP ve TAP değişkenleri arasındaki korelasyonlar incelendiğinde; GİKS değişkeni ile KDP ve RDP arasında pozitif yönlü kuvvetli bir ilişki olduğu, SMP ve TAP arasında anlamlı bir ilişki bulunmadığı görülmektedir. GİKS değişkeni ile KDP, RDP, SMP ve TAP değişkenleri arasında internette geçirilen saat dilimleri üzerinden gruplar arası anlamlı bir fark olup olmadığı sırası ile ortalamalar tablosu (Tablo 41) ve Kruskal-Wallis Test tablosu (Tablo 42) üzerinden incelendiğinde;

Tablo 41

GİKS Değişkeni ile KDP, RDP, SMP, TAP Arasındaki Ortalamalar Tablosu

GİKS		KDP	RDP	SMP	TAP
1 - 2 Saat	Ortalama	40,18	28,46	4,43	51,29
	N	117	117	117	117
	Std. Sapma	16,158	11,891	6,468	15,536
3 - 5 Saat	Ortalama	40,92	32,96	5,29	51,91
	N	275	275	275	275
	Std. Sapma	14,745	11,696	6,520	14,796
6 - 10 Saat	Ortalama	45,14	36,72	5,53	51,85
	N	179	179	179	179
	Std. Sapma	15,733	13,244	6,197	15,818
11+ Saat	Ortalama	49,81	39,85	4,90	51,13
	N	48	48	48	48
	Std. Sapma	14,431	12,558	4,865	13,048
Toplam	Ortalama	42,69	33,73	5,16	51,72
	N	619	619	619	619
	Std. Sapma	15,518	12,678	6,302	15,082

Tablo 42

GİKS Değişkeni ile KDP, RDP, SMP, TAP Arasındaki Hipotez Testi Tablosu

Sıfır Hipotezi	Test	p	Karar
KDP Dağılımı GİKS Kategorilerinde Aynıdır	Bağımsız- Örnekler Kruskal-Wallis Testi	,000	Sıfır Hipotezi Reddedildi
RDP Dağılımı GİKS Kategorilerinde Aynıdır	Bağımsız- Örnekler Kruskal-Wallis Testi	,000	Sıfır Hipotezi Reddedildi
SMP Dağılımı GİKS Kategorilerinde Aynıdır	Bağımsız- Örnekler Kruskal-Wallis Testi	,029	Sıfır Hipotezi Reddedildi
TAP Dağılımı GİKS Kategorilerinde Aynıdır.	Bağımsız- Örnekler Kruskal-Wallis Testi	,845	Sıfır Hipotezi Kabul Edildi

Anlamlılık düzeyi ,05

Tablo 42 incelendiğinde GİKS değişkeni ile KDP arasında p=0,000<0,05 olduğundan, gruplar arasında son derece anlamlı bir fark olduğu görülmektedir. Benzer şekilde; GİKS değişkeni ile

RDP arasında p=0,000<0,05 olduğundan gruplar arasında son derece anlamlı bir fark olduğu görülmektedir. GİKS değişkeni ile SMP arasında p=0,029<0,05 olduğundan gruplar arasında son derece anlamlı bir fark olduğu görülmektedir. GİKS değişkeni ile TAP arasında p=0,845>0,05 olduğundan gruplar arasında anlamlı bir fark olduğu söylenememektedir.

Bireysel Farklılıklar ve Bilgi Güvenliği Davranış Niyetleri Arasındaki İlişki

Çalışmanın bu aşaması bireylerin bilgi güvenliği konusunda, kendi söylemleri ile davranışları gösterip göstermediklerini hangi değişkenlerin etkiliyor olduğunun belirlenmesini içermektedir.

Çalışmaya esas teşkil eden bağımlı değişkenler(Y):

Y_{kdp} : Korumacı Davranış Puanı

Y_{rdp} :Riskli Davranış Puanı

iken, bu bağımlı değişkenler üzerindeki değişimleri açıklamaya çalışacak bağımsız değişkenler (X) ise şunlardır:

X_{cn}: Cinsiyet

X_{ed} : Eğitim Düzeyi

X_{ya} : Yaş Aralığı

X_{iky} : İnternet Kullanım Yılı

X_{giks} : Günlük İnternet Kullanım Süresi (Saat)

X_{uk}: Uyumluluk

$X_{ök}$: Özdenetim

X_{nk}: Nevrotizm

X_{gk}: Gelişime Açıklık

X_{dk}: Dışa dönüklük

X_{tap}: Tehlike Algısı Puanı

X_{smp}: Suça Maruziyet Puanı

Bağımlı değişken olan Y_{kdp} ile bağımsız değişkenler arasındaki ilişkinin tespiti için aralarındaki korelasyon değerleri incelendiğinde (Tablo 43);

Tablo 43

Y_{kdp} ile Bağımsız Değişkenler Arasındaki Korelasyon

		Y_{kdp}			Y_{kdp}			Y_{kdp}
X_{cn}	Pearson Korelasyon	-,119**	X_{giks}	Pearson Korelasyon	,173**	X_{gk}	Pearson Korelasyon	,298**
	p	,003		p	,000		p	,000
	N	619		N	619		N	619
X_{ed}	Pearson Korelasyon	,081*	X_{uk}	Pearson Korelasyon	,170**	X_{dk}	Pearson Korelasyon	,154**
	p	,043		p	,000		p	,000
	N	619		N	619		N	619
X_{ya}	Pearson Korelasyon	-,132**	$X_{ök}$	Pearson Korelasyon	,266**	X_{smp}	Pearson Korelasyon	-,014
	p	,001		p	,000		p	,725
	N	619		N	619		N	619
X_{iky}	Pearson Korelasyon	,136**	X_{nk}	Pearson Korelasyon	-,167**	X_{tap}	Pearson Korelasyon	,040
	p	,001		p	,000		p	,321
	N	619		N	619		N	619

**. Korelasyon 0.01 düzeyinde anlamlıdır (2-yönlü).
*. Korelasyon 0.05 düzeyinde anlamlıdır (2-yönlü).

Korumacı davranış puanı ile cinsiyet, yaş aralığı ve nevrotizm arasında negatif yönlü kuvvetli bir ilişki olduğu, ancak internet kullanım yılı, günlük internet kullanım saati, uyumluluk, özdenetim, gelişime açıklık, dışa dönüklük arasında pozitif yönlü kuvvetli bir ilişki olduğu görülmektedir. Korumacı davranış puanı ile eğitim düzeyi arasında ise pozitif yönlü anlamlı bir ilişki bulunmamaktadır. Özetle, Tablo 43 üzerindeki verilerden de anlaşılacağı üzere korumacı davranış puanı ile hemen tüm bağımsız değişkenler arasında ilişkinin boyutu ve yönü değişmekle birlikte anlamlı bir ilişki bulunmaktadır.

Korumacı davranış puanı bağımlı değişkenindeki değişimleri bağımsız (X) değişkenleri ile açıklamak için, istatistik analiz metotlarından biri olan basit doğrusal regresyon yöntemini kullanılmıştır.

Tablo 44

Y_{kdp} ile Bağımsız Değişkenler Arasındaki Regresyon Modeli[a]

Model		KT	Sd	KO	F	p
1	Regresyon	1155235,589	12	96269,632	480,338	,000[b]
	Artık Değer	121655,411	607	200,421		
	Toplam	1276891,000[d]	619			

a. Bağımlı Değişken: Korumacı Davranış Puanı
b. Tahmin Ediciler: Tehlike Algısı Puanı, Suça Maruziyet Puanı, GIKS, Nevrotizm, Yaş Aralığı, Eğitim Düzeyi, Cinsiyet, Dışa Dönüklük, IKY, Gelişime Açıklık, Özdenetim, Uyumluluk

Veriler için regresyon modeline ait Anova tablosu (Tablo 44) incelendiğinde, p=000<0,05 olduğu, modelin son derece anlamlı olduğu görülmektedir. Ancak modele ait bağımsız değişkenlerin bağımlı değişkeni açıklama oranı R kare değeri incelendiğinde bu oranın %18,7 olduğu görülmektedir (Tablo 45). Modelin anlamlılık düzeyi ile açıklama oranı arasında bir tutarsızlık olduğu açıktır.

Tablo 45

Y_{kdp} ile Bağımsız Değişkenler Arasındaki Regresyon Modeli Özeti

Model	R	R Kare	Düzeltilmiş R Kare	Tahminin Standart Hatası
1	,432[a]	,187	,173	14,109

a.Tahmin Ediciler: Tehlike Algısı Puanı, Suça Maruziyet Puanı, GIKS, Nevrotizm, Yaş Aralığı, Eğitim Düzeyi, Cinsiyet, Dışa Dönüklük, IKY, Gelişime Açıklık, Özdenetim, Uyumluluk

Aynı modeli model sabiti olmadan tekrar oluşturarak kestirim denkleminin daha doğru sonuç vermesini sağlamak istenildiğinde ve model tekrar oluşturulduğunda çıkan sonuç aşağıdaki gibidir (Tablo 46).

Tablo 46

Y_{kdp} ile Bağımsız Değişkenler Arasındaki Regresyon Modeli[a]

Model		KT	Sd	KO	F	p
1	Regresyon	1154873,275	10	115487,327	576,406	,000[b]
	Artık Değer	122017,725	609	200,358		
	Toplam	1276891,000	619			

a. Bağımlı Değişken: Korumacı Davranış Puanı
b. Tahmin Ediciler: Tehlike Algısı Puanı, Suça Maruziyet Puanı, GIKS, Nevrotizm, Yaş Aralığı, Eğitim Düzeyi, Cinsiyet, Dışa Dönüklük, IKY, Gelişime Açıklık, Özdenetim, Uyumluluk

Model sabiti olmadan oluşturulan modelin anlamlılık düzeyi, anova tablosu (Tablo 45) üzerinden incelendiğinde p=0,000<0,05 olduğundan model için son derece anlamlıdır denilebilmektedir. Aynı şekilde modelin bağımlı değişkeni hangi oranda açıkladığı incelendiğinde ise R kare değerinin 0,904 olduğu, bu durumda bağımsız değişkenlerin bağımlı değişkeni %90,4 oranında açıkladığı görülmektedir (Tablo 47).

Tablo 47

Y_{kdp} ile Bağımsız Değişkenler Arasındaki Model Sabiti Olmadan Oluşturulan Regresyon Modeli Özeti

Model	R	R Kare	Düzeltilmiş R Kare	Tahminin Standart Hatası
1	,951[a]	,904	,903	14,155

a.Tahmin Ediciler: Tehlike Algısı Puanı, Suça Maruziyet Puanı, GIKS, Nevrotizm, Yaş Aralığı, Eğitim Düzeyi, Cinsiyet, Dışa Dönüklük, IKY, Gelişime Açıklık, Özdenetim, Uyumluluk

Oluşturulan bu modelin hangi bağımsız değişkenlerden oluştuğu ve etki düzeyleri incelendiğinde ise; modelde bulunmasının anlamlı olduğu değişkenler sırasıyla günlük internet kullanım saati, özdenetim, gelişime açıklık ve uyumluluk değişkenleridir (Tablo 48).

Tablo 48

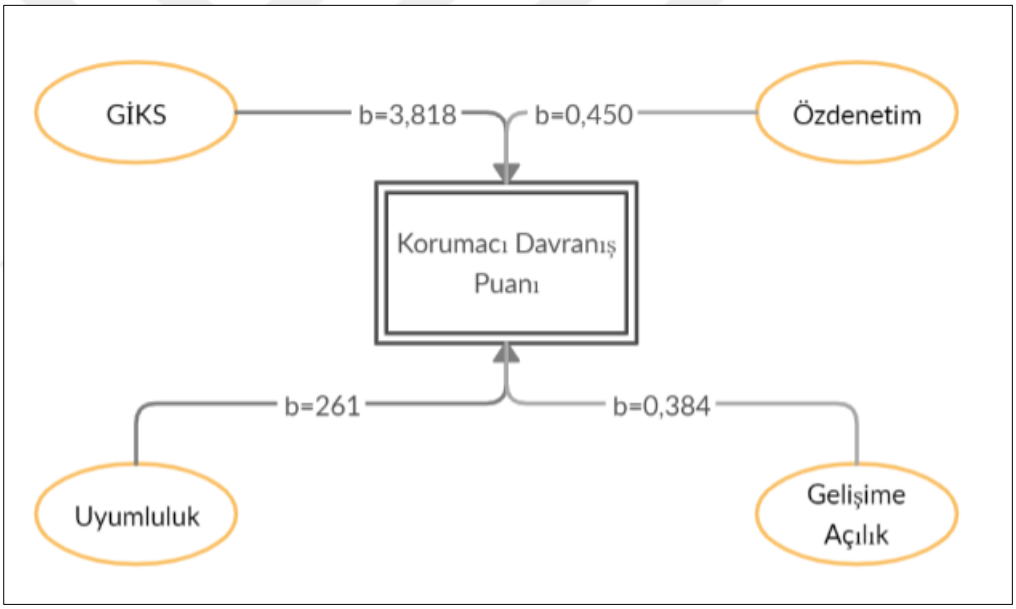
Y_{kdp} ile Bağımsız Değişkenler Katsayı Düzeyleri Tablosu[a]

Model		Standardize Edilmemiş Katsayılar		Standardize Edilmiş Katsayılar		
		B	Std. Hata	Beta	t	p.
1	X_{cn}	-2,121	1,201	-,079	-1,767	,078
	X_{ed}	,190	,560	,016	,338	,735
	X_{ya}	-1,470	,843	-,069	-1,743	,082
	X_{iky}	1,027	,721	,069	1,425	,155
	X_{giks}	3,818	,671	,203	5,686	,000
	X_{uk}	,249	,098	,186	2,541	,011
	X_{ok}	,450	,094	,338	4,809	,000
	X_{nk}	-,089	,087	-,040	-1,023	,307
	X_{gk}	,384	,083	,269	4,645	,000
	X_{dk}	,029	,090	,017	,320	,749
	X_{smp}	-,018	,092	-,003	-,197	,844
	X_{tap}	,050	,037	,059	1,341	,181

a. Bağımlı Değişken: Korumacı Davranış Puanı

Bu değişkenlerin modele etkisi incelendiğinde ise günlük internet kullanım saati değişkeninde bir birimlik değişikliğin bağımlı değişkende 3,886 birimlik değişime, özdenetim değişkeninde bir birimlik değişikliğin bağımlı değişkende 0,470 birimlik değişime, gelişime açıklık değişkeninde bir birimlik değişikliğin bağımlı değişkende 0,261 birimlik değişime sebep olduğu görülmektedir (Şekil 19). Etki düzeyine ilişkin oluşan regresyon denklemi ise:

Etki Düzeyi (Korumacı Davranış) = (Günlük İnternet Kullanım Saati)*3,818 + (Özdenetim Puanı)*0,450 + (Uyumluluk Puanı)*0,261 + (Gelişime Açıklık Puanı)* 0,384 şeklinde oluşmuştur.



Şekil 19. Korumacı davranış puanını etkileyen değişkenler ve etki değerleri

RDP ve Bireysel Farklılıklar Arasındaki İlişkinin İncelenmesi

Bağımlı değişken olan Y_{rdp} ile bağımsız değişkenler arasındaki ilişkinin tespiti için aralarındaki korelasyon değerleri incelendiğinde (Tablo 49);

Tablo 49

Y_{rdp} ile Bağımsız Değişkenler Arasındaki Korelasyon

		Y_{rdp}			Y_{rdp}			Y_{rdp}
X_{cn}	Pearson Korelasyon	-,012	X_{giks}	Pearson Korelasyon	,261**	X_{gk}	Pearson Korelasyon	,155**
	p	,773		p	,000		p	,000
	N	619		N	619		N	619
X_{ed}	Pearson Korelasyon	,211**	X_{uk}	Pearson Korelasyon	,063	X_{dk}	Pearson Korelasyon	,108**
	p	,000		p	,119		p	,007
	N	619		N	619		N	619
X_{ya}	Pearson Korelasyon	,062	$X_{ök}$	Pearson Korelasyon	-,039	X_{smp}	Pearson Korelasyon	,110**
	p	,126		p	,335		p	,006
	N	619		N	619		N	619
X_{iky}	Pearson Korelasyon	,130**	X_{nk}	Pearson Korelasyon	,068	X_{tap}	Pearson Korelasyon	-,119**
	p	,001		p	,089		p	,003
	N	619		N	619		N	619

**. Korelasyon 0.01 düzeyinde anlamlıdır (2-yönlü).

*. Korelasyon 0.05 düzeyinde anlamlıdır (2-yönlü).

Tablo 46 incelendiğinde Y_{rdp} ile eğitim düzeyi, internet kullanım yılı, günlük internet kullanım saati, gelişime açıklık, dışa dönüklük ve suça maruziyet puanı arasında pozitif yönlü, tehlike algısı puanı ile negatif yönlü bir ilişki olduğu görülmektedir. Bağımlı değişken olan Y_{rdp} bağımsız değişkenler ile açıklanmaya çalışıldığında oluşan modelin anlamlılık düzeyini gösteren ANOVA tablosu (Tablo 50) incelendiğinde p=000<0,05 olduğu ve modelin son derece anlamlı olduğu görülmektedir.

Tablo 50

Y_{rdp} ile Bağımsız Değişkenler Arasındaki Regresyon Modeli[a]

Model		KT	Sd	KO	F	p
1	Regresyon	723175,349	12	60264,612	454,549	,000
	Artık Değer	80476,651	607	132,581		
	Toplam	803652,000d	619			

a. Bağımlı Değişken: Riskli Davranış Puanı

Oluşturulan modelde bulunan bağımsız değişkenlerin bağımlı değişken olan riskli davranış puanını açıklama oranı incelendiğinde R kare değerinin 0,897 olduğu, bu durumda bağımsız değişkenlerin bağımlı değişkeni açıklama oranının % 89,7 olduğu görülmektedir (Tablo 51).

Tablo 51

Y_{rdp} ile Bağımsız Değişkenler Arasındaki Model Sabiti Olmadan Oluşturulan Regresyon Modeli Özeti

Model	R	R Kare	Düzeltilmiş R Kare	Tahminin Standart Hatası
1	,949[a]	,900	,898	11,514

a.Tahmin Ediciler: Tehlike Algısı Puanı, Suça Maruziyet Puanı, GIKS, Nevrotizm, Yaş Aralığı, Eğitim Düzeyi, Cinsiyet, Dışa Dönüklük, IKY, Gelişime Açıklık, Özdenetim, Uyumluluk

Oluşturulan bu modelin hangi bağımsız değişkenlerden oluştuğu ve etki düzeyleri incelendiğinde ise; modelde bulunmasının anlamlı olduğu değişkenler sırasıyla GİKS, eğitim düzeyi, yaş aralığı, İKY, uyumluluk, suça maruziyet puanı, gelişime açıklık, nevrotizm ve tehlike algısı puanı değişkenleridir. Modele alınan değişkenlerden sadece tehlike algısı puanı negatif etki ederken, diğer değişkenler pozitif etki etmektedir (Tablo 52).

Tablo 52

Y_{rdp} ile Bağımsız Değişkenler Katsayı Düzeyleri Tablosu[a]

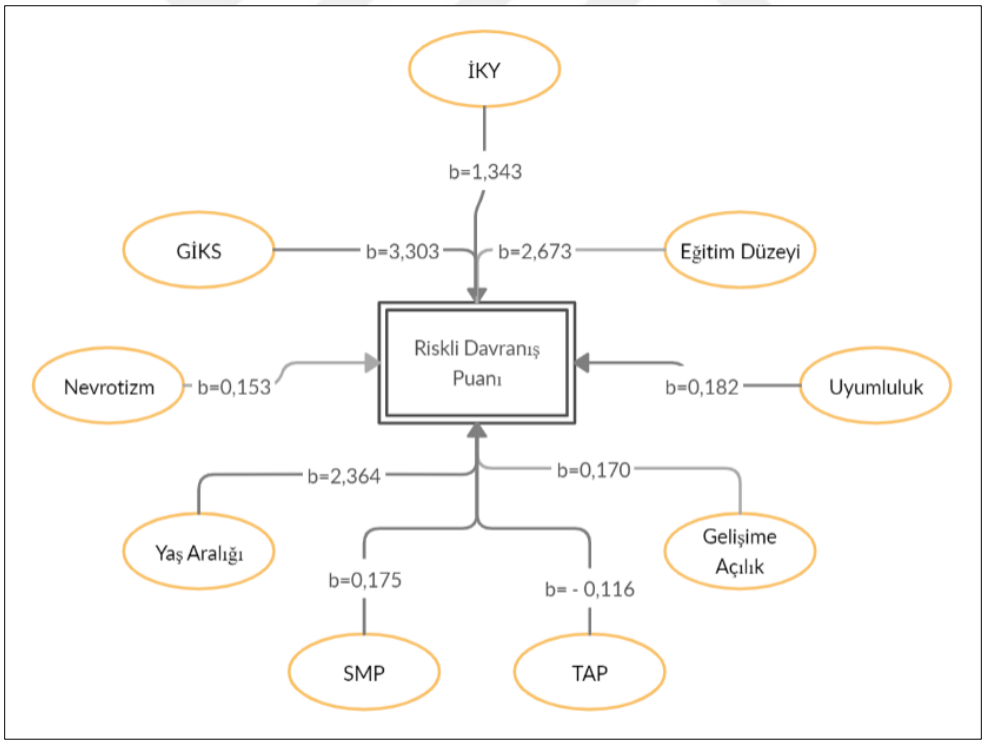
Model		Standardize Edilmemiş Katsayılar		Standardize Edilmiş Katsayılar		
		B	Std. Hata	Beta	t	p.
1	X_{cn}	,298	,976	,014	,306	,760
	X_{ed}	2,673	,456	,286	5,865	,000
	X_{ya}	2,364	,686	,140	3,448	,001
	X_{iky}	1,343	,586	,113	2,291	,022
	X_{giks}	3,303	,546	,221	6,049	,000
	X_{uk}	,182	,080	,172	2,284	,023
	X_{ok}	-,139	,076	-,131	-1,822	,069
	X_{nk}	,153	,070	,087	2,169	,030
	X_{gk}	,170	,067	,150	2,532	,012
	X_{dk}	,104	,073	,076	1,423	,155
	X_{smp}	,175	,075	,040	2,336	,020
	X_{tap}	-,116	,030	-,173	-3,840	,000

a. Bağımlı Değişken: Riskli Davranış Puanı

Bu değişkenlerin modele etkisi incelendiğinde ise İKY değişkeninde bir birimlik değişikliğin bağımlı değişkende 1,343 birimlik değişime, eğitim düzeyi değişkeninde bir birimlik değişikliğin bağımlı değişkende 2,673 birimlik değişime, uyumluluk değişkeninde bir birimlik değişikliğin bağımlı değişkende 0,182 birimlik değişime, gelişime açıklık değişkeninde bir

birimlik değişikliğin bağımlı değişkende 0,170 birimlik değişime, suça maruziyet puanı değişkeninde bir birimlik değişikliğin bağımlı değişkende 0,175 birimlik değişime, yaş aralığı değişkeninde bir birimlik değişikliğin bağımlı değişkende 2,368 birimlik değişime, nevrotizm değişkeninde bir birimlik değişikliğin bağımlı değişkende 0,53 birimlik değişime, GİKS değişkeninde bir birimlik değişikliğin bağımlı değişkende 3,303 birimlik değişime sebep olduğu görülmektedir (Şekil 20). Etki düzeyine ilişkin oluşan regresyon denklemi ise:

Etki Düzeyi (Riskli Davranış) = (Günlük İnternet Kullanım Saati)*3,303 + (İnternet Kullanım Yılı)*1,343 + (Eğitim Düzeyi)*2,673 + (Uyumluluk Puanı)* 0,182 + (Gelişime Açıklık Puanı)* 0,170 + (Nevrotizm Puanı)* 0,153 + (Yaş Aralığı)* 2,364 + (Suça Maruziyet Puanı)* 0,175 - (Tehlike Algısı Puanı)* 0,116 şeklinde oluşmuştur.



Şekil 20. Riskli davranış puanını etkileyen değişkenler ve etki değerleri

Şekil 20 incelendiğinde tehlike algısı puanı değişkeninde bir birimlik değişikliğin bağımlı değişkende negatif yönde 0,116 birimlik değişime sebep olduğu görülmektedir. Bu durum tehlike algısı düşük kullanıcıların daha çok riskli davranışta bulunduğunun göstergesidir.

Karar Verme ve Tasarım Planı

Bu aşamada toplanan ve analiz edilen veriler, bireylerin bilgi güvenliği konusunda korumacı ve riski davranışlarının demografik, sosyo-demografik, tehlike konusundaki algıları ve bilinçli ya da bilinçsiz maruz kaldıkları bir ihlal ya da olaydan etkilendikleri görülmüştür. Bu sebeple uygulama-2 aşamasında belirtilen değişkenlerin işe koşulmasının uygun olacağına karar verilmiştir.

Tasarımın Düzeltilmesi / Yenilenmesi

Uygulama-1 veri toplama sürecinde belirtilen tüm sorulara toplanan ve analiz edilen veriler ışığında cevap verilmiştir. Bu sebeple tasarımın düzeltilmesine veya yenilenmesine ihtiyaç duyulmamış, uygulamanın ikinci aşamasına geçilmiştir.

İkinci Döngü Geliştirme Raporu

Bu aşama, çevrimiçi öğretim sistemin uyarlanabilmesi için yapılan tasarıma göre uygulama-1 çıktılarına göre, katılımcıların belirlenen seçeneler üzerindeki davranışlar verilerinin toplanması, analizi, bulgu ve yorumları içermektedir. “Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin demografik özellikleri arasında anlamlı bir ilişki var mıdır?”, “bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin sosyo-demografik özellikleri arasında anlamlı bir ilişki var mıdır?”, ”bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin kişilik özellikleri arasında anlamlı bir fark var mıdır?”, “Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin tehlike algıları, suça maruz kalma durumları, riskli davranış özellikleri ve korumacı davranış özellikleri arasında anlamlı bir fark var mıdır?” ve “Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin yazma hızları ve dikkatleri

arasında anlamlı bir fark var mıdır?" araştırma sorularına bu bölüme cevap verilmiştir. Tasarım tabanlı araştırma yönteminin döngüsel adımlarını takip etektedir.

Veri Toplama Süreci

"E-Dönüşüm Sürecinde Kişisel Bilişim Güvenliği Davranışı ve Farkındalığının Analizi" başlıklı çalışması sonucu ortaya çıkan kişinin beyanatına dayalı 4 adet ölçek içeriğinde davranış olarak ölçülebilecek ve ölçülemeyecek seçenekler bulunmaktadır.

Davranış olarak ölçülebilecek seçenek örneği:

- *"İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım"*

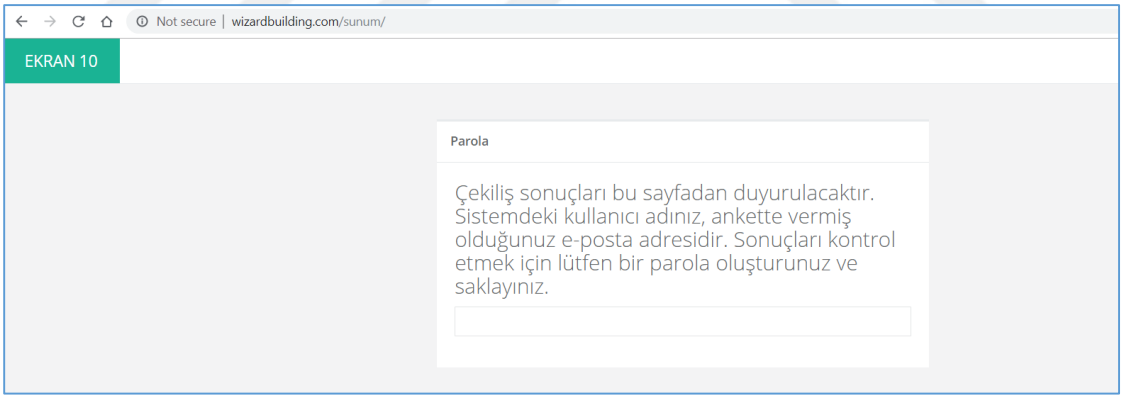
Davranış olarak ölçülemeyecek seçenek örneği:

- *"Virüs yazılımlarını tehlikeli bulurum."*

Bu seçeneklerden davranış olarak ölçülebilecek olanlar seçilerek, internet üzerinden yayınlanan bir web uygulaması üzerinden bu davranışları ölçmek için tasarım yapılmıştır. Konu ile ilgili olarak http://wizardbuilding.com/sunum/ ilk örnek web sitesi oluşturulmuştur. Bilgi güvenliği ölçeğinde davranışa dönüşebilecek olan seçenekler eposta ekinde kendilerine gönderilen dosyada sıra numarası ile sunulmuş olup, ilk örnek olarak hazırlanan web adresinde ilgili davranışın hangi ekranda ölçülmeye çalışıldığı da aynı satırda belirtilmiştir. Ekran sütununda "-" olarak işaretlenen satır, web sitesi üzerinde ilgili davranışı ölçebilecek bir ekranın tasarlanamadığını göstermektedir. Konu uzmanlarından web sitesi üzerinde kişinin ilgili ölçek maddesine verdiği cevabı haberi olmadan doğrulayabilmesi için hazırlanan web sitesindeki ilgili ekranları değerlendirerek uygunluğunu veya değiştirilmesi gerekli görülen kısmı belirtmesi ve ayrıca "-" olarak işaretlenen maddeler hakkında önerilerde bulunması istenmiştir. Örnek bir madde ve ekran görüntüsü aşağıda sunulmuştur (Bkz. Şekil 21 ve Şekil 22).

11	İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım.	10	Bu ekranda katılımcıdan, yapılacak olan çekilişi kontrol edebilmeleri için bir şifre belirlemeleri istenmektedir. Bu şifre aslında herhangi bir yerde kullanılmayacaktır. Amaç katılımcının belirlediği şifrenin karmaşık olup olmadığını ve bu sayede ölçeğe vermiş olduğu cevapla örtüşüp örtüşmediğini belirlemektir.
12	Elektronik/ Mobil imza kullanırım.	-	

Şekil 21. Uzman görüşü için gönderilen doküman



Şekil 22. İlk örnek web uygulamasında Madde-11 karşılığı olan sayfa

Bilgisayar ve Öğretim Teknolojileri Eğitimi, Bilgisayar Mühendisliği ve Bilişim Sistemleri bölümlerinden en az doktor unvanına sahip uzmanlardan görüş istenmiş ve yedi uzman görüşlerini bildirmiştir. Yapılan yorumlar EK 5'te sunulmuş ve içeriğe göre web uygulaması üzerinde gerekli düzenlemeler yapılmıştır.

Uzman görüşleri alındıktan sonra web uygulaması üzerinde gerekli düzenlemeler yapılmıştır. Ardından uygulamanın kullanılabilirliğinin ölçülmesi için sesli düşünme protokolü (think-aloud

protocol) uygulanmıştır. Sesli düşünme protokolü bir problem çözme işlemi esnasında araştırmacıya sesli ve zengin bilgi sağlayan bir çalışmadır. Araştırmacı problemi çözmek için çalışan kişileri gözleyerek onların problemi nasıl iyi çözdükleri, problemi nasıl tanımladıkları, bilgileri nasıl bir araya getirdikleri gibi bilgileri alarak çalışmalarına tekrar yön verebilirler (Fonteyn, Kuipers ve Grobe, 1993). Bir web sitesinin kullanılabilirliğinin ölçülmesi için uygulanabilen sesli düşünme protokolünde katılımcıların iki görevi tamamlaması beklenir. Bunlar web sitesi üzerinde gezinmek ve konuşmaktır (Stefano, Borsci ve Stamerra, 2010). Web sitesinin kullanılabilirliğini değerlendirmek için sesli düşünme protokolü uygulanırken, belirli sayıda kullanıcı kendilerinin değerlendirme işlemi yaptığını bilmeden, belirli bir süre içerisinde web sitesi üzerinde kendilerine verilen görevleri tamamlarken sesli olarak düşündüklerini ifade etmeleri istenir. Araştırmacı katılımcılara ait kaydedilen bu ses verilerinden web sitesine ait içeriğin okunması (örn: başlık) , yapılan etkinliğin tanımlanması (örn: alttaki bağlantıyı seçiyorum), anladığını açıklama (örn: bu bir açıklama gibi duruyor burayı tıklamalıyım sanırım) ve kullanıcı davranışı (örn: burada çok fazla bağlantı var hangisini seçeceğim?) gibi geliştirmeye yönelik bilgileri alarak gerekli iyileştirmelere karar verir (Cooke, 2010). Bu kapsamda farklı demografik özelliklerde beş kullanıcıya (Örn: Z kuşağı, ilköğretim öğrencisi, günlük internet kullanım saati 2, internet kullanım yılı 3, erkek; X kuşağı, üniversite mezunu, günlük internet kullanım saati 8, internet kullanım yılı 11+, kadın) web uygulaması kullandırılmış, protokol gereği olarak katılımcılara uygulamayı kullanırken o an nasıl hissettikleri, çekinmeden akıllarından geçebilecek herhangi bir şeyi yüksek sesle paylaşmaları istenmiş; işlem yapılırken kendilerine müdahale edilmeyeceği ve bu işlemin kamera ile kayıt altına alınacağı bildirilmiştir. Uygulama sonucunda aşağıda belirtilen gözlemler not edilmiş ve uygulama üzerinde ilgili değişiklikler yapılmıştır.

Bulgular

Katılımcı 1:

* *Ekran 3:* Kırmızı renkli alana sürüklemekte zorlandığı gözlendi. Kutucuğun alt tarafına doğru bırakmaya çalıştı ancak bu kısım kutucuğun dışı konumunda kaldı.

* *Ekran 5:* Bu ekranda ne yapacağını tam çözemedi.

* *Ekran 6:* Yönerge içeriğinde işlemi tamamlamak için 30 saniye süresi olduğunun bildirilmesine rağmen dikkat etmedi ve aramaya devam etti. Süre dolup ekran bir sonrakine geçmesine rağmen hala çerez arıyordu.

Katılımcı 2:

* *Ekran 3:* Katılımcı 1 ile aynı sıkıntıyı yaşadığı gözlendi.

Katılımcı 3:

* *Ekran 2:* Yönergede yön tuşları kullanarak işlem yapılması belirtilmesine rağmen fare ile topu sürüklemeye çalıştı.

* *Ekran 3:* Kırmızı alana sürüklemekte zorluk çekti.

* *Ekran 4:* Açılır kutudan seçim yapacağını tam kavrayamadı. “Sürüm numarası ibresini yazınız” kısmı aklını karıştırdı.

* *Ekran 5:* Metni nereye yazacağı konusunda tereddüt yaşadı.

Katılımcı 4:

* *Ekran 2:* Katılımcı 3 gibi, yönergede yön tuşları kullanarak işlem yapılması söylenmesine rağmen fare ile topu sürüklemeye çalıştı.

* *Ekran 3:* Kırmızı alana sürükleme konusunda sıkıntı çekti. 2. denemesinde başardı.

* *Ekran 4:* “Sürüm numarasını siz yazın” yönergesi aklını karıştırdı.

Katılımcı 5:

* *Ekran 5:* Metni yazmaya aslında yazılacak metni tarif eden "Metin:" ile başladı. Bu durum metin içerisinde bulunan "en az" ibaresini yazmayı atlaması ve bu sebeple bir sonraki ekrana geçmesini sağlayacak butonun çıkmaması sebebiyle oldu.

Yapılan Düzenlemeler:

* *Ekran 2:* Yönergede "Aşağıda bulunan ok tuşları" ibaresi kalın ve kırmızı olarak düzenlendi.

* *Ekran 3:* Kırmızı alan biraz daha belirginleştirilip silik bir şekilde "bu alana sürükleyin" ibaresi eklendi ve her sürüklenen maddeden sonra bu kısmın aşağı doğru uzaması sağlandı.

* *Ekran 4:* Açılır kutu açılmadan önce silik bir şekilde "Buradan seçiniz" şeklinde bir ibare eklendi. “Sürüm numarasını siz yazın” ibaresi ekran yüklenince değil, katılımcıya "Sürüm numaranız bu mu?" diye sorulduktan sonra belirmesi sağlandı.

* *Ekran 5:* Kutucuğun içine yazmaya başlanınca silinen "Bu kısma yazınız" şeklinde bir yönerge koyuldu. Yönergeye "tırnak içerisinde bulunan metni" ibaresi eklenip "Metin:" ibaresi kaldırıldı.

* *Ekran 6:* "Süre bitiminde işlem yapmamış iseniz ekran bir sonrakine otomatik olarak atlayacaktır" ibaresi kırmızı renkli olarak eklendi.

Alınan uzman görüşleri ve sesli düşünme protokolü sonucu belirlenen değişiklikler web uygulaması üzerinde gerçekleştirilmiştir. Web uygulaması farklı ekran çözünürlüklerinde ve cihazlardan aynı şekilde kullanılabilirliği sağlanarak tasarlanmıştır. http://wizardbuilding.com/anket/ adresi üzerinden yayınlanan web uygulamasına ait ekran görüntüleri ilgili ölçek maddesi ile birlikte EK 6’da sunulmuştur. Kullanılan ölçeklerde yer almamasına karşın kullanıcıların yazı yazma hızları ve oltalama olarak tabir edilen siber saldırılarda sıklıkla kullanılan, “URL yanıltması”, “hatalı yazım yönlendirmesi” gibi isimler altında incelenen (Typosquatting) veri ihlal yöntemi de çalışma kapsamına dâhil edilmiştir. Bu yöntemde URL içerisinde bulunan bazı harflerin benzer bir harfle değiştirilerek sahte bir web adresinin orijinali gibi görünmesini sağlayarak kullanıcının tuzak bir web adresine yönlendirilerek veri güvenliğinin ihlal edilmesine sebep olunmaktadır (Moore ve Edelman, 2010). Yöntem ile atak yapacak olan kimse popüler bir web sitesinin benzer bir örneğini alan adı olarak kaydettirir ve kullanıcının yazım yanlışı yaparak kendi sahte web sitesini ziyaret etmesini bekler (Tahir vd., 2018). West (2017) ise kullanıcının klavye kullanım dinamikleri ile web ortamında yapmış oldukları girdilerin birbiriyle kuvvetli bir ilişki olduğunu, istenilen

adrese doğru bir şekilde erişimlerinde etkisi olduğunu vurgulamıştır. Bu aşamadan sonra konu ile ilgili olarak "hatalı yazım yönlendirmesi" tanımlaması kullanılmıştır. Konu ile ilgili verinin toplanabilmesi için oluşturulan ekran görüntüsü EK 6'da verilmiştir.

Tasarımın Uygulanması

Veri toplama sürecinde planlandığı üzere, veri toplama işlemi hazırlanan www.wizardbuilding.com web sitesi üzerinden gerçekleştirilmiştir. Uygulamaya katılım çağrısı uygulama 1'e katılım sağlayan kullanıcıların vermiş oldukları eposta adreslerine web sitesi bağlantısı şu ileti gönderilerek yapılmıştır:

"Değerli Katılımcı,

Doktora tezim için hazırlamış olduğum "Bilişim Güvenliği ve Farkındalığı" anketine katılarak ilk aşamayı tamamlamama yardımcı olduğunuz için öncelikle çok teşekkür ederim. Ankete vermiş olduğunuz cevaplar doğrultusunda hazırlamış olduğum web sitesinin kullanılabilirliğinin değerlendirilmesi ve çalışmamın sonuçlanması için tekrar yardımınıza ihtiyaç duymaktayım. http://wizardbuilding.com/anket adresine erişim sağladıktan sonra bu e-posta adresini sisteme elle girerek sadece 5 dakikada tamamlayabileceksiniz. Daha önce belirtildiği gibi çekiliş bu değerlendirmenin nihayetlenmesi sonucunda yapılacaktır.

Katkılarınız için tekrar tekrar teşekkür ederim."

Verinin Toplanması ve Analizi

www.wizardbuilding.com web sitesi ile 2 ay süre zarfında veri toplanmaya devam edilmiştir. Uygulama-1 aşamasında çalışmaya katkı sağlayan ancak uygulama-2 aşamasına ilk 1 aylık süre zarfında katılım sağlamayan kullanıcılara hatırlatma epostası gönderilmiştir. 2 aylık süre soncunda 301 katılımcının her iki veri toplama aşamasına katkı sunduğu görülmüştür.

Bu aşamada;

- Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin demografik ve sosyo-demografik özellikleri arasında anlamlı bir ilişki var mıdır?

- Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin kişilik özellikleri arasında anlamlı bir fark var mıdır?
- Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin tehlike algıları, suça maruz kalma durumları, riskli davranış özellikleri ve korumacı davranış özellikleri arasında anlamlı bir fark var mıdır?
- Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin yazma hızları ve dikkatleri arasında anlamlı bir fark var mıdır? Sorularına yanıt aranmış ve analizler bu doğrultuda gerçekleştirilmiştir.

Bu aşamadaki analizler klasik istatistiki yöntemler kullanılarak gerçekleştirilmiş olup herhangi bir makine öğrenmesi algoritması kullanılmamıştır. Burada amaç ortaya konulmuş olan hipotezlerin onaylanması ve reddedilmesi durumlarını ortaya koymak ve bir sonraki uygulama sürecinde gerçekleştirilecek olan makine öğrenmesi algoritmasının işe koşulması sonrasında ortaya çıkan sonuçlarla birlikte değerlendirilmesinin sağlanmasıdır.

Bilgi Güvenliği Davranışları ile Demografik ve Sosyo-demografik Özellikler Arasındaki İlişki

Bu aşamada sıfır hipotezi H_0 kurularak kategorik değişkenler arasındaki ilişkileri araştırmak için Ki-Kare Bağımsızlık testi kullanılmış, güven aralığı %95 olarak analizler yapılmıştır. Her bir davranışa ait ilişki Tablo 52 üzerinde gösterilmiş olup, analiz tabloları EK 7'de verilmiştir. Gerçekleştirilen analizlere göre "H_0: Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin demografik ve sosyo-demografik özellikleri arasında anlamlı bir ilişki yoktur" için;

Tablo 53

Bilgi Güvenliği Davranışları ile Demografik ve Sosyo-demografik Özellikler Arasındaki İlişki

Davranış	Demografik ve Sosyo-demografik Değişkenler				
	Cinsiyet (H_0)	Eğitim Düzeyi (H_0)	Yaş Aralığı (H_0)	İKY (H_0)	GİKS (H_0)
Birden fazla elektronik posta adresi kullanırım	Reddedilmiştir.	Reddedilmiştir.	Kabul edilmiştir.	Reddedilmiştir.	Kabul edilmiştir.
Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim	Reddedilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.
Güvenlik duvarı, reklam önleyici vb. Programlar kullanırım	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.
Virüs temizleme, casus yazılım önleme vb. Programları kullanırım	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.
Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.
İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.	Reddedilmiştir.
Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.
Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.
Kurumsal e-posta adresimi günlük işlerde de kullanırım	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.
İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım	Kabul edilmiştir.	Reddedilmiştir.	Reddedilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.
İnternet ortamında gerektiği durumlarda özlük bilgilerimi (ad, soyad, doğum tarihi vb.) paylaşırım	Kabul edilmiştir.	Reddedilmiştir	Kabul edilmiştir.	Kabul edilmiştir.	Kabul edilmiştir.

Tablo 53 incelendiğinde bilgi güvenliğine yönelik olarak bireylerin söylem ve gerçek davranışları arasında sergilenen farkın, demografik ve sosyo-demografik özellikleri açısından genel olarak anlamlı bir fark oluşturmadığı görülmektedir.

Bilgi Güvenliği Davranışları ile Kişilik Özellikleri Arasındaki İlişki

Bu aşamada dört gruptan oluşan davranış durumları normal dağılım göstermediğinden ve gruplar homojen olmadığından analiz için parametrik olmayan testlerden Kruskal Wallis-H Testi, hangi grupların farklılık gösterdiğinin analizi için ise post hoc Tomhane's T2 testi %95 güven aralığında uygulanmıştır. Her bir davranışa ait ilişki analiz tabloları EK 8'de verilmiştir. Yapılan analizlere göre, "H_0: Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin kişilik özellikleri arasında anlamlı bir fark yoktur" için,

- "Birden fazla elektronik posta adresi kullanırım" davranışı için;
    - "Dışa dönüklük" kişilik özelliği için;
        - "Söyler ancak Yapmaz" ve "Söylemez ve Yapmaz" davranışları arasında 0,08 p değerinde ilişkinin varlığı görülmüş H_0 reddedilmiştir.

- "Güvenlik duvarı, reklam önleyici vb. programlar kullanırım" davranışı için;
    - Bir grubun 2'den az durumu olduğu için post hoc analizi yapılamamış ancak nevrotizm kişilik özeliği için 0.035 p değeri ile H_0 reddedilmiştir.

- "Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim" davranışı için;
    - "Uyumluluk" kişilik özelliği için;
        - "Söyler ve Yapar" ve "Söyler ancak Yapmaz" davranışları arasında 0,041 p değerinde ilişkinin varlığı görülmüş,
    - "Özdenetim" kişilik özelliği için;
        - "Söyler ve Yapar" ve "Söylemez ve Yapmaz" davranışları arasında 0,031 p değerinde ilişkinin varlığı görülmüş,
    - "Nevrotizm" kişilik özelliği için;

        - “Söyler ancak Yapmaz” ve “Söylemez ve Yapmaz” davranışları arasında 0,027 p değerinde ilişkinin varlığı görülmüş,
    - “Gelişime açıklık” kişilik özelliği için;
        - “Söyler ve Yapar” ve “Söylemez ve Yapmaz” davranışları arasında 0,037 p değerinde ilişkinin varlığı görülmüş,
    - “Dışa dönüklük” kişilik özelliği için;
        - “Söyler ancak Yapmaz” ve “Söylemez ve Yapmaz” davranışları arasında 0,048 p değerinde ilişkinin varlığı görülmüş,
        - “Söylemez ve Yapmaz” ve “Söylemez ancak Yapar” davranışları arasında 0,01 p değerinde ilişkinin varlığı görülmüş H_0 reddedilmiştir.

- “Virüs temizleme, casus yazılım önleme vb. Programları kullanırım” davranışı için;
    - H_0 kabul edilmiştir.

- “Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim” davranışı için;
    - H_0 kabul edilmiştir.

- “İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım” davranışı için;
    - “Nevrotizm” kişilik özelliği için;
        - “Söyler ancak Yapmaz” ve “Söylemez ve Yapmaz” davranışları arasında 0,05 p değerinde ilişkinin varlığı görülmüş,
        - “Söyler ve Yapar” ve “Söylemez ve Yapmaz” davranışları arasında 0,043 p değerinde ilişkinin varlığı görülmüş,
    - “Gelişime açıklık” kişilik özelliği için;
        - “Söyler ancak Yapar” ve “Söylemez ve Yapmaz” davranışları arasında 0,013 p değerinde ilişkinin varlığı görülmüş H_0 reddedilmiştir.

- ” Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim” davranışı için;
    - “Uyumluluk” kişilik özelliği için;

        - "Söyler ve Yapar" ve "Söyler ancak Yapmaz" davranışları arasında 0,029 p değerinde ilişkinin varlığı görülmüş,
        - "Söyler ancak Yapmaz" ve "Söylemez ve Yapmaz" davranışları arasında 0,013p değerinde ilişkinin varlığı görülmüş,
    - "Özdenetim" kişilik özelliği için;
        - "Söyler ancak Yapmaz" ve "Söylemez ve Yapmaz" davranışları arasında 0,033p değerinde ilişkinin varlığı görülmüş,
    - "Nevrotizm" kişilik özelliği için;
        - "Söyler ancak Yapmaz" ve "Söylemez ve Yapmaz" davranışları arasında 0,044 p değerinde ilişkinin varlığı görülmüş H_0 reddedilmiştir.

- "Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım" davranışı için;
    - H_0 kabul edilmiştir.

- "Kurumsal e-posta adresimi günlük işlerde de kullanırım" davranışı için;
    - "Özdenetim" kişilik özelliği için;
        - "Söyler ve Yapar" ve "Söylemez ve Yapmaz" davranışları arasında 0,000 p değerinde ilişkinin varlığı görülmüş,
        - "Söyler ancak Yapmaz" ve "Söylemez ve Yapmaz" davranışları arasında 0,003p değerinde ilişkinin varlığı görülmüş,
        - "Söyler ancak Yapmaz" ve "Söylemez ancak Yapar" davranışları arasında 0,000 p değerinde ilişkinin varlığı görülmüş,
    - "Gelişime açıklık" kişilik özelliği için;
        - "Söyler ve Yapar" ve "Söylemez ve Yapmaz" davranışları arasında 0,001 p değerinde ilişkinin varlığı görülmüş,
        - "Söyler ancak Yapmaz" ve "Söylemez ve Yapmaz" davranışları arasında 0,025 p değerinde ilişkinin varlığı görülmüş,
        - "Söylemez ancak Yapar" ve "Söylemez ve Yapmaz" davranışları arasında 0,029 p değerinde ilişkinin varlığı görülmüş,
    - "Dışa dönüklük" kişilik özelliği için;

        - "Söyler ve Yapar" ve "Söylemez ancak Yapar" davranışları arasında 0,039 p değerinde ilişkinin varlığı görülmüş,
        - "Söyler ve Yapar" ve "Söylemez ve Yapmaz" davranışları arasında 0,037 p değerinde ilişkinin varlığı görülmüş H_0 reddedilmiştir.

- "İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım" davranışı için
    - H_0 kabul edilmiştir.

- "İnternet ortamında gerektiği durumlarda özlük bilgilerimi (ad, soyad, doğum tarihi vb.) paylaşırım" davranışı için;
    - "Özdenetim" kişilik özelliği için;
        - "Söyler ve Yapar" ve "Söylemez ancak Yapar" davranışları arasında 0,001 p değerinde ilişkinin varlığı görülmüş,
    - "Nevrotizm" kişilik özelliği için;
        - "Söyler ve Yapar" ve "Söylemez ancak Yapar" davranışları arasında 0,001 p değerinde ilişkinin varlığı görülmüş H_0 reddedilmiştir.

Analizler incelendiğinde bilgi güvenliğine yönelik olarak bireylerin söylem ve gerçek davranışları arasında sergilenen farkın, kişilik özellikleri açısından genel olarak anlamlı bir fark oluşturduğu görülmektedir.

Bilgi Güvenliği Davranışları ile Tehlike Algısı, Suça Maruziyet Durumu, Riskli ve Korumacı Davranışları Arasındaki İlişki

Bu aşamada dört gruptan oluşan davranış durumları normal dağılım gösteren ve grupları homojen olan seçeneklerin analizi için tek yönlü MANOVA ve hangi grupların farklılık gösterdiğinin analizi için ise post hoc Tukey testi; normal dağılım göstermeyen ve grupları homojen olmayan seçeneklerin analizi için parametrik olmayan testlerden Kruskal Wallis-H Testi, hangi grupların farklılık gösterdiğinin analizi için ise post hoc Tomhane's T2 testi %95 güven aralığında uygulanmıştır. Her bir davranışa ait ilişki analiz tabloları EK 9'da verilmiştir. Yapılan analizlere göre, "H0: Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin

tehlike algıları, suça maruz kalma durumları, riskli davranış özellikleri ve korumacı davranış özellikleri arasında anlamlı bir fark yoktur" için;

- "Birden fazla elektronik posta adresi kullanırım" davranışı için;
    - "Riskli davranış puanı" için;
        - "Söyler ve Yapar" ve "Söylemez ancak Yapar" davranışları arasında 0,001 p değerinde ilişkinin varlığı görülmüş,
        - "Söyler ve Yapar" ve "Söylemez ve Yapmaz" davranışları arasında 0,002 p değerinde ilişkinin varlığı görülmüş,
        - "Söyler ancak Yapmaz" ve "Söylemez ancak Yapar" davranışları arasında 0,030 p değerinde ilişkinin varlığı görülmüş,
        - "Söyler ancak Yapmaz" ve "Söylemez ve Yapmaz" davranışları arasında 0,047 p değerinde ilişkinin varlığı görülmüş H_0 reddedilmiştir.

- "Güvenlik duvarı, reklam önleyici vb. programlar kullanırım" davranışı için;
    - "Riskli davranış puanı" için;
        - "Söyler ve Yapar" ve "Söylemez ve Yapmaz" davranışları arasında 0,025 p değerinde ilişkinin varlığı görülmüş,
        - "Söyler ancak Yapmaz" ve "Söylemez ve Yapmaz" davranışları arasında 0,000 p değerinde ilişkinin varlığı görülmüş H_0 reddedilmiştir.

- "Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim" davranışı için;
    - "Korumacı davranış puanı" için
        - "Söyler ve Yapar" ve "Söylemez ancak Yapar" davranışları arasında 0,002 p değerinde ilişkinin varlığı görülmüş,
        - "Söyler ve Yapar" ve "Söylemez ve Yapmaz" davranışları arasında 0,017 p değerinde ilişkinin varlığı görülmüş,
        - "Söyler ancak Yapmaz" ve "Söylemez ancak Yapar" davranışları arasında 0,016 p değerinde ilişkinin varlığı görülmüş H_0 reddedilmiştir.

- "Virüs temizleme, casus yazılım önleme vb. Programları kullanırım" davranışı için;

- “Korumacı davranış puanı” için
  - “Söyler ve Yapar” ve “Söylemez ve Yapmaz” davranışları arasında 0,046 p değerinde ilişkinin varlığı görülmüş H_0 reddedilmiştir.

- “Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim” davranışı için;
  - Bir grubun 2’den az durumu olduğu için post hoc analizi yapılamamış ancak H0 reddedilmiştir.

- “İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım” davranışı için;
  - “Korumacı davranış puanı” için;
    - “Söyler ve Yapar” ve “Söylemez ve Yapmaz” davranışları arasında 0,001 p değerinde ilişkinin varlığı görülmüş,
    - “Söylemez ve Yapmaz” ve “Söyler ancak Yapmaz” davranışları arasında 0,00 p değerinde ilişkinin varlığı görülmüş H_0 reddedilmiştir.

- ” Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim” davranışı için;
  - “Korumacı davranış puanı” için;
    - “Söyler ve Yapar” ve “Söylemez ancak Yapar” davranışları arasında 0,000 p değerinde ilişkinin varlığı görülmüş,
    - “Söyler ve Yapar” ve “Söylemez ve Yapmaz” davranışları arasında 0,000 p değerinde ilişkinin varlığı görülmüş,
    - “Söyler ancak Yapmaz” ve “Söylemez ancak Yapar” davranışları arasında 0,00 p değerinde ilişkinin varlığı görülmüş,
    - “Söyler ancak Yapmaz” ve “Söylemez ve Yapmaz” davranışları arasında 0,00 p değerinde ilişkinin varlığı görülmüş,
  - “Tehlike algısı puanı” için;
    - “Söyler ve Yapar” ve “Söylemez ancak Yapar” davranışları arasında 0,012 p değerinde ilişkinin varlığı görülmüş,
    - “Söyler ancak Yapmaz” ve “Söylemez ancak Yapar” davranışları arasında 0,006 p değerinde ilişkinin varlığı görülmüş H_0 reddedilmiştir.

- “Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım” davranışı için;
    - “Korumacı davranış puanı” için;
        - “Söyler ve Yapar” ve “Söylemez ancak Yapar” davranışları arasında 0,000 p değerinde ilişkinin varlığı görülmüş,
        - “Söyler ve Yapar” ve “Söylemez ve Yapmaz” davranışları arasında 0,000 p değerinde ilişkinin varlığı görülmüş,
        - “Söyler ancak Yapmaz” ve “Söylemez ve Yapmaz” davranışları arasında 0,036 p değerinde ilişkinin varlığı görülmüş H_0 reddedilmiştir.
- “Kurumsal e-posta adresimi günlük işlerde de kullanırım” davranışı için;
    - “Korumacı davranış puanı” için;
        - “Söyler ve Yapar” ve “Söylemez ancak Yapar” davranışları arasında 0,000 p değerinde ilişkinin varlığı görülmüş,
    - “Tehlike algısı puanı” için
        - “Söyler ve Yapar” ve “Söylemez ancak Yapar” davranışları arasında 0,015 p değerinde ilişkinin varlığı görülmüş H_0 reddedilmiştir.
- “İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım” davranışı için;
    - Bir grubun 2’den az durumu olduğu için post hoc analizi yapılamamış ancak H0 reddedilmiştir.
- “İnternet ortamında gerektiği durumlarda özlük bilgilerimi (ad, soyad, doğum tarihi vb.) paylaşırım” davranışı için;
    - “Riskli davranış puanı” için;
        - “Söyler ve Yapar” ve “Söylemez ancak Yapar” davranışları arasında 0,000 p değerinde ilişkinin varlığı görülmüş,
        - “Söyler ve Yapar” ve “Söylemez ve Yapmaz” davranışları arasında 0,000 p değerinde ilişkinin varlığı görülmüş,
        - “Söyler ancak Yapmaz” ve “Söylemez ve Yapmaz” davranışları arasında 0,036 p değerinde ilişkinin varlığı görülmüş H_0 reddedilmiştir.

Analizler incelendiğinde bilgi güvenliğine yönelik olarak bireylerin söylem ve gerçek davranışları arasında sergilenen farkın, tehlike algısı, suça maruziyet durumu, riskli ve korumacı davranışları açısından genel olarak anlamlı bir fark oluşturduğu görülmektedir.

Bilgi Güvenliği Davranışları ile Bireylerin Klavye Kullanım Hızı ve Dikkat Değişkenleri Arasındaki İlişki

Bu aşamada dört gruptan oluşan davranış durumları ile sürekli değişken olan yazma hızları arasındaki ilişki analiz edilirken; normal dağılım gösteren ve gruplar homojen olan seçeneklerin analizi için tek yönlü ANOVA ve hangi grupların farklılık gösterdiğinin analizi için ise post hoc Tukey testi; normal dağılım göstermeyen ve grupları homojen olmayan seçeneklerin analizi parametrik olmayan testlerden Kruskal Wallis-H Testi, hangi grupların farklılık gösterdiğinin analizi için ise post hoc Tomhane's T2 testi %95 güven aralığında uygulanmıştır. Kategorik değişkenler arasındaki ilişkileri araştırmak için Ki-Kare Bağımsızlık testi kullanılmış, güven aralığı %95 olarak analizler yapılmıştır. Her bir davranışa ait ilişki Tablo 54 üzerinde gösterilmiş olup, analiz tabloları EK 10'da verilmiştir. Gerçekleştirilen analizlere göre "H_0: Bilgi güvenliği konusunda farklı davranışlar sergileyen kişilerin yazma hızları ve dikkatleri arasında anlamlı bir fark yoktur**.**" için;

Tablo 54

Bilgi Güvenliği Davranışları ile Hatalı Yazım Yönlendirmesi Arasındaki İlişki

Davranış	Hatalı Yazım Yönlendirmesi Değişkenler	
	Yazma Hızı (*H0*)	Dikkat Durumu (*H0*)
Birden fazla elektronik posta adresi kullanırım	Reddedilmiştir.	Kabul edilmiştir.
Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim	Kabul edilmiştir.	Kabul edilmiştir.
Güvenlik duvarı, reklam önleyici vb. Programlar kullanırım	Kabul edilmiştir.	Kabul edilmiştir.
Virüs temizleme, casus yazılım önleme vb. Programları kullanırım	Kabul edilmiştir.	Reddedilmiştir.
Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim	Kabul edilmiştir.	Kabul edilmiştir.
İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım	Kabul edilmiştir.	Kabul edilmiştir.
Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim	Kabul edilmiştir.	Kabul edilmiştir.
Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım	Kabul edilmiştir.	Kabul edilmiştir.
Kurumsal e-posta adresimi günlük işlerde de kullanırım	Kabul edilmiştir.	Reddedilmiştir.
İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım	Kabul edilmiştir.	Kabul edilmiştir.
İnternet ortamında gerektiği durumlarda özlük bilgilerimi (ad, soyad, doğum tarihi vb.) paylaşırım	Kabul edilmiştir.	Kabul edilmiştir.

Analizler incelendiğinde bilgi güvenliğine yönelik olarak bireylerin söylem ve gerçek davranışları arasında sergilenen farkın, hatalı yazım yönlendirmesi değişkenleri açısından genel olarak anlamlı bir fark oluşturmadığı görülmektedir.

Karar Verme ve Tasarım Planı

Klasik istatistiki yöntemler kullanılarak yapılan analizler sonucu değişkenler arasındaki ilişkiler ortaya konmuştur. Farklı değişkenler için davranışlar konusunda anlamlı farklar gözlenirken, bazı değişken grupları için anlamlı farklar oluşmadığı ortaya koyulmuştur. Uygulama-3 aşamasında uygulanacak veri madenciliği işlemleri için öznitelik seçiminde bu aşamada yapılan analizlerin sonuçları da dâhil edilmiştir.

Tasarımın Düzeltilmesi / Yenilenmesi

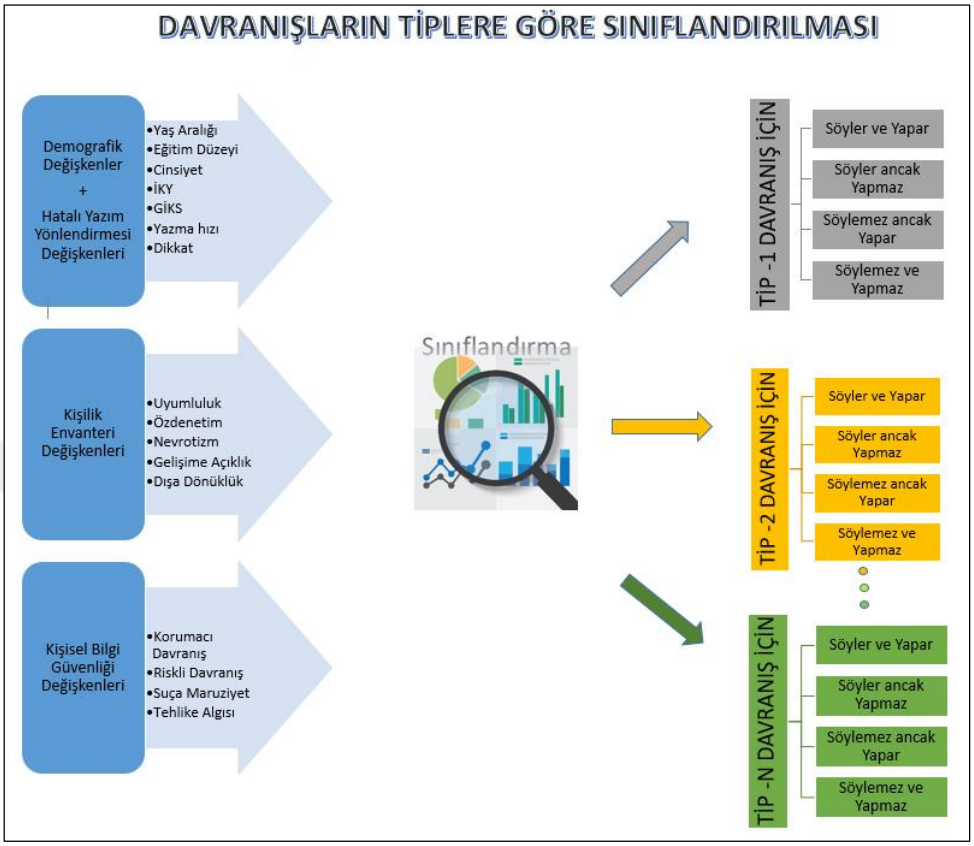
Uygulama-2 veri toplama sürecinde belirtilen tüm sorulara toplanan ve analiz edilen veriler ışığında cevap verilmiştir. Bu sebeple tasarımın düzeltilmesine veya yenilenmesine ihtiyaç duyulmamış, uygulamanın üçüncü aşamasına geçilmiştir.

Üçüncü Döngü Geliştirme Raporu

Bu aşama, ″bilgi güvenliği eğitimine yönelik olarak geliştirilen uyarlanabilir çevrimiçi öğrenme ortamı nasıl olmalıdır, “uyarlama nasıl gerçekleştirilmelidir?” ve “öğrenen modellemesi nasıl yapılmalıdır?” araştırma sorularına cevap verilmiştir. Tasarım tabanlı araştırma yönteminin döngüsel adımlarını takip etmektedir.

Veri Toplama Süreci

Bu aşamada veri madenciliği işlemlerini gerçekleştirmek Uygulama-1 ve Uygulama-2 aşamasında toplanan veriler kullanılmıştır. Var olan tasarım prensipleri ilkeleri ve kuramlar ile tasarımın yapılması aşamasında belirtilen akış şemasına uygun olarak Şekil 18’de görselleştirilen tasarımın uygulanması için bilgi güvenliğine yönelik davranışların Şekil 23 üzerinde gösterildiği şekilde sınıflandırılması tasarlanmıştır.



Şekil 23. Davranışların tiplere göre sınıflandırılması

Bilgi güvenliği konusunda var olan çevrimiçi öğrenme ortamlarının var olan tüm içeriği katılımcıya sunuyor olması ve ayrıca bilgi güvenliğine yönelik yapılan analizlerin kişinin kendi beyanına dayalı olarak adlandırılan ve katılımcıdan cevaplar alan ölçekler yardımıyla yapılıyor olması hazırlanan bu çalışmanın ana problem durumunu ortaya koymaktadır. Gerçekleştirilen analizler sonucunda demografik, bilgi güvenliğini bozmaya yönelik, kişilik ve kişisel bilgi güvenliği değişkenleri işe koşularak bir kullanıcının davranışlarının kendi görüşleri de kapsam içerisinde tutularak sınıflandırılması planlanmıştır. Bu sebeple riskli davranış ölçeği, korumacı davranış ölçeği, suça maruziyet ölçeği ve tehlike algısı ölçeği içerisinde yer alan ve davranış olarak ölçülebilecek olan seçenekler belirlenmiş ve önceki uygulama aşamalarında analizleri yapılmıştır. Şekil-23'te belirtilen tasarım ile ölçeklerde bulunan ve sadece davranış olarak ölçülebilecek seçenekler bağlamında tahmin edilebilecek davranışların yanı sıra; yapılan analizlere konu edilememiş ancak bilgi güvenliği konusunda çevrimiçi eğitime dâhil edilebilecek konuların da belirlenebilmesi için "TİP davranışlar" şeklinde bir sınıflandırma yapma işlemi gerçekleştirilmeye çalışılmıştır. Burada amaç; kullanıcının x davranışı için

(Örneğin "Birden fazla elektronik posta adresi kullanırım") ilgili değişkenlerle analizi sonucunda göstermesi tahmin edilen aksiyonun ("Söyler ve Yapar", "Söyler ancak Yapmaz", "Söylemez ve Yapmaz", "Söylemez ancak Yapar"); x davranışı ile aynı sınıfta olduğu değerlendirilen ancak tez kapsamında davranış olarak ölçülemeyen bir y davranışının (Örneğin; "Elektronik/mobil imza kullanırım") benzer şekilde sonuçlanacağından bahisle çevrimiçi eğitime dâhil edilmesinin sağlanmasıdır.

Bu kapsamda alan yazın taraması yapılmış ve bilgi güvenliği tehdit sınıflandırması çalışmaları incelenmiştir. İncelenen sınıflandırmalar ve kriterleri aşağıda sunulmuştur.

1- Gerić ve Hutinski (2007) tarafından yapılan sınıflandırma ve kriterleri;
    a. Tehdit alanı
        i. Fiziksel
        ii. Kişisel
        iii. İletişim ve Veri
        iv. Operasyonel
    b. Tehdit kaynağı
        i. İçeriden
        ii. Dışarıdan
    c. Tehdit sıklığı

2- Ruf vd. (2008) tarafından yapılan sınıflandırma ve kriterleri:
    a. Tehdidin motivasyonu
        i. Kazara
        ii. Niyetli
    b. Tehdidin kaynağı
        i. İçeriden
        ii. Dışarıdan
    c. Tehdidin ajanı
        i. İnsan
        ii. Teknolojik

3- Jouini, Rabai ve Aissa (2014) tarafından yapılan sınıflandırma ve kriterleri:
    a. Tehdidin kaynağı
        i. İçeriden
        ii. Dışarıdan
    b. Tehdit ajanı
        i. İnsan
        ii. Çevre
        iii. Teknolojik
    c. Tehdit motivasyonu
        i. Şüpheli
        ii. Şüpheli olmayan
    d. Tehdit niyeti
        i. Niyetli
        ii. Kazara
    e. Tehdit etkisi
        i. Bilginin yok edilmesi
        ii. Bilginin bozulması
        iii. Bilginin çalınması
        iv. Bilginin ifşası
        v. Bilginin kullanımının engellenmesi
        vi. Bilginin illegal olarak kullanılması
4- Keser ve Güldüren (2015) tarafından yapılan bilgi güvenliği farkındalığı kategori, gösterge ve madde sayıları
    a. Genel güvenlik (34 madde)
    b. Saldırı ve tehditler (21 madde)
    c. E-posta ve iletişim (8 madde)
    d. Mobil cihazlar (8 madde)
    e. Mahremiyet (8 Madde)
    f. Güvenli Gezinme (6 madde)
    g. Yazılım ve Uygulamalar (5 madde)

5- Alhabeeb, Almuhabied, Le ve Srinivasan (2010) tarafından yapılan sınıflandırma kriterleri:

a. Kayıp (Davranış olumlu şekilde gösterilmediği zaman yaşanabilecek kaybın boyutu)
    i. Düşük
    ii. Yüksek
b. Kritiklik (Davranış olumlu şekilde gösterilmediği zaman etkilenecek sistemin kritiklik boyutu)
    i. Düşük
    ii. Yüksek
c. Önceki Bilgi (Davranış sonucu kendi başına zarara uğratacak değil ancak zarara uğratacak bir durum için dayanak oluşturabilecek boyut)
    i. Düşük
    ii. Yüksek

Bu çalışma kapsamında ölçülemeyecek olan davranışların sınıflandırılması için Alhabeeb vd. (2010) tarafından yapılan çalışma temel alınmıştır. Bunun sebebi ise çalışma kapsamında kullanıcıların davranış biçimlerini etkilediği düşünülen değişkenlerle sınıflandırma kriterlerin örtüşmesidir. Bu sebeple EK 11'de gösterilen uzman görüş formu bilgi güvenliği alanında gerek akademik düzeyde, gerek suçla mücadelesinde gerekse de bu alanda yargı makamlarına bilirkişi olarak hizmet sunan uzmanlara gönderilerek ölçek kapsamındaki davranışların sınıflandırılması istenmiştir.

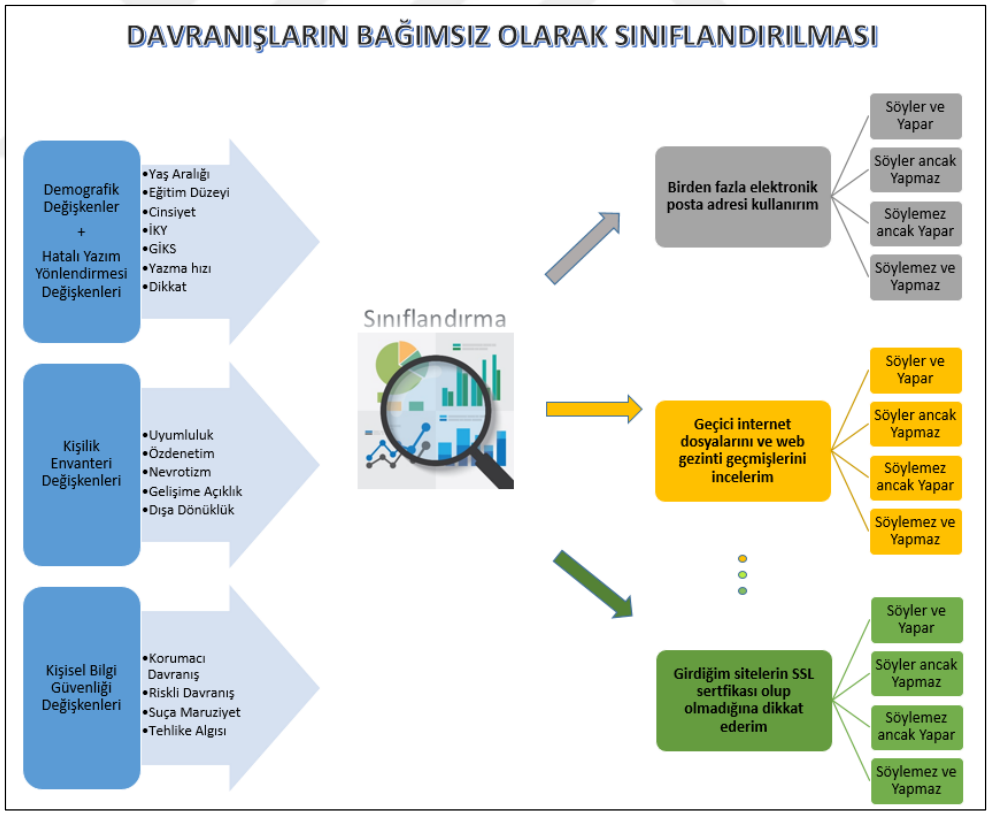
Tablo 55

Davranış Sınıflandırması için Alınan Uzman Görüşleri

DAVRANIŞLAR	U1	U2	U3	U4	U5	U6	U7	U8	U9	U10	U11	U12	U13
Birden fazla elektronik posta adresi kullanırım*	2	2	8	6	7	8	1	1	8	1	8	8	1
Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim*	3	8	4	8	6	2	2	3	6	2	8	8	2
Güvenlik duvarı, reklam önleyici vb. Programlar kullanırım*	8	8	8	8	6	4	8	8	6	8	8	5	5
Virüs temizleme, casus yazılım önleme vb. Programları kullanırım*	8	6	8	8	6	2	8	8	8	8	5	8	8
İçerik filtreleme programları kullanırım	1	1	3	1	1	1	1	1	6	8	4	1	8
e-posta filtreleme yazılımları kullanırım	1	2	3	2	6	1	1	5	6	7	1	8	4
İzleme yazılımları kullanarak internet üzerinde yapılan etkinlikler hakkında bilgi sahibi olurum	1	2	1	1	3	1	2	4	6	1	1	5	5
Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim*	2	2	1	1	1	1	1	4	-	1	8	5	1
Herkesin kullanımına açık bir bilgisayardan ayrılmadan önce geçici internet dosyalarını ve web gezinti geçmişlerini silerim	6	8	2	7	8	8	3	2	1	3	8	5	8
Dosyalarımı şifrelerim	7	2	6	8	8	8	8	7	7	5	5	8	3
İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım*	8	8	8	8	8	8	8	7	8	8	8	6	8
Elektronik/mobil imza kullanırım	4	2	6	1	8	4	1	5	8	7	8	8	1
İnternet sitelerine girerken genellikle sık kullanılanlar listesini kullanırım	1	1	1	1	3	1	4	1		1	8	1	1
Bilgisayarım şifre ile açılır	8	8	8	7	8	4	5	7	8	8	8	8	1
Bilgisayarımda otomatik kullan özelliğini kapatırım	4	3	1	1	2	2	8	7	-	8	1	5	1
Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim*	8	8	2	2	6	4	4	5	1	7	1	8	4
Parolalarımı sık sık değiştiririm	8	6	8	7	8	8	5	7	1	8	5	7	2
Kablosuz modem şifremi değiştiririm	8	6	3	2	6	4	2	5	1	4	1	8	3
Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım*	2	2	2	1	1	4	1	5	8	2	8	2	8
Kullandığım programların güncellemelerini düzenli olarak yaparım	4	4	3	4	2	2	4	7	8	8	8	2	7
Kurumsal e-posta adresimi günlük işlerde de kullanırım*	2	6	6	2	7	8	3	1	4	1	8	4	4
İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım*	1	2	6	4	2	8	4	5	1	1	5	6	1
İnternet ortamında gerektiği durumlarda özlük bilgilerimi (ad, soyad, doğum tarihi vb.) paylaşırım*	2	8	6	8	2	8	8	5	1	1	3	6	8

Bilgi güvenliği alanında çalışan 4 bilgisayar mühendisi, 2 akademisyen, 3 bilirkişi, 4 suç araştırma ve soruşturmacısı toplam 13 uzman katılımıyla gerçekleştirilen sonuç Tablo 55'te gösterilmiştir. (*) işaretli olan satırlar tez kapsamında ölçülen davranışları göstermektedir.

Alınan uzman görüşleri sonrasında, uzmanların bilgi güvenliğine yönelik davranışları sınıflandırmada tüm maddeler genelinde ortak bir paydada buluşamadıkları ancak bazı maddeler üzerinde hem fikir olabildikleri gözlemlenmiştir. Bu sebeple belirtilen uzman görüşleri gerçekleştirilecek olan makine öğrenmesi uygulamasının yorumlanması özelinde kullanılmış olup, algoritmanın işe koşulmasında davranışların bağımsız olarak kullanılmasına karar verilmiştir. Bu sebeple çalışma kapsamında makine öğrenmesi işlemi aşağıda verilen şemaya (Şekil 24) uygun olarak gerçekleştirilmiştir.



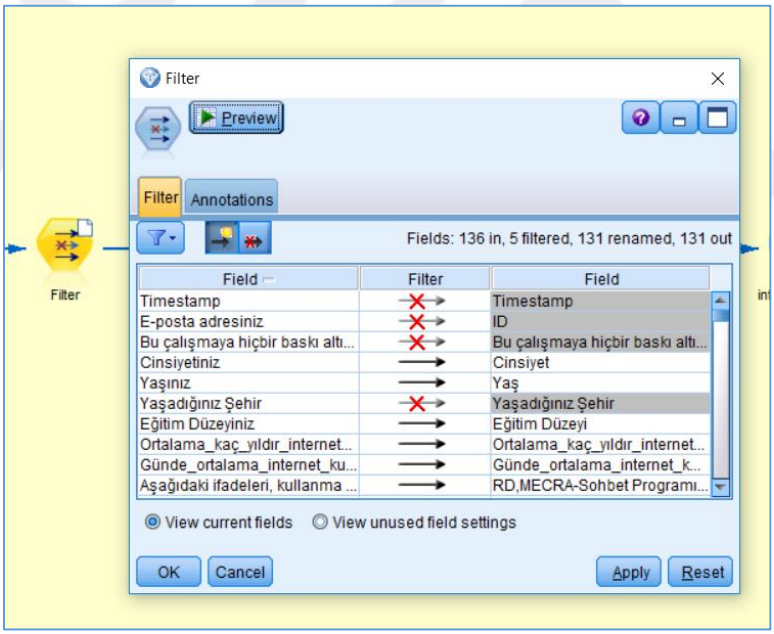
Şekil 24. Davranışların bağımsız olarak sınıflandırılması

Tasarımın Uygulanması

Veri madenciliği işlemleri birbiri ile bağımlı işlemlerden meydana gelmektedir. Yapılan tasarımın uygulanmasında belirtilen adımlar takip edilmiş olup aşağıda açıklanmıştır.

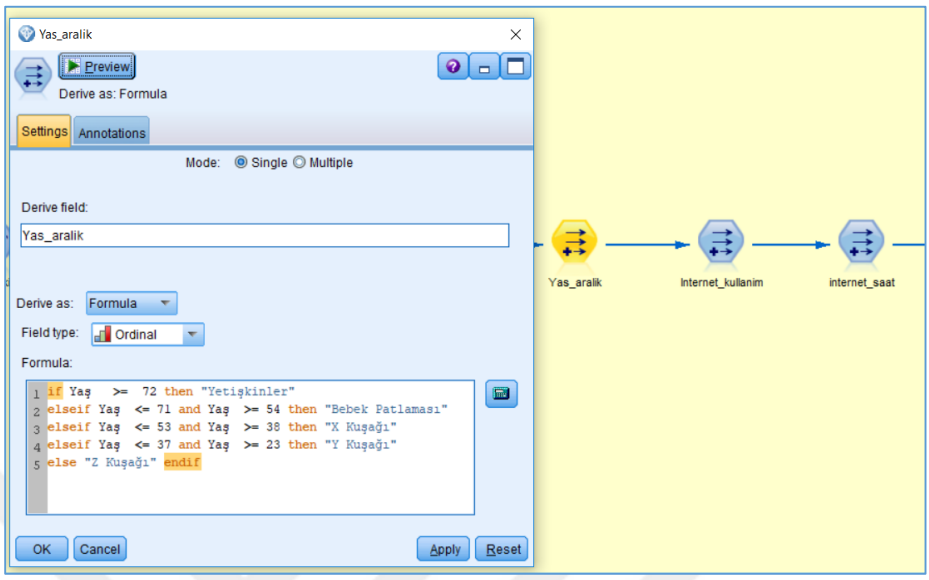
Veriler Üzerinde Yapılan Temizleme ve Dönüştürme İşlemleri

Bu çalışma kapsamında toplanan veriler daha önce de bahsedildiği gibi iki aşamada gerçekleştirilmiştir. Bu sebeple modelleme aşamasından önce yapılan işlemler her bir veri seti için ayrı ayrı gerçekleştirilmiştir. Öncelikli olarak virgülle ayrılmış değerler (comma seperated values, .csv) dosya formatında sisteme dâhil edilen, uygulama-1 aşamasında toplanan veriler üzerinde analize dâhil edilmeyecek olan değişkenler çıkarılmıştır (Şekil 25).



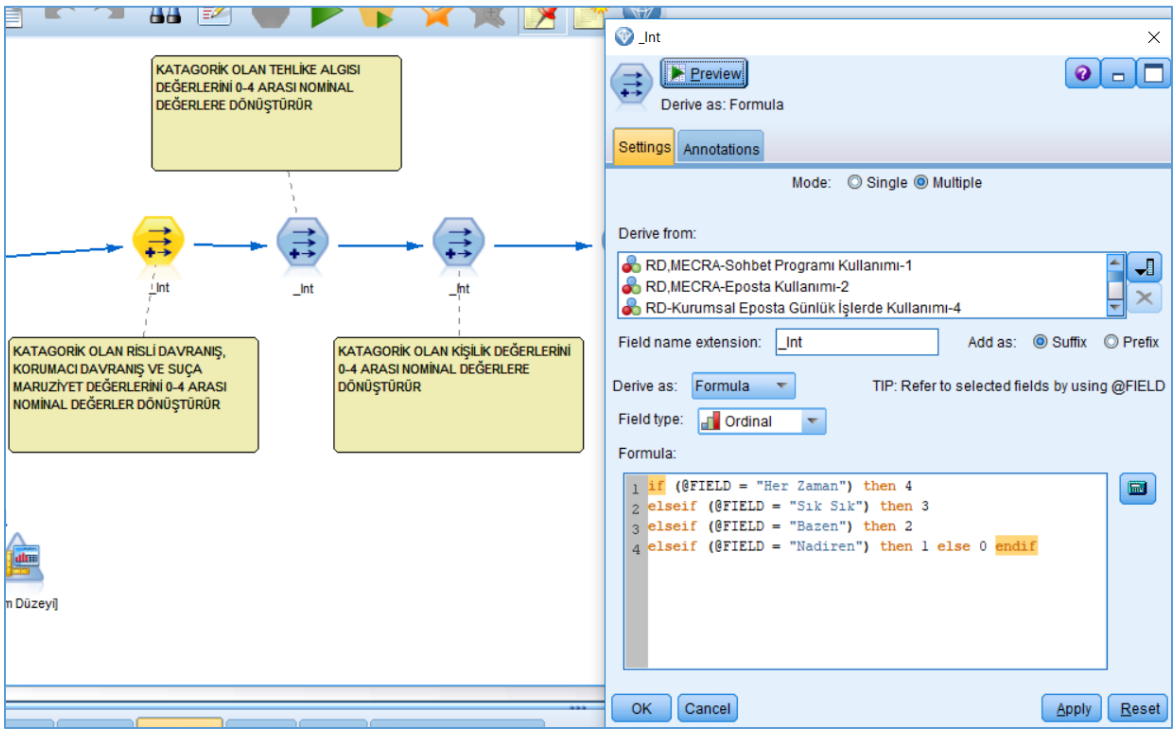
Şekil 25. Kullanılmayacak değişkenlerin filtrelenmesi

Bir sonraki aşamada kullanıcılardan sürekli değişken olarak alınan ve modelleme işlemlerinde kullanılacak olan "yaş aralığı", "internet kullanım yılı" ve "günlük internet kullanımı" değişkenleri alan yazına uygun bir şekilde kategorik değerlerine dönüştürülmüştür (Şekil 26).



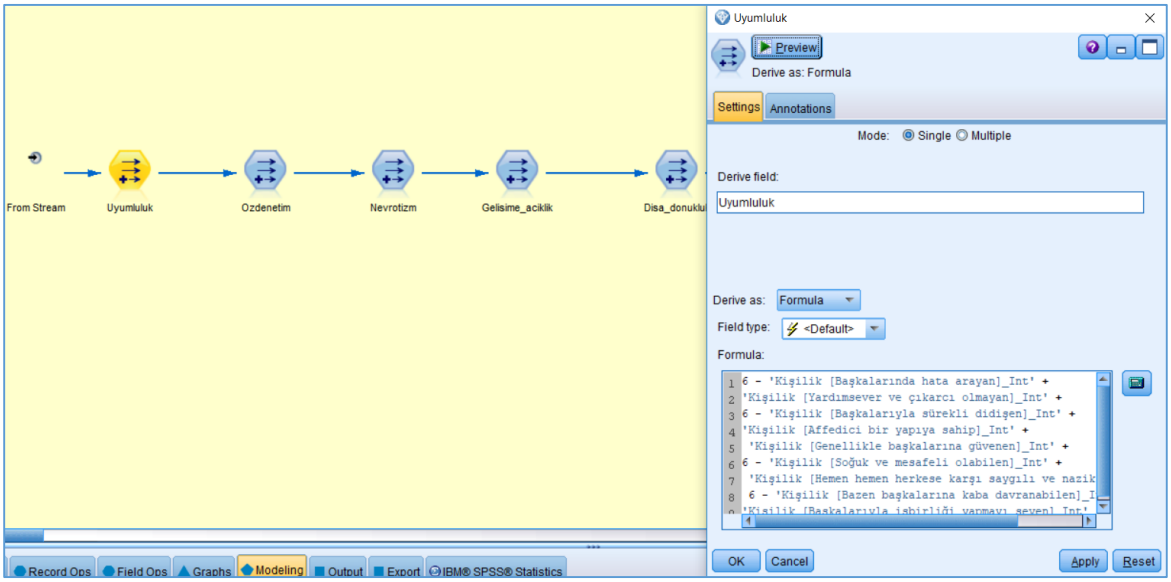
Şekil 26. Demografik sürekli verilerin kategorik değerlere dönüştürülmesi

Bir sonraki aşamada katılımcılardan kategorik olarak alınan "kişilik ölçeği" ve "kişisel bilgi güvenliği" verileri analizde işlemlerini kolaylaştırmak için miktar olarak ölçülemeyen kategorik bir veri çeşidi olan nominal değerlere dönüştürülmüştür (Şekil 27).



Şekil 27. Kategorik verilerin nominal değerlere dönüştürülmesi

Bir sonraki aşamada ölçeklerine asıllarına bağlı kalarak ve literatürde bulunun çalışmalara uygun olmasını sağlamak için "kişilik ölçeği" ve "kişisel bilgi güvenliği" ölçeklerinden elde edilen puanlar (Uyumluluk, Özdenetim, Nevrotizm, Gelişime Açıklık, Dışa Dönüklük, Korumacı Davranış, Riskli Davranış, Suça Maruziyet, Tehlike Algısı Puanları) dönüştürülen nominal değerler üzerinden elde edilmiştir (Şekil 28).

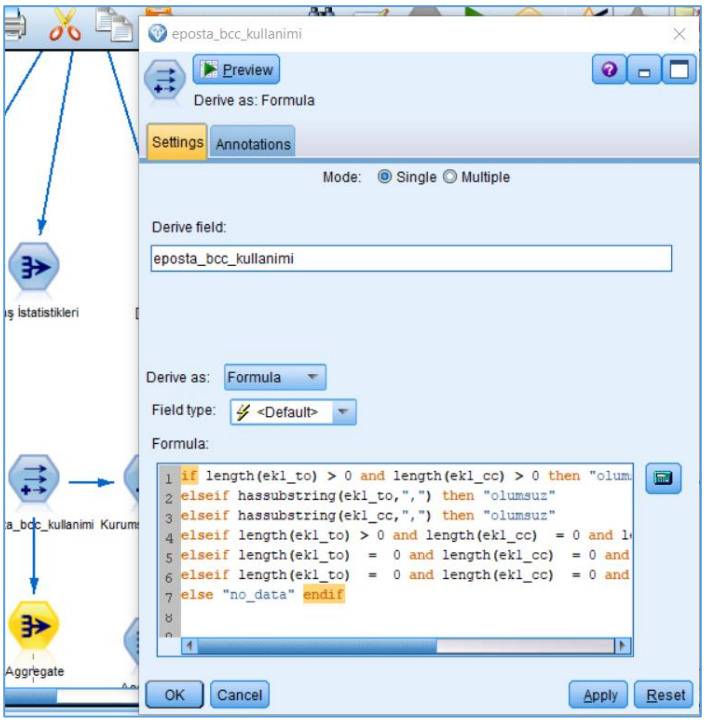


Şekil 28. Ölçek puanlarının hesaplanması

Sonraki aşamada csv formatında sisteme dâhil edilen veri toplama ikinci aşamasında elde edilen veriler sisteme dâhil edilmiştir. Bu aşamada toplanan veriler belirli bir düzen içerisinde toplanamamıştır. Bunun sebebi ise veri toplama ikinci aşamasının katılımcıların uygulama-2 aşamasında tanıtılan web uygulaması üzerindeki işlemleri sonucunda oluşmasıdır. Web uygulamasında ölçülecek davranış için katılımcının sıkılarak işlemi yarıda kesmesini engellemek için zorunlu olmayan alanlar bulunmaktadır. Bu sebeple analize dâhil edilecek her bir davranış için temizleme işlemi uygulanmıştır. Örnek olarak "Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım" davranışı için EK 6'da görselleştirilen web uygulaması sayfası kullanılmıştır. Belirtilen ekranda görülebileceği gibi katılımcı bu aşamayı hiçbir işlem yapmadan bir sonraki sayfaya geçebilmektedir. Aynı zamanda iletiyi sadece bir kişiye gönderen ve BCC kullanımının ölçülemediği örnekler de mevcuttur. Yapılan işleme ait temizleme kodu aşağıda sunulmuş olup Şekil 29'da görülen benzeri işlemler diğer davranışlar için de gerçekleştirilmiştir.

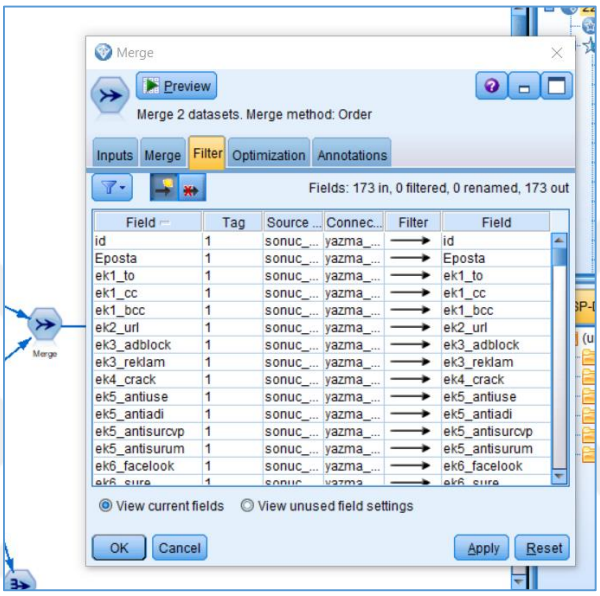
SPSS Modeler “derive” modülü üzerinde yapılan kodlama:

```
if length(ek1_to) > 0 and length(ek1_cc) > 0 then "olumsuz"
        elseif hassubstring(ek1_to,",") then "olumsuz"
        elseif hassubstring(ek1_cc,",") then "olumsuz"
        elseif length(ek1_to) > 0 and length(ek1_cc)  = 0 and length(ek1_bcc) > 0 then "olumlu"
        elseif length(ek1_to)  =  0 and length(ek1_cc)  = 0 and length(ek1_bcc) > 0 then "olumlu"
        elseif length(ek1_to)  =  0 and length(ek1_cc)  = 0 and hassubstring(ek1_bcc,",") then "olumlu"
  else "no_data"
  endif
```



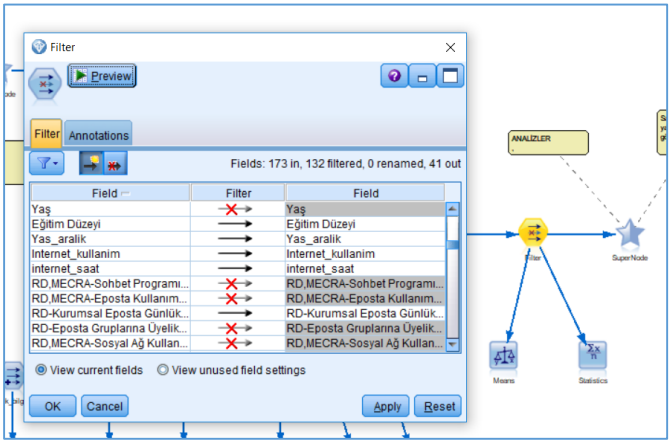
Şekil 29. Web uygulamasından alınan verilerin temizlenmesi işlemi

Bir sonraki aşamada ise veri toplama birinci ve ikinci aşamasında alınan ve temizleme işlemine tabi tutulan verilerin, her iki veri setinin de ortak değeri olan ve katılımcılar tarafından iki veri toplama aşamasında da ortak olarak sağlanmasına zorlanılan e-posta adresleri üzerinden birleştirilmesi işlemi uygulanmıştır (Şekil 30).



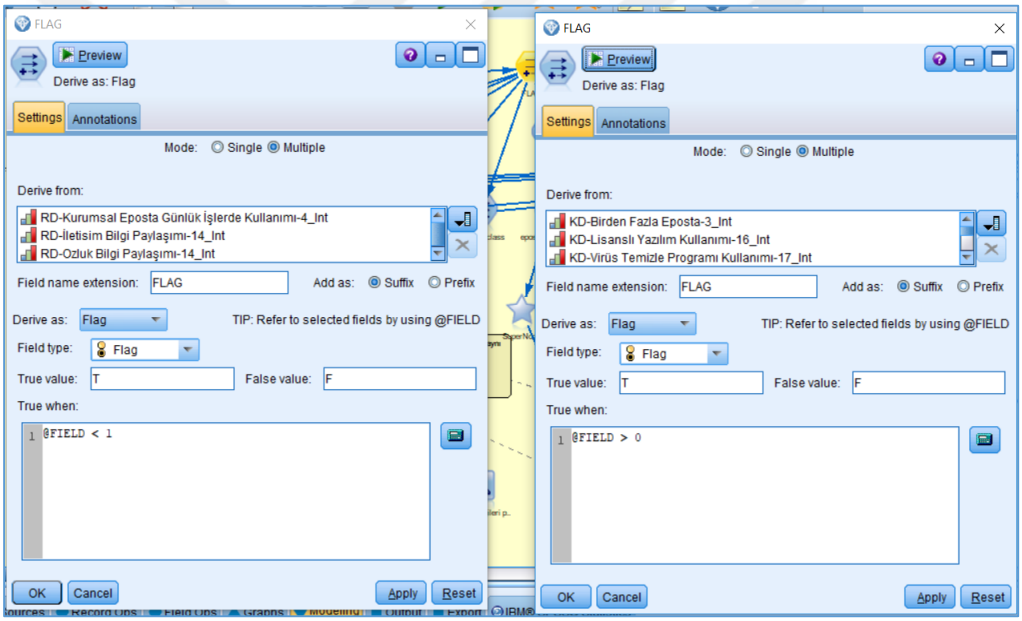
Şekil 30. Veri setlerinin birleştirilmesi işlemi

Bir sonraki adımda birleştirilen veriler üzerinde analize dâhil edilmeyecek olan değişkenlerin filtrelenmesi işlemi yapılmıştır. Örneğin; modellemede herhangi bir etkisi olmayacak olan, katılımcılara ait tekil kimliklendirme (ID) numaraları, katılım sağlamak için sisteme girdikleri e-posta adresleri vb. bu aşamada çıkarılmıştır (Şekil 31).



Şekil 31. Kullanılmayacak değişkenlerin filtrelenmesi

Veriler üzerinde son olarak "Doğru-Yanlış" (True-False) bayrak işlemi uygulanmıştır. Modelleme işlemi kullanıcının veri toplama birinci aşamasında ölçeklerde bu çalışma kapsamında davranış olarak ölçülebilen davranışlara vermiş oldukları cevaplar ve bu cevapları davranış olarak gösterip göstermediklerinin tahmin edilmeye çalışılması bağlamında tasarlandığından bayrak işlemi uygulanmıştır. Riskli davranışlar için 0 (hiçbir zaman) üzeri verilen cevaplar "yanlış" (False), 0 değeri "doğru" (True); korumacı davranışlar için ise tam tersi şekilde 0 üzeri verilen cevaplar "doğru" (True), 0 değeri "yanlış" (False) olarak kodlanmış ve bu sayede veriler karşılaştırma yapılabilmesine imkân tanıyacak şekilde iki kategoriye indirgenmiştir (Şekil 32).



Şekil 32. Bayrak işlemi

Verinin Toplanması ve Analizi

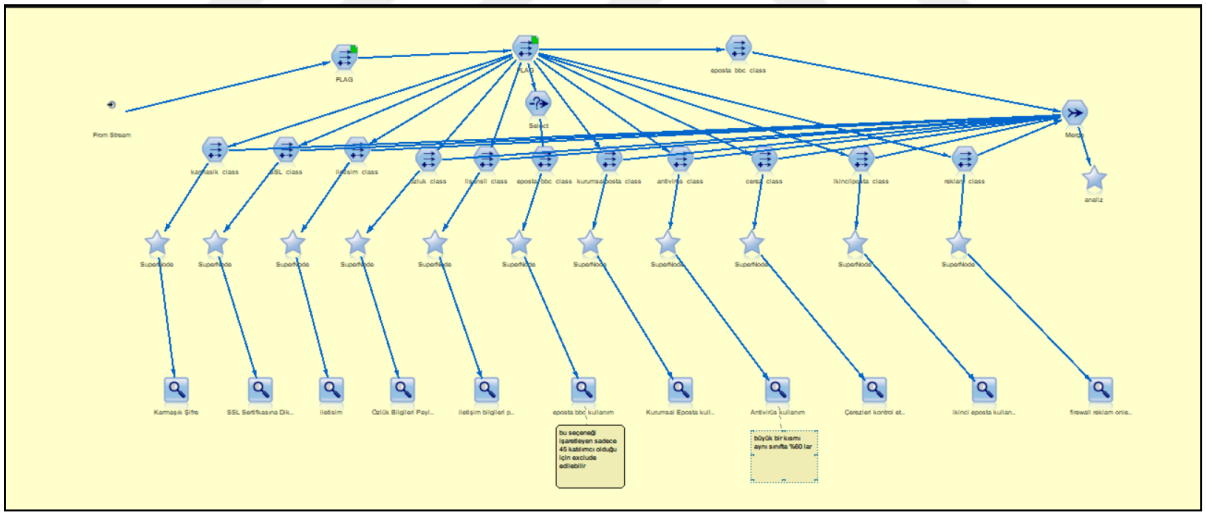
Veriler temizleme ve dönüştürme işlemleri yapılmasının ardından her bir davranış için ayrı ayrı olmak üzere modelleme işlemleri yapılmıştır. Modelleme işleminin nihai amacını katılımcılardan kendi söylemleri doğrultusunda, alınan demografik değişkenler olarak tanımlanan yaş aralığı, eğitim düzeyi, cinsiyet, internet kullanım yılı, günlük internet kullanımı, yazma hızı, dikkat; kişilik özellikleri değişkeni olarak tanımlanan uyumluluk, özdenetim, nevrotizm, gelişime açıklık, dışa dönüklük ve kişisel bilgi güvenliği değişkeni olarak tanımlanan korumacı davranış, riskli davranış, tehlike algısı ve suça maruziyet değişkenlerinin; gerçek

ortamdaki davranışları ile işlenerek katılımcıların her bir davranış için belirlenen bir sınıf içerisinde tanımlanmasının sağlanmasıdır.

Bu aşamada;

- Bilgi güvenliği eğitimine yönelik öğrenme ortamının uyarlanabilir olması için öğrenen modellemesi nasıl yapılmalıdır?
- Bilgi güvenliğine yönelik gerçekleştirilen davranışlar kapsamında klasik istatistiki yöntemler kullanılarak yapılan analizler sonucu ortaya çıkan ilişkiler ile makine öğrenmesi algoritması işe koşularak yapılan analizler sonucu ortaya çıkan ilişkiler arasında bir fark var mıdır? Sorularına yanıt aranmış ve işlemler bu doğrultuda gerçekleştirilmiştir.

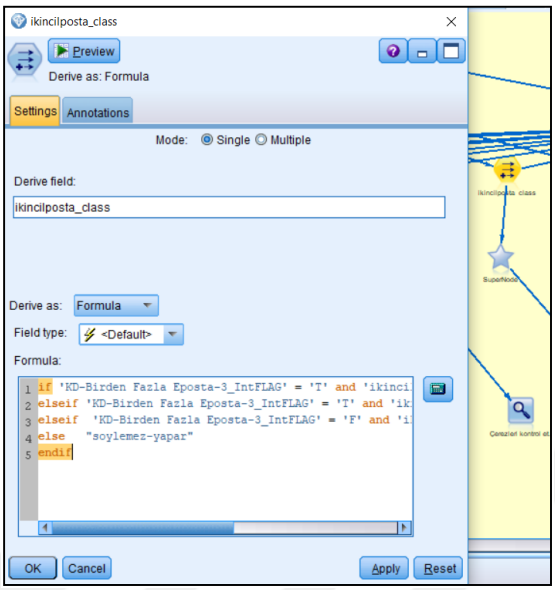
Çalışma kapsamında değerlendirilen tüm davranışlara ait modelleme işlemi görüntüsü Şekil-33'te sunulmuştur. Her bir modelleme işlemi için ortak kullanılan modüller sadece bir davranış için tanıtılmış ancak sonuçları ayrı ayrı sunulmuştur.



Şekil 33. Modelleme işlemi genel görüntüsü

Davranış-1: Birden fazla elektronik posta adresi kullanırım

Öncelikli olarak veri işleme aşamasında temizlenen veriler üzerinden hedef sınıflandırmamızı oluşturacak olan değişkenlerin bayrak (Flag) olarak ayrı bir sütunda tanımlanması "derive" modülü ile gerçekleştirilmiştir (Şekil 34).



*Şekil 34.*Hedef sınıflandırma değişkeninin oluşturulması

Hedef sınıflandırma işlemi için aşağıda belirtilen kod satırı "Birden fazla elektronik posta adresi kullanırım" davranışı için kullanılmış olup diğer davranışlar için de aynı kod düzenlenerek uygulanmıştır. Bayrak değişkeni için belirtilen "T" verisi kullanıcı tarafından ilgili davranışın kendi söylemi ile olumlu yönde gösterildiğinin belirtildiğini gösterirken "F" veriş davranışın olumsuz yönde gösterildiğinin belirtildiğini göstermektedir. "Olumlu" olarak belirtilen veri ise web uygulamasından alınan sonuca göre ilgili davranışın katılımcı tarafından olumlu olarak gösterildiğinin ölçüldüğünü "olumsuz" olarak belirtilen veri ise web uygulamasından alınan sonuca göre ilgili davranışının katılımcı tarafından olumsuz olarak gösterildiğini belirtmektedir.

Sınıflandırma değişkeni oluşturmada kullanılan kod satırı:

if 'KD-Birden Fazla Eposta-3_IntFLAG' = 'T' and 'ikincil_eposta' = 'olumlu' then "soyler-yapar"

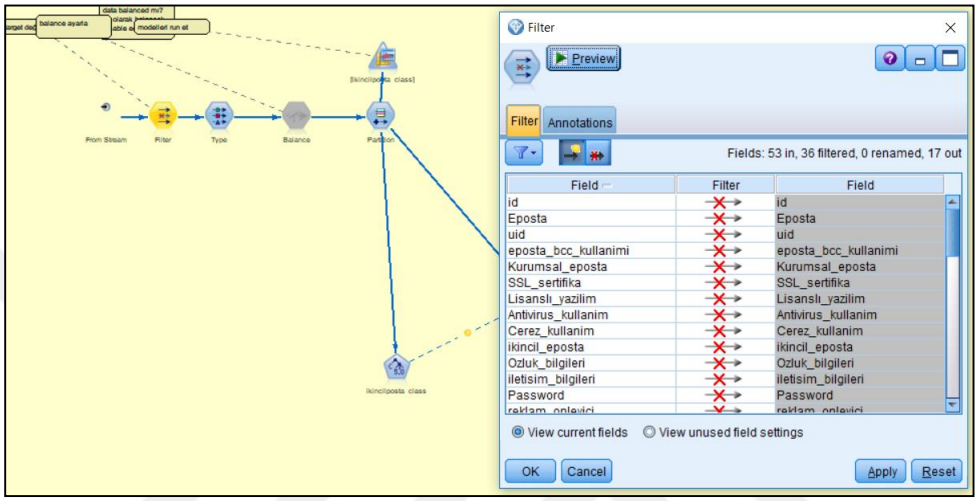
elseif 'KD-Birden Fazla Eposta-3_IntFLAG' = 'T' and 'ikincil_eposta' = 'olumsuz' then "soyler-yapmaz"

elseif 'KD-Birden Fazla Eposta-3_IntFLAG' = 'F' and 'ikincil_eposta' = 'olumsuz' then "soylemez-yapmaz"

else "soylemez-yapar"

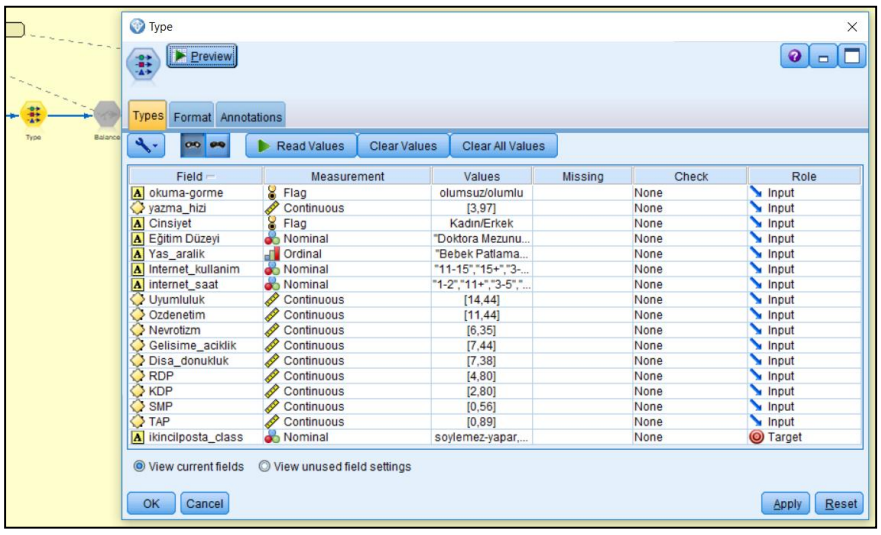
endif

Veri temizleme ve dönüştürme işlemleri sırasında kendisinden analiz edilebilecek verilere dönüştürülen değişkenler modellemede kullanılmamak üzere filtrelenmiştir (Şekil 35).



Şekil 35. Modellemeye dâhil edilmeyecek değişkenlerin filtrelenmesi

Bir sonraki aşamada modelleme için kullanılacak verilerin tipleri kontrol edilmiş ve elde bulunan verilerin sistem tarafından okunması sağlanmıştır. Bu aşama tahmin edilmeye çalışılacak olan nominal değişkenin (Şekil-31'de belirtilen) "hedef" (target) olarak belirlendiği bölümdür. Sınıflandırma algoritması hedef olarak belirtilen değişkenin değerlerine göre sınıflandırma işlemini ekranda belirtilen diğer değişkenleri kullanarak yapacaktır (Şekil 36).



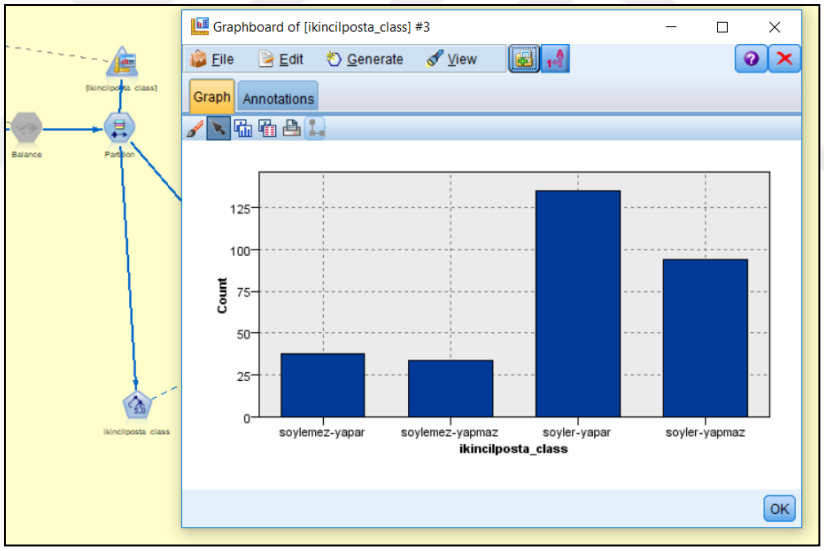
Şekil 36. Modelleme için kullanılacak hedef değişkenin belirlenmesi

Bir sonraki aşamada sınıflandırma yapılacak hedef değişken için katılımcı dağılımı incelenmiştir. Bu aşama daha önce açıklanan dengelenmemiş veri seti hakkında bilgi edinmek ve bir dengeleme işlemine gerek olup olmadığına karar vermek için işletilmektedir (Şekil 37). Grafikten de anlaşılacağı üzere hedef değişken üzerinde veriler dengesiz dağılım göstermektedir (Tablo 56).

Tablo 56

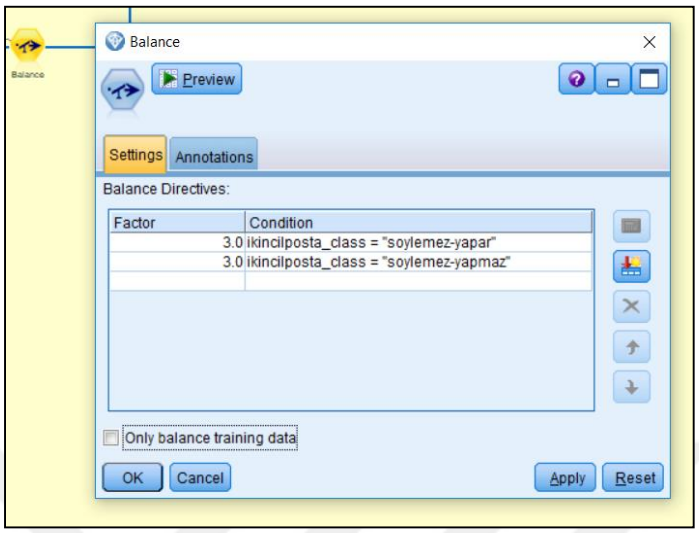
Hedef Davranış-1 İçin Katılımcı Sayıları

Hedef Değişken	Katılımcı Sayısı
Söylemez ancak Yapar	38
Söylemez ve Yapmaz	34
Söyler ve Yapar	138
Söyler ancak yapmaz	94



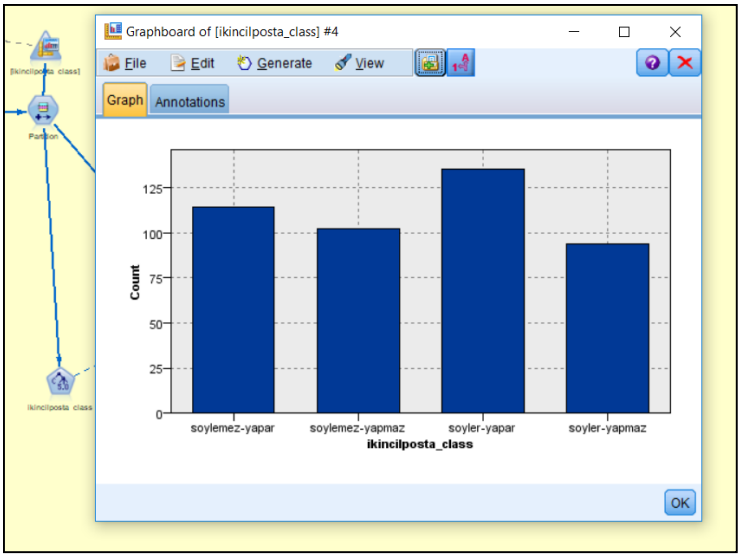
Şekil 37. Hedef değişkene göre katılımcı dağılımı

Bir önceki aşamada açıklandığı üzere; gerçek hayatta dengelenmemiş verilere örnek teşkil eden veri seti üzerinde dengeleme işlemi yapılması ihtiyacı duyulduğu anlaşılmış ve "Balance" modülü kullanılarak "Söylemez ancak Yapar" ile "Söylemez ve Yapmaz" sınıflarında bulunan veriler üzerinde dengeleme işlemi yapılmıştır (Şekil 38). "Balance" modülü rastgele çoğunluk sınıfın azaltılması ve azınlık sınıfın çoğaltılması yöntemlerini kullanmaktadır.



Şekil 38. Dengelenmemiş veri setinin dengelenmesi işlemi

Şekil 38'de gösterimi yapıldığı üzere "Söylemez ancak Yapar" ve "Söylemez ve Yapmaz" katılımcı sayıları rastgele örnek şeçimi ile 3 kat artırılmıştır. "Only balance training data" seçeneği işaretlenmemiş olup bu sayede hem modelin eğitilmesi için hem de test edilmesi için kullanılacak veri setleri dengelenmiştir. Dengeleme işleminden sonra veri seti üzerindeki katılımcı değerleri Şekil 39 üzerinde gösterilmiştir.



Şekil 39. Hedef değişkene göre dengelenmiş katılımcı dağılımı

Tablo 57 üzerinde dengeleme işleminden sonra hedef değişken üzerinde verilerin dengelenmiş dağılım gösterilmiştir.

Tablo 57

Hedef Değişken için Dengelenmiş Katılımcı Sayıları

Hedef Değişken	Katılımcı Sayısı
Söylemez ancak Yapar	114
Söylemez ve Yapmaz	102
Söyler ve Yapar	138
Söyler ancak Yapmaz	94

Bir sonraki aşamada IBM SPSS Modeler yazılımı üzerinde modül olarak bulunan ve modelimizde kullanacağımız verilerin "eğitim", "test" ve "doğrulama" için kullanılacağı parça alanlara bölünmesi işlemi gerçekleştirilmiştir. Bu işlemle kullanmış olduğumuz modelin daha büyük ve kullanmış olduğumuz veri setine benzer veri setleri için ne kadar iyi derecede çalıştığı hakkında fikir sahibi olmamız sağlanmaktadır.

Bu çalışma kapsamında gerçekleştirilen modelleme işlemlerinin performans değerlendirilmeleri karışıklık matrisi (Şekil 40) ve bu matristen elde edilen değerler sonucunda hesaplanan metrikler (Tablo 58) işe koşularak gerçekleştirilmiştir (Amidi, 2019).

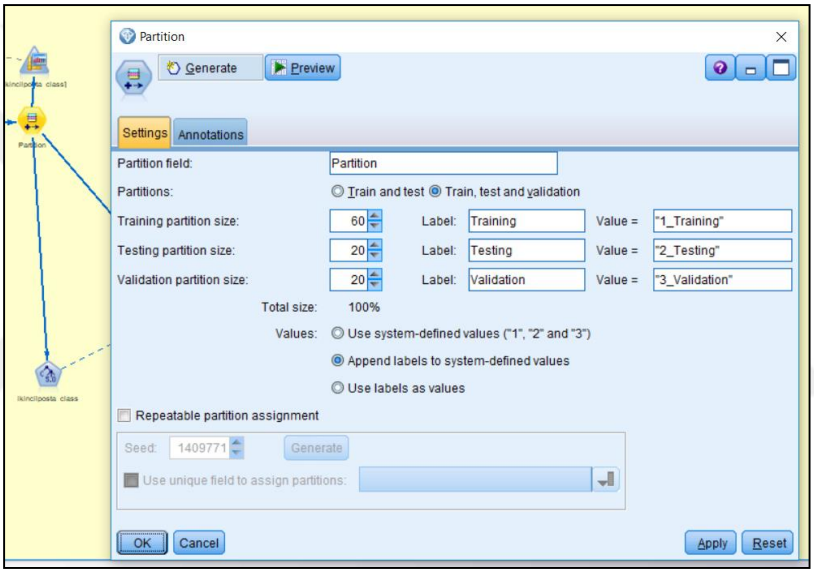
		TAHMİN SINIFI	
		+	-
GERÇEK SINIF	+	DP= Doğru Pozitif (TP =True Positive)	YN= Yanlış Negatif (FN = False Negative)
	-	YP = Yanlış Pozitif (FP = False Positive)	DN = Doğru Negatif (TN = True Negative)

Şekil 40. Karışıklık matrisi

Tablo 58

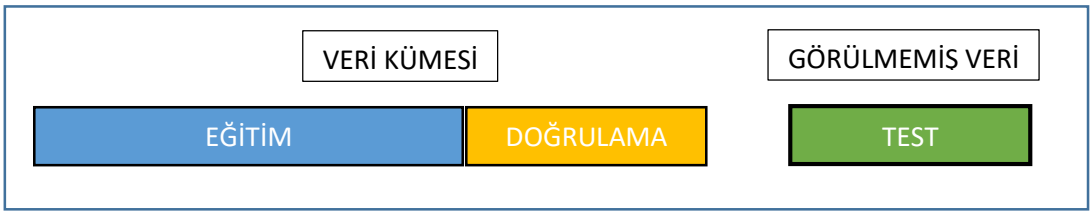
Metrik Değerler

Metrik	Formül	Açıklama
Doğruluk	(DP+DN) / (DP+DN+YP+YN)	Modelin genel performansı
Kesinlik	(DP) / (DP+YP)	Doğru tahminlerin ne kadar kesin olduğu
Geri çağırma	(DP) / (DP+YN)	Gerçek pozitif örneklerin oranı
Özgünlük	(DN) / (DN+YP)	Gerçek negatif örneklerin oranı
F1 skoru	(2DP) / (2DP+YP+YN)	Dengesiz sınıflar için yararlı hibrit metrik



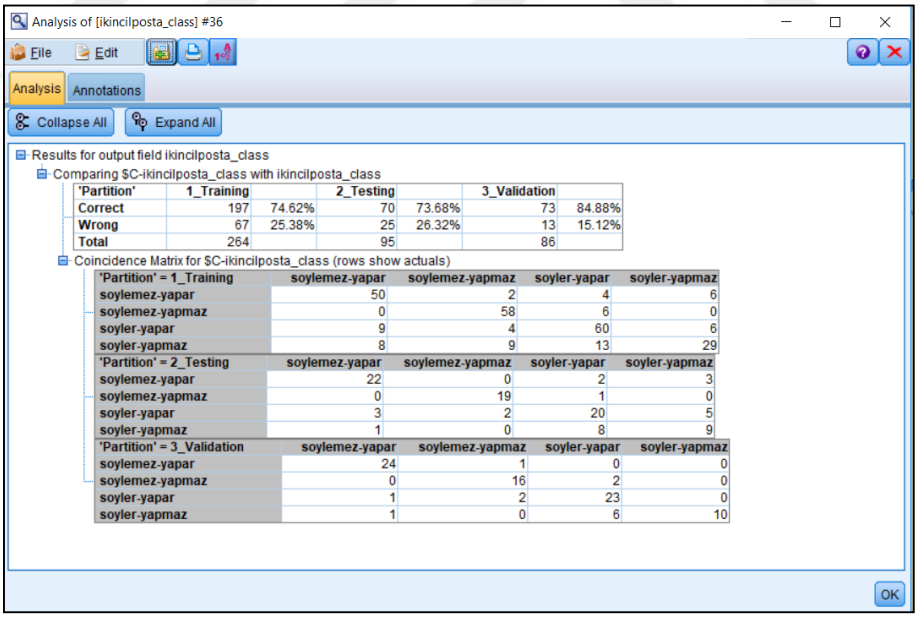
Şekil 41. Veri setinin eğitim, test ve doğrulama işlemleri için parçalara ayrılması

Şekil 41 üzerinde görüldüğü üzere veri setinin %60'lık kısmı modelin eğitilmesi, %20'lik kısmı modelin test edilmesi ve yine %20'lik kısmı ise doğrulama işlemi için kullanılmıştır. Modül ile yapılan doğrulama işlemi "Hold-out" ismi verilen yöntemle gerçekleştirilmektedir. Modül kullanım kolaylığı sağlaması sebebiyle araştırmacılar tarafından sıklıkla da kullanılmaktadır. Ancak hold-out metodu hem eğitim hem test hem de doğrulama için bir dezavantaj da yaratmaktadır.



Şekil 42. Hold-out yöntemi

Hold-out yöntemi Şekil 42 üzerinde açıklandığı gibi, modellenecek veri setinden Şekil 41 üzerinde tarif edildiği şekilde her bir durum için (eğitim, test ve doğrulama) araştırmacının belirlediği oranlarda rastgele örnek veriler seçmektedir. Şekil 41 üzerinde bulunan düzenlemeler özelinden bir örnekle; N=1000 olarak verilen bir veri setinin 600'lük bir bölümü modelin eğitilmesi, 200'lük bir bölümü modelin test edilmesi ve 200'lük bir bölümü de eğitim ve test işlemlerinin doğrulanması için rastgele olarak seçilmektedir. Bu durumun iki dezavantajı bulunmaktadır. Birincisi veri seti parçalara ayrılıp her bir ayrı bölümü ayrı bir işlem için kullanıldığı için daha küçük sayıda veri üzerinde çalışılmasına meydan vermektedir. İkinci dezavantajı ise veri setinden rastgele yapılan seçim işlemi şans faktörünü işe koşmaktadır. Veri setinden rasgele seçilen veriler modelleme için uygunsa modelin doğruluk oranı yüksek ancak modelleme için uygun değilse modelin doğruluk oranı düşük çıkabilmektedir. Şekil 43'te hold-out yöntemi kullanılarak yapılan modelleme işleminin analizi sunulmuş olup %84,88 doğruluk elde edilmiştir.



'Partition'	1_Training		2_Testing		3_Validation	
Correct	197	74.62%	70	73.68%	73	84.88%
Wrong	67	25.38%	25	26.32%	13	15.12%
Total	264		95		86	

Coincidence Matrix for $C-ikincilposta_class (rows show actuals)

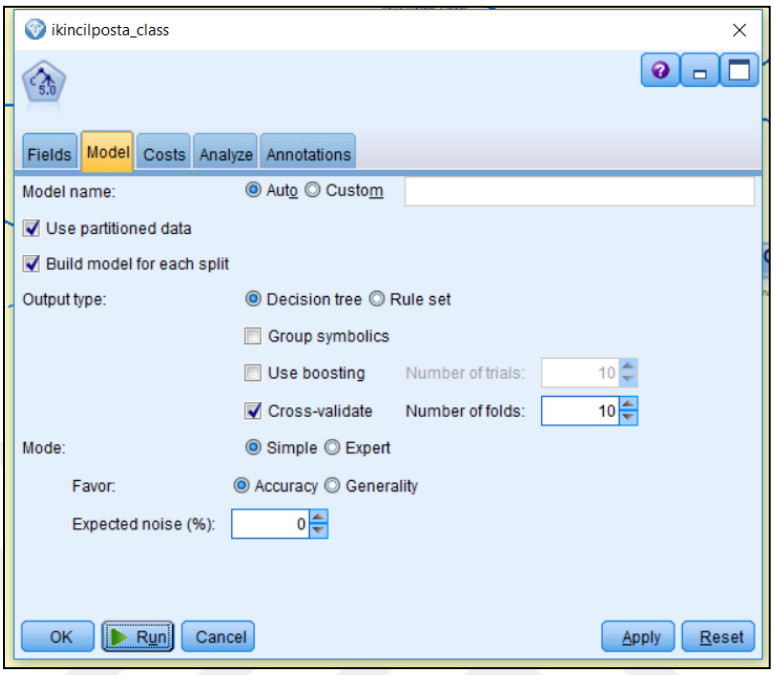
'Partition' = 1_Training	soylemez-yapar	soylemez-yapmaz	soyler-yapar	soyler-yapmaz
soylemez-yapar	50	2	4	6
soylemez-yapmaz	0	58	6	0
soyler-yapar	9	4	60	6
soyler-yapmaz	8	9	13	29

'Partition' = 2_Testing	soylemez-yapar	soylemez-yapmaz	soyler-yapar	soyler-yapmaz
soylemez-yapar	22	0	2	3
soylemez-yapmaz	0	19	1	0
soyler-yapar	3	2	20	5
soyler-yapmaz	1	0	8	9

'Partition' = 3_Validation	soylemez-yapar	soylemez-yapmaz	soyler-yapar	soyler-yapmaz
soylemez-yapar	24	1	0	0
soylemez-yapmaz	0	16	2	0
soyler-yapar	1	2	23	0
soyler-yapmaz	1	0	6	10

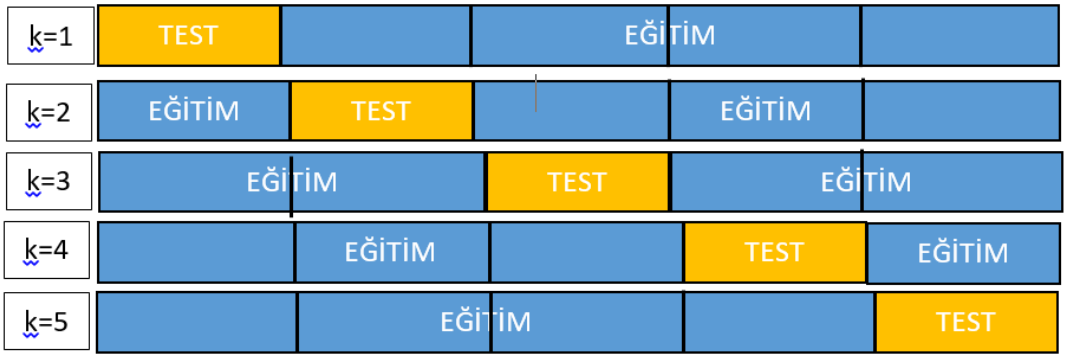
Şekil 43. Hold-out metodu kullanılarak gerçekleştirilen model analizi

Belirtilen dezavantajların önüne geçebilmek için modelleme aşamasında yazılım üzerinde modül olarak bulunmayan, ancak C5.0 sınıflandırma algoritması modülü ile gerçekleştirilebilen "K-katmanlı çapraz doğrulama" metodu 10 katmanlı olarak kullanılmıştır (Şekil 44).



Şekil 44. Modelleme için gerçekleştirilen k-katmanlı çapraz doğrulama işlemi

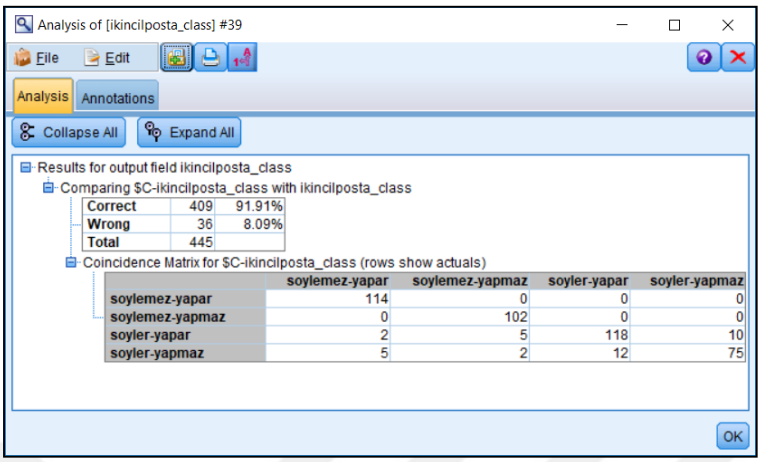
Bu yöntem alan yazında görece daha az verinin bulunduğu veri setlerinde modelin doğruluğunu artırdığı için kullanılmaktadır. Yöntem veri seti k adet gruba ayrıldıktan sonra her defasında bir grubun test geri kalan grupların eğitim amaçlı sıra ile kullanılması temeline dayanmaktadır. K-katmanlı çapraz doğrulama metodu Şekil 45'te açıklandığı üzere modellenecek veri setinden k sayıda katman oluşturulmakta ve her katman k sayıda parçaya bölünmektedir. Birinci katman için K_1 parçası test için kullanılmakta katmanda geri kalan k_{k-1}.parça eğitim için kullanılmaktadır. Bu işlem tekrarlayan bir şekilde her katmanda gerçekleştirilmektedir. Şekil 45 üzerinde bulunan düzenlemeler özelinden bir örnekle; N=1000 olarak verilen bir veri seti 5 eşit katmana bölünmekte ve her katman hala N=1000 veri setinden oluşmaktadır. Tüm katmanlar da k=5 için 5 eşit parçaya bölünmekte ve her parça da 200 veriden oluşmaktadır. Birinci katman için ilk 200 veri test için geri kalan 800 veri eğitim için kullanılmaktadır. İkinci katman için ise ikinci 200 veri test için kullanılmakta geri kalan 800 veri eğitim için kullanılmaktadır. Tekrarlayan bu işlem son katmana kadar gerçekleştirilmektedir. En son işlemden sonra her katman için hata oranı hesaplanarak ortalama doğruluk oranı bulunur. Bu sayede veri setinde bulunan tüm veriler k-1 kez hem eğitim hem de test işlemleri için kullanılabilmektedir. Bu da modellemenin doğruluk oranını artırmaktadır.



Şekil 45. K-Katmanlı çapraz doğrulama işlemi

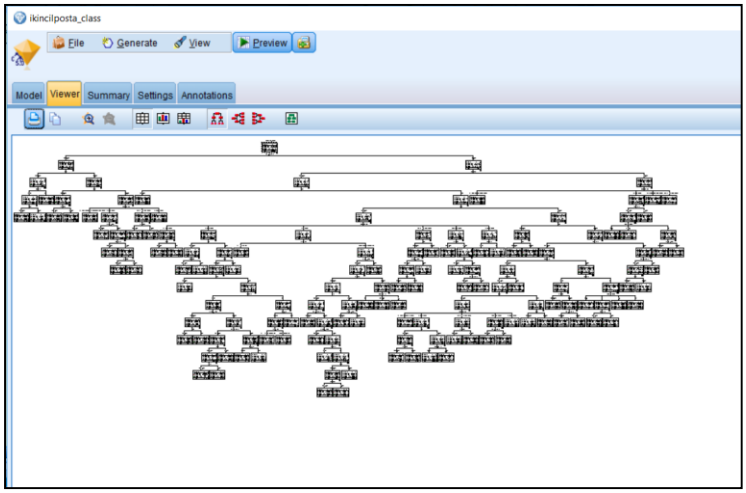
Veri madenciliği ve makine öğrenmesinde, modelin genelleme yeteneğinin yüksek olmasını sadece o veri seti üzerinde iyi çalışmasını değil hiç görmediği başka veri setleri üzerinde de iyi sonuçlar vermesi beklenir. Bu bahisle, veri setinin dengesiz dağılması, veri setinin küçük olmasından dolayı sıklıkla karşılaşılan bir sorun ise fazla uydurma ve az uydurmadır (overfitting ve underfitting). Fazla uydurma problemi; model oluşturulurken kullanılan veri seti üzerinde çok iyi çalışırken hiç tanımadığı bir veri seti üzerinde iyi sonuç vermemesidir. Az uydurma ise çalışılan veri seti üzerinde uyguladığımız modelin iyi kurgulanmaması sebebiyle iyi sonuçlar vermemesi ve hiç bilmediği veriler üzerinde de benzer sonuçlar üretmesidir. Az uydurma problemi görece daha sorunsuzdur çünkü başarısız olması kanıtlanmış bir modelleme üzerinde çalışmak için hiçbir araştırmacı ısrarcı olmaz ve modellemeyi yeniden kurgulamaya çalışır. Araştırmacılar için sorun yaratacak olan konu fazla uydurma problemidir. Alan yazında bu iki sorun için sıklıkla kullanılan iki yöntemden biri dışarda bırakma yöntemi ile doğrulama iken diğer k-katmanlı çapraz doğrulama yöntemidir. Bu sebeple tez kapsamında yukarıda bahsedilen avantajları da göz önüne alınarak k-katmanlı çapraz doğrulama yöntemi kullanılmıştır.

Şekil 46'da 10 katmanlı çapraz doğrulama işlemi yapılarak gerçekleştirilen modellemenin analiz sonuçları gösterilmekte olup %91,91 doğruluk elde edilmiştir. Şekil 43'te gösterilen Hold-out yöntemi kullanılarak gerçekleştirilen modelleme analizi ile karşılaştırıldığında modelin doğruluk oranındaki iyileştirme açıktır.

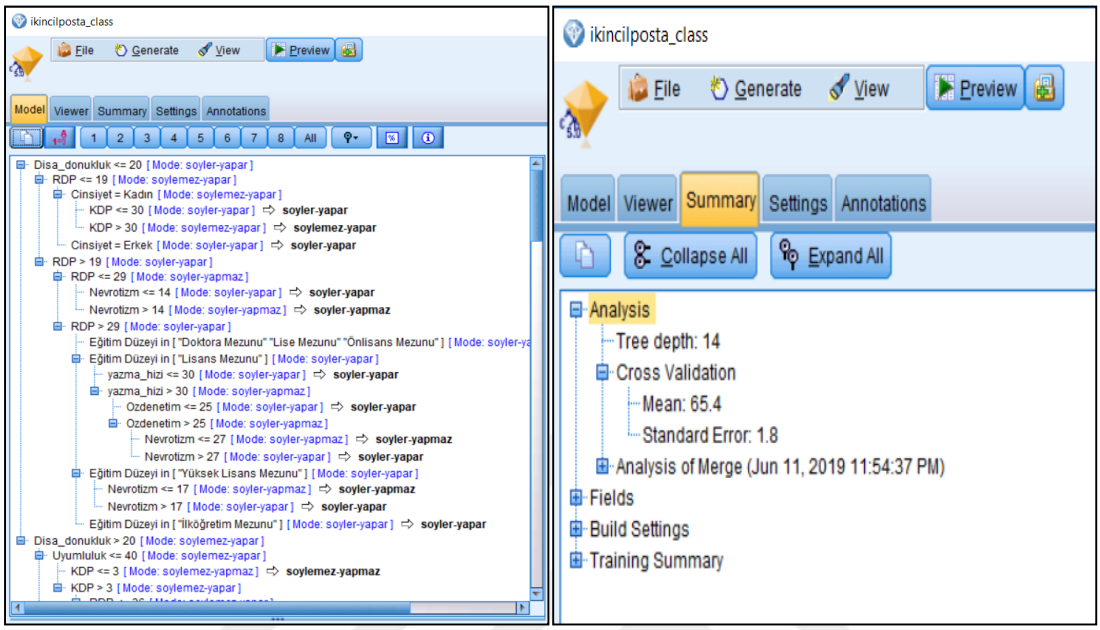


Şekil 46. K-Katmanlı çapraz doğrulama metodu kullanılarak gerçekleştirilen model analizi

Özniteliklerin test edildiği düğümlerden oluşan karar ağaçları işleyiş olarak akış şemalarına benzemektedirler. Karar ağaçları dallar ve yapraklardan oluşur ve karar ağacının en üstünde "kök" en alt yapısı ise "yaprak" olarak adlandırılır. Kök ve yapraklar arasında kalan yapı ise "dal" olarak adlandırılır ve özniteliklerin test edildiği düğümler altında oluşan dallar ulaşılabilecek sonuçlara karşılık gelir (Kantardzic, 2011; Özkan, 2008). C5.0 algoritması kullanılarak oluşturulan model ile ilgili davranış için oluşturulan karar ağacı Şekil 47'de, hangi değişkenlerin hangi diğer değişkenle ilişkili olarak sınıflandırma işleminde kullanıldığı, hangi değişkenlerin hangi parametreler doğrultusunda karar ağacı dallanmasında etkili oldukları kesit olarak Şekil 48'de gösterilmiştir.



Şekil 47. "Birden Fazla Elektronik Posta Adresi Kullanırım" davranışı için oluşturulan karar ağacı görüntüsü



Şekil 48. "Birden Fazla Elektronik Posta Adresi Kullanırım" davranışı için oluşturulan karar ağacı değerleri

Şekil 48'de belirtildiği üzere "birden fazla elektronik posta adresi kullanırım" davranışı için oluşturulan karar ağacı 14 katman derinliğindedir ve karar ağacını oluşturan kural setinin bir bölümünü göstermektedir. Kişilik özellikleri arasında yer alan "Dışa dönüklük" özniteliği kök düğüm olarak belirlenmiştir ve dallanma bu öznitelikten oluşturulmaya başlanmıştır.

"Birden fazla elektronik posta adresi kullanırım" davranışı için bir önceki aşamada gerçekleştirilen klasik istatistiki yöntemlerle belirlenen ilişkili değişkenler ile C5.0 algoritması kullanılarak dengelenmiş ve dengelenmemiş veri setleri için ayrı ayrı oluşturulan karar ağacında belirlenen ilişkili değişkenlerin karşılaştırılması Tablo 59 üzerinde sunulmuş, davranış için oluşturulan kural seti EK 12'de sunulmuştur.

Tablo 59

"Birden Fazla Elektronik Posta Adresi Kullanırım" Davranışı İçin Değişken Karşılaştırması

C5.0 Algoritması – İlişkili Öznitelikler – (Dengelenmiş veri seti)	C5.0 Algoritması – İlişkili Öznitelikler – (Dengelenmemiş veri seti)	Klasik İstatistiki Yöntemler – İlişkili Öznitelikler
- Cinsiyet - Eğitim Düzeyi - Yaş Aralığı - İKY - GİKS - Riskli Davranış Puanı - Korumacı Davranış Puanı - Tehlike Algısı Puanı - Suça Maruziyet Puanı - Nevrotizm Puan - Dışa Dönüklük Puanı - Uyumluluk Puanı - Gelişime Açıklık Puanı - Özdenetim Puanı - Yazma Hızı - Okuduğunu Görme	- Cinsiyet - Eğitim Düzeyi - İKY - GİKS - Riskli Davranış Puanı - Korumacı Davranış Puanı - Tehlike Algısı Puanı - Suça Maruziyet Puanı - Nevrotizm Puanı - Dışa Dönüklük Puanı - Uyumluluk Puanı - Özdenetim Puanı - Yazma Hızı - Dikkat Durumu	- Cinsiyet - Eğitim Düzeyi - Yaş Aralığı - İKY - Dışa Dönüklük Puanı - Riskli Davranış Puanı

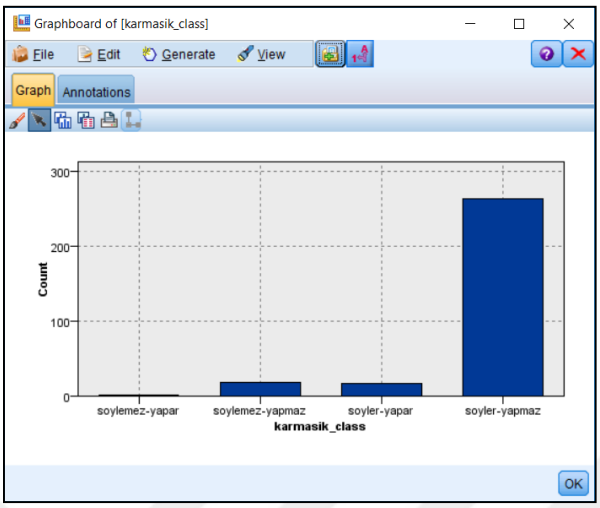
Davranış-2: İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım

Sınıflandırma yapılacak hedef öznitelik için katılımcı dağılımı incelenmiştir. Bu aşama daha önce açıklanan dengelenmemiş veri seti hakkında bilgi edinmek ve bir dengeleme işlemine gerek olup olmadığına karar vermek için işletilmektedir. (Şekil-43). Grafikten de anlaşılacağı üzere hedef değişken üzerinde veriler dengesiz dağılım göstermektedir (Tablo 60).

Tablo 60

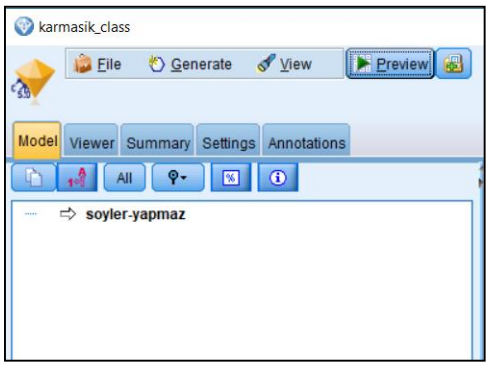
Hedef Davranış-2 için Katılımcı Sayıları

Hedef Değişken	Katılımcı Sayısı
Söylemez ancak Yapar	1
Söylemez ve Yapmaz	19
Söyler ve Yapar	17
Söyler ancak Yapmaz	264



Şekil 49. Hedef davranışa göre katılımcı dağılımı

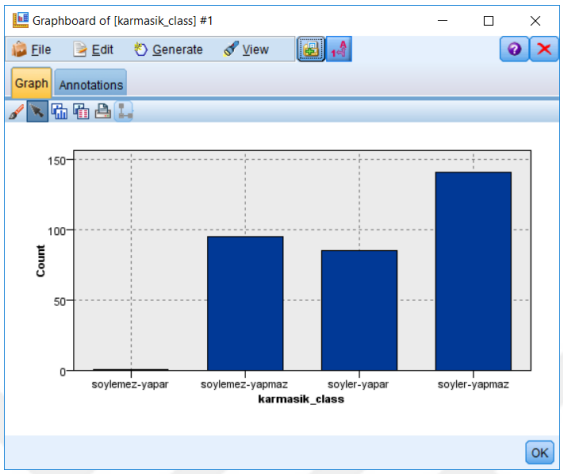
Şekil 49 üzerindeki verilerden de anlaşılacağı üzere bu durum daha önce de bahsedildiği gibi gerçek hayatta sıklıkla karşılaşılacak aşırı oranda dengelenmemiş bir veri seti örneğidir. "İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım" davranışı için "söyler ancak yapmaz" sonucunun tim katılımcıların yaklaşık olarak %87'sini oluşturduğu göstermektedir. Şekil 50 üzerinde de gösterildiği üzere dengelenmemiş şekli ile makine öğrenme algoritması işe koşulduğunda kendisine verilecek herhangi öznitelik seti için "söyler ancak yapmaz" sonucunu döndürmesi model için %87'lik bir başarı oranı sağlayacaktır. Bu sebeple C5.0 algoritması işe koşulduğunda herhangi bir kural seti sunmadan direk olarak "söyler ancak yapmaz" çıktısı vermektedir.



Şekil 50. Dengelenmemiş veri setinin sınıflandırma oluşumu

Şekil 51'de gösterimi yapıldığı üzere "Söylemez ve Yapmaz" ve "Söyler ve Yapar" katılımcı sayıları rastgele örnek seçimi ile artırılarak dengeleme işlemi yapılmıştır. "Söylemez ancak

Yapar” sınıfı sadece bir elemandan oluştuğu için herhangi bir dengeleme işlemine tabi tutulmamıştır.



Şekil 51. Hedef davranışa göre dengelenmiş katılımcı dağılımı

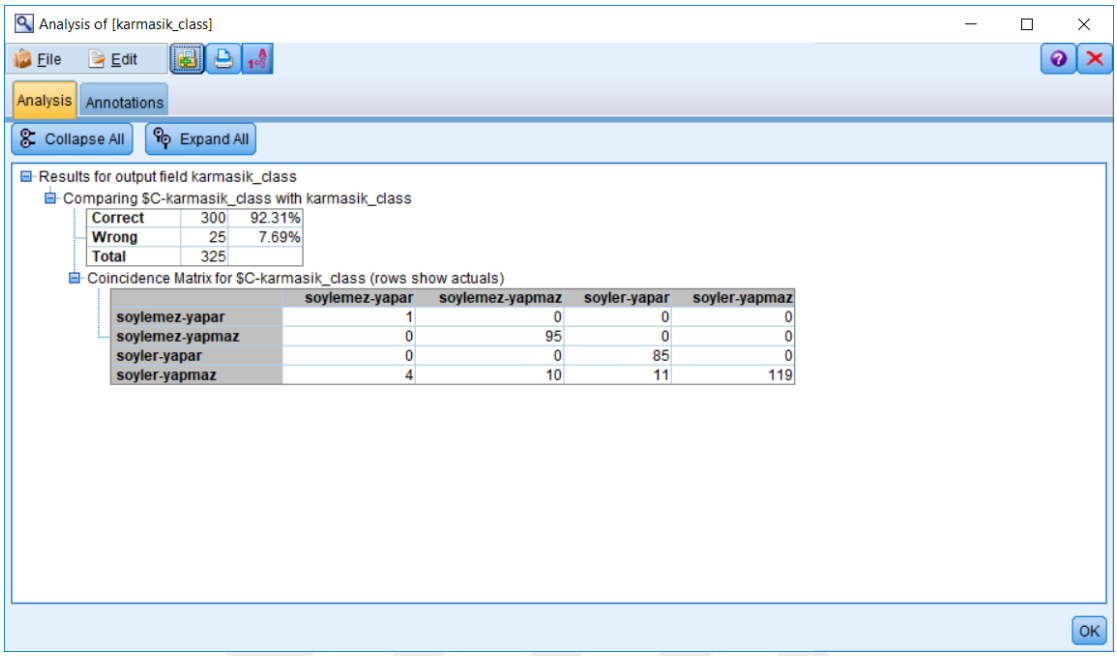
Tablo 61’de hedef davranış üzerinde dengeleme işlemi yapıldıktan sonra oluşan katılımcı sayıları gösterilmiştir.

Tablo 61

Hedef Değişken için Dengeleme İşlemi Yapılmış Katılımcı Sayıları

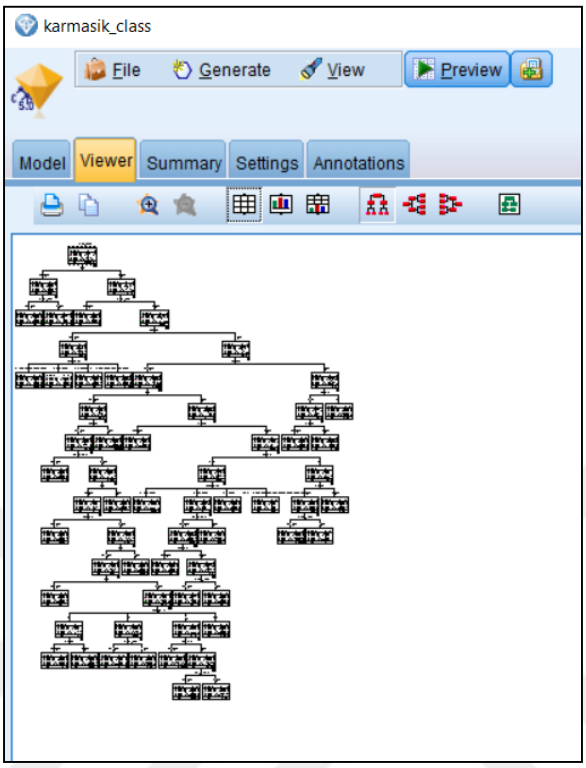
Hedef Değişken	Katılımcı Sayısı
Söylemez ancak Yapar	1
Söylemez ve Yapmaz	95
Söyler ve Yapar	85
Söyler ancak Yapmaz	129

Şekil 52’de 10 katmanlı çapraz doğrulama işlemi yapılarak gerçekleştirilen modellemenin analiz sonuçları gösterilmekte olup %92,31 doğruluk elde edilmiştir.

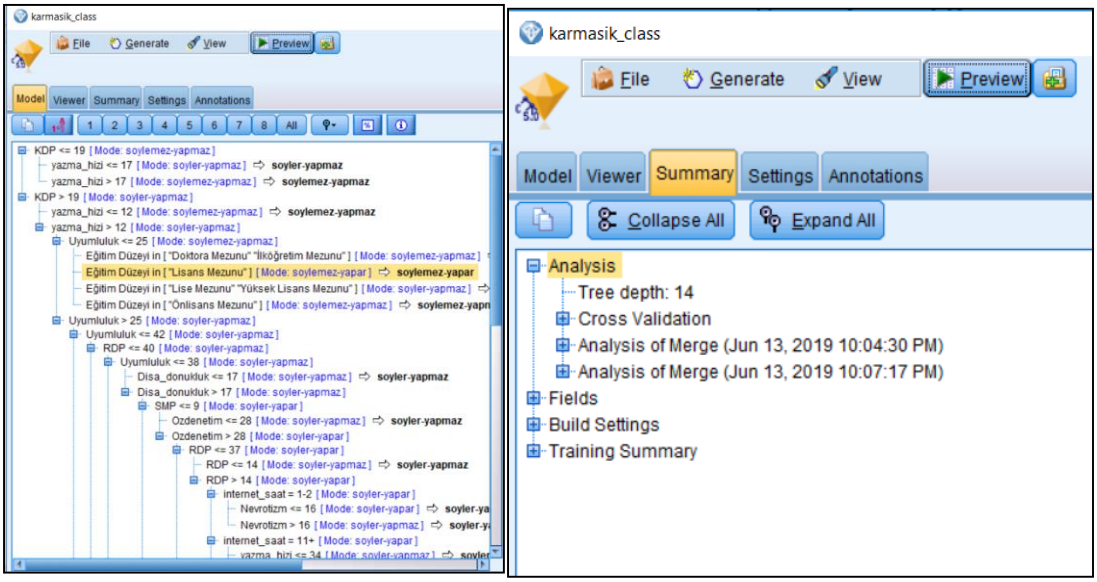


Şekil 52. Hedef davranış için gerçekleştirilen model analizi

C5.0 algoritması kullanılarak oluşturulan model ile ilgili davranış için oluşturulan karar ağacı Şekil 53'te, hangi değişkenlerin hangi diğer değişkenle ilişkili olarak sınıflandırma işleminde kullanıldığı, hangi değişkenlerin hangi parametreler doğrultusunda karar ağacı dallanmasında etkili oldukları kesit olarak Şekil 54'te gösterilmiştir.

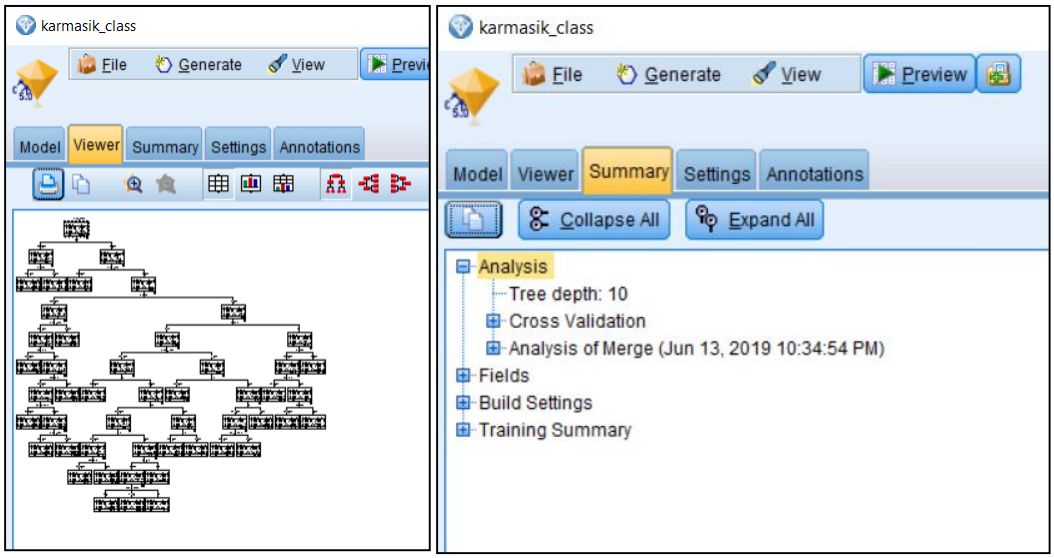


Şekil 53. "İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım" davranışı için oluşturulan karar ağacı görüntüsü



Şekil 54. "İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım" davranışı için oluşturulan karar ağacı değerleri

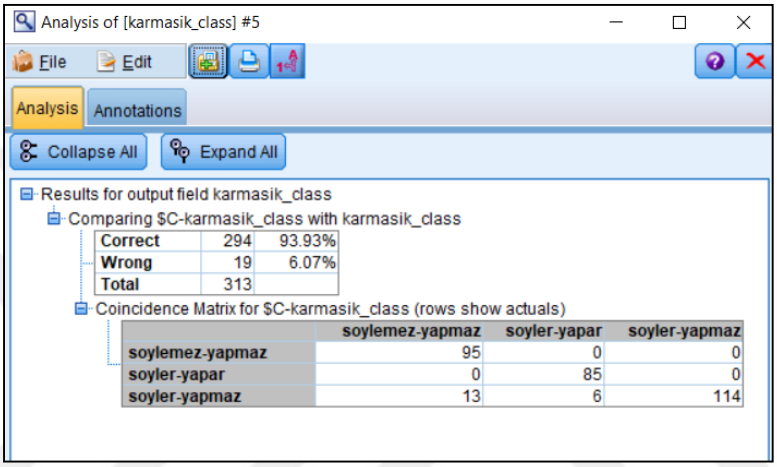
Şekil 54'te belirtildiği üzere "İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım" davranışı için oluşturulan karar ağacı 14 katman derinliğindedir ve karar ağacını oluşturan kural setinin bir bölümünü göstermektedir. Kişisel bilgi güvenliği özellikleri arasında yer alan "Korumacı Davranış Puanı" özniteliği kök düğüm olarak belirlenmiştir ve dallanma bu öznitelikten oluşturulmaya başlanmıştır. Şekil 54 üzerinde de görüleceği üzere sadece 1 elemandan oluşan "Söylemez ancak yapar" sınıfı hakkında da dallanma işlemi yapıldığı görülmektedir. Buna göre korumacı davranış puanı 19'dan büyük, yazma hızı 12'den büyük ve lisans mezunu bir denek modele girdi olarak verildiğinde "söylemez ancak yapar" sınıfına dâhil edilecektir. Bu durum veri azlığı sebebiyle gerçek hayatla uygun olmayacak ve modelin "yanlış-pozitif" (false-positive) sonuç üretmesine sebep olacaktır. Bu sebeple verimizde budama işlemi yapılarak modelleme tekrar edilmiştir. Budama işlemi gereksiz karşılaştırmaların ya da yaprakların modelden çıkarılması olarak tanımlanabilir (Yakut, 2012). Budama işlemi gerçekleştirildikten sonra oluşturulan model ile ilgili davranış için oluşturulan karar ağacı ve özellikleri Şekil 55'te gösterilmiştir. Karar ağacının 10 katman derinliğe düştüğü görülmektedir.



Şekil 55. Budama işlemi gerçekleştirildikten sonra oluşan karar ağacı ve özellikleri

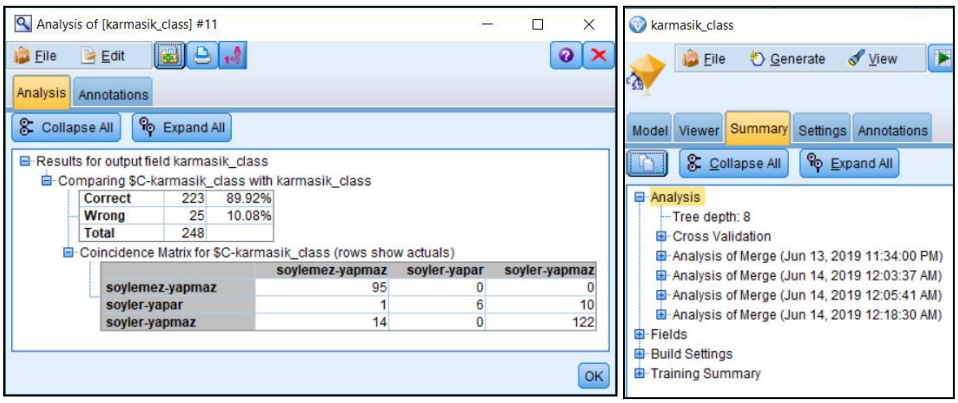
Şekil 56'da 10 katmanlı çapraz doğrulama ve budama işlemi yapılarak gerçekleştirilen modellemenin analiz sonuçları gösterilmekte olup %93,93 doğruluk elde edilmiştir. Sınıflar arasındaki örnek sayıları karşılaştırıldığında "söylemez ve yapmaz" ve "söyler ve yapar"

sınıflarının örnek sayılarının düşük olmasından dolayı her ne kadar dengeleme işlemi yapılarak modelleme işlemi gerçekleştirilmiş olsa da karışıklık matrisi incelendiğinde modelin herhangi "yanlış-pozitif" (false-positive) veya "yanlış-negatif" (false-negative) sonuç döndürmediği görülmektedir. Bu durum %100 lük bir başarı gibi görünse de aslında fazla uydurma (overfitting) durumuna bir örnek oluşturmaktadır.



Şekil 56. Hedef davranış-2 için budama işlemi uygulandıktan sonra gerçekleştirilen model analizi

Fazla uydurma problemi modelin gerçek hayatta kullanılmasıyla yanlış-pozitif sonuçlar döndürecek yani aslında o sınıfta olmaması gereken bir katılımcıyı o sınıftaymış gibi sınıflandıracaktır. "Yanlış-pozitif" sonuç döndürme örneğin kanserli olamayan bir hastanın kanserliymiş gibi sınıflandırılmasına bu sebeple gereksiz ilaç tedavisi almasına sebep olacak bir durumdur (Pham, 2010). Hedef davranış için "söyler ve yapar" sınıfında dengeleme işlemi yapılmamış, "söylemez ve yapmaz" sınıfında dengeleme işlemi yapılmıştır. Bu şekilde fazla uydurma durumu oluşabilecek olan "söylemez ve yapmaz" sınıfına dâhil olmaması gereken ancak işlem sonucu bu sınıfa dâhil edilen bir katılımcı konuyu biliyor/bilmiyor ancak davranışı gösteriyor olsa dahi ilgili eğitimi fazladan almış olacaktır. Bu da katılımcının sadece öğrenme sistemi üzerinde geçireceği vakti artıracak olup alınan ders bir tekrar niteliğinde olacak ve kanserli hasta örneğinde vurgulanan türde bir probleme sebep olmayacaktır. Devam eden aşamalarda dengeleme işlemleri aynı doğrultuda gerçekleştirilmiştir. Belirtilen dengeleme işleminden sonra davranışa ait nihai karışıklık matrisi ve 8 katmanlı karar ağacının özellikleri Şekil 57 üzerinde gösterilmiştir.



Şekil 57. Hedef davranış-2 için nihai karar ağacı özellikleri ve karışıklık matrisi analizi

"İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım" davranışı için bir önceki aşamada gerçekleştirilen klasik istatistiki yöntemlerle belirlenen ilişkili öznitelikler ile C5.0 algoritması kullanılarak oluşturulan karar ağacında belirlenen ilişkili değişkenlerin karşılaştırılması Tablo 62 üzerinde sunulmuş, davranış için oluşturulan kural seti EK 12'de sunulmuştur.

Tablo 62

"Birden fazla elektronik posta adresi kullanırım" Davranışı İçin Değişken Karşılaştırması

C5.0 Algoritması – İlişkili Öznitelikler – (Dengelenmiş veri seti)	C5.0 Algoritması – İlişkili Öznitelikler – (Dengelenmemiş veri seti)	Klasik İstatistiki Yöntemler – İlişkili Öznitelikler
- Cinsiyet - Eğitim Düzeyi - Riskli Davranış Puanı - Korumacı Davranış Puanı - Tehlike Algısı Puanı - Uyumluluk Puanı - Gelişime Açıklık Puanı - Özdenetim Puanı - Yazma Hızı	- Dengelenmemiş veri seti üzerinde herhangi bir karar ağacı oluşmamaktadır.	- GİKS - Korumacı Davranış Puanı - Uyumluluk Puanı - Nevrotizm Puanı - Gelişime Açıklık Puanı

Bu aşamadan sonra her bir davranış için ortak olan modüllerin kullanımına ilişkin bilgilendirme yapılmamış olup modelleme işlem ve sonuçları sunulmuştur.

Davranış-3: Güvenlik duvarı, reklam önleyici vb. programlar kullanırım.

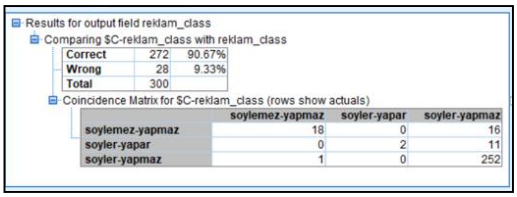
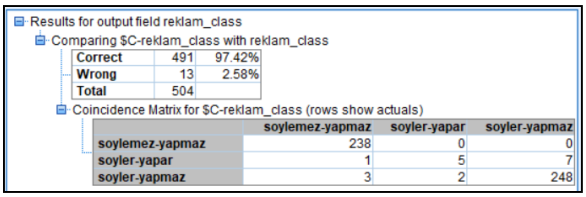
Sınıflandırma yapılacak hedef öznitelik için katılımcı dağılımı incelenmiştir. Bu aşama daha önce açıklanan dengelenmemiş veri seti hakkında bilgi edinmek ve bir dengeleme işlemine gerek olup olmadığına karar vermek için işletilmektedir. Dengelenmemiş veri seti üzerinde anlaşılacağı gibi "söylemez ancak yapar" sınıfı sadece bir örnek içermekte olduğundan budama işlemi yapılmış ve modelleme işlemine dâhil edilmemiştir. "Söyler ve Yapar" sınıfına dâhil olan veri seti üzerinde herhangi bir dengeleme işlemi yapılmamış olup "söylemez ve yapmaz" sınıfı üzerinde dengeleme işlemi yapılarak veri seti genişletilmiştir. Yapılan işlemler sonucu modelleme işlemine dâhil edilecek sınıf ve veri sayıları Tablo 63 üzerinde gösterilmiştir.

Tablo 63

Hedef Öznitelik için Katılımcı Sayıları

	Dengelenmemiş Veri Seti	Dengeleme İşlemi Yapılmış Veri Seti
Hedef Değişken	Katılımcı Sayısı	Katılımcı Sayısı
Söylemez ancak Yapar	1	-
Söylemez ve Yapmaz	34	238
Söyler ve Yapar	13	13
Söyler ancak Yapmaz	253	253

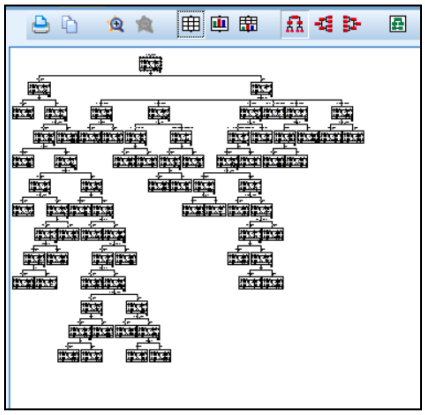
Tablo 63 üzerindeki verilerden de anlaşılacağı üzere bu durum daha önce de bahsedildiği gibi gerçek hayatta sıklıkla karşılaşılacak aşırı oranda dengelenmemiş bir veri seti örneğidir. "Güvenlik duvarı, reklam önleyici vb. Programlar kullanırım" davranışı için "söyler ancak yapmaz" sonucunun tüm katılımcıların yaklaşık olarak %84'ünü oluşturduğu göstermektedir. Veri setinin dengelenmemiş şekli ile dengeleme işlemi yapıldıktan sonra makine öğrenme algoritması işe koşulduğunda ortaya çıkan karar ağaçlarının karışıklık matris değerleri Şekil 58 üzerinde gösterilmiştir.

Dengeleme işlemi Yapılmamış Veri Seti için Karışıklık Matrisi	Dengeleme İşlemi Yapılmış Veri Seti için Karışıklık Matrisi
	

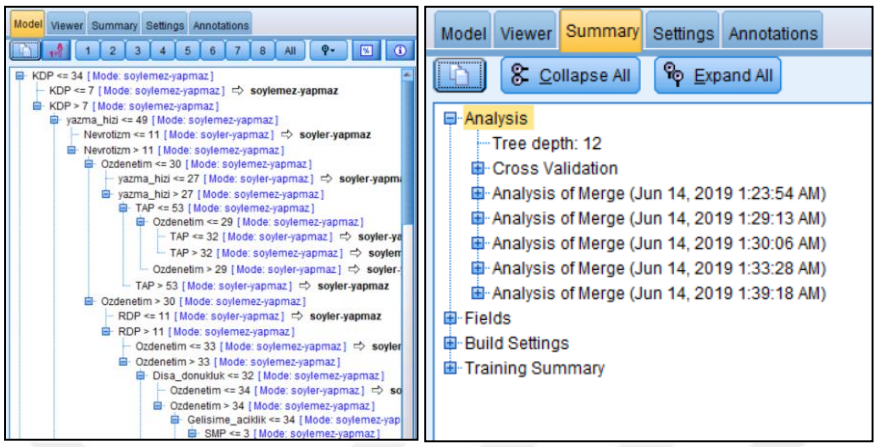
Şekil 58. Dengeleme işlemi yapılmış ve yapılmamış veri setleri için karar ağacı karışıklık matrisleri

Karışıklık matrisleri ayrı ayrı incelendiğinde hedef davranış için dengeleme işlemi yapılmış veri seti üzerinde koşulan karar ağacının doğruluk değerinin yüksek olmasına bakılmaksızın, "söyler ancak yapmaz" sınıfında gerçekleştirilen tahminlerin daha yüksek oranda olması ve ayrıca "söylemez ve yapmaz" sınıfında fazla uydurma probleminin olmasının davranışın gösterilmediği durumunu değiştirmediği için çalışma kapsamında tasarlanacak çevrimiçi eğitim ortamında dengelenmiş veri seti üzerinde işe koşulan karar ağacı kural setinin kullanılmasına karar verilmiştir.

C5.0 algoritması kullanılarak oluşturulan model ile ilgili davranış için oluşturulan karar ağacı Şekil 59'da, hangi değişkenlerin hangi diğer değişkenle ilişkili olarak sınıflandırma işleminde kullanıldığı, hangi değişkenlerin hangi parametreler doğrultusunda karar ağacı dallanmasında etkili oldukları kesit olarak Şekil 60'ta gösterilmiştir.



Şekil 59. "Güvenlik duvarı, reklam önleyici vb. Programlar kullanırım" davranışı için oluşturulan karar ağacı görüntüsü



Şekil 60. "Güvenlik duvarı, reklam önleyici vb. Programlar kullanırım" davranışı için oluşturulan karar ağacı değerleri

Şekil 60'da belirtildiği üzere "Güvenlik duvarı, reklam önleyici vb. programlar kullanırım." davranışı için oluşturulan karar ağacı 12 katman derinliğindedir ve karar ağacını oluşturan kural setinin bir bölümünü göstermektedir. Kişisel bilgi güvenliği özellikleri arasında yer alan "Korumacı Davranış Puanı" özniteliği kök düğüm olarak belirlenmiştir ve dallanma bu öznitelikten oluşturulmaya başlanmıştır.

"Güvenlik duvarı, reklam önleyici vb. Programlar kullanırım" davranışı için bir önceki aşamada gerçekleştirilen klasik istatistiki yöntemlerle belirlenen ilişkili öznitelikler ile C5.0 algoritması kullanılarak oluşturulan karar ağacında belirlenen ilişkili değişkenlerin karşılaştırılması Tablo 64 üzerinde sunulmuş, davranış için oluşturulan kural seti EK 12'de sunulmuştur.

Tablo 64

"Güvenlik duvarı, reklam önleyici vb. Programlar kullanırım " Davranışı için Öznitelik Karşılaştırması

C5.0 Algoritması – İlişkili Öznitelikler – (Dengelenmiş veri seti)	C5.0 Algoritması – İlişkili Öznitelikler – (Dengelenmemiş veri seti)	Klasik İstatistiki Yöntemler – İlişkili Öznitelikler
- Eğitim Düzeyi - Yaş Aralığı - Riskli Davranış Puanı - Korumacı Davranış Puanı - Tehlike Algısı Puanı - Suça Maruziyet Puanı - Nevrotizm Puanı - Gelişime Açıklık Puanı - Özdenetim Puanı - Dışa Dönüklük Puanı - Okuduğunu Görme - Yazma Hızı	- Eğitim Düzeyi - Yaş Aralığı - Korumacı Davranış Puanı - Suça Maruziyet Puanı - Özdenetim Puanı - Uyumluluk Puanı - Okuduğunu Görme	- Nevrotizm Puanı - Riskli Davranış Puanı

Davranış-4: Virüs temizleme, casus yazılım önleme vb. Programları kullanırım

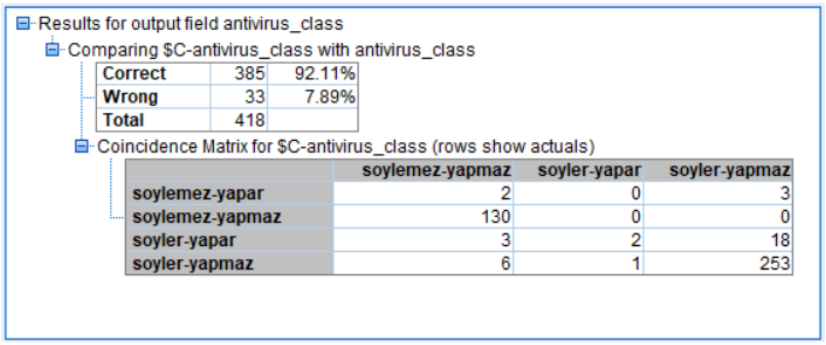
Sınıflandırma yapılacak hedef öznitelik için katılımcı dağılımı incelenmiştir. Bu aşama daha önce açıklanan dengelenmemiş veri seti hakkında bilgi edinmek ve bir dengeleme işlemine gerek olup olmadığına karar vermek için işletilmektedir. "Söyler ve Yapar" sınıfına dâhil olan veri seti üzerinde herhangi bir dengeleme işlemi yapılmamış olup "söylemez ve yapmaz" sınıfı üzerinde dengeleme işlemi yapılarak veri seti genişletilmiştir. Yapılan işlemler sonucu modelleme işlemine dâhil edilecek sınıf ve veri sayıları Tablo 65 üzerinde gösterilmiştir.

Tablo 65

Hedef Davranış-4 İçin Katılımcı Sayıları

	Dengelenmemiş Veri Seti	Dengeleme İşlemi Yapılmış Veri Seti
Hedef Değişken	Katılımcı Sayısı	Katılımcı Sayısı
Söylemez ancak Yapar	5	5
Söylemez ve Yapmaz	13	130
Söyler ve Yapar	23	23
Söyler ancak Yapmaz	260	260

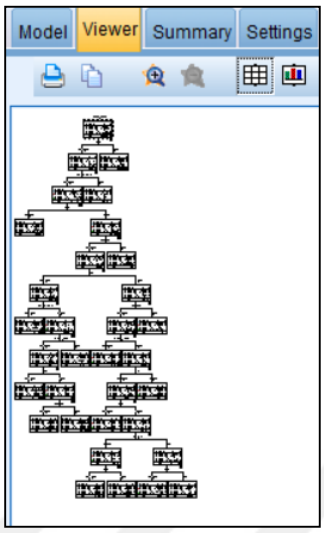
Tablo 65 üzerindeki verilerden de anlaşılacağı üzere bu durum daha önce de bahsedildiği gibi gerçek hayatta sıklıkla karşılaşılacak aşırı oranda dengelenmemiş bir veri seti örneğidir. "Virüs temizleme, casus yazılım önleme vb. Programları kullanırım" davranışı için "söyler ancak yapmaz" sonucunun tüm katılımcıların yaklaşık olarak %87'sini oluşturduğu göstermektedir. Veri setinin dengelenmemiş şekli herhangi bir karar ağacı oluşturulamamaktadır. Veri seti üzerinde dengeleme işlemi yapıldıktan sonra makine öğrenme algoritması işe koşulduğunda ortaya çıkan karar ağacının karışıklık matris değerleri Şekil 61 üzerinde gösterilmiştir.



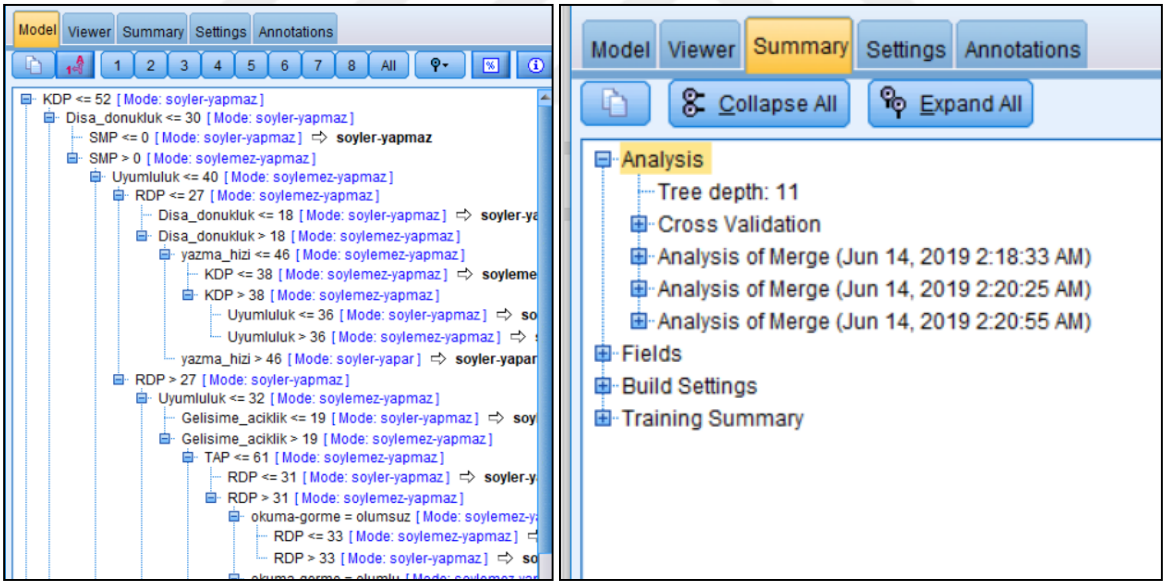
Şekil 61. Dengeleme işlemi yapılmış veri seti için karar ağacı karışıklık matrisi

Karışıklık matrisleri incelendiğinde hedef davranış için dengeleme işlemi yapılmış veri seti üzerinde koşulan karar ağacının doğruluk değerinin yüksek olmasına bakılmaksızın, "söylemez ancak yapar" ve "söyler ve yapar" sınıflarında gerçekleştirilen tahminlerin başarılı olmadığı görülmektedir. Ancak "söylemez ancak yapar" ve "söyler ve yapar" sınıflandırmalarının birbirleri arasında geçişlerin olmadığı, her iki sınıf içerisinde yanlış tahmin edilen katılımcıların yanlış-pozitif bir sonuçla "yapmaz" sınıflarından birine dâhil edildiği için tez kapsamında tasarlanacak çevrimiçi eğitim ortamında dengelenmiş veri seti üzerinde işe koşulan karar ağacı kural setinin kullanılmasına karar verilmiştir.

C5.0 algoritması kullanılarak oluşturulan model ile ilgili davranış için oluşturulan karar ağacı Şekil 62'de, hangi değişkenlerin hangi diğer değişkenle ilişkili olarak sınıflandırma işleminde kullanıldığı, hangi değişkenlerin hangi parametreler doğrultusunda karar ağacı dallanmasında etkili oldukları kesit olarak Şekil 63'te gösterilmiştir.



Şekil 62. "Virüs temizleme, casus yazılım önleme vb. Programları kullanırım" davranışı için oluşturulan karar ağacı görüntüsü



Şekil 63. "Virüs temizleme, casus yazılım önleme vb. Programları kullanırım" davranışı için oluşturulan karar ağacı değerleri

Şekil 63'te belirtildiği üzere "Virüs temizleme, casus yazılım önleme vb. Programları kullanırım" davranışı için oluşturulan karar ağacı 11 katman derinliğindedir ve karar ağacını oluşturan kural setinin bir bölümünü göstermektedir. Kişisel bilgi güvenliği özellikleri arasında yer alan "Korumacı Davranış Puanı" özniteliği kök düğüm olarak belirlenmiştir ve dallanma bu öznitelikten oluşturulmaya başlanmıştır.

“Virüs temizleme, casus yazılım önleme vb. Programları kullanırım” davranışı için bir önceki aşamada gerçekleştirilen klasik istatistiki yöntemlerle belirlenen ilişkili öznitelikler ile C5.0 algoritması kullanılarak oluşturulan karar ağacında belirlenen ilişkili değişkenlerin karşılaştırılması Tablo 66 üzerinde sunulmuş, davranış için oluşturulan kural seti EK 12’de sunulmuştur.

Tablo 66

“Virüs temizleme, casus yazılım önleme vb. Programları kullanırım” Davranışı için Öznitelik Karşılaştırması

C5.0 Algoritması – İlişkili Öznitelikler – (Dengelenmiş veri seti)	C5.0 Algoritması – İlişkili Öznitelikler – (Dengelenmemiş veri seti)	Klasik İstatistiki Yöntemler – İlişkili Öznitelikler
- Riskli Davranış Puanı - Korumacı Davranış Puanı - Tehlike Algısı Puanı - Suça Maruziyet Puanı - Uyumluluk Puanı - Dışa Dönüklük Puanı - Gelişime Açıklık Puanı - Okuduğunu Görme - Yazma Hızı	- Dengelenmemiş veri seti üzerinde herhangi bir karar ağacı oluşmamaktadır.	- Riskli Davranış Puanı - Okuduğunu Görme

Davranış -5: Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim.

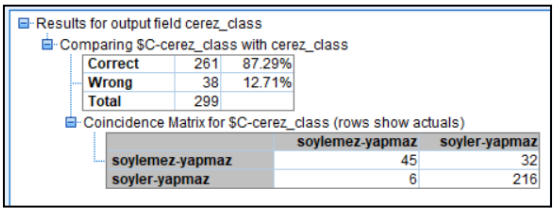
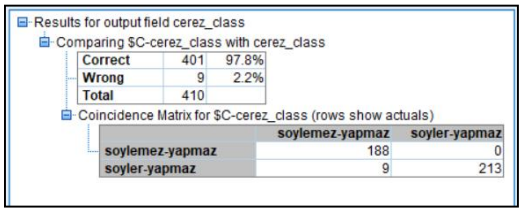
Sınıflandırma yapılacak hedef öznitelik için katılımcı dağılımı incelenmiştir. Bu aşama daha önce açıklanan dengelenmemiş veri seti hakkında bilgi edinmek ve bir dengeleme işlemine gerek olup olmadığına karar vermek için işletilmektedir. Dengelenmemiş veri seti üzerinde anlaşılacağı gibi “söylemez ancak yapar” ve “söyler ve yapar” sınıfları sadece bir örnek içermekte olduğundan budama işlemi yapılmış ve modelleme işlemine dâhil edilmemiştir. “Söylemez ve yapmaz” sınıfı üzerinde dengeleme işlemi yapılarak veri seti genişletilmiştir. Yapılan işlemler sonucu modelleme işlemine dâhil edilerek sınıf ve veri sayıları Tablo 67 üzerinde gösterilmiştir.

Tablo 67

Hedef Davranış-5 İçin Katılımcı Sayıları

Hedef Değişken	Dengelenmemiş Veri Seti Katılımcı Sayısı	Dengeleme İşlemi Yapılmış Veri Seti Katılımcı Sayısı
Söylemez ancak Yapar	1	-
Söylemez ve Yapmaz	77	188
Söyler ve Yapar	1	1
Söyler ancak Yapmaz	222	222

Tablo 67 üzerindeki verilerden de anlaşılacağı üzere bu durum daha önce de bahsedildiği gibi gerçek hayatta sıklıkla karşılaşılacak aşırı oranda dengelenmemiş 4 sınıflı bir veri seti örneğidir. "Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim" davranışı için "söylemez ve yapmaz" ve "söyler ancak yapmaz" sınıfları baz alındığında ise aşırı oranda dengelenmemiş veri setinden bahsetmek mümkün değildir. Veri setinin dengelenmemiş şekli ile dengeleme işlemi yapıldıktan sonra makine öğrenme algoritması işe koşulduğunda ortaya çıkan karar ağaçlarının karışıklık matris değerleri Şekil 64 üzerinde gösterilmiştir.

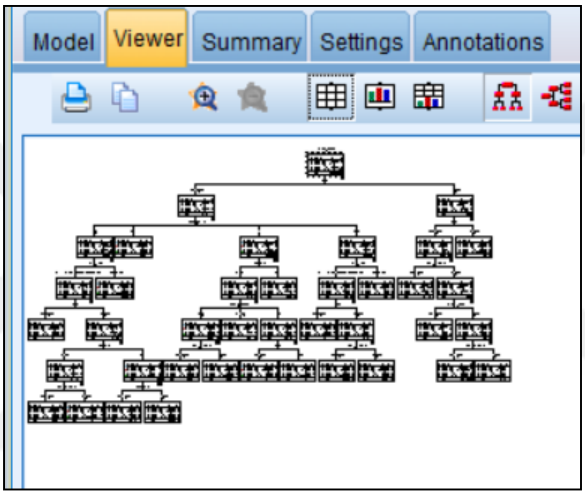
Dengeleme işlemi Yapılmamış Veri Seti için Karışıklık Matrisi	**Dengeleme İşlemi Yapılmış Veri Seti için Karışıklık Matrisi**
	

Şekil 64. Dengeleme işlemi yapılmış ve yapılmamış veri setleri için karar ağacı karışıklık matrisleri

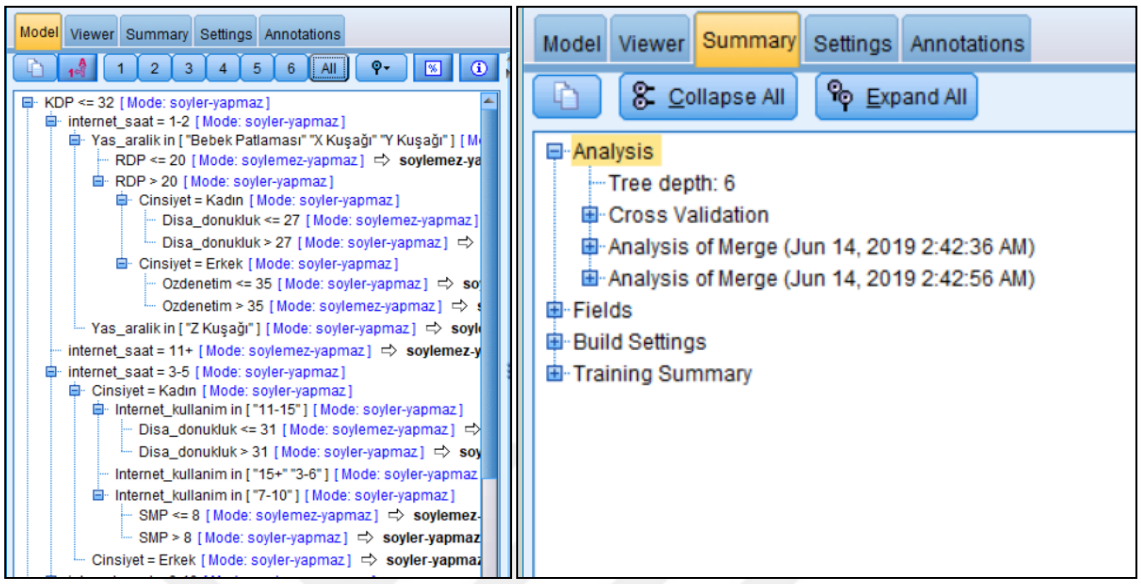
Karışıklık matrisleri ayrı ayrı incelendiğinde hedef davranış için dengeleme işlemi yapılmış veri seti üzerinde koşulan karar ağacının doğruluk değerinin yüksek olmasına bakılmaksızın, "söylemez ve yapmaz" sınıfında gerçekleştirilen tahminlerin fazla-uydurma ve ayrıca "söylemez ve yapmaz" sınıfında fazla uydurma probleminin olmasının yanı sıra "söyler ancak yapmaz" sınıfındaki tahmin oranının dengeleme işlemi yapılmamış veri seti üzerinde koşulan karar ağacından daha düşük olması sebebiyle tez kapsamında tasarlanan çevrimiçi eğitim

ortamında dengeleme işlemi yapılmamış veri seti üzerinde işe koşulan karar ağacı kural setinin kullanılmasına karar verilmiştir.

C5.0 algoritması kullanılarak oluşturulan model ile ilgili davranış için oluşturulan karar ağacı Şekil 65'te, hangi değişkenlerin hangi diğer değişkenle ilişkili olarak sınıflandırma işleminde kullanıldığı, hangi değişkenlerin hangi parametreler doğrultusunda karar ağacı dallanmasında etkili oldukları kesit olarak Şekil 66'da gösterilmiştir.



Şekil 65. "Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim" davranışı için oluşturulan karar ağacı görüntüsü



Şekil 66. "Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim." davranışı için oluşturulan karar ağacı değerleri

Şekil 66'da belirtildiği üzere "Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim" davranışı için oluşturulan karar ağacı 6 katman derinliğindedir ve karar ağacını oluşturan kural setinin bir bölümünü göstermektedir. Kişisel bilgi güvenliği özellikleri arasında yer alan "Korumacı Davranış Puanı" özniteliği kök düğüm olarak belirlenmiştir ve dallanma bu öznitelikten oluşturulmaya başlanmıştır.

"Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim" davranışı için bir önceki aşamada gerçekleştirilen klasik istatistiki yöntemlerle belirlenen ilişkili öznitelikler ile C5.0 algoritması kullanılarak oluşturulan karar ağacında belirlenen ilişkili değişkenlerin karşılaştırılması Tablo 68 üzerinde sunulmuş, davranış için oluşturulan kural seti EK 12'de sunulmuştur.

Tablo 68

"Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim" Davranışı için Öznitelik Karşılaştırması

C5.0 Algoritması – İlişkili Öznitelikler – (Dengelenmiş veri seti)	C5.0 Algoritması – İlişkili Öznitelikler – (Dengelenmemiş veri seti)	Klasik İstatistiki Yöntemler – İlişkili Öznitelikler
- Eğitim Düzeyi	- Cinsiyet	- Korumacı Davranış Puanı
- Yaş Aralığı	- Yaş Aralığı	
- Riskli Davranış Puanı	- Riskli Davranış Puanı	
- Korumacı Davranış Puanı	- Korumacı Davranış Puanı	
- Tehlike Algısı Puanı	- Suça Maruziyet Puanı	
- Suça Maruziyet Puanı	- Özdenetim Puanı	
- Gelişime Açıklık Puanı	- Dışa Dönüklük Puanı	
- Özdenetim Puanı	- İKY	
- Dışa Dönüklük Puanı	- GİKS	
- Uyumluluk Puanı	- Yazma Hızı	
- İKY		
- GİKS		
- Okuduğunu Görme		
- Yazma Hızı		

Davranış-6: Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim

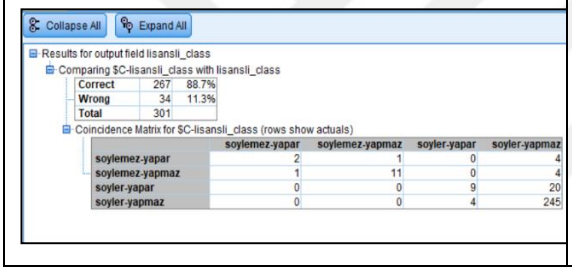
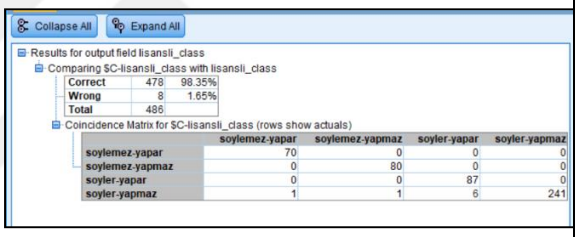
Sınıflandırma yapılacak hedef öznitelik için katılımcı dağılımı incelenmiştir. Bu aşama daha önce açıklanan dengelenmemiş veri seti hakkında bilgi edinmek ve bir dengeleme işlemine gerek olup olmadığına karar vermek için işletilmektedir. "Söylemez ancak yapar", "söylemez ve yapmaz" ve "söyler ve yapar" sınıfları üzerinde dengeleme işlemi yapılarak veri seti genişletilmiştir. Yapılan işlemler sonucu modelleme işlemine dâhil edilecek sınıf ve veri sayıları Tablo 69 üzerinde gösterilmiştir.

Tablo 69

Hedef Davranş-6 İçin Katılımcı Sayıları

	Dengelenmemiş Veri Seti	Dengeleme İşlemi Yapılmış Veri Seti
Hedef Değişken	Katılımcı Sayısı	Katılımcı Sayısı
Söylemez ancak Yapar	7	70
Söylemez ve Yapmaz	16	80
Söyler ve Yapar	29	87
Söyler ancak Yapmaz	249	222

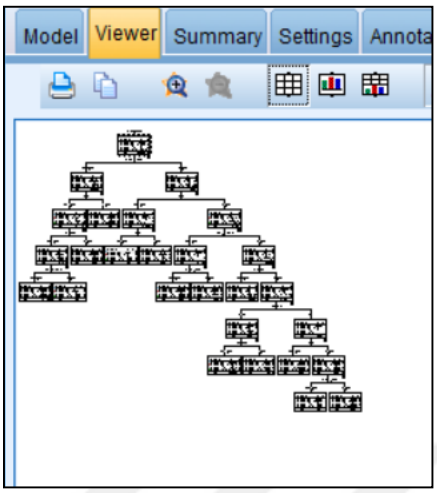
Tablo 69 üzerindeki verilerden de anlaşılacağı üzere bu durum daha önce de bahsedildiği gibi gerçek hayatta sıklıkla karşılaşılacak aşırı oranda dengelenmemiş 4 sınıflı bir veri seti örneğidir. "Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim" davranışı için "söyler ve yapar", "söylemez ve yapmaz" ve "söyler ancak yapmaz" sınıfları baz alındığında ise aşırı oranda dengelenmemiş veri setinden bahsetmek mümkün değildir. Veri setinin dengelenmemiş şekli ile dengeleme işlemi yapıldıktan sonra makine öğrenme algoritması işe koşulduğunda ortaya çıkan karar ağaçlarının karışıklık matris değerleri Şekil 67 üzerinde gösterilmiştir.

Dengeleme işlemi Yapılmamış Veri Seti için Karışıklık Matrisi	**Dengeleme İşlemi Yapılmış Veri Seti için Karışıklık Matrisi**
	

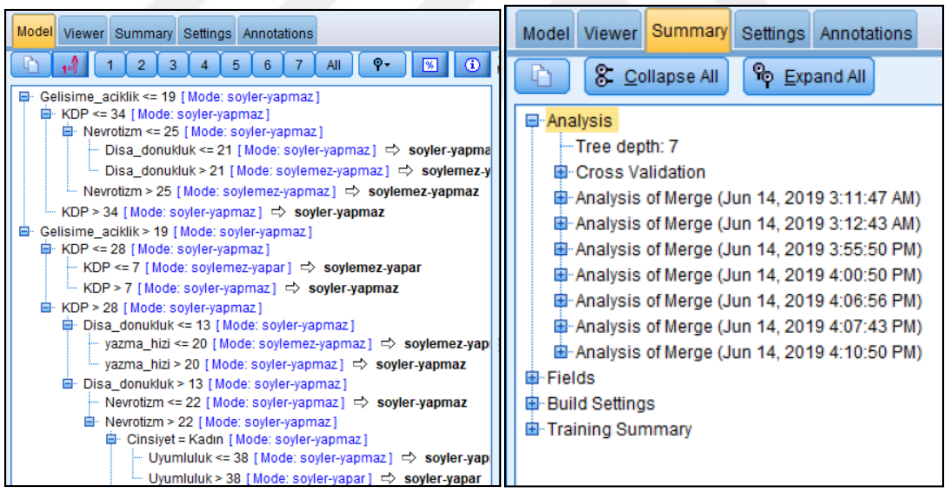
Şekil 67. Dengeleme işlemi yapılmış ve yapılmamış veri setleri için karar ağacı karışıklık matrisleri

Karışıklık matrisleri ayrı ayrı incelendiğinde hedef davranış için dengeleme işlemi yapılmış veri seti üzerinde koşulan karar ağacının doğruluk değerinin yüksek olmasına bakılmaksızın, dengeleme işlemi gerçekleştirilmiş olan sınıflarında gerçekleştirilen tahminlerin fazla-uydurma problemlerinin olması ayrıca dengeleme işlemi yapılmadan yapılan doğru-doğru (true-true) ve yanlış-yanlış (false-false) tahminlerin başarısı sebebiyle tez kapsamında tasarlanacak çevrimiçi eğitim ortamında dengeleme işlemi yapılmamış veri seti üzerinde işe koşulan karar ağacı kural setinin kullanılmasına karar verilmiştir.

C5.0 algoritması kullanılarak oluşturulan model ile ilgili davranış için oluşturulan karar ağacı Şekil 68'de, hangi değişkenlerin hangi diğer değişkenle ilişkili olarak sınıflandırma işleminde kullanıldığı, hangi değişkenlerin hangi parametreler doğrultusunda karar ağacı dallanmasında etkili oldukları kesit olarak Şekil 69'da gösterilmiştir.



Şekil 68. "Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim." davranışı için oluşturulan karar ağacı görüntüsü



Şekil 69. "Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim." davranışı için oluşturulan karar ağacı değerleri

Şekil 69'da belirtildiği üzere "Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim" davranışı için oluşturulan karar ağacı 7 katman derinliğindedir ve karar ağacını oluşturan kural setinin bir bölümünü göstermektedir. Kişilik özellikleri arasında yer alan "Gelişime Açıklık Puanı" özniteliği kök düğüm olarak belirlenmiştir ve dallanma bu öznitelikten oluşturulmaya başlanmıştır.

“Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim” davranışı için bir önceki aşamada gerçekleştirilen klasik istatistiki yöntemlerle belirlenen ilişkili öznitelikler ile C5.0 algoritması kullanılarak oluşturulan karar ağacında belirlenen ilişkili değişkenlerin karşılaştırılması Tablo 70 üzerinde sunulmuş, davranış için oluşturulan kural seti EK 12’de sunulmuştur:

Tablo 70

“Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim” Davranışı için Öznitelik Karşılaştırması

C5.0 Algoritması – İlişkili Öznitelikler – (Dengelenmiş veri seti)	C5.0 Algoritması – İlişkili Öznitelikler – (Dengelenmemiş veri seti)	Klasik İstatistiki Yöntemler – İlişkili Öznitelikler
- Eğitim Düzeyi - Cinsiyet - Yaş Aralığı - Riskli Davranış Puanı - Korumacı Davranış Puanı - Tehlike Algısı Puanı - Suça Maruziyet Puanı - Gelişime Açıklık Puanı - Özdenetim Puanı - Nevrotizm Puanı - Dışa Dönüklük Puanı - Uyumluluk Puanı - İnternet Kullanım Yılı - İnternet Kullanım Saati - Okuduğunu Görme Yazma Hızı	- Cinsiyet - Riskli Davranış Puanı - Korumacı Davranış Puanı - Dışa Dönüklük Puanı - Nevrotizm Puanı - Uyumluluk Puanı - Gelişime Açıklık Puanı - Cinsiyet Yazma Hızı	- Korumacı Davranış Puanı - Gelişime Açıklık Puanı - Özdenetim Puanı - Nevrotizm Puanı - Dışa Dönüklük Puanı - Uyumluluk Puanı

Davranış-7: Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim

Sınıflandırma yapılacak hedef öznitelik için katılımcı dağılımı incelenmiştir. Bu aşama daha önce açıklanan dengelenmemiş veri seti hakkında bilgi edinmek ve bir dengeleme işlemine gerek olup olmadığına karar vermek için işletilmektedir. Hedef davranış için kullanılacak olan veri seti sınıflarına ait katılımcı sayıları Tablo 71 üzerinde gösterilmiştir.

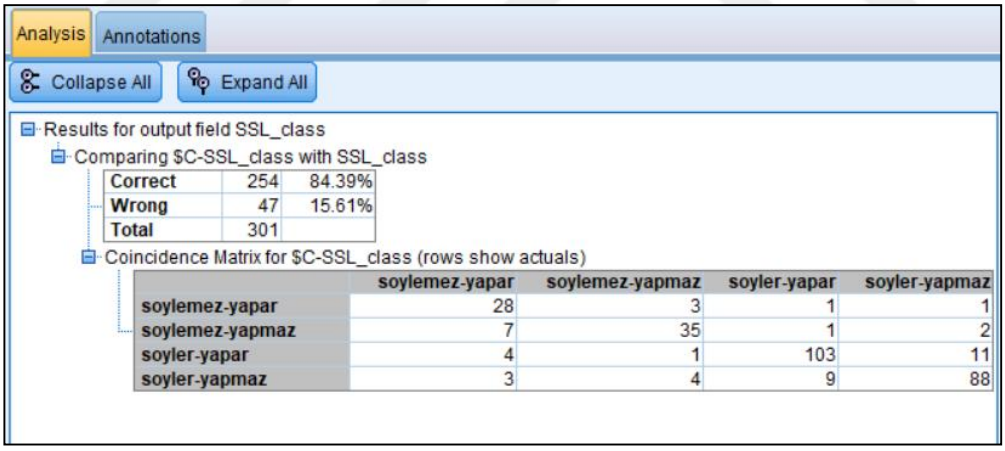
Tablo 71

Hedef Davranış-7 İçin Katılımcı Sayıları

Hedef Değişken	Dengelenmemiş Veri Seti Katılımcı Sayısı	Dengeleme İşlemi Yapılmış Veri Seti Katılımcı Sayısı
Söylemez ancak Yapar	33	-
Söylemez ve Yapmaz	45	-
Söyler ve Yapar	119	-
Söyler ancak Yapmaz	104	-

Tablo 71 üzerindeki verilerden de anlaşılacağı üzere aşırı oranda dengelenmemiş sorununun olmadığı 4 sınıflı bir veri seti örneğidir. Veri setinin dengelenmemiş şekli ile makine öğrenme algoritması işe koşulduğunda ortaya çıkan karar ağaçlarının karışıklık matris değeri Şekil 70 üzerinde gösterilmiştir.

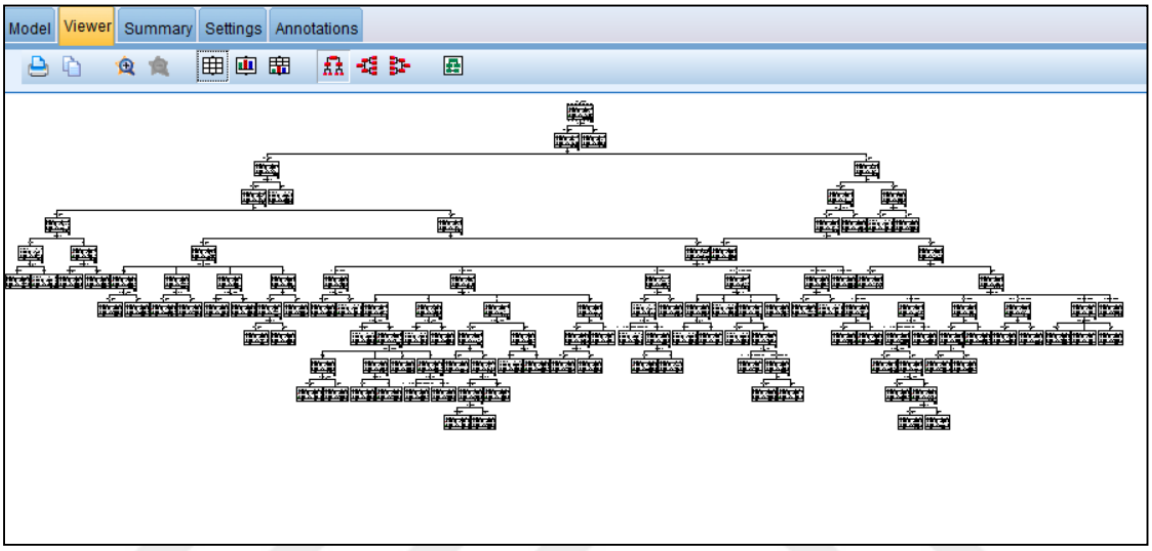
Dengeleme işlemi Yapılmamış Veri Seti için Karışıklık Matrisi



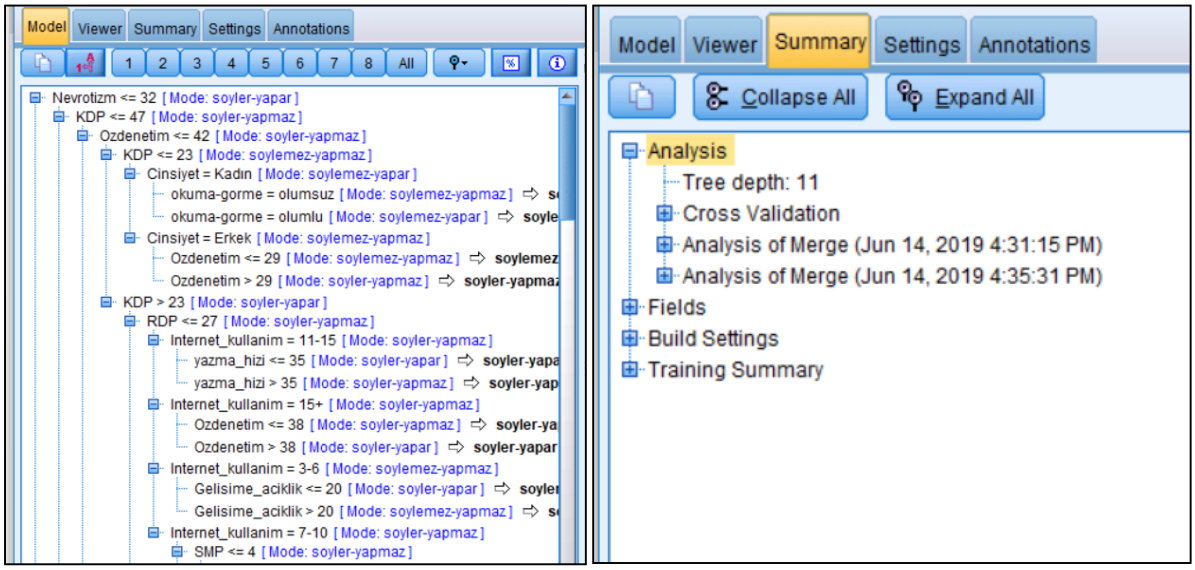
Şekil 70. Dengeleme işlemi yapılmamış veri seti için karar ağacı karışıklık matrisi

Karışıklık matrisi incelendiğinde hedef davranış için dengeleme işlemi yapılmamış veri seti üzerinde koşulan karar ağacının doğruluk değerinin %84.39 olduğu, gerçekleştirilen tahminlerin fazla-uydurma probleminin olmadığı ayrıca yapılan doğru-doğru (true-true) ve yanlış-yanlış (false-false) tahminlerin başarılı olduğunun görülmesi sebebiyle tez kapsamında tasarlanacak çevrimiçi eğitim ortamında dengeleme işlemi yapılmamış veri seti üzerinde işe koşulan karar ağacı kural setinin kullanılmasına karar verilmiştir.

C5.0 algoritması kullanılarak oluşturulan model ile ilgili davranış için oluşturulan karar ağacı Şekil 71'de, hangi değişkenlerin hangi diğer değişkenle ilişkili olarak sınıflandırma işleminde kullanıldığı, hangi değişkenlerin hangi parametreler doğrultusunda karar ağacı dallanmasında etkili oldukları kesit olarak Şekil 72'de gösterilmiştir.



Şekil 71. "Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim" davranışı için oluşturulan karar ağacı görüntüsü



Şekil 72. "Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim" davranışı için oluşturulan karar ağacı değerleri

Şekil 72'de belirtildiği üzere "Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim" davranışı için oluşturulan karar ağacı 11 katman derinliğindedir ve karar ağacını oluşturan kural setinin bir bölümünü göstermektedir. Kişilik özellikleri arasında yer alan "Nevrotizm Puanı" özniteliği kök düğüm olarak belirlenmiştir ve dallanma bu öznitelikten oluşturulmaya başlanmıştır.

"Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim" davranışı için bir önceki aşamada gerçekleştirilen klasik istatistiki yöntemlerle belirlenen ilişkili öznitelikler ile C5.0 algoritması kullanılarak oluşturulan karar ağacında belirlenen ilişkili değişkenlerin karşılaştırılması Tablo 72 üzerinde sunulmuş, davranış için oluşturulan kural seti EK 12'de sunulmuştur.

Tablo 72

"Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim" Davranışı için Öznitelik Karşılaştırması

C5.0 Algoritması – İlişkili Öznitelikler – (Dengelenmiş veri seti)	C5.0 Algoritması – İlişkili Öznitelikler – (Dengelenmemiş veri seti)	Klasik İstatistiki Yöntemler – İlişkili Öznitelikler
- Hedef veri seti üzerinde dengeleme işlemi yapılmamıştır.	- Eğitim Düzeyi - Cinsiyet - Yaş Aralığı - Riskli Davranış Puanı - Korumacı Davranış Puanı - Tehlike Algısı Puanı - Suça Maruziyet Puanı - Gelişime Açıklık Puanı - Özdenetim Puanı - Nevrotizm Puanı - Dışa Dönüklük Puanı - Uyumluluk Puanı - İKY - GİKS - Okuduğunu Görme Yazma Hızı	- Korumacı Davranış Puanı - Tehlike Algısı Puanı - Özdenetim Puanı - Nevrotizm Puanı - Uyumluluk Puanı

Davranış-8: Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım

Sınıflandırma yapılacak hedef öznitelik için katılımcı dağılımı incelenmiştir. Bu aşama daha önce açıklanan dengelenmemiş veri seti hakkında bilgi edinmek ve bir dengeleme işlemine

gerek olup olmadığına karar vermek için işletilmektedir. Tablo 73 üzerinde gösterildiği gibi "söyler ve yapar" sınıfında hiç katılımcı yokken "söylemez ancak yapar" sınıfında sadece bir katılımcı bulunmaktadır.

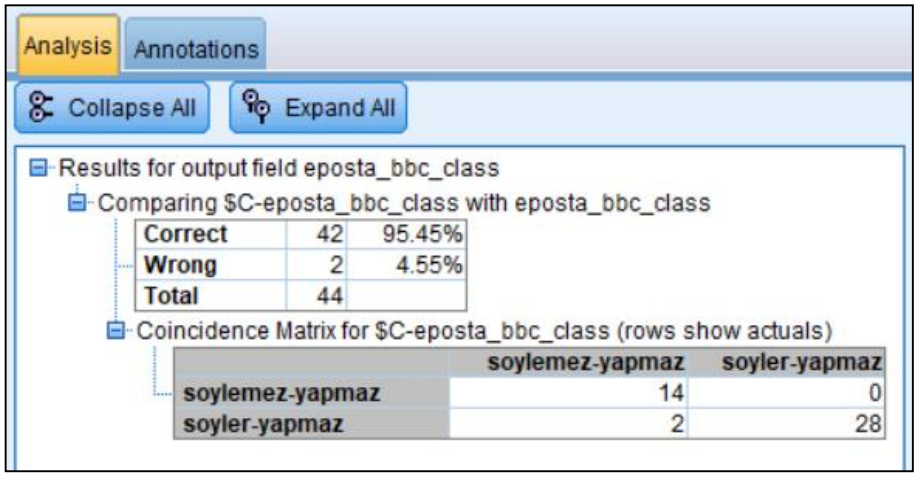
Tablo 73

Hedef Davranış-7 İçin Katılımcı Sayıları

	Dengelenmemiş Veri Seti	Dengeleme İşlemi Yapılmış Veri Seti
Hedef Değişken	Katılımcı Sayısı	Katılımcı Sayısı
Söylemez ancak Yapar	1	-
Söylemez ve Yapmaz	14	14
Söyler ve Yapar	-	-
Söyler ancak Yapmaz	30	30

Tablo 73 üzerindeki verilerden de anlaşılacağı üzere "Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım" davranışı için "söylemez ve yapmaz" ve "söyler ancak yapmaz" sınıfları baz alındığında ise aşırı oranda dengelenmemiş veri setinden bahsetmek mümkün değildir. Ancak sınıfların veri sayılarına bakıldığında büyük veri olarak adlandırılabilecek bir veri seti de yoktur. Bu sebeple "söylemez ancak yapar" sınıfı da analizden çıkarılarak sonuçlar incelenmeye çalışılmıştır (Şekil 73).

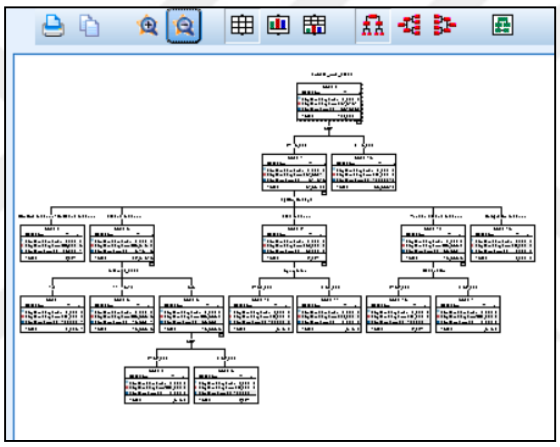
Dengeleme işlemi Yapılmamış Veri Seti için Karışıklık Matrisi



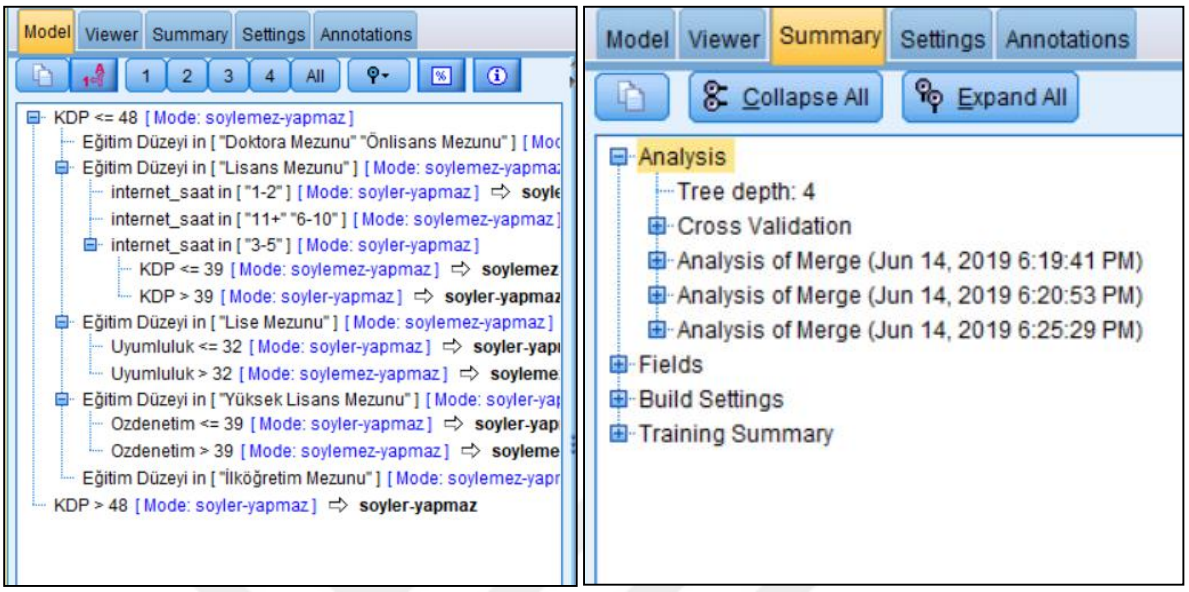
Şekil 73. Dengeleme işlemi yapılmış ve yapılmamış veri setleri için karar ağacı karışıklık matrisleri

Karışıklık matrisi incelendiğinde hedef davranış için veri seti üzerinde koşulan karar ağacının doğruluk değerinin yüksek olduğu, yapılan doğru-doğru (true-true) ve yanlış-yanlış (false-false) tahminlerin başarısı sebebiyle tez kapsamında tasarlanacak çevrimiçi eğitim ortamında işe koşulan karar ağacı kural setinin kullanılmasına karar verilmiştir.

C5.0 algoritması kullanılarak oluşturulan model ile ilgili davranış için oluşturulan karar ağacı Şekil 74'te, hangi değişkenlerin hangi diğer değişkenle ilişkili olarak sınıflandırma işleminde kullanıldığı, hangi değişkenlerin hangi parametreler doğrultusunda karar ağacı dallanmasında etkili oldukları kesit olarak Şekil 75'te gösterilmiştir.



Şekil 74. "Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım" davranışı için oluşturulan karar ağacı görüntüsü



Şekil 75. "Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım" davranışı için oluşturulan karar ağacı değerleri

Şekil 75'te belirtildiği üzere "Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım" davranışı için oluşturulan karar ağacı 4 katman derinliğindedir ve karar ağacını oluşturan kural setinin bir bölümünü göstermektedir. Kişisel bilgi güvenliği özellikleri arasında yer alan "Korumacı Puanı" özniteliği kök düğüm olarak belirlenmiştir ve dallanma bu öznitelikten oluşturulmaya başlanmıştır.

"Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım" davranışı için bir önceki aşamada gerçekleştirilen klasik istatistiki yöntemlerle belirlenen ilişkili öznitelikler ile C5.0 algoritması kullanılarak oluşturulan karar ağacında belirlenen ilişkili değişkenlerin karşılaştırılması Tablo 74 üzerinde sunulmuş, davranış için oluşturulan kural seti EK 12'de sunulmuştur.

Tablo 74

"Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım" Davranışı için Öznitelik Karşılaştırması

C5.0 Algoritması – İlişkili Öznitelikler – (Dengelenmiş veri seti)	C5.0 Algoritması – İlişkili Öznitelikler – (Dengelenmemiş veri seti)	Klasik İstatistiki Yöntemler – İlişkili Öznitelikler
- Veri üzerinde dengeleme işlemine ihtiyaç duyulmamıştır.	- Korumacı Davranış Puanı - Eğitim Düzeyi - İnternet Kullanım Saati - Uyumluluk Puanı - Özdenetim Puanı	- Korumacı Davranış Puanı

Bu aşamadan sonra C5.0 algoritması kullanılarak yapılan olan sınıflandırmalar "Riskli davranışlar" adı altında değerlendirilen davranışlardır. Burada "söyler ancak yapmaz" katılımcının olumlu davranışı gösterdiğini beyan ettiğini ancak olumlu davranışı göstermediğini; "söyler ve yapar" katılımcının olumlu davranışı gösterdiğini beyan ettiğini ve olumlu davranışı göstermediğini; "söylemez ancak yapar" katılımcının olumlu davranışı göstermediğini beyan ettiğini ancak olumlu davranışı gösterdiğini; "söylemez ve yapmaz" katılımcının olumlu davranışı göstermediğini beyan ettiğini ve olumlu davranışı göstermediğini bildirmektedir.

Davranış-9: Kurumsal e-posta adresimi günlük işlerde de kullanırım

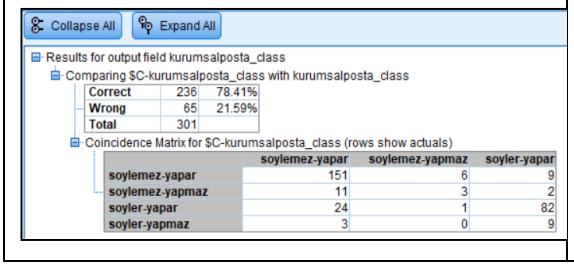
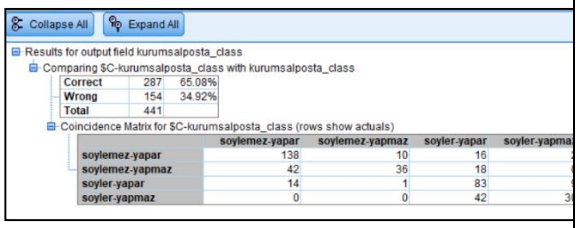
Sınıflandırma yapılacak hedef öznitelik için katılımcı dağılımı incelenmiştir. Bu aşama daha önce açıklanan dengelenmemiş veri seti hakkında bilgi edinmek ve bir dengeleme işlemine gerek olup olmadığına karar vermek için işletilmektedir. "Söyler ancak yapmaz" ve "söylemez ve yapmaz" sınıfları üzerinde dengeleme işlemi yapılarak veri seti genişletilmiştir. Yapılan işlemler sonucu modelleme işlemine dâhil edilecek sınıf ve veri sayıları Tablo 75 üzerinde gösterilmiştir.

Tablo 75

Hedef Davranış-9 İçin Katılımcı Sayıları

Hedef Değişken	Dengelenmemiş Veri Seti Katılımcı Sayısı	Dengeleme İşlemi Yapılmış Veri Seti Katılımcı Sayısı
Söylemez ancak Yapar	166	166
Söylemez ve Yapmaz	16	96
Söyler ve Yapar	107	107
Söyler ancak yapmaz	12	72

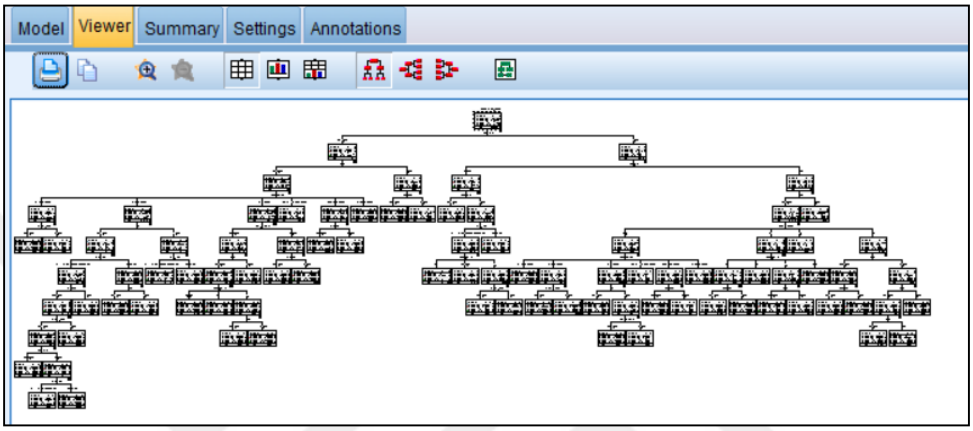
Tablo 75 üzerindeki verilerden de anlaşılacağı üzere bu ikişer sınıf kendi aralarında dengelenmiş veri sayılarına sahipken 4 sınıfın birbiri arasında dengelenmemiş veri sayılarından olduğu görünmektedir "Kurumsal e-posta adresimi günlük işlerde de kullanırım" riskli davranışı için veri setinin dengelenmemiş şekli ile dengeleme işlemi yapıldıktan sonra makine öğrenme algoritması işe koşulduğunda ortaya çıkan karar ağaçlarının karışıklık matris değerleri Şekil 76 üzerinde gösterilmiştir.

Dengeleme işlemi Yapılmamış Veri Seti için Karışıklık Matrisi	**Dengeleme İşlemi Yapılmış Veri Seti için Karışıklık Matrisi**
	

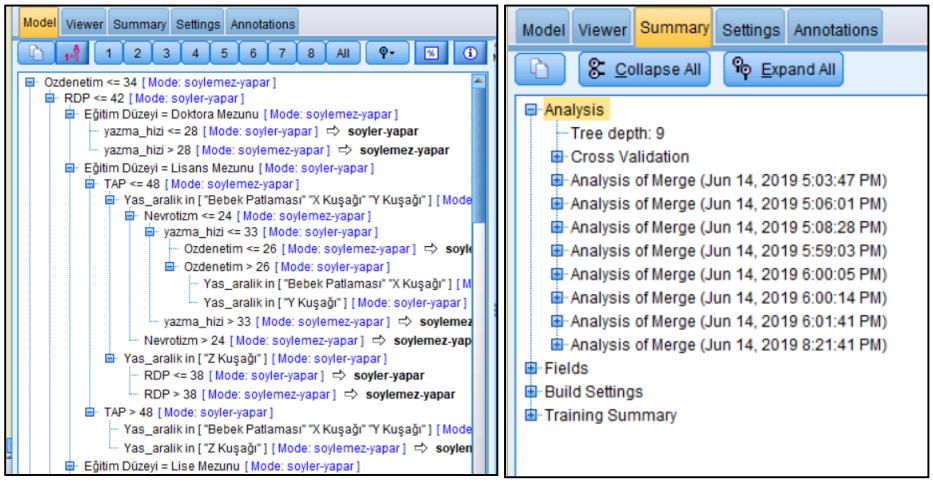
Şekil 76. Dengeleme işlemi yapılmış ve yapılmamış veri setleri için karar ağacı karışıklık matrisleri

Karışıklık matrisleri ayrı ayrı incelendiğinde hedef davranış için dengeleme işlemi yapılmış veri seti üzerinde koşulan karar ağacının doğruluk değerinin düşük çıkması ve dengeleme işlemi yapılmadan yapılan doğru-doğru (true-true) ve yanlış-yanlış (false-false) tahminlerin başarısı sebebiyle tez kapsamında tasarlanan çevrimiçi eğitim ortamında dengeleme işlemi yapılmamış veri seti üzerinde işe koşulan karar ağacı kural setinin kullanılmasına karar verilmiştir.

C5.0 algoritması kullanılarak oluşturulan model ile ilgili davranış için oluşturulan karar ağacı Şekil 77'de, hangi değişkenlerin hangi diğer değişkenle ilişkili olarak sınıflandırma işleminde kullanıldığı, hangi değişkenlerin hangi parametreler doğrultusunda karar ağacı dallanmasında etkili oldukları kesit olarak Şekil 78'de gösterilmiştir.



Şekil 77. "Kurumsal e-posta adresimi günlük işlerde de kullanırım" davranışı için oluşturulan karar ağacı görüntüsü



Şekil 78. "Kurumsal e-posta adresimi günlük işlerde de kullanırım" davranışı için oluşturulan karar ağacı değerleri

Şekil 78'de belirtildiği üzere "Kurumsal e-posta adresimi günlük işlerde de kullanırım" davranışı için oluşturulan karar ağacı 9 katman derinliğindedir ve karar ağacını oluşturan kural setinin bir bölümünü göstermektedir. Kişilik özellikleri arasında yer alan "Özdenetim Puanı"

özniteliği kök düğüm olarak belirlenmiştir ve dallanma bu öznitelikten oluşturulmaya başlanmıştır.

"Kurumsal e-posta adresimi günlük işlerde de kullanırım" davranışı için bir önceki aşamada gerçekleştirilen klasik istatistiki yöntemlerle belirlenen ilişkili öznitelikler ile C5.0 algoritması kullanılarak oluşturulan karar ağacında belirlenen ilişkili değişkenlerin karşılaştırılması Tablo 76 üzerinde sunulmuş davranışı için oluşturulan kural seti EK 12'de sunulmuştur.

Tablo 76

"Kurumsal e-posta adresimi günlük işlerde de kullanırım" Davranışı için Öznitelik Karşılaştırması

C5.0 Algoritması – İlişkili Öznitelikler – (Dengeleme işlemi yapılmış veri seti)	C5.0 Algoritması – İlişkili Öznitelikler – (Dengelenmemiş veri seti)	Klasik İstatistiki Yöntemler – İlişkili Öznitelikler
- Eğitim Düzeyi - Cinsiyet - Yaş Aralığı - Riskli Davranış Puanı - Korumacı Davranış Puanı - Tehlike Algısı Puanı - Suça Maruziyet Puanı - Gelişime Açıklık Puanı - Özdenetim Puanı - Nevrotizm Puanı - Dışa Dönüklük Puanı - Uyumluluk Puanı - İKY - GİKS - Okuduğunu Görme - Yazma Hızı	- Eğitim Düzeyi - Yaş Aralığı - Riskli Davranış Puanı - Korumacı Davranış Puanı - Tehlike Algısı Puanı - Gelişime Açıklık Puanı - Özdenetim Puanı - Nevrotizm Puanı - Dışa Dönüklük Puanı - Uyumluluk Puanı - İKY - GİKS - Okuduğunu Görme - Yazma Hızı	- Korumacı Davranış Puanı - Tehlike Algısı Puanı - Gelişime Açıklık Puanı - Özdenetim Puanı - Dışa Dönüklük Puanı - Okuduğunu Görme

Davranış-10: İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım

Sınıflandırma yapılacak hedef öznitelik için katılımcı dağılımı incelenmiştir. Bu aşama daha önce açıklanan dengelenmemiş veri seti hakkında bilgi edinmek ve bir dengeleme işlemine gerek olup olmadığına karar vermek için işletilmektedir. "Söyler ve yapar" ve "söyler ancak yapmaz" sınıfları üzerinde dengeleme işlemi yapılarak veri seti genişletilmiştir. Yapılan

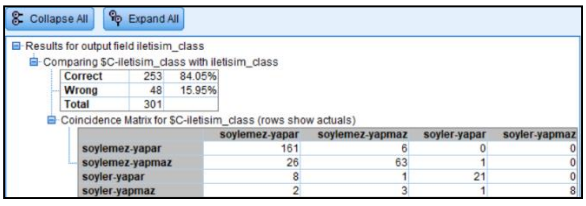
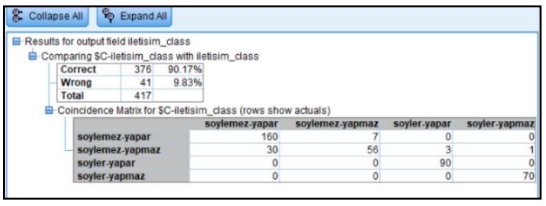
işlemler sonucu modelleme işlemine dâhil edilecek sınıf ve veri sayıları Tablo 77 üzerinde gösterilmiştir.

Tablo 77

Hedef Davranış-10 İçin Katılımcı Sayıları

	Dengelenmemiş Veri Seti	Dengeleme İşlemi Yapılmış Veri Seti
Hedef Değişken	Katılımcı Sayısı	Katılımcı Sayısı
Söylemez ancak Yapar	167	167
Söylemez ve Yapmaz	90	90
Söyler ve Yapar	30	90
Söyler ancak Yapmaz	14	70

Tablo 77 üzerindeki verilerden de anlaşılacağı üzere bu ikişer sınıf kendi aralarında dengelenmiş veri sayılarına sahipken 4 sınıfın birbiri arasında dengelenmemiş veri sayılarından olduğu görünmektedir "İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım" riskli davranışı için veri setinin dengelenmemiş şekli ile dengeleme işlemi yapıldıktan sonra makine öğrenme algoritması işe koşulduğunda ortaya çıkan karar ağaçlarının karışıklık matris değerleri Şekil 79 üzerinde gösterilmiştir.

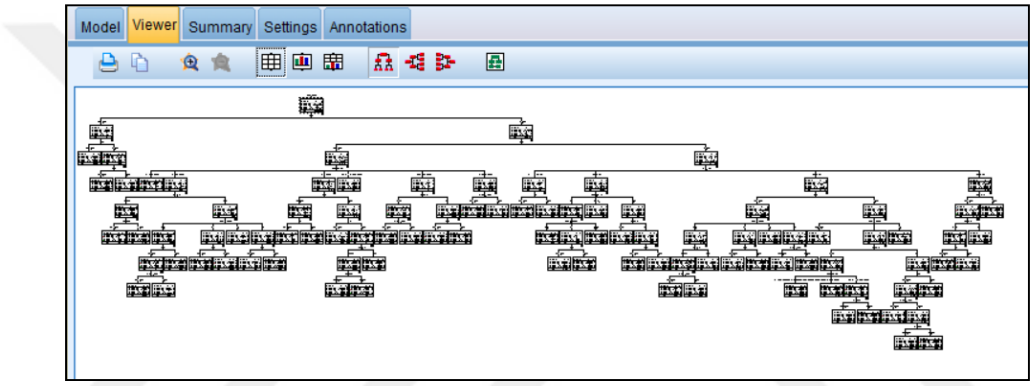
Dengeleme işlemi Yapılmamış Veri Seti için Karışıklık Matrisi	**Dengeleme İşlemi Yapılmış Veri Seti için Karışıklık Matrisi**
	

Şekil 79. Dengeleme işlemi yapılmış ve yapılmamış veri setleri için karar ağacı karışıklık matrisleri

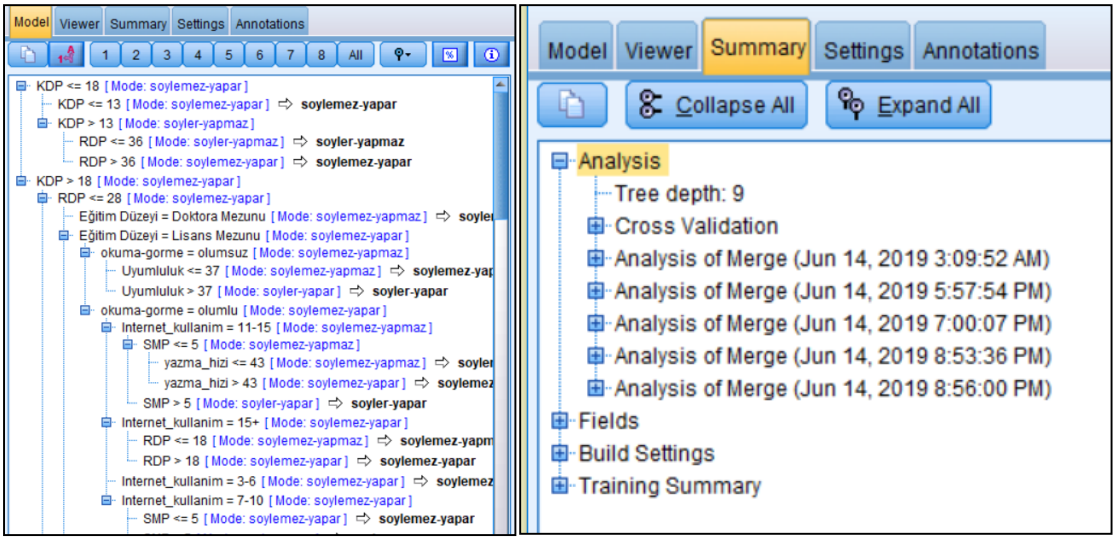
Karışıklık matrisleri ayrı ayrı incelendiğinde hedef davranış için dengeleme işlemi yapılmış veri seti üzerinde koşulan karar ağacının doğruluk değerinin yüksek olmasına bakılmaksızın, dengeleme işlemi gerçekleştirilmiş olan sınıflarında gerçekleştirilen tahminlerin fazla-uydurma problemlerinin olması ayrıca dengeleme işlemi yapılmadan yapılan doğru-doğru (true-true) ve

yanlış-yanlış (false-false) tahminlerin başarısı sebebiyle tez kapsamında tasarlanacak çevrimiçi eğitim ortamında dengeleme işlemi yapılmamış veri seti üzerinde işe koşulan karar ağacı kural setinin kullanılmasına karar verilmiştir.

C5.0 algoritması kullanılarak oluşturulan model ile ilgili davranış için oluşturulan karar ağacı Şekil 80'de, hangi değişkenlerin hangi diğer değişkenle ilişkili olarak sınıflandırma işleminde kullanıldığı, hangi değişkenlerin hangi parametreler doğrultusunda karar ağacı dallanmasında etkili oldukları kesit olarak Şekil 81'de gösterilmiştir.



Şekil 80. "İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım." davranışı için oluşturulan karar ağacı görüntüsü



Şekil 81. "İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım." davranışı için oluşturulan karar ağacı değerleri

Şekil 81'de belirtildiği üzere "İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım" riskli davranışı için oluşturulan karar ağacı 9 katman derinliğindedir ve karar ağacını oluşturan kural setinin bir bölümünü göstermektedir. Kişisel bilgi güvenliği özellikleri arasında yer alan "Korumacı Davranış Puanı" özniteliği kök düğüm olarak belirlenmiştir ve dallanma bu öznitelikten oluşturulmaya başlanmıştır.

"İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım" davranışı için bir önceki aşamada gerçekleştirilen klasik istatistiki yöntemlerle belirlenen ilişkili öznitelikler ile C5.0 algoritması kullanılarak oluşturulan karar ağacında belirlenen ilişkili değişkenlerin karşılaştırılması Tablo 78 üzerinde sunulmuş, davranış için oluşturulan kural seti EK 12'de sunulmuştur.

Tablo 78

"İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım" Davranışı için Öznitelik Karşılaştırması

C5.0 Algoritması – İlişkili Öznitelikler – (Dengeleme işlemi yapılmış veri seti)	C5.0 Algoritması – İlişkili Öznitelikler – (Dengelenmemiş veri seti)	Klasik İstatistiki Yöntemler – İlişkili Öznitelikler
- Eğitim Düzeyi	- Eğitim Düzeyi	- Eğitim Düzeyi
- Cinsiyet	- Cinsiyet	- Yaş Aralığı
- Yaş Aralığı	- Yaş Aralığı	
- Riskli Davranış Puanı	- Riskli Davranış Puanı	
- Korumacı Davranış Puanı	- Korumacı Davranış Puanı	
- Tehlike Algısı Puanı	- Tehlike Algısı Puanı	
- Suça Maruziyet Puanı	- Gelişime Açıklık Puanı	
- Gelişime Açıklık Puanı	- Özdenetim Puanı	
- Özdenetim Puanı	- Nevrotizm Puanı	
- Nevrotizm Puanı	- Dışa Dönüklük Puanı	
- Dışa Dönüklük Puanı	- Uyumluluk Puanı	
- Uyumluluk Puanı	- İKY	
- İKY	- GİKS	
- GİKS	- Okuduğunu Görme	
- Okuduğunu Görme	- Yazma Hızı	
- Yazma Hızı		

Davranış-11: İnternet ortamında gerektiği durumlarda özlük bilgilerimi (ad, soyad, doğum tarihi vb.) paylaşırım

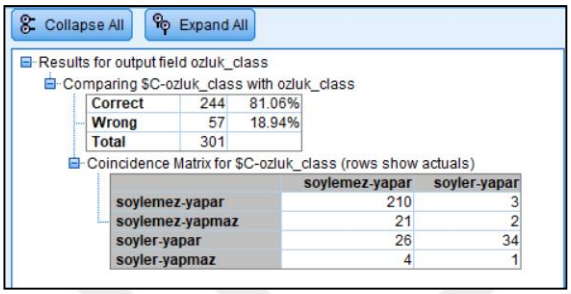
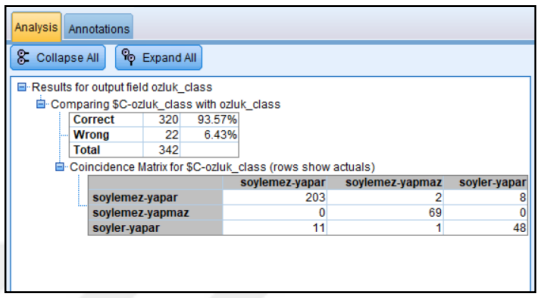
Sınıflandırma yapılacak hedef öznitelik için katılımcı dağılımı incelenmiştir. Bu aşama daha önce açıklanan dengelenmemiş veri seti hakkında bilgi edinmek ve bir dengeleme işlemine gerek olup olmadığına karar vermek için işletilmektedir. "Söyler ve yapar" ve "söyler ancak yapmaz" sınıfları üzerinde dengeleme işlemi yapılarak veri seti genişletilmiştir. Yapılan işlemler sonucu modelleme işlemine dâhil edilecek sınıf ve veri sayıları Tablo 79 üzerinde gösterilmiştir.

Tablo 79

Hedef Davranış-11 İçin Katılımcı Sayıları

	Dengelenmemiş Veri Seti	Dengeleme İşlemi Yapılmış Veri Seti
Hedef Değişken	Katılımcı Sayısı	Katılımcı Sayısı
Söylemez ancak Yapar	213	213
Söylemez ve Yapmaz	23	69
Söyler ve Yapar	60	60
Söyler ancak Yapmaz	5	-

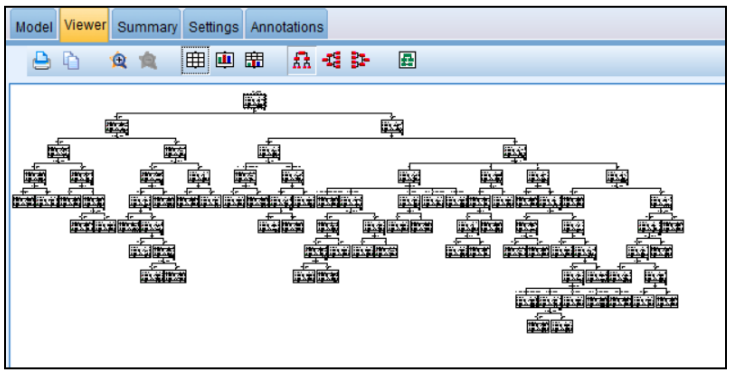
Tablo 79 üzerindeki verilerden de anlaşılacağı üzere "İnternet ortamında gerektiği durumlarda özlük bilgilerimi (ad, soyad, doğum tarihi vb.) paylaşırım" hedef davranışı için "söylemez ve yapmaz" sınıfı veri sayısında dengelem işlemi yapılmış "söyler ancak yapmaz" sınıfı ise modelleme dışı bırakılmıştır. Şekil 82 üzerinde gösterildiği üzere dengelenmemiş şekli ile makine öğrenme algoritması işe koşulduğunda "söyler ancak yapmaz" ve "söylemez ve yapmaz" sınıflarına dair herhangi bir sınıflandırma yapılamamakta ve ayrıca "söyler ve yapar" sınıfı için yaklaşık olarak %50 doğruluk oranında bir sınıflandırma yapılabilmektedir.

Dengeleme işlemi Yapılmamış Veri Seti için Karışıklık Matrisi	Dengeleme İşlemi Yapılmış Veri Seti için Karışıklık Matrisi
	

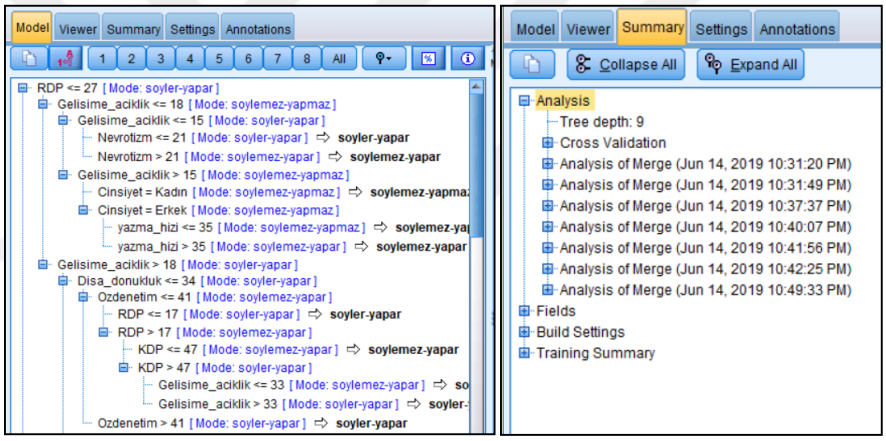
Şekil 82. Dengeleme işlemi yapılmış ve yapılmamış veri setleri için karar ağacı karışıklık matrisleri

Karışıklık matrisleri ayrı ayrı incelendiğinde hedef davranış için dengeleme işlemi yapılmış veri seti üzerinde koşulan karar ağacının doğruluk değerinin yüksek olmasına bakılmaksızın, dengeleme işlemi gerçekleştirilmiş olan sınıflarında gerçekleştirilen tahminlerin bir sınıf için fazla-uydurma probleminin olmasına rağmen, sınıfa dâhil edilecek katılımcıların yanlış-pozitif bir değerlendirme ile sadece tekrar niteliğinde bilgi alacak olması ve ayrıca dengeleme işlemi yapıldıktan sonra doğru-doğru (true-true) ve yanlış-yanlış (false-false) tahminlerin başarısı sebebiyle tez kapsamında tasarlanacak çevrimiçi eğitim ortamında dengeleme işlemi yapılmış veri seti üzerinde işe koşulan karar ağacı kural setinin kullanılmasına karar verilmiştir.

C5.0 algoritması kullanılarak oluşturulan model ile ilgili davranış için oluşturulan karar ağacı Şekil 83'te, hangi değişkenlerin hangi diğer değişkenle ilişkili olarak sınıflandırma işleminde kullanıldığı, hangi değişkenlerin hangi parametreler doğrultusunda karar ağacı dallanmasında etkili oldukları kesit olarak Şekil 84'te gösterilmiştir.



Şekil 83. "İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım." davranışı için oluşturulan karar ağacı görüntüsü



Şekil 84. "İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım." davranışı için oluşturulan karar ağacı değerleri

Şekil 84'te belirtildiği üzere "İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım" riskli davranışı için oluşturulan karar ağacı 9 katman derinliğindedir ve karar ağacını oluşturan kural setinin bir bölümünü göstermektedir. Kişisel bilgi güvenliği özellikleri arasında yer alan "Riskli Davranış Puanı" özniteliği kök düğüm olarak belirlenmiştir ve dallanma bu öznitelikten oluşturulmaya başlanmıştır.

"İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım" davranışı için bir önceki aşamada gerçekleştirilen klasik istatistiki yöntemlerle belirlenen ilişkili öznitelikler ile C5.0 algoritması kullanılarak oluşturulan karar ağacında belirlenen ilişkili

değişkenlerin karşılaştırılması Tablo 80 üzerinde sunulmuş, davranış için oluşturulan kural seti EK 12'de sunulmuştur.

Tablo 80

"İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım" Davranışı için Öznitelik Karşılaştırması

C5.0 Algoritması – İlişkili Öznitelikler – (Dengeleme işlemi yapılmış veri seti)	C5.0 Algoritması – İlişkili Öznitelikler – (Dengelenmemiş veri seti)	Klasik İstatistiki Yöntemler – İlişkili Öznitelikler
- Eğitim Düzeyi - Cinsiyet - Yaş Aralığı - Riskli Davranış Puanı - Korumacı Davranış Puanı - Tehlike Algısı Puanı - Suça Maruziyet Puanı - Gelişime Açıklık Puanı - Özdenetim Puanı - Nevrotizm Puanı - Dışa Dönüklük Puanı - Uyumluluk Puanı - GİKS - Okuduğunu Görme - Yazma Hızı	- Eğitim Düzeyi - Cinsiyet - Riskli Davranış Puanı - Özdenetim Puanı - Dışa Dönüklük Puanı - Uyumluluk Puanı - İKY	- Eğitim Düzeyi - Özdenetim Puanı - Nevrotizm Puanı - Riskli Davranış Puanı

Karar Verme ve Tasarım Planı

Tüm davranışların çatısı altında toplanabilecek bir sınıflandırma alınan uzman görüşleri sonucu gerçekleştirilememiştir. Bu sebeple riskli davranış ölçeği ve korumacı davranış ölçeği içerisinde yer alan ve davranış olarak ölçülebilecek olan seçeneklerin (modellemeye tabi tutulan 11 davranış) çevrimiçi öğretim sistemi üzerinde verilecek eğitim içeriği konuları olarak belirlenmesi kararına varılmıştır. Bu seçeneklerle ilgili devlet, özel sektör paydaşlar ve eğitim kurumlarının müfredatları ve içerikleri incelenerek prototip bir eğitim içeriği uygulama-4 aşamasında gerçekleştirilmiştir.

Tasarımın Düzeltilmesi / Yenilenmesi

Uygulama-4 veri toplama sürecinde belirtilen sınıflandırma işleminin uzman görüşleri sonucunda nihayetlendirilememesinden dolayı tasarım düzeltilmiş ve sadece üzerinde çalışılan 11 davranış özelinde içerik sunulmasına karar verilmiştir.

Dördüncü Döngü Geliştirme Raporu

Şimşek'in (2014) modelde tasarımın süreç içerisinde şekillendirilerek, ürünün bu süreç nihayetlendiğinde ortaya çıkmış olacağını belirttiği üzere; kavramsal çerçeve başlığı altında incelenen alan yazın ve gerçek hayat verileri, geliştirme 1, 2 ve 3 aşamalarında uygulanan veri toplama ve analiz sonuçları konu üzerindeki ihtiyacı ortaya koymuştur. Reviere (1996) ihtiyacı istenilen sonuçlar ile şu anki durum arasındaki fark olarak açıklarken, Hesketh ve Laidlaw (2002) ise bu farkı ortaya koymak için izlenen süreci ihtiyaç belirleme olarak tarif etmişler, Iwai vd. (1999) ise öğrenen grubu için belirlenen bu ihtiyaçların meydana getirdiği farklılıkları giderme yollarını bulma sürecini de ihtiyaç analizi olarak betimlemişlerdir. Demirel (2007) ihtiyaç analizini gerçekleştirilecek eğitim faaliyetlerinin planlanabilmesi için gerek duyulan bilgileri elde etme çalışması olarak tanımlamış, bu süreci 5 aşamada incelemiştir:

1- İhtiyacın değerlendirilmesi için hazırlık yapma
2- Değerlendirme için bilgi toplama
3- Toplanan bilgilerin analiz edilmesi
4- Analiz edilen bilgilerin rapor haline getirilmesi
5- Rapor haline getirilen bilgilerden yararlanılması/kullanılması

Gerçekleştirilen alan yazın taraması bilgi güvenliğine yönelik olarak alınan tedbirlerin genel olarak teknoloji kaynaklı olduğunu, ancak yapılan araştırmaların bu girişimlerin bilgi güvenliği ihlallerini ortadan kaldırmadığını göstermiştir. Zincirin en zayıf halkası olarak tabir edilen insan faktörünün bilgi güvenliği ihlal girişimlerinde genel hedef olarak belirlendiği, ancak insanların bilgi güvenliğine dair davranışları hakkında çalışmaların da belirli bir düzeyde kaldığı görülmüştür. Alan yazında yapılan çalışmaların büyü çoğunluğunun ise gerçek hayattaki davranışları ölçmeden kişinin kendi beyanatına dayalı ölçekler kullanılarak gerçekleştirildiği açıktır. Gerçek hayat uygulamalarda ise kamu kurum ve kuruluşları ile alanda çalışan bilgi

güvenliği derneklerinin çabaları ile farkındalık oluşturulmaya ve bilgi teknolojilerinin daha güvenli kullanılması için çeşitli tavsiyelerde bulunulduğu anlaşılmıştır. Bu tavsiyelerin genel olarak odaklı ve yüz yüze gerçekleştirilen seminer, konferans vb. şeklinde gerçekleştirildiği, sınırlı sayıda da çevrimiçi öğretim ortamının varlığı görülmüştür.

Ek olarak yapılan alan yazın araştırması ve toplanan ve analiz edilen veriler ışığında bireylerin bilgi güvenliğine yönelik tüm davranışlarının demografik, sosyo-demografik ve kişilik özellikleri, algı ve maruziyet gibi bireysel farklılık durumlarından etkilendiği sonucuna varılmıştır. Bu bilgiler ışığında mevcut olan çevrimiçi sistemlerin kullanıcıların bireysel ihtiyaçlarına cevap vermede yetersiz kaldığı sonucuna varılmıştır.

Bu bilgiler ışığında, bilgi teknolojileri ürünü kullanan 7'den 77'ye her bireyin erişebileceği, bilgi güvenliği konusunda daha güvenli ve risksiz davranışlar sağlamasına yönelik, bireysel farklılıklarını da göz önünde bulunduran bir öğretim sistemine olan ihtiyaç ortaya koyulmuştur.

Alan yazın taraması sonrası bireylerin karşılaşabilecekleri bilgi güvenliği ihlalleri ile ilgili konuların çok geniş bir kapsamının olduğu görülmüştür. Öğretilecek tüm içerik belirli ölçütlere dayalı olarak analiz edilerek sınıflandırılmaya çalışılmış ancak uzmanların üzerinde bir mutabakata varamaması sonucu ile davranış olarak ölçülen 11 konu üzerinde karar kılınmıştır. "Bilgi güvenliği eğitimine yönelik olarak geliştirilen uyarlanabilir öğrenme ortamı hakkında konu alanı uzmanlarının görüşleri nelerdir?" araştırma sorusunda bu aşamada cevap verilmiştir.

Hedeflerin Belirlenmesi

İhtiyaçların ve içeriğin analiz edilmesinde sonra, üzerinde karar kılınan 11 bilgi güvenliği davranışı hakkında öğrenme hedefleri belirlenmiştir. Öğretim sonucunda sisteme katılım tüm katılımcıların aşağıda sıralanan hedefleri gerçekleştirebilmesi amaçlanmış, hazırlanan öğretim programı Ek 13'te sunulmuştur.

- Korsan/lisanssız yazılımın ne olduğunu ifade edebilme,
- Korsan/lisanssız yazılım kullanımı sebebiyle karşılaşabilecek tehlikeleri açıklayabilme,
- Neden lisanslı yazılım kullanmasının gerektiğini ifade edebilme,
- Epostanın kullanım alanlarını açıklayabilme,
- İstenmeyen veya önemsiz eposta içeriklerine örnek verebilme,

- İstenmeyen veya önemsiz epostaların riskleri ifade edebilme,
- Kimlik avı eposta özelliklerini açıklayabilme,
- Kimlik avı epostasını örneklendirebilme,
- Neden birden fazla eposta adresi kullanılması gerektiğini açıklayabilme,
- Eposta gönderirken kullanılan gizli karbon kopya fonksiyonunu açıklayabilme,
- Geçici internet dosyası kavramını açıklayabilme,
- Geçici internet dosyalarını silmenin faydalarını sıralayabilme,
- Geçici internet dosyalarını silme adımlarını takip edebilme,
- Web gezini geçmişinin ne olduğunu ifade edebilme,
- Neden web gezinti geçmişinin silinmesi gerektiğini açıklayabilme,
- Web gezinti geçmişini silme adımlarını takip edebilme,
- SSL sertifikası kavramını açıklayabilme,
- SSL sertifikasının önemini ifade edebilme,
- Güvenlik duvarının ne olduğunu ifade edebilme,
- Güvenlik duvarı çalışma mantığını açıklayabilme,
- Neden güvenlik duvarı kullanılması gerektiğini açıklayabilme,
- Güvenlik duvarı kullanmanın neyden koruyamayacağını ifade edebilme,
- Kişisel olarak tanımlanabilir bilginin ne olduğunu ifade edebilme,
- İnternet ortamında iletişim bilgilerinin paylaşılmasının neden riskli olduğunu ifade edebilme,
- İnternet ortamında özlük bilgilerinin paylaşılmasının neden riskli olduğunu ifade edebilme,
- Kişisel olarak tanımlanabilir bilgilerini korumak için neler yapması gerektiğini açıklayabilme,
- Güçlü parolanın özelliklerini açıklayabilme,
- Güçlü parola oluşturabilme,
- Parola oluştururken yapılmamasına dikkat edilmesi gereken hususları açıklayabilme,
- Kurumsal epostanın ne olduğunu ifade edebilme,
- Kurumsal epostanın önemini açıklayabilme,
- Kurumsal eposta hesabının günlük işlemlerde kullanmanın risklerini açıklayabilme,
- Zararlı yazılımın ne olduğunu ifade edebilme,
- Zararlı yazılımların verebileceği zararlara örnekler verebilme,
- Zararlı yazılımlardan korunmak için neler yapılabileceğini açıklayabilme.

Prototipin Oluşturulması –Tasarım

Bu aşamada alan yazın taraması, uygulama 1, 2, 3 aşamalarında toplanan ve analiz edilen veriler ışığında gerçekleştirilen ihtiyaç ve içerik analizi ve öğrenme hedeflerine uygun olarak uyarlanabilir çevrimiçi öğretim sistemi prototip tasarımı gerçekleştirilmiştir. Çevrimiçi öğretim sisteminin uyarlanabilirliği kullanıcı modellemesi doğrultusunda gerçekleştirilmiştir. Bu kapsamda ilk olarak kullanıcının modellemesinin yapılabilmesi için gerekli bilgilerin elde edilmesi ile işe başlanmıştır. Bu kapsamda oluşturulan tasarım adımları aşağıda belirtilmiştir.

Tasarım 1. Adım

Bu aşamada katılımcının modellemesinin yapılabilmesi için gerekli olan demografik, sosyo-demografik, hatalı yazım yönlendirmesi değişkenleri ile Korumacı ve Riskli Davranış, Tehlike Algısı ve Suça Maruziyet ölçeklerinin uygulanması için tasarım gerçekleştirilmiştir. Bu kapsamda aşağıda belirtilen ögelerin prototip üzerinde uygulanmasına karar verilmiştir.

- Sisteme giriş yapan kullanıcıya eğitimin konusunun bildirilmesi.
- Eğitim içeriğinin kişiselleştirilmiş olarak kullanıcıya sunulacağı bu sebeple eğitime geçmeden önce, belirtilen kişiselleştirilme işlemlerinde kullanılmak üzere sorular sorulacağı ve bu soruların eksiksiz yanıtlanması gerektiğinin kullanıcıya bildirilmesi.
- İlk aşamada kullanıcıdan demografik, sosyo-demografik bilgileri, hatalı yazım yönlendirme değişkenlerinin alınması. Bu durum gerçek hayatta karşılaşılabilecek herhangi bir kayıt sisteminde karşılaşılabilecek durumla benzerlik göstermesi açısından tercih edilmiştir.
- Bir sonraki aşamada, kişilik özelliklerinin bilgi güvenliğine yönelik davranışlarda farklılığa sebebiyet verdiğinden, kendilerine kişilik testi uygulanacağı ve sonuçlarının eğitim içeriğinin kişiselleştirilmesi için kullanılacağının bildirilmesi.
- Bir sonraki aşamada, katılımcının bilgilerini güvende tutmak için bilişim teknolojileri üzerinde uyguladıkları belirli davranışlara göre kendilerinin dikkat ve korumacılık seviyelerini ölçecek korumacı davranış ölçeğinin uygulanacağı bildirilmiştir. Sonuçlarının eğitim içeriğinin kişiselleştirilmesi için kullanılacağının bildirilmesi.
- Bir sonraki aşamada, katılımcının belirli bilişim teknolojilerini kullanım alışkanlıklarından veya şekillerinden yola çıkarak kendilerini riske atma derecelerini ölçecek riskli davranış

ölçeğinin uygulanacağının bildirilmesi, sonuçlarının eğitim içeriğinin kişiselleştirilmesi için kullanılacağının vurgulanması.

- Bir sonraki aşamada, katılımcının kendi göstermiş olduğu bilinçli veya bilinçsiz bir davranış sonucunda bilgi güvenliğine yönelik bir ihlale veya olaya maruz kalma seviyesini ölçecek suça maruziyet ölçeğinin uygulanacağının bildirilmesi, sonuçlarının eğitim içeriğinin kişiselleştirilmesi için kullanılacağının vurgulanması.
- Bir sonraki aşamada, katılımcının belirli bilişim sistemleri ve teknolojileri hakkında aldıkları riskin seviyesini ölçecek tehlike algısı ölçeği uygulanacağının bildirilmesi, sonuçlarının eğitim içeriğinin kişiselleştirilmesi için kullanılacağının vurgulanması.

Tasarım 2. Adım

Bu aşamada katılımcıdan alınan bilgiler ışığında modelleme gerçekleştirilmiş ve kendisine sunulacak eğitimin kişiselleştirilmesi sağlanmıştır. Bu kapsamda, katılımcı eğitime konu olan her bir bilgi güvenliği davranışı için, uygulama-3 aşamasında gerçekleştirilen makine öğrenmesi işlemlerine uygun olarak 4 kategoriye ayrılmıştır. Örneğin; "Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim" davranışı için, alınan bilgiler ışığında katılımcı şu sınıflara ayrılmıştır;

1- Katılımcı girdiği sitelerin SSL sertifikası olup olmadığına dikkat ettiğini bildirir ve bunu davranış olarak da gösterir (Söyler ve Yapar).
2- Katılımcı girdiği sitelerin SSL sertifikası olup olmadığına dikkat ettiğini bildirir ancak bunu davranış olarak göstermez (Söyler ancak Yapmaz).
3- Katılımcı girdiği sitelerin SSL sertifikası olup olmadığına dikkat ettiğini bildirmez ancak bu durumu davranış olarak gösterir (Söylemez ancak Yapar).
4- Katılımcı girdiği sitelerin SSL sertifikası olup olmadığına dikkat ettiğini bildirmez ve bu durumu davranış olarak da göstermez (Söylemez ve Yapmaz).

Katılımcı verdiği cevaplar sonucu belirtilen sınıflardan birine dâhil edilmiştir. Belirlenen öğrenme hedefleri göz önüne alınarak her bir konu için ayrı ayrı olmak üzere, eğitim içeriğinin seviyesi oluşturulan sınıflandırmaya göre ayarlanmıştır. Sınıflandırmaya göre yapılan eğitim seviyesi genel durumu Tablo 81 üzerinde açıklanmıştır.

Tablo 81

Davranışa İlişkin Sınıflandırma Ve İlgili Eğitim İçeriği Genel Çerçevesi

Davranışa İlişkin Sınıflandırma	Eğitim İçeriği Seviyesi	Açıklama
Söyler ve Yapar	1	Sınıfa dâhil olan katılımcının konu hakkında bilgisi olduğu ve bunu davranışa dönüştürdüğünün "öngörüldüğü" katılımcıya bildirilir. İsteğe bağlı olarak konu hakkındaki eğitim içeriğine erişebileceği veya bir sonraki eğitim içeriğine geçebileceği bildirilir.
Söyler ancak Yapmaz	2	Sınıfa dâhil olan katılımcının konu hakkında bilgisi olduğu ancak bunu davranışa dönüştürmediğinin "öngörüldüğü" katılımcıya bildirilir. Katılımcı davranışa dönüştürülmeyen bu bilginin hangi durumlarda karşısına çıkabileceği ve ne gibi sorunlara yol açabileceği hakkında eğitim içeriğine erişir.
Söylemez ancak Yapar	3	Sınıfa dâhil olan katılımcının konu hakkında bilgisinin olmadığı ancak bu konuda doğru davranışı sergilediğinin "öngörüldüğü" katılımcıya bildirilir. Katılımcı konunun genel çerçevede ne olduğu teorik bilgisini içeren eğitim içeriğine erişir, hangi durumlarda, ne gibi sorunlara yol açabileceği hakkında eğitim içeriğine isteğe bağlı erişim sağlayabilir.
Söylemez ve Yapmaz	4	Sınıfa dâhil olan katılımcının konu hakkında bilgisinin olmadığı ve bu konuda doğru davranışı sergilemediği katılımcıya bildirilmeden; konunun genel çerçevede ne olduğu, hangi durumlarda, ne gibi sorunlara yol açabileceğinin işlendiği, konu hakkında örnek olay ve videoların bulunduğu en geniş eğitim içeriğine erişimi sağlanır.

Yapılan bu sınıflandırma ve öğrenme hedefleri dikkate alınarak, çevrimiçi öğretim sistemi üzerinde eğitime dâhil edilen 11 davranış hakkında içerik oluşturulmuştur. "Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim." davranışı için oluşturulan içerikle ilgili konu başlıkları örnek olarak Tablo 82 üzerinde diğer 10 davranış için oluşturulan konu başlıkları EK 14 üzerinde gösterilmiştir.

Tablo 82

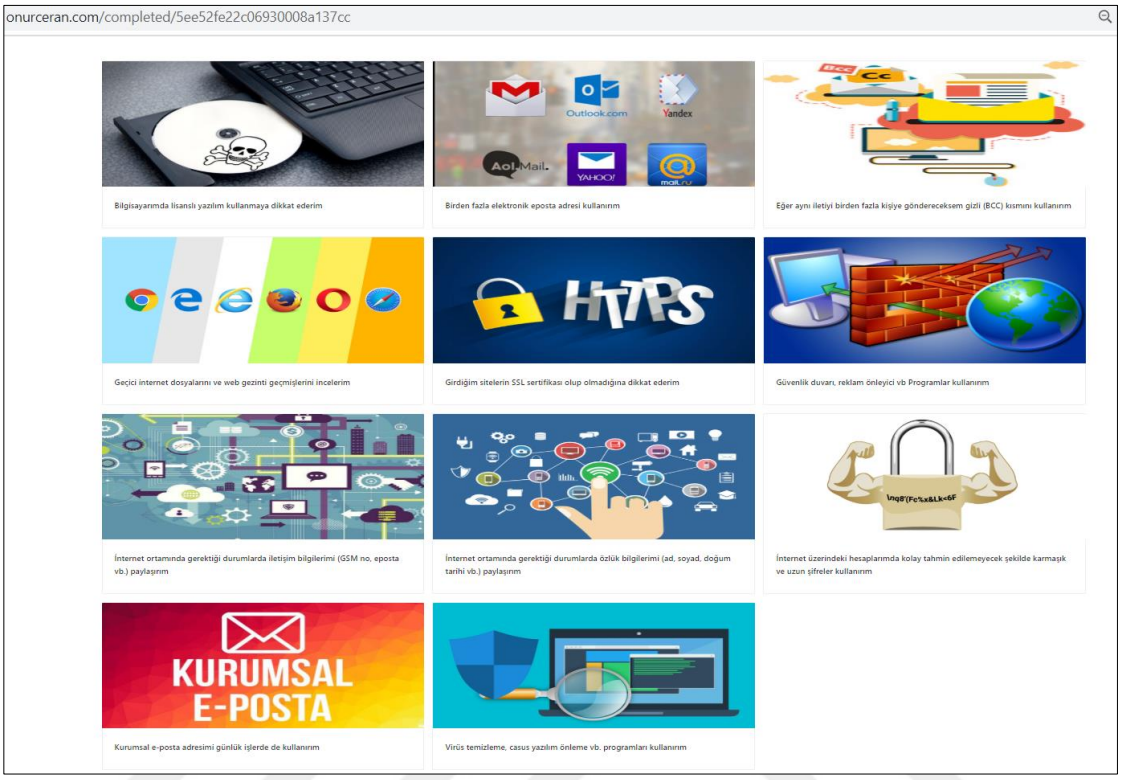
Davranış-1'e İlişkin Sınıflandırma Ve İlgili Eğitim İçeriği Örneği

Konu: Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim		
Davranışa İlişkin Sınıflandırma	Eğitim İçeriği Seviyesi	Konu Başlıkları
Söyler ve Yapar	1	- Eğitime katıl - Bir sonraki eğitim içeriğine devam et
Söyler ancak Yapmaz	2	- SSL sertifikası neden önemlidir? - SSL sertifikasına neden ihtiyaç duyarız?
Söylemez ancak Yapar	3	- SSL sertifikası nedir? - SSL sertifikası ne işe yarar? - İsteğe bağlı erişim • SSL sertifikası neden önemlidir? • SSL sertifikasına neden ihtiyaç duyarız?
Söylemez ve Yapmaz	4	- SSL sertifikası nedir? - SSL sertifikası ne işe yarar? - SSL sertifikası neden önemlidir? - SSL sertifikasına neden ihtiyaç duyarız? - Örneklerle video içeriği

Tasarım 3. Adım

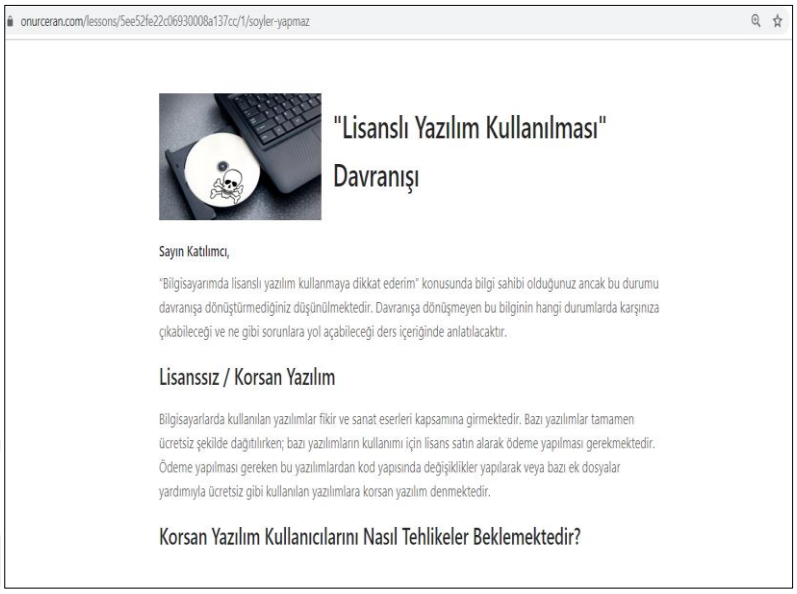
Bu aşamada uyarlanabilir çevrimiçi öğretim sisteminin, eğitim içeriğinin sunulacağı kullanıcı ara yüzü tasarımı yapılmıştır. Ara yüze ilişkin alınan tasarım kararları aşağıda sıralanmıştır.

- Kullanıcıyı tüm eğitim başlıklarının bulunduğu sayfa karşılayacaktır. Eğitim başlıkları içeriğe uygun görsellerle eğitim içeriğine bağlantı sağlayacak şekilde tasarlanmıştır. Kullanıcı eğitim konularından istediği seçeneği yaparak başlama esnekliğine sahiptir (Şekil 85).



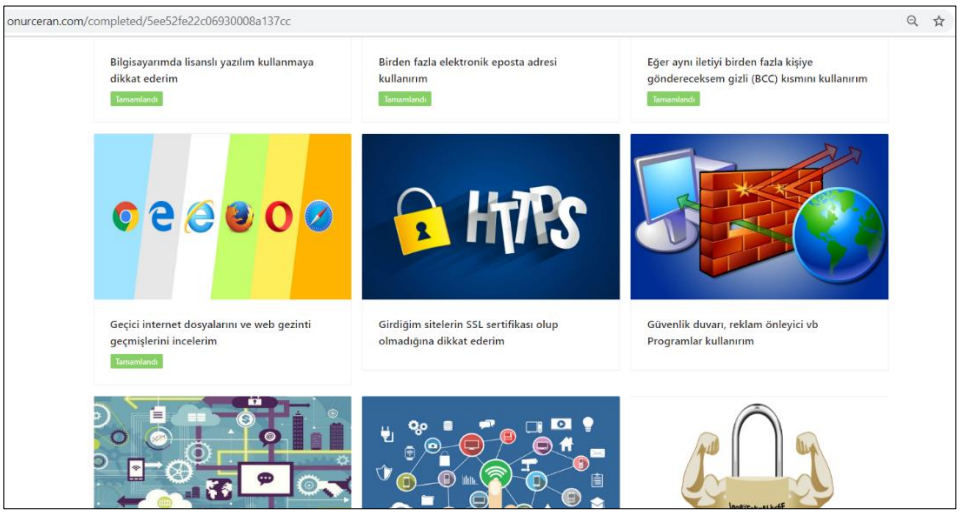
Şekil 85. Kullanıcı ara yüzü – birinci prototip, eğitim ana sayfası

- Kullanıcı eğitim konularından seçimi yaptığı zaman ilgili içeriğe yönlendirilmiştir. Seçimi yapılan sayfada kullanıcının ana sayfada görmüş olduğu aynı görselle birlikte davranış başlık olarak kullanılmıştır. Tasarım-2 adımında belirlenen konu başlıkları ve içeriği ile birlikte gerçekleştirilen modellemeye uygun olarak sunulmuştur. Şekil 86 üzerinde örneklendirildiği ve Tablo 81 üzerinde açıklandığı üzere kullanıcıya kendisinin ilgili davranışa ilişkin düşünülen bilgisi ve davranış şekli bildirilmiştir. İlgili örnekte "söyler ancak yapmaz" sınıfı için; *""Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim." konusunda bilgi sahibi olduğunuz ancak bu durumu davranışa dönüştürmediğiniz düşünülmektedir. Davranışa dönüşmeyen bu bilginin hangi durumlarda karşınıza çıkabileceği ve ne gibi sorunlara yol açabileceği ders içeriğinde anlatılacaktır."* ibaresi ile eğitime başlanılmaktadır.



Şekil 86. Kullanıcı ara yüzü – birinci prototip, konu içeriği sayfası

- Kullanıcı eğitimi tamamladıktan sonra bir sonraki eğitim içeriğine veya tamamlamadan ana sayfaya erişebilmektedir. Şekil 87'de görüldüğü üzere tamamlanan eğitim konusu başlığı altında "tamamlandı" ibaresi yer almaktadır. Kullanıcı eğitime ara verip tekrar giriş yaptığında tamamlanmamış eğitim içeriğine erişim sağlayabilmektedir. Eğitim konularının tamamı bitirildiğinde otomatik olarak ana sayfaya yönlendirme yapılmakta ve tüm konu başlıkları altında "tamamlandı" ibaresi gösterilmektedir.



Şekil 87. Kullanıcı ara yüzü – birinci prototip, tamamlanmış konu başlıkları

Prototipin Uygulanması – Araştırma

Tasarımı yapılan uyarlanabilir çevrimiçi öğrenme ortamı www.onurceran.com adresi üzerinden yayına alınmıştır. Web sitesinin tasarımı uzman görüşüne sunulmuştur. Bilgisayar ve Öğretim Teknolojileri anabilim dalı doktora derecesine sahip 3 uzman görüş bildirmişlerdir. Uzman görüşü için EK 3'te sunulan, "Çankaya İlçesi Milli Eğitim Müdürlüğü'ne Bağlı İlköğretim Okullarına ait Web Sitelerinin Grafik Tasarım Açısından İncelenmesi ve Örnek Web Sitesi Tasarımı Hazırlanması" başlıklı, araştırmacı Oğuzhan Korkut tarafından yüksek lisans çalışması kapsamında geliştirilen web tasarım ölçeği gerekli izinler (EK 4) alınarak kullanılmıştır. 3 uzmanın en az ikisinin mutabık kaldığı tasarıma ait öneriler Tablo 83 üzerinde sunulmuş ve hazırlanan prototip üzerinde gerekli değişiklikler yapılmıştır.

Tablo 83

Tasarıma Yönelik Uzman Görüşleri

Tasarıma İlişkin Öneriler	Açıklamalar
Web sitesinin logosu olmalıdır.	Tasarlanan logo web sitesine eklenmiştir.
Web sitesinde yer alan metinlerde önemli kısımların vurgularında renk, kalın yazı karakteri kullanılmalıdır.	Eğitim içeriğindeki önemli kısımlar kırmızı renkte, kalın yazı karakteri kullanılarak vurgulanmıştır.
Web sitesinde yer alan metinlerde her iki taraftan bloklama yapılmalıdır.	Tüm metin içeriği iki yana yaslanarak düzenlenmiştir.
Web sitesinde bir giriş ekranı bulunmalıdır.	Giriş ekranı eklenmiştir.
Web sitesinde yer alan fotoğraflar uygun çözünürlükte kullanılmalıdır.	Web sitesinde yer alan çözünürlüğü düşük fotoğraflar, çözünürlüğü yüksek olacak şekilde değiştirilmiştir.
Web sitesinde yer alan fotoğraflar uygun ölçülerde kullanılmalıdır.	Web sitesinde yer alan fotoğraflar sayfa yapısına uygun olarak ve aynı ebatta olacak şekilde düzenlenmiştir.
Web sitesinde tanıtıcı bilgilere yer verilmelidir.	Web sitesi giriş sayfasında geliştirilme amacı, içeriği ve kullanımına dair tanıtıcı bilgiler eklenmiştir.
Web sitesinde iletişim bilgileri bulunmalıdır	Web sitesi giriş sayfasında araştırmacıya ait iletişim bilgileri eklenmiştir.
Web sitesinin tasarımını yapan kişiye ilişkin bilgiler verilmelidir.	Web sitesi giriş sayfasında araştırmacıya ait bilgiler eklenmiştir.
Web sitesi üzerinde gezinmeyi kolaylaştırıcı site haritası bulunmalıdır.	Web sitesinde tüm eğitim konu başlıklarının bulunduğu sayfa ismi "site haritası" olarak değiştirilmiş ve her konu sayfasında ulaşılabilecek bağlantılar eklenmiştir.
Web sitesi üzerinde arama imkânı sunan bir arama motoru bulunmalıdır.	Web sitesinde eğitim içerikleri kişiselleştirilmiş olarak sunulması sebebiyle statik yapıda değildir. Bu sebeple arama motoru eklenememiştir.
Web sitesinin son güncellenme tarihi belirtilmelidir.	Web sitesi giriş sayfasında son güncellenme tarihi eklenmiştir.
Web sitesinde favorilere ekle ve ana sayfa yap seçenekleri bulunmalıdır.	Web sitesine ilgili ekleme yapılmış ancak bazı tarayıcıların bu desteği kaldırmasından dolayı işlem iptal edilmiştir.
Web sitesinde konu yazarlarına ait bilgiler bulunmalıdır.	Web sitesi giriş sayfasında, eğitim içeriğinin açık kaynaklardan derlenerek hazırlandığı bildirilmiştir.
Web sitesinde kullanıcılar için yararlı web adresleri verilmelidir.	Web sitesi, site haritasının bulunduğu sayfada bilgi güvenliği ile ilgili web adresleri "Yararlı Bağlantılar" başlığı altında eklenmiştir.
Web sitesi başlığı büyük harflerle yazılmalıdır.	Web sitesi başlığı güncellenmiştir.
Web sitesinde cevaplanan ölçekleri yanıtlamanın kullanıcının ne kadar vaktinin alacağı bildirilmelidir.	Web sitesi giriş sayfasında ölçekler yanıtlanırken harcanacak ortalama süre eklenmiştir.
Web sitesinde ölçeklere verilen yanıtların güvenliği ile ilgili bilgi verilmelidir.	Web sitesi giriş sayfasında ölçekler kapsamında kişisel tanımlayıcı bilgi istenmediği ve verilen cevapların 3. kişilerle paylaşılmayacağına dair ibare eklenmiştir.

Tasarımı yapılan uyarlanabilir çevrimiçi öğrenme ortamı üzerindeki eğitim içerikleri için 3 konu alanı uzmanından görüşler alınmıştır. Bu kapsamda bir uzman görüş formu hazırlanmıştır.

Hazırlanan formun uygunluğu Bilgisayar ve Öğretim Teknolojileri anabilim dalı doktora derecesine sahip 3 uzmanın görüşüne sorulmuştur. Nihai hali EK 15'te gösterilen "Eğitim İçeriği Uzman Görüş Formu" için 3 uzmanın verdiği öneriler Tablo 84 üzerinde gösterilmiştir.

Tablo 84

Eğitim İçeriği Uzman Görüş Formuna Yönelik Uzman Görüşleri

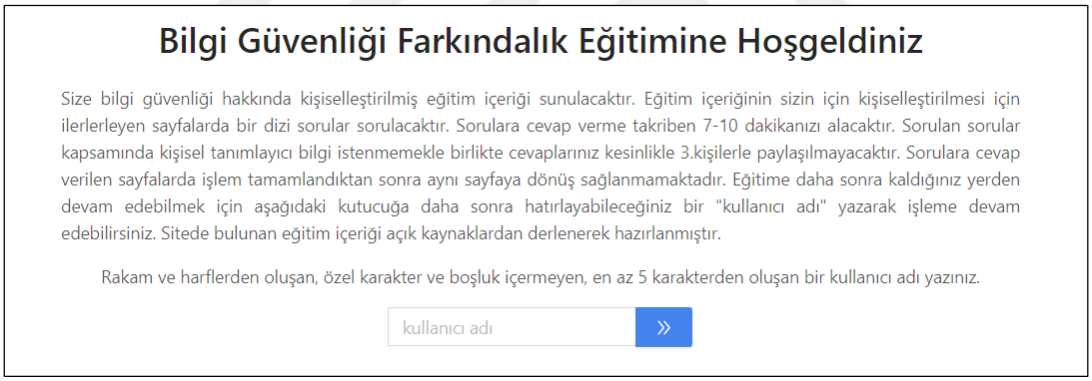
Forma İlişkin Öneriler	Açıklamalar
Gerçekleştirilen çalışmanın kapsamının görüş alınacak olan uzmana bildirilmesi gerekmektedir.	Çalışmanın doktora tezi kapsamında yapıldığı okul, anabilim dalı, danışman bilgileri ile eklenmiştir.
Eğitim içeriğini görebilmek için bir dizi ölçek yanıtlamak gerektiği ve alacağı süre görüş alınacak uzmana bildirilmelidir.	Form metnine eklenmiştir.
Form içerisinde kullanılan derecelendirme tablosu isimlendirilmelidir.	"Derecelendirme Kılavuz Tablosu" olarak isimlendirilmiştir.
Araştırmacıya ait iletişim bilgileri forma eklenmelidir.	Araştırmacıya ait eposta forma eklenmiştir.
Çevrimiçi öğrenme ortamının çalışma mantığı görüş alınacak uzmana bildirilmelidir.	Çevrimiçi öğrenme ortamının ölçeklere verilen yanıtlara göre kişiselleştirilmiş eğitim içeriği sunduğu form metnine eklenmiştir.
Uzmanların eklemek istedikleri bağımsız görüşler için bir bölüm oluşturulmalıdır	Uzman görüş formunun en alt kısmına ek görüş bölümü eklenmiş ve form metninde belirtilmiştir.
Yazım ve imla hataları, anlatım bozuklukları giderilmelidir.	Form kapsamında yazım ve imla hataları düzeltilmiştir. Çalışma kapsamında kullanılan ve başka bir araştırmacıya ait olan ölçek maddeleri üzerindeki anlatım bozukluğu değerlendirmeleri, ölçek maddeleri değiştirilemeyeceğinden işlem gerçekleştirilmemiştir.

Oluşturulan eğitim içeriği de uzman görüşüne sunulmuştur. Bu doğrultuda "Yönetim Bilişim Sistemleri" doktora derecesine sahip iki bilgi güvenliği uzmanı ve bir siber suçlarla mücadele biriminde çalışan, doktor adayı bir bilgi güvenliği uzmanı görüşlerini bildirmiştir. Eğitim içeriği için 3 uzmanın verdiği öneriler EK-16 üzerinde gösterilmiş, prototip bu doğrultuda güncellenmiştir.

Sistemin Kurulması

www.onurceran.com alan adı üzerinde yayın yapan uyarlanabilir çevrimiçi öğrenme ortamının tasarımında değişiklikler uzman görüşleri kapsamında yapılarak, sistemin son şeklini alması

sağlanmıştır. Buna göre; geliştirilen ilk prototip üzerinde kullanıcı öğrenme sisteme ilk erişim sağladığında doğrudan demografik ve sosyo-demografik soruların yer aldığı sayfaya yönlendirilirken, nihai sistemde bir giriş ekranı ile karşılanmaktadır. Şekil 88 üzerinde görüldüğü gibi kullanıcıya katıldığı eğitimin bilgi güvenliği farkındalığı üzerine olduğu ve eğitim içeriğinin kendisi için kişiselleştirilmiş olduğu bildirilmektedir. Belirtilen içeriğin kişiselleştirilebilmesi için bir dizi soru sorulacağı ve bu soruları yanıtlamak için harcayacağı vakit ortalama olarak bildirilmiştir. Kullanıcıların verdiği cevapların güvenliğinin sağlanacağı bu ekranda taahhüt edilmiştir. Öğrenme ortamının kullanımına yönelik bir dizi uyarı verilmiştir. Buna göre her bir ölçek tamamlandıktan sonra geri dönüş yapamayacağı, kendisinin belirleyeceği bir kullanıcı adı eğitime muhtelif zamanlarda kaldığı yerden devam edebileceği aktarılmıştır. Eğitim içeriğinin açık kaynak bilgilerden derlenerek hazırlandığı da ayrıca bu ekranda bildirilmiştir.



Şekil 88. Kullanıcı ara yüzü - eğitim giriş sayfası

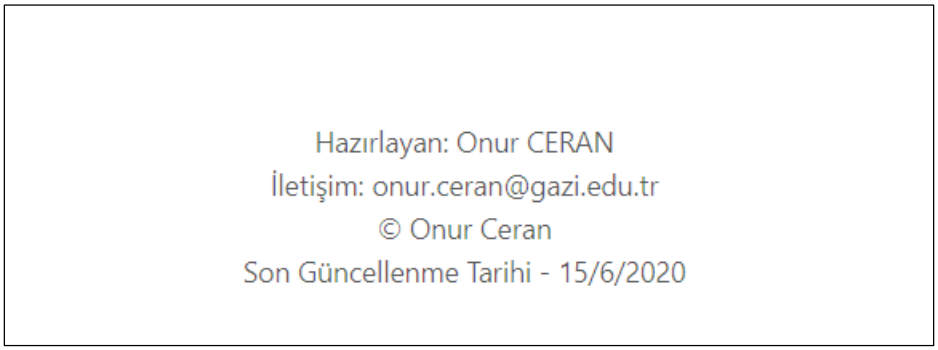
Geliştirilen ilk prototip üzerinde tarayıcı başlığı için “onurceran.com” kullanılıyorken, nihai sistem büyük harfler kullanılarak “KİŞİSELLEŞTİRİLMİŞ BİLGİ GÜVENLİĞİ FARKINDALIK EĞİTİMİ” olarak yeniden düzenlenmiştir. Tarayıcı başlığına ait ekran görüntüsü Şekil 89 üzerinde gösterilmiştir.

Şekil 89. Kullanıcı ara yüzü – tarayıcı başlığı

Geliştirilen ilk prototip üzerinde öğrenme ortamına özgü bir logo tasarımı yapılmamışken, içeriğe uygun olarak hazırlanan logo (Şekil 90) nihai sistem üzerinde farklı bölümlere eklenmiştir.

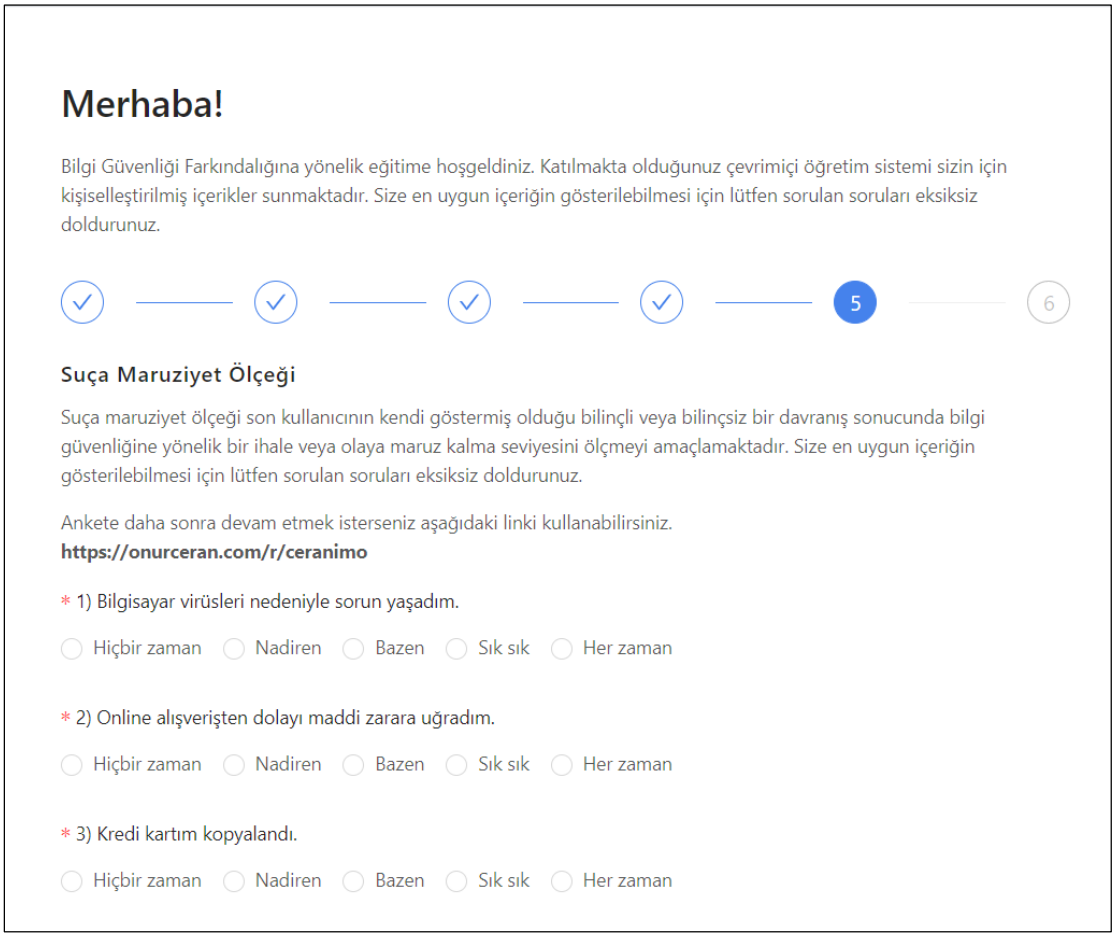
Şekil 90. Kullanıcı ara yüzü – logo

Geliştirilen ilk prototip üzerinde araştırmacıya ait herhangi bir bilgi verilmemişken, nihai sistem üzerine, alınan uzman görüşleri doğrultusunda künye bilgileri ve iletişim adresi eklenmiştir. Şekil 91 üzerinde belirtildiği gibi, öğrenme ortamının son güncellenme tarihi de araştırmacıya ait bilgiler altında sunulmuştur.



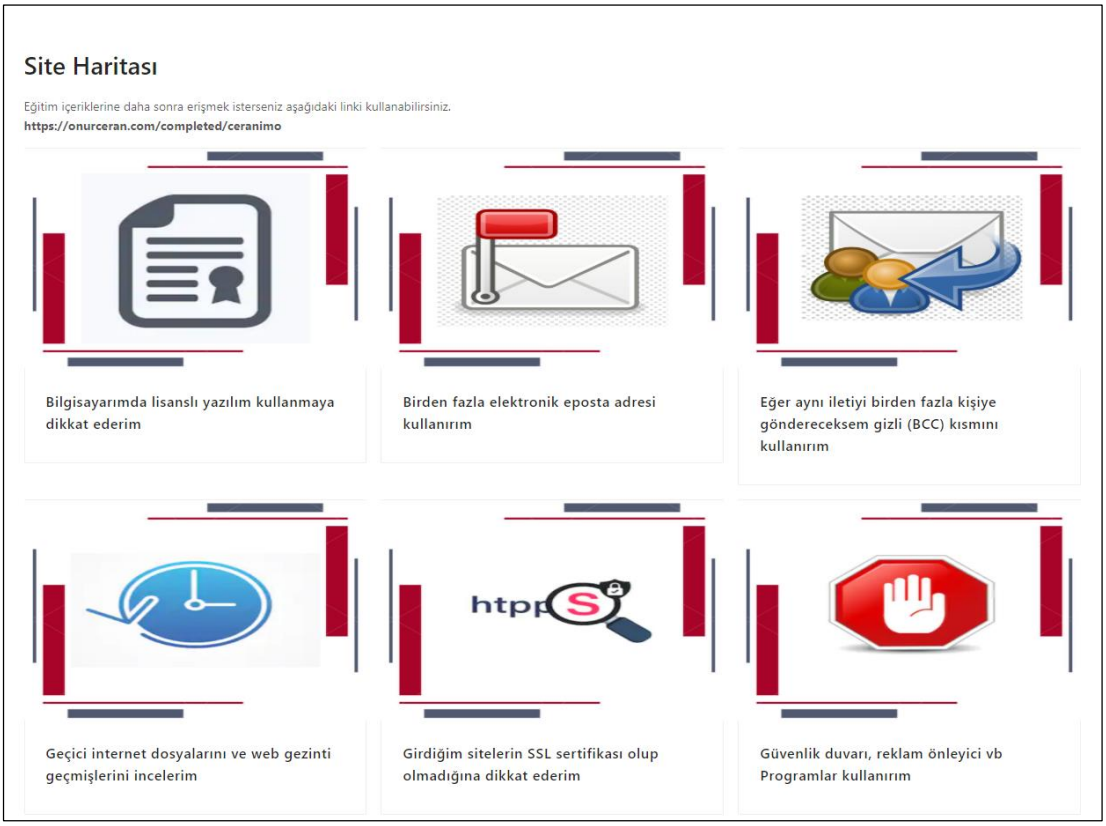
Şekil 91. Kullanıcı ara yüzü – çalışmacıya ait bilgiler

Öğrenme sistemi giriş sayfası üzerinde kullanıcı bir kullanıcı adı belirledikten sonra kişiselleştirme algoritmalarının çalışabilmesi için gerek duyulan ölçeklere yanıt vermeye başlayacak şekilde tasarıma karar verilmiştir. Toplam 6 farklı ölçeğe cevap vermesi istenen kullanıcı hangi aşamada olduğunu, geriye kaç aşama kaldığını sisteme eklenen bir işlem çubuğu vasıtası ile öğrenebilmektedir. Şekil 92 üzerinde örneklendirildiği gibi, her bir ölçeğin ne amaçla kullanıldığı ve içeriği kullanıcıya sunulmuştur. Ayrıca kullanıcının eğitime katılıma ara vermek istemesi durumunda, daha sonra kaldığı yerden devam edebilmesi için erişmesi gereken bağlantı adresi ilgili ölçeği yanıtlamaya başlamadan sunulmuştur.



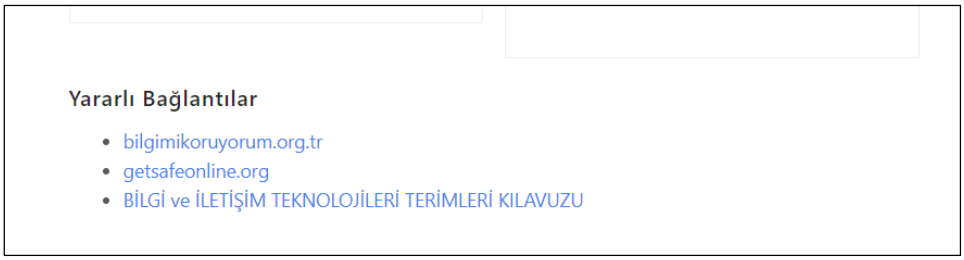
Şekil 92. Kullanıcı ara yüzü – ölçek sayfası

Geliştirilen ilk prototip üzerinde eğitim konu başlıklarını içeren ve isimlendirilmemiş olan sayfa nihai sistemde "site haritası" olarak belirlenmiştir. Şekil 93 üzerinde gösterildiği üzere; alınan uzman görüşü doğrultusunda, konu başlıklarına ait görseller aynı boyutta ve görsellikte olacak şekilde ve konuyu tarif eden ikonlar kullanılarak yeniden tasarlanmıştır.



Şekil 93. Kullanıcı ara yüzü – site haritası

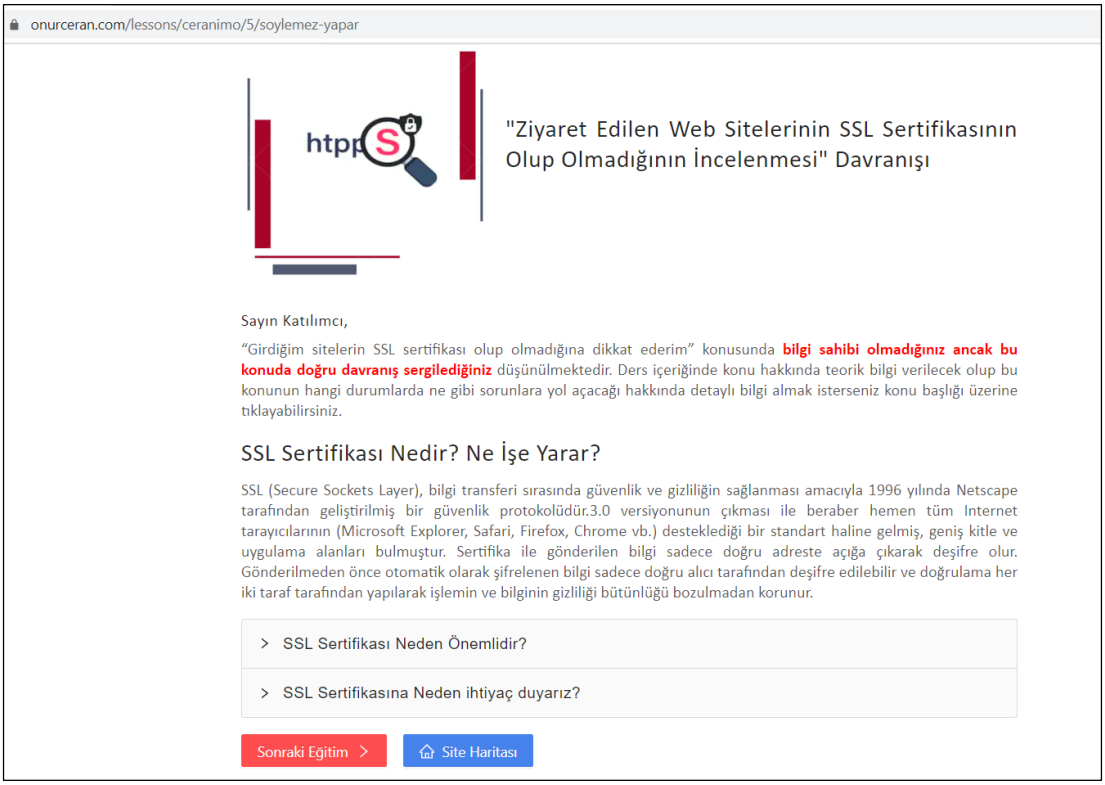
Kurulumu yapılan nihai sistem üzerinde kullanıcıya yararlı bağlantı adresleri sunulmuştur. Eğitim içeriği oluşturulurken de faydalanılan web adresleri Şekil 94 üzerinde gösterilmiş olup, mevcut çalışma kapsamında tasarımdan kaynaklı değinilmeyen ancak bilgi güvenliği alanında güncel bilgiler içeren web sitelerinden oluşmaktadır.



Şekil 94. Kullanıcı ara yüzü – yararlı bağlantılar

Alınan uzman görüşleri doğrultusunda, kurulan nihai sistemde önemi vurgulanmak istenen metinler kalın puntolarla ve kırmızı renkte ayarlanmıştır. Eğitimi verilen her bir davranış için

modellemenin elverdiği ölçüde 4 ayrı eğitim içeriği oluşturulmuştur. “Ziyaret edilen web sitelerinin SSL sertifikasının olup olmadığının incelenmesi” davranışı için örneği Şekil 95 üzerinde verilen “söylemez ancak yapar” sınıfıma özgü eğitim içeriğinde kullanıcıya neden bu içeriğin kendisine gösterildiği belirtilmiştir. Gerçekleştirilen tasarım doğrultusunda kullanıcının inisiyatifine bırakılan alanlar kayan bölmeler olarak ayarlanmıştır. “söyler ve yapar”, “söyler ancak yapmaz” ve “söylemez ve yapmaz” sınıflarına ait eğitim içeriği örnekleri EK 16 üzerinde gösterilmiştir.



Şekil 95. Kullanıcı ara yüzü – eğitim sayfası örneği

Alınan uzman görüşleri doğrultusunda eğitim içeriğinde bulunan tüm metinler sayfanın iki yanına yaslanarak düzenlenmiştir. Sistem üzerinde kullanılan tüm resimlerin uygun çözünürlükte kullanılmasına özen gösterilmiştir. Örneği EK 16 üzerinde verildiği üzere sayfa ölçeklendirmesi %250 oranında artırılarak incelendiğinde kullanılan resimlerin bozulmaya uğramadığı teyit edilmiştir. Uzman görüşlerinde yer almasına rağmen gerçekleştirilmeyen iki konu bulunmaktadır. Buna göre web sitesinde eğitim içerikleri kişiselleştirilmiş olarak sunulması sebebiyle statik yapıda olmaması bir arama motoru eklenmesine mani olmuştur.

Ayrıca bazı tarayıcıların destek vermemesinden dolayı “favorilerime ekle” ve “ana sayfam yap” özellikleri nihai sistem üzerinde kullanılamamıştır.

BÖLÜM V

SONUÇ VE TARTIŞMA

Bu bölümde amaçlar ve alt amaçlara ait toplanan verilerin analiz edilmesi ile ulaşılan sonuçlar ve bundan sonra yapılabilecek araştırmalara yönelik önerilere yer verilmiştir.

Sonuç

Bilgi güvenliğine yönelik uyarlanabilir bir öğrenme ortamının geliştirildiği bu çalışma internet ortamında duyurusu yapılan katılım çağrısına yanıt veren 619 kişiden toplanan veriler, bilgi güvenliğine yönelik davranış olarak ölçülebilen davranışlar ve uyarlanabilir öğrenme ortamda gerçekleştirilen uyarlamalar ile sınırlıdır. Pai, Lyu ve Wang (2010) Tayvan'da lise öğrencilerinin akademik başarısını tahmin etmek için veri madenciliği yöntemlerini kullandıkları çalışmada 500 öğrenci üzerinden topladıkları veriler üzerinde çalışmışlardır. McCuaig ve Baldwin (2012) bir değerlendirme yapmaya ihtiyaç duymadan veri madenciliği yöntemleri kullanarak öğrenenlerin başarı durumunu sınıflandırdıkları çalışmalarında 122 katılımcı verisi üzerinde çalışmışlardır. Sao Pedro vd. (2010) öğrencilerin meta-bilişsel planlama davranışlarını, gerçek zamanlı olarak öğrenme sistemi kütük kayıtları üzerinden toplanan veriler üzerinde veri madenciliği işlemleri ile belirledikleri çalışmalarında 148 öğrenci verisi üzerinde çalışmışlardır. Bu çalışmada veri madenciliği işlemleri için toplanan verilerin, erişilebilir örneklem bakımından benzer çalışmalara paralellik gösterdiği görülmektedir. Guruler, İstanbullu ve Karahasan (2010) ise öğrenenlerin akademik başarılarını karar ağaçları yöntemini kullanarak tahmin etmeye çalıştıkları çalışmalarında 3110 öğrenci verisi üzerinde çalışmalarını gerçekleştirmişlerdir. Vialardi vd. (2011) öğrencilere akademik dönem için, otomatik olarak ders atama önerisinde bulunma üzerine yaptıkları çalışmalarında 1991-2009

öğrenci kayıtlarını kullandıkları çalışmalarında veri madenciliği işlemlerini 161.247 örnek üzerinde gerçekleştirmişlerdir. Belirtilen çalışmaların veri setlerinin görece büyüklüğünün hazırda bulunan, daha önceden kayıt altına alınan veriler üzerinden gerçekleştirilmesinden kaynaklandığı düşünülmektedir.

Yapılan alan yazın taraması ve gerçek hayattan örnekler bilgi güvenliğine yönelik alınan tedbirlerin büyük çoğunluğunun teknik araç ve gereçlerle sağlanmaya çalışıldığını göstermektedir. TBMM - Bilişim ve İnternet Araştırma Komisyonu (BİAK) Raporunda Yer Alan Öneriler (2013) kitapçığında yer alan "Bilgi Güvenliğine Yönelik Öneriler" başlığı incelendiğinde; Siber Güvenlik Kurulunca yapılacak denetimler, altyapıda yapılacak güçlendirmeler, yükseköğretimde siber güvenlikle alakalı derslerin sayısında artış, bilgi sistemlerinden sorumlu personelin sürekli eğitimi, milli ürün geliştirilmesi ve paydaşlarla işbirliği konuları üzerinde durulduğu görülmektedir. Bilişim ve İnavosyon Derneği Siber Güvenlik Raporu (Kurtul vd., 2020) incelendiğinde bilgi güvenliğine yönelik yapılan önerilerin olay yönetimi, bilgi güvenliği yönetim sistemleri, güvenlik testleri, entegre veri sistemleri ve yerli donanım ve yazılım üzerine odaklanıldığı görülmektedir. Farkındalık eğitimi konusu ise kısa bir başlıkta değerlendirilmektedir. Bilgi güvenliğine yönelik olarak gerçekleştirirken bilimsel araştırmalarla birlikte teknolojik ürün oluşturulmasına yoğun emek ve yüksek bütçeler harcanmaktadır. Ancak bu çabalara rağmen tehditlerin azalmadığı ve sistemlere yönelik saldırıların tam olarak önlenemediği görülmektedir. Bu konuda zincirin en zayıf halkası olarak tanımlanabilecek son kullanıcıların bilgi güvenliğine yönelik olarak eğitim almasının önemi ortaya çıkmıştır. Ebeveynlerinin tablet bilgisayarı üzerinden çevrimiçi oyun oynayan 7 yaşındaki bir çocuktan, 77 yaşında su faturasını çevrimiçi hizmetler kullanarak ödeyen bir bireye kadar hemen herkesin bilgi güvenliğine yönelik farkındalıklarının oluşmasının, konuya ilişkin daha güvenli ve risk barındırmayan davranışlar sergileyebilmesinin önemi açıktır. Bilgi Güvenliği Derneği (Bostan ve Şengül, 2018), ilgili kurum ve kuruluşların son 30 yıl süresince bilgi güvenliği farkındalığı konusunu, özgü araç ve teknolojilerin tanıtım ve kullanımına dair faaliyetler kapsamında yürüttüklerini belirtmiş; bu durumun bireyde arzu edilen şekilde davranış geliştirmede yetersiz kaldığını vurgulamıştır. Eğitilmesi gereken hedef kitlenin 7'den 70'e hemen herkes olabilmesi ve büyüklüğü göz önüne alındığından faaliyetler için en uygun ortamın çevrimiçi öğrenme ortamları olduğu sonucuna varılmıştır. Zira konu hakkında hali hazırda gerçekleştirilen eğitim faaliyetlerinin büyük çoğunluğunun ilgi kurum ve kuruluşların

veya gönüllü bireylerin yüz yüze olarak gerçekleştirdikleri eğitim çalışmalarından ibaret olduğu görülmüştür. Bilgi Teknolojileri ve İletişim Başkanlığı (BTK, 2019) faaliyet raporu incelendiğinde; bilgi güvenliğine dair 100.000 adetten fazla broşür, kitap vb. materyal dağıtıldığı, 2018-2019 eğitim öğretim yılı süresince 242 eğitim faaliyeti kapsamında 37.260 öğrenci, öğretmen ve ebeveyne yüz yüze farkındalık eğitimi/semineri verildiği bildirilmiştir. Başkanlık altında yapılanan Bilinçlendirme Merkezi'nin hazırlamış olduğu, güvenli ve bilinçli internet kullanımına yönelik bilgilerin paylaşıldığı www.guvenliweb.org.tr adresi üzerinde, sadece "web güvenliği" konusunun 388.878 (EK 17) kez görüntülendiği görülmüştür.

Alan yazında insanı odak alan bilgi güvenliğine yönelik yapılan çalışma sayısının miktar olarak önemsenecek düzeyde olduğu görülmüştür. Ancak yine yapılan çalışmaların büyük bölümünün son kullanıcıların kendi beyanatları üzerine inşa edilmesi, davranışa yönelik bulguların göz ardı edilmesine sebebiyet vermektedir. Bu durum da kullanıcıların beyanları ve davranışları arasındaki farkın göz ardı edilmesine sebebiyet vermektedir. Karakasiliotis, Furnell ve Papadaki (2006) maillerin gerçek mi oltalama maili mi olduğunun tanımlanması için 179 katılımcı ile gerçekleştirdikleri çalışmalarında katılımcıların %45'inin oltalama maillerini belirleyebildiği ancak bunların büyük bir çoğunluğunun nasıl tanımladıklarını ikna edici bir şekilde açıklayamadıklarını belirtmiştir. Workman (2008) ise sosyal mühendislik saldırılarına maruz kalma durumlarını incelediği çalışmasında, katılımcıların hazırlanan anketlere verdiği cevapların gerçek yaşam uygulamalarındaki davranışları ölçmede yetersiz kalacağını belirterek anket üzerindeki değişkenleri davranış olarak gözlemlemeyi de çalışmasına dâhil etmiştir. Aburrous, Hossain, Dahal ve Thabtah (2010) yapmış oldukları çalışmada bir firmada çalışan 120 personele kredi kartı ve şifre bilgilerini vermeleri için oltalama epostası göndermiş ve daha sonra kendilerini banka yetkilisi gibi tanıtmışlardır. Deneye katılan personelin %32'si tüm kredi kartı bilgilerini paylaşırken, %16'sı sadece kullanıcı adını vermiş, %52'si ise bilgi vermeyi reddetmiştir. Deney sonucu katılımcılarla yapılan görüşmelerde, bilgilerini paylaşan kullanıcılar oltalama atakları ile bilgi alınan kişilerin kesinlikle kendileri olamayacağını beyan etmişlerdir. Araştırmacılar bu sebeple ölçekler yardımı ile yapılan araştırma sonuçlarının hatalı olabileceğini vurgulamışlardır.

Bu çalışma kapsamında son kullanıcıların demografik, sosyo-demografik, kişilik özellikleri ile korumacı ve riskli davranış durumları, tehlike algıları ve suça maruziyet seviyeleri göz önüne

alınarak, belirlenen bilgi güvenliği davranışlarına yönelik söylem ve hareketlerinin farklılaşma durumları incelenmiştir. Bu doğrultuda her bir farklı davranış için hangi birey özelliğinin hangi davranışı hangi söylem çerçevesinde etkilediği belirlenerek kullanıcılar üzerinde bir sınıflandırma işlemi yapılmıştır. Belirtilen sınıflandırma işlemi yapılırken öncelikle alan yazın taraması sonucu bilgi güvenliğine yönelik insan davranışlarını etkilediği hakkında çalışmalar yapılan kişilerin demografik ve sosyo-demografik özellikleri toplanmıştır. McCormac vd. (2017) bilgi güvenliği farkındalığı için bireysel farklılıklar üzerinde yapmış oldukları çalışmada kişilerin yaş, cinsiyet, kişilik özellikleri ve risk alma eğilimlerinin etkisini incelemişlerdir. Gratian vd. (2018) bireylerin cihaz güvenliği, şifre oluşturma ve güncelleme bilgi güvenliği davranışlarına bireysel farklılıklardan risk alma özellikleri, karar alma stilleri, demografik ve kişilik özelliklerinin etkisini incelemişlerdir. Bishop vd. (2020) bilgi güvenliğine dair bireysel farklılıkları inceledikleri çalışmalarında cinsiyet, yaş, eğitim, risk alma ve kişilik özellikleri, karar alma stilleri, planlanmış davranış ve korumacı motivasyon değişkenleri üzerinde durmuşlardır. Hadlington (2017) ve Chen, Chen ve Yang (2008) bilgi güvenliği ve suiistimalleri üzerine yaptıkları çalışmalarda internet bağımlılığının etkilerini ölçmüşlerdir. Bu çalışma kapsamında toplanan bireysel farklılıklara dair veriler de alanyazında ortak olarak çalışılan değişkenlerdendir. Alanyazında bilgi güvenliğine dair, bu çalışmaya dâhil edilmemiş olan değişkenlerin etkilerinin incelendiği çalışmalar da bulunmaktadır. Fogel ve Nehmad (2009) sosyal bireylerin internet üzerindeki riskli davranışlarını inceledikleri çalışmalarında güven, gizlilik davranışı, tutumu ve endişesi ile zaman baskısı değişkenlerinin etkilerini incelemişlerdir. Hu, West ve Smarandescu (2015) bilgi güvenliği ihlalleri konusunda kendini kontrol etme değişkenininin etkisini çalışırken, Parsons vd. (2015) bilgi güvenliğine dair karar alma konusunda organizasyonel bilgi güvenliği kültürünün etkisini incelemişlerdir.

Çalışma sonucunda ortaya çıkan uyarlanabilir çevrimiçi öğrenme ortamının hayata geçmesi 4 ayrı aşamada gerçekleştirilmiştir. Birinci aşamada alan yazın taraması sonucu bireylerin bilgi güvenliğine yönelik davranışlarında etkisi olan değişkenler incelenmiş ve üzerinde karar kılınanlara ait veriler gönüllü katılımcılardan toplanarak analiz edilmiştir. Gerçekleştirilen analizler katılımcıların bilgi güvenliği kapsamında korumacı davranışları üzerinde günlük internet kullanım saati, özdenetim, uyumluluk ve gelişime açıklık kişilik özellikleri değişkenlerinin etki ettiği görülmüştür. Kullanıcıların riskli davranışlarını ise yaş, internet kullanım yılı, günlük internet kullanım saati, eğitim düzeyi, uyumluluk, nevrotizm, gelişime

açıklık kişilik özellikleri ile suça maruziyet ve tehlike algısı değişkenlerinin etkidiği görülmüştür. Bulgulara paralel olarak, yapmış oldukları çalışmalarda; Whitty vd. (2015) şifre paylaşımı konusunda yaş değişkeninin etkili olduğunu; Hamburger ve Ben-Artzi (2000) yüksek nevrotizm kişilik özelliği gösteren kullanıcıların çevrimiçi uygulamalarda daha çok vakit geçirme ve fazlaca bilgisini ifşa etme eğiliminde olduğunu; Sumner, Byers ve Shearing (2011) yüksek dışa dönüklük ve uyumluluk gösteren bireylerin çevrimiçi gizliliğe daha çok önem verme ve yüksek nevrotizm ve gelişime açıklık gösteren bireylerin kendileri hakkında daha çok bilgi paylaşma eğiliminde olduğunu; Shropshire vd. (2015) özdenetim ve uyumluluk kişilik özelliği gösteren kullanıcıların güvenlik yazılımı kullanma eğiliminde olduğunu; Pattinson vd. (2015) gelişime açıklık kişilik özelliğinin oltalama saldırılarını belirlemede pozitif etkisinin olduğunu; Tekerek ve Tekerek (2013) daha yüksek eğitim seviyesinde olan kullanıcıların daha fazla bilgi güvenliği farkındalığının olduğunu belirtmişlerdir. Buna karşın yapmış oldukları çalışmalarda; Halevi vd. (2013), Sheng vd. (2010) ve Jagatic vd. (2007) cinsiyetin korumacı davranışlar konusunda belirleyici olduğunu; Dhamija vd. (2006) ve Mohebzada vd. (2012) yaş değişkeninin oltalama saldırılarına maruz kalma konusunda riskli davranışlara bir etkisinin bulunmadığını; Farooq vd. (2015) ise eğitim seviyesi ile bilgi güvenliği farkındalığı arasında istatistiki olarak bir korelasyonun bulunmadığını belirtmişlerdir. Alanyazına göre oluşan bu paralellik ve farklılıkların örneklem özelliklerinden kaynaklanıyor olabileceği değerlendirilmiştir. Bu çalışmada katılımcıların riskli davranışlarını etkileyen değişkenlerin görece fazla olması yapılan davranışın riskli olmadığının düşünülmesinden veya bilinçsiz olarak gerçekleştirilmesinden kaynaklandığı düşünülmektedir. Zira tehlike algısı ile riskli davranış puanları arasında negatif bir korelasyonun varlığı tespit edilmiştir.

Çalışmanın ikinci aşamasında kullanıcıların bilgi güvenliğine dair gerçek davranışları ölçülerek bir önceki aşamada kendi beyanatları doğrultusunda sağlamış oldukları değişkenlerle arasındaki ilişkiler incelenmiştir. Bu kapsamda, katılımcıların davranış olarak ölçülebilecek ölçek maddelerini sanki bir web sitesinin kullanılabilirliğini ölçmek için uyguluyor izlenimi verilerek sergiledikleri doğal davranışlarla yanıtlamaları amaçlanmıştır. Bitton, Boymgold, Puzis ve Shabtai (2020) akıllı telefon kullanıcılarının bilgi güvenliği farkındalıklarını ölçmek istedikleri deneysel çalışmalarında, aynı amaç doğrultusunda ve benzer bir şekilde, katılımcılara kendilerinin cihaz kullanım alışkanlıklarının izlendiğini belirterek veri toplamışlardır. Bu amaç için Sufian, Salleh ve Judi (2010) yapmış oldukları çalışmada katılımcılara veri toplama

aşamasında hiç haber vermemeyi tercih ederken; Wu (2013) inceleme periyodu süresini uzun tutup katılımcıların kayıtlarının alınıyor olduğunu unutabileceğini varsayarak çalışmasını sonuçlandırmıştır. Bu aşamada hayata geçirilen çevrimiçi öğrenme ortamı eğitimi içeriğinin uyarlanabilmesi için kullanıcıların sınıflandırılması konsepti belirlenmiştir. Toplana veriler ışığında kullanıcıların bir davranışı gerçekleştirdiğini söyler ve davranışı gerçekleştirir (söyler ve yapar), davranışı gerçekleştirdiğini söyler ancak davranışı gerçekleştirmez (söyler ancak yapmaz), davranışı gerçekleştirmediğini söyler ancak davranışı gerçekleştirir (söylemez ancak yapar) ve davranışı gerçekleştirmediğini söyler ve davranışı gerçekleştirmez (söylemez ve yapmaz) sınıfları oluşturulmuştur. Gerçekleştirilen analizler katılımcıların söylemleri (niyetleri) ile gerçek davranışları arasında oluşan bu farklılıkların veya benzeşmelerin kişilik özellikleri, tehlike algıları, maruz kaldıkları bilgi güvenliği ihlali olayları ve dikkatleriyle ilgili olan yazma hızları ve okuduklarını görme değişkenlerinden etkilendikleri sonucuna ulaşılmıştır.

Bu aşamada toplanan veriler paradoksal bir durumu ortaya çıkarmıştır. Çalışma kapsamında veri toplamak için duyuru ve çağrılar belirli bir amaç için bir araya gelen ve genellikle bilimsel araştırma yapan kullanıcılardan oluşan, sosyal medya ve eposta grupları üzerinden yapılmıştır. Bu çağrı yapılırken verilerin bir doktora tez çalışması kapsamında kullanılacağı metin içeriğinde belirtilmiştir. Katılımcılar söze binaen, akademik bir çalışmaya katkı sunduklarını düşündükleri ve yardımcı olmak için SSL sertifikası bulunmayan bir site üzerinden kişisel bilgilerini paylaşıp, şifre oluşturmuşlardır. Bu işlemleri yaparken, bu aşamaya katılan hiçbir kullanıcı resmi bir belge talebinde bulunmamıştır. Aynı senaryonun kötü niyetli bir amaçla da tekrarlanabilir olması bilgi güvenliği farkındalığına yönelik boşluğun bir göstergesi durumundadır.

Çalışmanın üçüncü aşamasında ise toplanıp üzerinde analiz işlemleri yapılan veriler ışığında kullanıcı modellemesi veri madenciliği teknikleri ve makine öğrenmesi algoritmaları kullanılarak gerçekleştirilmiştir. Farklı algoritmalar kullanılarak gerçekleştirilen denemelerde C5.0 karar ağacı algoritmasının daha iyi sonuçlar vermesi ve araştırmacıya sağladığı kolaylıklar sebebiyle çalışma kapsamında kullanılmasına karar verilmiştir. Abdar vd. (2015) yapmış oldukları çalışmada C5.0, sinir ağları, destek vektör makineleri, K-en yakın komşu ve lojistik regresyon algoritmalarını karşılaştırmışlar %93.02 doğruluk oranı ile C5.0 karar ağacı algoritmasının en iyi sonucu verdiğini belirtmişlerdir. Kazemi, Hajian ve Kiani (2018) benzer bir şekilde yapmış oldukları çalışmada C5.0, sinir ağları, bayes ağları ve ensemble

algoritmalarını karşılaştırmış % 95.66 doğruluk oranı ile C5.0 karar ağacı algoritmasının en iyi sonucu verdiğini vurgulamışlardır. Thombre (2012) ise sinir ağları, C5.0, lojistik regresyon ve M5' algoritmalarını karşılaştırdığı çalışmasında M5' algoritmasının diğer algoritmalara göre daha iyi sonuçlar verdiğini belirtmiştir. (Khoraskani, Kheradmand ve Khamseh (2017) benzer şekilde yapmış oldukları çalışmada sinir ağları, C5.0 ve CART algoritmalarını karşılaştırmış, sinir ağları algoritmalarının daha iyi sonuç verdiğini vurgulamışlardır. Alanyazında çoğaltılabilecek bu örneklere göre farklı algoritmaların farklı sonuçlar vermesinin kullanılan verinin yapısı ve hacminden kaynaklanabileceği değerlendirilmiştir. Bu aşamada klasik istatistiki yöntemlerin kullanılmasıyla ortaya çıkan sonuçlarla karşılaştırmalar yapılarak özellik belirleme (feature seection) işlemleri nihayetlendirilmiştir. Oluşturulan karar ağacında her bir bilgi güvenliği davranışı için algoritmalar oluşturulmuştur. Bilgi güvenliğine yönelik, ölçülen bazı davranışlarda belirlenen 4 sınıfın tamamının oluşmasına karşın bazı davranışlarda daha az sınıfın oluştuğu görülmüştür. Örneğin; "*Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim*" davranışı için 4 sınıfın (söyler ve yapar, söyler ancak yapmaz, söylemez ancak yapar, söylemez ve yapmaz) tamamına da kullanıcı dâhil edilebilirken, "*Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim*" davranışı için sadece 2 sınıfın (söyler ancak yapmaz, söylemez ve yapmaz) oluşturulabildiği görülmüştür. Daha az sınıf oluşturulabilen davranışlar incelendiğinde "yapmaz" sınıflarının çoğunlukta olduğu tespit edilmiştir. Bu durumun katılımcıların ilgili bilgi güvenliği davranışı konusunda yoğunlukla bilgisinin olmaması daha az olasılıkla uygulaması konusunda eksiklikleri bulunmasından kaynaklandığı değerlendirilmiştir. 4 sınıfın oluşturulabildiği davranışların ise gerçek yaşamda hemen her bilgisayar kullanıcısının karşılaştığı ve görece aşinalığı olabilecek davranışlar olduğu görülmüştür.

Çalışmanın dördüncü ve son aşamasını ise uyarlanabilir çevrimiçi öğrenme ortamının prototipinin oluşturulması oluşturmaktadır. Çalışma kapsamında uyarlama içerik üzerine gerçekleştirilmiştir. Kullanıcı modellemesi için gerekli olan bilgiler sistem girişinde kullanıcının veri girişi yapması ile sağlanmıştır. Bu doğrultuda her bir davranış için farklı sınıflarda tanımlanan kullanıcılara bulunduğu sınıfa ait eğitim içerikleri sunulması şeklinde tasarım yapılmıştır. Genel konsept olarak bilgi güvenliği davranışı için "söyler ve yapar" sınıfına kullanıcının isteğine bağlı olarak eğitim içeriğinin sunulması veya sunulmaması, "söyler ancak yapmaz" sınıfına bir ihlal veya sorunla karşılaşmaması için neler yapması ya da yapmaması gerektiği, "söylemez ancak yapar" sınıfı için davranışa ait kuramsal bilgilerin

zorunlu, yapması ve yapmaması gereken durumlar kullanıcının isteğine bağlı olarak sunulması, "söylemez ve yapmaz" sınıfına ilgili tüm eğitim içeriğinin zorunlu olarak sunulması şeklinde oluşturulmuştur. Konu alanı uzmanlarından alınan görüşler eğitim içeriklerinin konuya özgü uygunluğunu teyit etmişlerdir.

Yapılan alanyazın ve gerçek hayat uygulaması araştırmaları neticesinde; bilgi güvenliğe yönelik bilimsel araştırmaların teknik cihaz ve uygulamalar üzerine yoğunlaşması, gerçek davranışı ölçerek bilgi güvenliği farkındalığını araştıran çalışmaların ise sayıca ve görece az olması, gerçek hayattaki bilgi güvenliği farkındalık eğitimlerinin hedef kitle göz önüne alındığında çok az bir kısmına ulaşması ve çevrimiçi yapıda olan öğrenme ortamlarının ise kişiselleştirilmiş içerik sağlamadığı için kullanıcının fazla bilgi yüklemesi ve yönlendirme problemlerine yol açabilmesi problemleri olduğu görülmüştür. Gerçekleştirilen bu çalışma ile belirtilen problemlerin giderilmesi çabalarına katkı sağlanmıştır.

Öneriler

Bu aşamada çalışmanın sonuçlarına göre araştırmacılara ve yapılacak benzer çalışmalara yönelik öneriler sunulmaktadır. Yapılan öneriler araştırmaya ve uygulamaya yönelik iki başlık altında toplanmıştır.

Uygulamaya Yönelik Öneriler

1- Mevcut çalışma kapsamında prototip olarak hayata geçirilen öğrenme ortamı, katılımcıların ölçeklere verdiği yanıtlar, çalışma başlangıcında etik kuruldan bu yönde bir talepte bulunulmadığından, bir veri tabanına kaydedilmeden işlenecek şekilde tasarlanmıştır. Etik kurul izni ve katılımcının onayı doğrultusunda toplanacak kişisel olarak tanımlanabilir bilgilerle ölçeklere verilen cevapların bir veri tabanına kaydedilmesiyle üzerinde koşulan algoritmanın oluşturduğu kural setlerinin kendini yenileyebilir bir yapıya dönüştürülmesi sağlanabilir. Bu sayede her yeni kullanıcı ile oluşturulan sistemin daha doğru sonuçlar ortaya koyması sağlanabilir.

2- Çalışma ile kullanıcılara öğrenirken zamanını etkili kullanabilmesi sağlanmıştır. Ancak bu kapsamda kullanıcıların öğrenme ortamındaki gezinme bilgileri kayıt altına alınmamıştır. Her bir kullanıcının sistemde her bir konu üzerinde geçirdiği zaman, sayfalar arasındaki geçişler ve geri dönüşlerin kayıt altına alınarak incelenebilir bir yapıya kavuşturulması, öğrenme sisteminin etkililiğinin ölçülebilmesi ve sayfanın yeniden düzenlenmeye ihtiyacının olup olmadığının belirlenebilmesi kazanımını sağlayacağı düşünülmektedir.

Gelecekteki Çalışmalar İçin Öneriler

1- Mevcut çalışma kapsamında olası tüm bilgi güvenliği davranışları çatı bir yapıda sınıflandırılmaya çalışılmıştır ancak bu konuda başarı sağlanamamıştır. Bu durumun sınıflandırma için kullanılan çalışmanın uygun olmamasından veya görüşü alınan uzman sayısının yeterli olmayışından kaynaklanabileceği değerlendirilmektedir. Belirtilen şekilde bir sınıflandırmanın gerçekleştirilmesi ile her bir bilgi güvenliği davranışı için ayrı ayrı sınıflandırma yapmaya gerek kalmayacağı öngörülmektedir. Bu sayede yeni belirlenen bir bilgi güvenliği davranışının hangi sınıfta yer alabileceğine karar verilmesi ile o sınıfa özgü işlemler kolayca uygulanabilecektir.

2- Mevcut çalışma kapsamında bireylerin bilgi güvenliğine yönelik, sadece web ortamında ölçülebilecek belirli davranışları incelenebilmiştir. Örneğin "Bilgisayarım bir şifre ile açılır" davranışının varlığı web ortamında ölçülememiştir. Akıllı cihazlar, masaüstü sistemler vb. üzerinde geliştirilecek uygulamalarla daha fazla davranışın ölçülebileceği bu sayede daha geniş eğitim içeriği hazırlanabileceği değerlendirilmektedir.

3- Bu çalışmada sosyal medya, eposta grupları vb. ortamlarda duyurusu yapılarak çalışmaya gönüllü katılımcılar davet edilmiştir. İlk veri toplama aşamasında 619, ikinci veri toplama aşamasında ise 619 katılımcının 301'i çalışmaya katkı sağlamıştır. Eğitimi verilen bazı davranışlar için, benzer cevapları veren ve davranışları gösteren katılımcıların kümelenmesi sebebiyle belirlenen 4 kullanıcı sınıfı oluşmamıştır. Ayrıca veri madenciliği uygulamaları ne kadar fazla veri ile çalışırsa alınan sonuçların doğruluk oranında o derecede artış sağlamaktadır. Bu sebeple benzer çalışmaların daha fazla katılımcı ile gerçekleştirilmesi daha iyi sonuçların alınmasında etkili olacaktır.

4- Bu çalışma kapsamında makine öğrenmesi algoritmalarından kullanılan yazılımın sunduğu karar ağacı algoritmalarından bazıları karşılaştırılarak en iyi sonucu veren C5.0 algoritması kullanılmıştır. Benzer çalışmaların alan yazında bulunan farklı algoritmalar kullanılarak yinelenmesi ile farklı sonuçların alınabileceği düşünülmektedir.
5- Kullanılan parametreler değiştirilebilir bir yapıda olmadığı için çalışma da esnek bir yapıda değildir. Gerçekleştirilecek benzer çalışmaların revize edilebilecek bir yapıda tasarlanması diğer araştırmacıların da kullanabileceği bir ürüne dönüşebilmesi açısından yararlı olacaktır.
6- Yapılan çalışmanın etkililiğinin değerlendirilmesi, son kullanıcıların kullanımına sunularak ölçülmemiştir. Yapılan değerlendirme uzman görüşü alınarak gerçekleştirilmiştir. İşe vuruk olarak gerçekleştirilecek bir değerlendirmenin çalışmanın etkililiğini ölçmede daha iyi çıkarımların yapılabilmesine olanak sağlayacağı düşünülmektedir.

KAYNAKLAR

Abdar, M., Kalhori, S. R. N., Sutikno, T., Subroto, I. M. I., & Arji, G. (2015). Comparing Performance of Data Mining Algorithms in Prediction Heart Diseases. *International Journal of Electrical & Computer Engineering (2088-8708)*, *5*(6)., 1569-1575

Abraham, S., & Chengalur-Smith, I. (2010). An overview of social engineering malware: Trends, tactics, and implications. *Technology in Society*, *32*(3), 183-196.

Aburrous, M., Hossain, M. A., Dahal, K., & Thabtah, F. (2010). Experimental Case Studies for Investigating E-Banking Phishing Techniques and Attack Strategies. *Cognitive Computation*, *2*(3), 242-253. https://doi.org/10.1007/s12559-010-9042-7

ACM, J. T. F. (2017). *Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity* (Technical Report 1.0; CSEC2017, s. 123). ACM, IEEE, AIS SIGSEG.

Adıgüzel, O., Batur, H. Z., & Ekşili, N. (2014). Kuşakların değişen yüzü ve Y kuşağı ile ortaya çıkan yeni çalışma tarzı: Mobil yakalılar. *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *1*(19), 165-182.

Aggarwal, C. C., & Yu, P. S. (2000). Data mining techniques for personalization. *IEEE Data Eng. Bull.*, *23*(1), 4-9.

Aghaei, S., Nematbakhsh, M. A., & Farsani, H. K. (2012). Evolution of the world wide web: From WEB 1.0 TO WEB 4.0. *International Journal of Web & Semantic Technology*, *3*(1), 1-10.

Aher, S. B., & Lobo, L. (2012). A comparative study of association rule algorithms for course recommender system in e-learning. *International Journal of Computer Applications*, *39*(1), 48-52.

Ajzen, I., Brown, T. C., & Carvajal, F. (2004). Explaining the Discrepancy between Intentions and Actions: The Case of Hypothetical Bias in Contingent Valuation. *Personality and Social Psychology Bulletin*, *30*(9), 1108-1121. https://doi.org/10.1177/0146167204264079

Aldowah, H., Al-Samarraie, H., & Fauzy, W. M. (2019). Educational Data Mining and Learning Analytics for 21stcentury higher education: A Review and Synthesis. *Telematics and Informatics*, 37, 13-49.

Algarni, A. (2016). Data mining in education. *International Journal of Advanced Computer Science and Applications*, *7*(6), 456-461.

Alhabeeb, M., Almuhaideb, A., Le, P. D., & Srinivasan, B. (2010). Information Security Threats Classification Pyramid. *2010 IEEE 24th International Conference on Advanced Information Networking and Applications Workshops*, 208-213. https://doi.org/10.1109/WAINA.2010.39

Ally, M. (2004). Foundations of educational theory for online learning. *Theory and practice of online learning*, *2*, 15-44.

Al-Saggaf, Y. (2017). Information sharing on Facebook by Alone, Single and Lonely Female Users. *SEARCH: The Journal of the South East Asia Research Centrefor Communications and Humanities*, *9*(1), 97-116.

Alshammari, R., & Nur Zincir-Heywood, A. (2015). Identification of VoIP encrypted traffic using a machine learning approach. *Journal of King Saud University - Computer and Information Sciences*, *27*(1), 77-92. https://doi.org/10.1016/j.jksuci.2014.03.013

Amankwa, E., Loock, M., & Kritzinger, E. (2014). A conceptual analysis of information security education, information security training and information security awareness definitions. *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, 248-252. https://doi.org/10.1109/ICITST.2014.7038814

Amidi, S. (2019). *Makine Öğrenmesi ipuçları ve püf noktaları el kitabı*. Stanford University. https://stanford.edu/~shervine/l/tr/teaching/cs-229/cheatsheet-machine-learning-tips-and-tricks#classification-metrics sayfasından erişilmiştir.

Anastopoulos, V., & Katsikas, S. (2018). Design of a dynamic log management infrastructure using risk and affiliation network analysis. *Proceedings of the 22nd Pan-Hellenic Conference on Informatics - PCI '18*, 52-57. https://doi.org/10.1145/3291533.3291570

Anderson, C., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, *34*(3), 613. https://doi.org/10.2307/25750694

Anuradha, J. (2015). A brief introduction on Big Data 5Vs characteristics and Hadoop technology. *Procedia computer science*, *48*, 319-324.

Anyanwu, M. N., & Shiva, S. G. (2009). Comparative analysis of serial decision tree classification algorithms. *International Journal of Computer Science and Security*, *3*(3), 230-240.

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312. https://doi.org/10.1016/j.chb.2014.05.046

Arı, E. (2013). Temel Kavramlar. Içinde *Öğrenme Öğretme Kuram ve yaklaşımları* (2. bs, ss. 2-21). Pegem Akademi.

Arkorful, V., & Abaidoo, N. (2015). The role of e-learning, advantages and disadvantages of its adoption in higher education. *International Journal of Instructional Technology and Distance Learning*, *12*(1), 29-42.

Aronson, J. E., Liang, T.-P., & Turban, E. (2007). *Decision support systems and intelligent systems* (C. 7). Pearson Prentice-Hall New York.

Atalay, M., & Çelik, E. (2017). Büyük Veri Analizinde Yapay Zekâ Ve Makine Öğrenmesi Uygulamalari-Artificial Intelligence and Machine Learning Applications in Big Data Analysis. *Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, *9*(22), 155-172.

Average Time Spent Daily on Social Media. (2020). [Araştırma]. *Broadbandsearch*. Average Time Spent Daily on Social Media

Awan, M. S. K., Burnap, P., Rana, O., & Javed, A. (2015). Continuous Monitoring and Assessment of Cybersecurity Risks in Large Computing Infrastructures. *2015 IEEE 17th International Conference on High Performance Computing and Communications, 2015 IEEE 7th International Symposium on Cyberspace Safety and Security, and 2015 IEEE 12th International Conference on Embedded Software and Systems*, 1442-1447. https://doi.org/10.1109/HPCC-CSS-ICESS.2015.224

Aytekin, A., Çakır, F. S., Yücel, Y. B., & Kulaözü, İ. (2018). Algoritmaların Hayatımızdaki Yeri ve Önemi. *Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi*, *5*(7), 143-150.

Ayyagari, R. (2012). An exploratory analysis of data breaches from 2005-2011: Trends and insights. *Journal of Information Privacy and Security*, *8*(2), 33-56.

Babbie, E. R. (2016). *The practice of social research* (14. bs). Nelson Education.

Bagozzi, R. (2007). The Legacy of the Technology Acceptance Model and a Proposal for a Paradigm Shift. *Journal of the Association for Information Systems*, *8*(4), 244-254. https://doi.org/10.17705/1jais.00122

Baker, R. S., & Inventado, P. S. (2014). Educational data mining and learning analytics. Içinde *Learning analytics* (ss. 61-75). Springer.

Barab, S., & Squire, K. (2004). Design-Based Research: Putting a Stake in the Ground. *Journal of the Learning Sciences*, *13*(1), 1-14. https://doi.org/10.1207/s15327809jls1301_1

Baskaran, M. M., Henretty, T., Ezick, J., Lethin, R., & Bruns-Smith, D. (2019). Enhancing Network Visibility and Security through Tensor Analysis. *Future Generation Computer Systems*, *96*, 207-215. https://doi.org/10.1016/j.future.2019.01.039

Başaran, A. (2016). *Siber Savaş Cephesinden Notlar*. İstanbul: Arion

Bejtkovský, J. (2016). The current generations: The baby boomers, x, y and z in the context of human capital management of the 21st century in selected corporations in the Czech Republic. *Littera scripta*, *9*(2), 25-45.

Berg, K. L., Seymour, T., & Goel, R. (2013). History of databases. *International Journal of Management & Information Systems (IJMIS)*, *17*(1), 29-36.

Berger, H., & Jones, A. (2016). Cyber Security & Ethical Hacking For SMEs. *Proceedings of the The 11th International Knowledge Management in Organizations Conference on The changing face of Knowledge Management Impacting Society*, 12.

Berners-Lee, T., Dimitroyannis, D., Mallinckrodt, A. J., & McKay, S. (1994). World Wide Web. *Computers in Physics*, *8*(3), 298-299.

Bıçakçı, S. (2014). NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik. *International Relations/Uluslararasi Iliskiler*, *10*(40).

Bishop, L. M., Morgan, P. L., Asquith, P. M., Raywood-Burke, G., Wedgbury, A., & Jones, K. (2020). Examining human individual differences in cyber security and possible implications for human-machine interface design. *International Conference on Human-Computer Interaction*, 51-66.

Bitton, R., Boymgold, K., Puzis, R., & Shabtai, A. (2020). Evaluating the Information Security Awareness of Smartphone Users. *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, 1-13. https://doi.org/10.1145/3313831.3376385

Bostan, A., & Şengül, G. (2018). *Siber Güvenlik Farkındalığı Oluşturma*. Grafiker Yayınları. https://www.sasad.org.tr/uploaded/Siber-Guvenlik-ve-Savunma-Farkindalik-ve-Caydiricilik.pdf sayfasından erişilmiştir.

Brooks, C., & Craig, T. (2017). Predictive Modelling in Teaching and Learning. Içinde Columbia University, USA, C. Lang, G. Siemens, University of Texas at Arlington, USA, A. Wise, New York University, USA, D. Gasevic, & University of Edinburgh, UK (Ed.), *Handbook of Learning Analytics* (First, C. 1-61-68, ss. 319-326). Society for Learning Analytics Research (SoLAR). https://doi.org/10.18608/hla17.027

Brusilovsky, P. (1998). Adaptive educational systems on the world-wide-web: A review of available technologies. *Proceedings of Workshop" WWW-Based Tutoring" at 4th International Conference on Intelligent Tutoring Systems (ITS'98), San Antonio, TX*.

Brusilovsky, P. (2001). Adaptive Hypermedia. *User Modeling and User-Adapted Interaction*, *11*, 87-110.

Brusilovsky, P. (2007). Adaptive navigation support. Içinde *The adaptive web* (ss. 263-290). Springer.

Brusilovsky, P. (1996). Adaptive hypermedia: An attempt to analyze and generalize. *International Conference on Multimedia, Hypermedia, and Virtual Reality*, 288-304.

Brusilovsky, P., & Pesin, L. (1994). ISIS-Tutor: An intelligent learning environment for CDS/ISIS users. *Proceedings of CLCE, 94*.

Butavicius, M. A., Parsons, K., Pattinson, M. R., McCormac, A., Calic, D., & Lillie, M. (2017). Understanding susceptibility to phishing emails: Assessing the impact of individual differences and culture. *HAISA*, 12-23.

Büyüköztürk, Ş., Çakmak, E. K., Akgün, Ö. E., Karadeniz, Ş., & Demirel, F. (2014). *Bilimsel araştırma yöntemleri* (18. bs). Pagem Akademi.

Canbek, G., & Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi*, *9*(3).

Carstens, D. S., Malone, L. C., DeMara, R., & McCauley-Bell, P. R. (2004). Evaluation of the Human Impact of Password Authentication Practices on Information Security. *Informing Science Journal*, 67-85.

Ceruzzi, P. E. (2003). *A history of modern computing* (2nd bs). MIT press.

Chen, J. V., Chen, C. C., & Yang, H.-H. (2008). An empirical evaluation of key factors contributing to internet abuse in the workplace. *Industrial Management & Data Systems*.

Chen, S. (2002). A cognitive model for non–linear learning in hypermedia programmes. *British journal of educational technology*, *33*(4), 449-460.

Choi, M.-K., Robles, R. J., Hong, C., & Kim, T. (2008). Wireless network security: Vulnerabilities, threats and countermeasures. *International Journal of Multimedia and Ubiquitous Engineering*, *3*(3), 77-86.

Choudhury, N. (2014). World wide web and its journey from web 1.0 to web 4.0. *International Journal of Computer Science and Information Technologies*, *5*(6), 8096-8100.

Chrysafiadi, K., & Virvou, M. (2013). Student modeling approaches: A literature review for the last decade. *Expert Systems with Applications*, *40*(11), 4715-4729. https://doi.org/10.1016/j.eswa.2013.02.007

Ciloglugil, B., & Inceoglu, M. M. (2012). User Modeling for Adaptive E-Learning Systems. Içinde *Lecture Notes in Computer Science* (C. 7335, ss. 550-561).

Cios, K. J., Swiniarski, R. W., & Pedrycz, W. (2007). *Data Mining Methods for Knowledge Discovery*. Springer.

Clark, J., Leblanc, S., & Knight, S. (2011). Risks associated with USB Hardware Trojan devices used by insiders. *2011 IEEE International Systems Conference*, 201-208. https://doi.org/10.1109/SYSCON.2011.5929130

Clarke, N., Symes, J., Saevanee, H., & Furnell, S. (2016). Awareness of Mobile Device Security: A Survey of User's Attitudes. *International Journal of Mobile Computing and Multimedia Communications*, *7*(1), 15-31. https://doi.org/10.4018/IJMCMC.2016010102

Conklin, J. (1987). Hypertext: An introduction and SurvevJ. *computer*, *20*(9), 17-41.

Cooke, L. (2010). Assessing Concurrent Think-Aloud Protocol as a Usability Test Method: A Technical Communication Approach. *IEEE Transactions on Professional Communication*, *53*(3), 202-215. https://doi.org/10.1109/TPC.2010.2052859

Costante, E., Fauri, D., Etalle, S., den Hartog, J., & Zannone, N. (2016). A Hybrid Framework for Data Loss Prevention and Detection. *2016 IEEE Security and Privacy Workshops (SPW)*, 324-333. https://doi.org/10.1109/SPW.2016.24

Coughlin, T. (2018). *175 Zettabytes By 2025* [Enterprise Tech]. Forbes. https://www.forbes.com/sites/tomcoughlin/2018/11/27/175-zettabytes-by-2025/#744b69245459 sayfasından erişilmiştir.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, *32*, 90-101. https://doi.org/10.1016/j.cose.2012.09.010

Çakır, H., Çebi, A., & Özcan, S. (2013). BÖTE Nedir? Nasıl Tanımlanır? Okul Müzesiyle Başlayan Serüvenden İnsan Performans Teknolojilerine Uzanan Yolculuk. *Eğitim Teknolojisi Kuram ve Uygulama*, *3*(2), 102–111.

Çintiriz, H., & Durak, M. (2014). *Kurumsal Siber Güvenlik Tedbirlerinin Sistem Mühendisliği Yaklaşım Modeli İle Değerlendirilmesi*. 7. uluslararsı Bilgi Güvenliği ve Kriptoloji Konferansı.

Dash, R., Paramguru, R. L., & Dash, R. (2011). Comparative analysis of supervised and unsupervised discretization techniques. *International Journal of Advances in Science and Technology*, *2*(3), 29-37.

De Bra, P., Houben, G.-J., & Wu, H. (1999). AHAM: a Dexter-based reference model for adaptive hypermedia. *Proceedings of the tenth ACM Conference on Hypertext and hypermedia: returning to our diverse roots: returning to our diverse roots*, 147-156.

Demchenko, Y., De Laat, C., & Membrey, P. (2014). Defining architecture components of the Big Data Ecosystem. *2014 International Conference on Collaboration Technologies and Systems (CTS)*, 104-112.

Demirel, Ö. (2007). *Kuramdan uygulamaya eğitimde program geliştirme*. Pegem Akademi.

Denning, D. E. (2003). Cyber Security as an Emergent Infrastructure. *World Conference on Information Security Education*, 1-2.

Dev Mishra, A., & Beer Singh, Y. (2016). Big data analytics for security and privacy challenges. *2016 International Conference on Computing, Communication and Automation (ICCCA)*, 50-53. https://doi.org/10.1109/CCAA.2016.7813688

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). Why phishing works. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '06*, 581. https://doi.org/10.1145/1124772.1124861

Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, *43*(7), 125-128.

Dias, P., & Sousa, P. (1997). Understanding navigation and disorientation in hypermedia learning environments. *Journal of educational multimedia and hypermedia*, *6*(2), 173-185.

Dillon, A., & Gabbard, R. (1998). Hypermedia as an educational technology: A review of the quantitative research literature on learner comprehension, control, and style. *Review of educational research, 68*(3), 322-349.

Dimkov, T., Van Cleeff, A., Pieters, W., & Hartel, P. (2010). Two methodologies for physical penetration testing using social engineering. *Proceedings of the 26th annual computer security applications conference*, 399-408.

Dinov, I. D. (2018). Decision Tree Divide and Conquer Classification. Içinde *Data Science and Predictive Analytics* (ss. 307-343). Springer International Publishing. https://doi.org/10.1007/978-3-319-72347-1_9

Dodel, M., & Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human behavior*, *68*, 359-367.

Dursun, A., & Özkan, M. S. (2019). Genç Yetişkinlerin Aldatmaya Yönelik Niyetleri Üzerinde Aldatmaya Yönelik Tutum Ve Sosyal Medya Kullanımının Etkisi. *Kastamonu Eğitim Dergisi*, *27*(2), 475-484. https://doi.org/10.24106/kefdergi.2560

Dwivedi, Y. K., Williams, M. D., Mitra, A., Niranjan, S., & Weerakkody, V. (2011). Understanding advances in web technologies: Evolution from web 2.0 to web 3.0. *ECIS, 2011*, 257.

Edelson, D. C. (2002). Design Research: What We Learn When We Engage in Design. *Journal of the Learning Sciences*, *11*(1), 105-121. https://doi.org/10.1207/S15327809JLS1101_4

Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale (sebis). *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 2873-2882.

Eklund, J., & Brusilovsky, P. (1999). Interbook: An adaptive tutoring system. *UniServe Science News*, *12*(3), 8-13.

Emel, G. G., & Taşkın, Ç. (2005). Veri Madenciliğinde Karar Ağaçları ve Bir Satış Analizi Uygulaması. *Eskişehir Osmangazi Üniversitesi Sosyal Bilimler Dergisi*, *6*(2), 221-239.

Eminağaoğlu, M., & Gökşen, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir? Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11*(4).

European Union, & Agency for Network and Information Security. (2019). *ENISA threat landscape report 2018: 15 top cyberthreats and trends.* https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/at_download/fullReport sayfasından erişilmiştir.

Faaliyet Raporu (s. 149). (2019). Bilgi TEknolojileri ve İletişim Kurumu. https://www.btk.gov.tr/uploads/pages/faaliyet-raporlari/2019-genel-faaliyetraporu.pdf sayfasından erişilmiştir.

Facione, P. (1990). *Critical thinking: A statement of expert consensus for purposes of educational assessment and instruction (The Delphi Report)*.

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015). Information security awareness in educational institution: An analysis of students' individual factors. *2015 IEEE Trustcom/BigDataSE/ISPA, 1*, 352-359.

Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). From data mining to knowledge discovery in databases. *AI magazine, 17*(3), 37-37.

Feenberg, A. (1993). 7 7 Building a global network: The WBSI experience. *Global networks: Computers and international communication*, *185*.

Fernández, A., del Río, S., Chawla, N. V., & Herrera, F. (2017). An insight into imbalanced Big Data classification: Outcomes and challenges. *Complex & Intelligent Systems*, *3*(2), 105-120. https://doi.org/10.1007/s40747-017-0037-9

Filkins, B. (2016). *IT Security Spending Trends*. SANS.

Flores, W. R., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *computers & security*, *59*, 26-44.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in human behavior*, *25*(1), 153-160.

Fonteyn, M. E., Kuipers, B., & Grobe, S. J. (1993). A Description of Think Aloud Method and Protocol Analysis. *Qualitative Health Research*, *3*(4), 430-441. https://doi.org/10.1177/104973239300300403

Franke, U., & Brynielsson, J. (2014). Cyber situational awareness–a systematic review of the literature. *Computers & Security*, *46*, 18-31.

Frick, T. W., & Reigeluth, C. M. (1999). Formative research: A methodology for creating and improving design theories. *Instructional-design theories and models: A new paradigm of instructional theory*, *2*, 633-652.

Fu, M. R., Wang, Y., Li, C., Qiu, Z., Axelrod, D., Guth, A. A., Scagliola, J., Conley, Y., Aouizerat, B. E., Qiu, J. M., Yu, G., Van Cleave, J. H., Haber, J., & Cheung, Y. K. (2018). Machine learning for detection of lymphedema among breast cancer survivors. *mHealth*, *4*, 17-17. https://doi.org/10.21037/mhealth.2018.04.02

Gandomi, A., & Haider, M. (2015). Beyond the hype: Big data concepts, methods, and analytics. *International Journal of Information Management*, *35*(2), 137-144. https://doi.org/10.1016/j.ijinfomgt.2014.10.007

Gao, Y., & Zhang, S. (2018). Design of and Research on Autonomous Learning System for Distance Education based on Data Mining Technology. *Kuram ve Uygulamada Egitim Bilimleri*, *18*(6), 2633-2640.

Gerić, S., & Hutinski, Ž. (2007). İnformation System Security Threat Classification. *Journal of Information and Organizational Sciences*, *31*(1), 51-61.

Ghafir, I., Saleem, J., Hammoudeh, M., Faour, H., Prenosil, V., Jaf, S., Jabbar, S., & Baker, T. (2018). Security threats to critical infrastructure: The human factor. *The Journal of Supercomputing*, *74*(10), 4986-5002.

Giannadakis, N., Rowe, A., Ghanem, M., & Guo, Y. (2003). InfoGrid: Providing information integration for knowledge discovery. *Information Sciences*, *155*(3-4), 199-226. https://doi.org/10.1016/S0020-0255(03)00170-1

Golkarian, A., Naghibi, S. A., Kalantar, B., & Pradhan, B. (2018). Groundwater potential mapping using C5.0, random forest, and multivariate adaptive regression spline models in GIS. *Environmental Monitoring and Assessment*, *190*(3), 149. https://doi.org/10.1007/s10661-018-6507-8

Goncalves, J. F., da Silva e Silva, F. J., Vasconcelos, R. O., Baptista, G. L. B., & Endler, M. (2013). A security infrastructure for massive mobile data distribution. *Proceedings of the 11th ACM international symposium on Mobility management and wireless access*, 41-50.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, 345-358.

Gu, Q., Wang, X.-M., Wu, Z., Ning, B., & Xin, C.-S. (2016). An improved SMOTE algorithm based on genetic algorithm for imbalanced data classification. *Journal of Digital Information Management*, *14*(2), 92-103.

Gupta, B., Rawat, A., Jain, A., Arora, A., & Dhami, N. (2017). Analysis of Various Decision Tree Algorithms for Classification in Data Mining. *International Journal of Computer Applications*, *163*(8), 15-19. https://doi.org/10.5120/ijca2017913660

Guruler, H., Istanbullu, A., & Karahasan, M. (2010). A new student performance analysing system using knowledge discovery in higher educational databases. *Computers & Education*, *55*(1), 247-254.

Gülpınar, N., & Atıcı, K. B. (2014). Performance Evaluation of Mobile Phone Producers. Içinde *Encyclopedia of Business Analytics and Optimization* (ss. 1836-1846). IGI Global.

Gültaş, irfan, & Tüzüner, L. (2017). Verimlilik Karşıtı İş Davranışlarının Beş Faktör Kişilik Özellikleri ve Bilişsel Yetenek ile İlişkisi. *İstanbul Üniversitesi İşletme Fakültesi Dergisi*, *46*(1), 47-61.

Haber, M. J., & Hibbert, B. (2018). *Asset Attack Vectors*. Apress. https://doi.org/10.1007/978-1-4842-3627-7

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7), e00346.

Hadlington, L., & Chivers, S. (2018). Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors. *Policing: A Journal of Policy and Practice*, *14*(2), 479-492. https://doi.org/10.1093/police/pay027

Hadlington, L., Popovac, M., Janicke, H., Yevseyeva, I., & Jones, K. (2019). Exploring the role of work identity and work locus of control in information security awareness. *Computers & Security*, *81*, 41-48. https://doi.org/10.1016/j.cose.2018.10.006

Halevi, T., Lewis, J., & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. *Proceedings of the 22nd International Conference on World Wide Web*, 737-744.

Hamburger, Y. A., & Ben-Artzi, E. (2000). The relationship between extraversion and neuroticism and the different uses of the Internet. *Computers in human behavior*, *16*(4), 441-449.

Hammad, K. A. I., Fakharaldien, M., Zain, J., & Majid, M. (2015). Big data analysis and storage. *International Conference on Operations Excellence and Service Engineering*, 10-11.

Han, Jiawei, & Kamber, M. (2006). *Data mining: Concepts and techniques* (2nd ed). Elsevier ; Morgan Kaufmann.

Han, Jing, Haihong, E., Le, G., & Du, J. (2011). Survey on NoSQL database. *2011 6th international conference on pervasive computing and applications*, 363-366.

Hand, D. (2007). Principles of Data Mining. *Drug Safety*, *30*, 2.

Harmanci, H., Dayioğlu, H., & Kirkpinar, S. N. (2019). Üniversite Öğrencilerinin Sosyal Medya Bağımlılığı ve Olumlu Değerlendirme Korkusu ile Olumsuz Değerlendirme Korkusu Arasındaki İlişkinin İncelenmesi. *Karatay Sosyal Araştırmalar Dergisi*, *3*, 242-255.

He, H., & Garcia, E. A. (2009). Learning from Imbalanced Data. *IEEE Transactions on Knowledge and Data Engineering*, *21*(9), 1263-1284. https://doi.org/10.1109/TKDE.2008.239

He, W. (2013). Examining students' online interaction in a live video streaming environment using data mining and text mining. *Computers in Human Behavior*, *29*(1), 90-102.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106-125. https://doi.org/10.1057/ejis.2009.6

Hesketh, E. A., & Laidlaw, J. M. (2002). Developing the teaching instinct, 4: Needs Assessment. *Medical Teacher*, *24*(6), 594-597. https://doi.org/10.1080/0142159021000063907

Hogben, G., & Dekker, M. (2010). *Smartphones: Information security risks, opportunities and recommendations for users*. ENISA.

Holst, A. (2020). *Worldwide information security services spending from 2017 to 2020* (IT Services) [Technical]. Statista. https://www.statista.com/statistics/217362/worldwide-it-security-spending-since-2010/ sayfasından erişilmiştir.

Houben, G.-J. (2004). Challenges in Adaptive Web Information Systems: Don't Forget the Link! *ICWE Workshops*, 3-11.

Hu, Q., West, R., & Smarandescu, L. (2015). The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. *Journal of Management Information Systems*, *31*(4), 6-48.

Huang, M., Huang, H., & Chen, M. (2007). Constructing a personalized e-learning system based on genetic algorithm and case-based reasoning approach. *Expert Systems with Applications*, *33*(3), 551-564. https://doi.org/10.1016/j.eswa.2006.05.019

Internet Crime Report (s. 28). (2018). Internet Crime Complaint Center.

Irmak, H., & Reis, Z. A. (2018). A Web-Based Awareness Education Against Social Engineering Attacks Sosyal Mühendislik Saldırılarına Karşı Web Tabanlı Bir Farkındalık Eğitimi. *PREFACE OF THE EDITORS*, 108.

İşman, A. (2011). *Uzaktan Eğitim* (4. bs). Pagem Akademi.

Iwai, T., Kondo, K., Lim, D. S. J., Ray, G., & Shimizu, H. (1999). *Japanese language needs analysis 1998-1999* (s. 87). University of Hawai'i, Second Language Teaching & Curriculum Center.

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94-100.

Jayathilake, D. (2012). Towards structured log analysis. *2012 Ninth International Conference on Computer Science and Software Engineering (JCSSE)*, 259-264. https://doi.org/10.1109/JCSSE.2012.6261962

Jazayeri, M. (2007). Some trends in web application development. *Future of Software Engineering (FOSE'07)*, 199-213.

Jeon, W., Kim, J., Lee, Y., & Won, D. (2011). A practical analysis of smartphone security. *Symposium on Human Interface*, 311-320.

Jinnai, R., Inomata, A., Arai, I., & Fujikawa, K. (2017). Proposal of hardware device model for IoT endpoint security and its implementation. *2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, 91-93. https://doi.org/10.1109/PERCOMW.2017.7917533

Jones, S. J., & Burnett, G. E. (2007). Spatial skills and navigation of source code. *ACM SIGCSE Bulletin*, *39*(3), 231. https://doi.org/10.1145/1269900.1268852

Jones, T. S., & Richey, R. C. (2000). Rapid prototyping methodology in action: A developmental study. *Educational Technology Research and Development*, *48*(2), 63-80.

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of security threats in information systems. *Procedia Computer Science*, *32*, 489-496.

Jovanovic, M., Vukicevic, M., Milovanovic, M., & Minovic, M. (2012). Using data mining on student behavior and cognitive style data for improving e-learning systems: A case study. *International Journal of Computational Intelligence Systems*, *5*(3), 597-610. https://doi.org/10.1080/18756891.2012.696923

Kantardzic, M. (2011). *Data mining: Concepts, models, methods, and algorithms* (2nd ed). John Wiley : IEEE Press.

Karadeniz, Ş. (2006). Öğretim Amaçlı Hiper Metin, Hiper Ortam ve Çoklu Ortamlar için Tasarım İpuçları. *Yüzüncü Yıl Üniversitesi, Eğitim Fakültesi Dergisi.*, *3*(2), 12-33.

Karakasiliotis, A., Furnell, S. M., & Papadaki, M. (2006). *Assessing end-user awareness of social engineering and phishing*.

Kazemi, M. A. A., Hajian, S., & Kiani, N. (2018). Quality Control and Classification of Steel Plates Faults Using Data Mining. *Applied Mathematics & Information Sciences Letters*, *6*(2), 59-67. https://doi.org/10.18576/amisl/060202

Kelly, A. E. (2013). When is Design Research Appropriate? Içinde *Educational design research. An introduction Part A Part A* (ss. 134-151). SLO.

Kemp, S. (2019). *We are Social* (Global Digital Report, s. 221). https://wearesocial.com/global-digital-report-2019

Kent, K., & Murugiah, S. (2006). *Guide to Computer Security Log Management* (Technical Report Sy 800-92; s. 72). National Institute of Standards and Technology.

Keser, H., & Güldüren, C. (2015). Bilgi Güvenliği Farkındalık Ölçeği (BGFÖ) Geliştirme. *Kastamonu Eğitim Dergisi*, *23*(3), 1167-1184.

Khoraskani, M. M., Kheradmand, F., & Khamseh, A. A. (2017). Application and comparison of neural network, C5.0, and classification and regression trees algorithms in the credit risk evaluation problem (case study: A standard German credit dataset). *International Journal of Knowledge Engineering and Data Mining*, *4*(3/4), 259. https://doi.org/10.1504/IJKEDM.2017.091013

Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a Cybersecurity Curriculum: Professional Certifications as Valuable Guidance. *Journal of Information Systems Education*, *28*(2), 101-114.

Knutov, E., De Bra, P., & Pechenizkiy, M. (2009). AH 12 years later: A comprehensive survey of adaptive hypermedia methods and techniques. *New Review of Hypermedia and Multimedia*, *15*(1), 5-38. https://doi.org/10.1080/13614560902801608

Ko, S. S., & Rossen, S. (2017). *Teaching online: A practical guide* (Fourth edition). Routledge.

Kott, A., & Arnold, C. (2013). The Promises and Challenges of Continuous Monitoring and Risk Scoring. *IEEE Security & Privacy*, *11*(1), 90-93. https://doi.org/10.1109/MSP.2013.19

Krawczyk, B. (2016). Learning from imbalanced data: Open challenges and future directions. *Progress in Artificial Intelligence*, *5*(4), 221-232.

Krishnamurthy, B., & Wills, C. E. (2009). On the leakage of personally identifiable information via online social networks. *Proceedings of the 2nd ACM workshop on Online social networks*, 7-12.

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and applications*, *22*, 113-122.

KS, D., & Kamath, A. (2017). Survey on Techniques of Data Mining and its Applications. *International Journal of Emerging Research in Management &Technology*, *6*(2).

Kumaraguru, P. (2009). *Phishguru: A system for educating users about semantic attacks*. ProQuest.

Kurpjuhn, T. (2013). The evolving role of the UTM appliance. *Network Security*, *2013*(1), 8-11. https://doi.org/10.1016/S1353-4858(13)70018-7

Kurtul, A., Zeyveli, F., İnce, Y., Yıldız, K., Yüce, H., & Yakaryılmaz, F. (2020). *Siber Güvenlik Raporu* (s. 33) [Technical]. Bilişim ve İnovasyon Derneği. http://www.bilisiminovasyon.org.tr/webfiles/userfiles/files/siber_guvenlik_raporu.pdf sayfasından erişilmiştir.

Kuzu, A., Çankaya, S., & Mısırlı, Z. A. (2011). Tasarım Tabanlı Araştırma ve Öğrenme Ortamlarının Tasarımı ve Geliştirilmesinde Kullanımı. *Anadolu Journal of Educational Sciences International, 1*(1), 19-35.

Küçükkalay, M. (1997). Endüstri Devrimi ve Ekonomik Sonuçlarının Analizi. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, *2*(2).

Lakshmi, B. N., & Raghunandhan, G. H. (2011). A conceptual overview of data mining. *2011 National Conference on Innovations in Emerging Technology*, 27-32.

Larose, D. T., & Larose, C. D. (2014). *Discovering knowledge in data: An introduction to data mining* (C. 4). John Wiley & Sons.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., & Wolff, S. (2009). A brief history of the Internet. *ACM SIGCOMM Computer Communication Review*, *39*(5), 22-31.

Lema^ıtre, G., Guillaume, F., & Aridas, C. K. (2017). Imbalanced-learn: A Python Toolbox to Tackle the Curse of Imbalanced Datasets in Machine Learning. *Journal of Machine Learning Research*, *18*, 1-5.

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: Overview and issues. *Crime, Law and Social Change*, *67*(1), 3-20.

Lim, E.-P., Srivastava, J., Prabhakar, S., & Richardson, J. (1996). Entity identification in database integration. *Information Sciences*, *89*(1-2), 1-38.

Lin, C. F., Yeh, Y., Hung, Y. H., & Chang, R. I. (2013). Data mining for providing a personalized learning path in creativity: An application of decision trees. *Computers & Education*, *68*, 199-210. https://doi.org/10.1016/j.compedu.2013.05.009

Lineberry, S. (2007). The human element: The weakest link in information security. *Journal of Accountancy*, *204*(5), 44.

Liu, J., Xiao, Y., & Chen, C. P. (2012). Authentication and access control in the internet of things. *2012 32nd International Conference on Distributed Computing Systems Workshops*, 588-592.

Lyman, E. R. (1972). *A Summary of Plato Curriculum and Research Materials.*

M. Omar, & M. Dawson. (2013). Research in Progress—Defending Android Smartphones from Malware Attacks. *2013 Third International Conference on Advanced Computing and Communication Technologies (ACCT)*, 288-292. https://doi.org/10.1109/ACCT.2013.69

Machado, C. J. R., Lima, B. R. B., Maciel, A. M., & Rodrigues, R. L. (2016). An investigation of students behavior in discussion forums using Educational Data Mining. *SEKE*, 510-514.

Madani, A., Rezayi, S., & Gharaee, H. (2011). Log management comprehensive architecture in Security Operation Center (SOC). *2011 International Conference on Computational Aspects of Social Networks (CASoN)*, 284-289. https://doi.org/10.1109/CASON.2011.6085959

Madden, S. (2012). From Databases to Big Data. *IEEE Internet Computing*, *16*(3), 4-6. https://doi.org/10.1109/MIC.2012.50

Mahmood, A., Siponen, M., Straub, D., Rao, & Raghu, S. (2010). Moving Toward Black Hat Research in Information Systems Security: An Editorial Introduction to the Special Issue. *MIS Quarterly*, *34*(3), 431. https://doi.org/10.2307/25750685

Maimon, O., & Rokach, L. (Ed.). (2010). *Data Mining and Knowledge Discovery Handbook*. Springer US. https://doi.org/10.1007/978-0-387-09823-4

Maione, C., Nelson, D. R., & Barbosa, R. M. (2019). Research on social data by means of cluster analysis. *Applied Computing and Informatics*, *15*(2), 153-162.

Maletic, J. I., & Marcus, A. (2009). Data Cleansing: A Prelude to Knowledge Discovery. Içinde O. Maimon & L. Rokach (Ed.), *Data Mining and Knowledge Discovery Handbook* (ss. 19-32). Springer US. https://doi.org/10.1007/978-0-387-09823-4_2

Mandl, H., & Levin, J. R. (1989). *Knowledge Acquisition from Text and Pictures*. Elsevier.

Mariscal, G., Marbán, Ó., & Fernández, C. (2010). A survey of data mining and knowledge discovery process models and methodologies. *The Knowledge Engineering Review*, *25*(2), 137-166. https://doi.org/10.1017/S0269888910000032

Martinez, B., & John, V. (1998). Los Cinco Grandes across cultures and ethnic groups: Multitrait-multimethod analyses of the Big Five in Spanish and English. *Journal of Personality and Social Psychology*, *75*(3), 729-750.

McCarty, J. A., & Hastak, M. (2007). Segmentation approaches in data-mining: A comparison of RFM, CHAID, and logistic regression. *Journal of Business Research*, *60*(6), 656-662. https://doi.org/10.1016/j.jbusres.2006.06.015

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 151-156.

McCuaig, J., & Baldwin, J. (2012). Identifying Successful Learners from Interaction Behaviour. *International Educational Data Mining Society*.

McGill, T., & Thompson, N. (2018). Gender Differences in Information Security Perceptions and Behaviour. *29th Australasian Conference on Information Systems*.

Means, B., Toyama, Y., Murphy, R., Bakia, M., & Jones, K. (2009). *Evaluation of evidence-based practices in online learning: A meta-analysis and review of online learning studies*.

Micarelli, A., & Sciarrone, F. (1996). A case-based system for adaptive hypermedia navigation. *European Workshop on Advances in Case-Based Reasoning*, 266-279.

Mills, D. (2009). Analysis of a social engineering threat to information security exacerbated by vulnerabilities exposed through the inherent nature of social networking websites. *2009 Information Sfrankeecurity Curriculum Development Conference*, 139-141.

Mills, S., Lucas, S., Irakliotis, L., Rappa, M., Carlson, T., & Perlowitz, B. (2012). Demystifying big data: A practical guide to transforming the business of government. *TechAmerica Foundation, Washington*.

Mitnick, K. D., & Simon, W. L. (2009). *The art of intrusion: The real stories behind the exploits of hackers, intruders and deceivers*. John Wiley & Sons.

Mohamad, S. K., & Tasir, Z. (2013). Educational data mining: A review. *Procedia-Social and Behavioral Sciences*, *97*, 320-324.

Mohebzada, J. G., Zarka, A. E., Bhojani, A. H., & Darwish, A. (2012). Phishing in a university community: Two large scale phishing experiments. *2012 International Conference on Innovations in Information Technology (IIT)*, 249-254. https://doi.org/10.1109/INNOVATIONS.2012.6207742

Molenda, M. (2008). Historical foundations. *Handbook of research on educational communications and technology*, 3-20.

Moniruzzaman, A. B. M., & Hossain, S. A. (2013). Nosql database: New era of databases for big data analytics-classification, characteristics and comparison. *arXiv preprint arXiv:1307.0191*.

Moon, D., Im, H., Lee, J., & Park, J. (2014). MLDS: Multi-Layer Defense System for Preventing Advanced Persistent Threats. *Symmetry*, *6*(4), 997-1010. https://doi.org/10.3390/sym6040997

Moore, S., & Keen, E. (2018). *Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019*. https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019 sayfasından erişilmiştir.

Moore, T., & Edelman, B. (2010). Measuring the Perpetrators and Funders of Typosquatting. Içinde R. Sion (Ed.), *Financial Cryptography and Data Security* (C. 6052, ss. 175-191). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-14577-3_15

Morgan, S. (2019). *2019 Ofcial Annual Cybercrime Report* (s. 12). Herjavec. https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf sayfasından erişilmiştir.

Mowery, D. C., & Simcoe, T. (2002). Is the Internet a US invention?—An economic and technological history of computer networking. *Research Policy*, *31*(8-9), 1369-1387.

Naik, U., & Shivalingaiah, D. (2008). *Comparative Study of Web 1.0, Web 2.0 and Web 3.0*.

Nakic, J., Granic, A., & Glavinic, V. (2015). Anatomy of Student Models in Adaptive Learning Systems: A Systematic Literature Review of Individual Differences from 2001 to 2013. *Journal of Educational Computing Research*, *51*(4), 459-489. https://doi.org/10.2190/EC.51.4.e

Naqvi, R. (2015). Data mining in educational settings. *Pakistan Journal of Engineering, Technology & Science*, *4*(2).

Naseer, H., Graeme, S., Ahmad, A., & Maynard, S. (2017). *Towards an analytics-driven information security risk management: A contingent resource based perspective.* 2645-2655.

Neghina, D.-E., & Scarlat, E. (2013). Managing information technology security in the context of cyber crime trends. *International journal of computers communications & control*, *8*(1), 97-104.

Novikova, E. S., Bekeneva, Y. A., & Shorov, A. V. (2017). Towards visual analytics tasks for the security information and event management. *2017 International Conference "Quality Management,Transport and Information Security, Information Technologies" (IT&QM&IS)*, 90-93. https://doi.org/10.1109/ITMQIS.2017.8085770

Nyanchama, M. (2005). Enterprise Vulnerability Management and Its Role in Information Security Management. *Information Systems Security*, *14*(3), 29-56. https://doi.org/10.1201/1086.1065898X/45390.14.3.20050701/89149.6

Ohsaki, M., Wang, P., Matsuda, K., Katagiri, S., Watanabe, H., & Ralescu, A. (2017). Confusion-Matrix-Based Kernel Logistic Regression for Imbalanced Data Classification. *IEEE Transactions on Knowledge and Data Engineering*, *29*(9), 1806-1819. https://doi.org/10.1109/TKDE.2017.2682249

O'reilly, T. (2007). What is Web 2.0: Design patterns and business models for the next generation of software. *Communications & strategies*, *1*, 17.

Otter, M., & Johnson, H. (2000). Lost in hyperspace: Metrics and mental models. *Interacting with computers*, *13*(1), 1-40.

Öğütçü. (2010). *E-Dönüşüm Sürecinde Kişisel Bilişim Güvenliği Davranışı ve Farkındalığı Analizi*. Yüksek Lisans Tezi Başkent Üniversitesi, Ankara

Önaçan, M. B. K., & Atan, H. (2016). Siber Güvenlikte Lisansüstü Eğitim: Deniz Harp Okulu Örneği. *Trakya University Journal of Engineering Sciences*, *17*(1), 13-21.

Özkan, Y. (2008). *Veri Madenciliği Yöntemleri* (C. 1). Papatya Bilim Yayıncılık.

Özyurt, Ö., & Özyurt, H. (2015). Learning style based individualized adaptive e-learning environments: Content analysis of the articles published from 2005 to 2014. *Computers in Human Behavior*, *52*, 349-358. https://doi.org/10.1016/j.chb.2015.06.020

Pai, P.-F., Lyu, Y.-J., & Wang, Y.-M. (2010). Analyzing academic achievement of junior high school students by an improved rough set model. *Computers & Education*, *54*(4), 889-900.

Panigrahi, R., Srivastava, P. R., & Sharma, D. (2018). Online learning: Adoption, continuance, and learning outcome—A review of literature. *International Journal of Information Management*, *43*, 1-14. https://doi.org/10.1016/j.ijinfomgt.2018.05.005

Park, S., Jang, Y. J., & James, J. I. (2017). Possession of Child Exploitation Material in Computer Temporary Internet Cache. *Journal of Digital Forensics, Security and Law*, *12*(3), 3.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, *66*, 40-51.

Parsons, K. M., Young, E., Butavicius, M. A., McCormac, A., Pattinson, M. R., & Jerram, C. (2015). The influence of organizational information security culture on information security decision making. *Journal of Cognitive Engineering and Decision Making*, *9*(2), 117-129.

Patel, A., Qassim, Q., & Wills, C. (2010). A survey of intrusion detection and prevention systems. *Information Management & Computer Security*, *18*(4), 277-290. https://doi.org/10.1108/09685221011079199

Patidar, P., & Twari, A. (2013). Handling Missing Value in Decision Tree Algorithm. *International Journal of Computer Applications*, *70*(13), 31-35.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2015). Factors that influence information security behavior: An Australian web-based study. *International Conference on Human Aspects of Information Security, Privacy, and Trust*, 231-241.

Pérez, T., Gutiérrez, J., & Lopistéguy, P. (1995). An adaptive hypermedia system. *Proceedings of AI-ED*, *95*, 351-358.

Pham, H. N. A. (2010). *The Impact of Overfting and Overgeneralization on the Classifcation Accuracy in Data Mining* Doktora Tezi. Louisiana State University, Loisiana

Pivec, M., Dziabenko, O., & Schinnerl, I. (2003). Aspects of game-based learning. *3rd International Conference on Knowledge Management, Graz, Austria*, 216-225.

Preidys, S., & Sakalauskas, L. (2010). Analysis of students' study activities in virtual learning environments using data mining methods. *Technological and economic development of economy*, *16*(1), 94-108.

Rai, S., & Chukwuma, P. (2010). Beginning at the endpoint: Faced with an ever changing mix of new technologies, auditors should make these devices the starting point in security reviews. *Internal Auditor*, *67*(3), 25-27.

Ramageri, B. (2010). Data Mining Techniqes and Applications. *Indian Journal of Computer Science and Engineering*, *1*(4), 301-305.

Rastgoo, M., Lemaitre, G., Massich, J., Morel, O., Marzani, F., Garcia, R., & Meriaudeau, F. (2016). *Tackling the problem of data imbalancing for melanoma classification*. Bioimaging, Rome, Italy.

Reeves, T. C. (2000). Enhancing the worth of instructional technology research through "design experiments" and other development research strategies. *International Perspectives on Instructional Technology Research for the 21st Century*, *27*, 1-15.

Rehman, S. U., Song, W.-C., & Kang, M. (2014). Network-wide traffic visibility in OF@TEIN SDN testbed using sFlow. *The 16th Asia-Pacific Network Operations and Management Symposium*, 1-6. https://doi.org/10.1109/APNOMS.2014.6996541

Reid, R. C., & Gilbert, A. H. (2010). Using the Parkerian Hexad to introduce security in an information literacy class. *2010 Information Security Curriculum Development Conference*, 45-47.

Reigeluth, C. M. (1997). Instructional theory, practitioner needs, and new directions. *Educational Technology*, *37*(1), 42-47.

Reigeluth, Charles M. (1989). Educational technology at the crossroads: New mindsets and new directions. *Educational Technology Research and Development*, *37*(1), 67-80.

Reiser, RobertA. (2001). A history of instructional design and technology: Part I: A history of instructional media. *Educational Technology Research and Development*, *49*(1), 53-64. https://doi.org/10.1007/BF02504506

Reviere, R. (Ed.). (1996). *Needs assessment: A creative and practical guide for social scientists*. Taylor & Francis.

Richard, R., & Stephen, R. (1998). Cognitive Styles and Learning Strategis. *London: David Fulton*.

Riding, R. J., & Rayner, S. (1998). *Cognitive styles and learning strategies: Understanding style differences in learning and behaviour*. D. Fulton Publishers.

Ristoski, P., & Paulheim, H. (2016). Semantic Web in data mining and knowledge discovery: A comprehensive survey. *Journal of Web Semantics*, *36*, 1-22. https://doi.org/10.1016/j.websem.2016.01.001

Romero, C., & Ventura, S. (2020). Educational data mining and learning analytics: An updated survey. *WIREs Data Mining and Knowledge Discovery*, *10*(3). https://doi.org/10.1002/widm.1355

Rowe, D. C., Lunt, B. M., & Ekstrom, J. J. (2011). The role of cyber-security in information technology education. *Proceedings of the 2011 Conference on Information Technology Education - SIGITE '11*, 113. https://doi.org/10.1145/2047594.2047628

Rössling, G., & Müller, M. (2009). Social engineering: A serious underestimated problem. *Proceedings of the 14th annual ACM SIGCSE conference on Innovation and technology in computer science education*, 384-384.

Ruf, L., Thorn, A., Christen, T., Gruber, B., & Portmann, R. (2008). Threat modeling in security architecture-the nature of threats. *ISSS Working Group on Security Architectures*. https://pdfs.semanticscholar.org/09fc/831b360dce8f9924a67aed274f15bebf3e9b.pdf sayfasından erişilmiştir.

Sahu, H., Shrma, S., & Gondhalakar, S. (2011). A brief overview on data mining survey. *International Journal of Computer Technology and Electronics Engineering (IJCTEE)*, *1*(3), 114-121.

Salem, R., & Abdo, A. (2016). Fixing rules for data cleaning based on conditional functional dependency. *Future Computing and Informatics Journal*, *1*(1-2), 10-26.

Sanderson, M. (2007). Educational and Economic History: The Good Neighbours. *History of Education*, *36*, 429-445.

Sandhu, R., & Samarati, P. (1996). Authentication, access control, and audit. *ACM Computing Surveys (CSUR)*, *28*(1), 241-243.

Sao Pedro, M., Baker, R. Sj., Montalvo, O., Nakama, A., & Gobert, J. D. (2010). Using text replay tagging to produce detectors of systematic experimentation behavior patterns. *Educational Data Mining 2010*.

Sari, P. K., & Prasetio, A. (2017). Knowledge sharing and electronic word of mouth to promote information security awareness in social network site. *2017 International Workshop on Big Data and Information Security (IWBIS)*, 113-117. https://doi.org/10.1109/IWBIS.2017.8275111

Sarre, R., Lau, L. Y.-C., & Chang, L. Y. (2018). *Responding to cybercrime: Current trends*. Taylor & Francis.

Saxena, A., Kaushik, N., & Kaushik, N. (2018). Encryption and Decryption Technique Using Java. Içinde M. U. Bokhari, N. Agrawal, & D. Saini (Ed.), *Cyber Security* (C. 729, ss. 427-436). Springer Singapore. https://doi.org/10.1007/978-981-10-8536-9_40

Schmitt, D. P., Allik, J., McCrae, R. R., & Benet-Martínez, V. (2007). The geographic distribution of Big Five personality traits: Patterns and profiles of human self-description across 56 nations. *Journal of cross-cultural psychology*, *38*(2), 173-212.

Schwartz, P. M., & Solove, D. J. (2011). *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*. 86 N.Y.U.L.

Schwarz, G., & Martin, J. (2012). Comenius: Dead White Guy for Twenty-first Century Education. *Christian Scholar's Review*, *42*(1), 43-56. a9h.

Schwier, R. A., Campbell, K., & Kenny, R. (2004). Instructional designers' observations about identity, communities of practice and change agency. *Australasian Journal of Educational Technology, 20*(1). https://doi.org/10.14742/ajet.v20i1.1368

Scotney, B., & McClean, S. (1999). Efficient knowledge discovery through the integration of heterogeneous data. *Information and Software Technology, 41*(9), 569-578.

Shah, D. (2019). Year of MOOC-based Degrees: A Review of MOOC Stats and Trends in 2018. *Class Central Moocreport*. https://www.classcentral.com/report/moocs-stats-and-trends-2018/ sayfasından erişilmiştir.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 373-382.

Shirwaikar, R. D., Acharya, U. D., Makkithaya, K., Surulivelr, M., & Lewis, L. E. S. (2016). Machine Learning Techniques for Neonatal Apnea Prediction. *Journal of Artificial Intelligence, 9*(1), 33-38. https://doi.org/10.3923/jai.2016.33.38

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *computers & security, 49*, 177-191.

Simpson, A. (1990). Lost in hyperspace: How can designers help? *Intelligent Tutoring Media, 1*(1), 31-40. https://doi.org/10.1080/14626269009409085

Sinha, A. P., & Zhao, H. (2008). Incorporating domain knowledge into data mining classifiers: An application in indirect lending. *Decision Support Systems, 46*(1), 287-299. https://doi.org/10.1016/j.dss.2008.06.013

Sivarajah, U., Kamal, M. M., Irani, Z., & Weerakkody, V. (2017). Critical analysis of Big Data challenges and analytical methods. *Journal of Business Research, 70*, 263-286.

Sivogolovko, E., & Novikov, B. (2012). Validating cluster structures in data mining tasks. *Proceedings of the 2012 Joint EDBT/ICDT Workshops*, 245-250.

Smith, A. S. G. (1999). *Application of Machine Learning Algorithms in Adaptive Web-based Information Systems*. Doktora tezi. Middlesex University, Dubai

Somyürek, S. (2008). *Uyarlanabilir Eğitsel Web Ortamlarının Öğrencilerin Akademik Başarısına ve Gezinmesine Etkisi*, Doktora tezi. Gazi Ünizversitesi, Ankara

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security*, *24*(2), 124-133. https://doi.org/10.1016/j.cose.2004.07.001

Stefano, F., Borsci, S., & Stamerra, G. (2010). Web usability evaluation with screen reader users: Implementation of the partial concurrent thinking aloud technique. *Cognitive Processing*, *11*(3), 263-272. https://doi.org/10.1007/s10339-009-0347-y

Stern, M. K., & Woolf, B. P. (2000). Adaptive Content in an Online Lecture System. Içinde *Adaptive hypermedia and adaptive Web-based systems: International conference, AH 2000, Trento, Italy, August 28-30, 2000: Proceedings* (ss. 228-239). Springer.

Storey, V. C., & Song, I.-Y. (2017). Big data technologies and management: What conceptual modeling can do. *Data & Knowledge Engineering*, *108*, 50-67.

Sufian, B. İ., Salleh, S., & Judi, H. M. (2010). Activity Surveillance and Hawthorne Effect to Prevent Programming Plagiarism. *Journal of Computer Science*, *6*(11), 1341-1346. https://doi.org/10.3844/jcssp.2010.1341.1346

Su-lin, P., & Ji-zhang, G. (2009). C5.0 Classification Algorithm and Application on Individual Credit Evaluation of Banks. *Systems Engineering — Theory & Practice*, *29*(12), 94-104.

Sumner, C., Byers, A., & Shearing, M. (2011). Determining personality traits & privacy concerns from facebook activity. *Black Hat Briefings*, *11*(7), 197-221.

Sun, P., Finger, G., & Liu, Z. (2014). Mapping the evolution of eLearning from 1977–2005 to inform understandings of eLearning historical trends. *Education Sciences*, *4*(1), 155-171.

Sümer, N., Lajunen, T., & Özkan, T. (2005). Big five personality traits as the distal predictors of road accident. *Traffic and transport psychology: Theory and application*, *215*, 215-227.

Sümer, N., & Sümer, H. C. (2005). Beş faktör kişilik özellikleri ölçeği (Yayınlanmamış çalışma). *Erişim: https://scholar. google. com. tr*. sayfasından erişilmiştir.

Şahinaslan, E., Kantürk, A., Şahinaslan, Ö., & Borandağ, E. (2009). Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri. *XI. Akademik Bilişim Konferansı Bildirileri, Şanlıurfa*.

Şimşek, A. (2013). Öğretim Tasarımı ve Modelleri. Içinde *Öğretim teknolojilerinin temelleri: Teoriler, araştırmalar, eğilimler* (ss. 99-116). Pegem Akademi.

Şimşek, A. (2014). *Öğretim tasarımı* (3. bs, C. 13). Nobel Yayın Dağıtım.

Tadlaoui, M. A., Khaldi, M., & Carvalho, R. N. (2016). Learner Modeling in Adaptive Educational Systems: A Comparative Study. *International Journal of Modern Education and Computer Science*, *8*(3), 1-10. https://doi.org/10.5815/ijmecs.2016.03.01

Tahboub, R., & Saleh, Y. (2014). Data Leakage/Loss Prevention Systems (DLP). *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, 1-6. https://doi.org/10.1109/WCCAIS.2014.6916624

Tahir, R., Raza, A., Ahmad, F., Kazi, J., Zaffar, F., Kanich, C., & Caesar, M. (2018). It's All in the Name: Why Some URLs are More Vulnerable to Typosquatting. *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, 2618-2626. https://doi.org/10.1109/INFOCOM.2018.8486271

Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An Analysis of Information Security Awareness within Home and Work Environments. *2010 International Conference on Availability, Reliability and Security*, 196-203. https://doi.org/10.1109/ARES.2010.27

Taşpınar, M. (2014). Mesleki Eğitimde Uzaktan Eğitim ve Toplumsal algı. *Eğitim ve Öğretim Araştırmaları Dergisi*, *3*(4), 1-7.

TBMM. (2014). *Sanal Ortamda İşlenen Suçlar Sözleşmesi* (Resmi Sy 2014/6656; s. 53). https://www.resmigazete.gov.tr/eskiler/2014/08/20140809-5-1.pdf sayfasından erişilmiştir.

TBMM Bilişim ve İnternet Araştırma Komisyonu (BİAK) Raporunda Yer Alan Öneriler (s. 222). (2013). TBMM. https://www.tbmm.gov.tr/arastirma_komisyonlari/bilisim_internet/docs/rapor_ozeti.pdf sayfasından erişilmiştir.

TDK. (2020). Içinde *Türk Dil Kurumu*. https://sozluk.gov.tr/?kelime=tasar%C4%B1m sayfasından erişilmiştir.

Tekerek, M., & Tekerek, A. (2013). A Research on Students' Information Security Awareness. *Online Submission*, *2*(3), 61-70.

Thammasiri, D., Delen, D., Meesad, P., & Kasap, N. (2014). A critical assessment of imbalanced class distribution problem: The case of predicting freshmen student attrition. *Expert Systems with Applications*, *41*(2), 321-330. https://doi.org/10.1016/j.eswa.2013.07.046

The Design-Based Research Collective. (2003). Design-Based Research: An Emerging Paradigm for Educational Inquiry. *Educational Researcher*, *32*(1), 5-8. https://doi.org/10.3102/0013189X032001005

The Risk of Social Engineering on Information Security: A Survey of IT Professionals (s. 7). (2011). Dimensional Researh. https://www.stamx.net/files/The-Risk-of-Social-Engineering-on-Information-Security.pdf

Thomas, K., Huang, D., Wang, D., Bursztein, E., Grier, C., Holt, T. J., Kruegel, C., McCoy, D., Savage, S., & Vigna, G. (2015). *Framing dependencies introduced by underground commoditization*.

Thomas, S. A. (2000). *SSL and TLS essentials. Securing the Web John Wiley and Sons*. John Wiley and Sons.

Thombre, A. (2012). Comparing logistic regression, neural networks, c5. 0 and m5′ classification techniques. *International Workshop on Machine Learning and Data Mining in Pattern Recognition*, 132-140.

Tolhurst, D. (1995). Hypertext, Hypermedia, Multimedia Defined? *Educational Technology*, *35*(2), 21-26.

Trček, D., Trobec, R., Pavešić, N., & Tasič, J. F. (2007). Information systems security and human behaviour. *Behaviour & Information Technology*, *26*(2), 113-118.

Tripp, S. D., & Bichelmeyer, B. (1990). Rapid prototyping: An alternative instructional design strategy. *Educational Technology Research and Development*, *38*(1), 31-44.

TUİK. (2016). *Hanehalkı Bilişim Teknolojileri Kullanım Araştırması*. http://www.tuik.gov.tr/PreHaberBultenleri.do?id=21779 sayfasından erişilmiştir.

Ture, M., Tokatli, F., & Kurt, I. (2009). Using Kaplan–Meier analysis together with decision tree methods (C&RT, CHAID, QUEST, C4.5 and ID3) in determining recurrence-free survival of breast cancer patients. *Expert Systems with Applications*, *36*(2), 2017-2026. https://doi.org/10.1016/j.eswa.2007.12.002

Ueno, M. (2004). Online outlier detection system for learning time data in E-learning and It's evaluation. *Proc. of Computers and Advanced Technology in Education (CATE2004)*.

Valsamidis, S., Kontogiannis, S., Kazanidis, I., Theodosiou, T., & Karakos, A. (2012). A clustering methodology of web log data for learning management systems. *Journal of Educational Technology & Society*, *15*(2), 154-167.

Van den Akker, J. (1999). Principles and methods of development research. Içinde *Design approaches and tools in education and training* (ss. 1-14). Springer.

Van Hulse, J., & Khoshgoftaar, T. (2009). Knowledge discovery from imbalanced and noisy data. *Data & Knowledge Engineering*, *68*(12), 1513-1542. https://doi.org/10.1016/j.datak.2009.08.005

Vaughn, R. B., Dampier, D. A., & Warkentin, M. B. (2004). Building an information security education program. *Proceedings of the 1st Annual Conference on Information Security Curriculum Development - InfoSecCD '04*, 41. https://doi.org/10.1145/1059524.1059533

Velki, T., Solic, K., & Ocevcic, H. (2014). Development of Users' Information Security Awareness Questionnaire (UISAQ) — Ongoing work. *2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1417-1421. https://doi.org/10.1109/MIPRO.2014.6859789

Verduin, J. R., & Clark, T. A. (1991). *Distance education: The foundations of effective practice*. Jossey-Bass Inc Pub.

Verizon. (2012). *2012 Data Breach Investigations Report*. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012-ebk_en_xg.pdf sayfasından erişilmiştir.

Verizon. (2016). *2016 Data Breach Investigations Report*. https://regmedia.co.uk/2016/05/12/dbir_2016.pdf sayfasından erişilmiştir.

Vialardi, C., Chue, J., Peche, J. P., Alvarado, G., Vinatea, B., Estrella, J., & Ortigosa, Á. (2011). A data mining approach to guide students through the enrollment process based on academic performance. *User modeling and user-adapted interaction*, *21*(1-2), 217-248.

Wang, F., & Hannafin, M. J. (2005). Design-based research and technology-enhanced learning environments. *Educational technology research and development*, *53*(4), 5-23.

Wang, J. A., & Guo, M. (2009). OVM: An ontology for vulnerability management. *Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research Cyber Security and Information Intelligence Challenges and Strategies - CSIIRW '09*, 1. https://doi.org/10.1145/1558607.1558646

Wang, Y., & Liao, H.-C. (2011). Data mining for adaptive learning in a TESL-based e-learning system. *Expert Systems with Applications*, *38*(6), 6480-6485. https://doi.org/10.1016/j.eswa.2010.11.098

Warkentin, M., McBride, M., Carter, L., & Johnston, A. (2012). *The role of individual characteristics on insider abuse intentions*.

We are Social. (2016). *Digital in 2016* (s. 537). http://wearesocial.com/uk/special-reports/digital-in-2016

West, A. G. (2017). Analyzing the Keystroke Dynamics of Web Identifiers. *Proceedings of the 2017 ACM on Web Science Conference - WebSci '17*, 181-190. https://doi.org/10.1145/3091478.3091482

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: An examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3-7.

Wiharto, W., Kusnanto, H., & Herianto, H. (2016). Interpretation of Clinical Data Based on C4.5 Algorithm for the Diagnosis of Coronary Heart Disease. *Healthcare Informatics Research*, *22*(3), 186. https://doi.org/10.4258/hir.2016.22.3.186

Wiley, A., McCormac, A., & Calic, D. (2020). More than the individual: Examining the relationship between culture and Information Security Awareness. *Computers & Security*, *88*, 101640. https://doi.org/10.1016/j.cose.2019.101640

Witten, I. H., Frank, E., & Hall, M. A. (2011). *Data Mining: Practical machine learning tools and techniques* (C. 3). Morgan Kaufmann.

Woodard, B., Imboden, T., & Martin, N. L. (2013). An Undergraduate Information Security Program: More than a Curriculum. *Journal of Information Systems Education*, *24*(1), 9.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology*, *59*(4), 662-674. https://doi.org/10.1002/asi.20779

Wu, L. (2013). Social Network Effects on Productivity and Job Security: Evidence from the Adoption of a Social Networking Tool. *Information Systems Research*, *24*(1), 30-51. https://doi.org/10.1287/isre.1120.0465

Xu, D., Wang, H., & Su, K. (2002). Intelligent student profiling with fuzzy models. *Proceedings of the 35th Annual Hawaii International Conference on System Sciences*, 8. https://doi.org/10.1109/HICSS.2002.994005

Yakut, E. (2012). *Veri madenciliği tekniklerinden C5. 0 algoritması, destek vektör makineleri ile yapay sinir ağlarının sınıflandırma başarılarının karşılaştırılması: İmalat sektöründe bir uygulama* Doktora tezi. Atatürk Üniversitesi, Erzurum

Yan, X., & Gu, P. (1996). A review of rapid prototyping technologies and systems. *Computer Aided Design*, *28*(4), 307-318.

Zang, B., Huang, R., Wang, L., Chen, J., Tian, F., & Wei, X. (2016). An Improved KNN Algorithm Based on Minority Class Distribution for Imbalanced Dataset. *2016 International Computer Symposium (ICS)*, 696-700. https://doi.org/10.1109/ICS.2016.0143

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*.

Zhang, L. (2006). Thinking styles and the big five personality traits revisited. *Personality and Individual Differences*, *40*(6), 1177-1187. https://doi.org/10.1016/j.paid.2005.10.011

Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016). A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proceedings of the IEEE*, *104*(9), 1727-1765. https://doi.org/10.1109/JPROC.2016.2558521

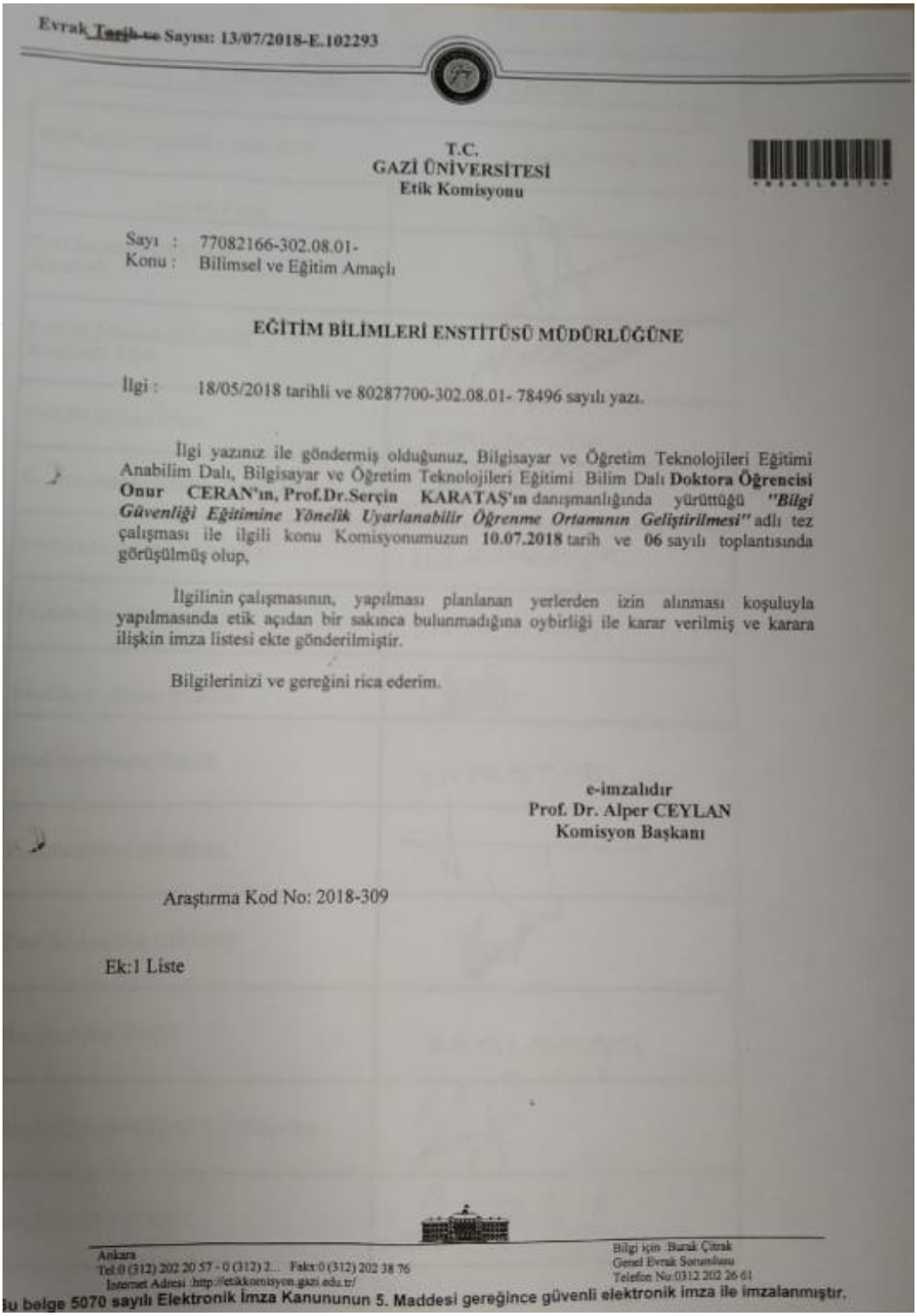
EKLER

EK 1. Bilgi Güvenliğine Dair Hazırlanan El Broşürleri

Emniyet Genel Müdürlüğü Tarafından Hazırlanan El Broşürü

Bilgi Teknolojileri ve İletişim Kurumu Tarafından Hazırlanan El Broşürü

EK 2. Etik Kurul İzni



Evrak Tarih-Sayısı: 13/07/2018-E.102293

T.C.
GAZİ ÜNİVERSİTESİ
Etik Komisyonu

Sayı : 77082166-302.08.01-
Konu : Bilimsel ve Eğitim Amaçlı

EĞİTİM BİLİMLERİ ENSTİTÜSÜ MÜDÜRLÜĞÜNE

İlgi : 18/05/2018 tarihli ve 80287700-302.08.01- 78496 sayılı yazı.

İlgi yazınız ile göndermiş olduğunuz, Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı, Bilgisayar ve Öğretim Teknolojileri Eğitimi Bilim Dalı **Doktora Öğrencisi Onur CERAN'ın, Prof.Dr.Serçin KARATAŞ'ın** danışmanlığında yürüttüğü ***"Bilgi Güvenliği Eğitimine Yönelik Uyarlanabilir Öğrenme Ortamının Geliştirilmesi"*** adlı tez çalışması ile ilgili konu Komisyonumuzun **10.07.2018** tarih ve **06** sayılı toplantısında görüşülmüş olup,

İlgilinin çalışmasının, yapılması planlanan yerlerden izin alınması koşuluyla yapılmasında etik açıdan bir sakınca bulunmadığına oybirliği ile karar verilmiş ve karara ilişkin imza listesi ekte gönderilmiştir.

Bilgilerinizi ve gereğini rica ederim.

e-imzalıdır
Prof. Dr. Alper CEYLAN
Komisyon Başkanı

Araştırma Kod No: 2018-309

Ek:1 Liste

Ankara
Tel:0 (312) 202 20 57 - 0 (312) 2... Faks:0 (312) 202 38 76
İnternet Adresi :http://etikkomisyon.gazi.edu.tr/

Bilgi için :Burak Çıtrak
Genel Evrak Sorumlusu
Telefon No:0312 202 26 61

Bu belge 5070 sayılı Elektronik İmza Kanununun 5. Maddesi gereğince güvenli elektronik imza ile imzalanmıştır.

EK 3. Ölçekler

Riskli Davranış Ölçeği

SORULAR	Hiçbir Zaman	Nadiren	Bazen	Sık Sık	Her Zaman
MSN Messenger, Gtalk, Skype ve benzeri sohbet programları kullanırım.					
Bir iletişim aracı olarak elektronik posta (e-posta) kullanırım.					
Kurumsal e-posta adresimi günlük işlerde kullanırım.					
İnternette e-posta gruplarına üye olurum.					
Facebook, Twitter ve benzeri sosyal ağ sitelerini kullanırım.					
Sosyal ağlarda gönderilen uygulama davetlerini kabul ederim.					
İnternet bankacılığı kullanırım.					
İnternet üzerinden alışveriş yaparım.					
E-vatandaşlık hizmetleri veren web sayfalarını (TC kimlik no sorgulama, sosyal güvenlik primi sorgulama vb.) kullanırım.					
İnternet üzerinden oyun oynarım.					
İnternet üzerinden müzik, film, program ve dosya indiririm/kaydederim.					
İnternet üzerinden video/film izlerim.					
İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM No, e-posta, adres) paylaşırım.					
İnternet ortamında gerektiği durumlarda özlük bilgilerimi paylaşırım (Ad, Soyad, Doğum Tarihi vb.)					
Sohbet (chat) yaparken dosya transferi yaparım.					
Bilgisayarımdaki dosyaları paylaşıma açarım.					
Halka açık internet erişimi olan yerlerde internet bankacılığı kullanırım.					
Parolalarımı başkalarıyla paylaşırım.					
Parolalarımı yazılı olarak kolay ulaşabileceğim yerlerde saklarım.					
Tanımadığım kişilerden gelen e postaları açarım, gelen ekleri indiririm.					

Korumacı Davranış Ölçeği

SORULAR	Hiçbir Zaman	Nadiren	Bazen	Sık Sık	Her Zaman
Birden fazla elektronik posta adresi kullanırım.					
Bilgisayarımda orijinal (lisanslı) yazılım kullanmaya dikkat ederim.					
Virüs temizleme, casus yazılım önleme vb. programları kullanırım.					
Güvenlik duvarı, reklam önleyici vb. programlar kullanırım.					
İçerik filtreleme programları kullanırım.					
E-posta filtreleme yazılımları kullanırım.					
İzleme yazılımları kullanarak internet üzerinde yapılan etkinlikler hakkında bilgi sahibi olurum.					
Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim.					
Herkesin kullanımına açık bir bilgisayardan ayrılmadan önce geçici internet dosyalarını ve Web gezinti geçmişlerini silerim.					
Dosyalarımı şifrelerim.					
İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım.					
Elektronik/ Mobil imza kullanırım.					
İnternet sitelerine girerken genellikle sık kullanılanlar listesini kullanırım.					
Bilgisayarım şifre ile açılır.					
Bilgisayarımda otomatik kullan özelliğini kapatırım.					
Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim.					
Parolalarımı sık sık değiştiririm.					
Kablosuz modem şifremi değiştiririm.					
Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım.					
Kullandığım programların güncellemelerini düzenli olarak yaparım.					

Suça Maruziyet Ölçeği

SORULAR	Hiçbir Zaman	Nadiren	Bazen	Sık Sık	Her Zaman
Bilgisayar virüsleri nedeniyle sorun yaşadım.					
Online alışverişten dolayı maddi zarara uğradım.					
Kredi kartım kopyalandı.					
Kişisel bilgilerimi internette paylaştığım için sıkıntı yaşadım.					
Elektronik bankacılık kullandığım için maddi zarara uğradım.					
Kişisel bilgilerim iznim olmadan üçüncü şahıslarla paylaşıldı/ internette yayınlandı.					
İnternet üzerindeki hesaplarıma ait kullanıcı adım ve şifrem ele geçirildi.					
İnternette kimliği belirsiz kişiler tarafından şahsıma yönelik hakaret, tehdit, ahlaksız teklif aldım.					
Kumar içerikli siteler nedeniyle zarara uğradım.					
Sosyal ağ siteleri nedeniyle zarara uğradım.					
Arkadaşlık siteleri nedeniyle zarara uğradım.					
İnternette gezerken isteğim dışında şiddet ya da pornografik içerikli yayınlarla karşılaştım.					
Bilgisayarımdaki dosyalarım çalındı/silindi.					
Adıma sahte hesaplar açıldı.					
İnternet üzerinden yaptığım yazışmalar isteğim ve bilgim dışında başkaları tarafından izlendi, kaydedildi.					

Tehlike Algısı Ölçeği

SORULAR	Çok Tehlikeli	Tehlikeli	Az Tehlikeli	Tehlikesiz	Fikrim Yok
Virüs yazılımları					
Virüs koruma programları					
Casus programlar (Keylogger, Screenlogger,Trojan vb.)					
Dosya paylaşım programları (Ares, Limewire vb.)					
ActiveX, Javascript vb. mobil kodlar					
Web tarayıcıları (Internet Explorer, Mozilla Firefox, Google Chrome vb.)					
Sohbet programları (Messenger, ICQ vb.)					
İstenmeyen/ Spam / Junk e-postalar					
Online oyunlar					
USB/Harici bellekler					
MS Office uygulamaları (Word, Excel vb.)					
Klavye kullanımı					
Kopya/ Kırık/ Korsan program kullanımı					
Müzik/ Resim/ Film gibi materyallerin herhangi bir bedel ödemeden indirilmesi					
Reklam içerikli e-postaların açılması					
Elektronik bankacılık kullanımı					
İnternet ortamında yabancılarla sohbet / bilgi paylaşımı					
İnternetten alışveriş yapılması					
Pornografik içerikli web sitelerine girilmesi					
Kumar, bahis sitelerine girilmesi					
Sosyal ağlara üye olunması (Facebook, Twitter vb.)					
Bluetooth kullanımı					
Kablosuz modem kullanımı					
İnternetten kontör yüklenmesi					
Kırık veya ücretsiz güvenlik programı kullanımı					
Bina girişlerinde güvenlik birimine nüfus cüzdanı veya sürücü belgesinin teslim edilmesi					
Kargo, GSM operatörü vs. gibi kuruluşlara nüfus cüzdanı bilgilerinin verilmesi					
Vatandaşlık numarasının başka şahıslar tarafından bilinmesi					

Büyük Beşli Kişilik Envanteri

Aşağıda sizi kısmen tanımlayan (ya da pek tanımlayamayan) bir takım özellikler sunulmaktadır. Örneğin, başkaları ile zaman geçirmekten hoşlanan birisi olduğunuzu düşünüyor musunuz? Lütfen aşağıda verilen özelliklerin sizi ne oranda yansıttığını ya da yansıtmadığını belirtmek için sizi en iyi tanımlayan rakamı her bir özelliğin yanına yazınız.

1 = Hiç katılmıyorum
2 = Biraz katılmıyorum
3 = Ne katılıyorum ne de katılmıyorum (kararsızım)
4 = Biraz katılıyorum
5 = Tamamen katılıyorum
Kendimi ..... biri olarak görüyorum

___ 1. Konuşkan
___ 2. Başkalarında hata arayan
___ 3. İşini tam yapan
___ 4. Bunalımlı, melankolik
___ 5. Orijinal, yeni görüşler ortaya koyan
___ 6. Ketum/vakur
___ 7. Yardımsever ve çıkarcı olmayan
___ 8. Biraz umursamaz
___ 9. Rahat, stresle kolay baş eden
___ 10. Çok değişik konuları merak eden
___ 11. Enerji dolu
___ 12. Başkalarıyla sürekli didişen
___ 13. Güvenilir bir çalışan
___ 14. Gergin olabilen
___ 15. Maharetli, derin düşünen
___ 16. Heyecan yaratabilen
___ 17. Affedici bir yapıya sahip
___ 18. Dağınık olma eğiliminde
___ 19. Çok endişelenen
___ 20. Hayal gücü yüksek
___ 21. Sessiz bir yapıda
___ 22. Genellikle başkalarına güvenen
___ 23. Tembel olma eğiliminde olan
___ 24. Duygusal olarak dengeli, kolayca keyfi kaçmayan
___ 25. Keşfeden, icat eden
___ 26. Atılgan bir kişiliğe sahip
___ 27. Soğuk ve mesafeli olabilen
___ 28. Görevi tamamlanıncaya kadar sebat edebilen
___ 29. Dakikası dakikasına uymayan
___ 30. Sanata ve estetik değerlere önem veren
___ 31. Bazen utangaç, çekingen olan
___ 32. Hemen hemen herkese karşı saygılı ve nazik olan
___ 33. İşleri verimli yapan
___ 34. Gergin ortamlarda sakin kalabilen
___ 35. Rutin işleri yapmayı tercih eden
___ 36. Sosyal, girişken
___ 37. Bazen başkalarına kaba davranabilen
___ 38. Planlar yapan ve bunları takip eden
___ 39. Kolayca sinirlenen
___ 40. Düşünmeyi seven, fikirler geliştirebilen
___ 41. Sanata ilgisi çok az olan
___ 42. Başkalarıyla işbirliği yapmayı seven
___ 43. Kolaylıkla dikkati dağılan
___ 44. Sanat, müzik ve edebiyatta çok bilgili

Web Sitesi Tasarım Ölçeği

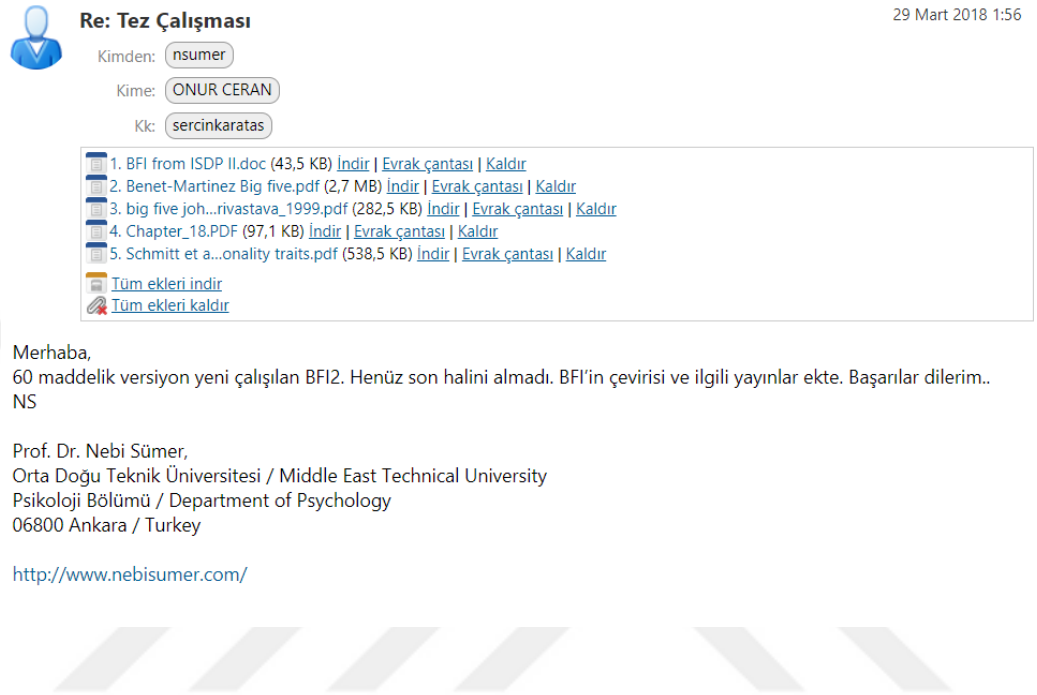
GRAFİK TASARIM ve KULLANILABİLİRLİĞE YÖNELİK ÖZELLİKLER	Evet (3)	Kısmen (2)	Hayır (1)
1. Sitede okulun logosu kullanılmış mı?	( )	( )	( )
2. Site tasarımında doku kullanılmış mı?	( )	( )	( )
3. Sitede arka planda doku kullanılmış mı?	( )	( )	( )
4. Sitede yer alan önemli unsurlar için vurgulama kullanılmış mı?	( )	( )	( )
5. Site tasarımında uygun renkler kullanılmış mı?	( )	( )	( )
6. Site tasarımında kullanılan renkler birbiri ile uyumlu mudur?	( )	( )	( )
7. Sitede sayfa zeminlerinde renk kullanılmış mı?	( )	( )	( )
8. Sitede kullanılan renk çeşidi çok kullanılmış mı?	( )	( )	( )
9. Site tasarımında göz yormayan renk kombinasyonları kullanılmış mı?	( )	( )	( )
10. Site tasarımında kullanılan renkler sayfa hiyerarşisine uygun mudur?	( )	( )	( )
11. Sitede yer alan metinlerde uygun renkler kullanılmış mı?	( )	( )	( )
12. Sitede yer alan metinler ile arka plan renkleri uyumlu mudur?	( )	( )	( )
13. Sitede yer alan metinlerde önemli kısımların vurgularında renk kullanılmış mı?	( )	( )	( )
14. Site tasarımında kullanılan çizgi öğelerinin renkleri birbiri ile uyumlu mudur?	( )	( )	( )
15. Sitede kullanılan grafik elemanların renkleri birbirleri ile uyumlu mudur?	( )	( )	( )
16. Sitede yer alan metinlerde uygun yazı karakteri kullanılmış mı?	( )	( )	( )
17. Sitede yer alan metinler de uygun yazı karakteri büyüklüğü kullanılmış mı?	( )	( )	( )
18. Sitede yer alan metinler sayfadaki görsel öğelerle uygun şekilde hizalanmış mı?	( )	( )	( )
19. Sitede yer alan metinlerde önemli kısımların vurgulamaları kalın yazı karakteri kullanılarak yapılmış mı?	( )	( )	( )
20. Sitede yer alan metinlerde uygun satır aralığı kullanılmış mı?	( )	( )	( )

GRAFİK TASARIM ve KULLANILABİLİRLİĞE YÖNELİK ÖZELLİKLER	Evet (3)	Kısmen (2)	Hayır (1)
21. Sitede yer alan metinlerde uygun paragraf aralığı kullanılmış mı?	( )	( )	( )
22. Sitede yer alan metinlerde uygun kelime aralığı kullanılmış mı?	( )	( )	( )
23. Sitede yer alan metinlerde uygun harf aralığı kullanılmış mı?	( )	( )	( )
24. Sitede yer alan uzun metinlerde tırnaksız yazı karakteri kullanılmış mı?	( )	( )	( )
25. Site tasarımında okul ismi site başlığında büyük harflerle yazılmış mı?	( )	( )	( )
26. Sitede yer alan metinlerde uygun tireleme yapılmış mı?	( )	( )	( )
27. Sitede yer alan metinlerde her iki taraftan bloklama kullanılmış mı?	( )	( )	( )
28. Site tasarımının belirli bir yönü var mıdır?	( )	( )	( )
29. Sitedeki görsel öğeler arasında devamlılık ilişkisi var mıdır?	( )	( )	( )
30. Sitedeki görsel öğeler arasında uygun aralık bırakılmış mı?	( )	( )	( )
31. Sitedeki görsel öğeler arasında bütünlük ilişkisi var mıdır?	( )	( )	( )
32. Sitedeki görsel öğeler orantılı olarak kullanılmış mı?	( )	( )	( )
33. Sitede kullanılan görsel öğeler sayfa hiyerarşisine uygun kullanılmış mı?	( )	( )	( )
34. Site tasarımında fotoğraf kullanılmış mı?	( )	( )	( )
35. Sitede yer alan fotoğraflar sayfa bütünlüğüne uygun kullanılmış mı?	( )	( )	( )
36. Sitede yer alan fotoğraflar uygun çözünürlükte kullanılmış mı?	( )	( )	( )
37. Sitede yer alan fotoğraflar uygun ölçülerde kullanılmış mı?	( )	( )	( )
38. Sitede yer alan fotoğrafların ışık ve renk değerleri uygun mudur?	( )	( )	( )
39. Site tasarımında illüstrasyon kullanılmış mı?	( )	( )	( )
40. Sitede yer alan illüstrasyonlar sayfa bütünlüğüne uygun kullanılmış mı?	( )	( )	( )
41. Sitede yer alan illüstrasyonlar uygun çözünürlükte kullanılmış mı?	( )	( )	( )
42. Site tasarımında animasyon kullanılmış mı?	( )	( )	( )

GRAFİK TASARIM ve KULLANILABİLİRLİĞE YÖNELİK ÖZELLİKLER	Evet (3)	Kısmen (2)	Hayır (1)
43. Sitede yer alan animasyonlar sayfa tasarımına uygun ölçülerde midir?	( )	( )	( )
44. Site tasarımında video (hareketli görüntüler) kullanılmış mı?	( )	( )	( )
45. Sitede yer alan videolar sayfa tasarımına uygun ölçülerde midir?	( )	( )	( )
46. Sitenin ideal görüntüsü için çözünürlük değerleri önerilmiş mi?	( )	( )	( )
47. Sitede okulun tarihçesi ve ismi ile ilgili tanıcı bilgiye yer verilmiş mi?	( )	( )	( )
48. Sitede okulun ulaşım ve iletişim bilgileri bulunuyor mu?	( )	( )	( )
49. Sitenin sayfaları ekrana hızlı yükleniyor mu?	( )	( )	( )
50. Sitede yer alan fotoğraf ve resimler sayfada hızlı yükleniyor mu?	( )	( )	( )
51. Sitede yer alan animasyon ve videolar sayfada hızlı yükleniyor mu?	( )	( )	( )
52. Sitenin tasarımını yapan kuruma/kişiye ilişkin bilgilere yer verilmiş mi?	( )	( )	( )
53. Sitede gezinmeyi kolaylaştıran bir site haritası var mı?	( )	( )	( )
54. Sitede açılışla gelen bir giriş ekranı bulunuyor mu?	( )	( )	( )
55. Site sayfalarından ana sayfaya doğrudan dönülebiliyor mu?	( )	( )	( )
56. Site sayfalarında dolaşmayı kolaylaştıran linkler bulunuyor mu?	( )	( )	( )
57. Sitede yer alan hizmetlere ilişkin menü başlıkları bulunuyor mu?	( )	( )	( )
58. Sitede yer alan tam metinlere bağlantılarla ulaşılıyor mu?	( )	( )	( )
59. Sitede arama imkânı sunan bir arama motoru bulunuyor mu?	( )	( )	( )
60. Sitede arama motorunda detaylı arama için seçenekler bulunuyor mu?	( )	( )	( )
61. Sitede duyuru ve haberlere yönelik bir menü bulunuyor mu?	( )	( )	( )
62. Sitenin son güncellenme tarihi belirtiliyor mu?	( )	( )	( )
63. Sitede favorilere ekle ve ana sayfa yap seçenekleri bulunuyor mu?	( )	( )	( )
64. Sitede konu yazarlarına ait bilgiler bulunuyor mu?	( )	( )	( )
65. Sitede kullanıcılar için yararlı web adresleri veriliyor mu?	( )	( )	( )

EK 4. Ölçeklerin Kullanımı için Alınan İzinler

Büyük Beşli Kişilik Envanteri Kullanımı için Alınan İzin



Re: Tez Çalışması 29 Mart 2018 1:56

Kimden: nsumer
Kime: ONUR CERAN
Kk: sercinkaratas

1. BFI from ISDP II.doc (43,5 KB) İndir | Evrak çantası | Kaldır
2. Benet-Martinez Big five.pdf (2,7 MB) İndir | Evrak çantası | Kaldır
3. big five joh...rivastava_1999.pdf (282,5 KB) İndir | Evrak çantası | Kaldır
4. Chapter_18.PDF (97,1 KB) İndir | Evrak çantası | Kaldır
5. Schmitt et a...onality traits.pdf (538,5 KB) İndir | Evrak çantası | Kaldır

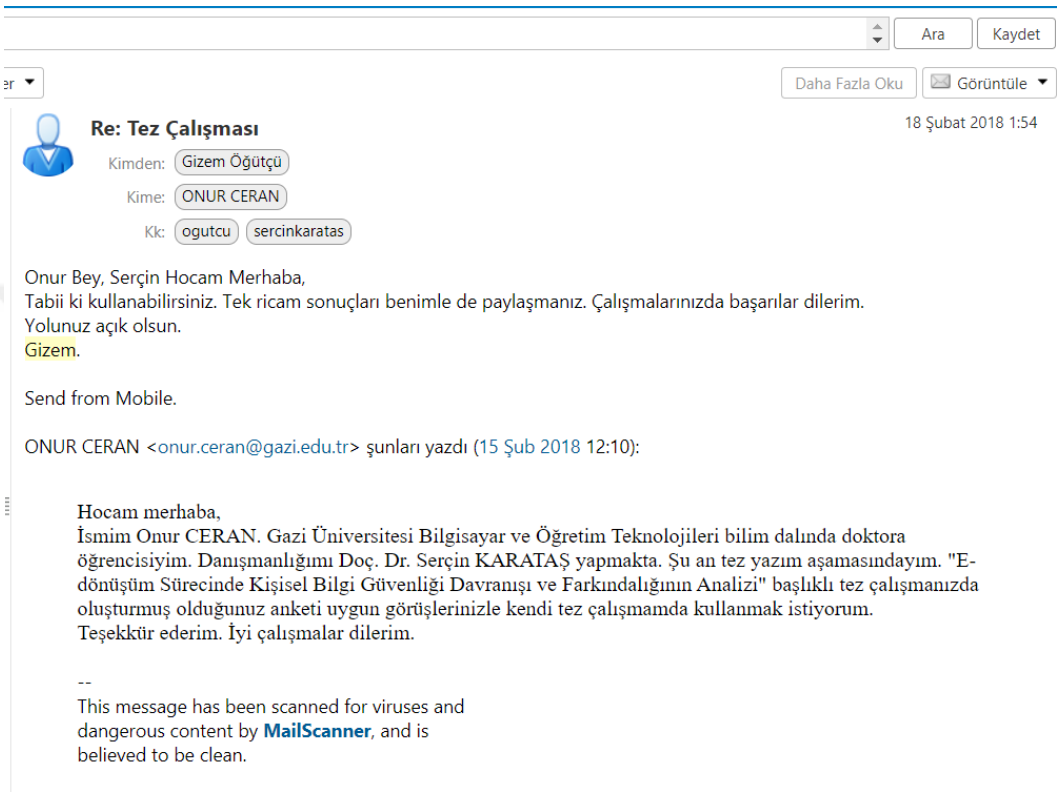
Tüm ekleri indir
Tüm ekleri kaldır

Merhaba,
60 maddelik versiyon yeni çalışılan BFI2. Henüz son halini almadı. BFI'in çevirisi ve ilgili yayınlar ekte. Başarılar dilerim..
NS

Prof. Dr. Nebi Sümer,
Orta Doğu Teknik Üniversitesi / Middle East Technical University
Psikoloji Bölümü / Department of Psychology
06800 Ankara / Turkey

http://www.nebisumer.com/

Korumacı Davranış, Riskli Davranış, Tehlike Algısı ve Suça Maruziyet Ölçekleri Kullanımı için Alınan İzin



Ara Kaydet

Daha Fazla Oku Görüntüle

Re: Tez Çalışması 18 Şubat 2018 1:54

Kimden: Gizem Öğütçü
Kime: ONUR CERAN
Kk: ogutcu sercinkaratas

Onur Bey, Serçin Hocam Merhaba,
Tabii ki kullanabilirsiniz. Tek ricam sonuçları benimle de paylaşmanız. Çalışmalarınızda başarılar dilerim.
Yolunuz açık olsun.
Gizem.

Send from Mobile.

ONUR CERAN <onur.ceran@gazi.edu.tr> şunları yazdı (15 Şub 2018 12:10):

Hocam merhaba,
İsmim Onur CERAN. Gazi Üniversitesi Bilgisayar ve Öğretim Teknolojileri bilim dalında doktora öğrencisiyim. Danışmanlığımı Doç. Dr. Serçin KARATAŞ yapmakta. Şu an tez yazım aşamasındayım. "E-dönüşüm Sürecinde Kişisel Bilgi Güvenliği Davranışı ve Farkındalığının Analizi" başlıklı tez çalışmanızda oluşturmuş olduğunuz anketi uygun görüşlerinizle kendi tez çalışmamda kullanmak istiyorum.
Teşekkür ederim. İyi çalışmalar dilerim.

--
This message has been scanned for viruses and
dangerous content by **MailScanner**, and is
believed to be clean.

Web Tasarım Ölçeği için Alınan İzin

Oguzhan Korkut Tez Icin

Gorusmek uzere 15:35

İyi aksamlar Onur bey 22:59

Hocam iyi aksamlar 22:59

Olcegimi kullanabilirsiniz elbette... 23:00

Hocam cok tesekkur ederim 23:00

Tez sanirim artik paylasiliyor sistemde, oradan olcegi alabiliyor musunu 23:01

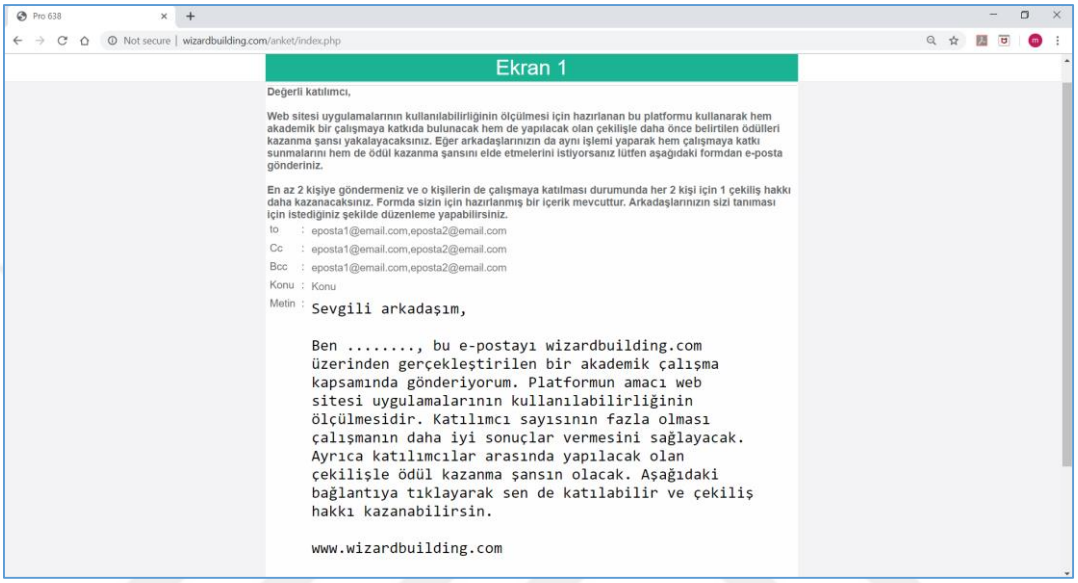
Dogrudur hocam tezinizi okudum 23:01

EK 5. www.wizarbuilding.com Web Sitesi İçin Alınan Uzman Görüşü

Ölçek Maddesi	U1	U2	U3	U4	U5	U6	U7
Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım.	Uygun	Uygun	Uygun	Uygun	Uygun	Uygun	Uygun
Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim.	Uygun	Uygun ancak katılımcıyı yorabilir. Kolaylaştırmak için yön tuşları yerine radyo butonu ile sorulabilir	Uygun	Ölçekte sıkıntı var. SSL bilmeyip https olunca güvenli olduğunu biliyorolabilir.	Uygun	Uygun	Uygun
Güvenlik duvarı, reklam önleyici vb. programlar kullanırım.	Uygun	Uygun ancak kullanıcıya ne yapacağı ile ilgili yönerge verilmelidir.	Uygun	Uygun ancak ölçekte sıkıntı var. reklam önleyici kontrol edildi diyelim güvenlik duvarı nasıl kontrol edilecek	Ekrana gerek olmadan Javascript ile kontol edilebilir mi?	Uygun buldum. Ancak kişilere başlangıçta sık kullandıkları tarayıcılarla bu uygulamayı test ettirecek bir yönlendirme yapılsa daha güzel olur. Çünkü linke tıkladığımda varsayılan ayarlara göre tarayıcı açıldığı için her zaman doğru sonuç vermeyebilir	Uygun
Virüs temizleme, casus yazılım önleme vb. programları kullanırım.	Uygun	Uygun	Burada ölçekle ilgili bir sorun var. Buna evet derse hangisini/hangilerini ya da hepsini mi kullandığını varsayacağız?	Uyuşma yoksa kontrol nasıl sağlanacak anlayamadım.	"diğer" seçeneğinin altında textbox ın ne olduğu anlaılmıyor. Yönerge koyulabilir	Uygun	Uygun
Kullandığım programların güncellemelerini düzenli olarak yaparım.	Uygun	Uygun	Uygun	Kullanıcı işletim sistemini update ediyor ancak ofis yazılımlarını update etmiyorsa ne olacak?	Ekran çok doğru kontol sağlamayabilir.	Görüş Bildirilmedi	Uygun
Bilgisayarımda orijinal (lisanslı) yazılım kullanmaya dikkat ederim.	Uygun	Uygun (geri dönüş sınırlı olabilir)	Uygun	Dikkat ederim ayrı kullanırım ayrıdır.	Uygun	Uygun	Uygun
Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim.	Uygun	Uygun (geri dönüş sınırlı olabilir)	Burada ölçekle ilgili bir sorun var. Geçici internet dosyalarını incelemek ayrı web gezinti geçmişini incelemek ayrı davranış.	Geçici internet dosyalarını kaç kişi inceliyor ki?	Uygun	Uygun	Uygun
Birden fazla elektronik posta adresi kullanırım.	Uygun	Uygun	Uygun	Ölçekte niye böyle birşey ölçülüyor?	Uygun	Uygun	Uygun
Kurumsal e-posta adresi günlük işlemlerde kullanılmamalıdır	Uygun	Uygun	Uygun	Bu bölümde nerede paylaştığı önemli. Kayıt için doğum tarihi istendiğinde sahte mi versin	Kişi bu alanların zorunlu olduğunu sanabilir.	Birincil e-posta alındığında bu e-posta veriliyorsa değerlendirilebilir.	Uygun
Ad, soyad, doğum tarihi gibi özlük bilgileri paylaşılmamalıdır	Uygun	Uygun ancak bilgi güvenliği konusundan dolayı katılımcı devam etmeyebilir	Uygun	Uygun	Uygun	Uygun	Uygun
GSM no, eposta, adres gibi iletişim bilgileri paylaşılmamalıdır	Uygun	Uygun	Uygun	Uygun	Uygun	Uygun buldum ancak senaryonun güçlendirilmesinde fayda olabilir.	Uygun
İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım.	Uygun	Uygun	Uygun	Görüş Bildirilmedi	Uygun	Uygun	Uygun
İçerik filtreleme programları kullanırım.	Görüş Bildirilmedi	Kullanıcıdan, sözü edilen yazılımlara örnek vermesi istenebilir	Görüş Bildirilmedi	Görüş Bildirilmedi	Görüş Bildirilmedi	Görüş Bildirilmedi	Görüş Bildirilmedi
E-posta filtreleme yazılımları kullanırım.	Görüş Bildirilmedi	Kullanıcıdan, sözü edilen yazılımlara örnek vermesi istenebilir	Görüş Bildirilmedi	Görüş Bildirilmedi	Görüş Bildirilmedi	Kullanmış olduğu e-posta adresleri bu konuda bence fikir verebilir. Kişi hala gmail, yahoo, Outlook vb.. güvenliğe daha fazla önem veren sunucular dışında mynet vb.. gibi posta sunucularını kullanıyorsa değerlendirmede kullanılabilir.	Görüş Bildirilmedi
İzleme yazılımları kullanarak internet üzerinde yapılan etkinlikler hakkında bilgi sahibi olurum.	Görüş Bildirilmedi	Görüş Bildirilmedi	İzleme yazılımının ne olduğunu bilmeyen kullanıcı hayır seçerse bilmiyor ama kullanıyor olabilir .	İzleme yazılımının ne olduğunu kullanıcı anlamayabilir	Görüş Bildirilmedi		Görüş Bildirilmedi
Herkesin kullanımına açık bir bilgisayardan ayrılmadan önce geçici internet dosyalarını ve Web gezinti geçmişlerini silerim.	Görüş Bildirilmedi	Görüş Bildirilmedi	Görüş Bildirilmedi	Görüş Bildirilmedi	Görüş Bildirilmedi	En azından bir önceki maddede yer alan kod çerezini sildirerek bu konuda bilgi ve becerisinin olduğu fikri oluşabilir.	Görüş Bildirilmedi
Dosyalarımı şifrelerim.	Görüş Bildirilmedi	Görüş Bildirilmedi	Görüş Bildirilmedi	Çok genel bir soru	Görüş Bildirilmedi	Uygulama içinde istenen bilgileri (senaryoya bağlı olarak) bir dosyada istenip dosya upload ettirilebilir. Sonra hızlıca kontrol edilir.	Görüş Bildirilmedi
Elektronik/ Mobil imza kullanırım.	Görüş Bildirilmedi	Görüş Bildirilmedi	Görüş Bildirilmedi	Bu soru geçerli olmayabilir.	E-imza ya da m-imza kullandığınız uygulamanın adlarını yazınız diye soru sorulabilir.	Cep telefonu bilgisine onay mesajı gönderip sonra bilgilerin kaydedilmesi sağlanabilir.	Görüş Bildirilmedi
İnternet sitelerine girerken genellikle sık kullanılanlar listesini kullanırım.	Görüş Bildirilmedi	İnternete girmek için birçok farklı araç olduğundan arayüzler farklıdır. (uygulaması zor)	Görüş Bildirilmedi	Amaç nedir?	Görüş Bildirilmedi	Ölçek maddesi sıkıntılı	Görüş Bildirilmedi
Bilgisayarımı şifre ile açılır.	Görüş Bildirilmedi	Görüş Bildirilmedi	Görüş Bildirilmedi	Madde kaldırılabilir	Görüş Bildirilmedi	Kısa süre verilip (30 sn. gibi) başlat +L tuşuna basıp ekran görüntüsünü dosya olarak yüklettirebilirsin. Böylelikle ekran yakalama ve şifre kullanıp kullanmadığı görülebilir.	Görüş Bildirilmedi
Bilgisayarımda otomatik kullan özelliğini kapatırım.	Görüş Bildirilmedi	Görüş Bildirilmedi	Ölçekteki soru anlaılmadı	Görüş Bildirilmedi	Görüş Bildirilmedi		Görüş Bildirilmedi
Parolalarımı sık sık değiştiririm.	Görüş Bildirilmedi	Görüş Bildirilmedi		Görüş Bildirilmedi	Görüş Bildirilmedi	Bilgisayar şifresinin değiştirilmesi bir activex ile yakalanabilir diye düşünüyorum ama onu yüklemek problem olabilir. Üzerine düşünülebilir.	12. soruyu test eden işlemi bir başka işlem için de tanıtıp tekrar şifre oluşturmasını isteyebilirsin
Kablosuz modem şifremi değiştiririm.	Görüş Bildirilmedi	Görüş Bildirilmedi	Ölçekteki soru ilk mi yoksa belli aralıklarla mı belli değil.	Belli aralıklarla sorulsa daha iyi olur	Görüş Bildirilmedi		Görüş Bildirilmedi
3ncü parti uygulama davetiyeleri kabul edilmemelidir	Görüş Bildirilmedi	Görüş Bildirilmedi	Görüş Bildirilmedi	Görüş Bildirilmedi	Görüş Bildirilmedi	3. parti kullanılan uygulamaların listesi istenebilir. İçinden zahmetli olsada ayıklanabilir.	Görüş Bildirilmedi
Parola başkalarıyla paylaşılmamalıdır	Görüş Bildirilmedi	Görüş Bildirilmedi	Görüş Bildirilmedi	Görüş Bildirilmedi	Görüş Bildirilmedi	Daha önce yazmış olduğum bir maddede şifreli dosyada oluşturulan parola da istenebilir. Bu şekilde değerlendirilebilir.	Görüş Bildirilmedi
Parola bir yerde yazılı olarak saklanmamalıdır	Görüş Bildirilmedi	Görüş Bildirilmedi	Görüş Bildirilmedi	Soruların yarısı kişinin davranışı yarısı genel davranışla ilgili. Tek tip olursa daha iyi olur.	Görüş Bildirilmedi	Üstteki madde ile bu da değerlendirilebilir.	Görüş Bildirilmedi

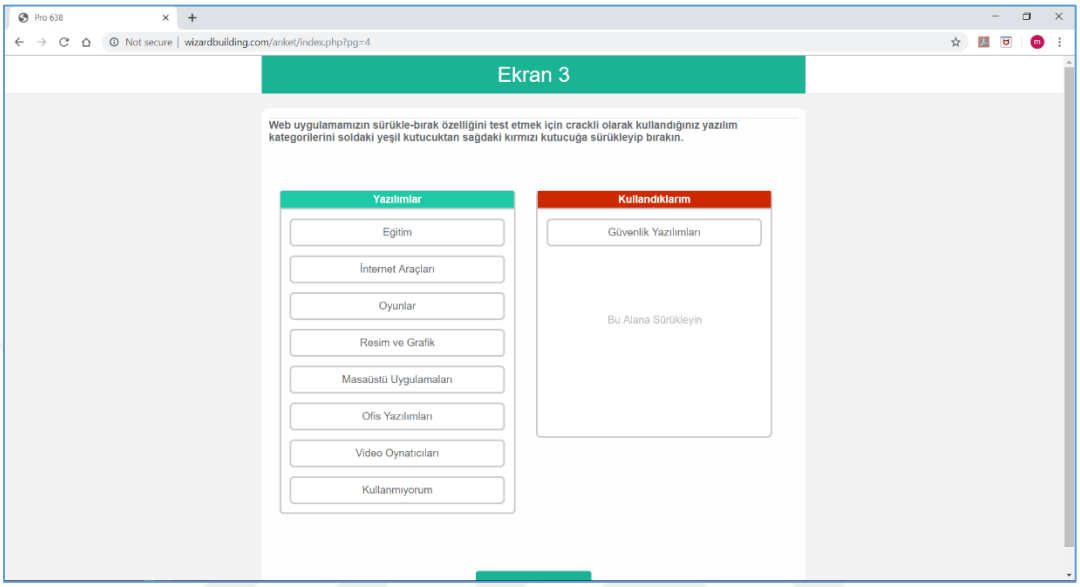
EK 6. http://wizardbuilding.com/anket/ Web Uygulamasına Ait Ekran Görüntüleri

Ekran 1: “Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım” maddesine karşılık gelen ekran

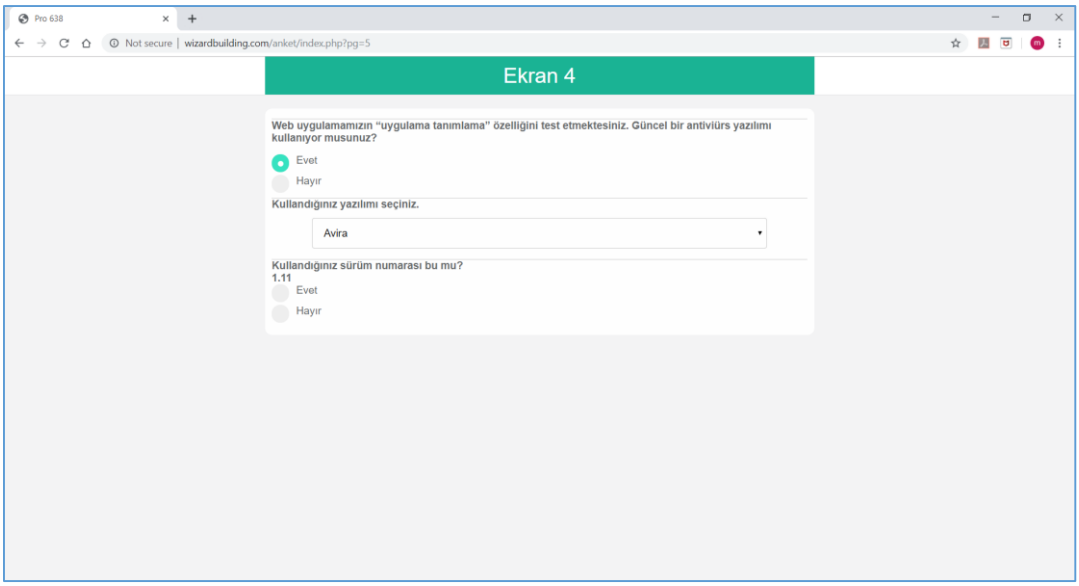


Ekran 2: “Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim.” maddesine karşılık gelen ekran

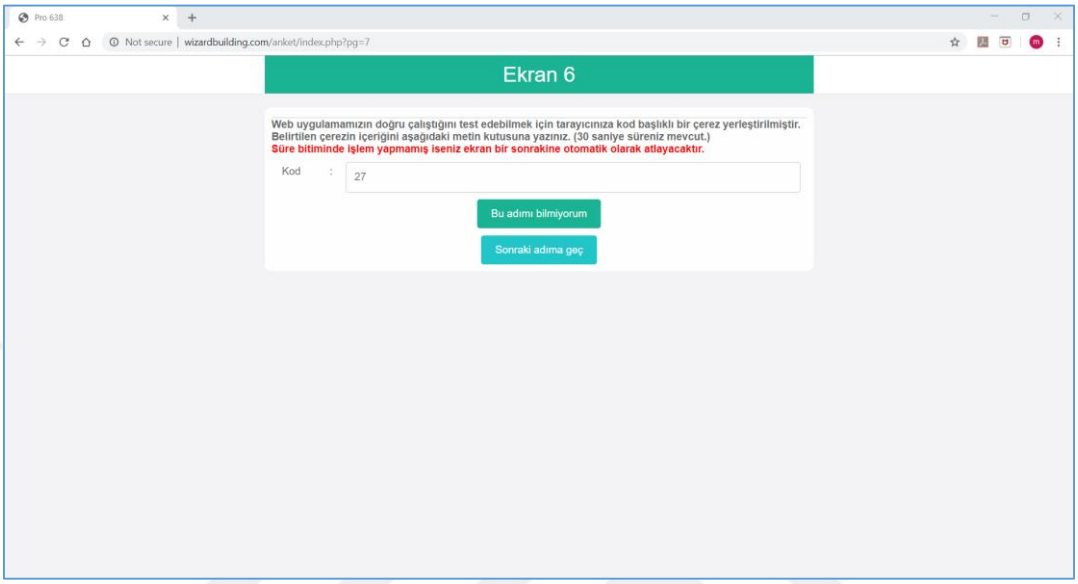
Ekran 3: “Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim.” maddesine karşılık gelen ekran



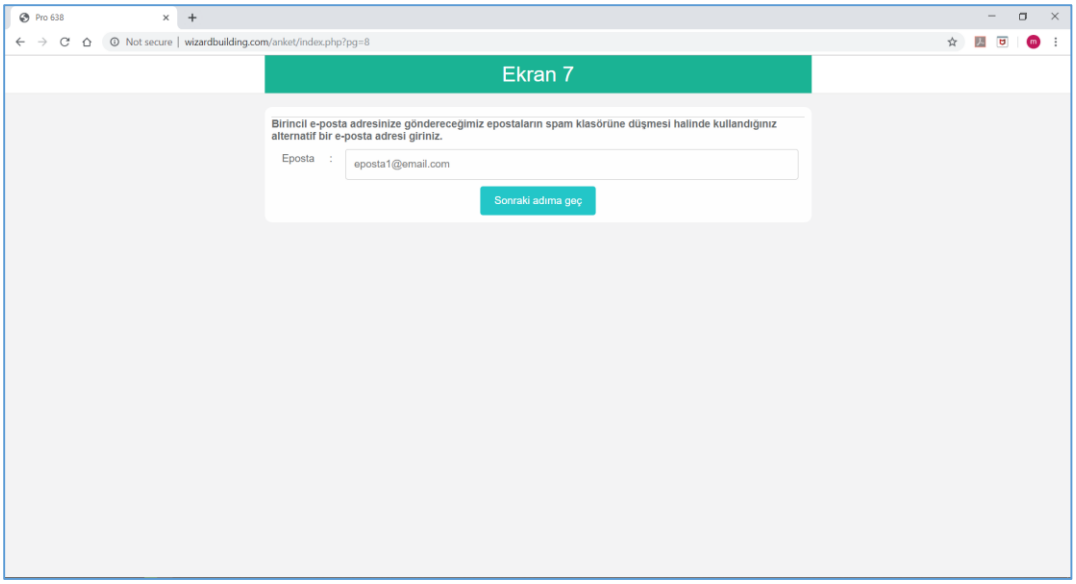
Ekran 4: “Virus temizleme, casus yazılım önleme vb. programları kullanırım.” maddesine karşılık gelen ekran



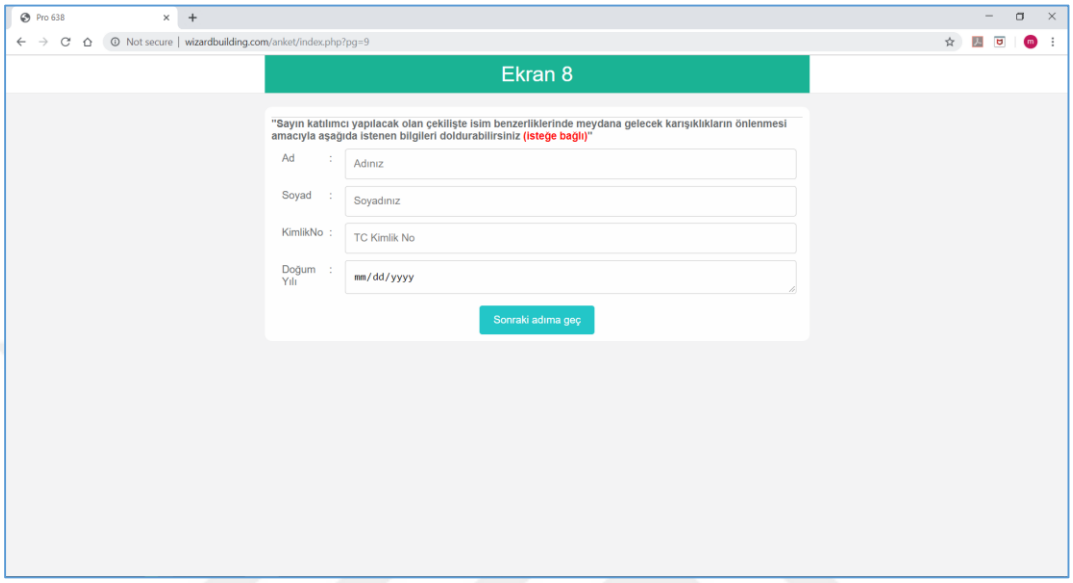
Ekran 6: “Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim.” maddesine karşılık gelen ekran



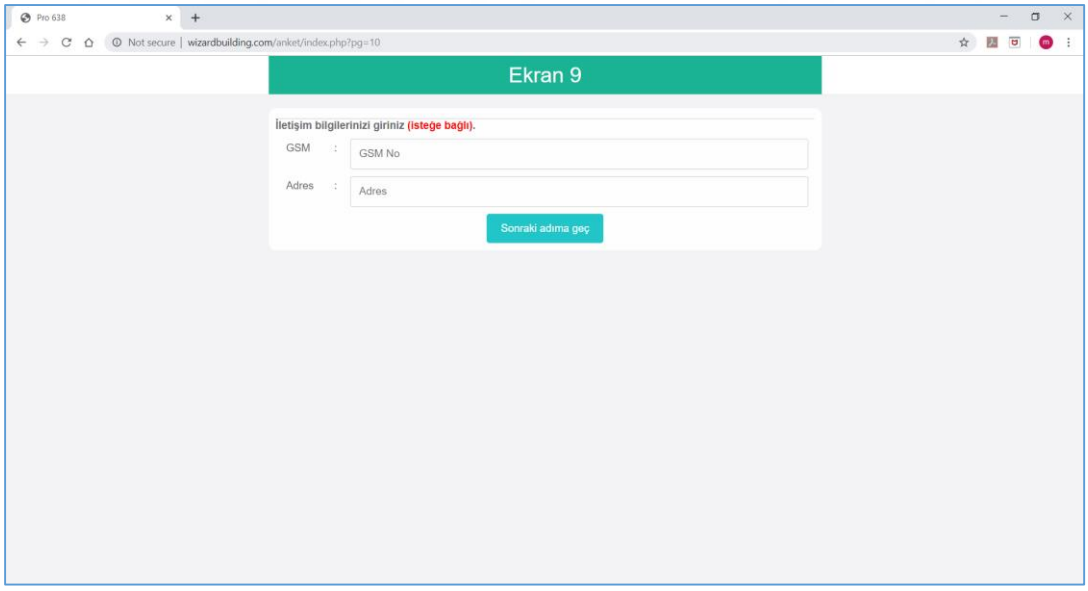
Ekran 7: “Birden fazla elektronik posta adresi kullanırım.” maddesine karşılık gelen ekran



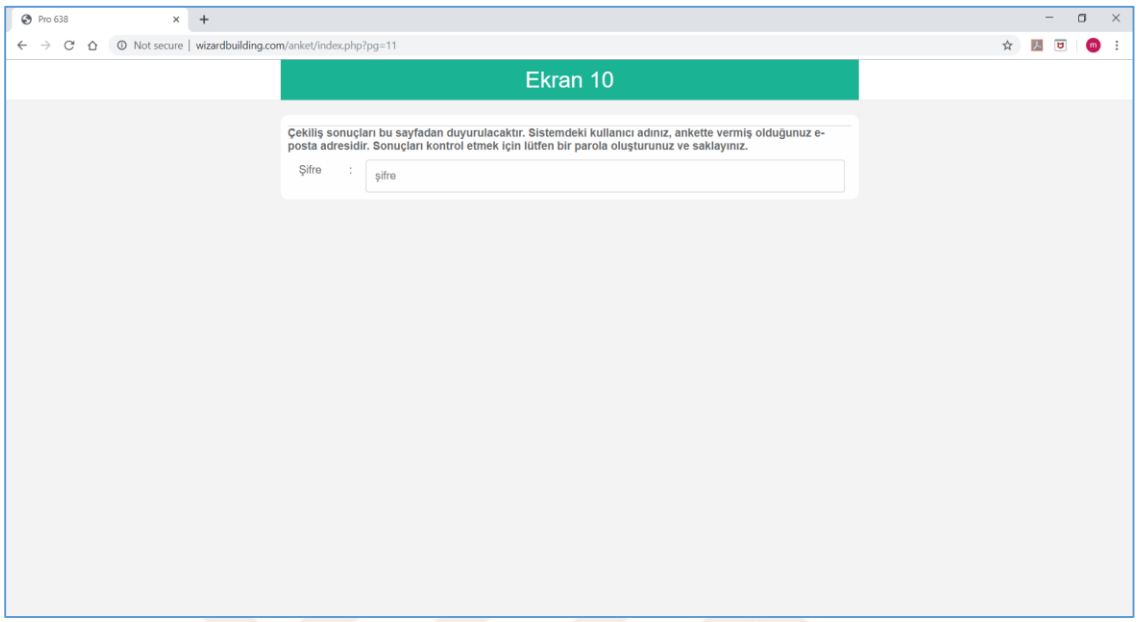
Ekran 8: “İnternet ortamında gerektiği durumlarda özlük bilgilerimi (ad, soyad, doğum tarihi vb.) paylaşırım.” maddesine karşılık gelen ekran



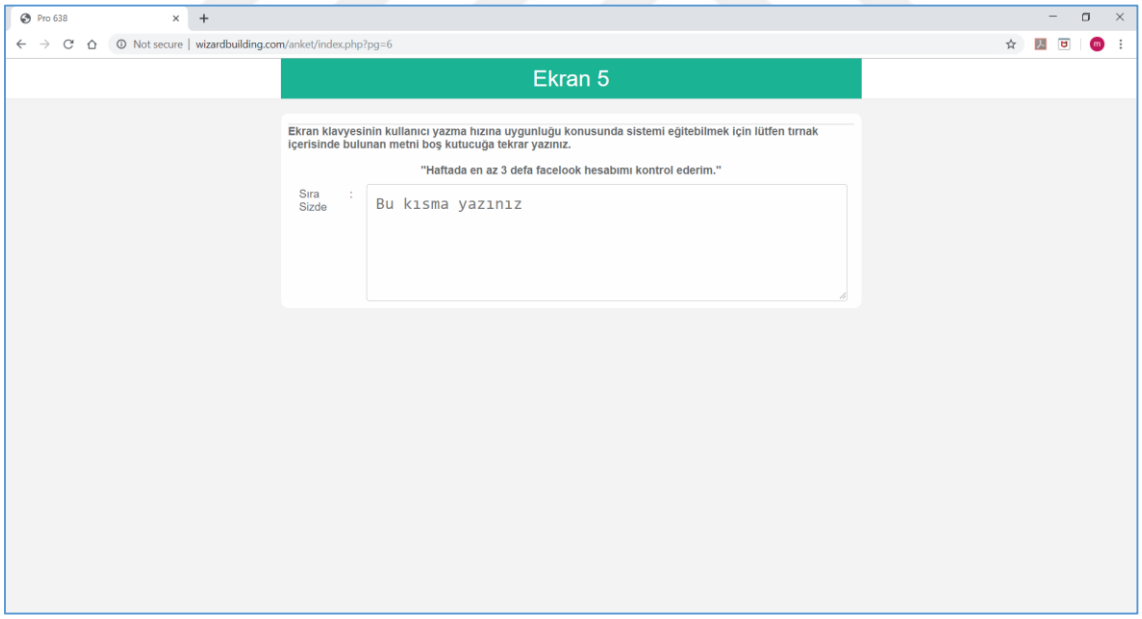
Ekran 9: “İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım.” maddesine karşılık gelen ekran



Ekran 10: “İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım.” maddesine karşılık gelen ekran



Ekran 5: “Hatalı yazım yönlendirmesi” maddesine karşılık gelen ekran



EK 7. Bilgi Güvenliği Davranışları ile Demografik ve Sosyo-demografik Özellikler Arasındaki İlişkiyi Gösterir Tablolar

Davranış: Birden fazla elektronik posta adresi kullanırım

Cinsiyet

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	9.587[a]	3	.022
Likelihood Ratio	10.339	3	.016
Linear-by-Linear Association	8.972	1	.003
N of Valid Cases	301		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 13.33.

Eğitim Düzeyi

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	29.221[a]	15	.015
Likelihood Ratio	29.050	15	.016
Linear-by-Linear Association	12.405	1	.000
N of Valid Cases	301		

a. 9 cells (37.5%) have expected count less than 5. The minimum expected count is .56.

Yaş Aralığı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	4.904[a]	9	.843
Likelihood Ratio	5.036	9	.831
Linear-by-Linear Association	.322	1	.570
N of Valid Cases	301		

a. 5 cells (31.3%) have expected count less than 5. The minimum expected count is .90.

İnternet Kullanım Yılı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	17.620[a]	9	.040
Likelihood Ratio	18.549	9	.029
Linear-by-Linear Association	9.003	1	.003
N of Valid Cases	301		

a. 3 cells (18.8%) have expected count less than 5. The minimum expected count is 1.69.

Günlük İnternet Kullanım Saati

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	5.267[a]	9	.810
Likelihood Ratio	5.469	9	.792
Linear-by-Linear Association	1.477	1	.224
N of Valid Cases	301		

a. 2 cells (12.5%) have expected count less than 5. The minimum expected count is 2.60.

Davranış: Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim.

Cinsiyet

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	7.357[a]	3	.061
Likelihood Ratio	7.404	3	.060
Linear-by-Linear Association	7.178	1	.007
N of Valid Cases	301		

a. 2 cells (25.0%) have expected count less than 5. The minimum expected count is 2.74.

Eğitim Düzeyi

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	10.263[a]	15	.803
Likelihood Ratio	14.109	15	.517
Linear-by-Linear Association	.180	1	.671
N of Valid Cases	301		

a. 16 cells (66.7%) have expected count less than 5. The minimum expected count is .12.

Yaş Aralığı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	8.303[a]	9	.504
Likelihood Ratio	9.012	9	.436
Linear-by-Linear Association	.000	1	.988
N of Valid Cases	301		

a. 9 cells (56.3%) have expected count less than 5. The minimum expected count is .19.

İnternet Kullanım Yılı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	8.895[a]	9	.447
Likelihood Ratio	10.351	9	.323
Linear-by-Linear Association	.055	1	.815
N of Valid Cases	301		

a. 8 cells (50.0%) have expected count less than 5. The minimum expected count is .35.

Günlük İnternet Kullanım Saati

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	8.692[a]	9	.466
Likelihood Ratio	8.742	9	.461
Linear-by-Linear Association	.301	1	.583
N of Valid Cases	301		

a. 8 cells (50.0%) have expected count less than 5. The minimum expected count is .53.

Davranış: Güvenlik duvarı, reklam önleyici vb. programlar kullanırım.

Cinsiyet

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	3.462[a]	3	.326
Likelihood Ratio	3.933	3	.269
Linear-by-Linear Association	2.968	1	.085
N of Valid Cases	301		

a. 2 cells (25.0%) have expected count less than 5. The minimum expected count is .39.

Eğitim Düzeyi

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	20.603[a]	15	.150
Likelihood Ratio	19.384	15	.197
Linear-by-Linear Association	4.097	1	.043
N of Valid Cases	301		

a. 15 cells (62.5%) have expected count less than 5. The minimum expected count is .02.

Yaş Aralığı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	2.000[a]	9	.991
Likelihood Ratio	2.728	9	.974
Linear-by-Linear Association	.896	1	.344
N of Valid Cases	301		

a. 9 cells (56.3%) have expected count less than 5. The minimum expected count is .03.

İnternet Kullanım Yılı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	12.917[a]	9	.166
Likelihood Ratio	14.024	9	.121
Linear-by-Linear Association	1.268	1	.260
N of Valid Cases	301		

a. 9 cells (56.3%) have expected count less than 5. The minimum expected count is .05.

Günlük İnternet Kullanım Saati

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	5.236[a]	9	.813
Likelihood Ratio	5.146	9	.821
Linear-by-Linear Association	.118	1	.731
N of Valid Cases	301		

a. 8 cells (50.0%) have expected count less than 5. The minimum expected count is .08.

Davranış: Virüs temizleme, casus yazılım önleme vb. programları kullanırım.

Cinsiyet

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	.211[a]	3	.976
Likelihood Ratio	.214	3	.975
Linear-by-Linear Association	.039	1	.843
N of Valid Cases	301		

a. 2 cells (25.0%) have expected count less than 5. The minimum expected count is 1.96.

Eğitim Düzeyi

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	16.008[a]	15	.382
Likelihood Ratio	18.534	15	.236
Linear-by-Linear Association	.116	1	.733
N of Valid Cases	301		

a. 17 cells (70.8%) have expected count less than 5. The minimum expected count is .08.

Yaş Aralığı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	4.176[a]	9	.899
Likelihood Ratio	5.044	9	.830
Linear-by-Linear Association	.023	1	.879
N of Valid Cases	301		

a. 10 cells (62.5%) have expected count less than 5. The minimum expected count is .13.

İnternet Kullanım Yılı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	6.451[a]	9	.694
Likelihood Ratio	7.928	9	.541
Linear-by-Linear Association	.052	1	.820
N of Valid Cases	301		

a. 9 cells (56.3%) have expected count less than 5. The minimum expected count is .25.

Günlük İnternet Kullanım Saati

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	5.637[a]	9	.776
Likelihood Ratio	7.654	9	.569
Linear-by-Linear Association	.010	1	.920
N of Valid Cases	301		

a. 9 cells (56.3%) have expected count less than 5. The minimum expected count is .38.

Davranış: Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim.

Cinsiyet

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	3.380[a]	3	.337
Likelihood Ratio	4.026	3	.259
Linear-by-Linear Association	.346	1	.557
N of Valid Cases	301		

a. 4 cells (50.0%) have expected count less than 5. The minimum expected count is .39.

Eğitim Düzeyi

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	19.267[a]	15	.202
Likelihood Ratio	13.406	15	.571
Linear-by-Linear Association	1.394	1	.238
N of Valid Cases	301		

a. 15 cells (62.5%) have expected count less than 5. The minimum expected count is .02.

Yaş Aralığı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	11.331[a]	9	.254
Likelihood Ratio	8.482	9	.486
Linear-by-Linear Association	.290	1	.590
N of Valid Cases	301		

a. 9 cells (56.3%) have expected count less than 5. The minimum expected count is .03.

İnternet Kullanım Yılı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	5.371[a]	9	.801
Likelihood Ratio	5.664	9	.773
Linear-by-Linear Association	.379	1	.538
N of Valid Cases	301		

a. 9 cells (56.3%) have expected count less than 5. The minimum expected count is .05.

Günlük İnternet Kullanım Saati

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	9.566[a]	9	.387
Likelihood Ratio	9.977	9	.352
Linear-by-Linear Association	.042	1	.837
N of Valid Cases	301		

a. 8 cells (50.0%) have expected count less than 5. The minimum expected count is .08.

Davranış: İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım.

Cinsiyet

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	4.304[a]	3	.230
Likelihood Ratio	4.863	3	.182
Linear-by-Linear Association	1.986	1	.159
N of Valid Cases	301		

a. 2 cells (25.0%) have expected count less than 5. The minimum expected count is .39.

Eğitim Düzeyi

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	10.270[a]	15	.802
Likelihood Ratio	14.403	15	.495
Linear-by-Linear Association	2.109	1	.146
N of Valid Cases	301		

a. 17 cells (70.8%) have expected count less than 5. The minimum expected count is .02.

Yaş Aralığı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	9.530[a]	9	.390
Likelihood Ratio	8.151	9	.519
Linear-by-Linear Association	.035	1	.851
N of Valid Cases	301		

a. 10 cells (62.5%) have expected count less than 5. The minimum expected count is .03.

İnternet Kullanım Yılı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	9.530[a]	9	.390
Likelihood Ratio	8.151	9	.519
Linear-by-Linear Association	.035	1	.851
N of Valid Cases	301		

a. 10 cells (62.5%) have expected count less than 5. The minimum expected count is .03.

Günlük İnternet Kullanım Saati

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	21.875[a]	9	.009
Likelihood Ratio	15.879	9	.069
Linear-by-Linear Association	.051	1	.821
N of Valid Cases	301		

a. 9 cells (56.3%) have expected count less than 5. The minimum expected count is .08.

Davranış: Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim

Cinsiyet

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	2.675[a]	3	.444
Likelihood Ratio	2.679	3	.444
Linear-by-Linear Association	2.319	1	.128
N of Valid Cases	301		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 12.94.

Eğitim Düzeyi

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	14.258[a]	15	.506
Likelihood Ratio	14.711	15	.472
Linear-by-Linear Association	.007	1	.933
N of Valid Cases	301		

a. 8 cells (33.3%) have expected count less than 5. The minimum expected count is .55.

Yaş Aralığı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	9.291[a]	9	.411
Likelihood Ratio	9.745	9	.371
Linear-by-Linear Association	3.503	1	.061
N of Valid Cases	301		

a. 5 cells (31.3%) have expected count less than 5. The minimum expected count is .88.

İnternet Kullanım Yılı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	2.593[a]	9	.978
Likelihood Ratio	2.366	9	.984
Linear-by-Linear Association	.534	1	.465
N of Valid Cases	301		

a. 2 cells (12.5%) have expected count less than 5. The minimum expected count is 1.64.

Günlük İnternet Kullanım Saati

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	7.608[a]	9	.574
Likelihood Ratio	7.799	9	.554
Linear-by-Linear Association	.067	1	.796
N of Valid Cases	301		

a. 2 cells (12.5%) have expected count less than 5. The minimum expected count is 2.52.

Davranış: Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım.

Cinsiyet

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	2.647[a]	3	.449
Likelihood Ratio	2.940	3	.401
Linear-by-Linear Association	.005	1	.943
N of Valid Cases	301		

a. 2 cells (25.0%) have expected count less than 5. The minimum expected count is .39.

Eğitim Düzeyi

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	8.762[a]	15	.890
Likelihood Ratio	8.482	15	.903
Linear-by-Linear Association	2.536	1	.111
N of Valid Cases	301		

a. 16 cells (66.7%) have expected count less than 5. The minimum expected count is .02.

Yaş Aralığı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	9.153[a]	9	.423
Likelihood Ratio	10.259	9	.330
Linear-by-Linear Association	2.813	1	.093
N of Valid Cases	301		

a. 9 cells (56.3%) have expected count less than 5. The minimum expected count is .03.

İnternet Kullanım Yılı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	7.070[a]	9	.630
Likelihood Ratio	9.367	9	.404
Linear-by-Linear Association	1.214	1	.271
N of Valid Cases	301		

a. 8 cells (50.0%) have expected count less than 5. The minimum expected count is .05.

Günlük İnternet Kullanım Saati

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	6.626[a]	9	.676
Likelihood Ratio	7.365	9	.599
Linear-by-Linear Association	.464	1	.496
N of Valid Cases	301		

a. 8 cells (50.0%) have expected count less than 5. The minimum expected count is .08.

Davranış: Kurumsal e-posta adresimi günlük işlerde de kullanırım. (Riskli Davranış)

Cinsiyet

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1.363[a]	3	.714
Likelihood Ratio	1.364	3	.714
Linear-by-Linear Association	1.089	1	.297
N of Valid Cases	301		

a. 1 cells (12.5%) have expected count less than 5. The minimum expected count is 4.31.

Eğitim Düzeyi

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	11.049[a]	15	.749
Likelihood Ratio	13.050	15	.598
Linear-by-Linear Association	4.391	1	.036
N of Valid Cases	301		

a. 12 cells (50.0%) have expected count less than 5. The minimum expected count is .18.

Yaş Aralığı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	5.972[a]	9	.743
Likelihood Ratio	8.539	9	.481
Linear-by-Linear Association	.271	1	.603
N of Valid Cases	301		

a. 8 cells (50.0%) have expected count less than 5. The minimum expected count is .29.

İnternet Kullanım Yılı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	6.898[a]	9	.648
Likelihood Ratio	7.196	9	.617
Linear-by-Linear Association	.176	1	.675
N of Valid Cases	301		

a. 8 cells (50.0%) have expected count less than 5. The minimum expected count is .55.

Günlük İnternet Kullanım Saati

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	3.551[a]	9	.938
Likelihood Ratio	3.242	9	.954
Linear-by-Linear Association	.024	1	.876
N of Valid Cases	301		

a. 7 cells (43.8%) have expected count less than 5. The minimum expected count is .84.

Davranış: İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım. (Riskli Davranış)

Cinsiyet

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1.730[a]	3	.630
Likelihood Ratio	1.765	3	.623
Linear-by-Linear Association	.419	1	.518
N of Valid Cases	301		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 5.49.

Eğitim Düzeyi

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	29.716[a]	15	.013
Likelihood Ratio	29.928	15	.012
Linear-by-Linear Association	3.352	1	.067
N of Valid Cases	301		

a. 12 cells (50.0%) have expected count less than 5. The minimum expected count is .23.

Yaş Aralığı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	19.408[a]	9	.022
Likelihood Ratio	16.221	9	.062
Linear-by-Linear Association	.046	1	.831
N of Valid Cases	301		

a. 7 cells (43.8%) have expected count less than 5. The minimum expected count is .37.

İnternet Kullanım Yılı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	6.173[a]	9	.722
Likelihood Ratio	5.444	9	.794
Linear-by-Linear Association	2.025	1	.155
N of Valid Cases	301		

a. 5 cells (31.3%) have expected count less than 5. The minimum expected count is .70.

Günlük İnternet Kullanım Saati

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	11.047[a]	9	.273
Likelihood Ratio	14.229	9	.114
Linear-by-Linear Association	2.004	1	.157
N of Valid Cases	301		

a. 4 cells (25.0%) have expected count less than 5. The minimum expected count is 1.07.

Davranış: İnternet ortamında gerektiği durumlarda özlük bilgilerimi (ad, soyad, doğum tarihi vb.) paylaşırım. (Riskli Davranış)

Cinsiyet

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	4.423[a]	3	.219
Likelihood Ratio	4.448	3	.217
Linear-by-Linear Association	1.150	1	.283
N of Valid Cases	301		

a. 2 cells (25.0%) have expected count less than 5. The minimum expected count is 1.96.

Eğitim Düzeyi

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	38.117[a]	15	.001
Likelihood Ratio	27.830	15	.023
Linear-by-Linear Association	1.001	1	.317
N of Valid Cases	301		

a. 14 cells (58.3%) have expected count less than 5. The minimum expected count is .08.

Yaş Aralığı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	15.187[a]	9	.086
Likelihood Ratio	14.358	9	.110
Linear-by-Linear Association	2.106	1	.147
N of Valid Cases	301		

a. 8 cells (50.0%) have expected count less than 5. The minimum expected count is .13.

İnternet Kullanım Yılı

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	7.321[a]	9	.604
Likelihood Ratio	8.939	9	.443
Linear-by-Linear Association	.004	1	.950
N of Valid Cases	301		

a. 6 cells (37.5%) have expected count less than 5. The minimum expected count is .25.

Günlük İnternet Kullanım Saati

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	11.953[a]	9	.216
Likelihood Ratio	11.821	9	.224
Linear-by-Linear Association	3.439	1	.064
N of Valid Cases	301		

a. 7 cells (43.8%) have expected count less than 5. The minimum expected count is .38.

EK 8. Bilgi Güvenliği Davranışları ile Kişilik Özellikleri Arasındaki İlişkiyi Gösterir Tablolar

Davranış: Birden fazla elektronik posta adresi kullanırım.

Test Statistics[a,b]

	Ozdenetim	Uyumluluk	Nevrotizm	Gelisime Aciklik	Disa Donukluk
Chi-Square	3.387	7.077	6.670	3.183	8.622
df	3	3	3	3	3
Asymp. Sig.	.336	.069	.083	.364	.035

a. Kruskal Wallis Test

b. Grouping Variable: Birden fazla elektronik posta adresi kullanırım

Davranış: Güvenlik duvarı, reklam önleyici vb. programlar kullanırım.

Test Statistics[a,b]

	Ozdenetim	Uyumluluk	Nevrotizm	Gelisime Aciklik	Disa Donukluk
Chi-Square	3.758	1.161	4.441	.691	.415
df	1	1	1	1	1
Asymp. Sig.	.053	.281	.035	.406	.519

a. Kruskal Wallis Test

b. Grouping Variable: Güvenlik duvarı, reklam önleyici vb. Programlar kullanırım

Davranış: Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim.

Test Statistics[a,b]

	Ozdenetim	Uyumluluk	Nevrotizm	Gelisime Aciklik	Disa Donukluk
Chi-Square	11.682	9.643	11.362	8.381	14.306
df	3	3	3	3	3
Asymp. Sig.	.009	.022	.010	.039	.003

a. Kruskal Wallis Test

b. Grouping Variable: Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim

Davranış: Virüs temizleme, casus yazılım önleme vb. programları kullanırım.

Test Statistics[a,b]

	Ozdenetim	Uyumluluk	Nevrotizm	Gelisime Aciklik	Disa Donukluk
Chi-Square	3.679	5.569	3.598	.931	4.229
df	3	3	3	3	3
Asymp. Sig.	.298	.135	.308	.818	.238

a. Kruskal Wallis Test

b. Grouping Variable: Virüs temizleme, casus yazılım önleme vb. Programları kullanırım

Davranış: Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim.

Test Statistics[a,b]

	Ozdenetim	Uyumluluk	Nevrotizm	Gelisime Aciklik	Disa Donukluk
Chi-Square	.784	1.470	2.867	3.838	1.061
df	3	3	3	3	3
Asymp. Sig.	.853	.689	.413	.280	.786

a. Kruskal Wallis Test

b. Grouping Variable: Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim

Davranış: İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım.

Test Statistics[a,b]

	Ozdenetim	Uyumluluk	Nevrotizm	Gelisime Aciklik	Disa Donukluk
Chi-Square	6.486	8.811	11.045	12.501	3.141
df	3	3	3	3	3
Asymp. Sig.	.090	.032	.011	.006	.370

a. Kruskal Wallis Test

b. Grouping Variable: İnternet üzerindeki hesaplarımda kolay tahmin edilemeycek şekilde karmaşık ve uzun şifreler kullanırım

Davranış: Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim.

Test Statistics[a,b]

	Ozdenetim	Uyumluluk	Nevrotizm	Gelisime Aciklik	Disa Donukluk
Chi-Square	8.315	11.746	8.137	3.654	4.915
df	3	3	3	3	3
Asymp. Sig.	.040	.008	.043	.301	.178

a. Kruskal Wallis Test

b. Grouping Variable: Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim

Davranış: Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım.

Test Statistics[a,b]

	Ozdenetim	Uyumluluk	Nevrotizm	Gelisime Aciklik	Disa Donukluk
Chi-Square	2.732	.958	.173	2.833	2.814
df	2	2	2	2	2
Asymp. Sig.	.255	.619	.917	.243	.245

a. Kruskal Wallis Test

b. Grouping Variable: Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım

H_0 Kabul edilmiştir.

Davranış: Kurumsal e-posta adresimi günlük işlerde de kullanırım. (Riskli Davranış)

Test Statistics[a,b]

	Ozdenetim	Uyumluluk	Nevrotizm	Gelisime Aciklik	Disa Donukluk
Chi-Square	15.275	5.685	2.051	14.799	14.553
df	3	3	3	3	3
Asymp. Sig.	.002	.128	.562	.002	.002

a. Kruskal Wallis Test

b. Grouping Variable: Kurumsal e-posta adresimi günlük işlerde de kullanırım

Davranış: İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım.

Test Statistics[a,b]

	Ozdenetim	Uyumluluk	Nevrotizm	Gelisime Aciklik	Disa Donukluk
Chi-Square	4.145	4.395	3.500	4.553	.664
df	3	3	3	3	3
Asymp. Sig.	.246	.222	.321	.208	.882

a. Kruskal Wallis Test

b. Grouping Variable: İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (Gsm no, eposta vb.) paylaşırım

Davranış: İnternet ortamında gerektiği durumlarda özlük bilgilerimi (ad, soyad, doğum tarihi vb.) paylaşırım. (Riskli Davranış)

Test Statistics[a,b]

	Ozdenetim	Uyumluluk	Nevrotizm	Gelisime Aciklik	Disa Donukluk
Chi-Square	14.470	1.873	16.195	3.655	5.014
df	3	3	3	3	3
Asymp. Sig.	.002	.599	.001	.301	.171

a. Kruskal Wallis Test

b. Grouping Variable: İnternet ortamında gerektiği durumlarda özlük bilgilerimi (ad,soyad , doğum tarihi vb.) paylaşırım

EK 9. Bilgi Güvenliği Davranışları ile Tehlike Algısı, Suça Maruziyet Durumu, Riskli ve Korumacı Davranışları Arasındaki İlişkiyi Gösterir Tablolar

Davranış: İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım.

Test Statistics[a,b]

	Riskli D P	Korumacı D P	Suca Maruziyet P	Tehlike Algisi P
Chi-Square	1.901	19.705	1.549	1.188
df	2	2	2	2
Asymp. Sig.	.387	.000	.461	.552

a. Kruskal Wallis Test

b. Grouping Variable: İnternet üzerindeki hesaplarımda kolay tahmin edilemeycek şekilde karmaşık ve uzun şifreler kullanırım

Davranış: Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim.

Test Statistics[a,b]

	Riskli D P	Korumacı D P	Suca Maruziyet P	Tehlike Algisi P
Chi-Square	3.442	85.071	6.489	14.953
df	3	3	3	3
Asymp. Sig.	.328	.000	.090	.002

a. Kruskal Wallis Test

b. Grouping Variable: Girdiğim sitelerin SSL sertfikası olup olmadığına dikkat ederim

Davranış: İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım. (Riskli Davranış)

Test Statistics[a,b]

	Riskli D P	Korumacı D P	Suca Maruziyet P	Tehlike Algisi P
Chi-Square	60.107	2.982	4.621	2.527
df	3	3	3	3
Asymp. Sig.	.000	.394	.202	.470

a. Kruskal Wallis Test

b. Grouping Variable: İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (Gsm no, eposta vb.) paylaşırım

Davranış: Kurumsal e-posta adresimi günlük işlerde de kullanırım. (Riskli Davranış)

Test Statistics[a,b]

	Riskli D P	Korumacı D P	Suca Maruziyet P	Tehlike Algisi P
Chi-Square	15.569	5.562	.380	7.915
df	3	3	3	3
Asymp. Sig.	.001	.135	.944	.048

a. Kruskal Wallis Test

b. Grouping Variable: Kurumsal e-posta adresimi günlük işlerde de kullanırım

Davranış: Virüs temizleme, casus yazılım önleme vb. programları kullanırım

Test Statistics[a,b]

	Riskli D P	Korumacı D P	Suca Maruziyet P	Tehlike Algisi P
Chi-Square	6.705	13.979	.796	1.888
df	3	3	3	3
Asymp. Sig.	.082	.003	.851	.596

a. Kruskal Wallis Test

b. Grouping Variable: Virus temizleme, casus yazılım önleme vb. Programları kullanırım

Davranış: Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim.

Test Statistics[a,b]

	Riskli D P	Korumacı D P	Suca Maruziyet P	Tehlike Algisi P
Chi-Square	5.873	21.426	3.411	3.963
df	3	3	3	3
Asymp. Sig.	.118	.000	.332	.265

a. Kruskal Wallis Test

b. Grouping Variable: Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim

Davranış: Birden fazla elektronik posta adresi kullanırım.

Test Statistics[a,b]

	Riskli D P	Korumacı D P	Suca Maruziyet P	Tehlike Algisi P
Chi-Square	20.890	3.591	1.644	4.620
df	3	3	3	3
Asymp. Sig.	.000	.309	.649	.202

a. Kruskal Wallis Test

b. Grouping Variable: Birden fazla elektronik posta adresi kullanırım

Davranış: Güvenlik duvarı, reklam önleyici vb. programlar kullanırım.

Test Statistics[a,b]

	Riskli D P	Korumacı D P	Suca Maruziyet P	Tehlike Algisi P
Chi-Square	1.246	36.449	2.856	.927
df	2	2	2	2
Asymp. Sig.	.536	.000	.240	.629

a. Kruskal Wallis Test

b. Grouping Variable: Güvenlik duvarı, reklam önleyici vb. Programlar kullanırım

Davranış: İnternet ortamında gerektiği durumlarda özlük bilgilerimi (ad, soyad, doğum tarihi vb.) paylaşırım. (Riskli Davranış)

Multivariate Tests[a]

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	.833	365.885[b]	4.000	294.000	.000	.833
	Wilks' Lambda	.167	365.885[b]	4.000	294.000	.000	.833
	Hotelling's Trace	4.978	365.885[b]	4.000	294.000	.000	.833
	Roy's Largest Root	4.978	365.885[b]	4.000	294.000	.000	.833
ozluk_paylasim_a	Pillai's Trace	.264	7.129	12.000	888.000	.000	.088
	Wilks' Lambda	.740	7.811	12.000	778.142	.000	.095
	Hotelling's Trace	.346	8.439	12.000	878.000	.000	.103
	Roy's Largest Root	.331	24.476[c]	4.000	296.000	.000	.249

a. Design: Intercept + İnternet ortamında gerektiği durumlarda özlük bilgilerimi (ad,soyad , doğum tarihi vb.) paylaşırım

b. Exact statistic

c. The statistic is an upper bound on F that yields a lower bound on the significance level.

Davranış: Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim.

Test Statistics[a,b]

	Riskli D P	Korumacı D P	Suca Maruziyet P	Tehlike Algisi P
Chi-Square	.390	15.026	3.377	4.418
df	3	3	3	3
Asymp. Sig.	.942	.002	.337	.220

a. Kruskal Wallis Test

b. Grouping Variable: Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim

Davranış: Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım.

Test Statistics[a,b]

	Riskli D P	Korumacı D P	Suca Maruziyet P	Tehlike Algisi P
Chi-Square	1.633	11.084	.950	1.372
df	2	2	2	2
Asymp. Sig.	.442	.004	.622	.504

a. Kruskal Wallis Test

b. Grouping Variable: Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım

EK 10. Bilgi Güvenliği Davranışları ile Bireylerin Klavye Kullanım Hızları ve Dikkat Değişkenleri Arasındaki İlişkiyi Gösterir Tablolar

Davranış: İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım.

Yazma Hızı

ANOVA

Yazma Hizi

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1253.300	3	417.767	1.466	.224
Within Groups	84344.096	296	284.946		
Total	85597.397	299			

Okuduğunu Görme

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	6.663[a]	3	.083
Likelihood Ratio	6.475	3	.091
Linear-by-Linear Association	1.425	1	.233
N of Valid Cases	301		

a. 1 cells (12.5%) have expected count less than 5. The minimum expected count is 4.79.

Davranış: İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım.

Yazma Hızı

ANOVA

Yazma Hizi

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	257.021	2	128.510	.447	.640
Within Groups	85340.376	297	287.341		
Total	85597.397	299			

Okuduğunu Görme

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	2.612[a]	2	.271
Likelihood Ratio	2.516	2	.284
Linear-by-Linear Association	.476	1	.490
N of Valid Cases	301		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 6.16.

Davranış: Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim.

Yazma Hızı	Okuduğunu Görme

ANOVA

Yazma Hizi

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1387.777	3	462.592	1.626	.183
Within Groups	84209.619	296	284.492		
Total	85597.397	299			

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	5.374[a]	3	.146
Likelihood Ratio	5.184	3	.159
Linear-by-Linear Association	3.689	1	.055
N of Valid Cases	301		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 11.29.

Davranış: İnternet ortamında gerektiği durumlarda özlük bilgilerimi (ad, soyad, doğum tarihi vb.) paylaşırım. (Riskli Davranış)

Yazma Hızı	Okuduğunu Görme

Test Statistics[a,b]

	Yazma Hizi
Chi-Square	4.111
df	3
Asymp. Sig.	.250

a. Kruskal Wallis Test

b. Grouping Variable: İnternet ortamında gerektiği durumlarda özlük bilgilerimi (ad, soyad , doğum tarihi vb.) paylaşırım

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	.654[a]	3	.884
Likelihood Ratio	.647	3	.886
Linear-by-Linear Association	.083	1	.773
N of Valid Cases	301		

a. 2 cells (25.0%) have expected count less than 5. The minimum expected count is 1.71.

Davranış: Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim.

Yazma Hızı

ANOVA

Yazma Hizi

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	518.901	3	172.967	.602	.614
Within Groups	85078.496	296	287.427		
Total	85597.397	299			

Okuduğunu Görme

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	2.878[a]	3	.411
Likelihood Ratio	3.148	3	.369
Linear-by-Linear Association	.295	1	.587
N of Valid Cases	301		

a. 2 cells (25.0%) have expected count less than 5. The minimum expected count is 2.40.

Davranış: Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım.

Yazma Hızı

ANOVA

Yazma Hizi

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	581.657	3	193.886	.675	.568
Within Groups	85015.740	296	287.215		
Total	85597.397	299			

Okuduğunu Görme

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	1.648[a]	3	.649
Likelihood Ratio	2.048	3	.562
Linear-by-Linear Association	.189	1	.664
N of Valid Cases	301		

a. 3 cells (37.5%) have expected count less than 5. The minimum expected count is .34.

Davranış: Kurumsal e-posta adresimi günlük işlerde de kullanırım. (Riskli Davranış)

Yazma Hızı

ANOVA

Yazma Hizi

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1333.065	3	444.355	1.561	.199
Within Groups	84264.332	296	284.677		
Total	85597.397	299			

Okuduğunu Görme

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	10.748[a]	3	.013
Likelihood Ratio	14.780	3	.002
Linear-by-Linear Association	6.907	1	.009
N of Valid Cases	301		

a. 2 cells (25.0%) have expected count less than 5. The minimum expected count is 3.76.

Davranış: Virüs temizleme, casus yazılım önleme vb. Programları kullanırım.

Yazma Hızı

ANOVA

Yazma Hizi

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	585.967	3	195.322	.680	.565
Within Groups	85011.430	296	287.201		
Total	85597.397	299			

Okuduğunu Görme

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	8.181[a]	3	.042
Likelihood Ratio	9.296	3	.026
Linear-by-Linear Association	.030	1	.862
N of Valid Cases	301		

a. 3 cells (37.5%) have expected count less than 5. The minimum expected count is 1.71.

Davranış: Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim.

Yazma Hızı

ANOVA

Yazma Hizi

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	1153.304	3	384.435	1.348	.259
Within Groups	84444.093	296	285.284		
Total	85597.397	299			

Okuduğunu Görme

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	6.629[a]	3	.085
Likelihood Ratio	7.111	3	.068
Linear-by-Linear Association	5.733	1	.017
N of Valid Cases	301		

a. 4 cells (50.0%) have expected count less than 5. The minimum expected count is .34.

Davranış: Birden fazla elektronik posta adresi kullanırım.

Yazma Hızı

ANOVA

Yazma Hizi

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	290.386	3	96.795	.336	.799
Within Groups	85307.011	296	288.199		
Total	85597.397	299			

Okuduğunu Görme

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	6.824[a]	3	.078
Likelihood Ratio	6.577	3	.087
Linear-by-Linear Association	1.424	1	.233
N of Valid Cases	301		

a. 0 cells (0.0%) have expected count less than 5. The minimum expected count is 11.63.

Davranış: Güvenlik duvarı, reklam önleyici vb. programlar kullanırım.

Yazma Hızı

ANOVA

Yazma Hizi

	Sum of Squares	df	Mean Square	F	Sig.
Between Groups	626.712	2	313.356	1.095	.336
Within Groups	84970.685	297	286.097		
Total	85597.397	299			

Okuduğunu Görme

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	2.541[a]	2	.281
Likelihood Ratio	2.569	2	.277
Linear-by-Linear Association	2.292	1	.130
N of Valid Cases	301		

a. 1 cells (16.7%) have expected count less than 5. The minimum expected count is 4.79.

EK 11. Bilgi Güvenliğine Dair Davranışların Sınıflandırılması için Hazırlanan Uzman Görüş Formu

Sayın …….

2. Sayfada verilen davranışlar kişi tarafından gerçekleştirilmediği zaman, karşılaşılabilecek durumun boyutunu sınıflandırmak için tabloda verilen girdilere göre davranışı etiketlemenizi rica ediyorum. Tablo altında basit bir örnekle açıklama yapılmıştır.

Type of Behavior	Loss	Criticality of the area	Prior Knowledge of attacker
Type 1	Low	Low	Low
Type 2	Low	Low	High
Type 3	Low	High	Low
Type 4	Low	High	High
Type 5	High	Low	Low
Type 6	High	Low	High
Type 7	High	High	Low
Type 8	High	High	High

Loss: Davranış olumlu şekilde gösterilmediği zaman yaşanabilecek kaybın boyutu.

Criticality: Davranış olumlu şekilde gösterilmediği zaman etkilenecek sistemin kritiklik bouyutu.

Prior Knowledge of attacker: Davranış sonucu kendi başına zarara uğratacak değil ancak zarara uğratacak bir durum için dayanak oluşturabilecek boyut.

Örnek: (Sadece örnek olarak verilmiştir. Farklı görüşler olabilir)

Korumacı davranış = “Bilgisayarım şifre ile açılır”

Loss = high

Criticality of the area = high => TYPE 8

Prior Knowledge of attacker = high

* Örneğin “**Kurumsal e-posta adresimi günlük işlerde de kullanırım”** davranışı olumsuz bir davranıştır. “**Birden fazla elektronik posta adresi kullanırım”** olumlu bir davranıştır. Sınıflama yaparken davranışı kötü etkiye sebebiyet verecek şekliyle ele alınız!

SN	DAVRANIŞ	TÜR
1	Birden fazla elektronik posta adresi kullanırım.	
2	Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim.	
3	Güvenlik duvarı, reklam önleyici vb. programlar kullanırım.	
4	Virus temizleme, casus yazılım önleme vb. programları kullanırım.	
5	İçerik filtreleme programları kullanırım.	
6	e-posta filtreleme yazılımları kullanırım.	
7	Izleme yazılımları kullanarak internet üzerinde yapılan etkinlikler hakkında bilgi sahibi olurum.	
8	Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim.	
9	Herkesin kullanımına açık bir bilgisayardan ayrılmadan önce geçici internet dosyalarını ve web gezinti geçmişlerini silerim.	
10	Dosyalarımı şifrelerim.	
11	İnternet üzerindeki hesaplarımda kolay tahmin edilemeycek şekilde karmaşık ve uzun şifreler kullanırım.	
12	Elektronik/mobil imza kullanırım	
13	İnternet sitelerine girerken genellikle sık kullanılanlar listesini kullanırım.	
14	Bilgisayarım şifre ile açılır.	
15	Bilgisayarımda otomatik kullan özelliğini kapatırım.	
16	Girdiğim sitelerin SSL sertfikası olup olmadığına dikkat ederim.	
17	Parolalarımı sık sık değiştiririm.	
18	Kablosuz modem şifremi değiştiririm.	
19	Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım.	
20	Kullandığım programların güncellemelerini düzenli olarak yaparım.	
21	Kurumsal e-posta adresimi günlük işlerde de kullanırım.	
22	İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (Gsm no, eposta vb.) paylaşırım.	
23	İnternet ortamında gerektiği durumlarda özlük bilgilerimi (ad,soyad , doğum tarihi vb.) paylaşırım	

EK 12. Kural Setleri

Davranış: Birden fazla elektronik posta adresi kullanırım.

```
Disa_donukluk <= 20 [ Mode: soyler-yapar ]
        RDP <= 19 [ Mode: soylemez-yapar ]
                Cinsiyet = Kadın [ Mode: soylemez-yapar ]
                        KDP <= 30 [ Mode: soyler-yapar ] => soyler-yapar
                KDP > 30 [ Mode: soylemez-yapar ] => soylemez-yapar
                Cinsiyet = Erkek [ Mode: soyler-yapar ] => soyler-yapar
        RDP > 19 [ Mode: soyler-yapar ]
                RDP <= 29 [ Mode: soyler-yapmaz ]
                        Nevrotizm <= 14 [ Mode: soyler-yapar ] => soyler-yapar
                        Nevrotizm > 14 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                RDP > 29 [ Mode: soyler-yapar ]
                        Eğitim Düzeyi in [ "Doktora Mezunu" "Lise Mezunu" "Önlisans Mezunu" ] [ Mode: soyler-yapar ] => soyler-yapar
                        Eğitim Düzeyi in [ "Lisans Mezunu" ] [ Mode: soyler-yapar ]
                                yazma_hizi <= 30 [ Mode: soyler-yapar ] => soyler-yapar
                                yazma_hizi > 30 [ Mode: soyler-yapmaz ]
                                        Ozdenetim <= 25 [ Mode: soyler-yapar ] => soyler-yapar
                                        Ozdenetim > 25 [ Mode: soyler-yapmaz ]
                                                Nevrotizm <= 27 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                Nevrotizm > 27 [ Mode: soyler-yapar ] => soyler-yapar
                        Eğitim Düzeyi in [ "Yüksek Lisans Mezunu" ] [ Mode: soyler-yapar ]
                                Nevrotizm <= 17 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                Nevrotizm > 17 [ Mode: soyler-yapar ] => soyler-yapar
                        Eğitim Düzeyi in [ "İlköğretim Mezunu" ] [ Mode: soyler-yapar ] => soyler-yapar
Disa_donukluk > 20 [ Mode: soylemez-yapar ]
        Uyumluluk <= 40 [ Mode: soylemez-yapar ]
                KDP <= 3 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                KDP > 3 [ Mode: soylemez-yapar ]
                        RDP <= 36 [ Mode: soylemez-yapar ]
                                Eğitim Düzeyi = Doktora Mezunu [ Mode: soyler-yapar ]
                                        SMP <= 5 [ Mode: soyler-yapar ] => soyler-yapar
                                        SMP > 5 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                Eğitim Düzeyi = Lisans Mezunu [ Mode: soylemez-yapmaz ]
                                        TAP <= 41 [ Mode: soylemez-yapar ]
```

```
                Uyumluluk <= 35 [ Mode: soyler-yapar ] => soyler-yapar
                Uyumluluk > 35 [ Mode: soylemez-yapar ] => soylemez-yapar
        TAP > 41 [ Mode: soylemez-yapmaz ]
                SMP <= 16 [ Mode: soylemez-yapmaz ]
                        KDP <= 7 [ Mode: soylemez-yapar ] => soylemez-yapar
                        KDP > 7 [ Mode: soylemez-yapmaz ]
                                Cinsiyet = Kadın [ Mode: soylemez-yapmaz ]
                                        Gelisime_aciklik <= 29 [ Mode: soyler-yapar ]
                                                SMP <= 3 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                SMP > 3 [ Mode: soyler-yapar ] => soyler-yapar
                                        Gelisime_aciklik > 29 [ Mode: soylemez-yapmaz ]
                                                Disa_donukluk <= 32 [ Mode: soylemez-yapmaz ]
                                                        KDP <= 64 [ Mode: soylemez-yapmaz ]
                                                                TAP <= 74 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                                                TAP > 74 [ Mode: soyler-yapar ] => soyler-yapar
                                                        KDP > 64 [ Mode: soyler-yapar ] => soyler-yapar
                                                Disa_donukluk > 32 [ Mode: soylemez-yapmaz ]
                                                        okuma-gorme = olumsuz [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                                        okuma-gorme = olumlu [ Mode: soylemez-yapar ] => soylemez-yapar
                                Cinsiyet = Erkek [ Mode: soyler-yapar ]
                                        okuma-gorme = olumsuz [ Mode: soylemez-yapmaz ]
                                                Yas_aralik in [ "Bebek Patlaması" "X Kuşağı" ] [ Mode: soyler-yapar ] => soyler-yapar
                                                Yas_aralik in [ "Y Kuşağı" "Z Kuşağı" ] [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                        okuma-gorme = olumlu [ Mode: soyler-yapar ] => soyler-yapar
                SMP > 16 [ Mode: soylemez-yapar ] => soylemez-yapar
Eğitim Düzeyi = Lise Mezunu [ Mode: soylemez-yapar ]
        Yas_aralik in [ "Bebek Patlaması" ] [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
        Yas_aralik in [ "X Kuşağı" "Y Kuşağı" "Z Kuşağı" ] [ Mode: soylemez-yapar ]
                yazma_hizi <= 46 [ Mode: soylemez-yapar ]
                        Nevrotizm <= 26 [ Mode: soylemez-yapar ]
                                TAP <= 67 [ Mode: soylemez-yapar ]
                                        Disa_donukluk <= 22 [ Mode: soyler-yapar ] => soyler-yapar
                                        Disa_donukluk > 22 [ Mode: soylemez-yapar ]
                                                Gelisime_aciklik <= 23 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                Gelisime_aciklik > 23 [ Mode: soylemez-yapar ]
                                                        Cinsiyet = Kadın [ Mode: soylemez-yapar ] => soylemez-yapar
                                                        Cinsiyet = Erkek [ Mode: soylemez-yapar ]
```

```
                                                                RDP <= 26 [ Mode: soyler-yapar ]
                                                                        Uyumluluk <= 37 [ Mode: soyler-yapar ] => soyler-yapar
                                                                        Uyumluluk > 37 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                                RDP > 26 [ Mode: soylemez-yapar ] => soylemez-yapar
                                                        TAP > 67 [ Mode: soylemez-yapar ]
                                                                yazma_hizi <= 22 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                                                yazma_hizi > 22 [ Mode: soylemez-yapar ] => soylemez-yapar
                                                Nevrotizm > 26 [ Mode: soyler-yapar ]
                                                        internet_saat in [ "1-2" ] [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                        internet_saat in [ "11+" "6-10" ] [ Mode: soyler-yapar ] => soyler-yapar
                                                        internet_saat in [ "3-5" ] [ Mode: soyler-yapar ] => soyler-yapar
                                        yazma_hizi > 46 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                Eğitim Düzeyi = Yüksek Lisans Mezunu [ Mode: soylemez-yapmaz ]
                                        SMP <= 16 [ Mode: soyler-yapmaz ]
                                                Gelisime_aciklik <= 39 [ Mode: soyler-yapmaz ]
                                                        SMP <= 2 [ Mode: soyler-yapar ] => soyler-yapar
                                                        SMP > 2 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                Gelisime_aciklik > 39 [ Mode: soylemez-yapar ] => soylemez-yapar
                                        SMP > 16 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                Eğitim Düzeyi = Önlisans Mezunu [ Mode: soylemez-yapar ]
                                        Nevrotizm <= 13 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                        Nevrotizm > 13 [ Mode: soylemez-yapar ]
                                                KDP <= 42 [ Mode: soylemez-yapar ] => soylemez-yapar
                                                KDP > 42 [ Mode: soyler-yapmaz ]
                                                        Disa_donukluk <= 28 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                        Disa_donukluk > 28 [ Mode: soyler-yapar ] => soyler-yapar
                                Eğitim Düzeyi = İlköğretim Mezunu [ Mode: soylemez-yapar ]
                                        Cinsiyet = Kadın [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                        Cinsiyet = Erkek [ Mode: soylemez-yapar ] => soylemez-yapar
RDP > 36 [ Mode: soyler-yapar ]
        KDP <= 22 [ Mode: soylemez-yapmaz ]
                KDP <= 20 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                KDP > 20 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
        KDP > 22 [ Mode: soyler-yapar ]
                Ozdenetim <= 42 [ Mode: soyler-yapar ]
                        Ozdenetim <= 36 [ Mode: soylemez-yapar ]
                                Uyumluluk <= 37 [ Mode: soylemez-yapar ]
```

SMP <= 7 [Mode: soylemez-yapar]
Eğitim Düzeyi in ["Doktora Mezunu" "Lise Mezunu"] [Mode: soyler-yapar] => soyler-yapar
Eğitim Düzeyi in ["Lisans Mezunu"] [Mode: soylemez-yapar]
TAP <= 52 [Mode: soyler-yapar]
Nevrotizm <= 20 [Mode: soyler-yapar] => soyler-yapar
Nevrotizm > 20 [Mode: soyler-yapmaz] => soyler-yapmaz
TAP > 52 [Mode: soylemez-yapar]
internet_saat in ["1-2" "11+"] [Mode: soylemez-yapar] => soylemez-yapar
internet_saat in ["3-5" "6-10"] [Mode: soyler-yapmaz] => soyler-yapmaz
Eğitim Düzeyi in ["Yüksek Lisans Mezunu"] [Mode: soylemez-yapar]
Nevrotizm <= 13 [Mode: soylemez-yapar] => soylemez-yapar
Nevrotizm > 13 [Mode: soyler-yapmaz] => soyler-yapmaz
Eğitim Düzeyi in ["Önlisans Mezunu"] [Mode: soyler-yapmaz]
Disa_donukluk <= 24 [Mode: soyler-yapmaz] => soyler-yapmaz
Disa_donukluk > 24 [Mode: soyler-yapar] => soyler-yapar
Eğitim Düzeyi in ["İlköğretim Mezunu"] [Mode: soylemez-yapar] => soylemez-yapar
SMP > 7 [Mode: soylemez-yapar]
SMP <= 16 [Mode: soylemez-yapar] => soylemez-yapar
SMP > 16 [Mode: soyler-yapar] => soyler-yapar
Uyumluluk > 37 [Mode: soyler-yapmaz] => soyler-yapmaz
Ozdenetim > 36 [Mode: soyler-yapar]
Cinsiyet = Kadın [Mode: soyler-yapar]
Nevrotizm <= 26 [Mode: soyler-yapar] => soyler-yapar
Nevrotizm > 26 [Mode: soyler-yapar]
Disa_donukluk <= 26 [Mode: soyler-yapar] => soyler-yapar
Disa_donukluk > 26 [Mode: soyler-yapmaz] => soyler-yapmaz
Cinsiyet = Erkek [Mode: soyler-yapmaz]
Internet_kullanim = 11-15 [Mode: soyler-yapmaz] => soyler-yapmaz
Internet_kullanim = 15+ [Mode: soyler-yapmaz]
Ozdenetim <= 38 [Mode: soyler-yapar] => soyler-yapar
Ozdenetim > 38 [Mode: soyler-yapmaz] => soyler-yapmaz
Internet_kullanim = 3-6 [Mode: soyler-yapmaz] => soyler-yapmaz
Internet_kullanim = 7-10 [Mode: soyler-yapar] => soyler-yapar
Ozdenetim > 42 [Mode: soyler-yapar]
Disa_donukluk <= 35 [Mode: soyler-yapar]
SMP <= 12 [Mode: soyler-yapar] => soyler-yapar
SMP > 12 [Mode: soylemez-yapar] => soylemez-yapar

```
                                        Disa_donukluk > 35 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
Uyumluluk > 40 [ Mode: soylemez-yapmaz ]
        Eğitim Düzeyi in [ "Doktora Mezunu" "İlköğretim Mezunu" ] [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
        Eğitim Düzeyi in [ "Lisans Mezunu" ] [ Mode: soyler-yapar ]
                Ozdenetim <= 43 [ Mode: soyler-yapar ]
                        Internet_kullanim in [ "11-15" ] [ Mode: soyler-yapmaz ] => soyler-yapmaz
                        Internet_kullanim in [ "15+" "3-6" ] [ Mode: soyler-yapar ] => soyler-yapar
                        Internet_kullanim in [ "7-10" ] [ Mode: soyler-yapar ]
                                yazma_hizi <= 29 [ Mode: soyler-yapar ] => soyler-yapar
                                yazma_hizi > 29 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                Ozdenetim > 43 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
        Eğitim Düzeyi in [ "Lise Mezunu" "Önlisans Mezunu" ] [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
        Eğitim Düzeyi in [ "Yüksek Lisans Mezunu" ] [ Mode: soyler-yapar ] => soyler-yapar
```

Davranış: İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım.

```
KDP <= 19 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
KDP > 19 [ Mode: soyler-yapmaz ]
        Uyumluluk <= 42 [ Mode: soyler-yapmaz ]
                yazma_hizi <= 12 [ Mode: soylemez-yapmaz ]
                        Uyumluluk <= 32 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                        Uyumluluk > 32 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                yazma_hizi > 12 [ Mode: soyler-yapmaz ]
                        Gelisime_aciklik <= 32 [ Mode: soyler-yapmaz ]
                                Cinsiyet = Kadın [ Mode: soyler-yapmaz ]
                                        RDP <= 39 [ Mode: soyler-yapmaz ]
                                                Uyumluluk <= 25 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                                Uyumluluk > 25 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                        RDP > 39 [ Mode: soylemez-yapmaz ]
                                                Eğitim Düzeyi in [ "Doktora Mezunu" ] [ Mode: soyler-yapar ] => soyler-yapar
                                                Eğitim Düzeyi in [ "Lisans Mezunu" ] [ Mode: soylemez-yapmaz ]
                                                        Ozdenetim <= 20 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                        Ozdenetim > 20 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                                Eğitim Düzeyi in [ "Lise Mezunu" "Yüksek Lisans Mezunu" ] [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                Eğitim Düzeyi in [ "Önlisans Mezunu" ] [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                                Eğitim Düzeyi in [ "İlköğretim Mezunu" ] [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                Cinsiyet = Erkek [ Mode: soyler-yapmaz ]
                                        Ozdenetim <= 31 [ Mode: soyler-yapmaz ]
                                                Ozdenetim <= 30 [ Mode: soyler-yapmaz ]
                                                        TAP <= 36 [ Mode: soyler-yapar ] => soyler-yapar
                                                        TAP > 36 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                Ozdenetim > 30 [ Mode: soyler-yapar ] => soyler-yapar
                                        Ozdenetim > 31 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                        Gelisime_aciklik > 32 [ Mode: soyler-yapmaz ] => soyler-yapmaz
        Uyumluluk > 42 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
```

Davranış: Güvenlik duvarı, reklam önleyici vb. programlar kullanırım.

```
KDP <= 34 [ Mode: soylemez-yapmaz ]
        KDP <= 7 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
```

KDP > 7 [Mode: soylemez-yapmaz]
yazma_hizi <= 49 [Mode: soylemez-yapmaz]
Nevrotizm <= 11 [Mode: soyler-yapmaz] => soyler-yapmaz
Nevrotizm > 11 [Mode: soylemez-yapmaz]
Ozdenetim <= 30 [Mode: soylemez-yapmaz]
yazma_hizi <= 27 [Mode: soyler-yapmaz] => soyler-yapmaz
yazma_hizi > 27 [Mode: soylemez-yapmaz]
TAP <= 53 [Mode: soylemez-yapmaz]
Ozdenetim <= 29 [Mode: soylemez-yapmaz]
TAP <= 32 [Mode: soyler-yapmaz] => soyler-yapmaz
TAP > 32 [Mode: soylemez-yapmaz] => soylemez-yapmaz
Ozdenetim > 29 [Mode: soyler-yapmaz] => soyler-yapmaz
TAP > 53 [Mode: soyler-yapmaz] => soyler-yapmaz
Ozdenetim > 30 [Mode: soylemez-yapmaz]
RDP <= 11 [Mode: soyler-yapmaz] => soyler-yapmaz
RDP > 11 [Mode: soylemez-yapmaz]
Ozdenetim <= 33 [Mode: soylemez-yapmaz] => soylemez-yapmaz
Ozdenetim > 33 [Mode: soylemez-yapmaz]
Disa_donukluk <= 32 [Mode: soylemez-yapmaz]
Ozdenetim <= 34 [Mode: soyler-yapmaz] => soyler-yapmaz
Ozdenetim > 34 [Mode: soylemez-yapmaz]
Gelisime_aciklik <= 34 [Mode: soylemez-yapmaz]
SMP <= 3 [Mode: soylemez-yapmaz]
TAP <= 39 [Mode: soyler-yapmaz] => soyler-yapmaz
TAP > 39 [Mode: soylemez-yapmaz] => soylemez-yapmaz
SMP > 3 [Mode: soyler-yapmaz] => soyler-yapmaz
Gelisime_aciklik > 34 [Mode: soylemez-yapmaz]
yazma_hizi <= 33 [Mode: soylemez-yapmaz] => soylemez-yapmaz
yazma_hizi > 33 [Mode: soylemez-yapmaz]
okuma-gorme = olumsuz [Mode: soylemez-yapmaz] => soylemez-yapmaz
okuma-gorme = olumlu [Mode: soyler-yapmaz] => soyler-yapmaz
Disa_donukluk > 32 [Mode: soyler-yapmaz] => soyler-yapmaz
yazma_hizi > 49 [Mode: soyler-yapmaz] => soyler-yapmaz
KDP > 34 [Mode: soyler-yapmaz]
Eğitim Düzeyi = Doktora Mezunu [Mode: soyler-yapmaz]
Nevrotizm <= 28 [Mode: soyler-yapmaz] => soyler-yapmaz
Nevrotizm > 28 [Mode: soylemez-yapmaz] => soylemez-yapmaz

```
Eğitim Düzeyi = Lisans Mezunu [ Mode: soyler-yapmaz ]
        Yas_aralik in [ "Bebek Patlaması" ] [ Mode: soylemez-yapmaz ]
                KDP <= 47 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                KDP > 47 [ Mode: soyler-yapmaz ] => soyler-yapmaz
        Yas_aralik in [ "X Kuşağı" "Y Kuşağı" "Z Kuşağı" ] [ Mode: soyler-yapmaz ]
                TAP <= 32 [ Mode: soylemez-yapmaz ]
                        SMP <= 5 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                        SMP > 5 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                TAP > 32 [ Mode: soyler-yapmaz ] => soyler-yapmaz
Eğitim Düzeyi = Lise Mezunu [ Mode: soylemez-yapmaz ]
        Yas_aralik in [ "Bebek Patlaması" "X Kuşağı" "Y Kuşağı" ] [ Mode: soylemez-yapmaz ]
                KDP <= 60 [ Mode: soylemez-yapmaz ]
                        yazma_hizi <= 20 [ Mode: soyler-yapmaz ]
                                okuma-gorme = olumsuz [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                okuma-gorme = olumlu [ Mode: soyler-yapar ] => soyler-yapar
                        yazma_hizi > 20 [ Mode: soylemez-yapmaz ]
                                Gelisime_aciklik <= 27 [ Mode: soyler-yapar ] => soyler-yapar
                                Gelisime_aciklik > 27 [ Mode: soylemez-yapmaz ]
                                        Disa_donukluk <= 31 [ Mode: soylemez-yapmaz ]
                                                SMP <= 1 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                SMP > 1 [ Mode: soylemez-yapmaz ]
                                                        SMP <= 9 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                                        SMP > 9 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                        Disa_donukluk > 31 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                KDP > 60 [ Mode: soyler-yapmaz ] => soyler-yapmaz
        Yas_aralik in [ "Z Kuşağı" ] [ Mode: soyler-yapmaz ] => soyler-yapmaz
Eğitim Düzeyi = Yüksek Lisans Mezunu [ Mode: soyler-yapmaz ] => soyler-yapmaz
Eğitim Düzeyi = Önlisans Mezunu [ Mode: soyler-yapmaz ]
        okuma-gorme = olumsuz [ Mode: soyler-yapmaz ]
                SMP <= 3 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                SMP > 3 [ Mode: soyler-yapar ] => soyler-yapar
        okuma-gorme = olumlu [ Mode: soyler-yapmaz ] => soyler-yapmaz
Eğitim Düzeyi = İlköğretim Mezunu [ Mode: soylemez-yapmaz ]
        yazma_hizi <= 27 [ Mode: soyler-yapmaz ] => soyler-yapmaz
        yazma_hizi > 27 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
```

Davranış: Virüs temizleme, casus yazılım önleme vb. programları kullanırım.

```
KDP <= 52 [ Mode: soyler-yapmaz ]
        Disa_donukluk <= 30 [ Mode: soyler-yapmaz ]
                SMP <= 0 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                SMP > 0 [ Mode: soylemez-yapmaz ]
                        Uyumluluk <= 40 [ Mode: soylemez-yapmaz ]
                                RDP <= 27 [ Mode: soylemez-yapmaz ]
                                        Disa_donukluk <= 18 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                        Disa_donukluk > 18 [ Mode: soylemez-yapmaz ]
                                                yazma_hizi <= 46 [ Mode: soylemez-yapmaz ]
                                                        KDP <= 38 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                                        KDP > 38 [ Mode: soylemez-yapmaz ]
                                                                Uyumluluk <= 36 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                                Uyumluluk > 36 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                                yazma_hizi > 46 [ Mode: soyler-yapar ] => soyler-yapar
                                RDP > 27 [ Mode: soyler-yapmaz ]
                                        Uyumluluk <= 32 [ Mode: soylemez-yapmaz ]
                                                Gelisime_aciklik <= 19 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                Gelisime_aciklik > 19 [ Mode: soylemez-yapmaz ]
                                                        TAP <= 61 [ Mode: soylemez-yapmaz ]
                                                                RDP <= 31 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                                RDP > 31 [ Mode: soylemez-yapmaz ]
                                                                        okuma-gorme = olumsuz [ Mode: soylemez-yapmaz ]
                                                                                RDP <= 33 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                                                                RDP > 33 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                                        okuma-gorme = olumlu [ Mode: soylemez-yapmaz ]
                                                                                SMP <= 3 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                                                SMP > 3 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                                        TAP > 61 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                        Uyumluluk > 32 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                        Uyumluluk > 40 [ Mode: soyler-yapmaz ] => soyler-yapmaz
        Disa_donukluk > 30 [ Mode: soyler-yapmaz ] => soyler-yapmaz
KDP > 52 [ Mode: soyler-yapmaz ] => soyler-yapmaz
```

Davranış: Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim.

```
KDP <= 32 [ Mode: soyler-yapmaz ]
        internet_saat = 1-2 [ Mode: soyler-yapmaz ]
                Yas_aralik in [ "Bebek Patlaması" "X Kuşağı" "Y Kuşağı" ] [ Mode: soylemez-yapmaz ]
                        RDP <= 20 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                        RDP > 20 [ Mode: soyler-yapmaz ]
                                Cinsiyet = Kadın [ Mode: soyler-yapmaz ]
                                        Disa_donukluk <= 27 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                        Disa_donukluk > 27 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                Cinsiyet = Erkek [ Mode: soyler-yapmaz ]
                                        Ozdenetim <= 35 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                        Ozdenetim > 35 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                Yas_aralik in [ "Z Kuşağı" ] [ Mode: soyler-yapmaz ] => soyler-yapmaz
        internet_saat = 11+ [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
        internet_saat = 3-5 [ Mode: soyler-yapmaz ]
                Cinsiyet = Kadın [ Mode: soyler-yapmaz ]
                        Internet_kullanim in [ "11-15" ] [ Mode: soyler-yapmaz ]
                                Disa_donukluk <= 31 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                Disa_donukluk > 31 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                        Internet_kullanim in [ "15+" "3-6" ] [ Mode: soyler-yapmaz ] => soyler-yapmaz
                        Internet_kullanim in [ "7-10" ] [ Mode: soyler-yapmaz ]
                                SMP <= 8 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                SMP > 8 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                Cinsiyet = Erkek [ Mode: soyler-yapmaz ] => soyler-yapmaz
        internet_saat = 6-10 [ Mode: soylemez-yapmaz ]
                Yas_aralik in [ "Bebek Patlaması" "X Kuşağı" "Y Kuşağı" ] [ Mode: soylemez-yapmaz ]
                        KDP <= 26 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                        KDP > 26 [ Mode: soylemez-yapmaz ]
                                Disa_donukluk <= 12 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                Disa_donukluk > 12 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                Yas_aralik in [ "Z Kuşağı" ] [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
KDP > 32 [ Mode: soyler-yapmaz ]
        KDP <= 67 [ Mode: soyler-yapmaz ]
                Disa_donukluk <= 24 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                Disa_donukluk > 24 [ Mode: soyler-yapmaz ]
                        yazma_hizi <= 42 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                        yazma_hizi > 42 [ Mode: soylemez-yapmaz ]
                                Disa_donukluk <= 34 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
```

Disa_donukluk > 34 [Mode: soyler-yapmaz] => soyler-yapmaz
KDP > 67 [Mode: soyler-yapmaz] => soyler-yapmaz

Davranış: Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim.

```
Gelisime_aciklik <= 19 [ Mode: soyler-yapmaz ]
        KDP <= 34 [ Mode: soyler-yapmaz ]
                Nevrotizm <= 25 [ Mode: soyler-yapmaz ]
                        Disa_donukluk <= 21 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                        Disa_donukluk > 21 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                Nevrotizm > 25 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
        KDP > 34 [ Mode: soyler-yapmaz ] => soyler-yapmaz
Gelisime_aciklik > 19 [ Mode: soyler-yapmaz ]
        KDP <= 28 [ Mode: soyler-yapmaz ]
                KDP <= 7 [ Mode: soylemez-yapar ] => soylemez-yapar
                KDP > 7 [ Mode: soyler-yapmaz ] => soyler-yapmaz
        KDP > 28 [ Mode: soyler-yapmaz ]
                Disa_donukluk <= 13 [ Mode: soyler-yapmaz ]
                        yazma_hizi <= 20 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                        yazma_hizi > 20 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                Disa_donukluk > 13 [ Mode: soyler-yapmaz ]
                        Nevrotizm <= 22 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                        Nevrotizm > 22 [ Mode: soyler-yapmaz ]
                                Cinsiyet = Kadın [ Mode: soyler-yapmaz ]
                                        Uyumluluk <= 38 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                        Uyumluluk > 38 [ Mode: soyler-yapar ] => soyler-yapar
                                Cinsiyet = Erkek [ Mode: soyler-yapmaz ]
                                        RDP <= 28 [ Mode: soyler-yapar ] => soyler-yapar
                                        RDP > 28 [ Mode: soyler-yapmaz ]
                                                yazma_hizi <= 23 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                                yazma_hizi > 23 [ Mode: soyler-yapmaz ] => soyler-yapmaz
```

Davranış: Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim.

```
Nevrotizm <= 32 [ Mode: soyler-yapar ]
        KDP <= 47 [ Mode: soyler-yapmaz ]
                Ozdenetim <= 42 [ Mode: soyler-yapmaz ]
                        KDP <= 23 [ Mode: soylemez-yapmaz ]
                                Cinsiyet = Kadın [ Mode: soylemez-yapar ]
                                        okuma-gorme = olumsuz [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                        okuma-gorme = olumlu [ Mode: soylemez-yapar ] => soylemez-yapar
                                Cinsiyet = Erkek [ Mode: soylemez-yapmaz ]
                                        Ozdenetim <= 29 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                        Ozdenetim > 29 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                        KDP > 23 [ Mode: soyler-yapar ]
                                RDP <= 27 [ Mode: soyler-yapmaz ]
                                        Internet_kullanim = 11-15 [ Mode: soyler-yapmaz ]
                                                yazma_hizi <= 35 [ Mode: soyler-yapar ] => soyler-yapar
                                                yazma_hizi > 35 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                        Internet_kullanim = 15+ [ Mode: soyler-yapmaz ]
                                                Ozdenetim <= 38 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                Ozdenetim > 38 [ Mode: soyler-yapar ] => soyler-yapar
                                        Internet_kullanim = 3-6 [ Mode: soylemez-yapmaz ]
                                                Gelisime_aciklik <= 20 [ Mode: soyler-yapar ] => soyler-yapar
                                                Gelisime_aciklik > 20 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                        Internet_kullanim = 7-10 [ Mode: soyler-yapmaz ]
                                                SMP <= 4 [ Mode: soyler-yapmaz ]
                                                        Ozdenetim <= 34 [ Mode: soyler-yapar ] => soyler-yapar
                                                        Ozdenetim > 34 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                SMP > 4 [ Mode: soyler-yapar ] => soyler-yapar
                                RDP > 27 [ Mode: soyler-yapar ]
                                        Eğitim Düzeyi = Doktora Mezunu [ Mode: soyler-yapmaz ]
                                                Gelisime_aciklik <= 25 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                Gelisime_aciklik > 25 [ Mode: soylemez-yapar ] => soylemez-yapar
                                        Eğitim Düzeyi = Lisans Mezunu [ Mode: soyler-yapar ]
                                                internet_saat = 1-2 [ Mode: soyler-yapar ]
                                                        Gelisime_aciklik <= 19 [ Mode: soylemez-yapar ] => soylemez-yapar
                                                        Gelisime_aciklik > 19 [ Mode: soyler-yapar ]
```

```
                    Internet_kullanim = 11-15 [ Mode: soyler-yapar ]
                        yazma_hizi <= 24 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                        yazma_hizi > 24 [ Mode: soyler-yapar ] => soyler-yapar
                    Internet_kullanim = 15+ [ Mode: soyler-yapar ]
                        Cinsiyet = Kadın [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                        Cinsiyet = Erkek [ Mode: soyler-yapar ] => soyler-yapar
                    Internet_kullanim = 3-6 [ Mode: soyler-yapar ] => soyler-yapar
                    Internet_kullanim = 7-10 [ Mode: soyler-yapmaz ]
                        Yas_aralik in [ "Bebek Patlaması" "X Kuşağı" "Y Kuşağı" ] [ Mode: soyler-yapmaz ] => soyler-yapmaz
                        Yas_aralik in [ "Z Kuşağı" ] [ Mode: soyler-yapar ] => soyler-yapar
            internet_saat = 11+ [ Mode: soyler-yapmaz ]
                yazma_hizi <= 21 [ Mode: soylemez-yapar ] => soylemez-yapar
                yazma_hizi > 21 [ Mode: soyler-yapmaz ] => soyler-yapmaz
            internet_saat = 3-5 [ Mode: soyler-yapar ]
                Gelisime_aciklik <= 30 [ Mode: soyler-yapar ]
                    SMP <= 4 [ Mode: soyler-yapar ] => soyler-yapar
                    SMP > 4 [ Mode: soylemez-yapmaz ]
                        Ozdenetim <= 29 [ Mode: soyler-yapar ]
                            Nevrotizm <= 26 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                            Nevrotizm > 26 [ Mode: soyler-yapar ] => soyler-yapar
                        Ozdenetim > 29 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                Gelisime_aciklik > 30 [ Mode: soyler-yapmaz ]
                    okuma-gorme = olumsuz [ Mode: soylemez-yapar ] => soylemez-yapar
                    okuma-gorme = olumlu [ Mode: soyler-yapmaz ] => soyler-yapmaz
            internet_saat = 6-10 [ Mode: soylemez-yapmaz ]
                SMP <= 3 [ Mode: soyler-yapar ]
                    Ozdenetim <= 34 [ Mode: soyler-yapar ] => soyler-yapar
                    Ozdenetim > 34 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                SMP > 3 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
Eğitim Düzeyi = Lise Mezunu [ Mode: soyler-yapar ]
        Nevrotizm <= 25 [ Mode: soylemez-yapar ]
            Yas_aralik in [ "Bebek Patlaması" "X Kuşağı" "Y Kuşağı" ] [ Mode: soylemez-yapar ] => soylemez-yapar
            Yas_aralik in [ "Z Kuşağı" ] [ Mode: soyler-yapar ]
                Cinsiyet = Kadın [ Mode: soyler-yapmaz ] => soyler-yapmaz
                Cinsiyet = Erkek [ Mode: soyler-yapar ] => soyler-yapar
        Nevrotizm > 25 [ Mode: soyler-yapar ] => soyler-yapar
Eğitim Düzeyi = Yüksek Lisans Mezunu [ Mode: soyler-yapar ]
```

```
                                        internet_saat = 1-2 [ Mode: soyler-yapar ]
                                                okuma-gorme = olumsuz [ Mode: soylemez-yapar ] => soylemez-yapar
                                                okuma-gorme = olumlu [ Mode: soyler-yapar ] => soyler-yapar
                                        internet_saat = 11+ [ Mode: soylemez-yapar ] => soylemez-yapar
                                        internet_saat = 3-5 [ Mode: soyler-yapar ]
                                                TAP <= 40 [ Mode: soylemez-yapar ] => soylemez-yapar
                                                TAP > 40 [ Mode: soyler-yapar ]
                                                        Yas_aralik in [ "Bebek Patlaması" "X Kuşağı" ] [ Mode: soyler-yapar ] => soyler-yapar
                                                        Yas_aralik in [ "Y Kuşağı" "Z Kuşağı" ] [ Mode: soylemez-yapmaz ]
                                                                RDP <= 40 [ Mode: soyler-yapar ] => soyler-yapar
                                                                RDP > 40 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                        internet_saat = 6-10 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                Eğitim Düzeyi = Önlisans Mezunu [ Mode: soyler-yapmaz ]
                                        Uyumluluk <= 37 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                        Uyumluluk > 37 [ Mode: soylemez-yapar ] => soylemez-yapar
                                Eğitim Düzeyi = İlköğretim Mezunu [ Mode: soyler-yapar ] => soyler-yapar
        Ozdenetim > 42 [ Mode: soylemez-yapar ] => soylemez-yapar
KDP > 47 [ Mode: soyler-yapar ]
        SMP <= 15 [ Mode: soyler-yapar ]
                Disa_donukluk <= 37 [ Mode: soyler-yapar ]
                        Nevrotizm <= 13 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                        Nevrotizm > 13 [ Mode: soyler-yapar ]
                                Uyumluluk <= 30 [ Mode: soyler-yapar ] => soyler-yapar
                                Uyumluluk > 30 [ Mode: soyler-yapar ]
                                        Eğitim Düzeyi = Doktora Mezunu [ Mode: soyler-yapar ]
                                                SMP <= 8 [ Mode: soyler-yapar ] => soyler-yapar
                                                SMP > 8 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                        Eğitim Düzeyi = Lisans Mezunu [ Mode: soyler-yapar ]
                                                Yas_aralik in [ "Bebek Patlaması" "X Kuşağı" "Y Kuşağı" ] [ Mode: soyler-yapar ]
                                                        Gelisime_aciklik <= 34 [ Mode: soyler-yapar ] => soyler-yapar
                                                        Gelisime_aciklik > 34 [ Mode: soyler-yapmaz ]
                                                                Gelisime_aciklik <= 39 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                                Gelisime_aciklik > 39 [ Mode: soyler-yapar ]
                                                                        Ozdenetim <= 39 [ Mode: soyler-yapar ] => soyler-yapar
                                                                        Ozdenetim > 39 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                                Yas_aralik in [ "Z Kuşağı" ] [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                        Eğitim Düzeyi = Lise Mezunu [ Mode: soyler-yapar ]
```

```
                                        SMP <= 5 [ Mode: soyler-yapar ]
                                                TAP <= 59 [ Mode: soyler-yapar ] => soyler-yapar
                                                TAP > 59 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                        SMP > 5 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                Eğitim Düzeyi = Yüksek Lisans Mezunu [ Mode: soyler-yapar ]
                                        RDP <= 27 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                        RDP > 27 [ Mode: soyler-yapar ] => soyler-yapar
                                Eğitim Düzeyi = Önlisans Mezunu [ Mode: soyler-yapar ]
                                        Internet_kullanim in [ "11-15" "15+" ] [ Mode: soyler-yapmaz ] => soyler-yapmaz
                                        Internet_kullanim in [ "3-6" ] [ Mode: soyler-yapar ] => soyler-yapar
                                        Internet_kullanim in [ "7-10" ] [ Mode: soyler-yapar ] => soyler-yapar
                                Eğitim Düzeyi = İlköğretim Mezunu [ Mode: soyler-yapar ] => soyler-yapar
                        Disa_donukluk > 37 [ Mode: soyler-yapar ] => soyler-yapar
                SMP > 15 [ Mode: soyler-yapar ]
                        Uyumluluk <= 35 [ Mode: soylemez-yapar ] => soylemez-yapar
                        Uyumluluk > 35 [ Mode: soyler-yapar ] => soyler-yapar
Nevrotizm > 32 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
```

Davranış: Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım.

```
KDP <= 48 [ Mode: soylemez-yapmaz ]
        Eğitim Düzeyi in [ "Doktora Mezunu" "Önlisans Mezunu" ] [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
        Eğitim Düzeyi in [ "Lisans Mezunu" ] [ Mode: soylemez-yapmaz ]
                internet_saat in [ "1-2" ] [ Mode: soyler-yapmaz ] => soyler-yapmaz
                internet_saat in [ "11+" "6-10" ] [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                internet_saat in [ "3-5" ] [ Mode: soyler-yapmaz ]
                        KDP <= 39 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                        KDP > 39 [ Mode: soyler-yapmaz ] => soyler-yapmaz
        Eğitim Düzeyi in [ "Lise Mezunu" ] [ Mode: soylemez-yapmaz ]
                Uyumluluk <= 32 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                Uyumluluk > 32 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
        Eğitim Düzeyi in [ "Yüksek Lisans Mezunu" ] [ Mode: soyler-yapmaz ]
                Ozdenetim <= 39 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                Ozdenetim > 39 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
        Eğitim Düzeyi in [ "İlköğretim Mezunu" ] [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
KDP > 48 [ Mode: soyler-yapmaz ] => soyler-yapmaz
```

Davranış: Kurumsal e-posta adresimi günlük işlerde de kullanırım.

```
Ozdenetim <= 34 [ Mode: soylemez-yapar ]
        RDP <= 42 [ Mode: soyler-yapar ]
                Eğitim Düzeyi = Doktora Mezunu [ Mode: soylemez-yapar ]
                        yazma_hizi <= 28 [ Mode: soyler-yapar ] => soyler-yapar
                        yazma_hizi > 28 [ Mode: soylemez-yapar ] => soylemez-yapar
                Eğitim Düzeyi = Lisans Mezunu [ Mode: soyler-yapar ]
                        TAP <= 48 [ Mode: soylemez-yapar ]
                                Yas_aralik in [ "Bebek Patlaması" "X Kuşağı" "Y Kuşağı" ] [ Mode: soylemez-yapar ]
                                        Nevrotizm <= 24 [ Mode: soylemez-yapar ]
                                                yazma_hizi <= 33 [ Mode: soyler-yapar ]
                                                        Ozdenetim <= 26 [ Mode: soylemez-yapar ] => soylemez-yapar
                                                        Ozdenetim > 26 [ Mode: soyler-yapar ]
                                                                Yas_aralik in [ "Bebek Patlaması" "X Kuşağı" ] [ Mode: soylemez-yapar ] => soylemez-yapar
                                                                Yas_aralik in [ "Y Kuşağı" ] [ Mode: soyler-yapar ] => soyler-yapar
                                                yazma_hizi > 33 [ Mode: soylemez-yapar ] => soylemez-yapar
                                        Nevrotizm > 24 [ Mode: soylemez-yapar ] => soylemez-yapar
                                Yas_aralik in [ "Z Kuşağı" ] [ Mode: soyler-yapar ]
                                        RDP <= 38 [ Mode: soyler-yapar ] => soyler-yapar
                                        RDP > 38 [ Mode: soylemez-yapar ] => soylemez-yapar
                        TAP > 48 [ Mode: soyler-yapar ]
                                Yas_aralik in [ "Bebek Patlaması" "X Kuşağı" "Y Kuşağı" ] [ Mode: soyler-yapar ] => soyler-yapar
                                Yas_aralik in [ "Z Kuşağı" ] [ Mode: soylemez-yapar ] => soylemez-yapar
                Eğitim Düzeyi = Lise Mezunu [ Mode: soyler-yapar ]
                        Disa_donukluk <= 26 [ Mode: soylemez-yapar ]
                                KDP <= 36 [ Mode: soyler-yapar ]
                                        internet_saat in [ "1-2" "6-10" ] [ Mode: soyler-yapar ] => soyler-yapar
                                        internet_saat in [ "11+" ] [ Mode: soyler-yapar ] => soyler-yapar
                                        internet_saat in [ "3-5" ] [ Mode: soyler-yapar ]
                                                KDP <= 23 [ Mode: soylemez-yapar ] => soylemez-yapar
                                                KDP > 23 [ Mode: soyler-yapar ] => soyler-yapar
                                KDP > 36 [ Mode: soylemez-yapar ] => soylemez-yapar
                        Disa_donukluk > 26 [ Mode: soyler-yapar ]
                                Nevrotizm <= 13 [ Mode: soylemez-yapar ] => soylemez-yapar
                                Nevrotizm > 13 [ Mode: soyler-yapar ] => soyler-yapar
```

```
                Eğitim Düzeyi = Yüksek Lisans Mezunu [ Mode: soylemez-yapar ] => soylemez-yapar
                Eğitim Düzeyi = Önlisans Mezunu [ Mode: soyler-yapar ]
                        Nevrotizm <= 22 [ Mode: soyler-yapar ] => soyler-yapar
                        Nevrotizm > 22 [ Mode: soylemez-yapar ] => soylemez-yapar
                Eğitim Düzeyi = İlköğretim Mezunu [ Mode: soyler-yapar ] => soyler-yapar
        RDP > 42 [ Mode: soylemez-yapar ]
                Uyumluluk <= 23 [ Mode: soyler-yapar ] => soyler-yapar
                Uyumluluk > 23 [ Mode: soylemez-yapar ] => soylemez-yapar
Ozdenetim > 34 [ Mode: soylemez-yapar ]
        okuma-gorme = olumsuz [ Mode: soylemez-yapar ]
                Ozdenetim <= 35 [ Mode: soylemez-yapar ] => soylemez-yapar
                Ozdenetim > 35 [ Mode: soylemez-yapar ]
                        Yas_aralik in [ "Bebek Patlaması" "X Kuşağı" "Y Kuşağı" ] [ Mode: soylemez-yapar ]
                                internet_saat in [ "1-2" ] [ Mode: soyler-yapar ] => soyler-yapar
                                internet_saat in [ "11+" "6-10" ] [ Mode: soylemez-yapar ] => soylemez-yapar
                                internet_saat in [ "3-5" ] [ Mode: soylemez-yapar ]
                                        yazma_hizi <= 24 [ Mode: soylemez-yapar ] => soylemez-yapar
                                        yazma_hizi > 24 [ Mode: soyler-yapar ] => soyler-yapar
                        Yas_aralik in [ "Z Kuşağı" ] [ Mode: soylemez-yapar ] => soylemez-yapar
        okuma-gorme = olumlu [ Mode: soylemez-yapar ]
                RDP <= 42 [ Mode: soylemez-yapar ]
                        Internet_kullanim = 11-15 [ Mode: soylemez-yapar ]
                                Eğitim Düzeyi = Doktora Mezunu [ Mode: soyler-yapar ] => soyler-yapar
                                Eğitim Düzeyi = Lisans Mezunu [ Mode: soylemez-yapar ]
                                        Gelisime_aciklik <= 24 [ Mode: soyler-yapar ] => soyler-yapar
                                        Gelisime_aciklik > 24 [ Mode: soylemez-yapar ] => soylemez-yapar
                                Eğitim Düzeyi = Lise Mezunu [ Mode: soylemez-yapar ]
                                        TAP <= 47 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                        TAP > 47 [ Mode: soylemez-yapar ]
                                                Disa_donukluk <= 28 [ Mode: soyler-yapar ] => soyler-yapar
                                                Disa_donukluk > 28 [ Mode: soylemez-yapar ] => soylemez-yapar
                                Eğitim Düzeyi = Yüksek Lisans Mezunu [ Mode: soylemez-yapar ] => soylemez-yapar
                                Eğitim Düzeyi = Önlisans Mezunu [ Mode: soylemez-yapar ]
                                        Uyumluluk <= 29 [ Mode: soyler-yapar ] => soyler-yapar
                                        Uyumluluk > 29 [ Mode: soylemez-yapar ] => soylemez-yapar
                                Eğitim Düzeyi = İlköğretim Mezunu [ Mode: soylemez-yapar ] => soylemez-yapar
                        Internet_kullanim = 15+ [ Mode: soylemez-yapar ]
```

internet_saat = 1-2 [Mode: soylemez-yapar]
Uyumluluk <= 37 [Mode: soylemez-yapar] => soylemez-yapar
Uyumluluk > 37 [Mode: soyler-yapar] => soyler-yapar
internet_saat = 11+ [Mode: soylemez-yapar] => soylemez-yapar
internet_saat = 3-5 [Mode: soylemez-yapar]
RDP <= 19 [Mode: soylemez-yapmaz] => soylemez-yapmaz
RDP > 19 [Mode: soylemez-yapar] => soylemez-yapar
internet_saat = 6-10 [Mode: soyler-yapar] => soyler-yapar
Internet_kullanim = 3-6 [Mode: soylemez-yapar] => soylemez-yapar
Internet_kullanim = 7-10 [Mode: soylemez-yapar]
RDP <= 24 [Mode: soyler-yapar]
Uyumluluk <= 34 [Mode: soylemez-yapar] => soylemez-yapar
Uyumluluk > 34 [Mode: soyler-yapar] => soyler-yapar
RDP > 24 [Mode: soylemez-yapar]
KDP <= 56 [Mode: soylemez-yapar]
SMP <= 5 [Mode: soylemez-yapar] => soylemez-yapar
SMP > 5 [Mode: soylemez-yapmaz] => soylemez-yapmaz
KDP > 56 [Mode: soylemez-yapmaz] => soylemez-yapmaz
RDP > 42 [Mode: soylemez-yapar] => soylemez-yapar

Davranış: İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım.

```
KDP <= 18 [ Mode: soylemez-yapar ]
        KDP <= 13 [ Mode: soylemez-yapar ] => soylemez-yapar
        KDP > 13 [ Mode: soyler-yapmaz ]
                RDP <= 36 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                RDP > 36 [ Mode: soylemez-yapar ] => soylemez-yapar
KDP > 18 [ Mode: soylemez-yapar ]
        RDP <= 28 [ Mode: soylemez-yapar ]
                Eğitim Düzeyi = Doktora Mezunu [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                Eğitim Düzeyi = Lisans Mezunu [ Mode: soylemez-yapar ]
                        okuma-gorme = olumsuz [ Mode: soylemez-yapmaz ]
                                Uyumluluk <= 37 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                Uyumluluk > 37 [ Mode: soyler-yapar ] => soyler-yapar
                        okuma-gorme = olumlu [ Mode: soylemez-yapar ]
                                Internet_kullanim = 11-15 [ Mode: soylemez-yapmaz ]
                                        SMP <= 5 [ Mode: soylemez-yapmaz ]
                                                yazma_hizi <= 43 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                                yazma_hizi > 43 [ Mode: soylemez-yapar ] => soylemez-yapar
                                        SMP > 5 [ Mode: soyler-yapar ] => soyler-yapar
                                Internet_kullanim = 15+ [ Mode: soylemez-yapar ]
                                        RDP <= 18 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                        RDP > 18 [ Mode: soylemez-yapar ] => soylemez-yapar
                                Internet_kullanim = 3-6 [ Mode: soylemez-yapar ] => soylemez-yapar
                                Internet_kullanim = 7-10 [ Mode: soylemez-yapar ]
                                        SMP <= 5 [ Mode: soylemez-yapar ] => soylemez-yapar
                                        SMP > 5 [ Mode: soyler-yapar ] => soyler-yapar
                Eğitim Düzeyi = Lise Mezunu [ Mode: soylemez-yapmaz ]
                        SMP <= 1 [ Mode: soylemez-yapmaz ]
                                TAP <= 51 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                TAP > 51 [ Mode: soyler-yapmaz ] => soyler-yapmaz
                        SMP > 1 [ Mode: soylemez-yapar ]
                                TAP <= 54 [ Mode: soylemez-yapar ] => soylemez-yapar
                                TAP > 54 [ Mode: soylemez-yapmaz ]
                                        okuma-gorme = olumsuz [ Mode: soyler-yapar ]
```

```
                                        Uyumluluk <= 29 [ Mode: soylemez-yapar ] => soylemez-yapar
                                        Uyumluluk > 29 [ Mode: soyler-yapar ] => soyler-yapar
                                okuma-gorme = olumlu [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
        Eğitim Düzeyi = Yüksek Lisans Mezunu [ Mode: soylemez-yapar ] => soylemez-yapar
        Eğitim Düzeyi = Önlisans Mezunu [ Mode: soylemez-yapar ]
                Cinsiyet = Kadın [ Mode: soyler-yapar ]
                        yazma_hizi <= 37 [ Mode: soyler-yapar ] => soyler-yapar
                        yazma_hizi > 37 [ Mode: soylemez-yapar ] => soylemez-yapar
                Cinsiyet = Erkek [ Mode: soylemez-yapar ]
                        KDP <= 55 [ Mode: soylemez-yapar ] => soylemez-yapar
                        KDP > 55 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
        Eğitim Düzeyi = İlköğretim Mezunu [ Mode: soylemez-yapar ]
                Gelisime_aciklik <= 35 [ Mode: soyler-yapar ] => soyler-yapar
                Gelisime_aciklik > 35 [ Mode: soylemez-yapar ] => soylemez-yapar
RDP > 28 [ Mode: soylemez-yapar ]
        Yas_aralik = Bebek Patlaması [ Mode: soylemez-yapar ]
                TAP <= 54 [ Mode: soyler-yapar ] => soyler-yapar
                TAP > 54 [ Mode: soylemez-yapar ] => soylemez-yapar
        Yas_aralik = X Kuşağı [ Mode: soylemez-yapar ]
                internet_saat in [ "1-2" ] [ Mode: soylemez-yapmaz ]
                        Internet_kullanim in [ "11-15" ] [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                        Internet_kullanim in [ "15+" ] [ Mode: soylemez-yapar ]
                                RDP <= 35 [ Mode: soylemez-yapar ] => soylemez-yapar
                                RDP > 35 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                        Internet_kullanim in [ "3-6" "7-10" ] [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                internet_saat in [ "11+" "3-5" ] [ Mode: soylemez-yapar ] => soylemez-yapar
                internet_saat in [ "6-10" ] [ Mode: soylemez-yapar ]
                        Cinsiyet = Kadın [ Mode: soylemez-yapar ] => soylemez-yapar
                        Cinsiyet = Erkek [ Mode: soylemez-yapar ]
                                KDP <= 55 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                KDP > 55 [ Mode: soylemez-yapar ] => soylemez-yapar
        Yas_aralik = Y Kuşağı [ Mode: soylemez-yapar ]
                RDP <= 33 [ Mode: soylemez-yapar ]
                        Internet_kullanim = 11-15 [ Mode: soylemez-yapar ]
                                okuma-gorme = olumsuz [ Mode: soylemez-yapmaz ]
                                        yazma_hizi <= 46 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
```

```
                                        yazma_hizi > 46 [ Mode: soylemez-yapar ] => soylemez-yapar
                                okuma-gorme = olumlu [ Mode: soylemez-yapar ] => soylemez-yapar
                        Internet_kullanim = 15+ [ Mode: soylemez-yapar ]
                                KDP <= 52 [ Mode: soylemez-yapar ] => soylemez-yapar
                                KDP > 52 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                        Internet_kullanim = 3-6 [ Mode: soylemez-yapar ] => soylemez-yapar
                        Internet_kullanim = 7-10 [ Mode: soylemez-yapar ]
                                yazma_hizi <= 21 [ Mode: soylemez-yapar ] => soylemez-yapar
                                yazma_hizi > 21 [ Mode: soyler-yapar ] => soyler-yapar
                RDP > 33 [ Mode: soylemez-yapar ]
                        Internet_kullanim in [ "11-15" "7-10" ] [ Mode: soylemez-yapar ] => soylemez-yapar
                        Internet_kullanim in [ "15+" ] [ Mode: soylemez-yapar ]
                                Cinsiyet = Kadın [ Mode: soylemez-yapmaz ]
                                        Eğitim Düzeyi in [ "Doktora Mezunu" "Lise Mezunu" "Önlisans Mezunu" "İlköğretim Mezunu" ] [ Mode: soylemez-
yapmaz ] => soylemez-yapmaz
                                        Eğitim Düzeyi in [ "Lisans Mezunu" ] [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                        Eğitim Düzeyi in [ "Yüksek Lisans Mezunu" ] [ Mode: soylemez-yapmaz ]
                                                Nevrotizm <= 21 [ Mode: soylemez-yapar ] => soylemez-yapar
                                                Nevrotizm > 21 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                Cinsiyet = Erkek [ Mode: soylemez-yapar ]
                                        RDP <= 50 [ Mode: soylemez-yapar ]
                                                Gelisime_aciklik <= 36 [ Mode: soylemez-yapar ] => soylemez-yapar
                                                Gelisime_aciklik > 36 [ Mode: soylemez-yapar ]
                                                        Nevrotizm <= 22 [ Mode: soylemez-yapar ] => soylemez-yapar
                                                        Nevrotizm > 22 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                        RDP > 50 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                        Internet_kullanim in [ "3-6" ] [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
        Yas_aralik = Z Kuşağı [ Mode: soylemez-yapmaz ]
                Ozdenetim <= 37 [ Mode: soylemez-yapar ]
                        Cinsiyet = Kadın [ Mode: soylemez-yapmaz ]
                                TAP <= 50 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                TAP > 50 [ Mode: soylemez-yapar ] => soylemez-yapar
                        Cinsiyet = Erkek [ Mode: soylemez-yapar ] => soylemez-yapar
                Ozdenetim > 37 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
```

Davranış: İnternet ortamında gerektiği durumlarda özlük bilgilerimi (ad, soyad, doğum tarihi vb.) paylaşırım

```
RDP <= 27 [ Mode: soyler-yapar ]
        Gelisime_aciklik <= 18 [ Mode: soylemez-yapmaz ]
                Gelisime_aciklik <= 15 [ Mode: soyler-yapar ]
                        Nevrotizm <= 21 [ Mode: soyler-yapar ] => soyler-yapar
                        Nevrotizm > 21 [ Mode: soylemez-yapar ] => soylemez-yapar
                Gelisime_aciklik > 15 [ Mode: soylemez-yapmaz ]
                        Cinsiyet = Kadın [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                        Cinsiyet = Erkek [ Mode: soylemez-yapmaz ]
                                yazma_hizi <= 35 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                yazma_hizi > 35 [ Mode: soylemez-yapar ] => soylemez-yapar
        Gelisime_aciklik > 18 [ Mode: soyler-yapar ]
                Disa_donukluk <= 34 [ Mode: soyler-yapar ]
                        Ozdenetim <= 41 [ Mode: soylemez-yapar ]
                                RDP <= 17 [ Mode: soyler-yapar ] => soyler-yapar
                                RDP > 17 [ Mode: soylemez-yapar ]
                                        KDP <= 47 [ Mode: soylemez-yapar ] => soylemez-yapar
                                        KDP > 47 [ Mode: soyler-yapar ]
                                                Gelisime_aciklik <= 33 [ Mode: soylemez-yapar ] => soylemez-yapar
                                                Gelisime_aciklik > 33 [ Mode: soyler-yapar ] => soyler-yapar
                        Ozdenetim > 41 [ Mode: soyler-yapar ] => soyler-yapar
                Disa_donukluk > 34 [ Mode: soylemez-yapar ]
                        RDP <= 14 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                        RDP > 14 [ Mode: soylemez-yapar ] => soylemez-yapar
RDP > 27 [ Mode: soylemez-yapar ]
        SMP <= 1 [ Mode: soylemez-yapar ]
                Yas_aralik in [ "Bebek Patlaması" "X Kuşağı" ] [ Mode: soyler-yapar ]
                        Ozdenetim <= 37 [ Mode: soylemez-yapar ] => soylemez-yapar
                        Ozdenetim > 37 [ Mode: soyler-yapar ] => soyler-yapar
                Yas_aralik in [ "Y Kuşağı" "Z Kuşağı" ] [ Mode: soylemez-yapar ]
                        SMP <= 0 [ Mode: soylemez-yapar ]
                                TAP <= 62 [ Mode: soylemez-yapar ] => soylemez-yapar
```

```
                    TAP > 62 [ Mode: soyler-yapar ] => soyler-yapar
                SMP > 0 [ Mode: soylemez-yapar ] => soylemez-yapar
SMP > 1 [ Mode: soylemez-yapar ]
        internet_saat = 1-2 [ Mode: soylemez-yapar ]
                Eğitim Düzeyi in [ "Doktora Mezunu" "Önlisans Mezunu" ] [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                Eğitim Düzeyi in [ "Lisans Mezunu" ] [ Mode: soylemez-yapar ]
                        Disa_donukluk <= 25 [ Mode: soylemez-yapmaz ]
                                Uyumluluk <= 37 [ Mode: soylemez-yapmaz ]
                                        Uyumluluk <= 28 [ Mode: soylemez-yapar ] => soylemez-yapar
                                        Uyumluluk > 28 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                Uyumluluk > 37 [ Mode: soylemez-yapar ] => soylemez-yapar
                        Disa_donukluk > 25 [ Mode: soylemez-yapar ]
                                Cinsiyet = Kadın [ Mode: soylemez-yapar ] => soylemez-yapar
                                Cinsiyet = Erkek [ Mode: soyler-yapar ] => soyler-yapar
                Eğitim Düzeyi in [ "Lise Mezunu" ] [ Mode: soylemez-yapar ]
                        Cinsiyet = Kadın [ Mode: soylemez-yapar ] => soylemez-yapar
                        Cinsiyet = Erkek [ Mode: soyler-yapar ] => soyler-yapar
                Eğitim Düzeyi in [ "Yüksek Lisans Mezunu" ] [ Mode: soylemez-yapar ] => soylemez-yapar
                Eğitim Düzeyi in [ "İlköğretim Mezunu" ] [ Mode: soylemez-yapar ] => soylemez-yapar
        internet_saat = 11+ [ Mode: soylemez-yapar ]
                okuma-gorme = olumsuz [ Mode: soylemez-yapmaz ]
                        Cinsiyet = Kadın [ Mode: soylemez-yapar ]
                                Ozdenetim <= 40 [ Mode: soylemez-yapar ] => soylemez-yapar
                                Ozdenetim > 40 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                        Cinsiyet = Erkek [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                okuma-gorme = olumlu [ Mode: soylemez-yapar ] => soylemez-yapar
        internet_saat = 3-5 [ Mode: soylemez-yapar ]
                Uyumluluk <= 22 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                Uyumluluk > 22 [ Mode: soylemez-yapar ]
                        Nevrotizm <= 8 [ Mode: soylemez-yapmaz ]
                                Gelisime_aciklik <= 37 [ Mode: soyler-yapar ] => soyler-yapar
                                Gelisime_aciklik > 37 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                        Nevrotizm > 8 [ Mode: soylemez-yapar ]
                                KDP <= 46 [ Mode: soylemez-yapar ] => soylemez-yapar
                                KDP > 46 [ Mode: soylemez-yapar ]
                                        KDP <= 52 [ Mode: soylemez-yapar ]
```

```
                                        Eğitim Düzeyi in [ "Doktora Mezunu" "İlköğretim Mezunu" ] [ Mode: soylemez-yapar ] => soylemez-yapar
                                        Eğitim Düzeyi in [ "Lisans Mezunu" ] [ Mode: soylemez-yapar ]
                                                Gelisime_aciklik <= 34 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                                Gelisime_aciklik > 34 [ Mode: soylemez-yapar ] => soylemez-yapar
                                        Eğitim Düzeyi in [ "Lise Mezunu" ] [ Mode: soylemez-yapar ] => soylemez-yapar
                                        Eğitim Düzeyi in [ "Yüksek Lisans Mezunu" ] [ Mode: soyler-yapar ] => soyler-yapar
                                        Eğitim Düzeyi in [ "Önlisans Mezunu" ] [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                                KDP > 52 [ Mode: soylemez-yapar ] => soylemez-yapar
internet_saat = 6-10 [ Mode: soylemez-yapar ]
        Gelisime_aciklik <= 23 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
        Gelisime_aciklik > 23 [ Mode: soylemez-yapar ]
                yazma_hizi <= 82 [ Mode: soylemez-yapar ]
                        Disa_donukluk <= 36 [ Mode: soylemez-yapar ]
                                Nevrotizm <= 27 [ Mode: soylemez-yapar ] => soylemez-yapar
                                Nevrotizm > 27 [ Mode: soylemez-yapar ]
                                        KDP <= 52 [ Mode: soylemez-yapar ] => soylemez-yapar
                                        KDP > 52 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                        Disa_donukluk > 36 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
                yazma_hizi > 82 [ Mode: soylemez-yapmaz ] => soylemez-yapmaz
```

EK 13. Bilgi Güvenliği Farkındalık Eğitimi Öğretim Programı

Bu eğitimle katılımcıya bilgi güvenliğine dair riskli ve korumacı davranışlarına yönelik farkındalık kazandırılması amaşlanmıştır.

KAZANIM VE AÇIKLAMALAR

Kazanım 1: Bilgisayarında lisanslı yazılım kullanmaya dikkat eder

Bilgi:

- Korsan/lisanssız yazılımın ne olduğunu ifade edebilir,
- Korsan/lisanssız yazılım kullanımı sebebiyle karşılaşabilecek tehlikeleri açıklayabilir,
- Neden lisanslı yazılım kullanmasının gerektiğini ifade edebilir

Kazanım 2: Birden fazla elektronik eposta adresi kullanır

Bilgi:

- Neden birden fazla eposta adresi kullanılması gerektiğini açıklaybilir
- Epostanın kullanım alanlarını açıklayabilir

Kazanım 3: Eğer aynı iletiyi birden fazla kişiye gönderecekse gizli (BCC) kısmını kullanır

Bilgi:

- Eposta gönderirken kullanılan gizli karbon kopya fonksiyonunu açıklayabilir
- İstenmeyen veya önemsiz eposta içeriklerine örnek verebilir,
- İstenmeyen veya önemsiz epostaların riskleri ifade edebilir

Kazanım 4: Geçici internet dosyalarını ve web gezinti geçmişlerini inceler

Bilgi:

- Geçici internet dosyası kavramını açıklayabilir,
- Geçici internet dosyalarını silmenin faydalarını sıralayabilir,
- Geçici internet dosyalarını silme adımlarını takip edebilir,

Kazanım 5: Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat eder

Bilgi:

- SSL sertifikası kavramını açıklayabilir,
- SSL sertifikasının önemini ifade edebilir,

Kazanım 6: Güvenlik duvarı, reklam önleyici vb. programlar kullanır

Bilgi:

- Güvenlik duvarının ne olduğunu ifade edebilir
- Güvenlik duvarı çalışma mantığını açıklayabilir,
- Neden güvenlik duvarı kullanılması gerektiğini açıklayabilir,
- Güvenlik duvarı kullanmanın neyden koruyamayacağını ifade edebilir

Kazanım 7: İnternet ortamında iletişim bilgilerini (GSM no, eposta vb.) paylaşmaz

Bilgi:

- Kişisel olarak tanımlanabilir bilginin ne olduğunu ifade edebilir,
- İnternet ortamında iletişim bilgilerinin paylaşılmasının neden riskli olduğunu ifade edebilir,
- Kişisel olarak tanımlanabilir bilgilerini korumak için neler yapması gerektiğini açıklayabilir,

Kazanım 8: İnternet ortamında özlük bilgilerini (ad, soyad, doğum tarihi vb.) paylaşmaz

Bilgi:

- İnternet ortamında özlük bilgilerinin paylaşılmasının neden riskli olduğunu ifade edebilir

Kazanım 9: İnternet üzerindeki hesaplarında kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanır

Bilgi:

- Güçlü parolanın özelliklerini açıklayabilir,
- Güçlü parola oluşturabilir,
- Parola oluştururken yapılmamasına dikkat edilmmesi gereken hususları açıklayabilir

Kazanım 10: Kurumsal e-posta adresimi günlük işlerde de kullanmaz

Bilgi:

- Kurumsal epostanın ne olduğunu ifade edebilir,
- Kurumsal epostanın önemini açıklayabilir,
- Kurumsal eposta hesabının günlük işlemlerde kullanmanın risklerini açıklayabilir,

Kazanım 11: Virüs temizleme, casus yazılım önleme vb. programları kullanır

Bilgi:

- Zararlı yazılımın ne olduğunu ifade edebilir,
- Zararlı yazılımların verebileceği zararlara örnekler verebilir,
- Zararlı yazılımlardan korunmak için neler yapılabileceğini açıklayabilir.

EK 14. Bilgi Güvenliğine Dair Hazırlanan Eğitim İçeriği Konu Başlıkları

"Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim" davranışı için oluşturulan içerikle ilgili konu başlıkları

Konu: Bilgisayarımda lisanslı yazılım kullanmaya dikkat ederim.		
Davranışa İlişkin Sınıflandırma	Eğitim İçeriği Seviyesi	Konu Başlıkları
Söyler ve Yapar	1	- Eğitime katıl - Bir sonraki eğitim içeriğine devam et
Söyler ancak Yapmaz	2	- Neden lisanssız yazılım kullanılıyor? - Lisanssız yazılım kullanıcılarını ne tür tehlikeler beklemektedir? - Lisanssız yazılım konusunda nasıl hareket edilmeli?
Söylemez ancak Yapar	3	- Lisanssız yazılım nedir? - İsteğe bağlı erişim • Lisanssız yazılım kullanıcılarını ne tür tehlikeler beklemektedir?
Söylemez ve Yapmaz	4	- Lisanssız yazılım nedir? - Neden lisanssız yazılım kullanılıyor? - Lisanssız yazılım kullanıcılarını ne tür tehlikeler beklemektedir? - Lisanssız yazılım konusunda nasıl hareket edilmeli? - Lisanslı yazılım kullanmanın yararları nelerdir? - Örneklerle video içeriği

"Birden fazla elektronik eposta adresi kullanırım" Davranışı için Oluşturulan İçerikle ilgili Konu Başlıkları

Konu: Birden fazla elektronik eposta adresi kullanırım.		
Davranışa İlişkin Sınıflandırma	Eğitim İçeriği Seviyesi	Konu Başlıkları
Söyler ve Yapar	1	- Eğitime katıl - Bir sonraki eğitim içeriğine devam et
Söyler ancak Yapmaz	2	- Epostanın kullanım alanları nelerdir? - İstenmeyen eposta nedir? - İstenmeyen e-posta nasıl çalışır? - İstenmeyen e-posta riskleri nedir? - Kimlik avı epostaları nasıl çalışır? - Risklerden kurtulmak için ne yapmalıyım?
Söylemez ancak Yapar	3	- Eposta nedir? - Epostanın kullanım alanları nelerdir? - İsteğe bağlı erişim • İstenmeyen e-posta nasıl çalışır? • İstenmeyen e-posta riskleri nedir? • Kimlik avı epostaları nasıl çalışır? • Risklerden kurtulmak için ne yapmalıyım?
Söylemez ve Yapmaz	4	- Eposta nedir? - Epostanın kullanım alanları nelerdir? - İsteğe bağlı erişim - İstenmeyen e-posta nasıl çalışır? - İstenmeyen e-posta riskleri nedir? - Kimlik avı epostaları nasıl çalışır? - Risklerden kurtulmak için ne yapmalıyım? - Örneklerle video içeriği

“Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım.” Davranışı için Oluşturulan İçerikle ilgili Konu Başlıkları

Konu: Eğer aynı iletiyi birden fazla kişiye göndereceksem gizli (BCC) kısmını kullanırım		
Davranışa İlişkin Sınıflandırma	Eğitim İçeriği Seviyesi	Konu Başlıkları
Söyler ve Yapar	1	- Modellemeye dâhil sınıf oluşmadı
Söyler ancak Yapmaz	2	- Epostanın adres satırındaki bölümler nelerdir? - Neden BCC kullanmak gerekir?
Söylemez ancak Yapar	3	- Modellemeye dâhil sınıf oluşmadı
Söylemez ve Yapmaz	4	- Epostanın adres satırındaki bölümler nelerdir? - Neden BCC kullanmak gerekir? - Örneklerle video içeriği

“Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim.” Davranışı için Oluşturulan İçerikle ilgili Konu Başlıkları

Konu: Geçici internet dosyalarını ve web gezinti geçmişlerini incelerim		
Davranışa İlişkin Sınıflandırma	Eğitim İçeriği Seviyesi	Konu Başlıkları
Söyler ve Yapar	1	- Modellemeye dâhil sınıf oluşmadı
Söyler ancak Yapmaz	2	- Geçici internet dosyalarını neden silmeliyim? - Geçici internet dosyalarını nasıl silebilirim? - Web gezinti geçmişi neden silinmelidir? - Web gezinti geçmişi nasıl silinir?
Söylemez ancak Yapar	3	- Modellemeye dâhil sınıf oluşmadı
Söylemez ve Yapmaz	4	- Geçici internet dosyaları ne işe yarar? - Geçici internet dosyalarını neden silmeliyim? - Web gezinti geçmişi nedir? - Web gezinti geçmişi nasıl silinir? - Örneklerle video içeriği

“Güvenlik duvarı, reklam önleyici vb. programlar kullanırım.” Davranışı için Oluşturulan İçerikle ilgili Konu Başlıkları

Konu: Güvenlik duvarı, reklam önleyici vb. Programlar kullanırım		
Davranışa İlişkin Sınıflandırma	Eğitim İçeriği Seviyesi	Konu Başlıkları
Söyler ve Yapar	1	- Eğitime katıl - Bir sonraki eğitim içeriğine devam et
Söyler ancak Yapmaz	2	- Bilgi Güvenliğini üst düzeye çıkarmak için neler yapılabilir? - Güvenlik duvarı hangi tehlikelerden korur? - Güvenlik duvarı hangi tehlikelerden korumaz?
Söylemez ancak Yapar	3	- Modellemeye dâhil sınıf oluşmadı
Söylemez ve Yapmaz	4	- Güvenlik duvarı nedir? - Güvenlik duvarı nasıl çalışır? - Bilgi Güvenliğini üst düzeye çıkarmak için neler yapılabilir? - Güvenlik duvarı hangi tehlikelerden korur? - Güvenlik duvarı hangi tehlikelerden korumaz? - Örneklerle video içeriği

“İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım.” Davranışı için Oluşturulan İçerikle ilgili Konu Başlıkları

Konu: İnternet ortamında gerektiği durumlarda iletişim bilgilerimi (GSM no, eposta vb.) paylaşırım		
Davranışa İlişkin Sınıflandırma	Eğitim İçeriği Seviyesi	Konu Başlıkları
Söyler ve Yapar	1	- Eğitime katıl - Bir sonraki eğitim içeriğine devam et
Söyler ancak Yapmaz	2	- İletişim bilgilerini paylaşmanın riskleri nelerdir? - Risk örneği - Risklerden korunmak için neler yapmalıyım?
Söylemez ancak Yapar	3	- Kişisel olarak tanımlanabilir bilgi nedir? - İsteğe bağlı erişim • İletişim bilgilerini paylaşmanın riskleri nelerdir? • Risk örneği • Risklerden korunmak için neler yapmalıyım?
Söylemez ve Yapmaz	4	- Kişisel olarak tanımlanabilir bilgi nedir? - İletişim bilgilerini paylaşmanın riskleri nelerdir? - Risk örneği - Risklerden korunmak için neler yapmalıyım? - Örneklerle video içeriği

"İnternet ortamında gerektiği durumlarda özlük bilgilerimi (ad, soyad, doğum tarihi vb.) paylaşırım." Davranışı için Oluşturulan İçerikle ilgili Konu Başlıkları

Konu: İnternet ortamında gerektiği durumlarda özlük bilgilerimi (ad, soyad, doğum tarihi vb.) paylaşırım		
Davranışa İlişkin Sınıflandırma	Eğitim İçeriği Seviyesi	Konu Başlıkları
Söyler ve Yapar	1	- Eğitime katıl - Bir sonraki eğitim içeriğine devam et
Söyler ancak Yapmaz	2	- Modellemeye dâhil sınıf oluşmadı
Söylemez ancak Yapar	3	- Kişisel olarak tanımlanabilir bilgi nedir? - Özlük bilgilerini paylaşmanın riskleri nelerdir? - İsteğe bağlı erişim • Risk örneği • Riskleri önlemek için neler yapmalıyım?
Söylemez ve Yapmaz	4	- Kişisel olarak tanımlanabilir bilgi nedir? - Özlük bilgilerini paylaşmanın riskleri nelerdir? - Risk örneği - Riskleri önlemek için neler yapmalıyım? - Örneklerle video içeriği

"İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım" Davranışı için Oluşturulan İçerikle ilgili Konu Başlıkları

Konu: İnternet üzerindeki hesaplarımda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanırım		
Davranışa İlişkin Sınıflandırma	Eğitim İçeriği Seviyesi	Konu Başlıkları
Söyler ve Yapar	1	- Eğitime katıl - Bir sonraki eğitim içeriğine devam et
Söyler ancak Yapmaz	2	- Zayıf parola kullanmanın riskleri nelerdir? - Şifre oluştururken neler yapmamalıyım?
Söylemez ancak Yapar	3	- Modellemeye dâhil sınıf oluşmadı
Söylemez ve Yapmaz	4	- Güçlü parola nedir? - Güçlü parola nasıl oluşturulur? - Parola önerileri neler olabilir? - Zayıf parola kullanmanın riskleri nelerdir? - Şifre oluştururken neler yapmamalıyım? - Örneklerle video içeriği

“Kurumsal e-posta adresimi günlük işlerde de kullanırım.” Davranışı için Oluşturulan İçerikle ilgili Konu Başlıkları

Konu: Kurumsal e-posta adresimi günlük işlerde de kullanırım		
Davranışa İlişkin Sınıflandırma	Eğitim İçeriği Seviyesi	Konu Başlıkları
Söyler ve Yapar	1	- Eğitime katıl - Bir sonraki eğitim içeriğine devam et
Söyler ancak Yapmaz	2	- Modellemeye dâhil sınıf oluşmadı
Söylemez ancak Yapar	3	- Kurumsal eposta nedir? - Kurumsal eposta neden önemlidir? - İsteğe bağlı erişim • Kurumsal eposta hesabı nasıl kullanılmalıdır? • Kurumsal eposta hesabını günlük işlemlerde kullanmanın riskleri nelerdir? • Risk örneği
Söylemez ve Yapmaz	4	- Kurumsal eposta nedir? - Kurumsal eposta neden önemlidir? - İsteğe bağlı erişim - Kurumsal eposta hesabı nasıl kullanılmalıdır? - Kurumsal eposta hesabını günlük işlemlerde kullanmanın riskleri nelerdir? - Risk örneği

“Virüs temizleme, casus yazılım önleme vb. programları kullanırım” Davranışı için Oluşturulan İçerikle ilgili Konu Başlıkları

Konu: Virüs temizleme, casus yazılım önleme vb. Programları kullanırım		
Davranışa İlişkin Sınıflandırma	Eğitim İçeriği Seviyesi	Konu Başlıkları
Söyler ve Yapar	1	- Eğitime katıl - Bir sonraki eğitim içeriğine devam et
Söyler ancak Yapmaz	2	- Zararlı programlar neler yapabilir? - Zararlı programlardan korunmak için neler yapmalıyım?
Söylemez ancak Yapar	3	- Modellemeye dâhil sınıf oluşmadı
Söylemez ve Yapmaz	4	- Zararlı yazılım nedir? - Zararlı programlar neler yapabilir? - Zararlı programlardan korunmak için neler yapmalıyım? - Bilgisayarımı nasıl korurum? - Örneklerle video içeriği

EK 15. Eğitim İçeriği Uzman Görüş Formu

Sayın……
Gazi Üniversitesi Eğitim Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı'nda Prof. Dr. Serçin KARATAŞ danışmanlığında hazırlanan "Bilgi Güvenliği Eğitimine Yönelik Uyarlanabilir Öğrenme Ortamının Geliştirilmesi" başlıklı doktora tezi çalışması kapsamında geliştirilen web sitesi, www.*******.com adresi üzerinde yayınlanmaktadır. Bu ortamda yer alan ve 8-10 dakika süren ölçek soruları yanıtlandıktan sonra, kullanıcıya kişiselleştirilmiş olarak bilgi güvenliğine yönelik eğitim içeriği sunulmaktadır. Belirtilen eğitimin konu listesi "Derecelendirme Kılavuz Tablosunda" sunulmuştur. Sizden, söz konusu eğitim içeriklerini ve içeriklerde yer alan çoklu medya öğelerini, alan uzmanı olarak kapsam ve konuya uygunluk açısından aşağıda belirtilen 3'lü derecelendirmeyi temel alarak puanlamanız, (varsa) konu ile ilgili görüşlerinizi "açıklama" sütununa ve eklemek istediğiniz başka bir husus var ise "ek görüş" bölümünde yazmanız beklenmektedir.

Katkılarınız için şimdiden teşekkür ederim,

Saygılarımla,

Onur CERAN

İletişim: ****@gazi.edu.tr

Derecelendirme Kılavuz Tablosu

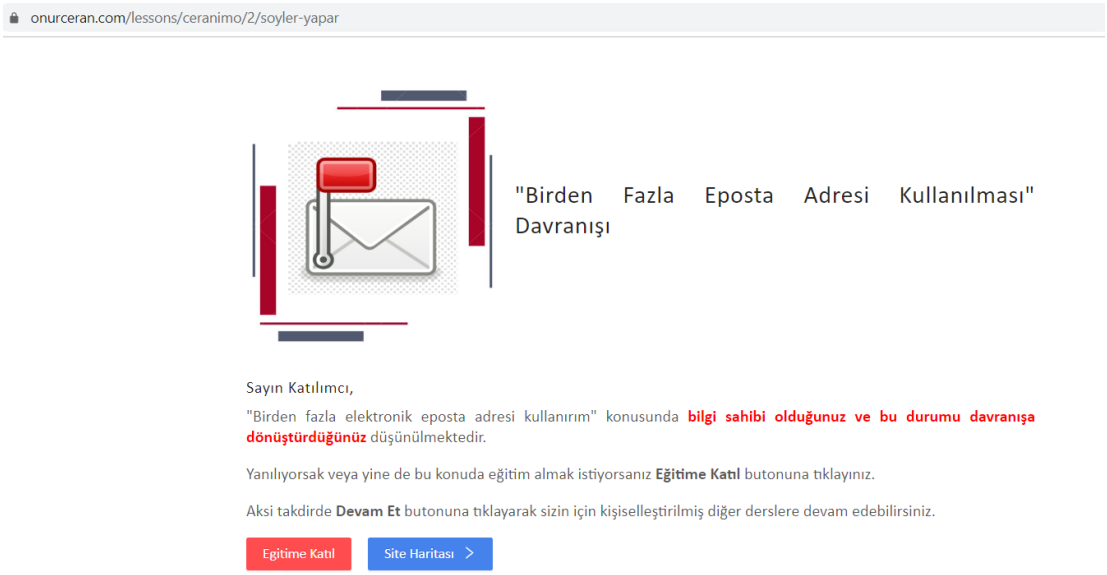
Puan Türü	Puanlamada dikkate alınacak ölçütler
Uygun	Konu içerikleri ve çoklu medyanın düzeltmeye ihtiyaç olmaksızın kullanılmasının uygun olduğunu düşünüyorsanız bu seçeneği işaretleyiniz.
Kısmen Uygun	Konu içerikleri ve çoklu medyanın açıklamalar kısmında belirtilen düzeltmeler doğrultusunda düzenlendikten sonra kullanılması gerektiğini düşünüyorsanız bu seçeneği işaretleyiniz.
Uygun değil	Konu içerikleri ve çoklu medyanın hedef kitleye uygun olmadığını düşünüyorsanız bu seçeneği işaretleyiniz.

Konu Başlığı	Uygun	Kısmen Uygun	Uygun Değil	Açıklama
Bilgisayarda lisanslı yazılım kullanmaya dikkat etme				
Birden fazla elektronik eposta adresi kullanma				
Eğer aynı ileti birden fazla kişiye gönderilecekse gizli (BCC) kısmını kullanma				
Geçici internet dosyalarını ve web gezinti geçmişlerini inceleme				
Girilen sitelerin SSL sertifikası olup olmadığına dikkat etme				
Güvenlik duvarı, reklam önleyici vb. programlar kullanma				
İnternet ortamında iletişim bilgilerini (GSM no, eposta vb.) paylaşmama				
İnternet ortamında özlük bilgilerini (ad, soyad, doğum tarihi vb.) paylaşmama				
İnternet üzerindeki hesaplarda kolay tahmin edilemeyecek şekilde karmaşık ve uzun şifreler kullanma				
Kurumsal e-posta adresini günlük işlerde kullanmama				
Virüs temizleme, casus yazılım önleme vb. programları kullanma				

Ek Görüş: ----------

EK 16. Sınıflara Ait Eğitim İçerikleri

“Söyler ve Yapar” Sınıfı için Eğitim İçeriği



“Söylemez ancak Yapar” Sınıfı için Eğitim İçeriği

onurceran.com/lessons/ceranimo/5/soylemez-yapar

"Ziyaret Edilen Web Sitelerinin SSL Sertifikasının Olup Olmadığının İncelenmesi" Davranışı

Sayın Katılımcı,

"Girdiğim sitelerin SSL sertifikası olup olmadığına dikkat ederim" konusunda **bilgi sahibi olmadığınız ancak bu konuda doğru davranış sergilediğiniz** düşünülmektedir. Ders içeriğinde konu hakkında teorik bilgi verilecek olup bu konunun hangi durumlarda ne gibi sorunlara yol açacağı hakkında detaylı bilgi almak isterseniz konu başlığı üzerine tıklayabilirsiniz.

SSL Sertifikası Nedir? Ne İşe Yarar?

SSL (Secure Sockets Layer), bilgi transferi sırasında güvenlik ve gizliliğin sağlanması amacıyla 1996 yılında Netscape tarafından geliştirilmiş bir güvenlik protokolüdür.3.0 versiyonunun çıkması ile beraber hemen tüm Internet tarayıcılarının (Microsoft Explorer, Safari, Firefox, Chrome vb.) desteklediği bir standart haline gelmiş, geniş kitle ve uygulama alanları bulmuştur. Sertifika ile gönderilen bilgi sadece doğru adreste açığa çıkarak deşifre olur. Gönderilmeden önce otomatik olarak şifrelenen bilgi sadece doğru alıcı tarafından deşifre edilebilir ve doğrulama her iki taraf tarafından yapılarak işlemin ve bilginin gizliliği bütünlüğü bozulmadan korunur.

> SSL Sertifikası Neden Önemlidir?

> SSL Sertifikasına Neden ihtiyaç duyarız?

Sonraki Eğitim > | Site Haritası

“Söylemez ve Yapmaz” Sınıfı için Eğitim İçeriği

onurceran.com/lessons/ceranimo/3/soylemez-yapmaz

"Epostanın Birden Fazla Kişiye Gönderilmesi Durumunda Gizli (BCC) Kısmının Kulanılması" Davranışı

E-Posta Göndermek için Adres Satırındaki Bölümler Nelerdir?

“TO (Alıcı)” : Bu ifade bazı e-posta servislerinde **“Alıcı”** olarak bazı e-posta servislerinde orijinal ifadesi olan “To” şeklinde ifade edilmektedir. Yazılan bir e-postanın gönderilmek istediğini kişilerin mail adreslerini bu alana yazılmaktadır. Virgül ile ayırarak istenildiği kadar mail adresi yazılabilir. Bu alana yazılan e-posta adresleri yazılı mailin direkt olarak hitap edildiği kişilerdir.

“CC” : Karbon Kopya anlamında kullanılmaktadır. Bu alana “To” alanında gönderilen e-posta adreslerine ek olarak göndermek istenilen e-posta adresleri yazılır. Bu alana yazılan e-posta adreslerine de, yazılan e-posta adresi gönderilecektir. Bu alana yazılan e-posta adresleri, yazılı mailin direk muhatabı değildir. Bu alana yazılan e-mail adresindeki kişilere hitaben yazılmaz. Genelde bir mail’in “To” maillerinde bulunan kişilere gönderildiğine dair bilgi amaçlı gönderilir. Buraya yazılan mail adreslerini “To” alanındakiler de görür.

“BCC” : Gizli Karbon Kopya olarak adlandırılır. Kapalı Karbon Kopya olarak da bilinir. Bu alana yazılan e-mail adreslerine de gönderilmek istenilen yazılı mail iletilir. Bu alana yazılan e-mail adreslerini “To” ve “CC” alıcıları göremez. Bu alanı sadece gönderici ve bu alanda yazılı e-mail adres sahibi alıcısı görür. Ancak “BCC” alanına yazılan kişiler, “To” ve “CC”deki alıcıların kimler olduğunu görebilir.

Neden BCC Kullanmak İsteriz?

EK 16. Ölçeklendirilmiş Web Sayfası Örneği

EK 17. www.guvenliweb.org.tr Ekran Görüntüsü

GAZİLİ OLMAK AYRICALIKTIR