T.C.
İÇİŞLERİ BAKANLIĞI
JANDARMA VE SAHİL GÜVENLİK AKADEMİSİ
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ

SUÇ ARAŞTIRMALARI ANA BİLİM DALI

SİBER SUÇ KORKUSU VE ÖNLEM ALMA STRATEJİLERİ: TRABZON TEKNOKENT ÖRNEĞİ

HAZIRLAYAN

ELİF HANBAY

YÜKSEK LİSANS TEZİ

EYLÜL 2023


JANDARMA VE SAHİL GÜVENLİK AKADEMİSİ
İÇİŞLERİ BAKANLIĞI
1904

T.C.

İÇİŞLERİ BAKANLIĞI

JANDARMA VE SAHİL GÜVENLİK AKADEMİSİ

GÜVENLİK BİLİMLERİ ENSTİTÜSÜ

SİBER SUÇ KORKUSU VE ÖNLEM ALMA STRATEJİLERİ: TRABZON TEKNOKENT ÖRNEĞİ

YÜKSEK LİSANS TEZİ

SUÇ ARAŞTIRMALARI ANA BİLİM DALI

HAZIRLAYAN

Elif HANBAY

TEZ DANIŞMANI

Dr. Öğr. Üyesi Gülçin ORHAN

ANKARA-2023

Elif HANBAY tarafından hazırlanan "Siber Suç Korkusu ve Önlem Alma Stratejileri: Trabzon Teknokent Örneği" adlı tez çalışması aşağıdaki jüri tarafından OY ÇOKLUĞU ile Jandarma ve Sahil Güvenlik Akademisi Güvenlik Bilimleri Enstitüsü Suç Araştırmaları Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Başkan: J. Alb. Doç. Dr. Naci AKDEMİR _____

Jandarma ve Sahil Güvenlik Akademisi Güvenlik Bilimleri Enstitüsü Müdürü

Bu tezin, kapsam ve kalite olarak Yüksek Lisans olduğunu onaylıyorum.

Üye (Danışman): Dr. Öğr. Üyesi Gülçin Orhan _____

Jandarma ve Sahil Güvenlik Akademisi, Suç Araştırmaları Ana Bilim Dalı

Bu tezin, kapsam ve kalite olarak Yüksek Lisans/Doktora Tezi olduğunu onaylıyorum.

Üye: Dr. Öğr. Üyesi Muzaffer BİLGİN _____

Eskişehir Osmangazi Üniversitesi Tıp Fakültesi, Biyoistatistik Anabilim Dalı

Bu tezin, kapsam ve kalite olarak Yüksek Lisans olduğunu onaylıyorum.

Tez Savunma Tarihi: 21/09/2023

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

Doç. Dr. Naci Akdemir
J. Alb.
Enstitü Müdürü

ETİK BEYAN

Jandarma ve Sahil Güvenlik Akademisi Güvenlik Bilimleri Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında; tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi, tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu, tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi, kullanılan verilerde herhangi bir değişiklik yapmadığımı, bu tezde sunduğum çalışmanın özgün olduğunu, bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Elif Hanbay

21.09.2023

T.C.
İÇİŞLERİ BAKANLIĞI
JANDARMA VE SAHİL GÜVENLİK AKADEMİSİ
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ

SİBER SUÇ KORKUSU VE ÖNLEM ALMA STRATEJİLERİ: TRABZON TEKNOKENT ÖRNEĞİ

(Yüksek Lisans Tezi)

Elif HANBAY

Eylül 2023

ÖZET

Dijitalleşen toplumsal yaşam, bireylerin günlük yaşamlarında karşılaşmış olduğu birçok suç türünü siber dünyaya taşımaktadır. Dolayısıyla pek çok birey, siber suç mağduru olmaya yönelik korku duymakta ve birtakım önlem alma stratejileri geliştirmektedir. Dolayısıyla bu çalışmada, Trabzon Teknokent çalışanlarında çeşitli değişkenlere göre siber suç türlerine maruz kalma korkusu incelenmiştir. Buradan hareketle, Trabzon Teknokent'te görev alan 143 katılımcıdan anket yoluyla veri toplanmıştır. Toplanılan kategorik veriler, frekans ve yüzde olarak gösterilmiş olup gruplara göre kategorik değişkenler arasındaki farklılık karşılaştırmalarında beklenen değer sayısı 5 ve üzerinde olan ya da beklenen değer sayısı 5'in altında olan hücrelerin oranı %20'yi geçmeyen RxC tablolarda Pearson ki-kare, beklenen değer sayısı 5'in altında olan hücrelerin oranı %20'yi geçen RxC tablolarda ise Fisher Freeman Halton testi kullanılmıştır. Betimsel istatistik ışığında, katılımcıların çoğunun sosyal medya kullanıcısı olduğu, gününün önemli bölümünde internet ortamında vakit geçirdiği ancak internet ortamında kullandığı hesapların şifrelerini sıklıkla değiştirmediği belirlenmiştir. Ayrıca katılımcıların cihazlarında antivirüs programı haricinde kendilerini siber suç türlerinden koruyabilecek koruyucuları iyi düzeyde kullandıkları tespit edilmiştir. Yapılan analizlere göre katılımcılarda siber suç korkusunun mevcut olduğu; cinsiyet, medeni durum, yaş, eğitim durumu, algılanan ekonomik durum, meslekte çalışma yılı, görev alınan sektör, internete en çok hangi araçtan erişim sağlandığı, kamuya açık alanlarda kablosuz ağlara erişim sağlama, kullanılan şifrelerin benzerliği, sosyal medya hesaplarını başka sitelere erişim için kullanma ve antivirüs programı kullanma durumu ile çeşitli siber suç türlerine maruz kalma korkusu arasında anlamlı farklılık saptanmıştır. Bu çalışma katılımcılarının siber suç mağduru olmamak adına daha fazla önlem alma stratejileri kullanmaya ve desteklenmeye gereksinimleri olduğu düşünülmektedir.

Bilim kodu : 113001

Anahtar Kelimeler : Dijitalleşme, siber suç, önlem alma stratejisi, internet.

Sayfa Adedi : 151

Öğretim Üyesi : Dr. Öğr. Üyesi Gülçin ORHAN

T.R.

MINISTRY OF INTERIOR

GENDARMERIE AND COAST GUARD ACADEMY

SECURITY SCIENCES INSTITUTE

(M. Sc. Thesis)

Elif HANBAY

September 2023

ABSTRACT

Digitalized social life brings many types of crimes that individuals face in their daily lives to the cyber world. Therefore, many individuals fear being a victim of cybercrime and develop some prevention strategies. Therefore, this study examines the fear of being exposed to cybercrime types according to various variables among Trabzon Technopolis employees. From this point of view, data were collected from 143 participants working in Trabzon Technopolis through a questionnaire. The categorical data collected are shown as frequencies and percentages, and in the comparisons of the differences between categorical variables according to the groups, Pearson chi-square test was used in RxC tables with an expected value number of 5 or more or the ratio of cells with an expected value number below 5 does not exceed 20%, and Fisher Freeman Halton test was used in RxC tables with an expected value number below 5 exceeding 20%. In the light of descriptive statistics, it was determined that most of the participants are social media users, spend a significant part of their day on the internet, but do not change the passwords of the accounts they use on the internet frequently. In addition, it was determined that the participants used the protectors that can protect themselves from cybercrime types at a good level, except for the antivirus program on their devices. According to the analyses, there was a significant difference between gender, marital status, age, education level, perceived economic status, years of employment, sector of employment, the most common means of accessing the internet, accessing wireless networks in public areas, similarity of passwords used, using social media accounts to access other sites and using antivirus programs and the fear of being exposed to various types of cybercrime. It is thought that the participants of this study need to use more precautionary strategies and need to be supported in order not to be victims of cybercrime.

Science Code : 113001

Keywords : Digitalization, cybercrime, prevention strategy, internet.

Page Number : 151

Lecturer : Asst. Prof. Gulcin ORHAN

TEŞEKKÜR

Öncelikle bu tez çalışmasıyla ilgili her konuda her zaman kendisine rahatlıkla danışabildiğim ve kendisinden yardım alabildiğim değerli danışmanım Dr. Öğr. Üyesi Gülçin Orhan'a, yüksek lisans öğrenimim süresince beni her konuda cesaretlendiren, yönlendiren, desteklerini esirgemeyen çok kıymetli abim Dr. Öğr. Üyesi Yusuf Kurt'a ve yengem Öğr. Gör. Gülten Kurt'a, Bu çalışmanın başından sonuna her anında sabrıyla, özverisiyle ve tüm içtenliğiyle bana destek olan ve çalışmamı kolaylaştıran sevgili eşim Abdurrahman Hanbay'a ve aileme teşekkürü bir borç bilirim.

İÇİNDEKİLER

DÖRDÜNCÜ BÖLÜM: TARTIŞMA

BEŞİNCİ BÖLÜM: SONUÇ

ŞEKİLLERİN LİSTESİ

ÇİZELGELERİN LİSTESİ

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış simgeler ve kısaltmalar açıklamaları ile birlikte aşağıda sunulmuştur.

Simge	Açıklama
%	Yüzde
n	Kişi sayısı
p	Anlamlılık değeri
H_1	Alternatif hipotez

Kısaltmalar	Açıklama
JSGA	Jandarma ve Sahil Güvenlik Akademisi
TCK	Türk Ceza Kanunu
S.S.	Standart sapma
V.B.	Ve benzerleri

GİRİŞ

Suç ve sapma olguları, geçmişten günümüze dek varlığını sürdürmekle birlikte çok yönlü kavramlar olarak karşımıza çıkmaktadır (Burkay, 2008). Suç kavramının tanımı, toplumlara ve kültürlere göre farklılık göstermekle birlikte, en kısa ve net olarak söz konusu ceza yasalarını ihlal eden insan davranışı şeklinde tanımlanmaktadır. Yasalarla sınırlandırılmış olan davranışlar ve eylemlerin yanı sıra yazılı olmayan kurallara (normlara) aykırı davranılması da sapma olarak tanımlanmaktadır. Teknolojinin gelişimi ve yaygınlaşmış olması ile internet tabanlı uygulamaların yaşantımızın vazgeçilmez bir unsuru haline gelmesi beraberinde suç ve sapmanın kapsamını değiştirmiş, suça ve işlenme yöntemlerine farklı bir boyut kazandırmıştır (Cengiz, 2019; Şenol ve Karataşoğlu, 2022). Teknoloji alanındaki hızlı gelişmelerin bir sonucu olarak bilişim sistemlerinin mevcut süreçlere uyumu, bazı birey ve grupların suç işleme amacıyla teknolojiyi araç ve de amaç olarak kullanmasına yol açmış ve dolayısıyla günümüz modern toplumlarında siber suçlar ortaya çıkmıştır (Cengiz, 2021; Sürer, 2014).

Siber suçlar, nitelikleri ve ortaya çıkışları açısından geleneksel suç türlerinden önemli farklılıklar göstermektedir. Siber suçun ve siber suç türlerinin ortaya çıkması için öncelikli olarak teknolojinin gelişmiş olması ve teknoloji kullanımının yaygınlaşmış olması gerekmektedir (Karataşoğlu, 2022). Son yıllarda yapılan araştırmalardan elde dilen bulgulardan hareketle siber suçlar, bilgi ve iletişim teknolojilerinin ve bu teknolojilere erişilebilirliğin gün geçtikçe daha da kolay hale gelmesi ile birlikte, siber ortamda işlenen suçların görülme sıklığının hızla arttığı bir suç türü olarak karşımıza çıkmaktadır. Dolayısıyla siber suçlar, günümüz modern toplumlarının ve teknolojinin suçları olarak kabul görmektedir (Cengiz, 2019).

Bilişim sistemi, ekonomik, teknik ve toplumsal alanlardaki iletişimde kullanılan her türlü bilgi ve verinin elektronik makineler aracılığı ile düzenli bir biçimde işlenmesini; bilginin toplanmasında, depolanmasında ve işlenmesinde ağlar aracılığıyla iletilip hizmete sunulmasında kullanılan tüm teknolojileri kapsamaktadır. Bu bağlamda bilişim sistemi, bilgi ve verilerin işlenmesi bilimi olarak belirtilmektedir (be.gazi.edu.tr). Avrupa Konseyi Siber Suç Sözleşmesi'nin tanımlar başlıklı birinci maddesinde bilişim sistemi, var olan bilgi ve verilerin herhangi bir program aracılığıyla otomatik olarak işleme tabi tutulmasını sağlayan, toplu veya tek bir biçimde sistematik ve akılcı şekilde işlenmesi olarak ifade edilmektedir. Bilişim sistemlerinin verilerin işlenmesini, saklanması ve aktarılmasını sağlaması

bakımından en önemli unsuru olan bilgisayarlar ve bilgisayarlar haricinde bilişim sistemi olarak nitelendirilebilecek cihazlar mevcuttur. Bu bilgiler ekseninde bilişim suçları (siber suçlar), bir bilgisayarda ya da bilgisayar olarak nitelendirilmemesine karşın veri iletişimi sağlayabilmesi sebebiyle bilişim alanı dâhilinde değerlendirilen elektronik veya mekanik araçlar üzerinden veya bu araçlarla veri aktarımı amacıyla bağlantı kurulabilen soyut veya somut ağlar üzerinden işlenebilmektedir (Bilgi Teknolojileri ve İletişim Kurumu, 2022).

Siber dünya, insan yaşamını kolaylaştıran birçok imkâna sahip olmakla beraber bireylerin zarar görmelerine de neden olabilecek bir ortamdır. Bireylerin siber dünyada zarar görmelerine sebep olabilecek unsurlardan birisini siber suçlar oluşturmaktadır (Cengiz, 2021). Siber dünyanın imkânlarından faydalanan siber suç türlerinin değişim göstermesi sonucu siber dünyada işlenen suç türleri de çeşitlenmiş ve karmaşıklaşmıştır (Yılmaz, 2018). Günlük yaşantıda aktif ve yoğun şekilde teknoloji kullanımı, bireylerin çevrimiçi ortamda siber güvenliğinin korunması ve siber suç mağduriyetlerinin yaşanmaması amacıyla birtakım stratejiler geliştirmeyi gerekli kılmıştır. Siber tehditlerin farkına varılması, bu tehditlere karşı geliştirilen dijital güvenlik tedbirlerinin güncel olarak kullanılması ve alışkanlık haline dönüştürülmesi, siber ortamda mağduriyet yaşama riskinin azaltılmasında oldukça önemlidir (Bilgi Teknolojileri ve İletişim Kurumu, 2022).

Siber dünyada işlenen suçlar gün geçtikçe artmakla birlikte farklı şekillerde gerçekleştirilen siber suç türleri ortaya çıkmaktadır. Böylece internet ve teknoloji, yeni hukuki düzenlemeleri de gerekli kılan bir problem alanı olmaktadır (Aliusta ve Benzer, 2018). Türkiye Cumhuriyeti Anayasası'nın bireylerin hak ve özgürlüklerini taahhüt altına alan yükümlülükleri ile Avrupa Konseyi'nin Siber Suçlar Sözleşmesi'ndeki yükümlülüklerini yerine getirmek ve bu alanda işlenen suçlarla etkili bir şekilde mücadele edilebilmek amacıyla 5237 sayılı Türk Ceza Kanunu'nda siber suçlar ayrı bir başlık altında toplanarak detaylandırmıştır (Bilgi Teknolojileri ve İletişim Kurumu, 2022).

Gündelik hayattaki aktif ve yoğun teknoloji kullanımı sonucunda siber dünyanın bir parçası haline gelen bireyler, gerçek dünyada karşılaştıkları suçlara oranla, siber ortamda daha ciddi ve tehlikeli olabilen suçlarla karşılaşabilmektedir. Siber ortamda uzmanlaşan siber suçlular, profesyonel bir şekilde devletler, topluluklar ve gruplar için geleneksel suçlulardan daha geniş kapsamlı mağduriyetlere neden olabilmektedir. Buradan hareketle, gündelik yaşamda siber suçlar ve siber suç tehditleri ile bir arada yaşayan bireylerin siber suç mağduru olma korkusu yaşamaları son derece olağan kabul edilmektedir (Yılmaz, 2018).

Bireylerin ve dolayısıyla toplumun refahını olumsuz şekilde etkilediği genel kabul görmüş olan siber suç korkusunun incelenmesi önemli görülmektedir (Brands ve Van Wilsem, 2021; Doran ve Burgess, 2012). Dolayısıyla bu tez çalışmasında, Trabzon'da bulunan bir teknokent çalışanlarında çeşitli değişkenlere göre siber suç türlerine maruz kalma korkusunun incelenmesi amaçlanmıştır.

Araştırmanın temel soruları şu şekildedir:

1. Sosyodemografik değişkenlere göre siber suç türlerine maruz kalma korkusu anlamlı bir farklılık göstermekte midir?

2. Katılımcıların siber suç mağduru olmaktan korunmada önlem alma stratejileri kullanımı nasıldır?

Bu araştırmanın hipotezleri aşağıda sıralanmaktadır:

1. H_1: Kadın ve erkek katılımcılar arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve kadın katılımcıların siber suç türlerine maruz kalma korkusu, erkek katılımcılardan daha yüksektir.

2. H_1: Bekâr ve evli katılımcılar arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve bekâr olan katılımcıların siber suç türlerine maruz kalma korkusu, evli olan katılımcılardan daha yüksektir.

3. H_1: Yaş grupları arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve yaşça daha büyük olan katılımcıların siber suç türlerine maruz kalma korkusu, yaşça daha genç olan katılımcılardan daha yüksektir.

4. H_1: Eğitim düzeyi grupları arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve eğitim düzeyi daha yüksek olan katılımcıların siber suç türlerine maruz kalma korkusu, eğitim düzeyi daha düşük olan katılımcılardan daha yüksektir.

5. H_1: Algılanan ekonomik durumu grupları arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve algıladıkları ekonomik durumu yeterli olan katılımcıların siber suç türlerine maruz kalma korkusu, yetersiz olan katılımcılardan daha yüksektir.

6. H_1: Mesleki tecrübe düzeyi grupları arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve mesleki tecrübe düzeyi daha fazla olan katılımcıların siber suç türlerine maruz kalma korkusu, diğer katılımcılardan daha yüksektir.

7. H_1: Görev alınan sektör grupları arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve diğer sektörlerde çalışan katılımcıların siber suç türlerine maruz kalma korkusu, yazılım-bilişim sektöründe çalışan katılımcılardan daha yüksektir.

8. H_1: İnternete erişim sağlama grupları arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve internete en çok mobil cihazdan erişim sağlayan katılımcıların siber suç türlerine maruz kalma korkusu, diğer katılımcılardan daha yüksektir.

9. H_1: Kamuya açık alanlarda bulunan kablosuz ağlara erişim sağlayan ve sağlamayan katılımcılar arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve kamuya açık alanlarda bulunan kablosuz ağlara erişim sağlayan katılımcıların siber suç türlerine maruz kalma korkusu, erişim sağlamayan katılımcılardan daha düşüktür.

10. H_1: Kullandığı şifreler benzer olan ve benzer olmayan katılımcılar arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve kullandığı şifreleri birbirinin benzeri olan katılımcıların siber suç türlerine maruz kalma korkusu, benzemeyen katılımcılardan daha düşüktür.

11. H_1: Sosyal medya hesaplarını başka sitelere erişim için kullanan ve kullanmayan katılımcılar arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve sosyal medya hesaplarını başka sitelere erişim için kullanmayan katılımcıların siber suç türlerine maruz kalma korkusu, kullanan katılımcılardan daha yüksektir.

12. H_1: Antivirüs programı kullanan ve kullanmayan katılımcılar arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve antivirüs programı kullanan katılımcıların siber suç türlerine maruz kalma korkusu, antivirüs programı kullanmayan katılımcılardan daha yüksektir.

Bu araştırma, Trabzon Teknokent'te görev alan bireylerin siber ortamdaki güvenlik algılarının veya kendilerini ne derece güvende hissettiklerinin saptanması açısından önem teşkil etmektedir. Siber suç korkusu, bireylerin gündelik yaşantılarında ve siber etkinliklerinde herhangi bir korku, kaygı vb. hissetmeden ya da herhangi bir tehdit algısı olmaksızın özgür bir şekilde davranış göstermelerine engel olan bir olgudur. Öyle ki siber

suç korkusu ve siber suç mağduru olma riski, bireylerin sosyal ya da siber aktivitelerini önemli derecede etkileyebilmektedir. Bu bağlamda bu çalışma, Trabzon Teknokentte çalışan bireylerin siber suç korkularının ve bu korku ile ilişkili olan değişkenlerin ortaya konulması açısından önem taşımaktadır. Teknokentler, teknoloji ile internetin sıklıkla ve yoğun olarak kullanıldığı alanlardan olup, burada çalışan bireylerin siber suç korkusuna yönelik önlem alma stratejilerinin neler olduğunun belirlenmesi, yine bu çalışma kapsamında ele alınmaktadır. Böylece genel olarak iyi derecede eğitim seviyesine sahip olan ve gündelik yaşamlarının önemli bir bölümünde teknoloji ve internetle bir arada olan teknokent çalışanlarının çeşitli değişkenlere göre siber suç korkularının ve önlem alma yöntemlerinin belirlenmesi, benzer örneklemler hakkında da fikir yürütmeye ve stratejiler belirlemeye temel veriler sağlayabilecektir.

Bu araştırma, belli bir zaman noktasında Trabzon'da faaliyet gösteren bir teknokentten toplanılan verilerle, diğer bir ifadeyle ilgili veri toplama aracının katılımcılara sunulduğu tarihte Trabzon Teknokent'te aktif hizmet sunup bu araştırmaya katılmayı kabul etmiş olan katılımcıların verileri ile sınırlıdır. Örneklemin belirli bir ili, kurumu ve zaman noktasını temsil etmesi sebebiyle araştırma sonuçlarının diğer teknokentlerde görev yapan örneklemlere genellenmesi doğru olmayacaktır. Fakat çalışma sonuçları, benzer örneklemlerdeki mevcut durum hakkında fikir verebilecektir. Bununla birlikte, katılımcıların veri toplama aracını kendilerini yansıtan şekilde doldurduğu kabul edilerek elde edilen veriler yorumlanmış ve önerilerde bulunulmuştur. Ayrıca elde edilen sonuçlar, veri toplama araçlarının güvenilirlikleri ile sınırlıdır.

Bu tez çalışması, beş bölümden oluşmaktadır. İlk bölümde, suç ve siber suç kavramlarına, siber suç türlerine, Türk Ceza Kanunu'nda bilişim suçlarına, suç korkusuna, siber suç korkusuna ve siber suç korkusuna ilişkin önlem alma stratejilerine değinilmiştir. İkinci bölümde, araştırmanın metodolojisi aktarılmış olup; üçüncü bölümde, araştırma kapsamında toplanılan verilerin analizleri sonucunda elde edilen bulgulara yer verilmiştir. Dördüncü ve beşinci bölümlerde ise tartışma ile sonuç ve öneriler yer almaktadır.

BİRİNCİ BÖLÜM
ARAŞTIRMANIN KAVRAMSAL ÇERÇEVESİ

1.1. Suç Kavramı

Toplumsal bir varlık olarak yaşamını sürdüren insandan, toplumsal düzenin ve devamlılığın sağlanabilmesi için belirli kurallar çerçevesinde yaşaması beklenmektedir. Bu kurallar, düzenli ve güvenli bir yaşamı hedeflemekle birlikte, bazı durumlar ve şartlar altında ihlal edilen bu kurallar suç olarak ortaya çıkmaktadır. Tarihin her döneminde suç olarak değerlendirilen davranışlar görülmekte ve bu davranışı sergileyen bireyler belirli yaptırımlar ile karşılaşmaktadır (Burkay, 2008).

Suç, toplumsal değişimler içerisinde farklılık gösteren eski ve dinamik bir olgu olarak karşımıza çıkmaktadır (Burkay, 2008; https://magdurbilgi.adalet.gov.tr/298/Suc-Nedir). Suç olgusu topluma, zamana ve mekâna göre farklı anlamlar ifade edebilmektedir. Belirli bir zaman dilimi içerisinde suç olarak nitelendirilmeyen bir davranış, farklı bir zamanda suç olarak nitelendirilmekte veya herhangi bir toplumda suç olarak değerlendirilmeyen bir davranış, farklı bir mekânda ve toplumda suç olarak kabul edilebilmektedir. Bu bağlamda suça yönelik genel geçer bir tanım yapmak oldukça güçtür (https://magdurbilgi.adalet.gov.tr/298/Suc-Nedir). Üzerine birçok tanımlar yapılan suç kavramı; yasal, siyasal, sosyolojik ve psikolojik bakış açıları ile ele alınmaktadır (İçli, 2013). Yasal bakış açısına göre suç, sosyal düzenin devamlılığının sağlanması bakımından korunması gereken hukuki değerlerin bilinçli bir şekilde ihlalini (kast) veya bu değerleri korumaya yönelik oluşturulan kurallara karşı özensizliği (taksir) ifade eden insan davranışı olarak tanımlanmaktadır (https://magdurbilgi.adalet.gov.tr/298/Suc-Nedir; Şengül ve Kasap, 2013). Diğer bir ifadeyle suç, Türk Ceza Kanunu'nda (TCK) belirtilen, hukuka aykırı ve cezai yaptırımla sonuçlanan eylemlerdir (Esgin, 2019). Dolayısıyla yasal bakış açısına göre suç, ceza yasasını ihlal eden davranıştır. Siyasal bakış açısı ise suçu, etkin gruplar tarafından yasaya yerleştirilen ve istenmeyen davranışların gerçekleştirilmesi ile yasa dışı olarak etiketlenen olgu şeklinde açıklamaktadır (İçli, 2013). Sosyolojik bakış açısına göre suç, toplum değerlerini çiğneyen ve toplum düzenini bozan tüm fiil ve eylemlerdir. Diğer bir deyişle suç, toplumsal normları ihlal eden davranıştır. Bu bakış açısına göre suç, toplumsal bir olgu olarak değerlendirilmekte olup, yalnız yaşayan bir bireyin gerçekleştirebileceği bir eylem olarak görülmemektedir. Başka bir deyişle suçlu davranışlar, kendiliğinden meydana gelmemektedir. Sosyolojik bakış açısıyla suçun ortaya çıktığı alan

toplumsal yapı olmakla birlikte, toplumsal yapılar farklılık gösterdiğinden suçun niteliği de toplumdan topluma farklılaşmaktadır (Bingöl, 2022). Sosyolojik yaklaşımın temelinin, insan davranışlarının dinamik yönleri ve asosyal değişme ile bağlantılı olması sebebiyle suça yönelik açıklayıcı bir bakış açısı sunulmaktadır (İçli, 2013). Böylece her toplumda görülen, geçmişten günümüze değin varlığını sürdüren suç olgusu, mevcut hukuk düzenine aykırı bir fiil olarak tanımlanmakla birlikte, oluşum gösterdiği toplumlarda ekonomik ve psikolojik açıdan olumsuz etkiye neden olmaktadır (Şentürk ve Kasap, 2013).

Suç ve suçluluk üzerine başta biyoloji, psikoloji ve sosyoloji olmak üzere birçok bilim dalında çalışmalar yapılmıştır. Özellikle 18. yüzyılın sonlarına doğru geliştirilen teorilerle, suç ve suçluluğu açıklamaya yönelik çalışmalar hız kazanmıştır (Esgin, 2019). 1897 yılında oluşturulmaya başlayan "Sosyolojik Suç Teorileri"nin kurucuları arasında Emile Durkheim, Robert Ezra Park, Ernest Burgess, Cilifford Shaw, Walter Reckless ve Frederick Trasher yer almaktadır. Sosyolojik teoriler suçlu davranışını, sosyoloji bilimi temelinde ele almakta ve suçun sosyal boyutlarına dikkati çekmektedir. Suçlu davranışı açıklayan sosyoloji teorileri; Sosyal Yapı Teorileri, Sosyal Süreç Teorileri ve Çatışma Teorileri olmak üzere üç ana başlık altında toplanmaktadır. Her bir teori kendi içerisinde alt gruplara ayrılmaktadır. Sosyal Yapı Teorileri; Fonksiyonalist Teoriler, Alt Kültürel Teoriler, Sosyal Ekoloji Teorileri ve Gerilim Teorileri olmak üzere dörde ayrılmaktadır. Sosyal Süreç Teorileri ise Sosyal Öğrenme ve Davranış Teorileri, Kontrol Teorileri ve Etiketleme Teorisi olarak üçe ayrılmaktadır. Çatışma Teorileri ise kendi alt başlığında Marxist kriminoloji olarak açıklanmaktadır (Burkay, 2008; İçli, 2013).

Sosyal Yapı Teorileri, toplum düzeninin ve sosyal yapının suç olgusu ile arasındaki bağlantıya dikkat çekmektedir. Bu teoriler suçu, mevcut sosyal yapının bir sonucu olarak görmekte olup, suçun toplumsal sistemle bağlantısını ve bu sosyal yapının niteliklerinin neler olduğunu açıklamaktadır (İçli, 2013). Fonksiyonalist Teoriler, toplumsal düzen içerisinde suçun olağan ve işlevsel olduğunu kabul etmektedir. Fonksiyonalist Teorilerin öncü isimlerinden Durkheim'a göre suç, bir toplumda zorunludur, normaldir, fonksiyoneldir ve sosyal değişme için şarttır. Bir toplumda var olan suç olgusu, zorunlu değişiklikleri beraberinde getirmekle birlikte bu değişiklikleri doğrudan hazırlamaktadır (Durkheim, 1994). Gerilim Teorileri, birtakım temel değerler üzerinde toplumun aynı olduğu varsayımına dayanmakta olup toplumda büyük çoğunluğun aileler, kitle iletişim araçları, veya okullar aracılığıyla sosyalleştiğini dikkate alarak neden bazı bireylerin sapkın davranışlarda bulunduğunu açıklamaktadır. Kuralları ve yasaları ihlal eden bireylerin, bu

davranışlarını toplumsal koşullara bir tepki olarak gören bu teoriler, suçu toplumun sosyal organizasyonunun bir sonucu olarak değerlendirmektedir (Burkay, 2008). Robert K. Merton, Gerilim Teorilerinin önde gelen temsilcilerinden olmakla birlikte "Social Structure and Anomie" (1938) isimli makalesinde, bazı toplumsal yapıların belirli kişilere olan etkisini vurgulamıştır. O'na göre suç, içerisinde bulunulan toplumsal koşulların beraberinde getirdiği bir olgudur. Durkheim'in ortaya koyduğu anomi kavramını geliştiren Merton, Durkheim'ın düzen eksikliği veya uyulması gerekli kuralların eksikliği olarak tanımladığı anomi kavramını, kültürün belirlediği amaçlar ile bunlara ulaşmanın yasal yolları arasındaki uyuşmazlık olarak tanımlamıştır. Merton, Gerilim Teorisi'nde anomi kavramını bir değişken olarak kullanmıştır (İçli, 2014).

Merton ve Durkheim'in geliştirdikleri Anomi Teorisi, çocuk ve yetişkin suçluluğunun alt kültür teorilerine çerçeve oluşturmuştur. Alt kültür grupları, karşılıklı ihtiyaçlar nedeniyle bir arada bulunan, benzer değer ve fikirleri paylaşan bireylerden oluşmaktadır. Alt kültür teorileri, toplumda belli grupların veya alt kültürlerin suçu onayladığını veya suçun oluşumuna neden olan değerlere sahip olduklarını savunmaktadır. Bahsi geçen bu gruplarla etkileşime giren bireyler, zaman geçtikçe grubun sosyal değerlerine uyum göstermekte ve suçlu faaliyetler içerisinde yer almaktadırlar. Alt kültür teorileri kendi içerisinde bazı yönlerden farklılık göstermektedir. Bu farklılıklar, suçlu değerlere sahip olan gruplar, bu grupların kaynağı ve bu grupların bireyi etkileme yollarıdır (İçli, 2014).

Alt kültür teorileri kriminolojide, alt sınıf içerisinde bulunan genç erkekler arasındaki suçluluğun, özellikle ergen çetelerini tespit edebilmek ve açıklayabilmek amacıyla geliştirilmiştir. Alt kültür teorisyenlerine göre suça sürüklenen çocuk alt kültürü, diğer alt kültürler gibi hâkim kültürün üyelerinin karşılaşmadıkları problemlere tepki olarak ortaya çıkmıştır. Alt kültür teorileri konusunda yapılan çalışmalarda Albert Cohen, Cloward ve Ohlin gibi isimler ön plana çıkmaktadır. Albert Cohen, yapısal kaynakların sınırlı olması sonucu görülen gerginlik sebebiyle suçlu davranışın (özellikle alt sınıfta suça sürüklenen çocukların suç davranışı) ortaya çıktığını vurgulamıştır (Burkay, 2008).

Sosyal Süreç Teorileri, sapkın ve suçlu davranışların kuşaktan kuşağa öğrenme ve kültürel yollarla geçtiğini öne süren teorilerdir. Bu teorilerde etkileşim kavramı sıkça kullanılmaktadır. Sosyal Süreç Teorilerine göre suçlu ve sapkın davranışlar, kişiler arası etkileşimlerin bir sonucu olarak meydana gelmektedir. 1930'lu yıllardan günümüze kadar etkili olan bu teorilerin temel noktası, özellikle suçlu davranışın gruplar arası etkileşim ve

toplumsallaşma sürecinin bir sonucu olduğu görüşüdür. Suçlu ve sapkın davranışların, gruplar arası veya kültürel etkileşim sonucu meydana geldiğini ifade eden sosyal süreç teorilerinin en önemli kavramı, sembolik etkileşimciliktir (Güçlü ve Akbaş, 2019). Sembolik etkileşimcilik kavramı, toplumda bulunan değerlerin ve normların, bireyler veya gruplar arası anlamlı etkileşimler sonucu oluştuğunu ve insan davranışlarının bu etkileşimler ile açıklanabileceğini ileri süren teorik yaklaşımdır. Toplumsal ilişkileri gündelik yaşam bakımından inceleyen sembolik etkileşimciliğin bakış açısıyla Sosyal Süreç Kuramları suçu, sosyopsikolojik bakış açısıyla ele almaktadır. Özetle bu teoriler, bireyler ve gruplar arası etkileşimler sonucunda kişilerin nasıl suç işlediğine yoğunlaşmaktadır (Bingöl, 2022).

Suçu açıklayan sosyolojik suç teorilerinden bir diğeri Sosyal Çatışma Teorileridir. Sosyal Çatışma Teorileri, toplumda çatışma durumunda olan sınıfların bulunduğunu ve suçun, toplumdaki eşitsizlikler sebebiyle oluşan çatışma ortamından kaynaklandığını savunmaktadır. İlaveten çatışma teorileri suç tanımlarının göreliliği, ilgili kişilerin kontrolünde sosyal kurumların rolü ve hukukun bir güç aracı olarak yasama ve yürütme rolü üzerinde durmaktadır (İçli, 2013; Sheley, 1991). Sosyal Çatışma Teorileri, diğer bir deyişle Marksist Teoriler, suçu kapitalist ekonomi koşullarının bir ürünü olarak kabul eden determinist bir hipotezden hareketle oluşturulmuş olup suçu, sosyal adaletsizliklere yönelik bir tepki olarak kabul etmektedir (Dönmezer, 1994). Sosyal Çatışma Teorilerinin düşünsel kaynağı Ralf Dahrendorf'tur. O'na göre:

> Tüm toplumlar değişimle daima karşı karşıyadır.
>
> Sosyal çatışma toplumun her alanında mevcuttur.
>
> Toplumda var olan tüm unsurlar, toplumun değişimine hizmet eder.
>
> Tüm toplumlarda değişim, bir kısım üyelerin diğer üyelere uyguladığı baskı ile mümkündür (İçli, 2013).

Çatışma Teorileri, fikir birliği yaklaşımına alternatif bir yaklaşım olarak ortaya çıkmıştır (Sheley, 1991). Bu yaklaşıma göre, bir davranışa veya kişiye suçlu etiketi vurulmuşsa bunun bir nedeni bulunmaktadır. Eğer bu etiketler bahsi geçen kesimlere bağlı değil ise ilgiler değiştiğinde suça veya sapkınlığa yönelik tanımlar da değişmektedir. Bu durumda herhangi bir davranışın ahlaklı - ahlaksız, suçlu / sapmış veya normal şeklinde tanımı yeniden yapılabilir (İçli, 2013).

Çatışmacı Kuramlar için sosyal çatışma güçlü bir araçtır. Her kim hukuka sahipse güce de sahiptir. Dolayısıyla hukukun bir güç aracı olduğu açıktır. Eğer yasalar, güçlü çıkar

gruplarının toplum içindeki konumlarını güçlendirmek için kullanılıyorsa ve belli davranışları yasaklıyorsa suç, çıkar gruplarının tanımlamalarına göre şekillenmektedir (Siegel, 1989). Çatışma Kuramlarına göre, gücün eşitsiz dağılımı çatışmayı yaratmaktadır. Bu kuramlara göre suç olgusu, gücü elinde bulunduran bireyler veya gruplar tarafından tanımlanmıştır. Yasaların kültürel olarak göreli olmasının yanı sıra doğru ile yanlışın kesin bir tanımı yoktur (İçli, 2013).

Marxist Kuramcılar ise suçlu davranışın açıklanmasında Marx'ın iki temel görüşünü kullanmıştır. İlk görüş, iş ve toplumsal yaşamda verimliliğin insan doğasının temeli olması ve sanayileşen kapitalist toplumlarda, yeterli düzeyde çalıştırılmayan insanlar ile çok sayıda işsiz insanın demoralize olmasıyla verimsiz hale gelmeleridir. Dolayısıyla bu kişiler, bütün suç türlerinin ve ahlaksızlığın öznesi durumuna gelmektedir. İkinci görüşte ise Marx, eşit olmayan kaynak dağılımının toplumda gücün de eşitsiz dağılımına neden olduğunu vurgulamıştır. Bu durumda varlıklı olmayan bireyler güçsüz olmakta, varlıklı olan bireyler ise gücü elinde bulundurarak toplumun geriye kalan kesimini kendi istekleri doğrultusunda kontrol edebilmektedir. Dolayısıyla Marx'a göre suç, toplumsal düzene karşı bilinçli olarak yapılan bir şiddet eğilimi olarak görülmemekte, yalnız bırakılan kişilerin hâkim olan şartlar karşısındaki mücadelesi olarak değerlendirilmektedir (Akpınar, 2018).

On dokuzuncu ve yirminci yüzyılın başlarında araştırmacılar, suç ve suçluluğun nedenlerini araştırırken insan bedenini ön planda tutmaktaydı (İçli, 2013). Freud ise insanların tüm davranışlarını yönlendiren etkenin, ilk çocukluk döneminde oluşan bilinçaltı olduğunu ifade etmiştir. Bu bağlamda bireylerin yalnızca biyolojik varlık olmadığını, içsel dinamiklerini şekillendirebilen psikolojik bir varlık olarak da değerlendirilmesi gerektiğini ortaya koymuştur (Bingöl, 2022). Yalnızca suç olgusu açısından değil, insan davranışlarının açıklanmasında da önemli katkılarda bulunan psikolojik yaklaşımların temelini oluşturan psikanalitik yaklaşıma göre insan, kendi içerisinde çelişkili noktaları bulunan, karmaşık karar verme yetisine sahip bireyi temsil etmektedir. Psikanalitik yaklaşımın temelini oluşturan Freud'a göre benlik, kendi içerisinde farklı ve birbirine karşıt unsurlardan oluşmaktadır. Bu yaklaşıma göre insan davranışının anlaşılabilmesi için yalnızca bilince değil, kişiliğimizin oluşumunda önemli etkileri olan bilinçdışına da odaklanılması gereklidir. Buradan hareketle Freud benliği; id, ego ve süperego kavramları üzerinden incelemektedir. İd, bireyin güdülerinin kaynağı olan temel arzularının olduğu kısımken; ego, benliğin mantıklı tarafını oluşturmaktadır. Genellikle ego, bireylerin isteklerini gerçekçi bir biçimde

nasıl elde edeceğini söylemektedir. Benliğin üçüncü kısmı olan süperego ise bireylerin arzu ve isteklerinden çok, ahlaki olan davranışları temsil eden bir rehber bölümüdür (İçli, 2013).

Freud'un yaklaşımına göre suçlu davranışın kaynağı, bireyin isteklerini ve davranışlarını sınırlandıran kuralları içselleştirme aşamasında yaşanılan dengesizliklerdir. Bu dengesizliklerin, suçlu davranışın ortaya çıkışında rolü olan ilk etken olmasının temel nedeni, zayıf bir süperegonun var oluşudur. Bireylerin uyması gereken temel kuralları ve nasıl davranması gerektiğine yönelik içsel bölümü oluşturan süperegonun zayıflığı, cinsel suçlar ve cinayet gibi şiddet suçlarını beraberinde getirmektedir. Aşırı gelişmiş bir süperego da bireylerin suç işlemesine yol açabilmektedir. Öyle ki bazı insanlar, cezalandırılma arzularından ötürü suç işlemektedir. Aşırı gelişmiş süperegoya sahip olan birey, istediklerini gerçekleştirdiğinde bu eylemi neden yaptığını sorgulamakta ve dolayısıyla kendisini suçlamaktadır. Birey, kendisini yaptıklarından dolayı suçlu hissettiği ölçüde süperego da o ölçüde cezalandırılmasını talep etmektedir. Böylece aşırı süperegonun yol açtığı cezalandırılma arzusu, suç davranışı ile sonuçlanmaktadır (Gökulu, 2019).

Freud yaklaşımında suç olgusu üzerine doğrudan açıklama yapmamış olsa da davranışları yönlendiren bir olgu olarak insanın temel içgüdülerinin bulunduğunu ve bu içgüdülerle kontrol etme ya da edememe durumlarının sapma davranışlarının ortaya çıkmasına neden olduğunu ortaya koymuş ve görüşleri, suça yönelik psikolojik açıklamaların ortaya çıkışında etkili olmuştur (İçli, 2013). Yine Freud'a göre saldırganlık ve şiddet, insanın doğasında bulunan temel içgüdülerdir. Freud, neredeyse tüm çalışmalarında nevrotik çatışmaların nedenini cinsellikle açıklarken, saldırganlık içgüdüsünü psikoseksüel gelişim süreci içerisinde değerlendirmiştir. Freud, daha sonraları saldırganlığı tepkisel açıdan inceleyerek bireyin kendini koruma içgüdüsü ile değerlendirmiştir. Bireyin doyuma ulaşmasını engelleyen veya bireyi tehdit eden durumlarda tepki göstereceğini belirterek bu tepkileri saldırganlık olarak açıklamıştır. Daha sonraki dönemlerde Freud saldırganlığı, tamamen biyolojik bir içgüdü olarak değerlendirmiş ve daha katı bir model oluşturmuştur (Başeğmez ve Özerk, 2021). Buna göre psikanalizin temel kavramları ve ilkelerinde insanlığın temelinde var olduğu savunulan iki temel içgüdü bulunmaktadır. Cinsellik (eros) olarak adlandırılan içgüdü, yaşamsal süreçleri korunmasını ve neslin devamlılığını sağlayan içgüdüdür. İkincisi olan ölüm içgüdüsü (thanatos) ise var olmama durumuna dönme eğilimidir. Buna göre tüm insanlar, bilinçdışı olarak ölüm içgüdüsü tarafından yönlendirilmektedir(https://acikders.ankara.edu.tr/pluginfile.php/133623/mod_resource/content/1/%2803%29%20Freud%20ve%20Psikanaliz.pdf).

İkinci Dünya Savaşı sonrası ve devam eden süreçte, ABD başta olmak üzere dünya genelindeki devletlerde gerek kamusal alanda gerekse bireylerin özel yaşantılarında ve yaşam tarzlarında öngörülemeyen değişimler ve dönüşümler oldukça hızlı bir biçimde yaşanmaya başlamıştır. Toplumsal yaşamdaki bu değişimler, beraberinde çeşitli sorunları da meydana getirmiştir. Bunlardan birisi, suç oranlarındaki artıştır. Suça sebebiyet veren aktörlerde herhangi bir değişiklik olmadığı halde suç oranlarındaki artışın kaynağı sorgulanmış ve bu noktada farklı bir suç mekanizmasının olabileceğine dikkat çekilmiştir (Birceviz, 2019). Suç, aslında her dönemde ve toplumda çeşitli nedenlere odaklanılarak açıklanmaya çalışılmıştır. Bin dokuz yüz kırklı yılların öncesinde oluşturulan suç teorileri, suçun kaynağını insan genetiğinde, doğaüstü güçlerde ve bireylerin cezadan kaçma amacıyla yapmış olduğu rasyonel tercihlerde aramıştır (Fidan ve Uludağ, 2023). Ortaya atılan Rasyonel Tercih Teorisi, bireylerin suç işleme kararının bir tercih sonucu alındığını açık bir şekilde ifade etmiş olsa da suçluların karşılaşması mümkün olan suç senaryolarının ya da suçlu davranışa yönelik tercihlerinin neler olacağını belirleyememesi sebebiyle suçlu davranışı açıklanmada yetersiz kalmıştır (Cullen ve Agnew, 2003). Cohen ve Felson yapmış oldukları çalışmada, ilk defa suç mekanizması üzerinde durmuşlar ve bu mekanizma ile suçun engellenebileceğini savunmuşlardır (Cohen ve Felson, 1979). Bu yeni yaklaşım, yani Rutin Aktiviteler Teorisi, sosyal hayatın değişmesi ile birlikte aşırı derecede artan suç olaylarının açıklamasını tartışmış; hayatın olağan akışı içinde mağdurların ve suçluların var olan günlük rutinlerinin suç sayısındaki artışın sebebi olduğu savunmuştur (Birceviz, 2019). Rutin Aktiviteler Teorisi ayrıca bireylerin karşısına çıkan suç fırsatlarındaki değişimi de daha net bir biçimde açıklayabilme özelliğine sahip görünmektedir (Cullen ve Agnew, 2003).

Rutin Aktiviteler Teorisi, zaman ve mekân uzamında insanların gündelik yaşamlarındaki sosyal faaliyetlerin, suça eğilimli bireylerin niyetlerini kolaylaştırıcı bir mekanizma haline nasıl dönüştüğünü ifade etmektedir. Önceki suç teorilerinde zaman, suç olayına etki eden bir kavram olarak düşünülmemiştir. Rutin Aktiviteler Teorisi ile mekân faktörünün yanına zaman faktörü de eklenerek suç daha kapsamlı olarak incelenmeye başlanmıştır (Cohen ve Felson, 1979). Rutin Aktiviteler Teorisi'ndeki zaman faktörünün temelinde, Amos Hawley'in 1950 yılında ortaya koyduğu İnsan Ekolojisi Teorisi bulunmaktadır. Hawley, bu teorisinde toplum yaşamının zamansal boyutlarını üç farklı boyutta incelemiştir. Bu üç boyut ritim, tempo ve zamanlamadır. Ritim, bir yerden bir yere gidiş gelişleri ve sosyal olayın ne zaman meydana geldiğini; tempo, birim zamanda ortaya

çıkan olay sayısını; zamanlama ise aslında birbirinden bağımsız olan faaliyetlerin ne kadar sistematik ve benzer şekilde meydana geldiğini ifade etmektedir (Clarke ve Felson, 2004).

Rasyonel Tercih Teorisi'nin aksine Rutin Aktiviteler Teorisi suçun unsurlarını da araştırmış ve bu unsurları uygun hedef, motive olmuş suçlu ve koruyucuların yokluğu olarak belirlemiştir. Sonraki dönemlerde teoriye, motive olmuş suçlunun engellenmesini sağlayan tutucular unsuru eklenmiştir. Bu bağlamda Rutin Aktiviteler Teorisi, suç olgusunu her açıdan incelemek ve açıklayabilmek maksadıyla suçun ne şekilde, nerede ve ne zaman meydana geldiğine odaklanan bir özellik taşımaktadır (Felson ve Eckert, 2018).

Yukarıda da belirtildiği üzere Rutin Aktiviteler Teorisi, suçun sıradan veya gündelik yaşamın (iş hayatı, aile hayatı, boş zaman aktiviteleri vb.) rutinlerinden kaynaklı oluşan fırsatların bir sonucu olduğunu ifade etmektedir. Suç, rastgele bir yöntemle değil, yukarıda belirtilen üç temel faktörün bir araya gelmesiyle ortaya çıkan fırsatların sonucunda oluşmaktadır (John ve Tierney, 2009). Yani suçun oluşabilmesi için suça eğilimi olan ve bu eğilimi gerçekleştirebilecek olan bir suçlu, bu suçluya uygun hedefi oluşturan bir kişi veya nesne, bu suçun gerçekleşmesini önleyebilecek olan koruyucuların yokluğu ve motive olmuş suçlunun engellenmesini sağlayan tutucular bir arada olması gereken unsurlardır (Cohen ve Felson, 1979; Felson ve Eckert, 2018).

Bir nedenle motive olmuş ve suç işleyebilecek durumda olan herhangi birisi, potansiyel suçlu olarak tanımlanmaktadır. Bu bağlamda potansiyel suçlu, gerçekleşmesi muhtemel suç için kendisine uygun hedef belirlemektedir. Yeterli koruyucuların olmaması durumunda ise hedefine yönelik suç eylemini gerçekleştirebilmekte ve mağduriyet durumu oluşabilmektedir (Fidan ve Uludağ, 2023). Rutin Aktiviteler Teorisi'ne göre, çoğu birey potansiyel suçlu olarak kabul edilmekte ve henüz suç işlememiş olanların önlerine suç işleyebilmek için gerekli fırsatların çıkmadığı değerlendirilmektedir. Sosyal aktivitelerin zamansal ve mekânsal birlikteliğinin bireylerin suça yönelik eğilimlerini gerçekleştirmesine yardımcı olduğu kabul edilmiş olup, potansiyel suçluların uygun fırsatlarla birlikte gerçek suçluya dönüştüğü savunulmaktadır (Felson,1998). Bu bağlamda, Zipf'in (1950) "En Az Çaba Prensibi" Rutin Aktiviteler Teorisi'ni açıklamaya yardımcı olmaktadır. Bu prensibe göre, insanlar elde etmek istedikleri şeyler için en az emek ve çaba göstermek istemektedir. Böylece suçlular da suç işlemek için gidebilecekleri en yakın yerler veya güzergâhlar üzerindeki hedefleri seçmektedir. Bu durumda suçluların yoğun bulunduğu bir mahalden veya onlara yakın bir yerden geçiliyorsa, üstelik koruyucular da yoksa suç mağduru olma

ihtimali yüksektir. Zipf'in ikinci prensibine göre de insanlar, bir konu üzerine fazla düşünmeden, mevcut bilgilere göre hareket etmektedirler. Öyle ki motive olmuş suçlular, yollarının kesiştiği ve koruyuculardan yoksun ilk hedef üzerinde suç fiilini gerçekleştirmektedir. Dolayısıyla Rutin Aktiviteler Teorisi'nin Zipf'in prensiplerinden etkilendiğini söylemek mümkündür. Ancak uzun zaman tasarlanarak ve oldukça emek harcanarak işlenen suç fiillerini açıklama konusunda Zipf'in prensiplerinin yetersiz kaldığı söylenebilir (Felson,1998).

Rutin Aktiviteler Teorisi'ne göre bir suçun meydana gelebilmesi için gerekli olan ikinci unsur, uygun bir hedeftir. Uygun hedef, motive olmuş suçlunun bir suçu işleyebilmek amacıyla uygun görüp belirlediği eşya, kişi veya nesne gibi bir hedeftir. Suçlular için bir hedefi uygun yapan şey, o hedefi çekici yapan unsurlardır. Cohen ve Felson (1979) uygun hedefin bileşenlerini değerli, görünür, erişilebilir, koruyuculardan yoksun olması ve hareket kabiliyeti unsurlarıyla açıklamıştır. Günümüzde sıkça kullanılan dizüstü bilgisayarlar, cep telefonları gibi ürünler, özellikle hırsızlık bağlamında düşünüldüğünde, taşıması kolay ve maddi değeri yüksek olduğundan uygun hedef olarak düşünülebilir (Birceviz,2019; Yılmaz, 2018).

Rutin Aktiviteler Teorisi'ne göre bir suçun gerçekleşebilmesinde gerekli üçüncü unsur, koruyucunun yokluğudur. Koruyucu kavramı ile ifade edilmek istenen şey, uygun bir hedef olarak belirlenmiş kişi veya nesneyi, motive olmuş suçludan koruyabilecek olan güvenlik görevlisi, yakın çevre veya alarm sistemi ya da güvenlik kamerası gibi ögelerdir. Koruyucular aracılığıyla bir suçun meydana gelmesinin önlenmesi, koruyucu unsurların fiziksel olarak var olmaları ile veya bir çeşit doğrudan müdahaleler ile gerçekleşebilmektedir (Cohen, Felson ve Land, 1980). Suç mağduru olma ihtimalinin en az olduğu alan, koruyucuların bulunduğu ortamlardır (Yılmaz, 2018).

Felson (1986,1995), Rutin Aktiviteler Teorisi'nde ifade edilen motive olmuş suçlu, uygun hedef ve hedefi suça karşı koruyabilecek olan koruyucuların yokluğu üçlüsünde, suçluları motive eden unsurun ne olduğunun veya suçlu davranışı engelleyebilecek faktörlerin varlığının dikkate alınmadığını vurgulayarak suçluları, suç işlemekten caydıracak olan koruyucular harici engelleyiciler üzerine yoğunlaşmıştır. Felson engelleyicilerin, Rutin Aktiviteler Teorisi'nde var olan üçlü yapıya dördüncü unsur olarak eklenmesi gerektiğini ifade etmiştir. Felson, Hirschi'nin Kontrol Teorisi'nden yola çıkarak yakın çevresine, sevdiklerine ve topluma bağlılığı güçlü olan bireylerin yakın çevrelerinin etkisiyle suç

işleme olasılığının azalacağı görüşünü, yani Engellenmiş Suçlu Yaklaşımı'nı savunmuştur. Bu yaklaşımda, bireyi yakından tanıyan çevresi tarafından tutulacağı, dolayısıyla suç işlemekten vazgeçirileceği ileri sürülmektedir (Felson, 1986). Bu yaklaşım ile Felson suçun, bireyin tutulması ile önlenebileceğine işaret etmektedir. Bahsi geçen düşünce ile suçlular, motive olmuş suçlu kategorisinden çıkartılarak, suç işlemesi muhtemel suçlu olarak değerlendirilebilmektedir. Motive olmuş kategorisindeki suçluların belli bir kararlılıkta suç işleme azmi varken, suç işlemesi muhtemel suçlu kategorisinde suç işleme ihtimali azalmış bir profil ortaya konmaktadır (Boeting, 2016).

1.2. Siber Suç Kavramı ve Siber Suç Türleri

İnternet teknolojisi ve internet tabanlı uygulamalar günümüzde toplumsal yaşamın bir parçası haline gelmiş olup, bireylere özgürlük vaat eden ve gündelik yaşantıyı kolaylaştıran bileşenler olarak görülmeye başlamıştır. Manuel Castells'in "ağ toplumu", Urlic Beck'in ise "risk toplumu" olarak adlandırdığı ve günümüz toplumlarında bazı belirsizlikler, tehditler ve güvensizlik ortamlarının ortaya çıktığı yönündeki görüşler, gelişen bilişim teknolojileri karşısında dikkatli olunması gerektiğini ortaya koymuştur (Sunay ve Birel, 2023). Öyle ki teknolojinin gelişimi ile beraber internet erişimli elektronik cihazların artışı ve yaygınlaşan internet ve internet tabanlı uygulamaların kullanımı, hayatı kolaylaştırma adına sağladığı imkânların yanı sıra güvenlik boyutunda yeni endişelerin meydana gelmesine sebep olmaktadır. Gelişen teknolojiyle birlikte farklı suç türleri de ortaya çıkmıştır (https://internet.btk.gov.tr/turkiye-de-bilisim-hukuku). Mağdurla fiziksel temas olmadan veya mağdurla aynı yerde bulunmaya gerek olmaksızın hırsızlık veya dolandırıcılık gibi suçları işlemek mümkün hale gelmiştir (Hekim ve Başıbüyük, 2013). Yeni bir suç türü olarak siber suçların, Türkiye'de bilişim suçu şeklinde kullanımına sık rastlanırken; dünya genelinde bilgisayar suçları, dijital suçlar, elektronik suçlar gibi çeşitli kullanımları olduğu görülmektedir. Siber suç kavramı literatürde farklı tanımlamalarla karşımıza çıkıyor olsa da bu kavramların ortak noktası, bilişim sistemleri veya elektronik ağlar aracılığı ile işlenen suçlar olmalarıdır. Bu yeni suç türünde tehdit unsuru olarak bilgisayarlar, virüsler ve zararlı yazılımlar kullanılmaktadır (Karataşoğlu, 2022).

Henüz Türkçe bir karşılığı olmayan ve İngilizce bir kelime olan "cyber" kelimesinin Türkçe'ye "siber" olarak çevrilmesinin sebebi, siber sözcüğüne gelişim aşamasında yüklenen dönemsel ve kültürel anlam bütünlüğüdür. Sanal gerçeklik, bilgisayar ağlarına ve internete ait olan anlamlarına gelen siber kavramı iletişim teknolojilerinin, bilgisayarların ve

sanal gerçekliğin kültürü ile bağlantılı olarak tanımlanması sebebiyle geniş bir alanı kapsamaktadır ve internet aracılığı ile gerçekleştirilen geleneksel suçları bünyesinde bulundurmaktadır (Avşar ve Öngören, 2010; https://www.nedir.com/siber; Küçükvardar, 2018). Siber suç kavramını, internet veya ağ yapılarına bağlı bilgi ve iletişim teknolojilerini kullanan bireylerin ve sistemlerin, sistem içerisinde mevcut dataların ve ağ - sistem güvenliklerinin hedef veya araç olarak kullanılması ile gerçekleştirilen hukuka aykırı eylemler olarak tanımlamak mümkündür (https://www.egm.gov.tr/siber/sibersucnedir; Suveren, 2019). Literatürde farklı tanımlamaları olan siber suç kavramı, bilgi teknolojileri kullanılarak gerçekleştirilen her ihlal için kullanılabilirken, yasayı ihlal eden ve o sebeple mahkumiyet cezası verilen bir eylem olarak da tanımlanabilir (Saini, vd., 2012). Marcum ve Higgins (2019) "cybercrime" isimli çalışmasında "melez suçlar" olarak tanımladığı siber suçları, fiziksel dünyada var olan suçlu davranışların siber ortamda işlenmeye başlaması olarak tanımlamıştır. Dolayısıyla siber suç kapsamında yeni suç türleri yer alabileceği gibi geleneksel suç davranışları esnek teknolojiler kullanılarak yeniden biçimlenebilmekte ve siber ortamda daha kolay işlenebilmektedir. Bu suçların bireylerin özel yaşam gizliliğini ihlal etme (dinleme, gözetleme, hesap veya bilgisayarları hacklemek), taciz, propaganda ve yalan haber yayma gibi manevi boyutları olabileceği gibi, dolandırıcılık ve kredi kartından para çekme gibi malvarlığına yönelik boyutları da olabilmektedir (Sunay ve Birel, 2023).

Siber suçlar, gelişime ve değişime en açık olan suçlardır. Öyle ki küreselleşen dünyada, yeni bir teknolojik gelişme hızlıca tüm dünyaya yayılmakta ve dolayısıyla gelişen teknoloji ile yeni siber suç türleri ortaya çıkmaktadır (https://internet.btk.gov.tr/turkiye-de-bilisim-hukuku). Bin dokuz yüz seksenli yıllardan sonra bilgisayar ve internet kullanımının yaygınlaşması sonucu ortaya çıkan siber suçların küresel ekonomiye maliyeti tahmini olarak milyarlarca doları bulabilmektedir. Siber suçların sadece ekonomik kayıp değil, çok yönlü olumsuz etkileri bulunmaktadır. Bu duruma örnek olarak, herhangi bir kuruluş, siber saldırı sonucu siber güvenlik eksiklikleri sebebiyle önemli derecede veri kayıpları yaşayabilirken, devletler de siber suçluların siber casusluk ve siber terörizm gibi faaliyetleri sebebiyle büyük çaplı zararlarla karşılaşabilmektedir (Küçükvardar, 2018; Yılmaz, 2018).

Siber suçların gündelik yaşantıdaki yıkıcı etkileri, çeşitli yönleriyle düzenlenmesini ve sınıflandırılmasını gerekli kılmıştır. Fakat siber uzayın hızla yenilenmesi ve gün geçtikçe daha fazla kullanıcı sayısına ulaşması sonucunda yeni ihlal yöntemlerinin ortaya çıkması, siber suçları sınıflandırma çalışmalarındaki zorlukları beraberinde getirmiştir. Siber suçların sınıflandırılması ile ilgilenen kimi uzmanlar siber suçları iki, üç ya da dört ana başlık altında

incelemektedir (Turhan, 2006). Yine siber suçlar, dar anlamda siber suçlar ve geniş anlamda siber suçlar şeklinde iki alt grupta da değerlendirilmektedir. Bu bağlamda siber suçların kendisine özgü suçlar olmasını sağlayan ayırt edici özelliği, işlenme yöntemleridir. Klasik suçlarda, suçun maddi unsurunu oluşturan eylemler faillerin fiziksel eylemleri ile meydana gelmekte iken siber suçlarda çoğunluklu olarak bilgisayarın klavyesine dokunulması dışında herhangi bir somut hareket olmamaktadır. Ancak siber suçlarda fiziksel eylemler sonucu oluşabilecek zararlardan çok daha fazlası oluşabilmektedir. Bu duruma ek olarak siber suçlar, klasik yöntemlere oranla daha hızlı, basit ve gözlerden uzak şekilde işlenebilmekle birlikte tespit edilebilmesi de daha zordur (Avşar ve Öngören, 2010). Siber suç faillerinin teknik bilgi ve donanıma sahip olduğunun altını çizen Turrini ve Gosh, siber suçları beş kategoride değerlendirmiştir. Bu kategoriye göre siber suçlar; güvenlik duvarlarının ihlali, zararlı yazılım üretme, hizmeti engellemeye yönelik saldırılar, dijital korsanlık ve diğer suçlar şeklindedir. Bu sınıflandırmaya benzer olarak literatürdeki çalışmalarda bilgisayar sistemleri ile işlenen klasik suçlar ve bilgisayar sistemlerine yönelik suçlar başlıklarını kullanan sınıflandırmalara rastlanılabilmektedir (Akman, 2020). İki bin yedi yılında Avrupa Komisyonu yeni bir sınıflandırma yaparak siber suçları elektronik ağlar vasıtasıyla işlenen klasik suçlar, elektronik medya üzerinde yayınlanan yasa dışı içeriğe ilişkin suçlar ve elektronik ağlara has suçlar şeklinde üç kategoriyle incelemiştir (EC, 2007). Birleşmiş Milletler ise siber suçları ifade ederken dört başlıklı bir sınıflandırma yapmıştır. Bu sınıflandırmayı, bilgisayar verilerinin ve sistemlerinin gizliliğine, bütünlüğüne ve kullanılabilirliğine karşı işlenen suçlar, bilgisayarla ilgili suçlar, içerikle ilgili suçlar ve telif hakkı ve ilgili hakların ihlali ile ilgili suçlar oluşturmaktadır (UNODC, 2020). David Wall, 2001 yılında siber suçlar hakkında yapmış olduğu çalışmasında siber suçları dört kategoriye ayırmıştır. Bunlardan ilki, izin olmadan giriş yoluyla zarara neden olmaktır. Hackleme, tahrif ve virüsler buna örnek verilebilir. Bir diğeri, siber aldatma ve hırsızlıklar, kredi kartı dolandırıcılığı veya fikri mülkiyet ihlalleri (korsanlık) gibi suçlardır. Diğer bir kategoride siber pornografi yer almaktadır. Son kategori ise siber şiddettir. Başka bir ifadeyle, başkalarına psikolojik veya fiziksel zarar verme, nefret söylemi veya taciz gibi kişinin korunmasına yönelik yasaların ihlal edilmesidir (Hatipoğlu ve Tunacan, 2021). Uluslararası Telekomünikasyon Birliği (ITU) siber suçları dört alt başlık içerisinde gruplandırmıştır:

1. Bilgisayarlarda mevcut verilerin ve sistemlerin kullanılabilirliği, gizliliği ve bütünlüğüne yönelik işlenen suçlar (yasal olmayan yöntemlerle veri hırsızlığı, verilerin değiştirilmesi ve verilere müdahale edilmesi),

2. Bilgisayar ile ilgili suçlar (kimlik hırsızlığı, dolandırıcılık, virüs yayma vb.),
3. Telif hakkı ile ilgili suçlar,
4. İçerikle bağlantılı suçlar (yalan haber, ırkçılık, müstehcen içerikli yayın satmak, şiddet ve nefret söylemleri) (Bilgi Teknolojileri ve İletişim Kurumu, 2022).

Siber suçlar, işlenme amaçları açısından klasik suçlarla benzerlik gösteriyor olsa da işlenme yöntemi veya aracı bakımından farklılıklar barındırmaktadır. Siber suçların işlenmesinde araç olarak bilgisayar, internet, pos makinesi, cep telefonu gibi teknolojik cihazlar kullanılması, siber suçları klasik suçlardan büyük ölçüde farklılaştırmaktadır. Siber suçlar, herhangi bir fiziksel ortama gereksinim duyulmadan herhangi bir internet ağı veya bilgisayar aracılığıyla dünyanın herhangi bir konumunda işlenebilmekte; kişi, kurum ve kuruluşlara büyük zararlar verebilmektedir. Siber suçların tamamına yakını, birtakım yöntemlerden biri veya birkaçının sentezi şeklinde meydana gelmektedir. Siber suç failleri, suçlu davranışın gerçekleştirilmesinde birden çok yöntem ve tekniği bir arada kullanabilmektedir (Ehliz, 2019).

Siber suçlar genellikle bünyesinde birtakım unsurları barındırmaktadır. Bu unsurlar, aşağıda sıralanmıştır:

1. Web sitelerinin ana sayfalarını silmek, istenilen yere yönlendirmek, sayfanın yapısı ile oynamak,
2. Erişime açık sitelerdeki içeriğe erişim sağlayarak veri kopyalama ile verileri çalmak, bilgi hırsızlığı yaparken kimliğini gizlemek amacıyla mevcut dosyaları değiştirmemek gibi önlemler almak,
3. Erişim engeli olmayan sitelerde tahribat oluşturarak bu siteleri saldırılarla kullanılamaz duruma getirmek,
4. Virüs ve benzeri zarar verici yazılımları, kişi ve kurumların bilgisayarlarına yükleyerek zararlar vermek, bu zararlı yazılımlar ile uzak sistemlere erişim sağlayarak sisteme veya kullanıcıya kalıcı tahribatlar vermek maksadıyla fiziksel zararlar vermek,
5. Bir sonraki siber suçta kullanmak üzere bilgi hırsızlığı yoluyla bilgiler elde etmek,
6. Yasal ve de yasal olmayan faaliyetlerin propaganda alanı olarak sanal ortamı kullanmak veya sanal ortamı yasal olmayan faaliyetleri organize eden bir merkez haline dönüştürerek kullanmak,

7. Farklı yöntemlerle erişim sağladıkları bilgisayarları kullanarak geniş çaplı hizmete erişimi engelleme saldırılarında bulunmak,
8. Telif hakkı içeren bilgisayar oyunlarıyla ve materyallerle ilgili mevcut yazılım koruma şifrelerini kırarak yasal olmayan şekilde kullanıma sunmak,
9. Sanal ortamı kişilerin haklarını ihlal ederek suç (tehdit, hakaret vb.) işleme alanı olarak kullanmak, sanal ortamı dolandırıcılık ve spam amaçlı kullanmak,
10. Sanal ortamda çocuk pornografisi depolamak, üretmek, paylaşmak ve erişime sunmak (Bilgi Teknolojileri ve İletişim Kurumu, 2022).

Başlıca siber saldırı türleri aşağıda detaylandırılmıştır:

1.2.1. Sniffing

Sniffing temelde verilerin akışını engellemek olarak ifade edilebilmektedir. Sniffing ile networkteki paketler yakalanabilmekte ve içeriğe erişim sağlanabilmektedir. Sniffing, bir ağ üzerindeki bilgisayarlar arasındaki veri hareketliliğinin takip edilebilmesi anlamına da gelmektedir. Bu amacın gerçekleştirilebilmesi maksadıyla çeşitli yazılımlar bulunmaktadır. Veri hareketliliğinin takip edilmesindeki yöntem, iki bilgisayar arasındaki tüm verilere erişim sağlanarak saklanmasıdır. Bu yöntem, siber korsanların kullandığı temel yöntemlerden birisidir. Sniffing'in amacı, şifrelere ve transfer edilen dosyalara erişim sağlayarak bilgilerin depolanmasıdır (Arslan, 2016).

1.2.2. Hizmet Dışı Bırakma

Bilişim sistemlerinin erişilebilirliğine yönelik düzenlenen "DoS saldırısı" olarak bilinen, hizmeti engelleme saldırılarıdır. DoS (Denial of Service), hizmeti aksatma veya hizmeti işlevsiz hale getirme anlamına gelmektedir. Bu saldırı, internet kullanıcılarına hizmet verilmemesine ya da çok yavaş bir hizmet sunulmasına yol açmaktadır. Günümüzde hizmet dışı bırakma saldırıları, birden fazla hatta ve binlerce bilgisayar kullanılarak yapılmaktadır. Bu tür saldırılara, dağıtım hizmeti engelleme saldırıları anlamına gelen Distributed DoS veya DDoS saldırıları denilmektedir. Bu tür saldırıların soruşturulması kolay olmamaktadır. Bunun nedeni, DDoS saldırılarının çoğunlukla bu iş için yazılmış botnet (bot networks) adı verilen zararlı yazılımlar aracılığıyla gerçekleştirilmesidir. Botnetler genellikle DDoS saldırılarında kullanılmakta ve saldırının hedefindeki internet adresleriyle bağlantı kurarak sunucuyu meşgul etmektedir (Hekim ve Başıbüyük, 2013).

1.2.3. IP Aldatması

Bilgisayarlar arasında gerçekleştirilen bağlantı, çeşitli protokollerle sağlanmaktadır. Bu protokoller aracılığıyla başka bir bilgisayara bağlanıldığında, bağlanılan bilgisayar kimliğini karşı tarafa tanıtmaktadır. Bağlantı sağlanan bilgisayara gerçek IP adresinin gösterilmemesi ve kimliğin gizlenmesine IP spoofing (aldatma) denir. Sahte IP paketi ile karşılaşan bilgisayar, paketin gerçekte gönderilen adresten gelip gelmediğini bilememektedir. Teoride bu durum mümkün olmakla birlikte pratikte, karşıdaki sisteme tam anlamıyla erişim sağlanmadan başkasının bilgisayarına farklı bir IP'den bağlanma söz konusu olmamaktadır. Ip aldatması genel olarak bir web sitesine zarar verilerek onu işlevsiz duruma getirmek için saldırı esnasında kaynağı gizleme amacıyla kullanılmaktadır (Arslan, 2016).

1.2.4. Sosyal Mühendislik Saldırıları

Sosyal mühendislik yöntemi, siber suçların işlenmesinde kullanılan en etkili yöntemlerden birisidir. Sosyal mühendislik yöntemi, insani zaaflardan (güven, iletişim, düşünce yapısı vb.) faydalanarak siber güvenlik süreçlerinin etkisiz hale getirilmesi şeklinde tanımlanabilmektedir. Bu yöntemde çeşitli bilgilere ulaşabilmek maksadıyla sisteme zarar verme, verileri çalma ve sistemi ele geçirme amacı vardır. Telefonla arama ve mesaj gönderme, oltalama, spam postalar gibi yöntemler sıkça kullanılan sosyal mühendislik yöntemleridir (Ehliz, 2019).

1.2.5. Bilgisayar Korsanlığı: Sistem Güvenliğini Aşarak Erişim Sağlama

Yetkisiz erişim sağlayabilmek amacıyla bir sistemin güvenlik önlemlerinin etkisiz hale getirilmesi bilgisayar korsanlığı olarak adlandırılmaktadır. Bu amaç doğrultusunda kullanılan pek çok yöntem mevcuttur. Bu yöntemlerin başında, işletim sistemlerinin pek çoğunda yaygın olarak kullanılan uygulama programlarında veya ağ bağlantılarında var olan açıkları bularak kötüye kullanım gelmektedir. Sistemlerde var olan açıkların tespit edilmesi ve yaralanabilme yollarının geliştirilmesi, bu sistemler hakkında bilgi ve donanım sahibi olmayı gerektirmektedir. Tespit edilen sistem açıklarına ilişkin bilgilerin paylaşıldığı çok sayıda internet sitesi mevcut olup, hacking amacıyla bu siteler takip edilmektedir. Dolayısıyla güncellenmeyen işletim sistemi veya uygulama programlarının üzerinde çalışan sistemlerin risk altında olduğu unutulmamalıdır (Hekim ve Başıbüyük, 2013).

1.2.6. Oltalama

Son dönemin en popüler siber suçlarından birisi olan oltalama (phishing) kavramı, çevrimiçi dolandırıcılık olarak tanımlanabilir. Oltalama kavramı, balık tutma anlamına gelen "fishing"den türetilmiştir. Oltalama yönteminin temel amacı, internet kullanıcılarını aldatarak kişilerin banka hesap numaralarına, kredi kartı bilgilerine ve bu hesaplara ait çevrimiçi şifrelere kadar birçok şahsi bilgileri ele geçirmektir. En yaygın örneği, kurbana sahte e-posta gönderilmesi sonucu çeşitli bilgilerinin ele geçirilmesidir. G-mail ve benzeri e-posta hizmetlerinin sayfaları titiz ve detaylı bir şekilde yeniden tasarlanarak hedef kişiye gönderilmekte ve hedef kişi, bilgilerini bu sahte sayfaya girdiğinde bilgilerinin tümü siber suçluların eline geçmektedir (Küçükvardar, 2018).

1.2.7. Casus Yazılım

Casus yazılım, kişisel bilgilerin toplanması veya onay alınmadan bilgisayarın yapılandırmasını değiştirebilen yazılımlar için kullanılan genel bir terimdir. Casus yazılımlar genellikle reklam yazılımı ya da önemli bilgileri izleyebilen yazılımla ilişkilendirilmektedir. İstenmeyen yazılım çeşitleri, ulaşılan bilgisayarda istenmeyen değişiklikler yapabilmekte ve bilgisayarın kilitlenmesine veya yavaşlamasına neden olabilmektedir. Bu programlar, web tarayıcısının arama sayfasını veya giriş sayfasını değiştirebilmekte ya da tarayıcıyı istenmeyen sitelere yönlendirebilmektedir (https://www.siberay.com/zararli-yazilimlar---2-casus-yazilim-keylogger-botnet).

1.2.8. Bilgisayar Virüsleri ve Solucanları

Bilgisayar virüsleri, bilgisayar kodlamada kullanılan dillerin imkânları aracılığıyla yazılan ve çeşitli yöntemlerle ağ veya USB bellek gibi harici depolama üzerinden diğer bilgisayarlara aktarılabilen bir çeşit bilgisayar kodlaması ve programıdır. Virüslerin, kodlama yoluyla ulaştığı hedef bilgisayarda nereye yerleşeceği ve hangi verileri kopyalayacağı, sileceği ve sisteme ne şekilde zarar vereceği belirlenmektedir. Genel olarak virüsler, sisteme zarar verme amacıyla kodlanmaktadır ve mümkün olduğu kadar yayılıp, ulaşabileceği maksimum sayıda sisteme zarar vermeyi amaçlamaktadırlar. Sıklıkla karşılaşılan virüs türü ".exe" uzantılı olup, çalıştırılarak kurulumu gerçekleşen dosyalarla bulaşan türdür. Bilgisayarlara virüslerin bulaşma yöntemleri sıklıkla e-posta, indirilen herhangi bir program, giriş yapılan zararlı linkler, izlenen bir video veya oynanan bir oyundur (Bilgi Teknolojileri ve İletişim Kurumu, 2022).

Solucanlar da tıpkı virüslerde olduğu gibi bir cihazdan diğer bir cihaza kopyalanmak amacıyla tasarlanmıştır. Bu kopyalanma işlemini herhangi bir programa gereksinim duymadan kendi başlarına gerçekleştirmektedir. Öncelikle bilgisayarda dosya veya veri transferi yapan işlevlerin denetimini ellerine geçirip bir kez sisteme bulaştıktan sonra ağdaki yeterince korunmayan tüm bilgisayarları ve sunucuları etkileyebilmektedir. Solucanların en büyük tehlikesi, büyük miktarlarda çoğalabilme yetenekleridir. Kullanıcıların veri ve dosya transfer yöntemlerini kullanarak, bağlantı halinde olunan tüm e-posta adreslerine ve bilgisayarlara geçiş yapabilmektedirler (https://www.kaspersky.com.tr/resource-center/threats/viruses-worms).

1.2.9. Klavye İşlemlerini Kaydeden Program (Keylogger)

Keylogger, tanım olarak klavye işlemlerini kaydeden programlar olmakla birlikte klavye kullanarak girilen bilgileri yakalayıp kaydeden ve bunları saldırgana gönderen casus yazılımlardır. Keylogger klavye işlemlerini kaydedip, önceden belirlenmiş adreslere yollanması, yazılan tüm bilgileri kaydedip suçlu kişiye göndermesi sebebiyle oldukça tehlikelidir. Bu durum, hem özel hayatın gizliliğinde hem de ticari ve bankacılık işlemlerinin güvenliği anlamında çok ciddi tehdit oluşturmaktadır. Yalnızca yazılım olarak değil, klavye altına yerleştirilen bir cihazla da gerçekleştirilebilen bu eylem, önemli ölçüde güvenlik açığı oluşturabilmektedir. İnternet üzerinden kredi kartı bilgileri girildiğinde bu program giriş yapılan tüm bilgileri kopyalayabilmektedir. Aynı yöntem, banka ATM'lerinin klavyelerine de yerleştirilerek kredi kartı bilgilerinin çalınmasında da kullanılabilmektedir (Ehliz, 2019).

1.2.10. Truva Atları

Truva atları, virüs ve diğer zararlı yazılımların aksine, bilgisayarlara bulaşmak için yararlı bir uygulama gibi (örneğin virüsleri temizliyor gibi) görünmektedir. Bu yöntemle, saldırgan truva atı olarak adlandırılan bu tehlikeli yazılım türünü kullanarak erişim sağladığı bilgisayarda yapmak istediği zararlı işlemleri gerçekleştirebilmektedir (https://berqnet.com/blog/truva-ati). Truva atları, bir program veya dosya içerisine zararlı yazılımlar aracılığıyla yüklenmekte, karşı bilgisayarla bağlantı kurabilmekte ve çeşitli bilgileri ele geçirebilmektedir. Truva atı programı, solucan veya virüs yazılımları gibi kendisini çoğaltamamaktadır. Truva atı yazılımı, kendisini faydalı bir işlem veya sistem dosyası gibi göstererek gizlemektedir. Truva atlarının uzaktan kontrol edilen truva atları, parola truva atları, imtiyazlı yükselen truva atları, anahtar kırıcı, yıkıcı truva atları ve şaka

programları gibi çeşitleri mevcuttur. Bunların hepsi, aynı amaca hizmet etmekle beraber, özellik olarak birbirlerinden ayrılmaktadırlar (Arslan, 2016).

1.3. Türk Ceza Kanunu'nda (TCK) Bilişim Suçları

Hızla değişen bilgi ve iletişim teknolojilerinin ihtiyaçları ışığında bilişim hukuku da sürekli güncellenmesi gereken bir alan olmaktadır. Bilişim suçlarına yönelik ülkemizde çeşitli kanunlar mevcuttur (Ermeydan, 2018). Bilişim alanında suçlar mevzuatımızda ilk defa 1991 yılında 765 sayılı TCK'ya eklenen düzenlemeler ile yerini almış ve bu suçlara ilişkin cezai yaptırımlar belirlenmiştir. Türk Ceza Kanunu'nda bilişim suçları ikili sınıflandırmaya tabi tutulmuştur. Bu sınıflandırmaya göre doğrudan bilişim suçları olarak Türk Ceza Kanunu'nun onuncu bölümünde bilişim sistemine karşı suçlar başlığı altında suç tipleri düzenlenmiş ve ceza kanununda yer alan klasik suç tiplerinin bazılarına, bilişim sistemi kullanılarak işlenen yeni fiiller eklenerek dolaylı bilişim suçları düzenlemesine gidilmiştir. Dolaylı bilişim suçları, bilişim sistemi kullanılmasıyla işlenebilecek suç çeşitleridir. Dolaylı bilişim suçlarına, TCK 142/2-e bendindeki hırsızlık suçunun, bilişim sistemi kullanılarak işlenmesi nitelikli hali örnek gösterilebilir (Öztürk vd., 2020).

TCK'nın ikinci kitabında "Topluma Karşı Suçlar" başlığını taşıyan üçüncü kısmın "Bilişim Sistemlerine Karşı Suçlar" başlığını taşıyan onuncu bölümünde düzenlenen bilişim suçları sırasıyla 243'üncü maddede düzenlenen "Bilişim Sistemine Girme", 244'üncü maddede düzenlenen "Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme", 245'inci maddede düzenlenen "Banka veya Kredi Kartlarının Kötüye Kullanılması" ve 245/A maddesinde düzenlenen "Yasak Cihaz ve Programlar" ve 246'ncı maddede düzenlenen "Tüzel Kişiler Hakkında Güvenlik Tedbirleri Uygulanması" şeklindedir (Ermeydan, 2018; Türk Ceza Kanunu, Madde:243,244,245,245/A)

Adli Sicil ve İstatistik Genel Müdürlüğü tarafından hizmete özel olarak yayınlanan rapora göre, 5237 sayılı Türk Ceza Kanunu'nun 243 ve 246. maddesi uyarınca bilişim alanında işlenen suçlar rakamsal olarak 2017 yılı ve öncesinde 7168 (%23,1), 2018 yılında 2242 (%7,2), 2019 yılında 7251(%23,4), 2020 yılında 6093 (%19,7) ve 2021 yılında 8239 (%26,6) olmak üzere toplamda 30993 olaydan meydana gelmiştir (https://adlisicil.adalet.gov.tr/Resimler/SayfaDokuman/31052022141642021H%C4%B0ZMETE%C3%96ZELK%C4%B0TAP.pdf).

5237 sayılı Türk Ceza Kanunu'nda yer alan bilişim suçları aşağıda detaylandırılmaktadır.

1.3.1. TCK Madde 243: Bilişim Sistemine Girme Suçu

Türk Ceza Kanunu'nun 243. maddesinde "bilişim sistemine girme" başlığı altında bir suç düzenlemesi oluşturulmuştur. Bu madde ile "bilişim sistemine hukuka aykırı olarak girmek veya orada kalmaya devam etmek" cezai yaptırım altına alınmaktadır. İlgili düzenleme ile bilişim sistemindeki verilerin ele geçirilmesi şart olarak aranmamakta, sisteme haksız olarak girmek veya orada kalmaya devam etmek suçun oluşmasına neden olmaktadır (Çetin, 2020).

Bilişim sistemine girme suçu, bilişim sistemine ulaşmayı sağlayan aracın parçalarına somut olarak yapılacak müdahaleleri kapsamamaktadır. İlgili düzenlemede "bilişim sistemine girmek" ifadesiyle, bilişim sisteminin tamamına ya da bir kısmının oluşturduğu dijital platforma erişim kastedilmektedir. Suçun kanuni ifadesinde, failin davranışlarıyla mağdura zarar vermek istemesi gibi bir psikolojik etken, amaç olarak aranmamaktadır. Dolayısıyla fiilin manevi unsurunun oluşabilmesi için genel kast yeterlidir. Söz konusu maddede, fiilin hukuka aykırı olarak gerçekleşmesi aranmaktadır. Buna göre, mağdurun geçerli rızası gibi hukuka uygunluk sebeplerinden birinin bulunması halinde, fiil suç teşkil etmeyecektir. Bu noktada dikkat edilmesi gereken, mağdurun rızası bulunsa bile sisteme girildikten sonra rızanın olmaması durumunda sistemde kalınmaya devam edilmesi halinde fiilin suç teşkil etmesidir (Yazıcıoğlu, 2008).

1.3.2. TCK Madde 244: Sistemi Engelleme, Bozma, Verileri Yok Etme veya Değiştirme

Türk Ceza Kanunu'nun 244. maddesi üç farklı suç tipini düzenlemektedir. "Bilişim sistemini engelleme ve bozma", "bilişim sisteminde bulunan verilere zarar verme" ve "bilişim sistemi kullanarak haksız menfaat sağlama" davranışları, aynı maddenin değişik fıkralarında farklı suç tipleri olarak yaptırım altına alınmıştır (Öztürk vd., 2020). Bahsi geçen "bilişim sistemini engelleme" ile kast edilen, sistemin işleyişinde geçici olarak kesinti meydana getirmektir. Bilişim sisteminin işleyişini bozma ise sistemden yararlanmanın kalıcı şekilde engellenmesi anlamına gelmektedir. Bu noktada ikili bir ayrıma gitmek gerekmektedir. Bilişim sisteminin işleyişinin bir bütün olarak sisteme karşı işlenen fiillerle bozulması mümkün olmakla birlikte, sistemin verilerine yapılacak müdahalelerle de

sistemin işleyişinin bozulması mümkündür. Sistemin verilerine yönelen fiilin, sistemin işleyişini engellemesi veya bozması durumu 244. maddenin birinci fıkrasına; sistemin işleyişini engellememesi veya bozmaması durumu ise 244. maddenin ikinci fıkrasına karşılık gelmektedir. 244. maddenin ikinci fıkrasında bilişim sistemindeki verilere zarar verme suçu düzenlenmiştir. İlgili fıkrada "sistemindeki verileri bozan, yok eden, değiştiren veya erişilmez kılan, sisteme veri yerleştiren, var olan verileri başka bir yere gönderen kişinin cezalandırılacağı" belirtilerek seçimlik hareketli bir suç düzenlemesine yer verilmiştir (Artuk, 2014). Engelleme veya bozma fiillerinden birinin işlenmesi, suçun gerçekleşmesi için yeterli görülmektedir. Üçüncü fıkrada ise ilk iki fıkrada düzenlenen suçların nitelikli haline yer verilmiştir. Bu fiillerin banka veya kredi kurumuna ya da kamu kurum veya kuruluşlarına ait bilişim sistemleri üzerinde işlenmesi cezalandırılmıştır. Son fıkrada bu fillerin işlenmesi sebebiyle haksız yarar sağlanması cezai yaptırımlarla belirlenmiştir (https://www.tahanci.av.tr/sistemi-engelleme-bozma-verileri-yok-etme-sucu/#sistemi-engelleme-bozma-verileri-yok-etme-veya-degistirme-sucu-tck-244).

Bahsi geçen madde, Avrupa Siber Suç Sözleşmesi'nin 4, 5 ve 8. maddelerinin iç hukuktaki görünümü niteliğindedir. Nitekim ilgili sözleşmenin 4. maddesi, taraflardan her birinin bilgisayar verilerine haksız yere zarar verilmesi, değiştirilmesi ve silinmesi gibi maddede belirtilen fiillerin kasten gerçekleştirildiği durumları, kendi iç hukukunda suç olarak tanımlanması için gerekli tedbirleri alması gerektiğini belirtmektedir. Sözleşmenin "sisteme müdahale" başlıklı 5. maddesinde de sözleşmeye taraf ülkelerden her birinin bilgisayar verilerine zarar verilmesi, değiştirilmesi gibi fiillerle haksız yere bir bilgisayar sistemi işleyişinin kasıtlı olarak engellendiği durumları, kendi iç hukukunda bir suç olarak tanımlanması sebebiyle gerekli tedbirleri almayı kabul ettiğini ifade etmektedir. Benzer şekilde ilgili sözleşmenin 8. maddesinde de sözleşmeye taraf devletlerin, maddede belirtilen fiillerin kasten ve haksız yere gerçekleştirilerek bir kimsenin mal kaybına sebep olunduğu durumların kendi iç hukukunda suç olarak tanımlanması amacıyla gerekli tedbirleri alacağı belirtilmektedir (Öztürk vd., 2020).

1.3.3. TCK Madde 245: Banka veya Kredi Kartlarının Kötüye Kullanılması

İlgili suçla korunmak istenen hukuki değer, banka veya kredi kartlarının hukuka aykırı kullanılmasıyla bankaların veya kredi kartı sahiplerinin zarara uğratılmasının önüne geçilmesi olarak belirtilmiştir. Bu çerçevede maddenin ilk fıkrasında başkasına ait banka veya kredi kartıyla hukuka aykırı yarar sağlama suçu, ikinci fıkrasında başkalarına ait banka

hesapları ile ilişkilendirerek sahte banka veya kredi kartı üretme, satma, devretme, satın alma veya kabul etme suçu, üçüncü fıkrasında ise sahte oluşturulan veya üzerinde sahtecilik yapılan banka veya kredi kartıyla hukuka aykırı yarar sağlama suçu, cezai yaptırım altına alınmıştır (Parlar, 2011).

Birinci fıkrada suçun maddi unsuru açısından dikkat çeken husus, düzenlemede "başkasına ait bir banka veya kredi kartını, her ne suretle olursa olsun ele geçiren veya elinde bulunduran kimse" ifadesinin yer almasıdır. İkinci fıkrada ise suçun maddi unsuru seçimlik olarak düzenlemiştir. Seçimlik hareketler; sahte banka veya kredi kartını üretmek, satmak, devretmek, satın almak veya kabul etmek olarak ifade edilmiştir. Maddede düzenlenen suçun oluşması için bu eylemlerin başkasına ait banka hesabı ile ilişkilendirerek işlenilmesi gerekmektedir. Üçüncü fıkrada ise "sahte oluşturulan veya üzerinde sahtecilik yapılan bir banka veya kredi kartını kullanmak suretiyle kendisine veya başkasına yarar sağlayan kişi" hakkında yaptırım düzenlenmiştir. Suçun oluşum şeklinde ilk olarak sahte oluşturulmuş ya da üzerinde değişiklik yapılarak sahte hale getirilmiş bir kartın bulunması gerekmektedir. İkinci olarak failin bahsedilen niteliklerdeki kartı kullanarak kendisine veya başkasına yarar sağlaması aranmaktadır (Tezcan, 2014).

1.4. Suç Korkusu

Korku, herhangi bir tehlike düşüncesi veya tehlike, risk, tehdit, kaygı veya endişe gibi uyarıcıların etkisiyle oluşan güvensizlik algısıdır. Alanyazında "fear of crime" olarak belirtilen suç korkusu ise toplumda var olan herhangi bir suçun mağduru olma ya da bu suçlardan zarar görebilme korkusu şeklinde ifade edilmektedir (Çalışkan, 2019; Çardak, 2022; Çelik ve Mirza, 2020; Öztürk ve Yıldız, 2017; Yavuz, 2019). Suç korkusu bilişsel, duygusal ve davranışsal boyutları olan karmaşık bir kavramdır (Çalışkan, 2019). Bu kavram üzerine literatürde fazlaca tanım var olmakla birlikte Ferraro'nun tanımı, suç korkusu araştırmalarının birçoğunda ön plana çıkmaktadır. Ferraro'nun tanımlamasına göre suç korkusu, bireyin suç veya suçla ilişkilendirdiği sembollere karşı geliştirmiş olduğu duygusal endişe veya korku olarak tanımlanmaktadır. Bu tanımlamadan da anlaşılacağı üzere suç korkusuna sebebiyet veren unsurlardan birisi suçtur. Suç korkusu, direkt olarak suça yönelik geliştirilebildiği gibi suç ile ilişkilendirilen sembollere karşı da geliştirilebilmektedir. Başka bir ifadeyle suç korkusu, suç olarak tanımlanabilecek bir eylemin olmaması durumunda da oluşabilen duygusal bir tepkidir. Bu bağlamda suç korkusu, suçtan kaynaklı oluşum göstermekte ancak suç olgusunun ötesine de geçebilmektedir (Yazgan, 2017).

Toplumsal dinamiklerin yıkılmasına karşılık gelen tehditler barındırması sebebiyle suç olgusu, toplumsal sorunların başında gelmektedir. Bununla birlikte suç olgusu, suça maruz kalanlar üzerindeki etkisiyle değerlendirildiğinde toplumsal alanda "suç mağduriyeti korkusu" oluştuğu görülmektedir. Suç korkusu, bireylerin herhangi bir suç karşısında mağdur olma ihtimallerini düşünmelerine ve korku duymalarına neden olan önemli bir konudur (Yavuz, 2019). Toplumsal yaşamın ve insanlığın var olduğu ilk günden ve birbirini etkilemeye başladığı ilk andan itibaren suç olgusu yaşamımızı etkilemektedir. Bu etkilenme neticesinde birey, suç ile yakın ilişki içerisinde olmuş ve suçtan etkilenen olarak suçun bıraktığı korku ile yaşamak zorunda kalmıştır (Boztoprak, 2021). Şenol ve diğerleri (2020), suç korkusu kavramının çağrıştırdığı iki duygudurumdan söz etmektedir. Bunlardan birisi, kişinin kendisinin suçu işleyen olma ihtimaline karşı duyduğu korkudur. Başka bir ifadeyle, kişinin suç işlemesi durumunda karşılaşacağı cezai yaptırımlarla ilgili duyduğu korkudur. Diğeri ise herhangi bir suçtan mağdur olma ve bunun bir sonucu olarak maddi veya manevi anlamda zarar görme ihtimali dâhilinde oluşan korku duygusudur.

Suç korkusu, suç olgusu ile çok yakından bağlantılı olmakla birlikte bazı durumlarda suçtan bağımsız bir olgu olabilmektedir. Kriminoloji literatüründe suç korkusu ile ilgili yapılan birçok araştırma, suç oranlarındaki artışa paralel olarak artan suç korkusunun, suç oranlarındaki azalma ile birlikte değişmediğini göstermektedir. Bu sebeple bazı durumlarda suç korkusu suçla birlikte değerlendirilirken, bazı durumlarda ise suçtan bağımsız bir olgu olarak değerlendirilmesi gereken önemli bir problemdir. Suç korkusu bazı durumlarda suçun kendisinden daha yaygın olmaktadır. Farklı suç türleri, farklı suç korkularının oluşmasına neden olabilmektedir (Çelik ve Mirza, 2020; Öztürk, 2015).

Bin dokuz yüz kırk üç yılında Abraham Maslow'un oluşturmuş olduğu İhtiyaçlar Piramidi Teorisi'nde fizyolojik ihtiyaçlardan başlayan piramidin herhangi bir basamağındaki ihtiyacın karşılanmaması halinde bir üst basamağa geçişin mümkün olmadığı belirtilmektedir. İhtiyaçlar Piramidi Teorisi'ndeki ikinci basamak güvenlik ihtiyacı olup, bu basamak fizyolojik ihtiyaçlardan sonra en önemli ihtiyaç olarak belirtilmektedir. Bireylerin güvenlik ihtiyaçları tamamlanmadan sosyal ihtiyaçlarına geçişini engelleyen birçok faktör söz konusudur (Yurtsal, 2016). Suç korkusu sebebiyle ihtiyaçlarını tamamlayamayan bireyler, sosyal çevrelerinden uzaklaşma sorunu ile karşılaşabilmektedir (Çalışkan, 2019).

Gerçek, ölçülebilen ve en önemlisi bireysel ve toplumsal boyutları olan bir kavram olarak karşımıza çıkan suç korkusu, günümüzde modern toplumların en ciddi

problemlerinden birisi olarak karşımıza çıkmaktadır (Boztoprak, 2021; Çardak, 2011; Yavuz, 2019). Bıraktığı sosyolojik ve psikolojik etkileri nedeniyle de suç korkusunun üzerinde durulması önem taşımaktadır (Boztoprak, 2021). Öyle ki suç korkusu, bireylerin fiziksel ve psikolojik açıdan zarar görmesinin yanı sıra sosyal ilişkilerinin sarsılmasına neden olabilmekte ve toplumsal düzeni bozabilmektedir (Öztürk ve Yıldız, 2017). Suç korkusu bireylerin yaşam kalitesini ve toplumu olumsuz anlamda etkileyen önemli bir sosyal sorun olarak karşımıza çıkmaktadır. Kalabalık yerlere gitmekte çekingen davranma, evde kimse olmadığı durumlarda hırsızlık ihtimaline karşı ışıkları açık tutma, toplu taşıma araçları ve gece taksi kullanımından kaçınma, internet ve sosyal medya hesaplarının şifrelerinin sıklıkla değiştirilmesi gibi davranışlar suç korkusunun günlük yaşamdaki yansımaları olarak karşımıza çıkmaktadır (Çelik ve Mirza, 2020).

Suç korkusu, toplumsal ve bireysel bir olgu olmakla birlikte, mekânsal boyutta da etkili olmaktadır. Suç korkusu, bir mekânın güvensiz olarak algılanmasına ve korku hissine neden olan sorunların başında yer almaktadır (Çelik ve Mirza, 2020). Risk ve tehlikelere daha yakın olunduğu düşünülen toplumsal alanların suça maruz kalma ihtimalini artırdığı düşünülmektedir. Medyanın olumsuz olaylara sıklıkla yer veriyor olması ve insanları suça teşvik ediyor olması, bir yönüyle suç korkusunu artırmaktadır. Suç korkusunun ortaya çıkması ve yaygınlaşmasında, kent ve metropol yaşamının güvensiz olarak nitelendirilmesi ve bu yöndeki haberlerin ön planda tutulması önemli bir rol oynamaktadır (Şenol ve Gülver, 2020).

Üniversite kampüslerinin güvensizlik algısı ile bağlantılı olarak suç korkusunun mekânsal etkilere sahip olduğu belirtilmektedir. Türkiye'de yapılan bir çalışmada, öğrencilerin bir üniversite kampüsünün fiziksel özelliklerine ilişkin suç korkusu algıları incelenmiş ve bu kampüste suça maruz kalma riskinin yüksek olduğu ve güvensiz algılanan yerler olduğu tespit edilmiştir. İlgili araştırma kapsamında suç korkusunu artıran unsurlar; kampüsteki kontrolsüz giriş, gecenin karanlık etkisi, suçla ilgili duyulan rivayetler ve şüpheli kişiler olduğu sonucuna ulaşılmıştır. Dolayısıyla bireylerin suç korkusunu ve güvenlik algısını fiziksel çevrenin niteliği belirleyebilmektedir (Çelik ve Mirza, 2020).

Modernleşme, sağlamış olduğu yeniliklerle hayatı kolaylaştıran fırsatlar sunmakla birlikte çeşitli sorunları da beraberinde getirmektedir. Modernleşmeyle ilgili olduğu söylenebilecek sorunlar içerisinde en önemlilerinden bir tanesi suç oranlarında yaşanan artışlardır (Şenol vd., 2020; Şenol ve Gülver, 2020). Kentleşme ve teknolojik gelişmelerle

beraber suç türlerindeki değişim ve suç oranlarındaki artış, suç mağduriyeti korkusunda da artışa neden olmuştur (Yavuz, 2019; Şenol vd., 2020; Şenol ve Gülver, 2020). Suç, evrensel bir olgu olmakla birlikte geleneksel toplumlardan ziyade modern toplumlarda daha sık görülmektedir (Şenol, vd., 2020). Özellikle kent yaşamında suç ile artan oranda hissedilen suç korkusu, kişileri çeşitli şekillerde etkilemektedir. Suç korkusu yaşayan bireylerin sosyal davranışlarını sınırlandırdıkları, şehrin güvensiz alanlarından kaçındıkları, güvensiz alanlarda yaşamaktan kaçınamayan insanların ise sokağa çıkmaktan korkarak evden dışarı çıkamaz duruma geldikleri yapılan araştırmaların bulgularındandır (Yılmaz, 2018).

Suç korkusu bireylerin yaşam kalitelerini, sosyal davranışlarını ve sosyal etkileşimlerini etkileyebilmekle birlikte toplumda bölünmeler oluşturabilen sosyal bir olgudur (Yılmaz, 2018). Suç korkusu sebebiyle kişiler arası ilişkilerde karşılıklı güven hissi azalmakta ve olumsuz psikolojik sonuçlar ortaya çıkmaktadır. Dolayısıyla suç korkusunun kişilerin günlük rutininde olumsuz etkiler bıraktığını söylemek mümkündür (Boztoprak, 2021). Suç korkusunu, suçun sosyal ve psikolojik maliyeti olarak nitelendirmek mümkündür. Suç ve suç korkusu, insanların temel ihtiyaçlarının başında gelen güven duygusunun tatmin edilememesinde oldukça önemlidir. Suç korkusu, bireyler arası etkileşim, iletişim ve sosyalleşmeyi engelleyen bir yönü olmasından kaynaklı, bireylerin toplumda yabancılaşma sorununu oluşturma potansiyeli açısından dikkat çekilmesi gereken bir konudur (Şenol, vd., 2020; Şenol ve Gülver, 2020).

Suç korkusu alanında yapılan pek çok çalışmada, suç korkusunun bireysel faktörlerin yanı sıra çevresel faktörlerden etkilenen karmaşık bir yapısı olduğu belirtilmektedir. Düzensizlik ve Toplumsal Kaygı Kuramları, çevresel faktörlerin suç korkusu üzerindeki etkisini ortaya koymak amacıyla geliştirilen kuramlardandır. Her iki kuram da önemli ölçüde Şikago Okulu teorisyenlerinin kentsel yapı ile suç arasında kurmuş oldukları bağlantıdan etkilenmiştir. Düzensizlik Kuramı, çevredeki fiziksel ve sosyal çözülmelerin suç korkusunu artırdığına dikkat çekerken; Toplumsal Kaygı Kuramı, sosyal ilişkiler ve sosyal sermaye ile suç korkusu arasındaki ilişkiye vurgu yapmaktadır (Öztürk, 2016; Yavuz, 2019).

Öztürk'ün (2016) suç korkusunu Düzensizlik ve Toplumsal Kaygı Kuramları kapsamında açıklamayı amaçlayan çalışmasında, Avrupa kentlerinin çoğunda olduğu gibi Mersin ilinde vatandaşların suç mağduriyet korkularının yüksek düzeyde olduğu görülmüştür. Bu sonucun ortaya çıkışında Mersin'in sosyoekonomik, toplumsal, kültürel ve tarihi yapısı ile yaşamış olduğu hızlı kentleşmenin etkili olduğu söylenebilmektedir.

Göçlerle kurulan Mersin ili, yine göçlerle büyüyerek kozmopolit bir hal almıştır. Mersin, ülke içinden (özellikle Güneydoğu ve Doğu Anadolu Bölgesinden) ve de ülke dışından (Suriye ve Irak) yoğun göçlerin durağı olan kenttir. Bu durum hoşgörüyü ve çok kültürlülüğü arttırıyor olsa da aynı zamanda birçok sosyal probleme kaynaklık etmektedir. Mersin ilinin yoğun göç alması; ilk olarak kentteki gelir dağılımını bozmuş, göçe bağlı olarak kentin toplumsal yapısı hızla dönüşmüştür. Kentte gerilimlerin artmasıyla, kente en son gelenler kentin yerlileri tarafından ötekileştirilmiştir. Bu gerilim, gruplar arası sosyal mesafenin artmasına neden olmuş ve güvensizlik hissinin ortaya çıkmasına neden olmuştur. Suç korkusunun yüksek çıkmasında etken olarak göç sonucu oluşan heterojen nüfus yapısının etken olduğu düşünülmektedir. Şehrin kozmopolit bir yapıya bürünmesinin kentte ikincil ilişkilere, sosyal bağların zayıflamasına ve bireylerin yalnızlaşmasına yol açacağı iddia edilmektedir. Kentin sosyal çeşitliliği içerisinde yaşayan bireyler sosyal belirsizliklerle mücadele etmek zorunda kalmakta ve bu durum, doğal olarak güvensizlik hissini ve suç korkusunu beraberinde getirmektedir.

Mağduriyet modeli, mağduriyet korkusunun kaynağı olarak geçmişte yaşanan mağduriyetleri temel almaktadır. Doğrudan ve dolaylı olarak mağduriyet geçmişi, korku oluşturma unsuru olarak değerlendirilmektedir. Savunmasızlık Teorisi, kişilerin suç karşısında güçsüz ve korunmasız olmalarının veya güvensiz ve korunmasız hissetmelerinin suç korkusunun daha fazla duyulmasına neden olduğunu ve mağduriyet korkusunun da temel nedeninin bu olduğuna vurgu yapmaktadır. Rutin Aktiviteler Teorisi bireylerin günlük yaşamlarından ve yaşam tarzından kaynaklı olarak suç ve suçluyla karşılaşma ihtimallerinin yüksek olduğunu ve bu durumun da suç korkusuna neden olduğunu vurgulamaktadır. Kırık Camlar Teorisi'nde ise Düzensizlik Teorisi'nden hareketle çevresel faktörlerin tahribatından sonra bu bölgelerin suçlulara açık alanlara dönüştüğünü ifade etmektedir. Bu yapıdaki alanlar, halk tarafından bilinmesi sebebiyle bu alanlardan uzaklaşılmasına ve bu alanların varlığının suç korkusu yaşanmasına neden olduğu belirtilmektedir (Yavuz, 2019).

Toplumsal Kontrol Modeli'nde, toplumu bir arada tutmayı sağlayan kontrol mekanizmalarının işlevsel olarak bozulması ve toplumsal kurumların görevlerini yerine getirememesi durumunda kişilerin yaşamış oldukları güvensizlik hissi sonucu suç korkusu yaşayacakları belirtilmektedir. Sosyal Problem Perspektifi'nde ise suçun etkilerinde toplumsal boyutun yansıtıldığı ve bu durumun daha çok mağduriyet korkusu oluşturduğu savunulmaktadır. Günümüzde medya, suçu yansıtma araçlarını elinde bulundurması sebebiyle suç mağduriyet korkusunun artmasına ve yayılmasına neden olmaktadır. Suç

mağduriyet korkusunu açıklamaya yönelik oluşturulan teorilerin tamamı, suçun kaynağı olan ya da suçlu davranışın daha kolay işlenmesine neden olan faktörlerle ilişkili olarak suç mağduriyet korkusunu artıran unsurları belirlemeyi amaçlamaktadır (Yavuz, 2019).

Bireysel suç teorileri, psikolojik suç teorileri ve biyolojik suç teorileri, sosyal bir olgu olarak karşımıza çıkan suç korkusunu açıklamada bazı durumlarda yetersiz kalabilmektedir. Dolayısıyla suç korkusunun, bireylerin toplumsal etkileşimlerini ve suçun toplumsal etkilerini inceleyen sosyolojik bir yaklaşımla incelenmesi, konunun daha iyi anlaşılabilmesi maksadıyla oldukça önemlidir (Yılmaz, 2018). Siber suçlar ve siber suç korkusu konusunda yapılmış bazı çalışmalarda Rutin Aktiviteler Teorisi'nden yararlanılmış olduğu görülmektedir (Alshalan, 2006; Bossler & Holt, 2009; Holt & Bossler, 2008; Leukfeldt & Yar, 2016; 48 Marcum, Higgins, & Ricketts, 2010; Reyns, Henson, & Fisher, 2011a; Williams, 2016; Yar, 2005).

Suç korkusunu tetikleyen unsurlardan birisi terör eylemleridir. Terör eylemleri, toplumsal alanda korkunun ve güvensizlik hissinin artmasına yol açmaktadır. Yıkım ve zarar verme amacı olan terör, intihar saldırılarıyla halkı korkutarak ve uzun süreli baskılar uygulayarak hedefine ulaşmaya çalışmakta ve eylemlerinde bu amacı gütmektedir. Terör eylemlerinin hangi vakitte ve nerede olacağının bilinmemesi ve özellikle kalabalık olan yer ve zamanlarda eylemlerin planlanması sebebiyle, kalabalıklardan korku duyulmasına ve kısa süreli de olsa bireylerin hayatlarında kısıtlamalara gidilmesine sebep olmaktadır. Sosyal hayattan uzaklaşılması kişilerin daha çok korkmalarına yol açmaktadır. Yaşanılan korkunun reaksiyonları, eylemlerin sık yapıldığı zamanlarda daha fazla olmaktadır (Yavuz, 2019).

Çeşitli suç türlerine karşı oluşan suç korkusunun farklı ülkelerde benzer şekilde ortaya çıkışı, araştırmacıların önemli derecede ilgisini çekmiştir(Şahin, 2015). Suç korkusu ile ilgili çalışmalar, 1960'lı yıllarda Amerika Birleşik Devletlerinde yaşanan siyasi ve sosyal sorunlar (gettolarda yaşanan isyanlar, etnik problemler ve Kennedy suikasti gibi sorunlar) sonrası başlamıştır. 1966 yılında Kanun Uygulama ve Adalet Dairesi Başkanlık Komisyonu'nun (President's Crime Comission on Law Enforcement and Administration of Justıce) yaptırdığı bir çalışma, Amerikalıların çoğunluğunun suç mağduru olmaktan korktuğunu ve bu korku nedeniyle davranışlarını sınırlandırdığnı ortaya koymuştur. Yapılan bu çalışma sonrası elde edilen rapora göre, halkın %43'ü suça maruz kalma korkusu sebebiyle gece dışarı çıkamamakta, %35'i yabancılarla konuşmamakta, %21'i geceleri

arabayla seyahati tercih etmekte, %20'si ise suça maruz kalmamak için farklı bir bölgeye taşınmak istemektedir (Öztürk, 2015; Şahin, 2015).

Suç korkusu üzerine yapılmış ilk dönem çalışmaları, bireylerin geceleri ya da yalnız oldukları vakitte korku duyup duymadığını anlamaya yönelik iken sonraki çalışmalarda etnik grupların, kadınların ve yaşlıların suç mağduriyeti korkusuna odaklanılmış ve ayrıca suç korkusunun nedenleri ve ilişkili olduğu faktörler incelenmeye çalışılmıştır (Çardak, 2011). Suç korkusunu açıklama amacıyla yapılan araştırmalarda cinsiyet, yaş, etnik köken, ekonomik ve sosyal yapı ve kişisel deneyimler gibi değişkenlerin göz önünde bulundurulması gerekmektedir (Yavuz, 2019). Öyle ki suç korkusunun yaş, cinsiyet, ekonomik yapı ve yaşanılan yer gibi çeşitli sosyodemografik faktörlerle ilişki içerisinde olduğu düşünülmektedir (Çardak, 2011; Öztürk ve Yıldız, 2017). Suç korkusunun temelinde bir neden değil birden çok nedeni olabilmektedir. Buna göre doğrudan bir suça maruz kalmış olmak, suç korkusunu açıklamada akla gelebilecek bir neden olsa da bu korkunun tek nedeni olarak düşünülmemelidir. Dolaylı olarak mağduriyet yaşamış olmak, yani kişinin yakın çevresindeki kişilerden birinin veya birilerinin suça maruz kalmış olması veya suçların medyada sıklıkla yer alması da suç korkusunu açıklayabilmektedir (Yavuz, 2019).

Suç korkusu üzerine yapılan sonraki çalışmalarda, suç korkusunun modern toplumlarda var olan önemli bir sosyal sorun olduğu, bu korkunun bireylerin yalnızca psikolojik olarak zarar görmesiyle sınırlı olmadığı, toplumsal dayanışma ve istikrarı zayıflattığı, huzursuzluk yarattığı, düzeni bozduğu, insanlar arasında ayrışma ve yabancı düşmanlığına sebep olduğu sonucuna ulaşılmıştır. Hatta Jackson bu durumu "suça karşı kaygı" kavramı çerçevesinde şekillendirerek ve mala ve kişiye yönelik suçları sınıflandırarak "imgesel risk" modelini oluşturmuştur (Çalışkan, 2019).

Araştırmalar, bir suçun mağduru olma korkusunun başlıca nedenlerinden birisi olması bakımından, özellikle cinsiyete dikkat çekmektedir. Bu konuda yapılmış çalışmalar, özellikle kadınların suç korkularının erkeklere oranla daha fazla olduğu sonucuna ulaşmıştır (Şenol ve Gülver, 2020). Ankara'da yaşayan kadınların suç mağduru olma korkusunu inceleyen bir çalışmada (Çardak, 2011), katılımcıların geçmişte yaşamış oldukları ya da kendi şahıslarına yönelik olmasa da bir başkasının başına gelen mağduriyetlerin suç korkularını etkilediği ve geçmişte yaşanan mağduriyetlerle suç korkusu arasında pozitif bir ilişki bulunduğu sonucuna ulaşılmıştır.

Suç korkusunu etkileyen önemli faktörlerden bir diğeri ise yaştır Araştırmalar, gençlerin genellikle daha fazla suç mağduru olduğunu vurgulasa da bir çalışmada, daha yüksek yaş grubunda olanların daha çok korku duyduğu sonucuna ulaşılmıştır (Şenol ve Gülver, 2020). Çardak'ın (2011) çalışmasında ise yaşı kaç olursa olsun her kadının suç korkusu duyduğu belirtilmektedir. Dolayısıyla yaş, kadınlara göre korkuyu ve mağduriyeti etkileyen bir faktör olmamaktadır. İlgili çalışmada, yaş değişkeni ile suç mağduriyeti arasında ise ilişki tespit edilmediği göze çarpmaktadır.

Şenol ve Gülver'in çalışmasında (2020), suç korkusunun ekonomik düzeyle ilişkisine bakıldığında, gelir seviyesi düşük olanların daha fazla korku duyduğu yönünde sonuçlara ulaşılmıştır. Çardak'ın çalışmasında, eğitim seviyeleri farklı olan kadın katılımcıların eğitim durumlarına göre korku düzeylerinin değişmemekte olduğu sonucuna ulaşılmıştır. İlgili çalışmada, kadınların ekonomik gücünün daha iyi şartlarda olmasının önemli olduğu ancak ekonomik gücün daha iyi olmasının suç korkusunu ve mağduriyetleri tamamen ortadan kaldırmayacağı vurgulanmıştır. Ekonomik durumun daha iyi bir düzeyde olması yalnızca daha iyi ve güvenli olarak nitelendirilebilecek konumlarda ikamet etmeyi ve günlük yaşamda toplu taşıma araçlarına olan mecburiyeti ortadan kaldırması bakımından önemli hususlardır. İlgili çalışmada ayrıca zengin ya da yoksul ayrımı yapılmaksızın her kadının suç mağduru olabileceği sonucuna ulaşılmıştır (Çardak, 2011).

Suçun toplumda artış göstermesi sebebiyle suç korkusu da artış göstermektedir. Dolayısıyla günümüz toplumları hem suçun hem de suç korkusunun ortaya çıkardığı sorunlarla baş etmek zorunda kalmaktadır (Öztürk ve Yıldız, 2017). Suçun kontrol altına alınabilmesi ve de önlenebilmesi için ihtiyaç duyulan toplumsal dayanışmayı olumsuz anlamda etkilemesi nedeniyle suç korkusu, suçla mücadelede olumsuz bir etkiye sahiptir. Bu nedenle suçla mücadele çalışmalarının yanında suç korkusunu önlemek ve başa çıkabilmek amacıyla programların geliştirilmesine ve uygulanmasına ihtiyaç vardır (Şahin, 2015).

Suç korkusunun toplumsal boyutu, bireylerin yaşamış oldukları güvensizlik hissi ve toplumdan kopmaya başlamaları ile açıklanmaktadır. Bireyin sosyal kurumlarla ilişkisi ve bu sosyal kurumların işleyişi, suç korkusunun azaltılması amacıyla hassasiyet gösterilen konular arasında yer almalıdır. Bunun yanı sıra yeterli güvenlik önlemlerinin alınması ve çevredeki fiziksel etmenlerin düzeltilmesi, suç korkusunun önlenmesinde önemli faktörlerdendir. Toplum içerisindeki kontrol mekanizmalarının etkisi göz önünde

bulundurularak bu alanlarda iyileştirme ve uyum çalışmalarının yapılması, suç korkusunun azaltılmasına yardımcı olabilir. Medyada sunulan haberlerin doğruluğuna ve güvenilirliğine dikkat edilerek medyanın topluma korku yayan faktör olmasının önüne geçilebilmesi de gerekli önlemler arasındadır (Yavuz, 2019).

1.5. Siber Suç Korkusu ve Siber Suçlara İlişkin Önlem Alma Stratejileri

Yukarıdaki bilgilerden hareketle suç korkusu, insanların davranışlarını ve yaşam kalitelerini nihai olarak etkileyen önemli bir sosyal sorun olarak özellikle son 50 yıldır araştırılan önemli araştırma konularından birisi olmuştur. Çevrimiçi internet kullanıcılarının gün geçtikçe artan sayısı ve toplumun dijitalleşmesi ile suç ve suçlunun oluşmasında çekicilik unsuru haline gelen siber ortam, önem kazanmaya başlamıştır (Erculj ve Mesko, 2022). Siber suç korkusu, kişisel tehdit değerlendirmesi ile siber suç mağduru olunması sebebiyle duyulan ya da mağdur olma riskine yönelik duyulan korkuyu temsil etmektedir (Akdemir, 2020). Siber suç mağduru olma riskinin artması, insanları gerçekleşebilecek siber suç saldırılarına karşı önlem almaya yöneltmektedir (Erculj ve Mesko, 2022). Suç korkusu toplumda sosyal etkileşimleri sınırlandırarak sosyal yardımlaşma ve dayanışmayı azaltmaktadır. Suç korkusu olan bireyler, davranışlarını güvenli hissettikleri zamanlarda güvenli alanlarla sınırlandırmakta olup şehrin güvensiz olarak nitelendirilen alanlarından kaçınmaktadır. Güvensiz alanlarda yaşamaktan kaçınamayan bireylerse sıklıkla kendi evlerinde kalıp sokağa çıkmaktan korkmaktadır. Siber suç korkusunda bu durum, bireylerin kendi evlerinden çıkmaya korkar hale gelmelerinden öte bir boyuttadır. Bireyler evlerinde veya kendilerini en güvende hissettikleri alanlarda dahi siber suç mağduru olma korkusu yaşayabilmektedir. Bu bağlamda suç korkusu, bireylerin sosyal davranışlarına ve günlük yaşamlarına etki eden sosyal bir olgu olarak karşımıza çıkmaktadır. Siber suç korkusu söz konusu olduğunda ise bu durum, bireylerin siber ortamdaki davranış ve etkileşimlerini etkileyen bir duruma dönüşmektedir (Alshalan, 2016).

Siber suç alanında yapılan araştırmalar, siber suçların dünyada hızla büyüyen bir suç türü olduğunu, bireyler ve de çevrimiçi yatırımcılar için büyük ölçüde tehdit oluşturduğunu göstermektedir. Geleneksel suç korkusu ve siber suç korkusu araştırmaları genellikle suç korkusunun belirleyicilerini ortaya koymayı amaçlamaktadır (Akdemir, 2020). Suç korkusuna yönelik belirleyicilerin siber suç korkusu için de geçerli olup olmaması bir tartışma konusu olsa da bu konuda yapılmış çalışmalar incelendiğinde bazı belirleyicilerin suç korkusu ve de siber suç korkusu için ortak olduğu görülmektedir. Bu ortak belirleyiciler

arasında sosyodemografik özellikler, suç ciddiyeti algısı, geçmiş mağduriyet deneyimi ve mağduriyet riski algısı bulunmaktadır (Henson, 2011; Yılmaz, 2018). Bununla beraber internet kullanım davranışları, geleneksel suç korkusunda belirleyici olmamakla birlikte siber suç korkusu için belirleyici unsurlar arasındadır (Yılmaz, 2018).

Siber suç korkusunun başlıca sosyodemografik belirleyicileri arasında cinsiyet, yaş ve sosyal statü değişkenleri bulunmaktadır. Kadınların siber suç mağduru olma olasılıkları daha az olmasına rağmen siber suç korkularının erkeklerden daha fazla olduğu vurgulanmaktadır (Akdemir, 2020; Alshalan, 2006; Yılmaz, 2018). İlgili yazın, kadınların çevrimiçi suçlardan daha fazla korksa da kötü amaçlı yazılımlarda ve çevrimiçi kimlik hırsızlığı korkusunda cinsiyet farkının olmadığını ortaya koymaktadır (Akdemir, 2020). Bununla birlikte, yaşlıların gençlere oranla daha fazla siber suç korkusu duyduğu sonucuna ulaşılmıştır. Fakat yaş faktöründe cinsiyet değişkeni dikkate alındığında genç kadınların yaşlı kadınlara oranla siber suç korkularının daha yoğun olduğu belirtilmektedir (Alshalan, 2016). Sosyal statü olarak değerlendirilen eğitim ve gelir düzeyi gibi değişkenlerle siber suç korkusu arasındaki ilişkiyi inceleyen çalışmalar, daha düşük sosyal statüye sahip bireylerin siber suçlardan daha çok korktuğunu göstermektedir. Ancak geleneksel suç korkusu ile siber suç korkusunun belirleyicilerini karşılaştıran Maddison ve Jeske (2014) çalışmalarında eğitim düzeyi ile siber suç korkusu arasında anlamlı bir ilişki bulmamıştır (akt. Akdemir, 2020).

Siber suç korkusunun bir diğer belirleyicisi olarak değerlendirilen değişken, siber suç bilgisidir. Abdulai'nin (2016) çalışmasında, siber suç bilgisi ile özel olarak banka kartı veya kredi kartı dolandırıcılığı mağduriyeti korkusu arasında ilişki olmadığı belirlenmiştir. Siber kimlik hırsızlığı korkusunda internet kullanım davranışlarının sosyodemografik faktörlere oranla göreceli olarak daha güçlü bir belirleyici olduğu belirtilmektedir (Roberts vd., 2013). İlaveten siber kimlik hırsızlığı korkusu, internet kullanımının yaygınlaşmasıyla artmakta olup evde internet kullanan bireylerdeki korku, evde internet kullanmayan bireylere oranla daha fazla bulunmuştur (Yılmaz, 2018). Diğer yandan çevrimiçi olarak gerçekleştirilen alışveriş, etkileşim, yayıncılık ve çevrimiçi indirme gibi davranışların, siber suç korkusu üzerinde belirleyici etkiye sahip olduğu ifade edilmektedir (Yu, 2014).

İlgili yazında mağduriyet riski algısının, siber suç korkusu belirleyicilerinden birisi olduğu belirtilmektedir. Henson'un 2011 yılında siber taciz mağduriyeti üzerine yaptığı araştırmada, siber taciz korkusu ve siber taciz riski algısı arasında ilişki olduğu

belirtilmektedir. Dolayısıyla yakın arkadaş veya bir yabancı tarafından siber taciz riski algısı ile yakın bir arkadaş, tanıdık veya bir yabancı tarafından siber taciz edilme korkusu arasında pozitif yönde anlamlı ilişki bulunduğu tespit edilmiştir (Henson, 2011; Yılmaz,2018).

Yukarıdaki bilgiler ışığında, farklı siber suç türleri için siber suç korkusunun belirleyicilerinin farklılaşabileceğinin dikkate alınması önemli görülmektedir. Dolayısıyla siber suç korkusuna spesifik suçlar temelinde yaklaşılması daha doğru olabilir. Siber suçlara yönelik önlem alma stratejilerinin siber suç korkusunun önlenmesi veya azaltılmasında etkisi olabilir. Önceki bölümde belirtildiği üzere çeşitli yöntemler kullanılarak dünyanın herhangi bir yerinden çok uzak başka bir noktaya siber saldırılar gerçekleşebilmekte ve böylece suç eylemi oluşabilmektedir. Öte yandan yeni suç türlerinin ortaya çıkması söz konusu olabilmekle birlikte bilinen suç davranışlarının siber ortamda daha kolay şekilde gerçekleştirilmesi söz konusu olabilmektedir. Bu bağlamda, elektronik ağlar üzerinden siber suçların herhangi bir zamanda anlık olarak gerçekleşebileceği göz önüne alındığında tahmin edilmesinin de olanaksız olabileceği belirtilebilir (Ehliz, 2019).

Günümüz toplumlarında küreselleşme ve teknolojik gelişmelerle birlikte fiziksel mesafeler ortadan kalkmaktadır. Bu gelişim ve dönüşüm yoluyla iletişim ve ulaşımın kolaylaşmasının yanı sıra dünyanın herhangi bir yerinden gelebilecek tehlikelere açık hale gelinmektedir. Bahsi geçen tehlikelerin en önemlilerinden birisi de siber suçlardır. Mekân ve zamandan bağımsız bir şekilde gerçekleştirilen siber suçların önlenmesinin bir takım güçlükleri mevcuttur. Kullanılan yazılım sistemleri ile devletlere ait bilgilerin ve güvenlik tedbirleri gibi oldukça önemli bilgilerin ele geçirilmesi tehdidiyle karşılaşan devletler, bu kapsamda güvenlik tedbirleri oluşturmaya çalışmaktadır (Sunay ve Birel, 2023). Türkiye'de siber suçlara yönelik oluşturulan siber tedbirler; hukuki boyut ve dijital suçlarla ilgili yapılan düzenlemeler, polisiye ve teknik yöntemler olmak üzere üç ana başlık altında toplanabilmektedir. Bu tedbirler aşağıda sıralanmıştır:

26.09.2004 tarihli 5237 sayılı Türk Ceza Kanunu'nda siber suçlar, farklı bir başlık altında toplanarak ayrıntılı bir şekilde hukuki düzenlemeler yapılmıştır.

Kaçakçılık ve Organize Suçlarla Mücadele Daire Başkanlığı bünyesinde kurulan Bilişim Suçları ve Sistemleri Şube Müdürlüğü 2010 yılında ikiye bölünmüştür. Bilişim Suçları Şube Müdürlüğü, tek başına ayrı bir müdürlük olarak devam etmektedir.

Adli bilişim ve siber güvenlik süreçleri olarak ikiye ayrılan teknik yöntemler, suçun işlenmiş olduğu siber uzay ortamda, bazı teknik yöntemlerle (geriye dönük kayıt ve veri

toplama, silinen kaybolan verileri geri getirme, veri analizi vb. süreçler) suçu aydınlatmaya yönelik delilleri toplamaktır (Bilgi Teknolojileri ve İletişim Kurumu, 2022).

Siber suçları önlemeye yönelik oluşturulan önlem alma stratejileri; güçlü parolalar kullanılması, mobil cihazların ve bilgisayarların güvenliğinin sağlanması (güvenlik duvarının etkinleştirilmesi, antivirüs ve kötü amaçlı yazılım kullanımı, casus yazılım saldırılarını engellemek), sosyal medya kullanımında bilinçli olmak, mobil cihazları güvenli hale getirmek, işletim sistemlerini güncel tutmak, verilerin korunması, kablosuz ağların güvenli hale getirilmesi, kimlik bilgilerinin korunması, dolandırıcılığa karşı dikkatli olunması ve doğru kişi veya kişilerden yardım istenmesi olarak on adımda özetlenebilir. Bu adımlar aşağıda detaylandırılmıştır (https://pcpc.gov.in/files/1.pdf):

Güçlü parolalar kullanılması: Farklı hesaplar için farklı kullanıcı kimliği veya şifre kombinasyonları kullanarak harfleri, sayıları ve özel karakterleri (toplamda en az 10 karakter) birleştirip şifreleri daha karmaşık hale getirmek ve bunları düzenli aralıklarla değiştirmek.

Mobil cihazların ve bilgisayarların güvenliğinin sağlanması:

1. Güvenlik duvarının etkinleştirilmesi: Güvenlik duvarının etkinleştirilmesi, siber saldırılara yönelik savunmanın ilk adımı olup kaynağı bilinmeyen, zararlı ve sahte sitelere bağlantıları engellemekte ve virüslerin cihazlara erişimini engellemektedir.
2. Antivirüs ve kötü amaçlı yazılım kullanımı: Virüsten koruma yazılımı yükleyerek ve yazılımı düzenli olarak güncelleyerek virüslerin bilgisayarlara veya mobil cihazlara bulaşması önlenmektedir.
3. Casus yazılım saldırılarını engellemek: Casus yazılımı saldırılarını önleyecek programlar yüklemek, casus yazılımların ve saldırıların bilgisayarlara sızmasını engellemektedir. Bu programların düzenli olarak güncelleştirilmesi de bu saldırıları engelleyebilmektedir.

Sosyal medya kullanımında bilinçli olmak: Sosyal medyada hangi bilgilerin yayınlandığına dikkat edilmesi gibi sosyal medyanın bilinçli olarak kullanılması gerekmektedir. Aynı zamanda güvenlik duvarının da kontrol edilmesi, siber suçlara yönelik savunmanın bir diğer adımını oluşturmaktadır.

Mobil cihazları güvenli hale getirmek: Mobil cihazların virüslere ve bilgisayar korsanlarına karşı savunmasız durumda olduğu göz önünde bulundurularak uygulamalar güvenilir kaynaklardan indirilmelidir.

İşletim sistemlerini güncel tutmak: İşletim sistemlerini güncel tutmak, uygulamaları ve işletim sistemini korumaktadır. Eski yazılımlara olası siber saldırıları önlemek için otomatik güncellemeleri açmak gerekli olmaktadır.

Verilerin korunması: Kişisel ve özel bilgileri içeren dosyalar için şifreleme yöntemi kullanımı, önemli dosyaların düzenli olarak yedeklemelerinin alınması ve başka bir dosyada saklanılması, siber saldırılara karşı savunmanın bir diğer önemli yöntemidir.

Kablosuz ağların güvenli hale getirilmesi: Kullanılan Wi-Fi (kablosuz) ağları, düzgün bir şekilde korunmadıkları takdirde izinsiz girişlere karşı savunmasızdır. Bu sebeple, güvenlik ayarlarının kontrol edilip değiştirilmesi gerekebilmektedir. Güvenli olmayan kablosuz ağlarda siber saldırılara maruz kalmamak için finansal veya kurumsal işlemler yapmaktan kaçınılmalıdır.

Kimlik bilgilerinin korunması: Çevrimiçi ortamlarda isim, adres, telefon numarası veya finansal bilgiler gibi kişisel bilgilerin paylaşılmasında dikkatli olunması gerekmektedir. Ayrıca web sitelerinin güvenli olduğundan (örneğin, çevrimiçi alışveriş yaparken) emin olunması ve gizlilik ayarlarının etkinleştirilmesi (örneğin, sosyal ağ sitelerine erişirken) önemlidir.

Dolandırıcılığa karşı dikkatli olunması: Kaynağı bilinmeyen bir bağlantıya veya dosyaya giriş yapılmaması, e-posta veya mesajların kaynağının kontrol edilmesi ve kaynağın doğrulanması, siber ortamda dolandırıcılığa maruz kalmamak adına en etkili yöntemlerdendir. Bilgilerin doğrulanmasını veya kullanıcı kimliğinin ya da parolanın doğrulamasını isteyen e-postalar yanıtlanmamalıdır. Bu önlemler, siber suçlara yönelik oluşturulan etkili stratejilerdendir.

Doğru kişi veya kişilerden yardım istenmesi: Herhangi bir siber suç saldırısı ile karşı karşıya kalınması durumunda (örneğin, çocuk istismarı gibi yasa dışı internet içeriği veya ticari bir dolandırıcılık), bu konuda yetkili kişilerden yardım istenilmesi, siber suçları önlemeye yönelik oluşturulan bir yöntemdir.

İKİNCİ BÖLÜM

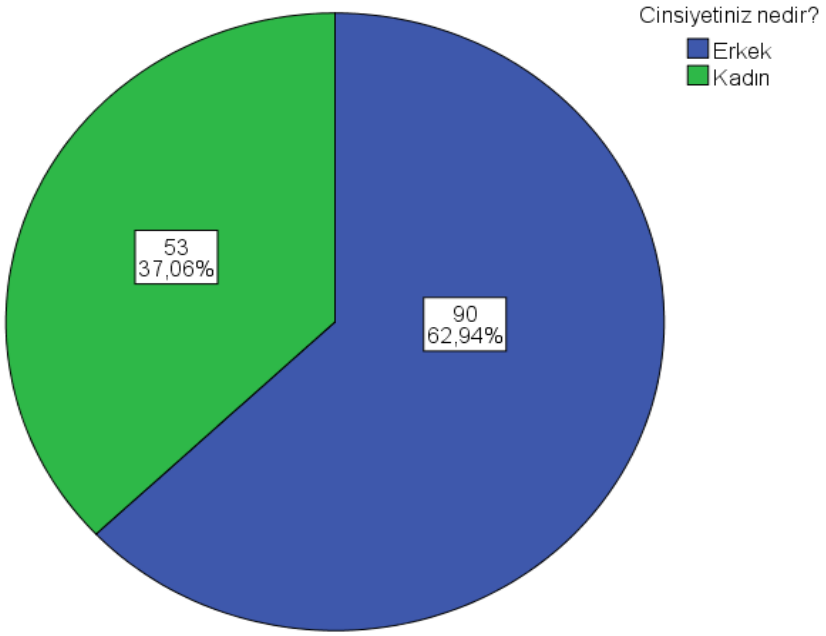
METODOLOJİ

2.1. Araştırma Deseni: Nicel Araştırma

Bilim, olgu ve olayları, tarafsız ve önyargısız bir şekilde doğrulama ve anlama yöntemidir. Araştırma yöntemleri, bilimsel düşüncenin bir sonucu olmakla birlikte bilimsel araştırma, karşılıklı olarak etkilenilen ve takip edilen aşama ya da etkinliklerden oluşan sistematik bir süreçtir (Büyüköztürk, 2013). Bilimsel araştırmalar, nitel ve nicel araştırma olarak iki şekilde gerçekleştirilmektedir. Nitel araştırma, gözlem ve görüşme gibi nitel veri toplama tekniklerinin kullanıldığı, olgu ve olayların gerçekçi ve bütüncül bir yaklaşımla açıklanması amacıyla belirli süreçlerin takip edildiği araştırma türüdür (Aydın, 2018). Nicel araştırmalar, sayısal olarak ölçülebilen verilerin istatistiksel analizleri ile sosyal olguların incelendiği ve bu sosyal olgular arasında neden - sonuç ilişkilerinin tespit edilerek toplumsal düzenin kanunlarını belirlemeyi amaçlayan araştırmalardır. Başka bir ifadeyle, daha önceden oluşturulmuş olan hipotezlerin test edilmesi amacıyla, geniş kapsamlı örneklemlerden nicel veriler toplayarak, bu verilerin istatistiki olarak çözümlenmesini sağlayan ve ulaşılan sonuçları genelleme amacı taşıyan araştırmalardır. Nicel veriler; gözlem, anket, alan araştırmaları ya da görüşmeler yoluyla elde edilebilmektedir (https://www.bingol.edu.tr/media/204988/sayt-bolum8-Sosyolojide-Nicel-ve-Nitel-Arastirma-Yontemleri.pdf). Bu çalışma, nicel yöntemli olarak tasarlanmıştır. Siber suç korkusu ve önlem alma staratejilerine dair bir teknokentteki genel görünümü nicel yöntemle kapsayıcı bir şekilde tasvir edebilmenin ve betimleyebilmenin olanaklı olduğu düşünülmektedir.

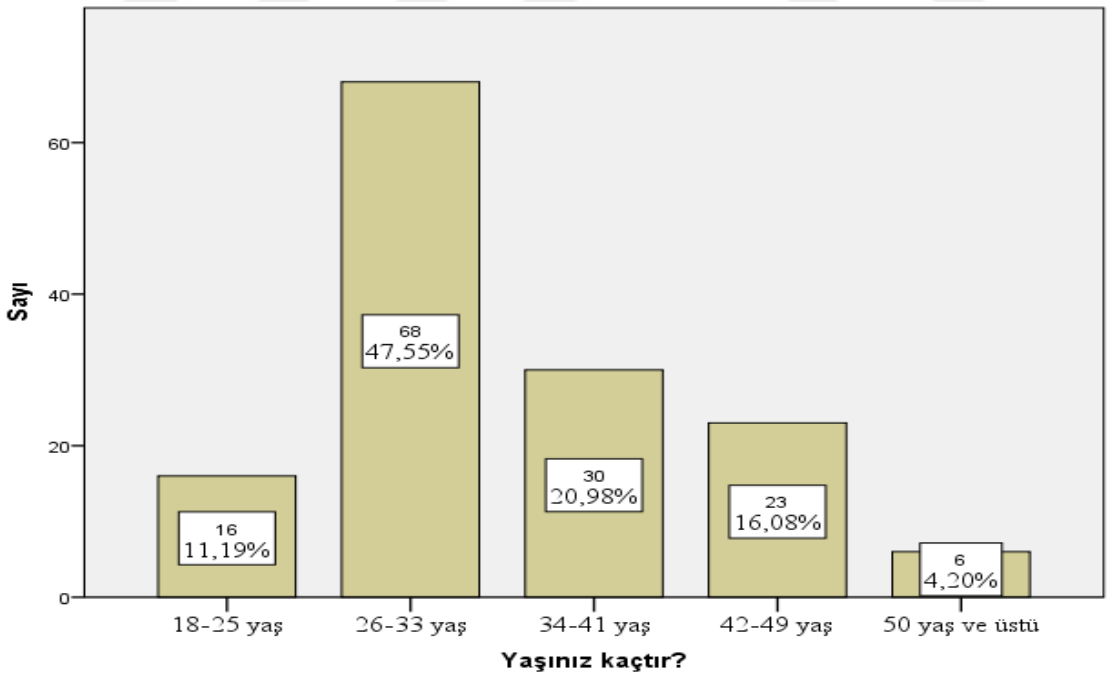
2.2. Çalışma Grubu

Bu çalışmanın evrenini, araştırmanın gerçekleştirildiği tarihte Türkiye'de aktif faaliyet gösteren 81 teknokentte hizmet sunan kişiler oluşturmaktadır. Örneklemi ise Trabzon ilinde faaliyet gösteren bir Teknokent'te hizmet sunup bu araştırmaya katılmaya onay veren 143 kişi oluşturmaktadır. Aşağıda araştırmanın katılımcılarına ait betimsel istatistik bulguları sıralanmıştır:



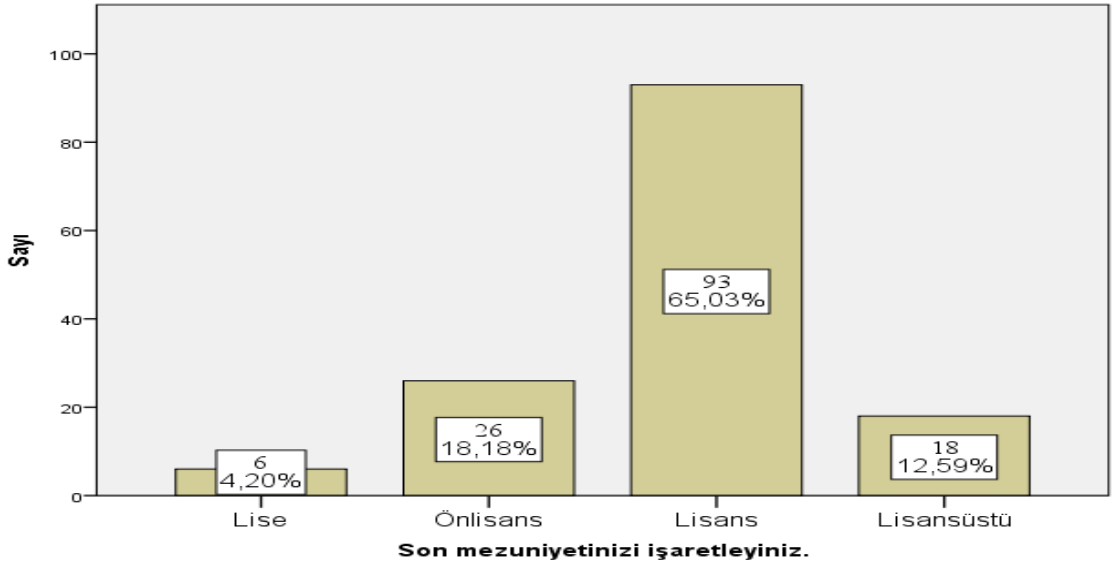
Şekil 2.1. Katılımcıların Cinsiyet Dağılımları

Çalışmanın katılımcı sayısı toplamda 143 kişi olup; %62,94'ü erkek katılımcı, %37,06'sı kadın katılımcıdan oluşmaktadır.



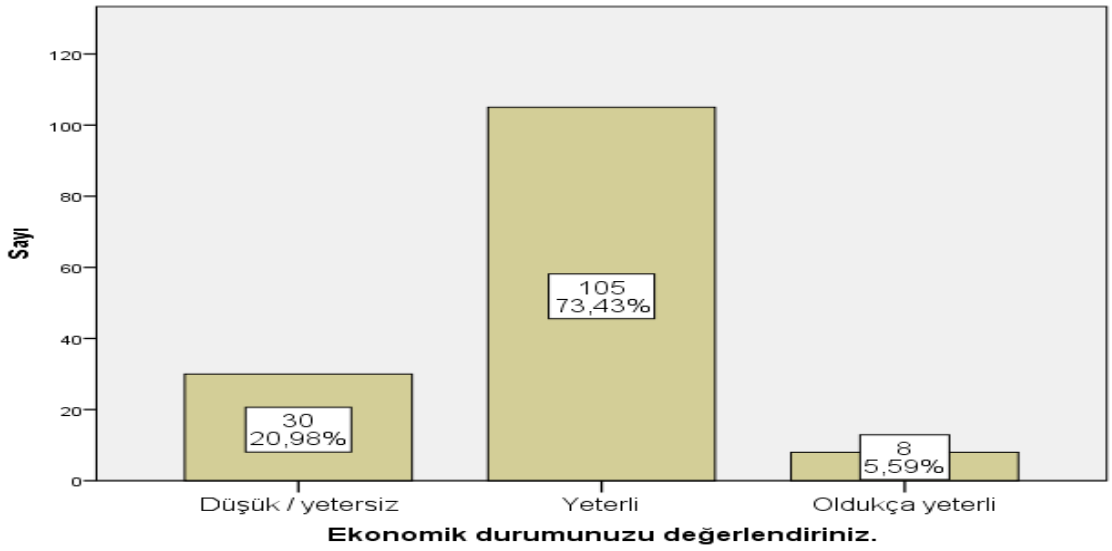
Şekil 2.2. Katılımcıların Yaş Dağılımları

Katılımcıların yaşları dört gruba ayrılmış olup; 18-25 yaş arası katılımcılar %11,19, 26-33 yaş arası katılımcılar %47,55, 34-41 yaş arası katılımcılar %20,98, 42-49 yaş arası katılımcılar %16,08, 50 yaş üstü katılımcılar ise %4,20'lik kısımdan oluşmaktadır.



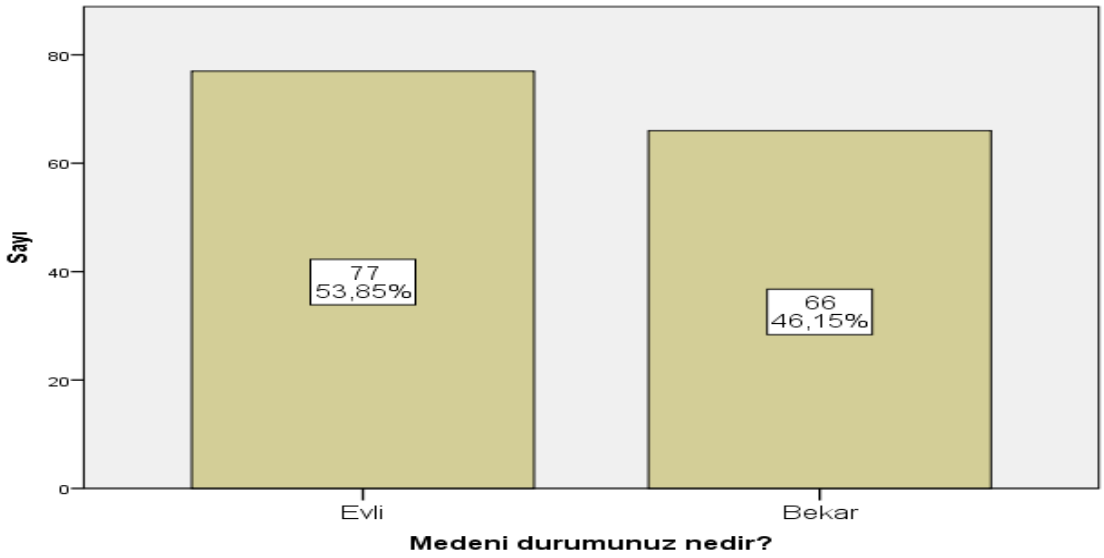
Şekil 2.3. Katılımcıların Eğitim Durumu Dağılımları

Katılımcıların eğitim düzeyleri lise, önlisans, lisans ve lisansüstü olarak dört gruba ayrılmış olup; lise mezunu katılımcılar %4,20, önlisans mezunu katılımcılar %18,18, lisans mezunu katılımcılar %65,03, lisansüstü mezunu katılımcılar %12,59'luk kısmı oluşturmaktadır.



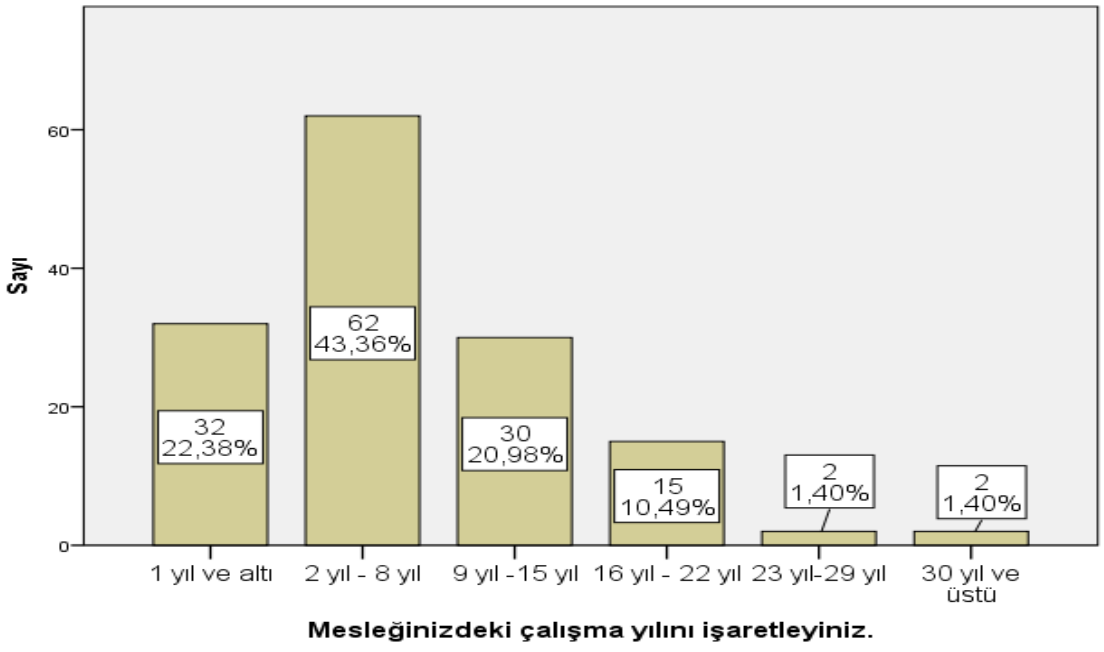
Şekil 2.4. Katılımcıların Ekonomik Durum Değerlendirmeleri

Katılımcıların ekonomik durum algıları düşük/yetersiz, yeterli ve oldukça yeterli olmak üzere üç gruba ayrılmış olup; ekonomik durum algısı düşük/yetersiz olarak belirten katılımcı %20,98, yeterli olarak belirtenler %73,43, oldukça yeterli olarak belirtenler ise %5,59'luk kısmı oluşturmaktadır.



Şekil 2.5. Katılımcıların Medeni Hal Dağılımları

Katılımcıların medeni durum dağılımına bakıldığında evli olanlar %53,85, bekâr olanlar ise %46,15'lik kısmı oluşturmaktadır.



Şekil 2.6. Katılımcıların Mesleki Tecrübe Dağılımları

Katılımcıların mesleklerinde çalışma yılları 1 yıl ve altı, 2-8 yıl, 9-15 yıl, 16-22 yıl, 23-29 yıl, 30 yıl ve üstü olmak üzere toplamda 6 gruba ayrılmış olup; katılımcıların mesleki çalışma yılının 1 yıl ve altı olan kısım %22,38, 2-8 yıl arası %43,36, 9-15 yıl %20,98, 16-22 yıl %10,49, 23-29 yıl arası %1,40, 30 yıl ve üstü ise %1,40'lık dilimini kaplamaktadır.

Katılımcıların Trabzon Teknokent kurumundaki görev dağılımları oldukça geniş bir yelpazede olup, bu görev dağılımları; yönetici, muhasebe, teknik personel, mühendis, ar-ge uzmanı, yazılımcı vb. şeklindedir. Katılımcıların görev aldıkları sektörler ise yazılım ve bilişim teknolojileri, elektrik ve elektronik, makine, biyoteknoloji, enerji, sağlık- medikal, gıda, kimya, savunma, mimarlık, inşaat, orman ve denizcilik olmak üzere 13 farklı alandan oluşmaktadır.

2.3. Veri Toplama Aracı: Yüz Yüze ve Web Tabanlı Anket Çalışması

Geliştirilen hipotezlerin test edilebilmesi amacıyla araştırma evrenini temsil etmesi sebebiyle seçilen örnekleme yöneltmek üzere 45 sorudan oluşan anket formu oluşturulmuştur. Anket sorularının oluşturulmasında daha önce suç korkusu ve siber suç korkusunun ölçülebilmesi amacıyla oluşturulmuş ve literatürde yer alan farklı çalışmalarda kullanılan ve geliştirilen sorular araştırılmıştır.

Araştırmada kullanılan anket formunun ilk bölümü genel ve sosyodemografik sorular olarak altı kapalı uçlu ve iki açık uçlu olmak üzere toplam 8 sorudan oluşmaktadır. Bu sorular katılımcının "yaşı, cinsiyeti, gelir ve eğitim durumu, medeni hali, meslekteki çalışma yılı, çalıştığı kurumdaki konumu ve çalışılan kurumun hangi alanda faaliyet gösterdiği" sorularından oluşmaktadır. Anket formunun diğer bölümünde yer alan sorular aşağıda sıralanmıştır:

1. Ne zamandır internet kullanıcısısınız?

2. İnternete en çok hangi araçlardan erişim sağlıyorsunuz?

3. Gününüzün ne kadarlık bölümünü internete bağlı olarak geçiyorsunuz?

4. Sosyal medya kullanıcısı mısınız?

5. Finansal işlemlerinizi daha sıklıkla internet üzerinden yapmayı tercih ediyor musunuz?

6. İnternet ortamında kullanılan hesapların şifrelerini genellikle ne sıklıkla değiştiriyorsunuz?

7. Bu zamana kadar siber suç mağduriyeti yaşadınız mı? (banka hesap numaranızın, sosyal medya hesabınızın, e-posta hesabınızın veya başlıca kişisel verilerinizin ele geçirilmesi veya verilerinizin çalınması suretiyle tarafınıza yönelik sahte hesap açılması, siber zorbalık, siber hırsızlık, siber ortamda haberleşme gizliliğinizin ihlali gibi)

8. Siber suçları önlemeye yönelik mevcut yasal mevzuatı/yazılı düzenlemeleri yeterli buluyor musunuz?

9. Siber suçların mağduru olmamak için almış olduğunuz bireysel önlemlerin yeterliliği ne düzeydedir?

10. Kamuya açık alanlarda bulunan kablosuz ağlara erişim sağlıyor musunuz?

11. Kullandığınız şifreler benzer mi farklı mı?

12. Şifrelerinizi başkaları ile paylaşır mısınız?

13. Sosyal medya hesaplarınızı başka sitelere erişim için de kullanır mısınız?

14. Sanal ortamdaki hesaplarınıza erişirken "iki faktörlü koruma" sistemi kullanıyor musunuz?

15. Telefonunuza erişmek için herhangi bir kod, şifre veya başka bir güvenlik tedbiri kullanıyor musunuz?

16. Telefonunuzda bulunan uygulamaları günceller misiniz?

17. Cihazlarınızın işletim sistemini günceller misiniz?

18. Antivirüs programı kullanıyor musunuz?

Anket formunun bir bölümü, Trabzon Teknokent çalışanlarının çeşitli siber suçların mağduru olma korkusunun düzeyini belirlemek amacıyla oluşturulmuş olup, her bir suç türü için “mağdur olmak konusunda hiç korku yaşamıyorum, mağdur olmak konusunda biraz korku duyuyorum, mağdur olmak konusunda orta düzeyde korku duyuyorum, mağdur olmak konusunda çok korku duyuyorum, mağdur olmak konusunda aşırı düzeyde korku duyuyorum” olmak üzere beş seçenek ve 18 sorudan oluşmaktadır.

İlgili sorular; “E-posta veya sosyal paylaşım sitelerine ait parolalarınızın çalınması konusunda, banka hesap bilgilerinizin (hesap/kart numarası vb.) çalınması yoluyla zarara uğratılmanız konusunda, kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalmanız konusunda, bilgisayar korsanlığına (kişisel bilgisayarınıza

veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalmanız konusunda, truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalmanız konusunda, keylogger ve screenlogger gibi casus yazılımlara (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde kaydedilmesi) maruz kalmanız konusunda, siber zorbalığa (internet erişimli cihazınız vasıtasıyla ısrarcı, tekrarlayıcı ve zarar verici türden davranışlar; siber ortamlarda izniniz olmadan fotoğraflarınızın yayınlanması, spam içeren e-postalar almanız, siber ortamda ısrarlı şekilde rahatsız edilmeniz veya hakarete uğramanız gibi) maruz kalmanız konusunda, siber tacize (siber ortamda taciz davranışlarına) maruz kalmanız konusunda, siber şantaja veya siber tehdide (siber ortamda şantaj veya tehdit davranışlarına) maruz kalmanız konusunda, siber hırsızlığa (internet ortamındaki hesaplarınızdan mali varlığınızın/paranızın çalınmasına) maruz kalmanız konusunda, siber ortamda haberleşme gizliliğinizin ihlali (kayıt altına alınması ya da ifşası gibi) konusunda, siber dolandırıcılığa (örneğin, internet ortamında satılıyor gibi görünen fakat gerçekte olmayan ürünü para ödeyerek almanız) maruz kalmanız konusunda, sniffing'e (bir ağ üzerindeki bilgisayarlar arasındaki veri trafiğinin dinlenmesi suretiyle şifrelerinizin ele geçirilmesi) maruz kalmanız konusunda, zombi ordulara (haberiniz olmaksızın internet erişimli cihazınızın ciddi suçlar işlenmesi amacıyla kullanılması) maruz kalmanız konusunda, sosyal ağ üzerinden sahtekârlığa (örneğin, sosyal medya hesaplarına erişim sağlayan kişiler tarafından o hesapta yer alan kişilerden acil maddi destek talep edilmesi) maruz kalmanız konusunda, siber yer tespitine (çevrimiçi kaynaklardaki veriler vasıtasıyla coğrafi konumunuzun tespit edilmesi) maruz kalmanız konusunda, bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalmanız konusunda ve siber terörizme (bilgisayar sistemlerini kullanılarak terör faaliyetlerinin icrası) maruz kalmanız konusunda suç mağduru olma korkunuz nedir?" şeklindedir.

2.4. İşlem

Araştırmanın yürütülebilmesi için öncelikle Trabzon Teknokent yönetimine kurum uygulama izni için bulunulmuştur. Uygulama izninin alınmasını müteakip Jandarma ve Sahil Güvenlik Akademisi Etik Kurulu'ndan 09.06.23 tarihli ve 2023/2 sayılı Etik Kurul Onayı alınmıştır. Bu işlemlerin ardından Trabzon Teknokent çalışanlarına araştırmacı tarafından Bilgilendirilmiş Onam Formu sunulmuştur. Bilgilendirilmiş Onam Formu'na onay veren katılımcılara ilgili anket formu sunularak veri toplama işlemi bir aylık sürede tamamlanmıştır.

Bu araştırmanın veri toplama yöntemini, araştırmacı tarafından yüz yüze olarak uygulanan anket çalışması ve web tabanlı (inter-survey) anket çalışması oluşturmuştur. Web tabanlı anket uygulaması, Teknokent'teki katılımcılarla birebir yapılan görüşmelerde katılımcıların web tabanlı anket çalışmasını doldurmayı tercih etmeleri durumunda anket adresinin paylaşılarak anketi doldurmalarıyla gerçekleşmiştir.

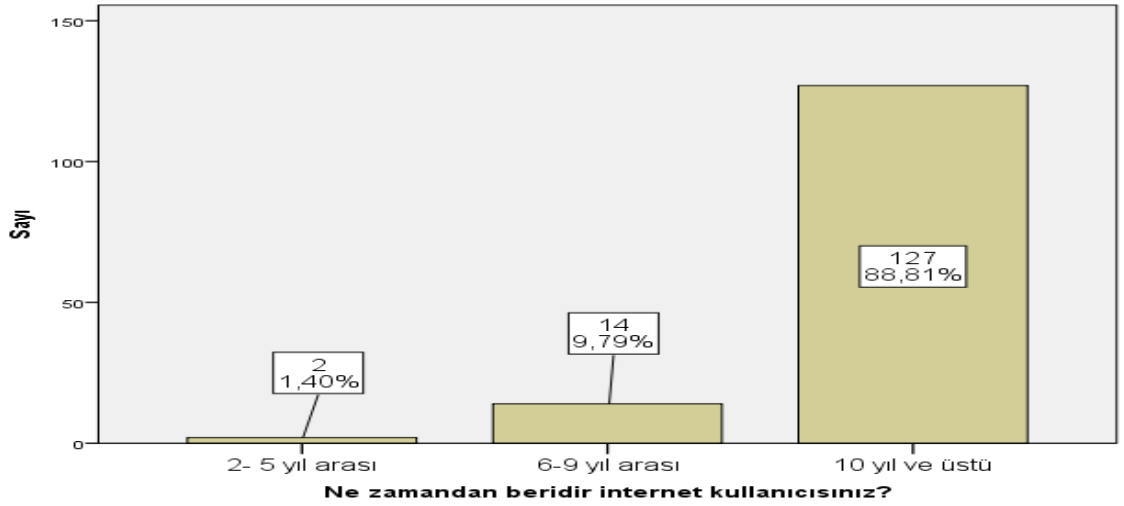
Veriler uygun paket programa girilerek istatistiksel analizler yapılmıştır. Kategorik veriler, frekans ve yüzde olarak gösterilmiş olup gruplara göre kategorik değişkenler arasındaki farklılık karşılaştırmalarında beklenen değer sayısı 5 ve üzerinde olan ya da beklenen değer sayısı 5'in altında olan hücrelerin oranı %20'yi geçmeyen RxC tablolarda Pearson ki-kare, beklenen değer sayısı 5'in altında olan hücrelerin oranı %20'yi geçen RxC tablolarda ise Fisher Freeman Halton testi kullanılmıştır. İstatiksel anlamlılık, $p<0.05$ olarak kabul edilmiştir.

ÜÇÜNCÜ BÖLÜM

BULGULAR

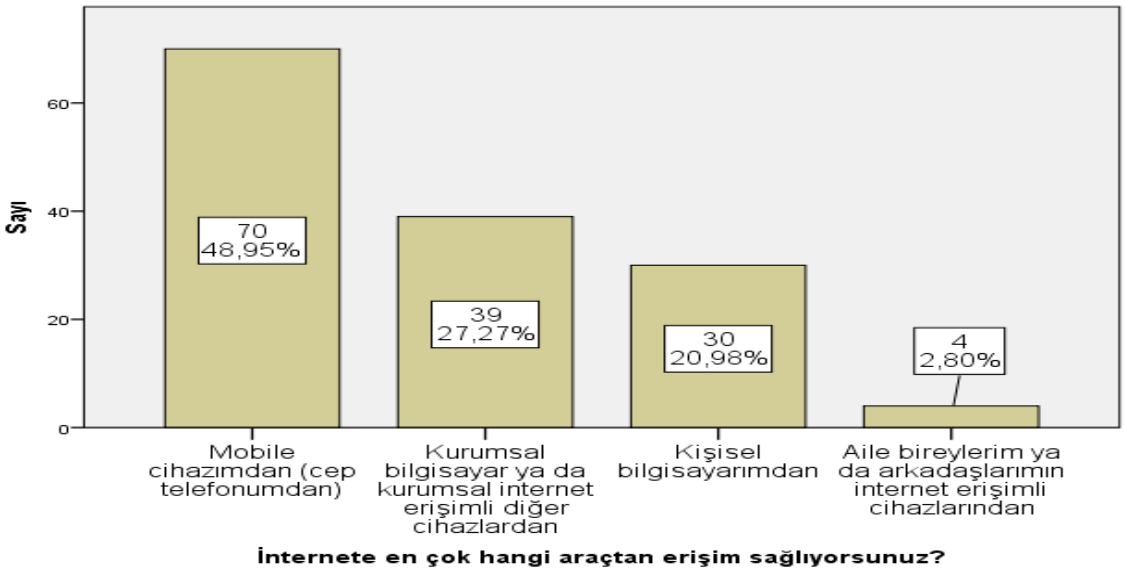
Çalışmanın bu bölümünde, katılımcılara yöneltilen soruların analizi sonucu elde edilen bulgular sıralanmıştır.

3.1. Betimsel İstatistik



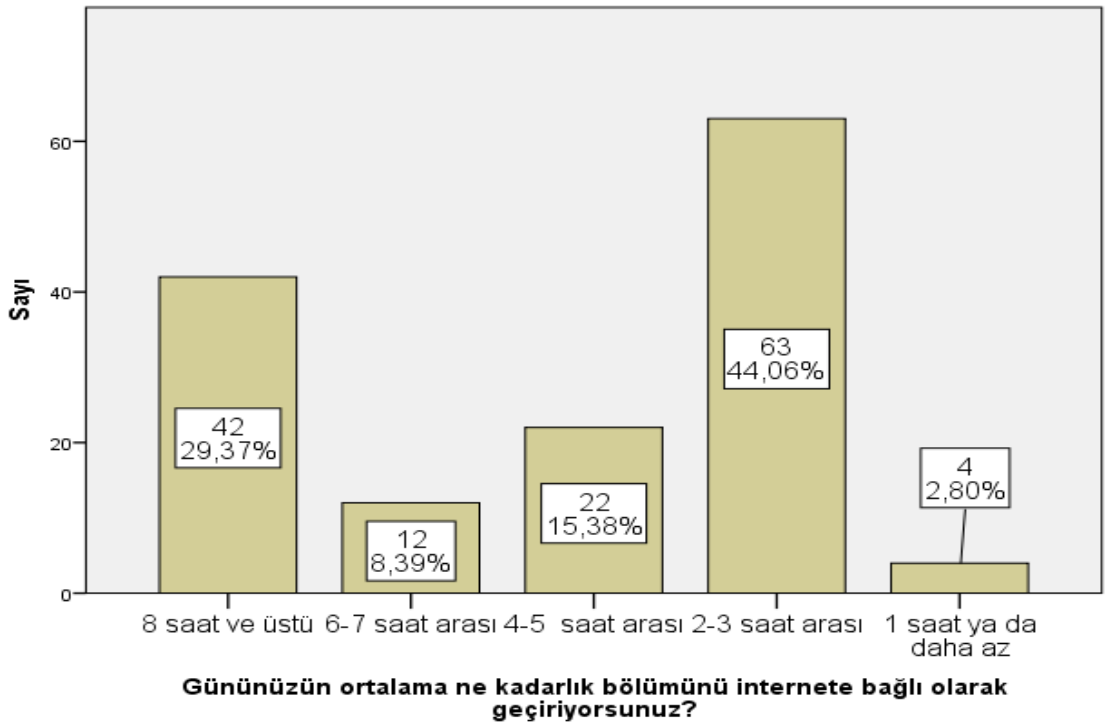
Şekil 3.1. Katılımcıların İnternet Kullanma Geçmişine İlişkin Dağılımları

Katılımcıların "Ne zamandan beridir internet kullanıcısısınız?" sorusuna sunulan seçenekler 2-5 yıl arası, 6-9 yıl arası, 10 yıl ve üstü şeklindedir. 2-5 yıl arası internet kullanıcısı olanlar %1,40, 6-9 yıl arası %9,79, 10 yıl ve üstü internet kullanıcısı olanlar ise %88,81'lik kısımdan oluşmaktadır.



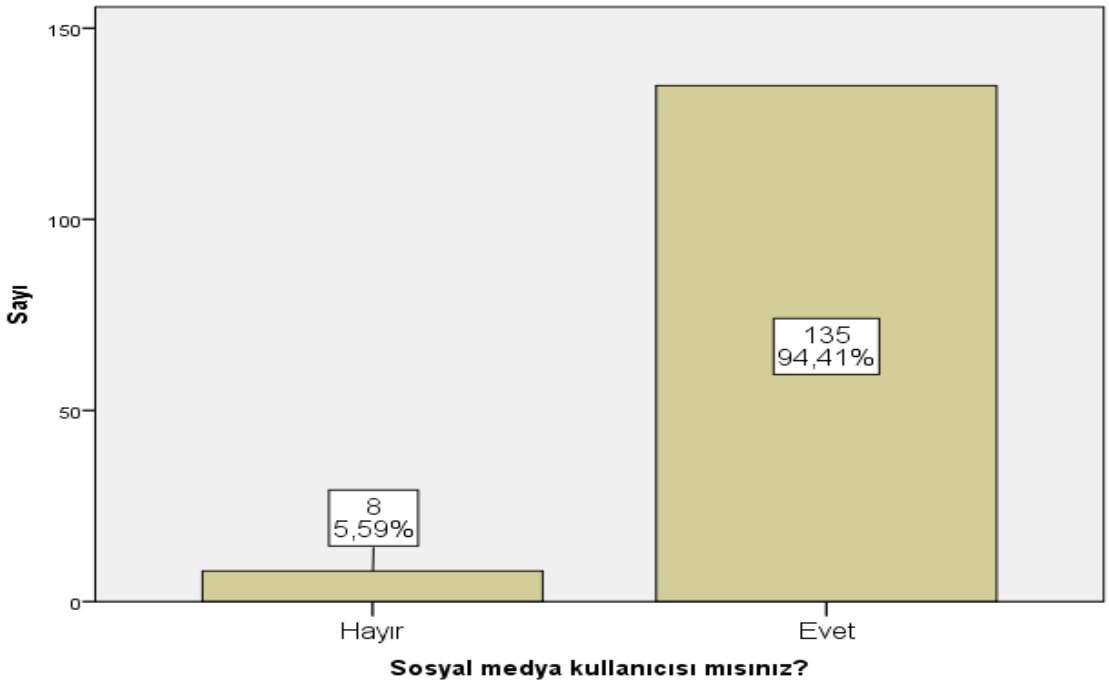
Şekil 3.2. Katılımcıların İnternete Erişim Aracı Dağılımları

Katılımcıların “İnternete en çok hangi araçtan erişim sağlıyorsunuz?” sorusuna sunulan seçenekler; mobil cihazımdan, kurumsal bilgisayar ya da kurumsal internet erişimli diğer cihazlardan, kişisel bilgisayarımdan, aile bireylerim ya da arkadaşlarımın internet erişimli cihazlarından olmak üzere dört gruba ayrılmıştır. İnternete mobil cihazdan erişim sağlayan katılımcılar %48,95, kurumsal bilgisayar ya da kurumsal internet erişimli diğer cihazlardan erişim sağlayanlar %27,27, kişisel bilgisayarından erişim sağlayanlar %20,98, aile bireylerim ya da arkadaşlarımın internet erişimli cihazlarından erişim sağlıyorum cevabını verenler %2,80’lik kısımdan oluşmaktadır.



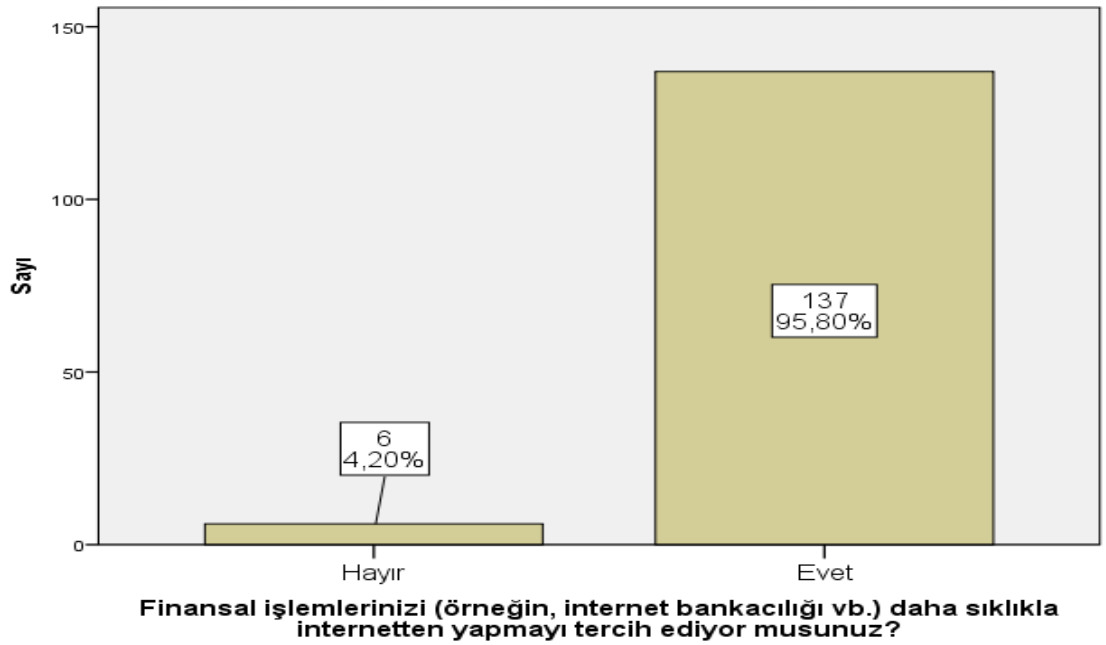
Şekil 3.3. Katılımcıların Günlük İnternette Geçirdikleri Süre Dağılımları

Katılımcıların günlük internette geçirdikleri süre dağılımları 8 saat ve üstü, 6-7 saat arası, 4-5 saat arası, 2-3 saat arası, 1 saat ya da daha az olarak beş gruba ayrılmış olup; 8 saat ve üstü olarak belirtenler %29,37, 6-7 saat arası %8,39, 4-5 saat arası %15,38, 2-3 saat arası %44,06, 1 saat ya da daha az ise %2,80’lik kısımdan oluşmaktadır.



Şekil 3.4. Katılımcıların Sosyal Medya Kullanım Dağılımları

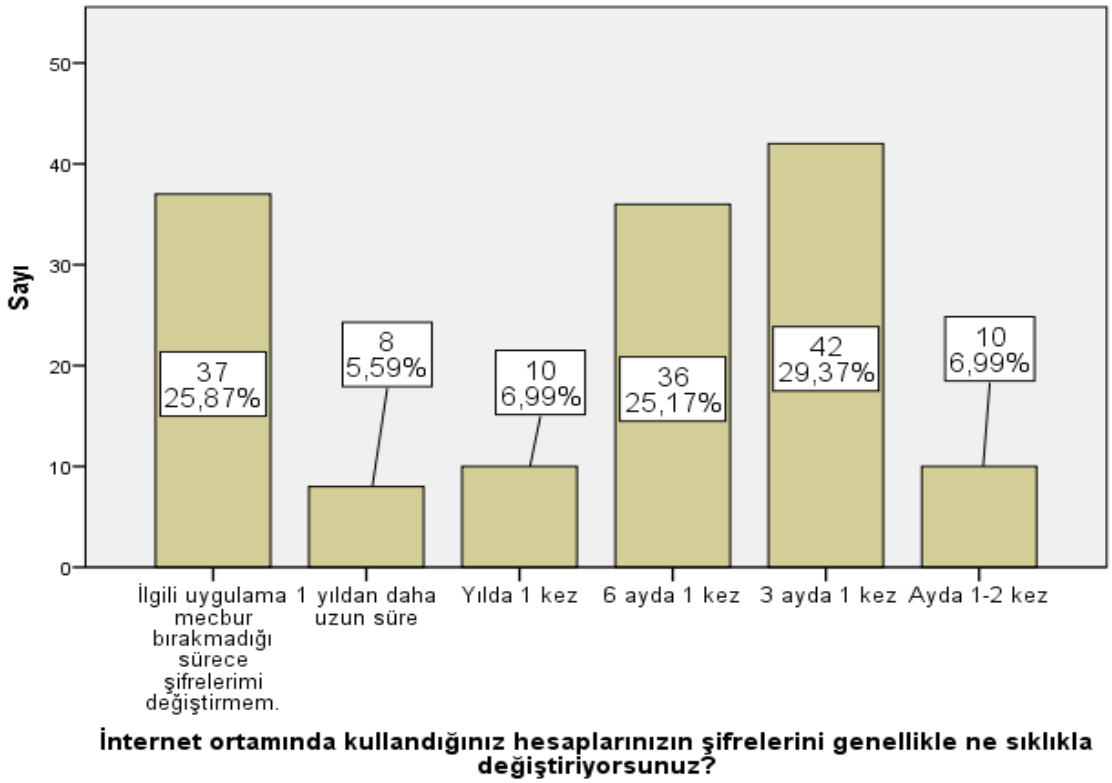
Katılımcıların sosyal medya kullanım dağılımlarını belirlemek amacıyla oluşturulan "Sosyal medya kullanıcı mısınız?" sorusu yöneltilmiş olup evet olarak cevaplayanlar %94,41, hayır olarak cevaplayanların oranı %5,59'dur.



Şekil 3.5. Finansal İşlemlerini İnternetten Yapan Katılımcıların Dağılımları

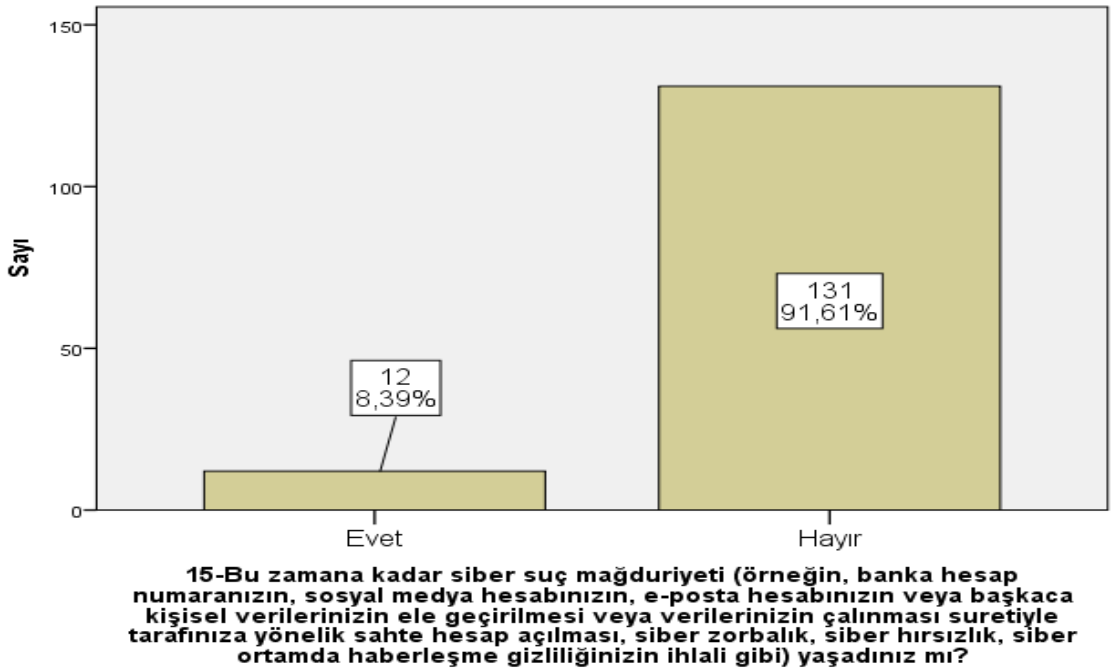
Katılımcıların finansal işlemlerini internetten yapanların dağılımlarını belirlemek amacıyla "Finansal işlemlerinizi (internet bankacılığı vb.) daha sıklıkla yapmayı tercih

ediyor musunuz?" sorusu yöneltilmiş olup evet cevabını veren katılımcı %95,80, hayır cevabını veren katılımcı %4,20'dir.



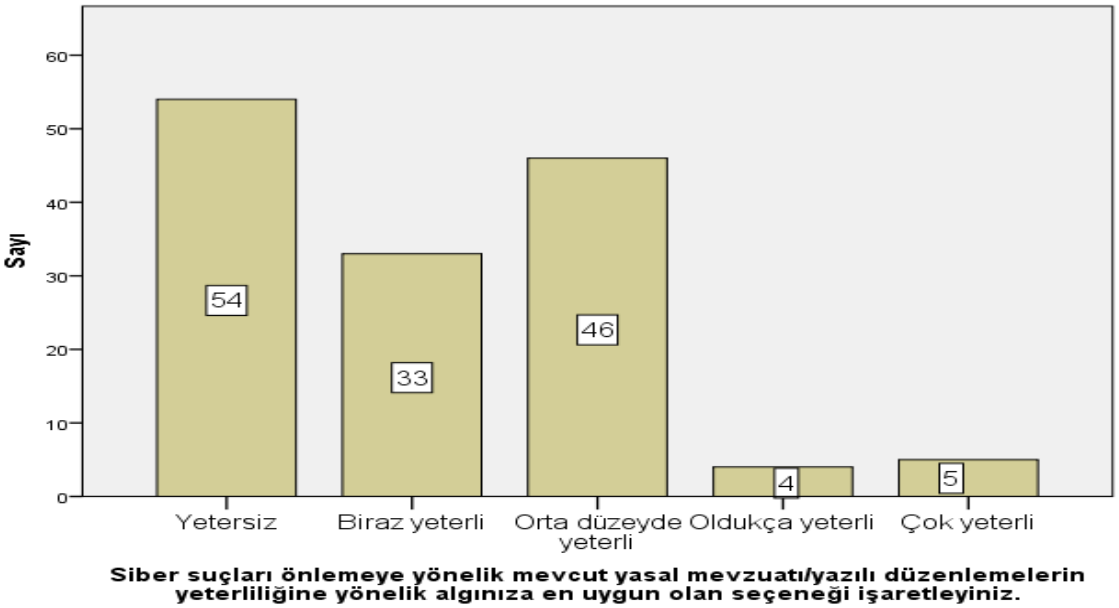
Şekil 3.6. Katılımcıların Şifrelerini Değiştirme Sıklığına İlişkin Dağılımlar

Katılımcıların şifrelerini değiştirme sıklığına ilişkin dağılımları belirlemek amacıyla oluşturulan "İnternet ortamında kullandığınız hesapların şifrelerini genellikle ne sıklıkla değiştiriyorsunuz?" sorusu katılımcılara sorulmuş olup; ilgili uygulama mecbur bırakmadığı sürece şifrelerimi değiştirmem, 1 yıldan daha uzun süre, yılda 1 kez, 6 ayda 1 kez, 3 ayda bir kez, ayda 1-2 kez şeklinde altı gruba ayrılmıştır. İlgili uygulama mecbur bırakmadığı sürece şifrelerimi değiştirmem cevabını veren katılımcı %25,87, 1 yıldan daha uzun süre cevabını veren katılımcı %5,59, yılda 1 kez cevabını veren katılımcı %6,99, 6 ayda bir kez %25,17, 3 ayda 1 kez cevabını veren katılımcı %29,37, ayda 1-2 kez cevabını veren katılımcı %6,99'luk kısımdan oluşmaktadır.



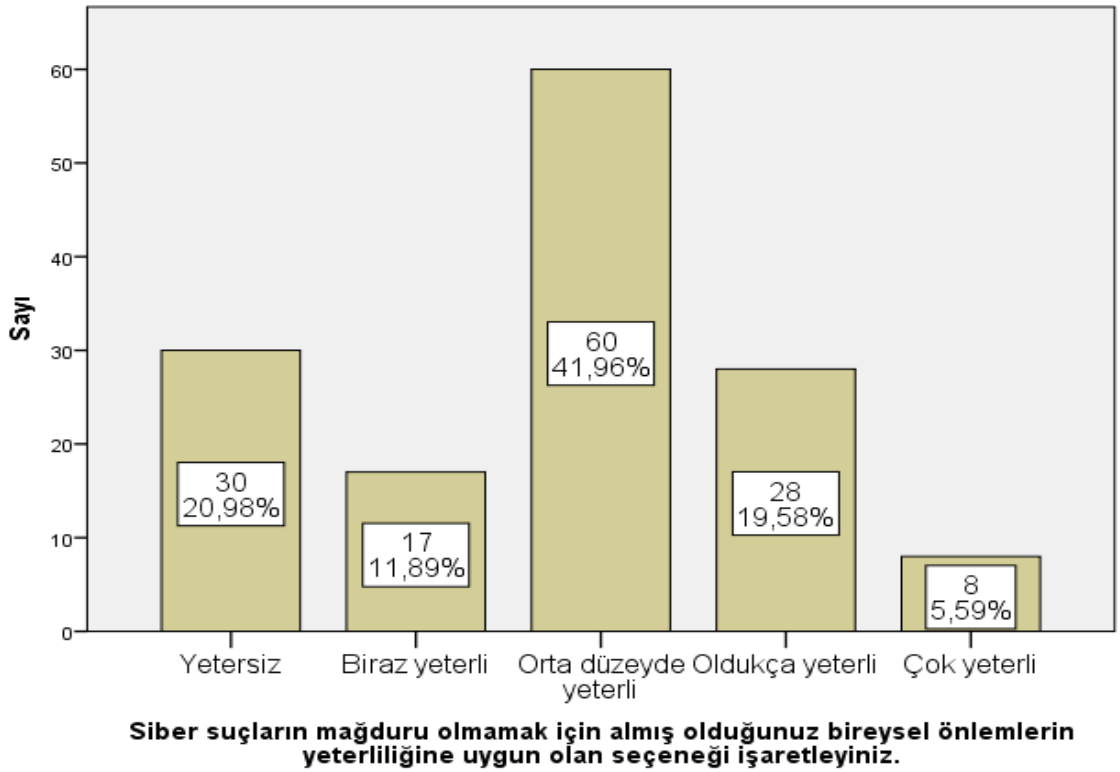
Şekil 3.7. Katılımcıların Siber Suç Mağduriyet Durumu Dağılımları

Katılımcıların siber suç mağduriyet durumu dağılımlarını belirlemek amacıyla oluşturulan "Bu zamana kadar siber suç mağduriyeti (örneğin, banka hesap numaranızın, sosyal medya hesabınızın, e-posta hesabınızın veya başkaca kişisel verilerinizin ele geçirilmesi veya verilerinizin çalınması suretiyle tarafınıza yönelik sahte hesap açılması, siber zorbalık, siber hırsızlık, siber ortamda haberleşme gizliliğinizin ihlali gibi) yaşadınız mı?" sorusuna verilen cevapların %91,61'lik kısmı hayır cevabı, %8,39'u ise evet cevabından oluşmaktadır.



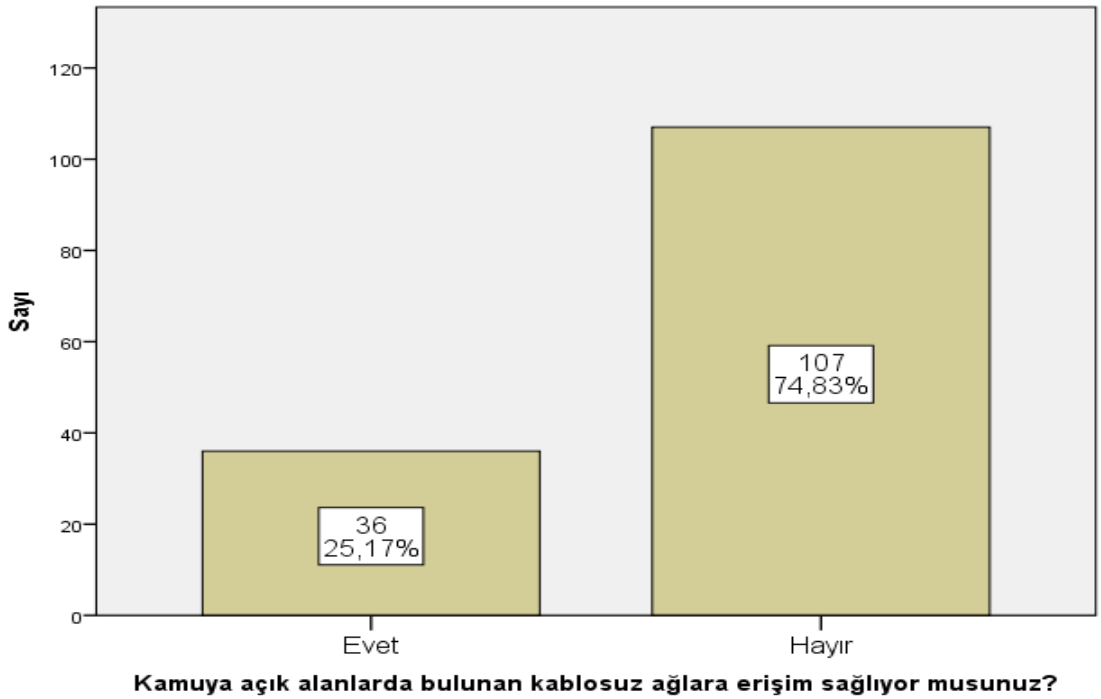
Şekil 3.8. Katılımcıların Siber Suçların Önlenmesinde Mevzuat/Düzenlemelerin Yeterliliğine Yönelik Algıları

Katılımcıların siber suçların önlenmesinde mevzuat/düzenlemelerin yeterliliğine yönelik algılarını belirlemek amacıyla oluşturulan "Siber suçları önlemeye yönelik mevcut yasal mevzuat/yazılı düzenlemelerin yeterliliğine yönelik algınıza en uygun olan seçeneği işaretleyiniz" ifadesinin cevapları yetersiz, biraz yeterli, orta düzeyde yeterli, oldukça yeterli, çok yeterli olarak beş gruba ayrılmıştır. Yetersiz cevabını veren kişi sayısı 54, biraz yeterli cevabını veren kişi sayısı 33, orta düzeyde yeterli cevabını veren kişi sayısı 46, oldukça yeterli cevabını veren kişi sayısı 4, çok yeterli cevabını veren kişi sayısı ise 5'tir.



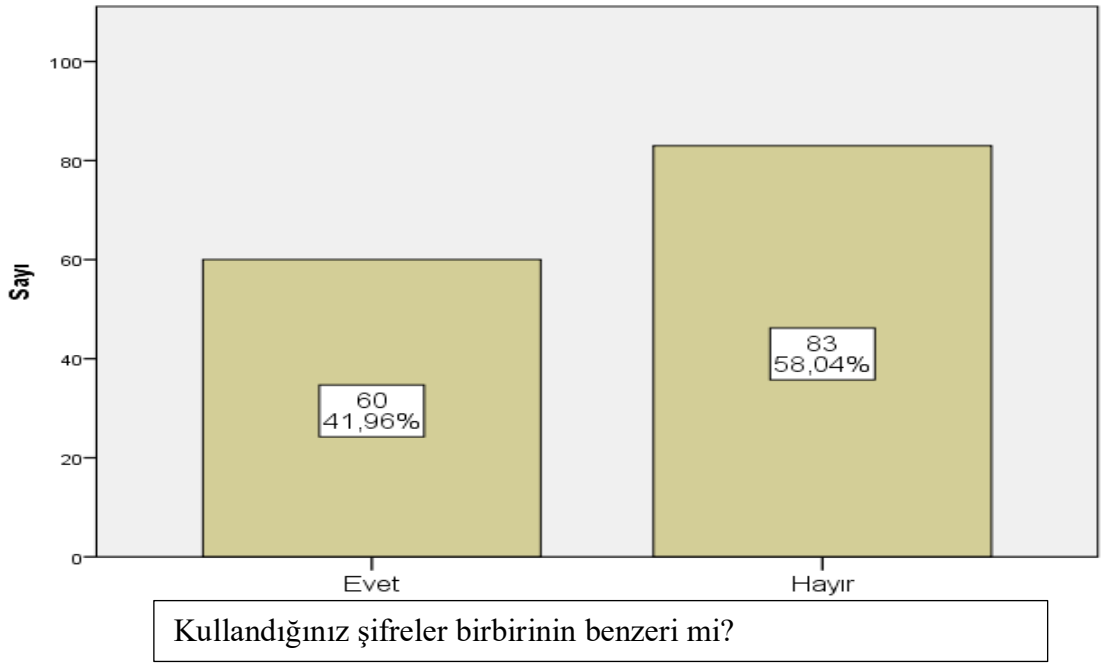
Şekil 3.9. Katılımcıların Siber Suça Yönelik Aldıkları Önlemlerin Yeterliliğine İlişkin Dağılımlar

Katılımcıların siber suça yönelik aldıkları önlemlerin yeterliliğine ilişkin dağılımları belirlemek amacıyla oluşturulan "Siber suçların mağduru olmamak için almış olduğunuz bireysel önlemlerin yeterliliğine uygun olan seçeneği işaretleyiniz" sorusuna verilen cevaplar yetersiz, biraz yeterli, orta düzeyde yeterli, oldukça yeterli, çok yeterli beş seçenekten oluşmaktadır. Yetersiz cevabını veren kişi oranı %20,98, biraz yeterli cevabını veren kişi oranı %11,89, orta düzeyde yeterli cevabını veren kişi oranı %41,96, oldukça yeterli cevabını veren kişi oranı %19,58, çok yeterli cevabını veren kişi oranı ise %5,59'dur.



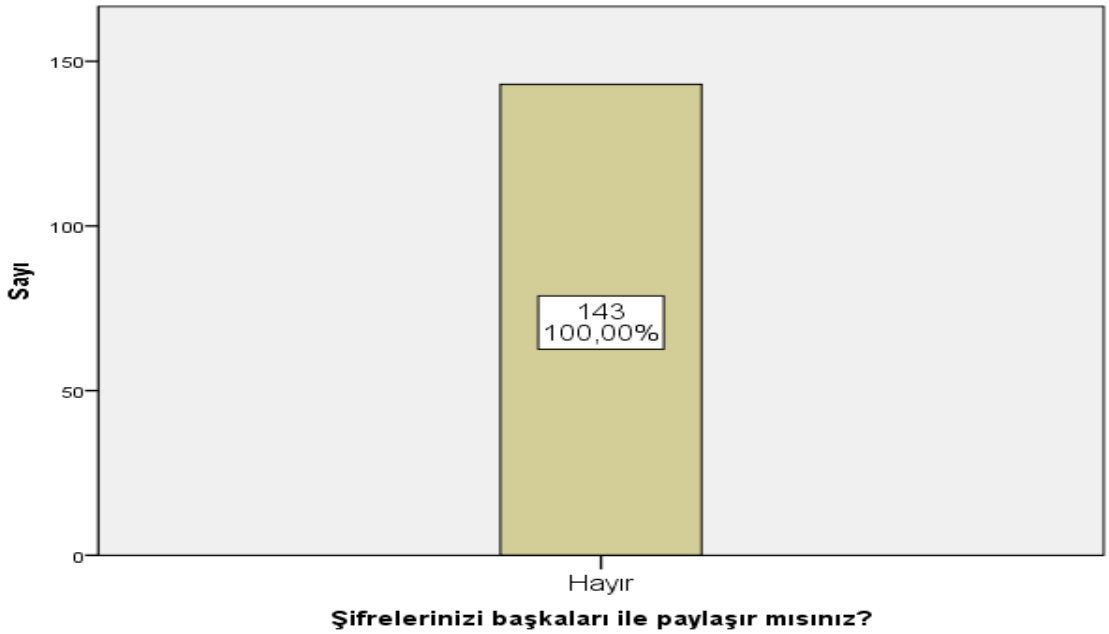
Şekil 3.10. Katılımcıların Kamuya Açık Alanlarda Bulunan Kablosuz Ağları Kullanma Dağılımları

Katılımcıların kamuya açık alanlarda bulunan kablosuz ağları kullanma dağılımlarını belirlemek amacıyla oluşturulan "Kamuya açık alanlarda bulunan kablosuz ağlara erişim sağlıyor musunuz?" sorusuna verilen cevapların %25,17 evet, %74,83 hayır cevabı vermiştir.



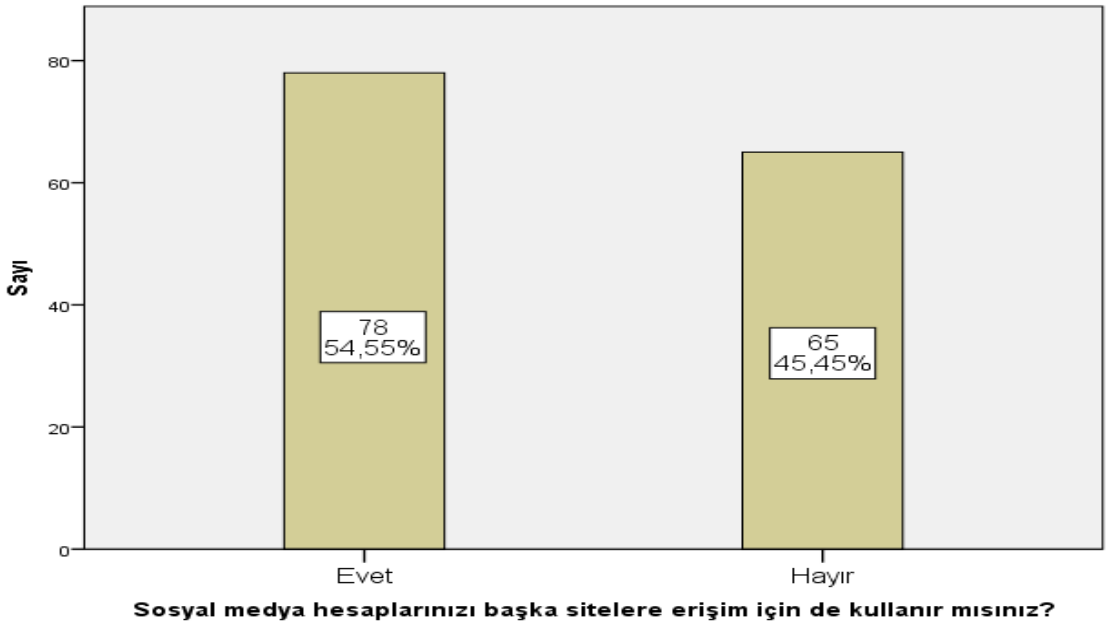
Şekil 3.11. Katılımcıların Kullandıkları Şifrelerin Benzersizlik Dağılımları

Katılımcıların kullandıkları şifrelerin benzersizlik dağılımlarını belirlemek amacıyla oluşturulan "Kullandığınız şifreler birbirleri ile benzer mi?" sorusuna verilen cevapların %41,96 sı evet cevabı iken %58,04 ü hayır cevabını oluşturmaktadır.



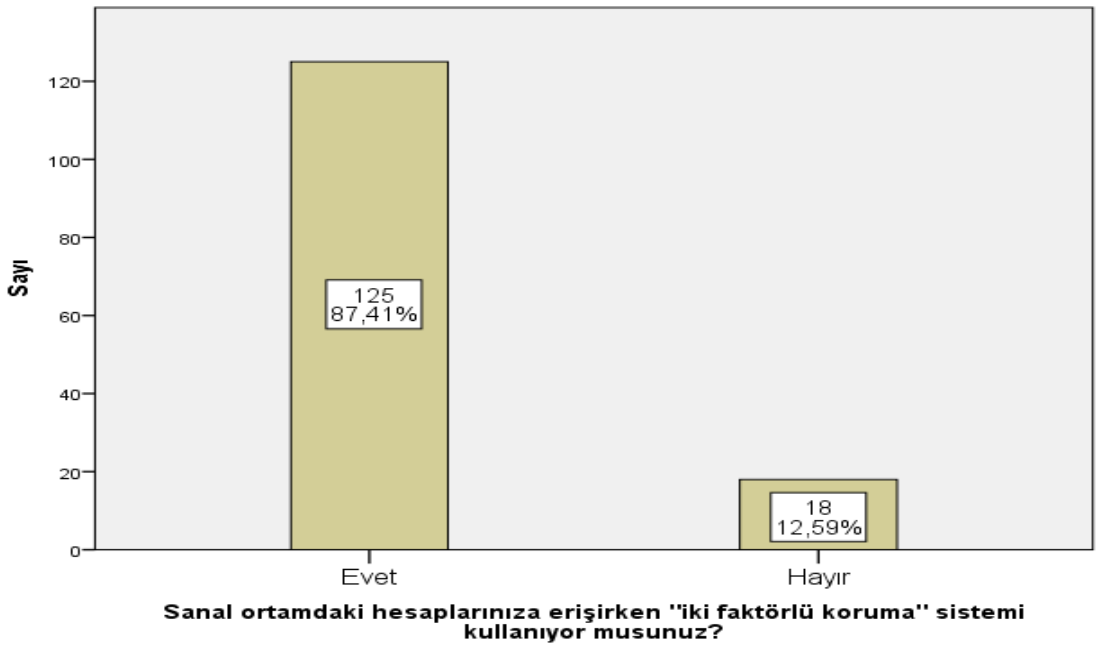
Şekil 3.12. Katılımcıların Kullandıkları Şifreleri Başkalarıyla Paylaşma Dağılımları

Katılımcıların kullandıkları şifreleri başkalarıyla paylaşma dağılımlarını belirlemek amacıyla oluşturulan "Şifrelerinizi başkaları ile paylaşır mısınız?" sorusuna verilen cevapların %100 oranında hayır şeklindedir.



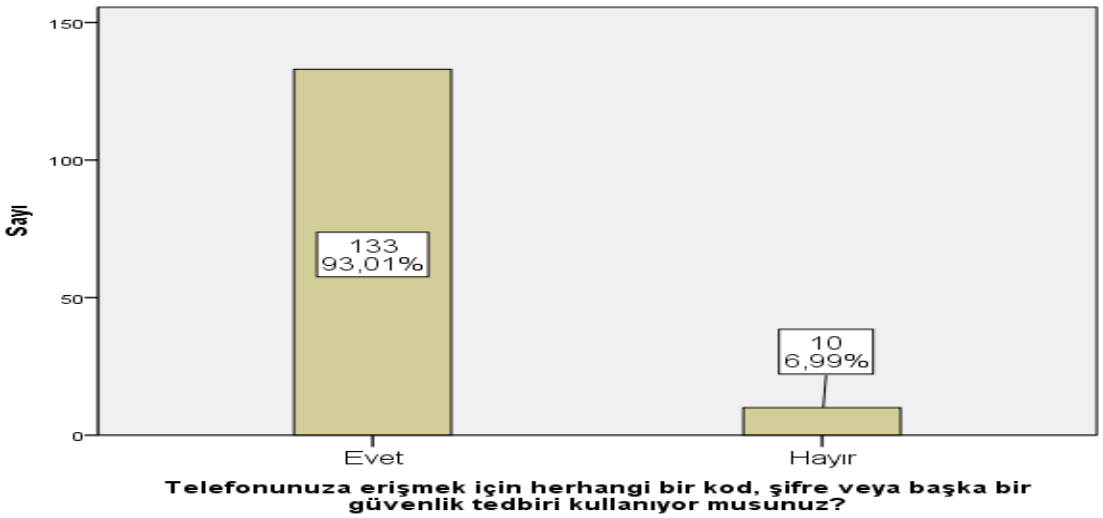
Şekil 3.13. Katılımcıların Sosyal Medya Hesaplarını Başka Sitelere Erişmede Kullanıp Kullanmadıklarına İlişkin Dağılımlar

Katılımcıların sosyal medya hesaplarını başka sitelere erişmede kullanıp kullanmadıklarına ilişkin dağılımları belirlemek amacıyla oluşturulan “Sosyal medya hesaplarınızı başka sitelere erişim için de kullanır mısınız?” sorusuna verilen cevapların %54,55 i evet iken, %45,45’i hayır cevabı vermiştir.



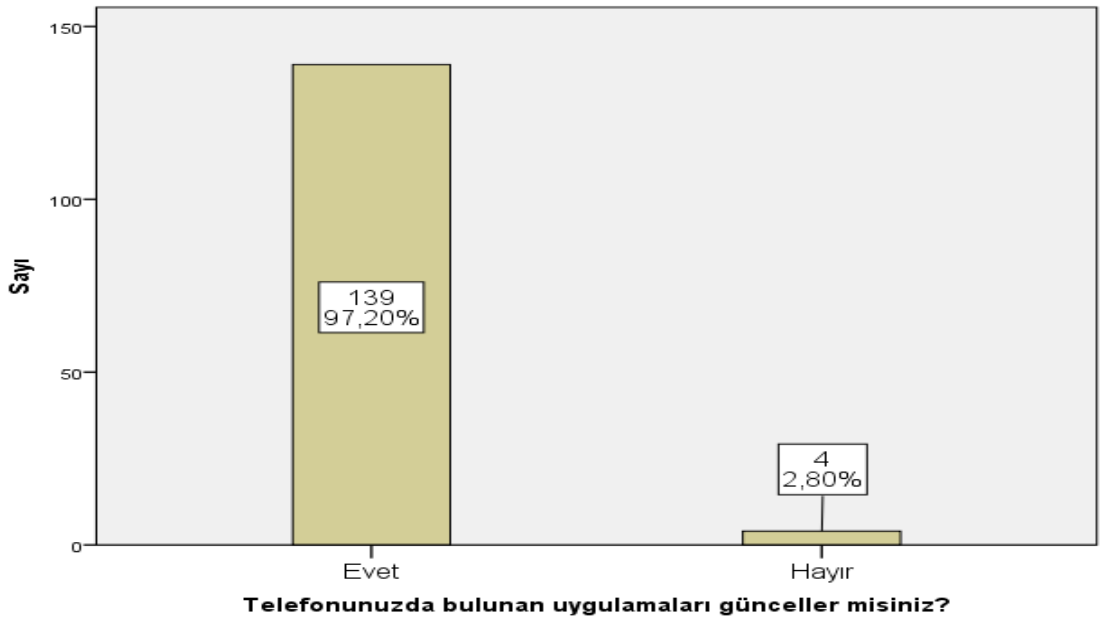
Şekil 3.14. Katılımcıların Sanal Ortamdaki Hesaplarına Erişmede "İki Faktörlü Koruma" Sistemi Kullanıp Kullanmadıklarına İlişkin Dağılımlar

Katılımcıların sanal ortamdaki hesaplarına erişmede "iki faktörlü koruma" sistemi kullanıp kullanmadıklarına ilişkin dağılımları belirlemek amacıyla oluşturulan “Sanal ortamdaki hesaplarınıza erişirken iki faktörlü koruma sistemi kullanıyor musunuz?” sorusuna verilen cevapların %87,41’i evet iken, hayır cevabını verenler %12,59’dur.



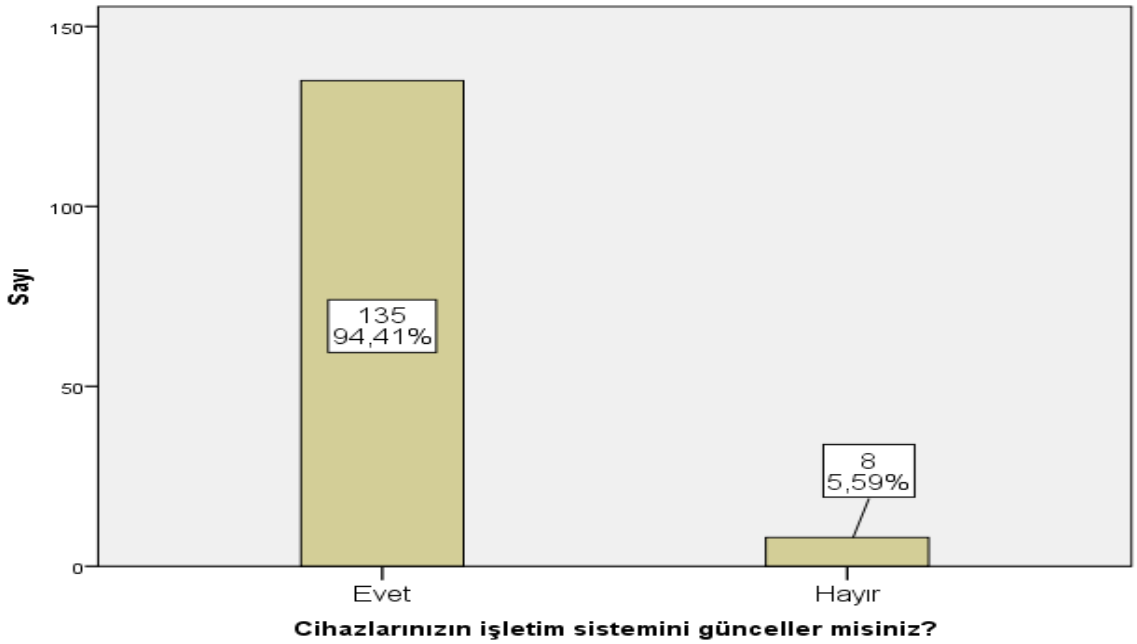
Şekil 3.15. Katılımcıların Telefonlarına Erişmede Herhangi Bir Kod, Şifre veya Başka Bir Güvenlik Tedbiri Kullanma Durumu Dağılımları

Katılımcıların telefonlarına erişmede herhangi bir kod, şifre veya başka bir güvenlik tedbiri kullanma durumu dağılımlarını belirlemek amacıyla oluşturulan "Telefonunuza erişmek için herhangi bir kod, şifre veya başka bir güvenlik tedbiri kullanıyor musunuz?" sorusuna verilen cevapların %93,01'i evet, %6,99'u ise hayır şeklindedir.



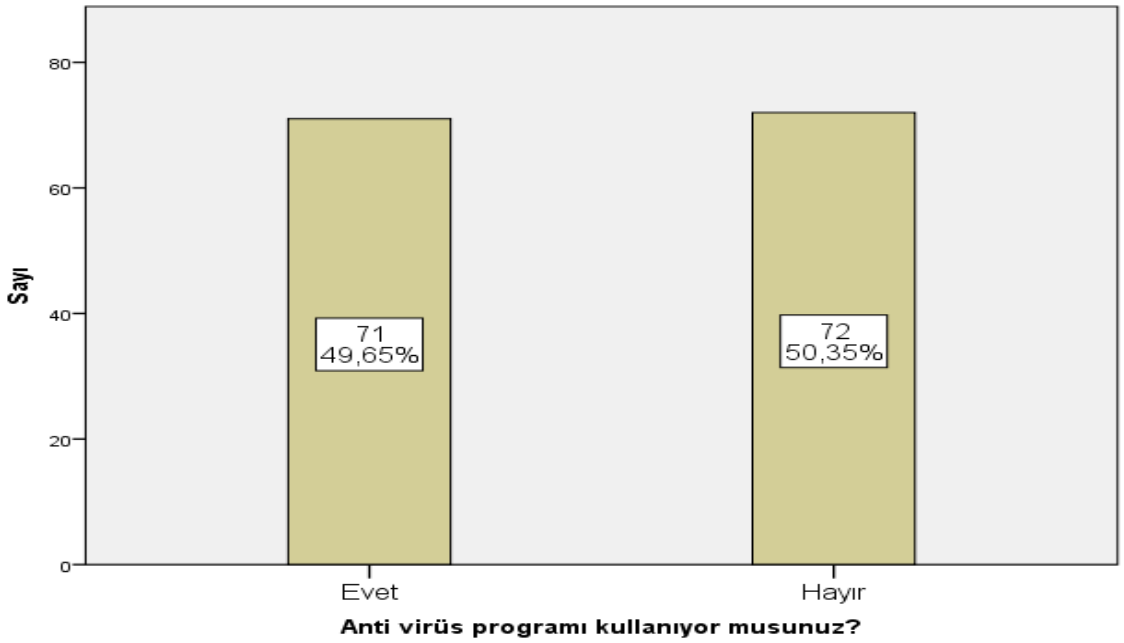
Şekil 3.16. Katılımcıların Telefonlarında Bulunan Uygulamaları Güncelle Dağılımları

Katılımcıların telefonlarında bulunan uygulamaları güncelle dağılımlarını belirlemek amacıyla oluşturulan "Telefonunuzda bulunan uygulamaları günceller misiniz?" sorusuna verilen cevapların %97,20 si evet iken %2,80'i hayır şeklindedir.



Şekil 3.17. Katılımcıların Cihazlarındaki İşletim Sistemini Güncelleme Dağılımları

Katılımcıların cihazlarındaki işletim sistemini güncelleme dağılımlarını belirlemek amacıyla oluşturulan "Cihazların işletim sistemini günceller misiniz?" sorusuna verilen cevapların %94,41 i evet iken %5,59'u hayır şeklindedir.



Şekil 3.18. Katılımcıların Cihazlarında Anti Virüs Programı Kullanma Dağılımları

Katılımcıların cihazlarında anti virüs programı kullanma dağılımlarını belirlemek amacıyla oluşturulan "Antivirüs programı kullanıyor musunuz?" sorusuna verilen cevapların %49,65 i evet iken, %50,35 i hayır cevabını vermiştir.

3.2. Katılımcıların Çeşitli Değişkenlere Göre Siber Suç Türlerine Maruz Kalma Korkusunun İncelenmesi

Katılımcıların cinsiyete göre siber suç türlerine maruz kalma korkusunun istatistiksel sonuçları çizelge 3.1.'de verilmiştir.

Çizelge 3.1. Katılımcıların Cinsiyete Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143)

		Cinsiyet			
		Kadın (N=53)	**Erkek (N=90)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
1. E-posta veya sosyal paylaşım sitelerine ait parolalarınızın çalınması konusunda	Hiç Korku Duymuyorum	2 (3.8)	22 (24.4)	29.006	**0.000**
	Biraz Korku Duyuyorum	9 (17.0)	32 (35.6)		
	Orta Düzeyde Korku Duyuyorum	20 (37.7)	26 (28.9)		
	Çok Korku Duyuyorum	18 (34.0)	10 (11.1)		
	Aşırı Düzeyde Korku Duyuyorum	4 (7.5)	0 (0.0)		
2. Banka hesap bilgilerinizin (hesap/kart numarası vb.) çalınması yoluyla zarara uğratılmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	6 (6.7)	14.757	**0.004****
	Biraz Korku Duyuyorum	2 (3.8)	10 (11.1)		
	Orta Düzeyde Korku Duyuyorum	16 (30.2)	34 (37.8)		
	Çok Korku Duyuyorum	21 (39.6)	34 (37.8)		
	Aşırı Düzeyde Korku Duyuyorum	14 (26.4)	6 (6.7)		
3. Kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	6 (6.7)	16.456	**0.001****
	Biraz Korku Duyuyorum	4 (7.5)	10 (11.1)		
	Orta Düzeyde Korku Duyuyorum	17 (32.1)	46 (51.1)		
	Çok Korku Duyuyorum	24 (45.3)	26 (28.9)		
	Aşırı Düzeyde Korku Duyuyorum	8 (15.1)	2 (2.2)		
4. Bilgisayar korsanlığına (kişisel bilgisayarınıza veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	16 (17.8)	16.900	**0.002**
	Biraz Korku Duyuyorum	9 (17.0)	24 (26.7)		
	Orta Düzeyde Korku Duyuyorum	24 (45.3)	34 (37.8)		
	Çok Korku Duyuyorum	16 (30.2)	14 (15.6)		
	Aşırı Düzeyde Korku Duyuyorum	4 (7.5)	2 (2.2)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.1. Katılımcıların Cinsiyete Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Cinsiyet			
		Kadın (N=53)	Erkek (N=90)	İstatistiksel Analiz	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
5. Truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	12 (13.3)	20.362	**0.000****
	Biraz Korku Duyuyorum	11 (20.8)	28 (31.1)		
	Orta Düzeyde Korku Duyuyorum	22 (41.5)	38 (42.2)		
	Çok Korku Duyuyorum	16 (30.2)	12 (13.3)		
	Aşırı Düzeyde Korku Duyuyorum	4 (7.5)	0 (0.0)		
6. Keylogger ve screenlogger gibi casus yazılımlara maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	10 (11.1)	11.210	**0.020****
	Biraz Korku Duyuyorum	13 (24.5)	18 (20.0)		
	Orta Düzeyde Korku Duyuyorum	20 (37.7)	42 (46.7)		
	Çok Korku Duyuyorum	16 (30.2)	18 (20.0)		
	Aşırı Düzeyde Korku Duyuyorum	4 (7.5)	2 (2.2)		
7. Siber zorbalığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	10 (11.1)	20.034	**0.000****
	Biraz Korku Duyuyorum	4 (7.5)	20 (22.2)		
	Orta Düzeyde Korku Duyuyorum	25 (47.2)	40 (44.4)		
	Çok Korku Duyuyorum	20 (37.7)	20 (22.2)		
	Aşırı Düzeyde Korku Duyuyorum	4 (7.5)	0 (0.0)		
8. Siber tacize (siber ortamda taciz davranışlarına) maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (3.8)	14 (15.6)	13.772	**0.007**
	Biraz Korku Duyuyorum	5 (9.4)	18 (20.0)		
	Orta Düzeyde Korku Duyuyorum	24 (45.3)	42 (46.7)		
	Çok Korku Duyuyorum	18 (34.0)	14 (15.6)		
	Aşırı Düzeyde Korku Duyuyorum	4 (7.5)	2 (2.2)		
9. Siber şantaja veya siber tehdide (siber ortamda şantaj veya tehdit davranışlarına) maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (3.8)	10 (11.1)	18.234	**0.001****
	Biraz Korku Duyuyorum	5 (9.4)	28 (31.1)		
	Orta Düzeyde Korku Duyuyorum	20 (37.7)	34 (37.8)		
	Çok Korku Duyuyorum	22 (41.5)	16 (17.8)		
	Aşırı Düzeyde Korku Duyuyorum	4 (7.5)	2 (2.2)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.1. Katılımcıların Cinsiyete Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Cinsiyet			
		Kadın (N=53)	Erkek (N=90)	İstatistiksel Analiz	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
10. Siber hırsızlığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	10 (11.1)	16.629	**0.002**
	Biraz Korku Duyuyorum	4 (7.5)	24 (26.7)		
	Orta Düzeyde Korku Duyuyorum	27 (50.9)	34 (37.8)		
	Çok Korku Duyuyorum	18 (34.0)	18 (20.0)		
	Aşırı Düzeyde Korku Duyuyorum	4 (7.5)	4 (4.4)		
11. Siber ortamda haberleşme gizliliğinizin ihlali (kayıt altına alınması ya da ifşası gibi) konusunda	Hiç Korku Duymuyorum	0 (0.0)	10 (11.1)	18.613	**0.000****
	Biraz Korku Duyuyorum	7 (13.2)	26 (28.9)		
	Orta Düzeyde Korku Duyuyorum	26 (49.1)	30 (33.3)		
	Çok Korku Duyuyorum	16 (30.2)	24 (26.7)		
	Aşırı Düzeyde Korku Duyuyorum	4 (7.5)	0 (0.0)		
12. Siber dolandırıcılığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	8 (8.9)	21.039	**0.000****
	Biraz Korku Duyuyorum	6 (11.3)	34 (37.8)		
	Orta Düzeyde Korku Duyuyorum	29 (54.7)	32 (35.6)		
	Çok Korku Duyuyorum	14 (26.4)	14 (15.6)		
	Aşırı Düzeyde Korku Duyuyorum	4 (7.5)	2 (2.2)		
13. Sniffinge maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	6 (6.7)	11.383	**0.018****
	Biraz Korku Duyuyorum	6 (11.3)	20 (22.2)		
	Orta Düzeyde Korku Duyuyorum	25 (47.2)	46 (51.1)		
	Çok Korku Duyuyorum	18 (34.0)	16 (17.8)		
	Aşırı Düzeyde Korku Duyuyorum	4 (7.5)	2 (2.2)		
14. Zombi ordulara maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	6 (6.7)	24.123	**0.000****
	Biraz Korku Duyuyorum	6 (11.3)	32 (35.6)		
	Orta Düzeyde Korku Duyuyorum	21 (39.6)	38 (42.2)		
	Çok Korku Duyuyorum	22 (41.5)	12 (13.3)		
	Aşırı Düzeyde Korku Duyuyorum	4 (7.5)	2 (2.2)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.1. Katılımcıların Cinsiyete Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Cinsiyet			
		Kadın (N=53)	Erkek (N=90)	İstatistiksel Analiz	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
15. Sosyal ağ üzerinden sahtekârlığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	18 (20.0)	29.884	**0.000**
	Biraz Korku Duyuyorum	5 (9.4)	18 (20.0)		
	Orta Düzeyde Korku Duyuyorum	24 (45.3)	42 (46.7)		
	Çok Korku Duyuyorum	18 (34.0)	12 (13.3)		
	Aşırı Düzeyde Korku Duyuyorum	6 (11.3)	0 (0.0)		
16. Siber yer tespitine maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (3.8)	18 (20.0)	15.063	**0.003**
	Biraz Korku Duyuyorum	11 (20.8)	22 (24.4)		
	Orta Düzeyde Korku Duyuyorum	24 (45.3)	38 (42.2)		
	Çok Korku Duyuyorum	12 (22.6)	12 (13.3)		
	Aşırı Düzeyde Korku Duyuyorum	4 (7.5)	0 (0.0)		
18. Siber terörizme maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (3.8)	14 (15.6)	12.616	**0.011**
	Biraz Korku Duyuyorum	11 (20.8)	14 (15.6)		
	Orta Düzeyde Korku Duyuyorum	18 (34.0)	42 (46.7)		
	Çok Korku Duyuyorum	16 (30.2)	10 (11.1)		
	Aşırı Düzeyde Korku Duyuyorum	6 (11.3)	10 (11.1)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Siber suç türlerine maruz kalma korkusunun cinsiyete göre farklılaşıp farklılaşmadığına ilişkin yapılan istatistiksel analizler sonucunda siber suç türlerine maruz kalma korkusundan bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalma korkusu (χ^2=7.915, p=0.093) hariç diğerlerinin cinsiyete göre anlamlı olarak farklılaştığı bulunmuştur (p<0.001, p<0.01, p<0.05). Buna göre kadınların %41.5'i e-posta veya sosyal paylaşım sitelerine ait parolaların çalınması konusunda çok ve aşırı düzeyde korku yaşarken, erkeklerde bu oran %11.1; kadınların %66.'sı banka hesap bilgilerinin (hesap/kart numarası vb.) çalınması yoluyla zarara uğratılma konusunda çok ve aşırı düzeyde korku yaşarken, erkeklerde bu oran %44.5; kadınların %60.4'ü kimlik hırsızlığına maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erkeklerde bu oran %31.1; kadınların %37.7'si bilgisayar korsanlığına (kişisel bilgisayarınıza veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalma konusunda çok ve aşırı düzeyde korku

yaşarken, erkeklerde bu oran %17.8; kadınların %37.7'si truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erkeklerde bu oran %13.3; kadınların %37.7'si keylogger ve screenlogger gibi casus yazılımlara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erkeklerde bu oran %22.2; kadınların %45.2'si siber zorbalığa maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erkeklerde bu oran %22.2; kadınların %41.5'i siber tacize (siber ortamda taciz davranışlarına) maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erkeklerde bu oran %17.8; kadınların %49'u siber şantaja veya siber tehdide (siber ortamda şantaj veya tehdit davranışlarına) maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erkeklerde bu oran %20; kadınların %41.5'i siber hırsızlığa maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erkeklerde bu oran %24.4; kadınların %37.7'si siber ortamda haberleşme gizliliğinin ihlali (kayıt altına alınması ya da ifşası gibi) konusunda çok ve aşırı düzeyde korku yaşarken, erkeklerde bu oran %26.7; kadınların %33.9'u siber dolandırıcılığa maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erkeklerde bu oran %17.8; kadınların %41.5'i sniffinge maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erkeklerde bu oran %20; kadınların %49'u zombi ordulara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erkeklerde bu oran %15.5; kadınların %45.3'ü sosyal ağ üzerinden sahtekârlığa maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erkeklerde bu oran %13.3; kadınların %30.1'i siber yer tespitine maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erkeklerde bu oran %13.3 ve kadınların %41.5'i siber terörizme maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erkeklerde bu oran %22.2'dir. Bu sonuçlar, siber suç türlerine maruz kalma açısından korku oranlarının kadınlarda daha yüksek olduğunu göstermektedir.

Katılımcıların medeni duruma göre siber suç türlerine maruz kalma korkusunun istatistiksel sonuçları çizelge 3.2.'de verilmiştir.

Çizelge 3.2. Katılımcıların Medeni Duruma Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143)

		Medeni Durum			
		Evli (N=77)	Bekâr (N=66)	İstatistiksel Analiz	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
1. E-posta veya sosyal paylaşım sitelerine ait parolalarınızın çalınması konusunda	Hiç Korku Duymuyorum	6 (7.8)	18 (27.3)	10.258	**0.033**
	Biraz Korku Duyuyorum	25 (32.5)	16 (24.2)		
	Orta Düzeyde Korku Duyuyorum	26 (33.8)	20 (30.3)		
	Çok Korku Duyuyorum	18 (23.4)	10 (15.2)		
	Aşırı Düzeyde Korku Duyuyorum	2 (2.6)	2 (3.0)		
3. Kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (2.6)	4 (6.1)	12.225	**0.012****
	Biraz Korku Duyuyorum	2 (2.6)	12 (18.2)		
	Orta Düzeyde Korku Duyuyorum	35 (45.5)	28 (42.4)		
	Çok Korku Duyuyorum	32 (41.6)	18 (27.3)		
	Aşırı Düzeyde Korku Duyuyorum	6 (7.8)	4 (6.1)		
4. Bilgisayar korsanlığına (kişisel bilgisayarınıza veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalmanız konusunda	Hiç Korku Duymuyorum	4 (5.2)	12 (18.2)	10.944	**0.025**
	Biraz Korku Duyuyorum	15 (19.5)	18 (27.3)		
	Orta Düzeyde Korku Duyuyorum	38 (49.4)	20 (30.3)		
	Çok Korku Duyuyorum	18 (23.4)	12 (18.2)		
	Aşırı Düzeyde Korku Duyuyorum	2 (2.6)	4 (6.1)		
5. Truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (2.6)	10 (15.2)	9.934	**0.041**
	Biraz Korku Duyuyorum	25 (32.5)	14 (21.2)		
	Orta Düzeyde Korku Duyuyorum	30 (39.0)	30 (45.5)		
	Çok Korku Duyuyorum	18 (23.4)	10 (15.2)		
	Aşırı Düzeyde Korku Duyuyorum	2 (2.6)	2 (3.0)		
6. Keylogger ve screenlogger gibi casus yazılımlara maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (2.6)	8 (12.1)	9.475	**0.046**
	Biraz Korku Duyuyorum	17 (22.1)	14 (21.2)		
	Orta Düzeyde Korku Duyuyorum	30 (39.0)	32 (48.5)		
	Çok Korku Duyuyorum	24 (31.2)	10 (15.2)		
	Aşırı Düzeyde Korku Duyuyorum	4 (5.2)	2 (3.0)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Siber suç türlerine maruz kalma korkusunun medeni duruma göre farklılaşıp farklılaşmadığına ilişkin yapılan istatistiksel analizler sonucunda siber suç türlerine maruz kalma korkusundan e-posta veya sosyal paylaşım sitelerine ait parolaların çalınması (χ^2=10.258, p=0.033), kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalma (χ^2=12.225, p=0.012), bilgisayar korsanlığına (kişisel bilgisayarınıza veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalma (χ^2=10.944, p=0.025), truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalma (χ^2=9.934, p=0.041) ve keylogger ve screenlogger gibi casus yazılımlara maruz kalma (χ^2=9.475, p=0.046) korkularının medeni duruma göre anlamlı olarak farklılaştığı bulunmuştur ($p<0.05$). Buna göre evlilerin %26'sı e-posta veya sosyal paylaşım sitelerine ait parolalarının çalınması konusunda çok ve aşırı düzeyde korku yaşarken, bekârlarda bu oran %18.2; evlilerin %49.4'ü kimlik hırsızlığına maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, bekârlarda bu oran %33.4; evlilerin %75.4'ü bilgisayar korsanlığına (kişisel bilgisayarınıza veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, bekârlarda bu oran %54.6; evlilerin %26'sı truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, bekârlarda bu oran %18.2 ve evlilerin %36.4'ü keylogger ve screenlogger gibi casus yazılımlara maruz kalma konusunda"çok ve aşırı düzeyde korku yaşarken, bekârlarda bu oran %18.2'dir. Bu sonuçlar siber suç türlerine maruz kalma açısından korku oranlarının evlilerde daha yüksek olduğunu göstermektedir.

Katılımcıların yaşa göre siber suç türlerine maruz kalma korkusunun istatistiksel sonuçları çizelge 3.3.'te verilmiştir.

Çizelge 3.3. Katılımcıların Yaşa Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143)

		Yaş					
		18-25 (N=22)	**26-33 (N=68)**	**34-41 (N=30)**	**42-49 (N=23)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
1. E-posta veya sosyal paylaşım sitelerine ait parolalarınızın çalınması konusunda	Hiç Korku Duymuyorum	8 (36.4)	10 (14.7)	0 (0.0)	6 (26.1)	20.061	**0.043**
	Biraz Korku Duyuyorum	4 (18.2)	18 (26.5)	12 (40.0)	7 (30.4)		
	Orta Düzeyde Korku Duyuyorum	6 (27.3)	26 (38.2)	10 (33.3)	4 (17.4)		
	Çok Korku Duyuyorum	4 (18.2)	12 (17.6)	6 (20.0)	6 (26.1)		
	Aşırı Düzeyde Korku Duyuyorum	0 (0.0)	2 (2.9)	2 (6.7)	0 (0.0)		
3. Kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (9.1)	2 (2.9)	0 (0.0)	2 (8.7)	19.441	**0.041**
	Biraz Korku Duyuyorum	4 (18.2)	4 (5.9)	6 (20.0)	0 (0.0)		
	Orta Düzeyde Korku Duyuyorum	6 (27.3)	32 (47.1)	14 (46.7)	11 (47.8)		
	Çok Korku Duyuyorum	8 (36.4)	26 (38.2)	6 (20.0)	10 (43.5)		
	Aşırı Düzeyde Korku Duyuyorum	2 (9.1)	4 (5.9)	4 (13.3)	0 (0.0)		
7. Siber zorbalığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	4 (18.2)	4 (5.9)	0 (0.0)	2 (8.7)	20.091	**0.032**
	Biraz Korku Duyuyorum	2 (9.1)	14 (20.6)	8 (26.7)	0 (0.0)		
	Orta Düzeyde Korku Duyuyorum	8 (36.4)	32 (47.1)	10 (33.3)	15 (65.2)		
	Çok Korku Duyuyorum	8 (36.4)	16 (23.5)	10 (33.3)	6 (26.1)		
	Aşırı Düzeyde Korku Duyuyorum	0 (0.0)	2 (2.9)	2 (6.7)	0 (0.0)		

*Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.3. Katılımcıların Yaşa Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Yaş					
		18-25 (N=22)	26-33 (N=68)	34-41 (N=30)	42-49 (N=23)	İstatistiksel Analiz	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
14. Zombi ordulara maruz kalmanız konusunda	Hiç Korku Duymuyorum	4 (18.2)	0 (0.0)	0 (0.0)	2 (8.7)	25.049	**0.005**
	Biraz Korku Duyuyorum	4 (18.2)	14 (20.6)	14 (46.7)	6 (26.1)		
	Orta Düzeyde Korku Duyuyorum	8 (36.4)	34 (50.0)	6 (20.0)	11 (47.8)		
	Çok Korku Duyuyorum	6 (27.3)	16 (23.5)	8 (26.7)	4 (17.4)		
	Aşırı Düzeyde Korku Duyuyorum	0 (0.0)	4 (5.9)	2 (6.7)	0 (0.0)		

*Fisher Freeman Halton testi, [a]Sütun yüzdesi

Siber suç türlerine maruz kalma korkusunun yaşa göre farklılaşıp farklılaşmadığına ilişkin yapılan istatistiksel analizler sonucunda siber suç türlerine maruz kalma korkusundan e-posta veya sosyal paylaşım sitelerine ait parolaların çalınması (χ^2=20.061, p=0.043), kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalma (χ^2=19.441, p=0.041), siber zorbalığa maruz kalma (χ^2=20.091, p=0.032) ve zombi ordulara maruz kalma (χ2=25.049, p=0.005) korkularının yaşa göre anlamlı olarak farklılaştığı bulunmuştur (p<0.01, p<0.05). Buna göre yaşı 34-41 olanların %60'ı ve 26-33 olanların %58.7'si e-posta veya sosyal paylaşım sitelerine ait parolalarının çalınması konusunda orta, çok ve aşırı düzeyde korku yaşarken, yaşı 42-49 ve 18-25 olanlarda bu oran sırasıyla %43.5 ve %45.5; yaşı 34-41 olanların %80'i, 42-49 olanların %91.3'ü ve 26-33 olanların %91.2'si kimlik hırsızlığına maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, yaşı 18-25 olanlarda bu oran %72.8; yaşı 42-49 olanların %91.3'ü siber zorbalığa maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, yaşı 18-25, 26-33 ve 34-41 olanlarda bu oran sırasıyla %72.8, %73.5 ve %73.3; yaşı 18-25 olanların %27.3'ü, 26-33 olanların %29.4'ü ve 34-41 olanların %33.4'ü zombi ordulara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, yaşı 42-49 olanlarda bu oran %17.4'tür.

Katılımcıların eğitim durumuna göre siber suç türlerine maruz kalma korkusunun istatistiksel sonuçları çizelge 3.4.'te verilmiştir.

Çizelge 3.4. Katılımcıların Eğitim Durumuna Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143)

		Eğitim Durumu				
		Lise-Önlisans (N=32)	**Lisans (N=93)**	**Lisansüstü (N=18)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
1. E-posta veya sosyal paylaşım sitelerine ait parolalarınızın çalınması konusunda	Hiç Korku Duymuyorum	16 (50.0)	8 (8.6)	0 (0.0)	51.651	**0.000**
	Biraz Korku Duyuyorum	4 (12.5)	29 (31.2)	8 (44.4)		
	Orta Düzeyde Korku Duyuyorum	0 (0.0)	40 (43.0)	6 (33.3)		
	Çok Korku Duyuyorum	10 (31.3)	14 (15.1)	4 (22.2)		
	Aşırı Düzeyde Korku Duyuyorum	2 (6.3)	2 (2.2)	0 (0.0)		
2. Banka hesap bilgilerinizin (hesap/kart numarası vb.) çalınması yoluyla zarara uğratılmanız konusunda	Hiç Korku Duymuyorum	4 (12.5)	2 (2.2)	0 (0.0)	30.083	**0.000**
	Biraz Korku Duyuyorum	6 (18.8)	6 (6.5)	0 (0.0)		
	Orta Düzeyde Korku Duyuyorum	2 (6.3)	44 (47.3)	4 (22.2)		
	Çok Korku Duyuyorum	14 (43.8)	29 (31.2)	12 (66.7)		
	Aşırı Düzeyde Korku Duyuyorum	6 (18.8)	12 (12.9)	2 (11.1)		
4. Bilgisayar korsanlığına (kişisel bilgisayarınıza veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalmanız konusunda	Hiç Korku Duymuyorum	10 (31.3)	6 (6.5)	0 (0.0)	41.068	**0.000**
	Biraz Korku Duyuyorum	4 (12.5)	23 (24.7)	6 (33.3)		
	Orta Düzeyde Korku Duyuyorum	4 (12.5)	50 (53.8)	4 (22.2)		
	Çok Korku Duyuyorum	12 (37.5)	10 (10.8)	8 (44.4)		
	Aşırı Düzeyde Korku Duyuyorum	2 (6.3)	4 (4.3)	0 (0.0)		

*Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.4. Katılımcıların Eğitim Durumuna Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Eğitim Durumu				
		Lise-Önlisans (N=32)	Lisans (N=93)	Lisansüstü (N=18)	İstatistiksel Analiz	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
5. Truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalmanız konusunda	Hiç Korku Duymuyorum	6 (18.8)	6 (6.5)	0 (0.0)	17.639	**0.012**
	Biraz Korku Duyuyorum	6 (18.8)	27 (29.0)	6 (33.3)		
	Orta Düzeyde Korku Duyuyorum	8 (25.0)	46 (49.5)	6 (33.3)		
	Çok Korku Duyuyorum	10 (31.3)	12 (12.9)	6 (33.3)		
	Aşırı Düzeyde Korku Duyuyorum	2 (6.3)	2 (2.2)	0 (0.0)		
6. Keylogger ve screenlogger gibi casus yazılımlara maruz kalmanız konusunda	Hiç Korku Duymuyorum	6 (18.8)	4 (4.3)	0 (0.0)	15.138	**0.034**
	Biraz Korku Duyuyorum	2 (6.3)	25 (26.9)	4 (22.2)		
	Orta Düzeyde Korku Duyuyorum	12 (37.5)	42 (45.2)	8 (44.4)		
	Çok Korku Duyuyorum	10 (31.3)	18 (19.4)	6 (33.3)		
	Aşırı Düzeyde Korku Duyuyorum	2 (6.3)	4 (4.3)	0 (0.0)		
7. Siber zorbalığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	10 (31.3)	0 (0.0)	0 (0.0)	35.135	**0.000**
	Biraz Korku Duyuyorum	2 (6.3)	18 (19.4)	4 (22.2)		
	Orta Düzeyde Korku Duyuyorum	10 (31.3)	49 (52.7)	6 (33.3)		
	Çok Korku Duyuyorum	8 (25.0)	24 (25.8)	8 (44.4)		
	Aşırı Düzeyde Korku Duyuyorum	2 (6.3)	2 (2.2)	0 (0.0)		
8. Siber tacize (siber ortamda taciz davranışlarına) maruz kalmanız konusunda	Hiç Korku Duymuyorum	14 (43.8)	2 (2.2)	0 (0.0)	41.893	**0.000**
	Biraz Korku Duyuyorum	2 (6.3)	19 (20.4)	2 (11.1)		
	Orta Düzeyde Korku Duyuyorum	6 (18.8)	50 (53.8)	10 (55.5)		
	Çok Korku Duyuyorum	8 (25.0)	18 (19.4)	6 (33.3)		
	Aşırı Düzeyde Korku Duyuyorum	2 (6.3)	4 (4.3)	0 (0.0)		

*Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.4. Katılımcıların Eğitim Durumuna Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Eğitim Durumu				
		Lise-Önlisans (N=32)	Lisans (N=93)	Lisansüstü (N=18)	İstatistiksel Analiz	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
8. Siber tacize (siber ortamda taciz davranışlarına) maruz kalmanız konusunda	Hiç Korku Duymuyorum	14 (43.8)	2 (2.2)	0 (0.0)	41.893	**0.000**
	Biraz Korku Duyuyorum	2 (6.3)	19 (20.4)	2 (11.1)		
	Orta Düzeyde Korku Duyuyorum	6 (18.8)	50 (53.8)	10 (55.5)		
	Çok Korku Duyuyorum	8 (25.0)	18 (19.4)	6 (33.3)		
	Aşırı Düzeyde Korku Duyuyorum	2 (6.3)	4 (4.3)	0 (0.0)		
9. Siber şantaja veya siber tehdide (siber ortamda şantaj veya tehdit davranışlarına) maruz kalmanız konusunda	Hiç Korku Duymuyorum	10 (31.3)	2 (2.2)	0 (0.0)	25.650	**0.000**
	Biraz Korku Duyuyorum	6 (18.8)	21 (22.6)	6 (33.3)		
	Orta Düzeyde Korku Duyuyorum	6 (18.8)	42 (45.2)	6 (33.3)		
	Çok Korku Duyuyorum	8 (25.0)	24 (25.8)	6 (33.3)		
	Aşırı Düzeyde Korku Duyuyorum	2 (6.3)	4 (4.3)	0 (0.0)		
10. Siber hırsızlığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	8 (25.0)	0 (0.0)	2 (11.1)	35.232	**0.000**
	Biraz Korku Duyuyorum	6 (18.8)	16 (17.2)	6 (33.3)		
	Orta Düzeyde Korku Duyuyorum	8 (25.0)	51 (54.8)	2 (11.1)		
	Çok Korku Duyuyorum	8 (25.0)	22 (23.7)	6 (33.3)		
	Aşırı Düzeyde Korku Duyuyorum	2 (6.3)	4 (4.3)	2 (11.1)		
11. Siber ortamda haberleşme gizliliğinizin ihlali (kayıt altına alınması ya da ifşası gibi) konusunda	Hiç Korku Duymuyorum	8 (25.0)	2 (2.2)	0 (0.0)	22.928	**0.001**
	Biraz Korku Duyuyorum	4 (12.5)	21 (22.6)	8 (44.4)		
	Orta Düzeyde Korku Duyuyorum	8 (25.0)	42 (45.2)	6 (33.3)		
	Çok Korku Duyuyorum	10 (31.3)	26 (28.0)	4 (22.2)		
	Aşırı Düzeyde Korku Duyuyorum	2 (6.3)	2 (2.2)	0 (0.0)		

*Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.4. Katılımcıların Eğitim Durumuna Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Eğitim Durumu				
		Lise-Önlisans (N=32)	Lisans (N=93)	Lisansüstü (N=18)	İstatistiksel Analiz	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
12. Siber dolandırıcılığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	8 (25.0)	0 (0.0)	0 (0.0)	31.401	**0.000**
	Biraz Korku Duyuyorum	8 (25.0)	26 (28.0)	6 (33.3)		
	Orta Düzeyde Korku Duyuyorum	6 (18.8)	47 (50.5)	8 (44.4)		
	Çok Korku Duyuyorum	8 (25.0)	18 (19.4)	2 (11.1)		
	Aşırı Düzeyde Korku Duyuyorum	2 (6.3)	2 (2.2)	2 (11.1)		
13. Sniffinge maruz kalmanız konusunda	Hiç Korku Duymuyorum	6 (18.8)	0 (0.0)	0 (0.0)	18.834	**0.009**
	Biraz Korku Duyuyorum	4 (12.5)	18 (19.4)	4 (22.2)		
	Orta Düzeyde Korku Duyuyorum	12 (37.5)	51 (54.8)	8 (44.4)		
	Çok Korku Duyuyorum	8 (25.0)	20 (21.5)	6 (33.3)		
	Aşırı Düzeyde Korku Duyuyorum	2 (6.3)	4 (4.3)	0 (0.0)		
14. Zombi ordulara maruz kalmanız konusunda	Hiç Korku Duymuyorum	6 (18.8)	0 (0.0)	0 (0.0)	24.094	**0.000**
	Biraz Korku Duyuyorum	10 (31.3)	22 (23.7)	6 (33.3)		
	Orta Düzeyde Korku Duyuyorum	6 (18.8)	47 (50.5)	6 (33.3)		
	Çok Korku Duyuyorum	8 (25.0)	20 (21.5)	6 (33.3)		
	Aşırı Düzeyde Korku Duyuyorum	2 (6.3)	4 (4.3)	0 (0.0)		
15. Sosyal ağ üzerinden sahtekârlığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	14 (43.8)	4 (4.3)	0 (0.0)	35.607	**0.000**
	Biraz Korku Duyuyorum	2 (6.3)	17 (18.3)	4 (22.2)		
	Orta Düzeyde Korku Duyuyorum	6 (18.8)	50 (53.8)	10 (55.6)		
	Çok Korku Duyuyorum	8 (25.0)	18 (19.4)	4 (22.2)		
	Aşırı Düzeyde Korku Duyuyorum	2 (6.3)	4 (4.3)	0 (0.0)		

*Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.4. Katılımcıların Eğitim Durumuna Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Eğitim Durumu				
		Lise-Önlisans (N=32)	Lisans (N=93)	Lisansüstü (N=18)	İstatistiksel Analiz	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
16. Siber yer tespitine maruz kalmanız konusunda	Hiç Korku Duymuyorum	12 (37.5)	8 (8.6)	0 (0.0)	29.386	**0.000**
	Biraz Korku Duyuyorum	6 (18.8)	23 (24.7)	4 (22.2)		
	Orta Düzeyde Korku Duyuyorum	4 (12.5)	48 (51.6)	10 (55.6)		
	Çok Korku Duyuyorum	8 (25.0)	12 (12.9)	4 (22.2)		
	Aşırı Düzeyde Korku Duyuyorum	2 (6.3)	2 (2.2)	0 (0.0)		
18. Siber terörizme maruz kalmanız konusunda	Hiç Korku Duymuyorum	10 (31.3)	4 (4.3)	2 (11.1)	36.595	**0.000**
	Biraz Korku Duyuyorum	4 (12.5)	21 (22.6)	0 (0.0)		
	Orta Düzeyde Korku Duyuyorum	4 (12.5)	46 (49.5)	10 (55.6)		
	Çok Korku Duyuyorum	8 (25.0)	12 (12.9)	6 (33.3)		
	Aşırı Düzeyde Korku Duyuyorum	6 (18.8)	10 (10.8)	0 (0.0)		

*Fisher Freeman Halton testi, [a]Sütun yüzdesi

Siber suç türlerine maruz kalma korkusunun eğitim durumuna göre farklılaşıp farklılaşmadığına ilişkin yapılan istatistiksel analizler sonucunda siber suç türlerine maruz kalma korkusundan kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalma (χ^2=13.249, p=0.066) ve bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalma konusu (χ^2=8.235, p=0.371) haricinde diğer siber suç türlerinin eğitim durumuna göre anlamlı olarak farklılaştığı bulunmuştur (p<0.001, p<0.01, p<0.05). Buna göre lisans mezunu olanların %60.3'ü ve lisansüstü mezunu olanların %55.5'i e-posta veya sosyal paylaşım sitelerine ait parolalarınızın çalınması konusunda" orta, çok ve aşırı düzeyde korku yaşarken,

lise-ön lisans mezunlarında bu oran %37.6; lisans mezunu olanların %91.4'ü ve lisansüstü mezunu olanların %100'ü banka hesap bilgilerinin (hesap/kart numarası vb.) çalınması yoluyla zarara uğratılma konusunda orta, çok ve aşırı düzeyde korku yaşarken, lise-ön lisans mezunlarında bu oran %68.9; lisans mezunu olanların %68.9'u ve lisansüstü mezunu olanların %66.6'sı bilgisayar korsanlığına (kişisel bilgisayarınıza veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, lise-ön lisans mezunlarında bu oran %56.3; lise-ön lisans mezunu olanların %37.6'sı ve lisansüstü mezunu olanların %33.3'ü truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, lisans mezunlarında bu oran %15.1; lise-ön lisans mezunu olanların %37.6'sı ve lisansüstü mezunu olanların %33.3'ü keylogger ve screenlogger gibi casus yazılımlara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, lisans mezunlarında bu oran %23.7; lisans mezunu olanların %80.7'si ve lisansüstü mezunu olanların %77.7'si siber zorbalığa maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, lise-ön lisans mezunlarında bu oran %62.6; lisans mezunu olanların %77.5'i ve lisansüstü mezunu olanların %88.8'i siber tacize (siber ortamda taciz davranışlarına) maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, lise-ön lisans mezunlarında bu oran %50.1; lisans mezunu olanların %75.3'ü ve lisansüstü mezunu olanların %66.6'sı siber şantaja veya siber tehdide (siber ortamda şantaj veya tehdit davranışlarına) maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, lise-ön lisans mezunlarında bu oran %50.1; lisansüstü mezunu olanların %44.4'ü siber hırsızlığa maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, lise-ön lisans ve lisans mezunlarında bu oran sırasıyla %31.3 ve %28; lise-ön lisans mezunu olanların %37.6'sı ve lisans mezunu olanların %30.2'si siber ortamda haberleşme gizliliğinin ihlali (kayıt altına alınması ya da ifşası gibi) konusunda çok ve aşırı düzeyde korku yaşarken, lisansüstü mezunlarında bu oran %22.2; lisans mezunu olanların %72.1'i ve lisansüstü mezunu olanların %66.6'sı siber dolandırıcılığa maruz kalmanız konusunda orta, çok ve aşırı düzeyde korku yaşarken, lise-ön lisans mezunlarında bu oran %50.1; lisans mezunu olanların %80.6'sı ve lisansüstü mezunu olanların %77.7'si sniffinge maruz kalmanız konusunda orta, çok ve aşırı düzeyde korku yaşarken, lise-ön lisans mezunlarında bu oran %68.8; lisans mezunu olanların %76.3'ü ve lisansüstü mezunu olanların %66.6'sı zombi ordulara maruz kalmanız konusunda orta, çok ve aşırı düzeyde korku yaşarken, lise-ön lisans mezunlarında bu oran %50.1; lisans mezunu olanların %77.5'i ve lisansüstü mezunu olanların %77.8'i sosyal ağ üzerinden sahtekârlığa maruz kalmanız konusunda orta, çok ve aşırı düzeyde korku yaşarken, lise-ön lisans mezunlarında bu oran %50.1; lisans mezunu olanların %66.7'si ve

lisansüstü mezunu olanların %77.8'i siber yer tespitine maruz kalmanız konusunda orta, çok ve aşırı düzeyde korku yaşarken, lise-ön lisans mezunlarında bu oran %43.8 ve lisans mezunu olanların %73.2'si ve lisansüstü mezunu olanların %88.9'u siber terörizme maruz kalmanız konusunda orta, çok ve aşırı düzeyde korku yaşarken, lise-ön lisans mezunlarında bu oran %56.3'tür. Bu sonuçlar siber suç türlerine maruz kalma açısından korku oranlarının genel olarak lisansüstü ve lisans mezunlarında daha yüksek olduğunu göstermektedir.

Katılımcıların algılanan ekonomik duruma göre siber suç türlerine maruz kalma korkusunun istatistiksel sonuçları çizelge 3.5.'te verilmiştir.

Çizelge 3.5. Katılımcıların Algılanan Ekonomik Duruma Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143)

		Algılanan Ekonomik Durum			
		Yetersiz (N=105)	**Yeterli (N=38)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
1. E-posta veya sosyal paylaşım sitelerine ait parolalarınızın çalınması konusunda	Hiç Korku Duymuyorum	24 (22.9)	0 (0.0)	15.627	**0.003**
	Biraz Korku Duyuyorum	31 (29.5)	10 (26.3)		
	Orta Düzeyde Korku Duyuyorum	30 (28.6)	16 (42.1)		
	Çok Korku Duyuyorum	16 (15.2)	12 (31.6)		
	Aşırı Düzeyde Korku Duyuyorum	4 (3.8)	0 (0.0)		
2. Banka hesap bilgilerinizin (hesap/kart numarası vb.) çalınması yoluyla zarara uğratılmanız konusunda	Hiç Korku Duymuyorum	4 (3.8)	2 (5.3)	12.478	**0.011****
	Biraz Korku Duyuyorum	10 (9.5)	2 (5.3)		
	Orta Düzeyde Korku Duyuyorum	32 (30.5)	18 (47.4)		
	Çok Korku Duyuyorum	39 (37.1)	16 (42.1)		
	Aşırı Düzeyde Korku Duyuyorum	20 (19.0)	0 (0.0)		
4. Bilgisayar korsanlığına (kişisel bilgisayarınıza veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalmanız konusunda	Hiç Korku Duymuyorum	14 (13.3)	2 (5.3)	14.210	**0.004****
	Biraz Korku Duyuyorum	25 (23.8)	8 (21.1)		
	Orta Düzeyde Korku Duyuyorum	48 (45.7)	10 (26.3)		
	Çok Korku Duyuyorum	14 (13.3)	16 (42.1)		
	Aşırı Düzeyde Korku Duyuyorum	4 (3.8)	2 (5.3)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.5. Katılımcıların Algılanan Ekonomik Duruma Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Algılanan Ekonomik Durum			
		Yetersiz (N=105)	**Yeterli (N=38)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
5. Truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalmanız konusunda	Hiç Korku Duymuyorum	10 (9.5)	2 (5.3)	10.932	**0.019****
	Biraz Korku Duyuyorum	33 (31.4)	6 (15.8)		
	Orta Düzeyde Korku Duyuyorum	44 (41.9)	16 (42.1)		
	Çok Korku Duyuyorum	14 (13.3)	14 (36.8)		
	Aşırı Düzeyde Korku Duyuyorum	4 (3.8)	0 (0.0)		
10. Siber hırsızlığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	10 (9.5)	0 (0.0)	12.790	**0.011**
	Biraz Korku Duyuyorum	22 (21.0)	6 (15.8)		
	Orta Düzeyde Korku Duyuyorum	45 (42.9)	16 (42.1)		
	Çok Korku Duyuyorum	20 (19.0)	16 (42.1)		
	Aşırı Düzeyde Korku Duyuyorum	8 (7.6)	0 (0.0)		
12. Siber dolandırıcılığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	6 (5.7)	2 (5.3)	12.542	**0.008****
	Biraz Korku Duyuyorum	28 (26.7)	12 (31.6)		
	Orta Düzeyde Korku Duyuyorum	51 (48.6)	10 (26.3)		
	Çok Korku Duyuyorum	14 (13.3)	14 (36.8)		
	Aşırı Düzeyde Korku Duyuyorum	6 (5.7)	0 (0.0)		
16. Siber yer tespitine maruz kalmanız konusunda	Hiç Korku Duymuyorum	16 (15.2)	4 (10.5)	11.240	**0.020****
	Biraz Korku Duyuyorum	29 (27.6)	4 (10.5)		
	Orta Düzeyde Korku Duyuyorum	44 (41.9)	18 (47.4)		
	Çok Korku Duyuyorum	12 (11.4)	12 (31.6)		
	Aşırı Düzeyde Korku Duyuyorum	4 (3.8)	0 (0.0)		
17. Bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalmanız konusunda	Hiç Korku Duymuyorum	14 (13.3)	6 (15.8)	11.542	**0.018**
	Biraz Korku Duyuyorum	28 (26.7)	4 (10.5)		
	Orta Düzeyde Korku Duyuyorum	37 (35.2)	12 (31.6)		
	Çok Korku Duyuyorum	20 (19.0)	16 (42.1)		
	Aşırı Düzeyde Korku Duyuyorum	6 (5.7)	0 (0.0)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.5. Katılımcıların Algılanan Ekonomik Duruma Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Algılanan Ekonomik Durum			
		Yetersiz (N=105)	**Yeterli (N=38)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
18. Siber terörizme maruz kalmanız konusunda	Hiç Korku Duymuyorum	12 (11.4)	4 (10.5)	17.155	**0.002**
	Biraz Korku Duyuyorum	21 (20.0)	4 (10.5)		
	Orta Düzeyde Korku Duyuyorum	44 (41.9)	16 (42.1)		
	Çok Korku Duyuyorum	12 (11.4)	14 (36.8)		
	Aşırı Düzeyde Korku Duyuyorum	16 (15.2)	0 (0.0)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Siber suç türlerine maruz kalma korkusunun algılanan ekonomik duruma göre farklılaşıp farklılaşmadığına ilişkin yapılan istatistiksel analizler sonucunda siber suç türlerine maruz kalma korkusundan e-posta veya sosyal paylaşım sitelerine ait parolaların çalınması (χ^2=15.627, p=0.003), banka hesap bilgilerinizin (hesap/kart numarası vb.) çalınması yoluyla zarara uğratılma (χ^2=12.478, p=0.011), bilgisayar korsanlığına (kişisel bilgisayarınıza veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalma (χ^2=14.210, p=0.004), truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalma (χ^2=10.932, p=0.019), siber hırsızlığa maruz kalma (χ^2=12.790, p=0.011), siber dolandırıcılığa maruz kalma (χ^2=12.542, p=0.008), siber yer tespitine maruz kalma (χ^2=11.240, p=0.020), bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalma (χ^2=11.542, p=0.018) ve siber terörizme maruz kalma (χ^2=17.155, p=0.002) korkularının algılanan ekonomik duruma göre anlamlı olarak farklılaştığı bulunmuştur (p<0.01, p<0.05). Buna göre ekonomik durumunu yeterli olarak algılayanların %31.6'sı e-posta veya sosyal paylaşım sitelerine ait parolalarının çalınması konusunda çok ve aşırı düzeyde korku yaşarken, ekonomik durumunu yetersiz olarak algılayanlarda bu oran %19; ekonomik durumunu yetersiz olarak algılayanların %56.1'i banka hesap bilgilerinin (hesap/kart numarası vb.) çalınması yoluyla zarara uğratılma konusunda çok ve aşırı düzeyde korku yaşarken, ekonomik durumunu yeterli olarak algılayanlarda bu oran %42.1; ekonomik durumunu yeterli olarak algılayanların %47.4'ü bilgisayar korsanlığına (kişisel bilgisayarınıza veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, ekonomik durumunu yetersiz olarak algılayanlarda bu oran %17.1; ekonomik durumunu yeterli olarak algılayanların %36.8'i

truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, ekonomik durumunu yetersiz olarak algılayanlarda bu oran %17.1; ekonomik durumunu yeterli olarak algılayanların %42.1'i siber hırsızlığa maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, ekonomik durumunu yetersiz olarak algılayanlarda bu oran %26.6; ekonomik durumunu yeterli olarak algılayanların %36.8'i siber dolandırıcılığa maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, ekonomik durumunu yetersiz olarak algılayanlarda bu oran %19; ekonomik durumunu yeterli olarak algılayanların %31.6'sı siber yer tespitine maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, ekonomik durumunu yetersiz olarak algılayanlarda bu oran %15.2; ekonomik durumunu yeterli olarak algılayanların %42.1'i bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, ekonomik durumunu yetersiz olarak algılayanlarda bu oran %24.7 ve ekonomik durumunu yeterli olarak algılayanların %36.8'i siber terörizme maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, ekonomik durumunu yetersiz olarak algılayanlarda bu oran %26.6'dır. Bu sonuçlar siber suç türlerine maruz kalma açısından korku oranlarının genel olarak ekonomik durumunu yeterli olarak algılayanlarda daha yüksek olduğunu göstermektedir.

Katılımcıların mesleğindeki çalışma yılına göre siber suç türlerine maruz kalma korkusunun istatistiksel sonuçları çizelge 3.6.'da verilmiştir.

Çizelge 3.6. Katılımcıların Mesleğindeki Çalışma Yılına Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143)

		Mesleğindeki Çalışma Yılı				
		1 Yıl ve Altı (N=32)	**2-8 Yıl Arası (N=62)**	**9 Yıl ve Üzeri (N=49)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
1. E-posta veya sosyal paylaşım sitelerine ait parolalarınızın çalınması konusunda	Hiç Korku Duymuyorum	16 (50.0)	6 (9.7)	2 (4.1)	44.851	**0.000**
	Biraz Korku Duyuyorum	8 (25.0)	20 (32.3)	13 (26.5)		
	Orta Düzeyde Korku Duyuyorum	6 (18.8)	26 (41.9)	14 (28.6)		
	Çok Korku Duyuyorum	2 (6.3)	8 (12.9)	18 (36.7)		
	Aşırı Düzeyde Korku Duyuyorum	0 (0.0)	2 (3.2)	2 (4.1)		
2. Banka hesap bilgilerinizin (hesap/kart numarası vb.) çalınması yoluyla zarara uğratılmanız konusunda	Hiç Korku Duymuyorum	2 (6.3)	2 (3.2)	2 (4.1)	16.848	**0.021****
	Biraz Korku Duyuyorum	8 (25.0)	4 (6.5)	0 (0.0)		
	Orta Düzeyde Korku Duyuyorum	10 (31.3)	24 (38.7)	16 (32.7)		
	Çok Korku Duyuyorum	8 (25.0)	24 (38.7)	23 (46.9)		
	Aşırı Düzeyde Korku Duyuyorum	4 (12.5)	8 (12.9)	8 (16.3)		
3. Kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalmanız konusunda	Hiç Korku Duymuyorum	4 (12.5)	0 (0.0)	2 (4.1)	20.808	**0.004****
	Biraz Korku Duyuyorum	8 (25.0)	2 (3.2)	4 (8.2)		
	Orta Düzeyde Korku Duyuyorum	12 (37.5)	30 (48.4)	21 (42.9)		
	Çok Korku Duyuyorum	6 (18.8)	24 (38.7)	20 (40.8)		
	Aşırı Düzeyde Korku Duyuyorum	2 (6.3)	6 (9.7)	2 (4.1)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.6. Katılımcıların Mesleğindeki Çalışma Yılına Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Mesleğindeki Çalışma Yılı				
		1 Yıl ve Altı (N=32)	2-8 Yıl Arası (N=62)	9 Yıl ve Üzeri (N=49)	İstatistiksel Analiz	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
4. Bilgisayar korsanlığına (kişisel bilgisayarınıza veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalmanız konusunda	Hiç Korku Duymuyorum	10 (31.3)	4 (6.5)	2 (4.1)	18.380	**0.010****
	Biraz Korku Duyuyorum	8 (25.0)	14 (22.6)	11 (22.4)		
	Orta Düzeyde Korku Duyuyorum	6 (18.8)	30 (48.4)	22 (44.9)		
	Çok Korku Duyuyorum	6 (18.8)	12 (19.4)	12 (24.5)		
	Aşırı Düzeyde Korku Duyuyorum	2 (6.3)	2 (3.2)	2 (4.1)		
5. Truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalmanız konusunda	Hiç Korku Duymuyorum	8 (25.0)	2 (3.2)	2 (4.1)	30.559	**0.000****
	Biraz Korku Duyuyorum	4 (12.5)	28 (45.2)	7 (14.3)		
	Orta Düzeyde Korku Duyuyorum	16 (50.0)	22 (35.5)	22 (44.9)		
	Çok Korku Duyuyorum	4 (12.5)	8 (12.9)	16 (32.7)		
	Aşırı Düzeyde Korku Duyuyorum	0 (0.0)	2 (3.2)	2 (4.1)		
6. Keylogger ve screenlogger gibi casus yazılımlara maruz kalmanız konusunda	Hiç Korku Duymuyorum	6 (18.8)	2 (3.2)	2 (4.1)	17.875	**0.012****
	Biraz Korku Duyuyorum	4 (12.5)	18 (29.0)	9 (18.4)		
	Orta Düzeyde Korku Duyuyorum	18 (56.3)	26 (41.9)	18 (36.7)		
	Çok Korku Duyuyorum	4 (12.5)	12 (19.4)	18 (36.7)		
	Aşırı Düzeyde Korku Duyuyorum	0 (0.0)	4 (6.5)	2 (4.1)		
7. Siber zorbalığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	8 (25.0)	0 (0.0)	2 (4.1)	21.130	**0.002****
	Biraz Korku Duyuyorum	4 (12.5)	14 (22.6)	6 (12.2)		
	Orta Düzeyde Korku Duyuyorum	14 (43.8)	30 (48.4)	21 (42.9)		
	Çok Korku Duyuyorum	6 (18.8)	16 (25.8)	18 (36.7)		
	Aşırı Düzeyde Korku Duyuyorum	0 (0.0)	2 (3.2)	2 (4.1)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.6. Katılımcıların Mesleğindeki Çalışma Yılına Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Mesleğindeki Çalışma Yılı				
		1 Yıl ve Altı (N=32)	2-8 Yıl Arası (N=62)	9 Yıl ve Üzeri (N=49)	İstatistiksel Analiz	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
10. Siber hırsızlığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	6 (18.8)	2 (3.2)	2 (4.1)	17.100	**0.018****
	Biraz Korku Duyuyorum	6 (18.8)	18 (29.0)	4 (8.2)		
	Orta Düzeyde Korku Duyuyorum	14 (43.8)	24 (38.7)	23 (46.9)		
	Çok Korku Duyuyorum	6 (18.8)	14 (22.6)	16 (32.7)		
	Aşırı Düzeyde Korku Duyuyorum	0 (0.0)	4 (6.5)	4 (8.2)		
11. Siber ortamda haberleşme gizliliğinizin ihlali (kayıt altına alınması ya da ifşası gibi) konusunda	Hiç Korku Duymuyorum	6 (18.8)	2 (3.2)	2 (4.1)	17.550	**0.013****
	Biraz Korku Duyuyorum	10 (31.3)	18 (29.0)	5 (10.2)		
	Orta Düzeyde Korku Duyuyorum	8 (25.0)	22 (35.5)	26 (53.1)		
	Çok Korku Duyuyorum	8 (25.0)	18 (29.0)	14 (28.6)		
	Aşırı Düzeyde Korku Duyuyorum	0 (0.0)	2 (3.2)	2 (4.1)		
12. Siber dolandırıcılığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	4 (12.5)	2 (3.2)	2 (4.1)	20.226	**0.003****
	Biraz Korku Duyuyorum	16 (50.0)	18 (29.0)	6 (12.2)		
	Orta Düzeyde Korku Duyuyorum	8 (25.0)	28 (45.2)	25 (51.0)		
	Çok Korku Duyuyorum	4 (12.5)	12 (19.4)	12 (24.5)		
	Aşırı Düzeyde Korku Duyuyorum	0 (0.0)	2 (3.2)	4 (8.2)		
13. Sniffinge maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (6.3)	2 (3.2)	2 (4.1)	16.566	**0.019****
	Biraz Korku Duyuyorum	10 (31.3)	14 (22.6)	2 (4.1)		
	Orta Düzeyde Korku Duyuyorum	16 (50.0)	28 (45.2)	27 (55.1)		
	Çok Korku Duyuyorum	4 (12.5)	14 (22.6)	16 (32.7)		
	Aşırı Düzeyde Korku Duyuyorum	0 (0.0)	4 (6.5)	2 (4.1)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.6. Katılımcıların Mesleğindeki Çalışma Yılına Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Mesleğindeki Çalışma Yılı				
		1 Yıl ve Altı (N=32)	2-8 Yıl Arası (N=62)	9 Yıl ve Üzeri (N=49)	İstatistiksel Analiz	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
13. Sniffinge maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (6.3)	2 (3.2)	2 (4.1)	16.566	**0.019****
	Biraz Korku Duyuyorum	10 (31.3)	14 (22.6)	2 (4.1)		
	Orta Düzeyde Korku Duyuyorum	16 (50.0)	28 (45.2)	27 (55.1)		
	Çok Korku Duyuyorum	4 (12.5)	14 (22.6)	16 (32.7)		
	Aşırı Düzeyde Korku Duyuyorum	0 (0.0)	4 (6.5)	2 (4.1)		
14. Zombi ordulara maruz kalmanız konusunda	Hiç Korku Duymuyorum	4 (12.5)	0 (0.0)	2 (4.1)	17.182	**0.015****
	Biraz Korku Duyuyorum	10 (31.3)	20 (32.3)	8 (16.3)		
	Orta Düzeyde Korku Duyuyorum	14 (43.8)	26 (41.9)	19 (38.8)		
	Çok Korku Duyuyorum	4 (12.5)	12 (19.4)	18 (36.7)		
	Aşırı Düzeyde Korku Duyuyorum	0 (0.0)	4 (6.5)	2 (4.1)		
15. Sosyal ağ üzerinden sahtekârlığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	12 (37.5)	4 (6.5)	2 (4.1)	24.447	**0.000****
	Biraz Korku Duyuyorum	6 (18.8)	12 (19.4)	5 (10.2)		
	Orta Düzeyde Korku Duyuyorum	10 (31.3)	32 (51.6)	24 (49.0)		
	Çok Korku Duyuyorum	4 (12.5)	12 (19.4)	14 (28.6)		
	Aşırı Düzeyde Korku Duyuyorum	0 (0.0)	2 (3.2)	4 (8.2)		
16. Siber yer tespitine maruz kalmanız konusunda	Hiç Korku Duymuyorum	10 (31.3)	6 (9.7)	4 (8.2)	17.490	**0.015****
	Biraz Korku Duyuyorum	4 (12.5)	20 (32.3)	9 (18.4)		
	Orta Düzeyde Korku Duyuyorum	10 (31.3)	28 (45.2)	24 (49.0)		
	Çok Korku Duyuyorum	8 (25.0)	6 (9.7)	10 (20.4)		
	Aşırı Düzeyde Korku Duyuyorum	0 (0.0)	2 (3.2)	2 (4.1)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.6. Katılımcıların Mesleğindeki Çalışma Yılına Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Mesleğindeki Çalışma Yılı				
		1 Yıl ve Altı (N=32)	**2-8 Yıl Arası (N=62)**	**9 Yıl ve Üzeri (N=49)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
18. Siber terörizme maruz kalmanız konusunda	Hiç Korku Duymuyorum	6 (18.8)	6 (9.7)	4 (8.2)	27.166	**0.000**
	Biraz Korku Duyuyorum	0 (0.0)	18 (29.0)	7 (14.3)		
	Orta Düzeyde Korku Duyuyorum	14 (43.8)	26 (41.9)	20 (40.8)		
	Çok Korku Duyuyorum	6 (18.8)	4 (6.5)	16 (32.7)		
	Aşırı Düzeyde Korku Duyuyorum	6 (18.8)	8 (12.9)	2 (4.1)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Siber suç türlerine maruz kalma korkusunun mesleğindeki çalışma yılına göre farklılaşıp farklılaşmadığına ilişkin yapılan istatistiksel analizler sonucunda siber suç türlerine maruz kalma korkusundan siber tacize maruz kalma (χ^2=11.197, p=0.168), siber şantaja veya siber tehdide (siber ortamda şantaj veya tehdit davranışlarına) maruz kalma (χ^2=8.929, p=0.336) ve bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalma korkusu (χ^2=7.159, p=0.520) haricinde diğer siber suç türlerinin meslekte çalışma yılına göre anlamlı

olarak farklılaştığı bulunmuştur ($p<0.001$, $p<0.01$, $p<0.05$). Buna göre, 9 yıl ve üzeri çalışanların %40.8'i e-posta veya sosyal paylaşım sitelerine ait parolalarının çalınması konusunda çok ve aşırı düzeyde korku yaşarken, 1 yıl ve altı ile 2-8 yıl arası çalışanlarda bu oran sırasıyla %6.3 ve %16.1; 9 yıl ve üzeri çalışanların %63.2'si ve 2-8 yıl arası çalışanların %51.6'sı banka hesap bilgilerinin (hesap/kart numarası vb.) çalınması yoluyla zarara uğratılma konusunda çok ve aşırı düzeyde korku yaşarken, 1 yıl ve altı çalışanlarda bu oran %37.5; 9 yıl ve üzeri çalışanların %44.9'u ve 2-8 yıl arası çalışanların %48.4'ü kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, 1 yıl ve altı çalışanlarda bu oran %25.1; 9 yıl ve üzeri çalışanların %73.5'i ve 2-8 yıl arası çalışanların %71'i bilgisayar korsanlığına (kişisel bilgisayarınıza veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, 1 yıl ve altı çalışanlarda bu oran %43.9; 9 yıl ve üzeri çalışanların %36.8'i truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, 1 yıl ve altı ile 2-8 yıl arası çalışanlarda bu oran sırasıyla %12.5 ve %16.1; 9 yıl ve üzeri çalışanların %40.8'i ve 2-8 yıl arası çalışanların %25.9'u keylogger ve screenlogger gibi casus yazılımlara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, 1 yıl ve altı çalışanlarda bu oran %12.5; 9 yıl ve üzeri çalışanların %40.8'i ve 2-8 yıl arası çalışanların %29'u siber zorbalığa maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, 1 yıl ve altı çalışanlarda bu oran %18.8; 9 yıl ve üzeri çalışanların %40.9'u ve 2-8 yıl arası çalışanların %29.1'i siber hırsızlığa maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, 1 yıl ve altı çalışanlarda bu oran %18.8; 9 yıl ve üzeri çalışanların %85.8'i ve 2-8 yıl arası çalışanların %67.7'si siber ortamda haberleşme gizliliğinizin ihlali (kayıt altına alınması ya da ifşası gibi) konusunda orta, çok ve aşırı düzeyde korku yaşarken, 1 yıl ve altı çalışanlarda bu oran %50; 9 yıl ve üzeri çalışanların %32.7'si ve 2-8 yıl arası çalışanların %22.6'sı siber dolandırıcılığa maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, 1 yıl ve altı çalışanlarda bu oran %12.5; 9 yıl ve üzeri çalışanların %36.8'i ve 2-8 yıl arası çalışanların %29.1'i sniffinge maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, 1 yıl ve altı çalışanlarda bu oran %12.5; 9 yıl ve üzeri çalışanların %40.8'i ve 2-8 yıl arası çalışanların %25.9'u zombi ordulara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, 1 yıl ve altı çalışanlarda bu oran %12.5; 9 yıl ve üzeri çalışanların %36.8'i ve 2-8 yıl arası çalışanların %22.6'sı sosyal ağ üzerinden sahtekârlığa maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, 1 yıl ve altı çalışanlarda bu oran %12.5; 9 yıl ve üzeri çalışanların %24.5'i

ve 1 yıl ve altı çalışanların %25'i siber yer tespitine maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, 2-8 yıl arası çalışanlarda bu oran %12.9 ve 9 yıl ve üzeri çalışanların %36.8'i ve 1 yıl ve altı çalışanların %37.6'sı siber terörizme maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, 2-8 yıl arası çalışanlarda bu oran %19.4'tür. Bu sonuçlar siber suç türlerine maruz kalma açısından korku oranlarının genel olarak 9 yıl ve üzeri ile 2-8 yıl arası çalışanlarda daha yüksek olduğunu göstermektedir.

Katılımcıların görev aldığı sektöre göre siber suç türlerine maruz kalma korkusunun istatistiksel sonuçları çizelge 3.7.'de verilmiştir.

Çizelge 3.7. Katılımcıların Görev Aldığı Sektöre Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143)

		Görev Aldığı Sektör			
		Yazılım ve Bilişim (N=63)	**Diğer (N=80)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
1. E-posta veya sosyal paylaşım sitelerine ait parolalarınızın çalınması konusunda	Hiç Korku Duymuyorum	8 (12.7)	16 (20.0)	11.436	**0.018**
	Biraz Korku Duyuyorum	26 (41.3)	15 (18.8)		
	Orta Düzeyde Korku Duyuyorum	19 (30.2)	27 (33.8)		
	Çok Korku Duyuyorum	10 (15.9)	18 (22.5)		
	Aşırı Düzeyde Korku Duyuyorum	0 (0.0)	4 (5.0)		
14. Zombi ordulara maruz kalmanız konusunda	Hiç Korku Duymuyorum	4 (6.3)	2 (2.5)	13.037	**0.007****
	Biraz Korku Duyuyorum	24 (38.1)	14 (17.5)		
	Orta Düzeyde Korku Duyuyorum	22 (34.9)	37 (46.3)		
	Çok Korku Duyuyorum	13 (20.6)	21 (26.3)		
	Aşırı Düzeyde Korku Duyuyorum	0 (0.0)	6 (7.5)		
15. Sosyal ağ üzerinden sahtekârlığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	8 (12.7)	10 (12.5)	11.387	**0.019**
	Biraz Korku Duyuyorum	16 (25.4)	7 (8.8)		
	Orta Düzeyde Korku Duyuyorum	26 (41.3)	40 (50.0)		
	Çok Korku Duyuyorum	13 (20.6)	17 (21.3)		
	Aşırı Düzeyde Korku Duyuyorum	0 (0.0)	6 (7.5)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.7. Katılımcıların Görev Aldığı Sektöre Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Görev Aldığı Sektör			
		Yazılım ve Bilişim (N=63)	Diğer (N=80)	İstatistiksel Analiz	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
17. Bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalmanız konusunda	Hiç Korku Duymuyorum	13 (20.6)	7 (8.8)	9.669	**0.045**
	Biraz Korku Duyuyorum	11 (17.5)	21 (26.3)		
	Orta Düzeyde Korku Duyuyorum	23 (36.5)	26 (32.5)		
	Çok Korku Duyuyorum	16 (25.4)	20 (25.0)		
	Aşırı Düzeyde Korku Duyuyorum	0 (0.0)	6 (7.5)		
18. Siber terörizme maruz kalmanız konusunda	Hiç Korku Duymuyorum	11 (17.5)	5 (6.3)	14.296	**0.005**
	Biraz Korku Duyuyorum	10 (15.9)	15 (18.8)		
	Orta Düzeyde Korku Duyuyorum	30 (47.6)	30 (37.5)		
	Çok Korku Duyuyorum	11 (17.5)	15 (18.8)		
	Aşırı Düzeyde Korku Duyuyorum	1 (1.6)	15 (18.8)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Siber suç türlerine maruz kalma korkusunun görev aldığı sektöre göre farklılaşıp farklılaşmadığına ilişkin yapılan istatistiksel analizler sonucunda siber suç türlerine maruz kalma korkusundan e-posta veya sosyal paylaşım sitelerine ait parolaların çalınması (χ^2=11.436, p=0.018), zombi ordulara maruz kalma (χ^2=13.037, p=0.007), sosyal ağ üzerinden sahtekârlığa maruz kalma (χ^2=11.387, p=0.019), bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalma (χ^2=9.669, p=0.045) ve siber terörizme maruz kalma (χ^2=14.296, p=0.005) korkularının görev aldığı sektöre göre anlamlı olarak farklılaştığı bulunmuştur (p<0.01, p<0.05). Buna göre, diğer sektörde görev alanların %27.5'i e-posta veya sosyal paylaşım sitelerine ait parolalarınının çalınması konusunda çok ve aşırı düzeyde korku yaşarken, yazılım ve bilişim sektöründe görev alanlarda bu oran %15.9; diğer sektörde görev alanların %33.8'i zombi ordulara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, yazılım ve bilişim sektöründe görev alanlarda bu oran %20.6; diğer sektörde görev alanların %28.8'i sosyal ağ üzerinden sahtekârlığa maruz kalmanız konusunda çok ve aşırı düzeyde korku yaşarken, yazılım ve bilişim sektöründe görev alanlarda bu oran %20.6; diğer sektörde görev alanların %32.5'i bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalmanız konusunda çok ve aşırı düzeyde korku yaşarken, yazılım ve bilişim sektöründe görev alanlarda bu oran %25.4 ve

diğer sektörde görev alanların %37.6'sı siber terörizme maruz kalmanız konusunda çok ve aşırı düzeyde korku yaşarken, yazılım ve bilişim sektöründe görev alanlarda bu oran %19.1'dir. Bu sonuçlar, siber suç türlerine maruz kalma açısından korku oranlarının diğer sektörde görev alanlarda daha yüksek olduğunu göstermektedir.

Katılımcıların internete en çok hangi araçtan erişim sağladığına göre siber suç türlerine maruz kalma korkusunun istatistiksel sonuçları çizelge 3.8.'de verilmiştir.

Çizelge 3.8. Katılımcıların İnternete En Çok Hangi Araçtan Erişim Sağladığına Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143)

		İnternete Erişim Sağlama (En Çok)				
		Mobil Cihaz (N=70)	**Kişisel Bilgisayar (N=30)**	**Kurumsal Cihazlar (N=43)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
2. Banka hesap bilgilerinizin (hesap/kart numarası vb.) çalınması yoluyla zarara uğratılmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	2 (6.7)	4 (9.3)	30.961	**0.000**
	Biraz Korku Duyuyorum	10 (14.3)	2 (6.7)	0 (0.0)		
	Orta Düzeyde Korku Duyuyorum	14 (20.0)	18 (60.0)	18 (41.9)		
	Çok Korku Duyuyorum	32 (45.7)	6 (20.0)	17 (39.5)		
	Aşırı Düzeyde Korku Duyuyorum	14 (20.0)	2 (6.7)	4 (9.3)		
3. Kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (2.9)	2 (6.7)	2 (4.7)	17.164	**0.018**
	Biraz Korku Duyuyorum	6 (8.6)	4 (13.3)	4 (9.3)		
	Orta Düzeyde Korku Duyuyorum	22 (31.4)	16 (53.3)	25 (58.1)		
	Çok Korku Duyuyorum	34 (48.6)	8 (26.7)	8 (18.6)		
	Aşırı Düzeyde Korku Duyuyorum	6 (8.6)	0 (0.0)	4 (9.3)		
9. Siber şantaja veya siber tehdide (siber ortamda şantaj veya tehdit davranışlarına) maruz kalmanız konusunda	Hiç Korku Duymuyorum	8 (11.4)	0 (0.0)	4 (9.3)	19.231	**0.009**
	Biraz Korku Duyuyorum	18 (25.7)	6 (20.0)	9 (20.9)		
	Orta Düzeyde Korku Duyuyorum	16 (22.9)	20 (66.7)	18 (41.9)		
	Çok Korku Duyuyorum	24 (34.3)	4 (13.3)	10 (23.3)		
	Aşırı Düzeyde Korku Duyuyorum	4 (5.7)	0 (0.0)	2 (4.7)		

*Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.8. Katılımcıların İnternete En Çok Hangi Araçtan Erişim Sağladığına Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		İnternete Erişim Sağlama (En Çok)				
		Mobil Cihaz (N=70)	Kişisel Bilgisayar (N=30)	Kurumsal Cihazlar (N=43)	İstatistiksel Analiz	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
10. Siber hırsızlığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	6 (20.0)	4 (9.3)	30.134	**0.000**
	Biraz Korku Duyuyorum	20 (28.6)	0 (0.0)	8 (18.6)		
	Orta Düzeyde Korku Duyuyorum	24 (34.3)	18 (60.0)	19 (44.2)		
	Çok Korku Duyuyorum	20 (28.6)	6 (20.0)	10 (23.3)		
	Aşırı Düzeyde Korku Duyuyorum	6 (8.6)	0 (0.0)	2 (4.7)		
11. Siber ortamda haberleşme gizliliğinizin ihlali (kayıt altına alınması ya da ifşası gibi) konusunda	Hiç Korku Duymuyorum	4 (5.7)	4 (13.3)	2 (4.7)	21.613	**0.003**
	Biraz Korku Duyuyorum	22 (31.4)	4 (13.3)	7 (16.3)		
	Orta Düzeyde Korku Duyuyorum	16 (22.9)	18 (60.0)	22 (51.2)		
	Çok Korku Duyuyorum	26 (37.1)	4 (13.3)	10 (23.3)		
	Aşırı Düzeyde Korku Duyuyorum	2 (2.9)	0 (0.0)	2 (4.7)		
13. Sniffinge maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (2.9)	2 (6.7)	2 (4.7)	24.142	**0.000**
	Biraz Korku Duyuyorum	18 (25.7)	0 (0.0)	8 (18.6)		
	Orta Düzeyde Korku Duyuyorum	24 (34.3)	24 (80.0)	23 (53.5)		
	Çok Korku Duyuyorum	22 (31.4)	4 (13.3)	8 (18.6)		
	Aşırı Düzeyde Korku Duyuyorum	4 (5.7)	0 (0.0)	2 (4.7)		
18. Siber terörizme maruz kalmanız konusunda	Hiç Korku Duymuyorum	4 (5.7)	4 (13.3)	8 (18.6)	21.024	**0.005**
	Biraz Korku Duyuyorum	18 (25.7)	2 (6.7)	5 (11.6)		
	Orta Düzeyde Korku Duyuyorum	20 (28.6)	18 (60.0)	22 (51.2)		
	Çok Korku Duyuyorum	16 (22.9)	4 (13.3)	6 (14.0)		
	Aşırı Düzeyde Korku Duyuyorum	12 (17.1)	2 (6.7)	2 (4.7)		

*Fisher Freeman Halton testi, [a]Sütun yüzdesi

Siber suç türlerine maruz kalma korkusunun internete en çok hangi araçtan erişim sağladığına göre farklılaşıp farklılaşmadığına ilişkin yapılan istatistiksel analizler sonucunda siber suç türlerine maruz kalma korkusundan banka hesap bilgilerin (hesap/kart numarası vb.) çalınması yoluyla zarara uğratılma (χ^2=30.961, p=0.000), kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalma (χ^2=17.164, p=0.018), siber şantaja veya siber tehdide (siber ortamda şantaj veya tehdit davranışlarına) maruz kalma (χ^2=19.231, p=0.009), siber hırsızlığa maruz kalma (χ^2=30.134, p=0.000), siber ortamda haberleşme gizliliğinizin ihlali (χ^2=21.613, p=0.003), sniffinge maruz kalma (χ^2=24.142, p=0.000) ve siber terörizme maruz kalma (χ^2=21.024, p=0.005) korkularının internete en çok hangi araçtan erişim sağladığına göre anlamlı olarak farklılaştığı bulunmuştur (p<0.001, p<0.01, p<0.05). Buna göre, mobil cihazdan erişim sağlayanların %65.7'si ve kurumsal cihazlardan erişim sağlayanların %48.8'i banka hesap bilgilerininin (hesap/kart numarası vb.) çalınması yoluyla zarara uğratılma konusunda çok ve aşırı düzeyde korku yaşarken, kişisel bilgisayardan erişim sağlayanlarda bu oran %26.7; mobil cihazdan erişim sağlayanların %57.2'si kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kişisel bilgisayardan ve kurumsal cihazlardan erişim sağlayanlarda bu oran sırasıyla %26.7 ve %27.9; mobil cihazdan erişim sağlayanların %40'ı ve kurumsal cihazlardan erişim sağlayanların %28'i siber şantaja veya siber tehdide (siber ortamda şantaj veya tehdit davranışlarına) maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kişisel bilgisayardan erişim sağlayanlarda bu oran %13.3; mobil cihazdan erişim sağlayanların %37.2'si ve kurumsal cihazlardan erişim sağlayanların %28'i siber hırsızlığa maruz kalmanız konusunda çok ve aşırı düzeyde korku yaşarken, kişisel bilgisayardan erişim sağlayanlarda bu oran %20; mobil cihazdan erişim sağlayanların %40'ı ve kurumsal cihazlardan erişim sağlayanların %28'i siber ortamda haberleşme gizliliğinin ihlali (kayıt altına alınması ya da ifşası gibi) konusunda çok ve aşırı düzeyde korku yaşarken, kişisel bilgisayardan erişim sağlayanlarda bu oran %13.3; mobil cihazdan erişim sağlayanların %37.1'i ve kurumsal cihazlardan erişim sağlayanların %23.3'ü sniffinge maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kişisel bilgisayardan erişim sağlayanlarda bu oran %13.3 ve mobil cihazdan erişim sağlayanların %40'ı siber terörizme maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kişisel bilgisayardan ve kurumsal cihazlardan erişim sağlayanlarda bu oran sırasıyla %20 ve %18.7'dir. Bu sonuçlar, siber suç

türlerine maruz kalma açısından korku oranlarının genel olarak mobil cihazdan ve kurumsal cihazlardan erişim sağlayanlarda daha yüksek olduğunu göstermektedir.

Katılımcıların kamuya açık alanlarda bulunan kablosuz ağlara erişim sağlama durumuna göre siber suç türlerine maruz kalma korkusunun istatistiksel sonuçları çizelge 3.9.'da verilmiştir.

Çizelge 3.9. Katılımcıların Kamuya Açık Alanlarda Bulunan Kablosuz Ağlara Erişim Sağlama Durumuna Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143)

		Kamuya Açık Alanlarda Bulunan Kablosuz Ağlara Erişim Sağlama			
		Evet (N=36)	**Hayır (N=107)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
1. E-posta veya sosyal paylaşım sitelerine ait parolalarınızın çalınması konusunda	Hiç Korku Duymuyorum	4 (11.1)	20 (18.7)	13.569	**0.010**
	Biraz Korku Duyuyorum	8 (22.2)	33 (30.8)		
	Orta Düzeyde Korku Duyuyorum	8 (22.2)	38 (35.5)		
	Çok Korku Duyuyorum	14 (38.9)	14 (13.1)		
	Aşırı Düzeyde Korku Duyuyorum	2 (5.6)	2 (1.9)		
3. Kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (5.6)	4 (3.7)	15.418	**0.002****
	Biraz Korku Duyuyorum	2 (5.6)	12 (11.2)		
	Orta Düzeyde Korku Duyuyorum	12 (33.3)	51 (47.7)		
	Çok Korku Duyuyorum	12 (33.3)	38 (35.5)		
	Aşırı Düzeyde Korku Duyuyorum	8 (22.2)	2 (1.9)		
4. Bilgisayar korsanlığına (kişisel bilgisayarınıza veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (5.6)	14 (13.1)	10.175	**0.031****
	Biraz Korku Duyuyorum	8 (22.2)	25 (23.4)		
	Orta Düzeyde Korku Duyuyorum	10 (27.8)	48 (44.9)		
	Çok Korku Duyuyorum	14 (38.9)	16 (15.0)		
	Aşırı Düzeyde Korku Duyuyorum	2 (5.6)	4 (3.7)		
5. Truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (5.6)	10 (9.3)	12.658	**0.009****
	Biraz Korku Duyuyorum	6 (16.7)	33 (30.8)		
	Orta Düzeyde Korku Duyuyorum	12 (33.3)	48 (44.9)		
	Çok Korku Duyuyorum	14 (38.9)	14 (13.1)		
	Aşırı Düzeyde Korku Duyuyorum	2 (5.6)	2 (1.9)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.9. Katılımcıların Kamuya Açık Alanlarda Bulunan Kablosuz Ağlara Erişim Sağlama Durumuna Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Kamuya Açık Alanlarda Bulunan Kablosuz Ağlara Erişim Sağlama			
		Evet (N=36)	**Hayır (N=107)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
6. Keylogger ve screenlogger gibi casus yazılımlara maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (5.6)	8 (7.5)	17.774	**0.000****
	Biraz Korku Duyuyorum	4 (11.1)	27 (25.2)		
	Orta Düzeyde Korku Duyuyorum	10 (27.8)	52 (48.6)		
	Çok Korku Duyuyorum	16 (44.4)	18 (16.8)		
	Aşırı Düzeyde Korku Duyuyorum	4 (11.1)	2 (1.9)		
9. Siber şantaja veya siber tehdide (siber ortamda şantaj veya tehdit davranışlarına) maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (5.6)	10 (9.3)	9.715	**0.035****
	Biraz Korku Duyuyorum	6 (16.7)	27 (25.2)		
	Orta Düzeyde Korku Duyuyorum	10 (27.8)	44 (41.1)		
	Çok Korku Duyuyorum	14 (38.9)	24 (22.4)		
	Aşırı Düzeyde Korku Duyuyorum	4 (11.1)	2 (1.9)		
12. Siber dolandırıcılığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (5.6)	6 (5.6)	19.764	**0.000****
	Biraz Korku Duyuyorum	4 (11.1)	36 (33.6)		
	Orta Düzeyde Korku Duyuyorum	12 (33.3)	49 (45.8)		
	Çok Korku Duyuyorum	16 (44.4)	12 (11.2)		
	Aşırı Düzeyde Korku Duyuyorum	2 (5.6)	4 (3.7)		
13. Sniffinge maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (5.6)	4 (3.7)	13.370	**0.005****
	Biraz Korku Duyuyorum	4 (11.1)	22 (20.6)		
	Orta Düzeyde Korku Duyuyorum	12 (33.3)	59 (55.1)		
	Çok Korku Duyuyorum	14 (38.9)	20 (18.7)		
	Aşırı Düzeyde Korku Duyuyorum	4 (11.1)	2 (1.9)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.9. Katılımcıların Kamuya Açık Alanlarda Bulunan Kablosuz Ağlara Erişim Sağlama Durumuna Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Kamuya Açık Alanlarda Bulunan Kablosuz Ağlara Erişim Sağlama			
		Evet (N=36)	**Hayır (N=107)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
14. Zombi ordulara maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (5.6)	4 (3.7)	19.142	**0.000****
	Biraz Korku Duyuyorum	6 (16.7)	32 (29.9)		
	Orta Düzeyde Korku Duyuyorum	8 (22.2)	51 (47.7)		
	Çok Korku Duyuyorum	16 (44.4)	18 (16.8)		
	Aşırı Düzeyde Korku Duyuyorum	4 (11.1)	2 (1.9)		
15. Sosyal ağ üzerinden sahtekârlığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (5.6)	16 (15.0)	22.763	**0.000****
	Biraz Korku Duyuyorum	4 (11.1)	19 (17.8)		
	Orta Düzeyde Korku Duyuyorum	10 (27.8)	56 (52.3)		
	Çok Korku Duyuyorum	18 (50.0)	12 (11.2)		
	Aşırı Düzeyde Korku Duyuyorum	2 (5.6)	4 (3.7)		
16. Siber yer tespitine maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (5.6)	18 (16.8)	12.684	**0.013**
	Biraz Korku Duyuyorum	6 (16.7)	27 (25.2)		
	Orta Düzeyde Korku Duyuyorum	14 (38.9)	48 (44.9)		
	Çok Korku Duyuyorum	12 (33.3)	12 (11.2)		
	Aşırı Düzeyde Korku Duyuyorum	2 (5.6)	2 (1.9)		
18. Siber terörizme maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (5.6)	14 (13.1)	14.681	**0.005**
	Biraz Korku Duyuyorum	4 (11.1)	21 (19.6)		
	Orta Düzeyde Korku Duyuyorum	12 (33.3)	48 (44.9)		
	Çok Korku Duyuyorum	14 (38.9)	12 (11.2)		
	Aşırı Düzeyde Korku Duyuyorum	4 (11.1)	12 (11.2)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Siber suç türlerine maruz kalma korkusunun kamuya açık alanlarda bulunan kablosuz ağlara erişim sağlama durumuna göre farklılaşıp farklılaşmadığına ilişkin yapılan istatistiksel analizler sonucunda siber suç türlerine maruz kalma korkusundan e-posta veya sosyal paylaşım sitelerine ait parolaların çalınması (χ^2=13.569, p=0.010), kimlik hırsızlığına

(kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalma konusunda (χ^2=15.418, p=0.002), bilgisayar korsanlığına (kişisel bilgisayarınıza veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalma (χ^2=10.175, p=0.031), truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalma (χ^2=12.658, p=0.009), keylogger ve screenlogger gibi casus yazılımlara maruz kalma (χ^2=17.774, p=0.000), siber şantaja veya siber tehdide (siber ortamda şantaj veya tehdit davranışlarına) maruz kalma (χ^2=9.715, p=0.035), siber dolandırıcılığa maruz kalma (χ^2=19.764, p=0.000), sniffinge maruz kalma (χ^2=13.370, p=0.005), zombi ordulara maruz kalma (χ^2=19.142, p=0.000), sosyal ağ üzerinden sahtekârlığa maruz kalma (χ^2=22.763, p=0.000), siber yer tespitine maruz kalma (χ^2=12.684, p=0.013) ve siber terörizme maruz kalma (χ^2=14.681, p=0.005) korkularının kamuya açık alanlarda bulunan kablosuz ağlara erişim sağlama durumuna göre anlamlı olarak farklılaştığı bulunmuştur ($p<0.001$, $p<0.01$, $p<0.05$). Buna göre, kablosuz ağlara erişim sağlayanların %44.5'i e-posta veya sosyal paylaşım sitelerine ait parolalarının çalınması konusunda çok ve aşırı düzeyde korku yaşarken, erişim sağlamayanlarda bu oran %15; kablosuz ağlara erişim sağlayanların %55.5'i kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erişim sağlamayanlarda bu oran %37.4; kablosuz ağlara erişim sağlayanların %44.5'i bilgisayar korsanlığına (kişisel bilgisayarınıza veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erişim sağlamayanlarda bu oran %18.7; kablosuz ağlara erişim sağlayanların %44.5'i truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erişim sağlamayanlarda bu oran %15; kablosuz ağlara erişim sağlayanların %55.5'i keylogger ve screenlogger gibi casus yazılımlara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erişim sağlamayanlarda bu oran %18.7; kablosuz ağlara erişim sağlayanların %50'si siber şantaja veya siber tehdide (siber ortamda şantaj veya tehdit davranışlarına) maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erişim sağlamayanlarda bu oran %24.3; kablosuz ağlara erişim sağlayanların %50'si siber dolandırıcılığa maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erişim sağlamayanlarda bu oran %14.9; kablosuz ağlara erişim sağlayanların %50'si sniffinge maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erişim sağlamayanlarda bu oran %20.6; kablosuz ağlara erişim sağlayanların %55.5'i zombi ordulara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erişim

sağlamayanlarda bu oran %18.7; kablosuz ağlara erişim sağlayanların %55.6'sı sosyal ağ üzerinden sahtekârlığa maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erişim sağlamayanlarda bu oran %14.9; kablosuz ağlara erişim sağlayanların %38.9'u siber yer tespitine maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erişim sağlamayanlarda bu oran %13.1 ve kablosuz ağlara erişim sağlayanların %50'si siber terörizme maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, erişim sağlamayanlarda bu oran %22.4'tür. Bu sonuçlar siber suç türlerine maruz kalma açısından korku oranlarının kablosuz ağlara erişim sağlayanlarda daha yüksek olduğunu göstermektedir.

Katılımcıların kullandığı şifrelerin benzerlik durumuna göre siber suç türlerine maruz kalma korkusunun istatistiksel sonuçları çizelge 3.10.'da verilmiştir.

Çizelge 3.10. Katılımcıların Kullandığı Şifrelerin Benzerlik Durumuna Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143)

		Kullanılan Şifrelerin Benzerlik Durumu			
		Benzer (N=60)	**Benzer Değil (N=83)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
1. E-posta veya sosyal paylaşım sitelerine ait parolalarınızın çalınması konusunda	Hiç Korku Duymuyorum	2 (3.3)	22 (26.5)	26.886	**0.000**
	Biraz Korku Duyuyorum	12 (20.0)	29 (34.9)		
	Orta Düzeyde Korku Duyuyorum	28 (46.7)	18 (21.7)		
	Çok Korku Duyuyorum	14 (23.3)	14 (16.9)		
	Aşırı Düzeyde Korku Duyuyorum	4 (6.7)	0 (0.0)		
2. Banka hesap bilgilerinizin (hesap/kart numarası vb.) çalınması yoluyla zarara uğratılmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	6 (7.2)	10.999	**0.022**
	Biraz Korku Duyuyorum	2 (3.3)	10 (12.0)		
	Orta Düzeyde Korku Duyuyorum	24 (40.0)	26 (31.3)		
	Çok Korku Duyuyorum	22 (36.7)	33 (39.8)		
	Aşırı Düzeyde Korku Duyuyorum	12 (20.0)	8 (9.6)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.10. Katılımcıların Kullandığı Şifrelerin Benzerlik Durumuna Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Kullanılan Şifrelerin Benzerlik Durumu			
		Benzer (N=60)	**Benzer Değil (N=83)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
3. Kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	6 (7.2)	20.369	**0.000****
	Biraz Korku Duyuyorum	4 (6.7)	10 (12.0)		
	Orta Düzeyde Korku Duyuyorum	24 (40.0)	39 (47.0)		
	Çok Korku Duyuyorum	22 (36.7)	28 (33.7)		
	Aşırı Düzeyde Korku Duyuyorum	10 (16.7)	0 (0.0)		
4. Bilgisayar korsanlığına (kişisel bilgisayarınıza veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	16 (19.3)	17.700	**0.000**
	Biraz Korku Duyuyorum	12 (20.0)	21 (25.3)		
	Orta Düzeyde Korku Duyuyorum	32 (53.3)	26 (31.3)		
	Çok Korku Duyuyorum	12 (20.0)	18 (21.7)		
	Aşırı Düzeyde Korku Duyuyorum	4 (6.7)	2 (2.4)		
5. Truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	12 (14.5)	23.811	**0.000**
	Biraz Korku Duyuyorum	10 (16.7)	29 (34.9)		
	Orta Düzeyde Korku Duyuyorum	34 (56.7)	26 (31.3)		
	Çok Korku Duyuyorum	12 (20.0)	16 (19.3)		
	Aşırı Düzeyde Korku Duyuyorum	4 (6.7)	0 (0.0)		
6. Keylogger ve screenlogger gibi casus yazılımlara maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	10 (12.0)	21.632	**0.000****
	Biraz Korku Duyuyorum	8 (13.3)	23 (27.7)		
	Orta Düzeyde Korku Duyuyorum	28 (46.7)	34 (41.0)		
	Çok Korku Duyuyorum	18 (30.0)	16 (19.3)		
	Aşırı Düzeyde Korku Duyuyorum	6 (10.0)	0 (0.0)		
7. Siber zorbalığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	10 (12.0)	14.643	**0.004****
	Biraz Korku Duyuyorum	8 (13.3)	16 (19.3)		
	Orta Düzeyde Korku Duyuyorum	30 (50.0)	35 (42.2)		
	Çok Korku Duyuyorum	18 (30.0)	22 (26.5)		
	Aşırı Düzeyde Korku Duyuyorum	4 (6.7)	0 (0.0)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.10. Katılımcıların Kullandığı Şifrelerin Benzerlik Durumuna Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Kullanılan Şifrelerin Benzerlik Durumu			
		Benzer (N=60)	**Benzer Değil (N=83)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
9. Siber şantaja veya siber tehdide (siber ortamda şantaj veya tehdit davranışlarına) maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (3.3)	10 (12.0)	13.886	**0.006**
	Biraz Korku Duyuyorum	10 (16.7)	23 (27.7)		
	Orta Düzeyde Korku Duyuyorum	24 (40.0)	30 (36.1)		
	Çok Korku Duyuyorum	18 (30.0)	20 (24.1)		
	Aşırı Düzeyde Korku Duyuyorum	6 (10.0)	0 (0.0)		
10. Siber hırsızlığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	10 (12.0)	22.072	**0.000****
	Biraz Korku Duyuyorum	8 (13.3)	20 (24.1)		
	Orta Düzeyde Korku Duyuyorum	28 (46.7)	33 (39.8)		
	Çok Korku Duyuyorum	16 (26.7)	20 (24.1)		
	Aşırı Düzeyde Korku Duyuyorum	8 (13.3)	0 (0.0)		
11. Siber ortamda haberleşme gizliliğinizin ihlali (kayıt altına alınması ya da ifşası gibi) konusunda	Hiç Korku Duymuyorum	0 (0.0)	10 (12.0)	16.753	**0.000****
	Biraz Korku Duyuyorum	10 (16.7)	23 (27.7)		
	Orta Düzeyde Korku Duyuyorum	28 (46.7)	28 (33.7)		
	Çok Korku Duyuyorum	18 (30.0)	22 (26.5)		
	Aşırı Düzeyde Korku Duyuyorum	4 (6.7)	0 (0.0)		
12. Siber dolandırıcılığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	8 (9.6)	21.283	**0.000****
	Biraz Korku Duyuyorum	10 (16.7)	30 (36.1)		
	Orta Düzeyde Korku Duyuyorum	30 (50.0)	31 (37.3)		
	Çok Korku Duyuyorum	14 (23.3)	14 (16.9)		
	Aşırı Düzeyde Korku Duyuyorum	6 (10.0)	0 (0.0)		
13. Sniffinge maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	6 (7.2)	17.381	**0.000****
	Biraz Korku Duyuyorum	6 (10.0)	20 (24.1)		
	Orta Düzeyde Korku Duyuyorum	34 (56.7)	37 (44.6)		
	Çok Korku Duyuyorum	14 (23.3)	20 (24.1)		
	Aşırı Düzeyde Korku Duyuyorum	6 (10.0)	0 (0.0)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.10. Katılımcıların Kullandığı Şifrelerin Benzerlik Durumuna Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Kullanılan Şifrelerin Benzerlik Durumu			
		Benzer (N=60)	**Benzer Değil (N=83)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
14. Zombi ordulara maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	6 (7.2)	18.159	**0.000****
	Biraz Korku Duyuyorum	10 (16.7)	28 (33.7)		
	Orta Düzeyde Korku Duyuyorum	26 (43.3)	33 (39.8)		
	Çok Korku Duyuyorum	18 (30.0)	16 (19.3)		
	Aşırı Düzeyde Korku Duyuyorum	6 (10.0)	0 (0.0)		
15. Sosyal ağ üzerinden sahtekârlığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	0 (0.0)	18 (21.7)	20.965	**0.000**
	Biraz Korku Duyuyorum	6 (10.0)	17 (20.5)		
	Orta Düzeyde Korku Duyuyorum	34 (56.7)	32 (38.6)		
	Çok Korku Duyuyorum	16 (26.7)	14 (16.9)		
	Aşırı Düzeyde Korku Duyuyorum	4 (6.7)	2 (2.4)		
16. Siber yer tespitine maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (3.3)	18 (21.7)	23.099	**0.000**
	Biraz Korku Duyuyorum	10 (16.7)	23 (27.7)		
	Orta Düzeyde Korku Duyuyorum	36 (60.0)	26 (31.3)		
	Çok Korku Duyuyorum	8 (13.3)	16 (19.3)		
	Aşırı Düzeyde Korku Duyuyorum	4 (6.7)	0 (0.0)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Siber suç türlerine maruz kalma korkusunun kullandığı şifrelerin benzerlik durumuna göre farklılaşıp farklılaşmadığına ilişkin yapılan istatistiksel analizler sonucunda siber suç türlerine maruz kalma korkusundan siber tacize (siber ortamda taciz davranışlarına) maruz kalma konusunda (χ^2=8.873, p=0.061), bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalma konusunda (χ^2=8.918, p=0.058) ve siber terörizme maruz kalma korkusu (χ^2=8.925, p=0.061) haricinde diğer siber suç türlerinin, kullandığı şifrelerin benzerlik durumuna göre anlamlı olarak farklılaştığı bulunmuştur (p<0.001, p<0.01, p<0.05). Buna göre şifreleri benzer olanların %76.7'si e-posta veya sosyal paylaşım sitelerine ait parolalarının çalınması konusunda orta, çok ve aşırı düzeyde korku yaşarken, şifreleri benzer olmayanlarda bu oran %38.6; şifreleri benzer olanların %96.7'si banka hesap bilgilerinin (hesap/kart numarası vb.) çalınması yoluyla zarara uğratılma konusunda orta,

çok ve aşırı düzeyde korku yaşarken, şifreleri benzer olmayanlarda bu oran %80.7; şifreleri benzer olanların %53.4'ü kimlik hırsızlığına maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, şifreleri benzer olmayanlarda bu oran %33.7; şifreleri benzer olanların %80'i bilgisayar korsanlığına (kişisel bilgisayarınıza veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, şifreleri benzer olmayanlarda bu oran %55.4; şifreleri benzer olanların %83.4'ü truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, şifreleri benzer olmayanlarda bu oran %50.6; şifreleri benzer olanların %40'ı keylogger ve screenlogger gibi casus yazılımlara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, şifreleri benzer olmayanlarda bu oran %19.3; şifreleri benzer olanların %86.7'si siber zorbalığa maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, şifreleri benzer olmayanlarda bu oran %68.7; şifreleri benzer olanların %40'ı siber şantaja veya siber tehdide (siber ortamda şantaj veya tehdit davranışlarına) maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, şifreleri benzer olmayanlarda bu oran %24.1; şifreleri benzer olanların %40'ı siber hırsızlığa maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, şifreleri benzer olmayanlarda bu oran %24.1; şifreleri benzer olanların %83.4'ü siber ortamda haberleşme gizliliğinizin ihlali (kayıt altına alınması ya da ifşası gibi) konusunda orta, çok ve aşırı düzeyde korku yaşarken, şifreleri benzer olmayanlarda bu oran %60.2; şifreleri benzer olanların %83.3'ü siber dolandırıcılığa maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, şifreleri benzer olmayanlarda bu oran %54.2; şifreleri benzer olanların %90'ı sniffinge maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, şifreleri benzer olmayanlarda bu oran %68.7; şifreleri benzer olanların %83.3'ü zombi ordulara maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, şifreleri benzer olmayanlarda bu oran %59.1; şifreleri benzer olanların %90'ı sosyal ağ üzerinden sahtekârlığa maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, şifreleri benzer olmayanlarda bu oran %57.9 ve şifreleri benzer olanların %80'i siber yer tespitine maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, şifreleri benzer olmayanlarda bu oran %50.6'dır. Bu sonuçlar, siber suç türlerine maruz kalma açısından korku oranlarının şifreleri benzer olanlarda daha yüksek olduğunu göstermektedir.

Katılımcıların sosyal medya hesaplarını başka sitelere erişim için kullanma durumuna göre siber suç türlerine maruz kalma korkusunun istatistiksel sonuçları çizelge 3.11.'de verilmiştir.

Çizelge 3.11. Katılımcıların Sosyal Medya Hesaplarını Başka Sitelere Erişim için Kullanma Durumuna Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143)

		Sosyal Medya Hesaplarını Başka Sitelere Erişim için Kullanma Durumu			
		Evet (N=78)	**Hayır (N=65)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
3. Kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalmanız konusunda	Hiç Korku Duymuyorum	4 (5.1)	2 (3.1)	13.792	**0.004****
	Biraz Korku Duyuyorum	12 (15.4)	2 (3.1)		
	Orta Düzeyde Korku Duyuyorum	38 (48.7)	25 (38.5)		
	Çok Korku Duyuyorum	18 (23.1)	32 (49.2)		
	Aşırı Düzeyde Korku Duyuyorum	6 (7.7)	4 (6.2)		
6. Keylogger ve screenlogger gibi casus yazılımlara maruz kalmanız konusunda	Hiç Korku Duymuyorum	6 (7.7)	4 (6.2)	13.599	**0.006****
	Biraz Korku Duyuyorum	12 (15.4)	19 (29.2)		
	Orta Düzeyde Korku Duyuyorum	44 (56.4)	18 (27.7)		
	Çok Korku Duyuyorum	14 (17.9)	20 (30.8)		
	Aşırı Düzeyde Korku Duyuyorum	2 (2.6)	4 (6.2)		
7. Siber zorbalığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	10 (12.8)	0 (0.0)	14.439	**0.003****
	Biraz Korku Duyuyorum	16 (20.5)	8 (12.3)		
	Orta Düzeyde Korku Duyuyorum	34 (43.6)	31 (47.7)		
	Çok Korku Duyuyorum	16 (20.5)	24 (36.9)		
	Aşırı Düzeyde Korku Duyuyorum	2 (2.6)	2 (3.1)		
10. Siber hırsızlığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	10 (12.8)	0 (0.0)	14.711	**0.004****
	Biraz Korku Duyuyorum	18 (23.1)	10 (15.4)		
	Orta Düzeyde Korku Duyuyorum	32 (41.0)	29 (44.6)		
	Çok Korku Duyuyorum	16 (20.5)	20 (30.8)		
	Aşırı Düzeyde Korku Duyuyorum	2 (2.6)	6 (9.2)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.11. Katılımcıların Sosyal Medya Hesaplarını Başka Sitelere Erişim için Kullanma Durumuna Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Sosyal Medya Hesaplarını Başka Sitelere Erişim için Kullanma Durumu			
		Evet (N=78)	**Hayır (N=65)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
13. Sniffinge maruz kalmanız konusunda	Hiç Korku Duymuyorum	4 (5.1)	2 (3.1)	14.349	**0.004****
	Biraz Korku Duyuyorum	22 (28.2)	4 (6.2)		
	Orta Düzeyde Korku Duyuyorum	36 (46.2)	35 (53.8)		
	Çok Korku Duyuyorum	14 (17.9)	20 (30.8)		
	Aşırı Düzeyde Korku Duyuyorum	2 (2.6)	4 (6.2)		
14. Zombi ordulara maruz kalmanız konusunda	Hiç Korku Duymuyorum	6 (7.7)	0 (0.0)	20.932	**0.000****
	Biraz Korku Duyuyorum	30 (38.5)	8 (12.3)		
	Orta Düzeyde Korku Duyuyorum	24 (30.8)	35 (53.8)		
	Çok Korku Duyuyorum	16 (20.5)	18 (27.7)		
	Aşırı Düzeyde Korku Duyuyorum	2 (2.6)	4 (6.2)		
15. Sosyal ağ üzerinden sahtekârlığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	16 (20.5)	2 (3.1)	18.216	**0.000**
	Biraz Korku Duyuyorum	16 (20.5)	7 (10.8)		
	Orta Düzeyde Korku Duyuyorum	26 (33.3)	40 (61.5)		
	Çok Korku Duyuyorum	18 (23.1)	12 (18.5)		
	Aşırı Düzeyde Korku Duyuyorum	2 (2.6)	4 (6.2)		
17. Bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalmanız konusunda	Hiç Korku Duymuyorum	14 (17.9)	6 (9.2)	19.237	**0.000**
	Biraz Korku Duyuyorum	26 (33.3)	6 (9.2)		
	Orta Düzeyde Korku Duyuyorum	18 (23.1)	31 (47.7)		
	Çok Korku Duyuyorum	16 (20.5)	20 (30.8)		
	Aşırı Düzeyde Korku Duyuyorum	4 (5.1)	2 (3.1)		
18. Siber terörizme maruz kalmanız konusunda	Hiç Korku Duymuyorum	14 (17.9)	2 (3.1)	13.994	**0.005**
	Biraz Korku Duyuyorum	18 (23.1)	7 (10.8)		
	Orta Düzeyde Korku Duyuyorum	26 (33.3)	34 (52.3)		
	Çok Korku Duyuyorum	12 (15.4)	14 (21.5)		
	Aşırı Düzeyde Korku Duyuyorum	8 (10.3)	8 (12.3)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Siber suç türlerine maruz kalma korkusunun sosyal medya hesaplarını başka sitelere erişim için kullanma durumuna göre farklılaşıp farklılaşmadığına ilişkin yapılan istatistiksel analizler sonucunda siber suç türlerine maruz kalma korkusundan kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalma (χ^2=13.792, p=0.004), keylogger ve screenlogger gibi casus yazılımlara maruz kalma (χ^2=13.599, p=0.006), siber zorbalığa maruz kalma (χ^2=14.439, p=0.004), siber hırsızlığa maruz kalma (χ^2=14.711, p=0.004), sniffinge maruz kalma (χ^2=14.349, p=0.004), zombi ordulara maruz kalma (χ^2=20.932, p=0.000), sosyal ağ üzerinden sahtekârlığa maruz kalma (χ^2=18.216, p=0.000), bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalma (χ^2=19.237, p=0.000) ve siber terörizme maruz kalma (χ^2=13.994, p=0.005) korkularının sosyal medya hesaplarını başka sitelere erişim için kullanma durumuna göre anlamlı olarak farklılaştığı bulunmuştur ($p<0.001$, $p<0.01$). Buna göre, sosyal medya hesaplarını başka sitelere erişim için kullanmayanların %55.4'ü kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kullananlarda bu oran %30.8; sosyal medya hesaplarını başka sitelere erişim için kullanmayanların %37'si keylogger ve screenlogger gibi casus yazılımlara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kullananlarda bu oran %20.5; sosyal medya hesaplarını başka sitelere erişim için kullanmayanların %40'ı siber zorbalığa maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kullananlarda bu oran %23.1; sosyal medya hesaplarını başka sitelere erişim için kullanmayanların %40'ı siber hırsızlığa maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kullananlarda bu oran %23.1; sosyal medya hesaplarını başka sitelere erişim için kullanmayanların %37'si sniffinge maruz kalmanız konusunda çok ve aşırı düzeyde korku yaşarken, kullananlarda bu oran %20.5; sosyal medya hesaplarını başka sitelere erişim için kullanmayanların %87.7'si zombi ordulara maruz kalmanız konusunda orta, çok ve aşırı düzeyde korku yaşarken, kullananlarda bu oran %53.9; sosyal medya hesaplarını başka sitelere erişim için kullanmayanların %86.2'si sosyal ağ üzerinden sahtekârlığa maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, kullananlarda bu oran %59; sosyal medya hesaplarını başka sitelere erişim için kullanmayanların %81.6'sı bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalmanız konusunda orta, çok ve aşırı düzeyde korku yaşarken, kullananlarda bu oran %48.7 ve sosyal medya hesaplarını başka sitelere erişim için kullanmayanların %86.1'i siber terörizme maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, kullananlarda

bu oran %59'dur. Bu sonuçlar, siber suç türlerine maruz kalma açısından korku oranlarının sosyal medya hesaplarını başka sitelere erişim için kullanmayanlarda daha yüksek olduğunu göstermektedir.

Katılımcıların antivirüs programı kullanma durumuna göre siber suç türlerine maruz kalma korkusunun istatistiksel sonuçları çizelge 3.12.'de verilmiştir.

Çizelge 3.12. Katılımcıların Antivirüs Programı Kullanma Durumuna Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143)

		Antivirüs Programı Kullanma			
		Evet (N=71)	**Hayır (N=72)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
1. E-posta veya sosyal paylaşım sitelerine ait parolalarınızın çalınması konusunda	Hiç Korku Duymuyorum	14 (19.7)	10 (13.9)	15.639	**0.003**
	Biraz Korku Duyuyorum	11 (15.5)	30 (41.7)		
	Orta Düzeyde Korku Duyuyorum	28 (39.4)	18 (25.0)		
	Çok Korku Duyuyorum	14 (19.7)	14 (19.4)		
	Aşırı Düzeyde Korku Duyuyorum	4 (5.6)	0 (0.0)		
2. Banka hesap bilgilerinizin (hesap/kart numarası vb.) çalınması yoluyla zarara uğratılmanız konusunda	Hiç Korku Duymuyorum	4 (5.6)	2 (2.8)	10.053	**0.034**
	Biraz Korku Duyuyorum	6 (8.5)	6 (8.3)		
	Orta Düzeyde Korku Duyuyorum	22 (31.0)	28 (38.9)		
	Çok Korku Duyuyorum	23 (32.4)	32 (44.4)		
	Aşırı Düzeyde Korku Duyuyorum	16 (22.5)	4 (5.6)		
3. Kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalmanız konusunda	Hiç Korku Duymuyorum	4 (5.6)	2 (2.8)	11.007	**0.023****
	Biraz Korku Duyuyorum	6 (8.5)	8 (11.1)		
	Orta Düzeyde Korku Duyuyorum	23 (32.4)	40 (55.6)		
	Çok Korku Duyuyorum	30 (42.3)	20 (27.8)		
	Aşırı Düzeyde Korku Duyuyorum	8 (11.3)	2 (2.8)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.12. Katılımcıların Antivirüs Programı Kullanma Durumuna Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Antivirüs Programı Kullanma			
		Evet (N=71)	**Hayır (N=72)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
4. Bilgisayar korsanlığına (kişisel bilgisayarınıza veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalmanız konusunda	Hiç Korku Duymuyorum	12 (16.9)	4 (5.6)	16.058	**0.003**
	Biraz Korku Duyuyorum	13 (18.3)	20 (27.8)		
	Orta Düzeyde Korku Duyuyorum	22 (31.0)	36 (50.0)		
	Çok Korku Duyuyorum	18 (25.4)	12 (16.7)		
	Aşırı Düzeyde Korku Duyuyorum	6 (8.5)	0 (0.0)		
5. Truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalmanız konusunda	Hiç Korku Duymuyorum	8 (11.3)	4 (5.6)	15.023	**0.003**
	Biraz Korku Duyuyorum	11 (15.5)	28 (38.9)		
	Orta Düzeyde Korku Duyuyorum	30 (42.3)	30 (41.7)		
	Çok Korku Duyuyorum	18 (25.4)	10 (13.9)		
	Aşırı Düzeyde Korku Duyuyorum	4 (5.6)	0 (0.0)		
7. Siber zorbalığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	8 (11.3)	2 (2.8)	18.639	**0.000****
	Biraz Korku Duyuyorum	6 (8.5)	18 (25.0)		
	Orta Düzeyde Korku Duyuyorum	27 (38.0)	38 (52.8)		
	Çok Korku Duyuyorum	26 (36.6)	14 (19.4)		
	Aşırı Düzeyde Korku Duyuyorum	4 (5.6)	0 (0.0)		
8. Siber tacize (siber ortamda taciz davranışlarına) maruz kalmanız konusunda	Hiç Korku Duymuyorum	10 (14.1)	6 (8.3)	16.887	**0.001**
	Biraz Korku Duyuyorum	5 (7.0)	18 (25.0)		
	Orta Düzeyde Korku Duyuyorum	30 (42.3)	36 (50.0)		
	Çok Korku Duyuyorum	20 (28.2)	12 (16.7)		
	Aşırı Düzeyde Korku Duyuyorum	6 (8.5)	0 (0.0)		
9. Siber şantaja veya siber tehdide (siber ortamda şantaj veya tehdit davranışlarına) maruz kalmanız konusunda	Hiç Korku Duymuyorum	6 (8.5)	6 (8.3)	10.151	**0.034**
	Biraz Korku Duyuyorum	11 (15.5)	22 (30.6)		
	Orta Düzeyde Korku Duyuyorum	24 (33.8)	30 (41.7)		
	Çok Korku Duyuyorum	26 (36.6)	12 (16.7)		
	Aşırı Düzeyde Korku Duyuyorum	4 (5.6)	2 (2.8)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.12. Katılımcıların Antivirüs Programı Kullanma Durumuna Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Antivirüs Programı Kullanma			
		Evet (N=71)	**Hayır (N=72)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
10. Siber hırsızlığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	6 (8.5)	4 (5.6)	19.647	**0.000****
	Biraz Korku Duyuyorum	4 (5.6)	24 (33.3)		
	Orta Düzeyde Korku Duyuyorum	33 (46.5)	28 (38.9)		
	Çok Korku Duyuyorum	22 (31.0)	14 (19.4)		
	Aşırı Düzeyde Korku Duyuyorum	6 (8.5)	2 (2.8)		
11. Siber ortamda haberleşme gizliliğinizin ihlali (kayıt altına alınması ya da ifşası gibi) konusunda	Hiç Korku Duymuyorum	8 (11.3)	2 (2.8)	20.049	**0.000****
	Biraz Korku Duyuyorum	7 (9.9)	26 (36.1)		
	Orta Düzeyde Korku Duyuyorum	28 (39.4)	28 (38.9)		
	Çok Korku Duyuyorum	24 (33.8)	16 (22.2)		
	Aşırı Düzeyde Korku Duyuyorum	4 (5.6)	0 (0.0)		
12. Siber dolandırıcılığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	6 (8.5)	2 (2.8)	14.813	**0.005****
	Biraz Korku Duyuyorum	12 (16.9)	28 (38.9)		
	Orta Düzeyde Korku Duyuyorum	33 (46.5)	28 (38.9)		
	Çok Korku Duyuyorum	14 (19.7)	14 (19.4)		
	Aşırı Düzeyde Korku Duyuyorum	6 (8.5)	0 (0.0)		
13. Sniffinge maruz kalmanız konusunda	Hiç Korku Duymuyorum	4 (5.6)	2 (2.8)	20.209	**0.000****
	Biraz Korku Duyuyorum	4 (5.6)	22 (30.6)		
	Orta Düzeyde Korku Duyuyorum	35 (49.3)	36 (50.0)		
	Çok Korku Duyuyorum	24 (33.8)	10 (13.9)		
	Aşırı Düzeyde Korku Duyuyorum	4 (5.6)	2 (2.8)		
14. Zombi ordulara maruz kalmanız konusunda	Hiç Korku Duymuyorum	2 (2.8)	4 (5.6)	12.256	**0.011****
	Biraz Korku Duyuyorum	12 (16.9)	26 (36.1)		
	Orta Düzeyde Korku Duyuyorum	29 (40.8)	30 (41.7)		
	Çok Korku Duyuyorum	24 (33.8)	10 (13.9)		
	Aşırı Düzeyde Korku Duyuyorum	4 (5.6)	2 (2.8)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Çizelge 3.12. Katılımcıların Antivirüs Programı Kullanma Durumuna Göre Siber Suç Türlerine Maruz Kalma Korkusunun İstatistiksel Sonuçları (N=143) Devamı

		Antivirüs Programı Kullanma			
		Evet (N=71)	**Hayır (N=72)**	**İstatistiksel Analiz**	
İfadeler	**Yanıtlar**	**N (%)[a]**	**N (%)[a]**	**χ^2**	**p***
15. Sosyal ağ üzerinden sahtekârlığa maruz kalmanız konusunda	Hiç Korku Duymuyorum	12 (16.9)	6 (8.3)	11.709	**0.017**
	Biraz Korku Duyuyorum	7 (9.9)	16 (22.2)		
	Orta Düzeyde Korku Duyuyorum	32 (45.1)	34 (47.2)		
	Çok Korku Duyuyorum	14 (19.7)	16 (22.2)		
	Aşırı Düzeyde Korku Duyuyorum	6 (8.5)	0 (0.0)		
16. Siber yer tespitine maruz kalmanız konusunda	Hiç Korku Duymuyorum	12 (16.9)	8 (11.1)	16.073	**0.002**
	Biraz Korku Duyuyorum	11 (15.5)	22 (30.6)		
	Orta Düzeyde Korku Duyuyorum	26 (36.6)	36 (50.0)		
	Çok Korku Duyuyorum	18 (25.4)	6 (8.3)		
	Aşırı Düzeyde Korku Duyuyorum	4 (5.6)	0 (0.0)		
17. Bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalmanız konusunda	Hiç Korku Duymuyorum	8 (11.3)	12 (16.7)	13.794	**0.007**
	Biraz Korku Duyuyorum	12 (16.9)	20 (27.8)		
	Orta Düzeyde Korku Duyuyorum	21 (29.6)	28 (38.9)		
	Çok Korku Duyuyorum	24 (33.8)	12 (16.7)		
	Aşırı Düzeyde Korku Duyuyorum	6 (8.5)	0 (0.0)		
18. Siber terörizme maruz kalmanız konusunda	Hiç Korku Duymuyorum	8 (11.3)	8 (11.1)	14.378	**0.006**
	Biraz Korku Duyuyorum	5 (7.0)	20 (27.8)		
	Orta Düzeyde Korku Duyuyorum	30 (42.3)	30 (41.7)		
	Çok Korku Duyuyorum	16 (22.5)	10 (13.9)		
	Aşırı Düzeyde Korku Duyuyorum	12 (16.9)	4 (5.6)		

*Ki-kare testi, **Fisher Freeman Halton testi, [a]Sütun yüzdesi

Siber suç türlerine maruz kalma korkusunun antivirüs programı kullanma durumuna göre farklılaşıp farklılaşmadığına ilişkin yapılan istatistiksel analizler sonucunda siber suç türlerine maruz kalma korkusundan keylogger ve screenlogger gibi casus yazılımlara maruz kalma korkusu (χ^2=7.135, p=0.121) haricinde diğer siber suç türlerinin, antivirüs programı kullanma durumuna göre anlamlı olarak farklılaştığı bulunmuştur (p<0.001, p<0.01, p<0.05). Buna göre antivirüs programı kullananların %64.7'si e-posta veya sosyal paylaşım

sitelerine ait parolalarının çalınması konusunda orta, çok ve aşırı düzeyde korku yaşarken, kullanmayanlarda bu oran %44.4; antivirüs programı kullananların %54.9'u banka hesap bilgilerinin (hesap/kart numarası vb.) çalınması yoluyla zarara uğratılma konusunda çok ve aşırı düzeyde korku yaşarken, kullanmayanlarda bu oran %50; antivirüs programı kullananların %53.6'sı kimlik hırsızlığına (kişisel verilerinizin izniniz dışında hukuka aykırı şekilde üçüncü kişilere verilmesi, dağıtılması veya bu verilerinizin üçüncü kişilerce ele geçirilmesi) maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kullanmayanlarda bu oran %30.6; antivirüs programı kullananların %33.9'u bilgisayar korsanlığına (kişisel bilgisayarınıza veya kurumsal bilgisayarınıza izinsiz giriş yapılması) maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kullanmayanlarda bu oran %16.7; antivirüs programı kullananların %31'i truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kullanmayanlarda bu oran %13.9; antivirüs programı kullananların %36.6'sı keylogger ve screenlogger gibi casus yazılımlara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kullanmayanlarda bu oran %19.5; antivirüs programı kullananların %42.2'si siber zorbalığa maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kullanmayanlarda bu oran %19.4; antivirüs programı kullananların %36.7'si siber tacize (siber ortamda taciz davranışlarına) maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kullanmayanlarda bu oran %16.7; antivirüs programı kullananların %42.2'si siber şantaja veya siber tehdide (siber ortamda şantaj veya tehdit davranışlarına) maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kullanmayanlarda bu oran %19.5; antivirüs programı kullananların %39.5'i siber hırsızlığa maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kullanmayanlarda bu oran %22.2; antivirüs programı kullananların %39.4'ü siber ortamda haberleşme gizliliğinin ihlali (kayıt altına alınması ya da ifşası gibi) konusunda çok ve aşırı düzeyde korku yaşarken, kullanmayanlarda bu oran %22.2; antivirüs programı kullananların %74.7'si siber dolandırıcılığa maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, kullanmayanlarda bu oran %58.3; antivirüs programı kullananların %39.4'ü sniffinge maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kullanmayanlarda bu oran %16.7; antivirüs programı kullananların %39.4'ü zombi ordulara maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kullanmayanlarda bu oran %16.7; antivirüs programı kullananların %73.3'ü sosyal ağ üzerinden sahtekârlığa maruz kalma konusunda orta, çok ve aşırı düzeyde korku yaşarken, kullanmayanlarda bu oran %69.4; antivirüs programı kullananların %31'i siber yer tespitine maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kullanmayanlarda bu oran %8.3; antivirüs programı

kullananların %42.3'ü bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kullanmayanlarda bu oran %16.7 ve antivirüs programı kullananların %39.4'ü siber terörizme maruz kalma konusunda çok ve aşırı düzeyde korku yaşarken, kullanmayanlarda bu oran %19.5'tir. Bu sonuçlar, siber suç türlerine maruz kalma açısından korku oranlarının antivirüs programı kullananlarda daha yüksek olduğunu göstermektedir.

Günlük internet kullanım süresi, internet ortamında kullanılan şifreleri değiştirme sıklığı, siber suçları önlemeye yönelik mevcut yasal mevzuatı/yazılı düzenlemelerin yeterliliğine yönelik algı durumu ve siber suçların mağduru olmamak için alınan bireysel önlemlerin yeterliliği değişkenlerinin kategori sayısının fazla ve bazı kategorilerdeki frekansların oldukça düşük olması; internet kullanıcısı olma süresi, sosyal medya kullanıcısı olma durumu, finansal işlemleri internetten yapma durumu, geçmişte siber suç mağduriyeti yaşama durumu, sanal ortamdaki hesaplara erişirken iki faktörlü koruma sistemini kullanma durumu, telefona erişmek için herhangi bir kod, şifre veya başka bir güvenlik tedbiri kullanma durumu, telefonda bulunan uygulamaları güncelleme durumu ve cihazların işletim sistemini güncelleme durumu değişkenlerinin kategori sayısı iki olup belirtilen bu değişkenlere ait kategorilerden birisinin frekansının oldukça düşük olması ve şifreleri başkaları ile paylaşma durumu değişkeninin ise tek kategoriden oluşmasından dolayı belirtilen değişkenlere yönelik istatistiksel analizler yapılmamıştır.

DÖRDÜNCÜ BÖLÜM

TARTIŞMA

4.1. Giriş

İnternet ve internet tabanlı teknolojilerin gündelik yaşantımıza dâhil olmasının beraberinde getirdiği dijitalleşme, dünya üzerinde yaşanan birçok değişim ve dönüşümle birlikte kültür, eğitim ve suç gibi olguların yanı sıra günlük rutin aktivitelerinde de değişimine sebep olmuştur. Bu durum, dijitalleşen suç olgusunu da beraberinde getirerek siber suçların ve siber suç mağdurlarının ortaya çıkmasına neden olmuştur. Siber suçlar, kendilerini sürekli olarak yenileyen ve teknolojik gelişmelere uyum sağlayabilen bir nitelikte olduğundan siber suça karşı alınan önlemler, yeni bir siber suç yöntemi geliştirilene kadar geçerliliğini koruyabilmektedir (Uludağ ve Fidan, 2023). Konuyla ilgili çalışmalar, siber ortamdaki suç olgusunun varlığını göstermekle birlikte, siber dünyada suçların gerçek dünyada işlendiğinden daha kolay bir şekilde işlenebildiğini göstermektedir. Suç korkusu, işlenen suçların bir sonucu ve suçlarla mücadeleyi güçleştiren bir faktör olarak ortaya çıkmaktadır. Ancak suçla mücadelede önceliklerden birisi, suç korkusunu azaltabilmek olmalıdır. Buradan hareketle, öncelikle suç korkusu düzeyinin ve suç korkusuyla ilişkili değişkenlerin belirlenmesi önem taşımaktadır (Yurtsal, 2016).

Trabzon ilindeki Teknokent çalışanlarında siber suç türlerine maruz kalma korkusunun çeşitli sosyodemografik değişkenlerine göre farklılaşıp farklılaşmadığını incelemeyi hedefleyen bu çalışmada, araştırmaya katılımcı olmayı kabul eden 143 gönüllüden anket yöntemiyle veri toplanmış ve toplanan veriler uygun paket programa girilerek analiz edilmiştir.

4.2. Katılımcıların Siber Suç Mağduriyetine Yönelik Önlem Alma Stratejilerine İlişkin Bulguların Tartışılması

Yapılan analizler, katılımcıların büyük bir kısmının (%88,8) 10 yıl ve daha uzun süredir internet kullanıcısı olduğunu ve önemli bir oranının (%48,5) internete mobil cihazından eriştiğini göstermektedir. Bu bulgu, ilgili yazında belirtildiği üzere (Cengiz, 2019; Yılmaz, 2018) gün geçtikçe teknolojinin hayatımızla iç içe olduğu görüşüyle tutarlı görünmektedir. Katılımcıların %44'ü günde 2-3 saat arasında, %29,3 gibi azımsanmayacak bir oranı ise günde 8 saat ve üzeri süre internette vakit geçirmektedir. Katılımcıların internette geçirdiği vaktin uzunluğu, örneklemin teknokent çalışanları olmasıyla da

açıklanabilmektedir. Katılımcıların düşük bir oranının (%8,3) geçmişte siber suç mağduru olduğu, önemli çoğunluğunun (%37,7) siber suçların önlenmesine yönelik mevzuat veya düzenlemeleri yetersiz olarak algıladığı belirlenmiştir. Katılımcıların neredeyse tamamının (%94,4) sosyal medya kullanıcısı olması dikkat çekici olmuştur. Yine katılımcıların tamamına yakınının (%95,8) finansal işlemlerini internet üzerinden gerçekleştirdiği görülmektedir. Bu çalışmanın katılımcılarının büyük bir oranının hem sosyal medya kullanıcısı olduğu hem de finansal işlemlerini internet üzerinden gerçekleştirdiği dikkate alındığında, kişisel ve maddi bilgilerinin başkaca platformlara sızmaması adına önlem alma stratejilerini iyi düzeyde kullanıyor olmaları beklenmektedir. Örneğin, internet ortamında kullanılan şifrelerin sık aralıklarla ve mecbur kalınmadıkça değiştirilmesi, siber suç mağduru olmaya karşı iyi bir önlem alma stratejisi olarak düşünülebilir. Ancak bu çalışmanın katılımcılarının internet ortamında kullandığı hesaplarının şifrelerini değiştirme sıklığına bakıldığında %29,3'ünün 3 ayda 1 kez, %25,8'inin ise mecbur kalmadığı sürece değiştirmediği göze çarpmaktadır. Yine katılımcıların %41,9'unun siber suçların mağduru olmamak için almış olduğu bireysel önlemleri orta düzeyde yeterli bulduğu, %20,9'unun yetersiz bulduğu, %5,5'inin ise çok yeterli bulduğu görülmektedir. Yoğun düzeyde internet ve internet kaynaklı teknolojilerin kullanımına karşın bazı katılımcıların önlem alma stratejilerinden yeteri kadar istifade edemedikleri, yine de bu konuda farkındalığa sahip oldukları söylenebilir. Bu çalışma katılımcılarının siber suçların mağduru olmamaları için internet teknolojilerini daha bilinçli kullanabilmeleri adına hizmet içi eğitimlerle desteklenmelerinde yarar olacağı düşünülmektedir.

Bilindiği üzere kamuya açık alanlarda (restoran, otel, havaalanı, alışveriş merkezi gibi) bulunan kablosuz ağlara erişim, birçok yerde halka açık veya şifresiz şekilde sağlanabilmektedir. Ancak kolaylıkla erişim sağlanabilen bu ağların, büyük bir güvenlik riski oluşturduğu kaçınılmaz bir gerçektir. Genellikle şifresiz kullanılan veya şifre gerektirmeden bağlantı kurulabilen bu ağlar, güvensiz kablosuz ağlar kapsamındadır. Siber saldırganlar bu ağlara erişim sağlayarak, ağ üzerindeki iletişimi takip edebilir, sahte sitelere yönlendirebilir veya kredi kartı gibi şahsi bilgileri kolaylıkla ele geçirebilmektedirler. Dolayısıyla kablosuz ağlarda güvenliğin sağlanması, siber güvenlik kapsamında oldukça önemlidir. Katılımcıların büyük bir oranının (%74,8) kamuya açık alanlarda kablosuz ağlardan internete erişim sağlamadığı görülmektedir. Bu bulgu, katılımcıların kamuya açık ağlarda daha fazla siber mağdur olabileceklerinin farkında olduğuna işaret etmektedir.

İnternet ortamında şifrelerin benzer veya aynı kullanılması, internet kullanıcısının rutin bir faaliyeti olarak kabul edilebilir. Bu davranış kullanıcıyı siber suçun hedefi haline getirmekte ve de Rutin Aktiviteler Teorisi bağlamında motive olmuş bir suçlu, sanal ortamda müsait ve erişilebilir olan bu kullanıcıları hedef olarak belirleyebilmektedir (Cohen ve Felson, 1979; Felson ve Eckert, 2018; John ve Tierney, 2009). İnternet kullanıcısının benzer veya aynı şifreleri kullanıyor olması, bir sitedeki hesabının ele geçirilmesi sonucunda diğer bütün sitelerdeki hesaplarını da risk altına almaktadır. Katılımcıların %58'inin internet ortamında kullandığı şifrelerin birbirine benzer olmadığı ancak azımsanmayacak bir oranının (%41,96) farklı uygulama ya da platformlarda benzer şifre kullandığı göze çarpmaktadır. Ayrıca katılımcıların %54,5 gibi önemli bir oranının sosyal medya hesaplarını başka sitelere erişimde kullandığı göze çarpmaktadır. Bu sonuçlara göre katılımcıların yarıdan fazlasının benzer şifrelerin kullanılmaması konusunda farkındalıkların iyi bir seviyede olduğu söylenebilir. İlaveten katılımcıların tamamının, kullandığı şifreleri başkalarıyla paylaşmadığını belirttiği görülmektedir. Bu bulgu, katılımcıların siber suç türlerinin bazılarına hedef olmaktan korunabileceklerini düşündürmektedir. Buradan hareketle, katılımcıların siber suçun hedefi olarak yaptığı davranışlar incelendiğinde kendilerinin orta düzeyde önlem alma stratejileri kullandığı söylenebilir.

İki faktörlü kimlik doğrulama ya da iki adımlı kimlik doğrulama, kişisel hesap veya uygulamalara normal oturum açma yönteminin yanı sıra ikinci bir koruma yöntemi eklemektedir. İki faktörlü kimlik doğrulama, yetki sahibi olmayan kişilerin, yetki için gerekli faktörlerin tamamına erişim sağlayamaması amacıyla oluşturulmuştur (https://tr.wikipedia.org/wiki/%C4%B0ki_fakt%C3%B6rl%C3%BC_kimlik_do%C4%9Frulama). Bu çalışmada katılımcıların %87,4'nin sanal ortamdaki hesaplarına erişirken iki faktörlü koruma sistemi kullandığı tespit edilmiştir. İlaveten katılımcıların tamamına yakınının (%93) telefonlarına erişmede güvenlik tedbiri kullandığı görülmektedir.

İşletim sistemlerinin ve uygulamaların siber ortamda gelişen tehditlerin hedefi olduğu düşünüldüğünde, bu tehditlere karşı sürekli olarak kendilerini geliştirmek ve bunun sonucu olarak da kendilerini güncellemek durumundadırlar. Yeni gelişen bir tehdide karşılık olarak güncellenen işletim sistemi veya uygulama tehdidi bertaraf edebilirken, güncellenmeyenler koruyucusuz kalarak siber suçluların hedefleri olmaya devam edebilmektedir. Güncellenen sistemlere erişim sağlayamayan siber suçlu, güncellenmeyen sistemlere yönelmektedir (Birceviz, 2020). Bu çalışmada katılımcıların neredeyse

tamamının (%97,2) telefonlarında bulunan uygulamaları, yine büyük bir oranının (%94,4) cihazlarındaki işletim sistemini güncellediği görülmektedir.

Antivirüs programları, virüslere karşı oluşturulmuş temizleme ve kurtarma işlemlerini gerçekleştiren koruyucu programlara verilen genel isimdir. Antivirüs programları virüsleri tespit etmek, kontrol altında tutmak veya silmek için çeşitli yöntemler izlemektedir. Antivirüs programları bu bağlamda ele alındığında koruyucu olarak değerlendirilebilmektedir(https://it.bilgi.edu.tr/tr/guvenlik/antivirus/#:~:text=Antivir%C3%BCs%20programlar%C4%B1%2C%20vir%C3%BCslere%20kar%C5%9F%C4%B1%20yaz%C4%B1lm%C4%B1%C5%9F,silmek%20i%C3%A7in%20%C3%A7e%C5%9Fitli%20y%C3%B6ntemler%20izler). Bu çalışmada katılımcıların cihazlarında antivirüs programı kullanma dağılımlarının birbirine yakın olduğu ancak daha büyük oranının (%50,35) cihazlarında antivirüs programı kullanmadığını belirttiği dikkat çekici bir bulgudur. Antivirüs programlarının ücretli bir koruyucu olması, bu bulguyu açıklar nitelikte olabilir. Katılımcıları suçtan koruyabilecek koruyucular kullanım alışkanlıklarına ilişkin elde edilen bulgular ışığında, katılımcıların cihazlarında antivirüs programı kullanımı haricinde kendilerini siber suç türlerinden koruyabilecek diğer koruyucuları iyi düzeyde kullandıkları, başka bir deyişle siber suçlara karşı önlem alma stratejilerinin iyi düzeyde olduğu söylenebilmektedir.

Araştırma sorularından birisi olan "katılımcıları siber suç mağduru olmaktan korumada önlem alma stratejileri kullanımları nasıldır?" sorusuna, katılımcıları siber suçtan koruyabilecek koruyucular kullanma alışkanlıklarının iyi düzeyde olduğu ve katılımcıların siber suçun hedefi olarak yaptığı davranışlar incelendiğinde kendilerinin orta düzeyde önlem alma stratejileri kullandığı, ilgili bulgular ışığında söylenebilmektedir. Bu çalışma katılımcılarının teknokent çalışanları olduğu dikkate alındığında kendilerinin siber suçlardan korunma stratejileri konusunda toplum popülasyonuna göre daha bilgili ve bilinçli olabileceği, böylece siber suçların mağduru olma konusunda önlem alma stratejilerini daha iyi düzeyde kullanıyor olabilecekleri değerlendirildiğinde ulaşılan sonuçların farklı sektör örneklemlerine ya da topluma genellenmesi riskli sonuçlar doğurabilir.

4.3. Katılımcıların Çeşitli Değişkenlere Göre Siber Suç Korkularına İlişkin Bulguların Tartışılması

Siber suç mağduriyetini ölçmeyi hedefleyen ankete göre katılımcılar mağdur olma konusunda %45'ten daha fazla oranda "zaman zaman" veya "genellikle" korku yaşadıklarını belirtmişlerdir. Buradan hareketle, katılımcılarda siber suç korkusunun bulunduğu

söylenebilir. Katılımcıların en fazla korku yaşadığı siber suç türünü "kimlik hırsızlığı" ve "sniffing" oluştururken, en az korku duyduğu siber suç türünü "bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçu" oluşturmuştur. Bu çalışmanın bulgusu ile Ankara Teknokent örnekleminde siber suç korkusunu inceleyen Yılmaz'ın çalışmasının (2018) bulguları uyumlu görünmektedir. İlgili çalışmanın katılımcılarında da siber suç korkusu olduğu tespit edilmiştir. Ayrıca Yılmaz (2011), Meško ve Bernik'in (2011) çalışmalarında da bu çalışmanın bulgusu ile tutarlı olarak katılımcıların en fazla korku duyduğu siber suç türlerinden birisi "kimlik hırsızlığı" olmuştur. Brands ve Van Wilsem (2021) tarafından yapılan ve Hollanda halkının örneklem grubunda olduğu çalışma, katılımcıların orta düzeyde siber mali suç korkusu yaşadığını göstermektedir.

Siber suç türlerine maruz kalma korkusunun cinsiyete göre farklılaşıp farklılaşmadığına ilişkin yapılan istatistiksel analizler sonucunda siber suç türlerine maruz kalma korkusundan bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalma haricinde diğer siber suç türlerinin cinsiyete göre anlamlı olarak farklılaştığı bulunmuştur. Siber suç türlerine maruz kalma açısından korku oranlarının kadınlarda daha yüksek olduğu tespit edilmiştir. Bu bulguyla tutarlı olacak şekilde Çardak'ın çalışmasına (2011) göre, yaşı kaç olursa olsun her kadın suç korkusu duymaktadır. İlgili yazın da (Pereira, Spitzberg ve Matos, 2016; van Eijk, 2017) kadınların suç korkusu duyduğunu vurgulamaktadır. Bu kapsamda araştırmanın birinci hipotezi olan "kadın ve erkek katılımcılar arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve kadın katılımcıların siber suç türlerine maruz kalma korkusu, erkek katılımcılardan daha yüksektir" hipotezi, bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalma haricindeki diğer siber suç türleri için doğrulanmıştır. Virtanen (2017) tarafından yapılan çalışmada da bu çalışmanın sonuçlarıyla tutarlı olarak kadınların daha yüksek düzeyde siber suç korkusu duyduğu belirlenmiştir. Sosyal ağlarda suç korkusunu konu alan başka bir çalışmada (Yurtsal, 2016), bu çalışmanın bulgusuyla uyumlu olmayacak şekilde cinsiyet değişkeni ile suç korkusu arasında ilişki bulunmamıştır. Bu çalışmanın bulgusu, Akdemir'in çalışmasının (2020) siber suç korkusunda cinsiyet farklılığı olmadığına yönelik bulgusuyla tutarlı olmamıştır. Alshalan (2006) tarafından yapılan çalışma ise bu çalışmanın bulgusuyla tutarlı olacak şekilde kadınların siber suç korkusunun erkeklerden daha yoğun olduğu sonucuna ulaşılmıştır. Bazı siber suç korkusu araştırmaları, kadınların çevrimiçi suçlardan daha fazla korktuğunu ve çevrimiçi kimlik hırsızlığı veya kötü amaçlı yazılım korkusunda cinsiyet farkı olmadığını göstermektedir (akt. Akdemir,2020). Yılmaz (2018)

tarafından Ankara Teknokent örneklemi ile yapılan çalışmada ise çalışmada yer alan 16 siber suç türünün 14'ünde kadınların erkeklere kıyasla anlamlı düzeyde daha yüksek siber suç korkusu yaşadığı tespit edilmiştir.

Siber suç türlerine maruz kalma korkusunun medeni duruma göre farklılaşıp farklılaşmadığına ilişkin yapılan istatistiksel analizler sonucunda, e-posta veya sosyal paylaşım sitelerine ait parolaların çalınması korkusunun, kimlik hırsızlığına, bilgisayar korsanlığına, truva atları, solucanlar, virüsler ve zararlı yazılımlara, keylogger ve screenlogger gibi zararlı yazılımlara maruz kalma korkusunun medeni duruma göre anlamlı olarak farklılaştığı bulunmuştur. İlgili siber suç türlerine maruz kalma açısından korku oranlarının evlilerde daha yüksek olduğu tespit edilmiştir. Bu kapsamda "bekâr ve evli katılımcılar arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve bekâr olan katılımcıların siber suç türlerine maruz kalma korkusu, evli olan katılımcılardan daha yüksektir" hipotezi doğrulanmamıştır**.** Evli olmanın bireye sosyal destek aracı olarak işlev sağlayabileceği, dolayısıyla siber suç türlerine maruz kalma korkusunun evli olan katılımcılarda daha düşük düzeyde görüleceği düşünülerek ilgili hipotez kurulmuştu. Fakat bu çalışmada, beş siber suç türlerinde evli katılımcıların bekâr katılımcılardan anlamlı düzeyde daha yüksek siber suç korkusuna sahip olması, bu görüşü doğrulamamıştır.

Siber suç türlerine maruz kalma korkusunun yaşa göre farklılaşıp farklılaşmadığına ilişkin yapılan analizler sonucunda, e-posta veya sosyal paylaşım sitelerine ait parolaların çalınmasına, kimlik hırsızlığına, siber zorbalığa ve zombi ordulara maruz kalma korkularının yaşa göre anlamlı olarak farklılaştığı bulunmuştur. Yaşı 34-41 olanların %60'ı ve 26-33 olanların %58.7'si e-posta veya sosyal paylaşım sitelerine ait parolalarınızın çalınması konusunda orta, çok ve aşırı düzeyde korku yaşarken, yaşı 42-49 ve 18-25 olanlarda bu oran sırasıyla %43.5 ve %45.5; yaşı 34-41 olanların %80'i, 42-49 olanların %91.3'ü ve 26-33 olanların %91.2'si kimlik hırsızlığına maruz kalmanız konusunda orta, çok ve aşırı düzeyde korku yaşarken, yaşı 18-25 olanlarda bu oran %72.8; yaşı 42-49 olanların %91.3'ü siber zorbalığa maruz kalmanız konusunda orta, çok ve aşırı düzeyde korku yaşarken, yaşı 18-25, 26-33 ve 34-41 olanlarda bu oran sırasıyla %72.8, %73.5 ve %73.3; yaşı 18-25 olanların %27.3'ü, 26-33 olanların %29.4'ü ve 34-41 olanların %33.4'ü zombi ordulara maruz kalmanız konusunda çok ve aşırı düzeyde korku yaşarken, yaşı 42-49 olanlarda bu oran %17.4 olarak bulunmuştur. Araştırmanın üçüncü hipotezi "yaş grupları arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve yaşça daha büyük olan katılımcıların siber suç türlerine maruz kalma korkusu, yaşça daha genç olan katılımcılardan daha

yüksektir" şeklinde idi. Yaşça büyük bireylerin sahip olduğu bilişsel özellikleri sebebiyle teknolojiye daha zor adapte olacakları düşünülerek siber suç mağduru olma korkularının da daha yüksek olacağı öngörülmüştü. Öyle ki Brands ve Van Welsem (2021) tarafından yürütülen çalışmada, yaşça daha büyük olan Hollandalı katılımcıların siber mali suç korkusu, diğer katılımcılardan anlamlı düzeyde yüksek bulunmuştur. Yine ilgili yazında yaşça daha büyük olan bireylerin genç bireylere oranla daha yoğun düzeyde siber suç korkusu duyduğu ifade edilmektedir. Ancak genç kadınların yaşlı kadınlara oranla siber suç korkularının daha yüksek düzeyde olduğu da belirtilmektedir (Alshalan, 2016). Bir başka çalışmada ise (Akdemir, 2020) ileri yaştaki internet kullanıcıları, diğer yaş gruplarına kıyasla siber suçlardan daha fazla korkmaktadırlar. Kadınların suç korkusunu konu alan Çardak'ın çalışmasında (2011) da kadınların suç korkusu yaş değişkenine göre farklılaşmamıştır. Pereira, Spitzberg ve Matos'un (2016) 12-16 yaşları arasında 627 ergen örneklemiyle siber mağduriyetin yaygınlığını belirlemek amacıyla yürüttüğü çalışmasında, yaşça daha küçük olan kız ergenlerin daha yüksek düzeyde korku duyduğu ortaya konmuştur.

Siber suç türlerine maruz kalma korkusunun eğitim durumuna göre farklılaşıp farklılaşmadığına ilişkin yapılan analizler sonucunda, kimlik hırsızlığına ve bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalma korkusu hariç diğer siber suç türlerinin eğitim durumuna göre anlamlı olarak farklılaştığı bulunmuştur. Elde edilen sonuçlar, siber suç türlerine maruz kalma açısından korku oranlarının genel olarak lisansüstü ve lisans mezunlarında daha yüksek olduğunu göstermiştir. Yapılan analizler neticesinde iki suç türü özelinde doğrulanan araştırmanın dördüncü hipotezi "eğitim düzeyi grupları arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve eğitim düzeyi daha yüksek olan katılımcıların siber suç türlerine maruz kalma korkusu, eğitim düzeyi daha düşük olan katılımcılardan daha yüksektir" şeklinde idi. Bu hipotezin oluşturulmasındaki düşünce, eğitim düzeyi yükseldikçe siber tehlikelere yönelik bilgi düzeyinin de artacağı ve bu durumun siber suç korkusunu artıracağı idi. Bu çalışma bulgularıyla tutarlı şekilde Brands ve Van Welsem (2021) ve Akdemir tarafından yapılan çalışmalarda (2020) da eğitim düzeyi ve siber suç korkusu arasında anlamlı ilişki saptanmıştır. Akdemir'in çalışması (2020) daha yüksek eğitim düzeyine sahip internet kullanıcılarının daha yüksek düzeyde siber suç korkusuna sahip olduğunu göstermiştir. Brands ve Van Welsem (2021) tarafından yürütülen çalışmada ise düşük eğitim düzeyine sahip Hollandalı katılımcıların siber mali suç korkusu yüksek bulunmuştur. Virtanen tarafından yürütülen çalışmada (2017) daha düşük sosyal statü, daha yüksek siber suç

korkusuyla ilişkili bulunmuştur. Yılmaz tarafından yürütülen çalışmada (2018) da araştırmada yer alan 16 suç türünden yalnızca bilgisayar korsanlığı ve bilişim sistemleri aracılığıyla işlenen nefret ve ayrımcılık suçu korkusu ile eğitim düzeyi arasında anlamlı ilişki saptanmıştır. Maddison ve Jeske (2014) ve Yılmaz (2018) tarafından yapılan çalışmalarda, bu bulgularla uyumsuz olarak eğitim düzeyi ve siber suç korkusu arasında ilişki bulunmamıştır. Çardak'ın kadınlarda suç korkusunu konu aldığı çalışmasında (2011) da suç korkusunun eğitim düzeylerine göre farklılaşmadığı belirlenmiştir.

Siber suç türlerine maruz kalma korkusunun algılanan ekonomik duruma göre farklılaşıp farklılaşmadığına ilişkin olarak e-posta veya sosyal paylaşım sitelerine ait parolaların çalınması, banka hesap bilgilerinin çalınması yoluyla zarara uğratılma, bilgisayar korsanlığına maruz kalma, truva atları, solucanlar, virüsler ve zararlı yazılımlara maruz kalma, siber hırsızlığa maruz kalma, siber dolandırıcılığa maruz kalma siber yer tespitine maruz kalma, bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalma, siber terörizme maruz kalma korkularının algılanan ekonomik duruma göre anlamlı olarak farklılaştığı bulunmuştur. Buna göre, ilgili siber suç türlerine maruz kalma açısından korku oranlarının genel olarak ekonomik durumunu yeterli olarak algılayanlarda daha yüksek olduğunu göstermektedir. Araştırmanın beşinci hipotezi "algılanan ekonomik durumu grupları arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve algıladıkları ekonomik durumu yeterli olan katılımcıların siber suç türlerine maruz kalma korkusu, yetersiz olan katılımcılardan daha yüksektir" şeklindedir. Dolayısıyla bu çalışmada, sekiz siber suç türü için ilgili hipotezin doğrulandığı söylenebilir. Bazı çalışmalarda (Roberts vd., 2013; Virtanen, 2017; Brands ve van Wilsem, 2021) daha düşük eğitim düzeyine sahip olan katılımcılarda siber suç korkusu daha yüksek belirlenmiştir. Ancak Akdemir'in çalışmasına (2020) göre, daha yüksek gelir düzeyine sahip olan internet kullanıcıları, daha yüksek düzeyde siber suç korkusu duymaktadırlar.

Araştırmanın üç siber suç türü haricindeki suç türleri için doğrulanan altıncı hipotezi "mesleki tecrübe düzeyi grupları arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve mesleki tecrübe düzeyi daha fazla olan katılımcıların siber suç türlerine maruz kalma korkusu, diğer katılımcılardan daha yüksektir" şeklinde idi. Siber suç türlerine maruz kalma korkusunun meslekteki çalışma yılına göre farklılaşıp farklılaşmadığına ilişkin yapılan analizler sonucunda; siber tacize maruz kalma, siber şantaja veya siber tehdide maruz kalma ve bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalma haricinde diğer siber suç türlerinin meslekte çalışma yılına göre anlamlı olarak

farklılaştığı bulunmuştur. Buna göre belirtilen siber suç türlerine maruz kalma açısından korku oranlarının genel olarak 9 yıl ve üzeri ile 2-8 yıl arası çalışanlarda daha yüksek olduğu belirlenmiştir.

Siber suç türlerine maruz kalma korkusunun görev alınan sektöre göre farklılaşıp farklılaşmadığına ilişkin yapılan analizler sonucunda; e-posta veya sosyal paylaşım sitelerine ait parolaların çalınması, zombi ordulara maruz kalma, sosyal ağ üzerinden sahtekârlığa maruz kalma, bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna maruz kalma ve siber terörizme maruz kalma korkularının görev alınan sektöre göre anlamlı olarak farklılaştığı bulunmuştur. Buna göre ilgili siber suç türlerine maruz kalma açısından korku oranlarının diğer sektörde görev alanlarda yazılım ve bilişim sektöründe görev alanlara kıyasla daha yüksek olduğu ortaya konulmuştur. Araştırmanın yedinci hipotezi "görev alınan sektör grupları arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve diğer sektörlerde çalışan katılımcıların siber suç türlerine maruz kalma korkusu, yazılım-bilişim sektöründe çalışan katılımcılardan daha yüksektir" şeklindedir. Hipotezin kurulmasındaki düşünce, siber uzay hakkında mesleği sebebiyle bilgi sahibi olan meslek kollarındaki bireylerin siber suç korkusundan korunacağı şeklindedir. Yapılan analizler sonucunda ilgili hipotez, beş siber suç türü için doğrulanmıştır.

Siber suç türlerine maruz kalma korkusundan banka hesap bilgilerinin çalınması yoluyla zarara uğratılma, kimlik hırsızlığına maruz kalma, siber şantaja veya siber tehdide maruz kalma, siber hırsızlığa maruz kalma, siber ortamda haberleşme gizliliğinin ihlali, sniffinge maruz kalma ve siber terörizme maruz kalma korkularının internete en çok hangi araçtan erişim sağladığına göre anlamlı olarak farklılaştığı bulunmuştur. Buna göre belirtilen siber suç türlerine maruz kalma açısından korku oranlarının genel olarak mobil cihazdan ve kurumsal cihazlardan erişim sağlayanlarda daha yüksek olduğu saptanmıştır. Dolayısıyla sekizinci hipotez olan "internete erişim sağlama grupları arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve internete en çok mobil cihazdan erişim sağlayan katılımcıların siber suç türlerine maruz kalma korkusu, diğer katılımcılardan daha yüksektir" hipotezinin yedi siber suç türü özelinde doğrulandığı söylenilebilir.

Siber suç türlerine maruz kalma korkusunun kamuya açık alanlarda bulunan kablosuz ağlara erişim sağlama durumuna göre farklılaşıp farklılaşmadığına ilişkin yapılan analizler sonucunda; e-posta veya sosyal paylaşım sitelerine ait parolaların çalınması korkusuna, kimlik hırsızlığına, bilgisayar korsanlığına, truva atları, solucanlar, virüsler ve zararlı yazılımlara, keylogger ve screenlogger gibi casus yazılımlara, siber şantaja veya siber

tehdide, siber dolandırıcılığa, sniffinge, zombi ordulara, sosyal ağ üzerinden sahtekârlığa, siber yer tespitine ve siber terörizme maruz kalma korkularının kamuya açık alanlarda bulunan kablosuz ağlara erişim sağlama durumuna göre anlamlı olarak farklılaştığı bulunmuştur. Buna göre belirtilen siber suç türlerine maruz kalma açısından korku oranlarının kablosuz ağlara erişim sağlayanlarda daha yüksek olduğu bulgulanmıştır. Araştırmanın dokuzuncu hipotezi "kamuya açık alanlarda bulunan kablosuz ağlara erişim sağlayan ve sağlamayan katılımcılar arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve kamuya açık alanlarda bulunan kablosuz ağlara erişim sağlayan katılımcıların siber suç türlerine maruz kalma korkusu, erişim sağlamayan katılımcılardan daha düşüktür" şeklindedir. Ancak yapılan analizler, bu hipotezi doğrulamamıştır. İlgili hipotezin kurulmasındaki düşünce, siber suç türlerine maruz kalma korkusu yüksek olan katılımcıların bir suç önleme stratejisi olarak kamuya açık alanlarda bulunan kablosuz ağlara erişim sağlamamayı tercih edeceği idi. Öyle ki Akdemir (2020) tarafından da siber suç korkusunun, koruma tedbirleri kullanımını teşvik ettiği belirtilmektedir. Fakat Brands ve Van Wilsem'in (2021) çalışmasında siber suç korkusu ile kişisel bilgisayarda koruyucu kullanma davranışı arasında ilişki tespit edilmemiştir. Katılımcıların gündelik ve çalışma hayatlarındaki mecburiyetlerden ötürü siber suç korkuları yüksek bile olsa internete erişim sağlamak için kamuya açık kablosuz ağlara erişim sağlamak zorunda olmaları olasılığı da göz önünde bulundurulmalıdır.

Siber suç türlerine maruz kalma korkusunun kullandığı şifrelerin benzerlik durumuna göre farklılaşıp farklılaşmadığına ilişkin yapılan istatistiksel analizler sonucunda; siber tacize, bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna, siber terörizme maruz kalma korkusu hariç diğer siber suç türlerinin, kullandığı şifrelerin benzerlik durumuna göre anlamlı olarak farklılaştığı bulunmuştur. Buna göre, ilgili siber suç türlerine maruz kalma açısından korku oranlarının şifreleri benzer olanlarda daha yüksek olduğunu göstermektedir. Fakat araştırmanın onuncu hipotezi "kullandığı şifreler benzer olan ve benzer olmayan katılımcılar arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve kullandığı şifreleri birbirinin benzeri olan katılımcıların siber suç türlerine maruz kalma korkusu, benzemeyen katılımcılardan daha düşüktür" şeklindedir. Yani siber suç korkusu yüksek olan katılımcıların güvenlik önlemi olarak çeşitli platformlarda farklı şifreler kullanacağı öngörülmüştü. Fakat bulgular, bu görüşü doğrulamamıştır. Bu bulgular, Brands ve Van Wilsem'in (2021) ve Akdemir'in (2020) çalışmasının bulguları ile uyumlu olmamıştır. Akdemir'e göre (2020) siber suç korkusu internet kullanıcılarını, şifre yönetim

stratejileri kullanmaya teşvik etmekte olup, siber suç korkusu yüksek olan katılımcılar karmaşık şifreler ve farklı çevrimiçi hesaplar için farklı şifreler kullanmaktadır. Farklı platformlarda farklı şifreler kullanılması konusunda bu çalışmanın katılımcılarına yönelik kurumlarında yapılacak bilgilendirmeler ya da hizmet içi eğitimler sunulması suretiyle siber suç korkularında azalma sağlanması hedeflenebilir.

Yapılan analizlere göre; kimlik hırsızlığına, keylogger ve screenlogger gibi casus yazılımlara, siber zorbalığa siber hırsızlığa, sniffinge, zombi ordulara, sosyal ağ üzerinden sahtekârlığa, bilişim sistemleri vasıtasıyla işlenen nefret ve ayrımcılık suçuna ve siber terörizme maruz kalma korkularının sosyal medya hesaplarını başka sitelere erişim için kullanma durumuna göre anlamlı olarak farklılaştığı bulunmuştur. Buna göre, siber suç türlerine maruz kalma açısından korku oranlarının sosyal medya hesaplarını başka sitelere erişim için kullanmayanlarda daha yüksek olduğunu göstermiştir. Araştırmanın on birinci hipotezi "sosyal medya hesaplarını başka sitelere erişim için kullanan ve kullanmayan katılımcılar arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve sosyal medya hesaplarını başka sitelere erişim için kullanmayan katılımcıların siber suç türlerine maruz kalma korkusu, kullanan katılımcılardan daha yüksektir" şeklindedir. Dolayısıyla bazı siber suç türleri bazında ilgili hipotez doğrulanmıştır. Elde edilen sonuç, bu çalışma kapsamında anlamlı farklılık tespit edilen suç türlerine yönelik siber suç korkusu yüksek olan katılımcıların suç önleme stratejisi olarak sosyal medya hesaplarını başka sitelere erişim amacıyla kullanmıyor olduğunu düşündürmektedir.

Araştırmanın on ikinci hipotezi de "antivirüs programı kullanan ve kullanmayan katılımcılar arasında siber suç türlerine maruz kalma korkusu açısından fark vardır ve antivirüs programı kullanan katılımcıların siber suç türlerine maruz kalma korkusu, antivirüs programı kullanmayan katılımcılardan daha yüksektir" şeklindedir. Siber suç türlerine maruz kalma korkusunun antivirüs programı kullanma durumuna göre farklılaşıp farklılaşmadığına ilişkin yapılan analizler sonucunda, keylogger ve screenlogger gibi casus yazılımlara maruz kalma hariç diğer siber suç türlerinin, antivirüs programı kullanma durumuna göre anlamlı olarak farklılaştığı bulunmuştur. Buna göre, siber suç türlerine maruz kalma açısından korku oranlarının antivirüs programı kullananlarda daha yüksek olduğu belirlenmiştir. Antivirüs programı kullanmanın, siber suçlara ilişkin önlem alma stratejisi olarak işlev göreceği düşünülerek kurulan bu hipotezin keylogger ve screenlogger gibi casus yazılımlara maruz kalma korkusu hariç diğer siber suç türleri için doğrulandığı

görülmektedir. Ancak Brands ve Van Wilsem'in (2021) çalışmasında siber suç korkusu ile kişisel bilgisayarda koruyucu kullanma davranışı arasında ilişki tespit edilmemiştir.

BEŞİNCİ BÖLÜM

SONUÇ

5.1. Giriş

Günümüzde internet tabanlı teknolojiler, hayatımızın her alanında var olan önemli bir ihtiyaç halini almıştır. Bilgisayar, internet ve çeşitli mobil teknolojiler, modern toplumu yeniden şekillendirmekle birlikte bu teknolojilerin sağladığı imkânlar, suç ve sapkınlığın doğasını da önemli ölçüde değiştirmiştir. İnternet kullanıcılarının gün geçtikçe çoğalması ve toplumun dijitalleşmesi, suç ve suçlunun ortaya çıkışında siber ortamın çekicilik kazanmasına, dolayısıyla siber suçların ortaya çıkışına etkide bulunmuştur (Erculj ve Mesko, 2022; Holt ve Bossler, 2016). İlgili yazın, en hızlı büyüyen suç türü olarak siber suçların, çevrimiçi yatırımcılar ve bireyler için ciddi bir tehdit oluşturduğuna dikkati çekmektedir (Akdemir, 2020).

İşlenen suçun bir sonucu olarak düşünülebilen suç korkusu, suçlarla mücadeleyi zorlaştıran bir etkendir. Dolayısıyla suç korkusunu azaltmak, suçla mücadelenin öncelikleri arasında yer almalıdır. Suç korkusunun azaltılabilmesinde öncelikli olarak suç korkusunun düzeyinin ve ilişkili olduğu değişkenlerin belirlenmesi önem arz etmektedir. İlgili yazın, siber ortamda işlenen suçların gerçek dünyada işleniyor gibi kolaylıkla işlenebildiğini vurgulamaktadır (Yurtsal, 2016). Ancak yapılan çalışmalar, daha ziyade geleneksel suç korkusu ile ilişkili etmenleri ortaya koymayı amaçlamıştır (Akdemir, 2020). Siber suç mağduru olma riskinin artması, beraberinde siber suç korkusunun gelişimine zemin hazırlamakla birlikte, gerçekleşebilecek olan siber suç saldırılarına karşı da önlem almaya yöneltmektedir (Erculj ve Mesko, 2022). Bu bağlamda bu çalışma, Trabzon Teknokent örneği üzerinden siber suç korkusunu ve önlem alma stratejilerini konu edinmiştir. Siber suç korkusu üzerine yapılan boylamsal çalışmaların yetersiz düzeyde olduğu bilinmektedir (Brands ve van Wilsem, 2021). Bu çalışma bulgularının, siber suç korkusu ile ilgili farklı kültürlerde, farklı örneklemlerde ve farklı yöntemlerle yürütülmesi beklenen gelecek çalışmalara temel oluşturması ve literatüre bilgisel katkı sağlaması bakımından önem teşkil etmektedir. Bu çalışma kapsamında çeşitli değişkenlere göre siber suç korkusunun anlamlı şekilde farklılaştığı görülmektedir. Buradan hareketle, teknolojiyle yoğun olarak vakit geçiren bireylerin ve bu araştırmanın katılımcıları gibi mesleği gereği bilişim teknolojileriyle iç içe olan sektör çalışanlarının siber suça yönelik önlem alma stratejileri kullanımının desteklenmesi önerilir.

Bireyle başlayıp toplumsal alanda etki gösteren bir olgu olan suç kavramının etkilerinin en az düzeye indirgenmesi için suçu oluşturan unsurların dikkatli bir şekilde araştırılıp belirlenmesi gereklidir. Bu konu ile ilgili yapılmış çalışmaların ulaştığı sonuçlar, suçu etkileyen birden çok etmenin bulunduğu şeklindedir (Yavuz, 2019). Siber suçlar yapısı itibarı ile karmaşık ve çeşitli olmakla birlikte dijital teknoloji hayatımızda merkezi bir rol oynadıkça siber suçlar da çeşitlenmeye devam edecektir (Holt ve Bossler, 2016). Siber suçluların kendilerini sürekli olarak yenilemekte olmasından hareketle günümüzde henüz suç olarak tanımlanmamış birtakım eylemlerin, gelecekte suç olarak karşımıza çıkabilme ihtimali oldukça yüksektir. Siber suç ve siber suç korkusu konusunda yapılacak çalışmalarda bu durumun göz önünde bulundurulması önerilmektedir (Birceviz, 2019). Rutin Aktiviteler Teorisi'nin sunduğu varsayımlar da dikkate alınarak siber suçların mağduru olma riski altında olan bireylere yönelik daha fazla önlem alma stratejilerinin geliştirilmesi, siber suç mağdurlarının psikolojik bakımdan desteklenmesi, siber suçlu olma potansiyeli taşıyan bireylere ve siber suçlulara yönelik olarak suç işlemekten caydırıcı tedbirlerin ve suç önleme programlarının geliştirilmesi, bu suçla mücadelede öncelikli hedeflerden olmalıdır

KAYNAKÇA

Abdulai, M. (2016). *Determinants of fear of cybercrime victimisation: a study of credit/debit card fraud among students of the University of Saskatchewan*. (Yüksek Lisans Tezi). University of Saskatchewan, Saskatchewan.

Akdemir, N. (2020). Siber suç korkusunun internet kullanıcılarının davranışsal adaptasyonları, kişisel verilerin paylaşımı kararları ve güvenlik tedbirlerini uygulama niyetleri üzerindeki etkilerinin ölçülmesi. *International Journal of Eurasia Social Sciences, (e-ISSN: 2146-1961) 627-648.*

Akman, Y. (2020) *Dijital dönüşüm ve yenilik yönetimi*. İstanbul:İskenderiye Kitap.

Akpınar, İ. (2018). Suç olgusu, suç teorileri ve kadın suçluluğu: Kayseri örneği. (Yayımlanmamış yüksek lisans tezi). Niğde Ömer Halisdemir Üniversitesi Sosyal Bilimler Enstitüsü, Niğde.

Aldoori, A. (2020). *Uluslararası hukukta siber suçla mücadele.* (Yayınlanmamış yüksek lisans tezi). İstanbul Üniversitesi Sosyal Bilimler Enstitüsü,İstanbul.

Aliusta, C. & Benzer, R. (2018). Avrupa Siber Suçlar Sözleşmesi ve Türkiye'nin dahil olma süreci. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 4(2), s:35-42.

Alshalan, A. (2006). *Cyber-crime fear and victimization: an analysis of a national survey*. (Unpublished Doctoral Thesis). Mississippi State University, Mississippi.

Arslan, M. E. (2016). Siber güvenlik ve siber saldırı türleri. Gazi Üniversitesi Sosyal Bilişim Enstitüsü, Ankara.

Artuk, M. E., Gökcen, A., Yenidünya, A. C. (2014). *Ceza hukuku özel hükümler*. Ankara, Adalet Yayınevi.

Avşar, B. Z. & Öngören, G. (2010). *Bilişim hukuku*. İstanbul:Türkiye Bankalar Birliği.

Aydın., N. (2018). Nitel araştırma yöntemleri. *Uluslararası Beşeri ve Sosyal Bilimler İnceleme Dergisi*, 2(2).

Başeğmez, A. C. & Özerk, H. (2021) İnsanın saldırgan ve şiddet içeren davranışlarını psikoterapi kuramlarının ele alış biçimlerinin değerlendirilmesi. *Opus- International Journal of Society Researches* .(e-ISSN : 2528-9535), 18(44), 8475-8499.

Bernik, I. & Mesko, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto, *Revija Za Kriminalistiko İn Kriminologijo* / 62(3), pp. 242-252.

Bilgi Teknolojileri ve İletişim Kurumu, (2022). Dijitalleşen dünyada bilişim suçları ve mücadele yöntemleri. Sektörel araştırma ve strateji geliştirme dairesi başkanlığı.

Bingöl, İ. (2022). Sosyolojik suç teorilerine kuramsal bir yaklaşım: sosyal süreç teorileri. *Bingöl Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 24, 640-652.

Birceviz, F. (2019). Rutin aktiviteler teorisi bağlamında siber suç mağduriyeti. (Yayımlanmış yüksek lisans tezi). Milli Savunma Üniversitesi Alparslan Sosyal Bilimler Enstitüsü, İstanbul.

Boeting, B. P., (2006). The *Routine Activity Theory: A Model for Addressing Specific Crime Issues*. *FBI Law Enforcement Bulletin*, 75(6), pp.12-19.

Boeting, B.. P. (2006). The routine activity theory: a model for addressing specific crime ıssues. *FBI Law Enforcement Bulletin,* 75(6), pp.12-19.

Boztoprak, A. (2021). Suç korkusu: Karamanoğlu Mehmetbey Üniversitesi öğrencileri üzerinde bir inceleme.(Yayımlanmamış yüksek lisans tezi). KMÜ Sosyal Bilimler Enstitüsü, Karaman.

Brands, J. & Van Wilsem, J. (2021). Connected and fearful? exploring fear of online financial crime, ınternet behaviour and their relationship. *European Journal of Criminology*, 18(2), 213-234.

Brands, J. & Wilsem, J. V. (2016). Connected and fearful? Exploring fear of online financial crime, Internet behaviour and their relationship. *European Journal of Criminology,* 18(2).

Burkay, S. (2008). Suç teorileri ve suç olgusu: Antalya örneği. (Yayımlanmamış yüksek lisans tezi). Akdeniz Üniversitesi Sosyal Bilimler Enstitüsü, Antalya.

Burkay, S. (2008, Ekim). Teorik çerçevede suç. *ETHOS: Felsefe ve Toplumsal Bilimlerde Diyaloglar,* Sayı: 2/4.

Büyüköztürk, Ş., Çakmak, E., Akgün, Ö. A., Karadeniz, Ş. & Demirel, F. (2013). *Eğitimde bilimsel araştırma yöntemleri.* 25. Baskı, Ankara: Almat Basım Yayıncılık Ambalaj Sanayi Tic. Ltd. Şti.

Cengiz, G. (2021). Siber suçlar, sosyal medya ve siber etik. *İletişim Çalışmaları Dergisi*, 7 (3), 407-424.

Clarke, R. V. & Felson, M. (2004). Routine Activity and Rational Choice. Advances in Criminological Theory,Volume 5. New Brunswick, NJ: Transaction Publishers.

Cohen, L. E. & Felson, M. (1979). Social change and crime rate trends: a routine activity approach. *American Sociological Review*, 44(4).

Cohen, L. E., Marcus, F.& Land, K. C. (1980). Property crime rates in the United States: a macrodynamic analysis, 1947-1977; with ex ante forecasts fort he mid-1980s. *American Journal of Sociology*, 86(1).

Cullen, F. T. & Agnew, R. (2003). *Criminological theory: past to present - essential readings*, Second Edition. Los Angeles, CA: Roxbury Publishing Company.

Çalışkan, M. (2019). İstanbul'da "kadına şiddet" ve "kadın cinayeti" vakalarına yönelik, nicel-nitel bir inceleme, Araştırma Makalesi.

Çardak, B. (2011). Kadınların suç korkuları üzerine nitel bir çalışma, *Güvenlik Bilimleri Dergisi*, 1(1), 23-45.

Çelik, F. & Mirza, E. (2020). Öğrencilerin Selçuk Üniversitesi, Alaeddin Keykubad Kampüsü'ne yönelik suç korkusu. *Inonu University Journal of Art and Design*, 1-21.

Çetin, M. S. (2020). Yargıtay kararları ışığında bilişim sistemine girme veya kalma suçu (TCK m. 243). Araştırma Makalesi.

Doran, B, & Burgess, M. B. (2012). Why is fear of crime a serious social problem? In: Doran B, Burgess M. B. (eds) *Putting Fear of Crime on the Map*. New York: Springer, 9–23.

Dönmezer, S. (1994). *Toplum bilim*. İstanbul:Beta Basım Yayın.

Durkheim, E. (2019). *Sosyolojik Yöntemin Kuralları*. (Çev. Özcan Doğan), Ankara,:Doğubatı Yayınları.(Orijinal çalışma basım tarihi 1994).

Ehliz, H. (2019). *Bilişim suçlarının ulusal ve uluslararası düzeyde değişen güvenlik algısı üzerinde etkisi*. (Yayımlanmış yüksek lisans tezi) İstanbul Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

Ergün Bülbül, S., (2000). Çoklu karşılaştırma testleri ve bir örnek uygulama. Öneri Dergisi 3(14), 95-100.

Ejik, V. (2017). Fear of cybercrime in Europe: examining the effects of victimization and vulnerabilities. *Psychiatry Pscyology and Law*, 24(3),1-16.

ErculJ, V. Mesko, G. (2022). Fear of crime measurement of fear of ordinary crimes and fear of crimes in cyberspace. *Evija Za Kriminalistiko İn Kriminologijo*. (4), 308–318.

Ermeydan, D. (2018). *Türk Ceza Kanunu'nda bilişim suçları*, (Yayımlanmamış yüksek lisans tezi). Çağ Üniversitesi Sosyal Bilimler Enstitüsü, Mersin.

Felson, M., (1986). Linking Criminal Choices, Routine Activities, Informal Control, and Criminal Outcomes", in Derek B. Cornish and Ronald V. Clarke (eds), The Reasoning Criminal: Rational Choice Perspectives on Offending, New York, NY: Springer-Verlag, pp.119-128.

Felson, M. (1995). Those Who Discourage Crime. in John E. Eck and David Weisburd (eds), Crime and Place, Crime Prevention Studies, Volume 4. Criminal Justice Press, Monsey, New York, U.S.A. and The Police Executive Research Forum, Washington, D.C.. Willow Tree Press.

Felson, M. (1998). *Crime and everyday life*, Second Edition. Thousand Oaks: Pine Forge Press, A Sage Publications Company.

Felson, M., Eckert, M. A. (2018). *Crime and everyday life: a brief ıntroduction*, 6th Edition, United States: SAGE Publications.

Fidan, S., & Uludağ, B. C. (2023). Rutin aktiviteler teorisi bağlamında dijitalleşen dünyada siber suç mağdurları. *Habitus Toplumbilim Dergisi*, (4), 175-210.

Gökulu, G. (2019). Sembolik etkileşimci teorinin gündelik yaşam sosyolojisine katkıları. *Ekev Akademi Dergisi. 80, 173-190.*

Güçlü, İ. & Akbaş, H. (2019). *Suç sosyolojisi; kavram, yöntem, uygulama*. (2.Baskı) Ankara, Gazi Kitabevi.

Gürkan, T. & Koran, N. (2015). Suç korkusu konusunda yapılan bilimsel araştırmaların analizi. *Gündelik hayat sosyolojisi açısından suç ve suç korkusu*, 571-585. Ankara: Serya Yayıncılık.

Hatipoğlu, C. & Tunacan, T. (2021). Türkiye'de siber saldırı ve tespit yöntemleri: bir literatür taraması. *BŞEÜ Fen Bilimleri Dergisi*,8(1), 430-445.

Hekim, H. & Başıbüyük, O. (2013). Siber suçlar ve Türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi,* 4 (2). 135-158.

Henson, B. (2011). *Fear of crime online: examining the effects of online victimization and perceived risk on fear of cyberstalking victimization*. (Doktora Tezi). University of Cincinnati, Cincinnati.

Holt, T. J., & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1–25.

Holt, T. J., & Bossler, A. M. (2008). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization, *Deviant Behavior*, 30(1), 1-25.

İçli, T. G. (2013). *Kriminoloji,* Ankara, Seçkin Yayıncılık.

İnönü Üniversitesi Sanat ve Tasarım Dergisi, Öğrencilerin Selçuk Üniversitesi, Alaeddin Keykubad Kampüsü'ne Yönelik Suç Korkusu.

John, T., & Tierney, J. (2009). *Key perspectives in criminology*. Berkshire: McGraw-Hill Education.

Küçükvardar, M. (2018). Suç olgusunun değişen yüzü siber suçlar. *ISophos: International Journal of Information, Technology and Philosophy,* 1(1), 1-17.

Leukfeldtaand, E. R. & Yar, M. (2015). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Devıant Behavıor*, 37(3), 263–280.

Maddison, J. & Jeske, D. (2014). Fear and percieved likelihood of victimization in traditional and cyber settings. *International Journal of Cyber Behavior*, 4(4):23-40.

Marcum, C. D., Ricketts, M. L. & Higgins, G. E. (2010). Assessing sex experiences of online victimization: an examination of adolescent online behaviors using routine activity theory. *Sage Journal*,35(4).

Öztük, M. & Yıldız, M. (2017). Yaşam doyumu ve suç korkusu arasındaki ilişki (Mersin örneği), *MCBÜ Sosyal Bilimler Dergisi,* 15(1), 657-673.

Öztürk, E., Ateş, A. ve Erdoğan, B. (2020). *Siber suçların hukuksal yönleri ve psikolojik dinamikleri.* Siber Psikoloji. Türkiye Klinikleri:Ankara. p.48-55.

Öztürk, M. (2016). Düzensizlik ve toplumsal kaygı teorileri bağlamında suç korkusunun incelenmesi: Mersin örneği. *CÜ Sosyal Bilimler Dergisi*, 40 (1),281-292.

Öztürk, Ş. (2015). Sosyal medyada etik sorunlar, *Selçuk İletişim Dergisi*, 9 (1), 287-311.

Parlar, A. (2011). *Türk ceza hukukunda bilişim suçları*. Ankara: Bilge Yayınevi.

Pereira, F, Spitzberg, B. & Matos, M. (2016). Cyber-harassment victimization in Portugal: Prevalence, fear and help-seeking among adolescents. *Computers in Human Behavior, 62(2),136-146.*

Reyns, B. W., Henson, B. & Fisher, B. S. (2011). Being pursued online: applying cyberlifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, 38(11):1149-1169.

Saini, H., Rao, Y. S. ve Panda, T. C. (2012). Cyber-crimes and their ımpacts: a review. *International Journal of Engineering Research and Applications*, 2(2), 202-209.

Setiawan, N. Vd. (2018). Impact of cybercrime in e-business and trust, *İnternational Journal of Civil Engineering and Technology*.

Sheley, J.,H. (1991). *Criminology*: a contemporary handbook (sociology). Wadsworth Publishing, Belmont.

Siegel, L. J. (1989). *Criminology.* St. Paul, MN: West Pub Comp.

Smith, I. B., Sutherland A, & Jackson, J. (2013). The role of neighbourhoods in shaping crime and perceptions of crime. In: Manley D, Van Ham M, Bailey N, et al. (eds) *Neighbourhood Effects or Neighbourhood Based Problems? A Policy Context*. Dordrecht: Springer, 67–87.

Sunay, M. M. & Birel, E. (2023). Yapısal fonksiyonalist bağlamda siber suçların analizi. *Socrates Journal of Interdisciplinary Social Studies*, Year 9, Volume 25.

Suveren, Y. (2019). *Küreselleşme, internet ve yeni suçlar: siber dünya ve siber suçlar, suç sosyolojisi,* Açıköğretim Fakültesi,Eskişehir.

Sürer, M. (2014). Siber suçlar üzerine bir araştırma; Afyonkarahisar örneği. (Yayımlanmamış yüksek lisans tezi). Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Afyonkarahisar.

Şahin, D. A. (2015). *Gündelik hayat sosyolojisi açısından suç ve suç korkusu.* 1-2. Ankara: Serya Yayıncılık.

Şenol, D. & Gülver, Ö. (2020). Suçun sosyal psikolojik maliyeti: suç korkusu ve suç korkusuna neden olan faktörler. *Toplum ve Kültür Araştırmaları Dergisi,* 5, 25-41.

Şenol, D. & Karataşoğlu, E., B., (2022, Ocak), Siber suçlara sosyolojik bir bakış, *International Academic Social Resources Journal,* (e-ISSN: 2636-7637), Vol:7, Issue:33; pp:36-53.

Şentürk, F. & Kasap, M. (2013). Beyaz Yaka Suçları ve Finansal Yolsuzluklar. Çankırı Karatekin Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 3(2), 143-167.

Tabachnick, B. G., & Fidell, L. S. (2007). *Using multivariate statistics*,(5th ed.). New York: Allyn and Bacon.

Tezcan, D. (2019). Bilişim suçlarında uluslararası adli yardımlaşma, *Yaşar Hukuk Dergisi*, 1 (2).

Tonta, Y. (2018). Varyans Analizi (ANOVA), Kovaryans Analizi (ANCOVA), Faktöriyel ANOVA, Çoklu Varyans Analizi(MANOVA).

Turhan, O. (2006). Bilgisayar ağları ile ilgili suçlar. Uzmanlık Tezi, Devlet Planlama Teşkilatı, Ankara.

Van Eijk, G. (2017). Socioeconomic marginality in sentencing: The built-in bias in risk assessment tools and the reproduction of social inequality. *Punishment & Society*, *19*(4), 463-481.

Virtanen, S. V. (2017). Fear of cybercrime in Europe: examining the effects of victimization and vulnerabilities. *Psychiatry Pscyology and Law*, 24(3), 323-338.

Williams, M. L. (2016). Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level *The British Journal of Criminology*, 56(1), 21–48.

Yar, M. (2005). The novelty of 'cybercrime'an assessment in light of routine activity theory. *European Journal of Criminology*, 2(4), 407-427.

Yavuz, Y. (2019). Suç mağduru olma korkusuna sosyolojik bir bakış. *Toplum ve Kültür Araştırmaları Dergisi*, 4, 28-52.

Yazgan, Ç. Ü. (2017). Suç korkusu, içinde Ed. Güllüpınar, F. Suç Sosyolojisi, Eskişehir: Anadolu Üniversitesi Yayınları. s. 66-96.

Yazıcıoğlu, R. Y. (2008). "*Hukukumuzda TCK'nın 243'üncü madde kapsamında bilişim sistemine girme eylemi"* 9-10 Ekim 2008 Yargıtay Bilişim Hukuku Konferansı Yargıtay Başkanlığı Yayını, Ankara. S-81.

Yılmaz, Y. (2018) Siber suç korkusu ve önlem alma stratejileri: Ankara'daki teknokentler örneği. (Yayımlanmamış Yüksek Lisans Tezi). Hacettepe Üniversitesi, Ankara.

Yu, S. (2014). Fear of cyber crime among college students in the United States: An exploratory study. *International Journal of Cyber Criminology*, 8(1), 36.

European Commission. (2007). "Digital transformation", (Erişim tarihi: 11.03.2021)

https://ec.europa.eu/growth/industry/policy/digitaltransformation_en

UNODC, (2019) Cyberspionage.

https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-14/key-

(Erişim tarihi:12.03.2021)

https://magdurbilgi.adalet.gov.tr/298/Suc-Nedir) Erişim tarihi: 10.08.2022

Hiremath, S., Mutyal, P. & Bishnoi, S. (2019). 10 Cyber crime prevention tips. Erişim tarihi: 10.08.2022, https://pcpc.gov.in/files/1.pdf.

(https://berqnet.com/blog/truva-ati).(Erişim tarihi: 24.08.2022)

Tahancı, F. (2018). Sistemi engelleme, bozma, verileri yok etme veya değiştirme suçu TCK 244. Erişim tarihi: 12.08.2022, https://www.tahanci.av.tr/sistemi-engelleme-bozma-verileri-yok-etme-sucu/#sistemi-engelleme-bozma-verileri-yok-etme-veya-degistirme-sucu-tck-244.

Doğan, B. (2013). Banka veya kredi kartının kötüye kullanılması suçu nedir? Erişim tarihi: 18.09.2022, https://barandogan.av.tr/blog/ceza-hukuku/banka-veya-kredi-kartinin-kotuye-kullanilmasi-sucu-cezasi-tck.html)

Türkiye’de bilişim hukuku. (2019). Erişim tarihi: 20.09.22, https://internet.btk.gov.tr/turkiye-de-bilisim-hukuku

Siber ne demek? (2016). Erişim tarihi: 25.09.2022, https://www.nedir.com/siber

EGM, Siber suç nedir? (2022). Erişim tarihi: 04.10.2022, https://www.egm.gov.tr/siber/sibersucnedir()

Psikanaliz Sigmund Freud, (2022). Erişim tarihi: 15.07.2023, (https://acikders.ankara.edu.tr/pluginfile.php/133623/mod_resource/content/1/%2803%29%20Freud%20ve%20Psikanaliz.pdf

Sosyolojide nicel ve nitel araştırma yöntemleri, (2022). Erişim tarihi; 25.07.2023, https://www.bingol.edu.tr/media/204988/sayt-bolum8-Sosyolojide-Nicel-ve-Nitel-Arastirma-Yontemleri.pdf

Adli Sicil Ve İstatistik Genel Müdürlüğü, (2021). Adli istatistikler, Erişim tarihi: 07.06.23, https://adlisicil.adalet.gov.tr/Resimler/SayfaDokuman/31052022141642021H%C4%B0ZMETE%C3%96ZELK%C4%B0TAP.pdf9

Bilgisayar virüsü veya bilgisayar solucanı nedir? (2020). Erişim tarihi:17.09.2022, https://www.kaspersky.com.tr/resource-center/threats/viruses-worms

SİBERAY, Zararlı yazılımlar (casus yazılım,keylogger, botnet), Erişim tarihi: 02.12.2022, https://www.siberay.com/zararli-yazilimlar---2-casus-yazilim-keylogger-botnet.

İki faktörlü kimlik doğrulama, (2016). Erişim tarihi:02.12.2022

https://tr.wikipedia.org/wiki/%C4%B0ki_fakt%C3%B6rl%C3%BC_kimlik_do%C4%9Frulama.

İstanbul Bilgi Üniversitesi, Antivirüs programı nedir? (2021). Erişim tarihi: 04.12.2022, https://it.bilgi.edu.tr/tr/guvenlik/antivirus/#:~:text=Antivir%C3%BCs%20programlar%C4%B1%2C%20vir%C3%BCslere%20kar%C5%9F%C4%B1%20yaz%C4%B1lm%C4%B1%C5%9F,silmek%20i%C3%A7in%20%C3%A7e%C5%9Fitli%20y%C3%B6ntemler%20izler.

Sözüer, A. & Topçuoğlu, T. (2023). Kriminoloji 2 suç teorileri, Erişim tarihi:06.19.2023,https://slideplayer.biz.tr/slide/1944293/.

Türkiye'deki teknokentler listesi, (2023). Erişim tarihi; 25.07.2023, https://tr.wikipedia.org/wiki/T%C3%BCrkiye%27deki_teknokentler_listesi.

Gazi Üniversitesi Bilişim Enstitüsü, Bilişim sistemleri hakkında, (2021). Erişim Tarihi; 28.08.2023,https://be.gazi.edu.tr/view/page/286398/bilisim-sistemleri hakkinda#:~:text=Bili%C5%9Fim%20sistemleri%2C%20bilginin%20toplanmas%C4%B1nda%2C%20i%C5%9Flenmesinde,bilgisayarlar%20d%C3%A2hil%20b%C3%BCt%C3%BCn%20teknolojileri%20kapsar.

Bilişim suçları ve cezaları, (2023). Erişim tarihi: Erişim tarihi: 25.05.2023, https://kadimhukuk.com.tr/makale/bilisimsuclaricezalari/#:~:text=Bili%C5%9Fim%20sistemine%20girme%20su%C3%A7u%2C%20TCK%20madde%20243'te%20d%C3%BCzenlenmi%C5%9F%20olup,veya%20adli%20para%20cezas%C4%B1%20verilir.

https://yunus.hacettepe.edu.tr/~tonta/courses/fall2007/sb5002/sb5002-10-varyansanalizi.pdf.

Herkese açık wi-fi ağları güvenli mi? (2019). Erişim tarihi: 18.06.2023, https://berqnet.com/blog/halka-acik-kablosuz-aglara-dikkat-edin**.**

Arslan, K. (2018). Spss ile Mann Whitney U testi. Erişim tarihi: 24.09.2023 https://www.galloglu.com/blog/spss-mann-whitney-u-test.

EKLER

EK-1 Etik Kurul Onayı

Ek

Krl.İşl.:0590- -23/Krl.İşl.Ks.A.liği Haziran 2023

T.C.
İÇİŞLERİ BAKANLIĞI
Jandarma ve Sahil Güvenlik Akademisi Başkanlığı

ETİK KURULU KARARLARI

TOPLANTI NO : **2023/2**
TOPLANTI TARİHİ : 09 Haziran 2023 Cuma, saat 11.00
TOPLANTI YERİ : Fakülte Dekanlığı Toplantı Salonu.

TOPLANTIYA KATILANLAR : Akd.Bşk.Yrd. (Fakülte Dekanı) Prof.Dr. İ.Hakkı DEMİRCİOĞLU, J.Alb.Dr. Adnan ABDULVAHİTOĞLU, Dr.Öğr.Üyesi Ali YILDIRIM, Öğr.Gör.Dr. Kürşad GÜÇ, Dis. ve Huk.İş.Ş.Md. J.Huk.Yzb. Hakan BULDU.

TOPLANTIYA KATILMAYANLAR : Adli Bil.Enst.Md. Prof.Dr. G.İbrahim ÖĞÜNÇ.

1. JSGA'nın 2021-2022/1 sayılı Senato Kararı ile 14 Ekim 2021 tarihinde teşkil edilen Etik Kurulu 09 Haziran 2023 Cuma günü saat 11.00'de toplandı.
2. Toplantı yeter sayısının (5/6) bulunduğu tespit edildi.
3. Toplantı gündem maddelerinin görüşülmesine geçildi.

Gündem 7 - Yüksek Lisans Öğrencisi Elif HANBAY'a ait "Siber Suç Korkusu ve Önlem Alma Stratejileri: Trabzon Teknokent Örneği" isimli yüksek lisans tez çalışmasının değerlendirilmesi.

Karar 7 - Yüksek Lisans Öğrencisi Elif HANBAY'a ait "Siber Suç Korkusu ve Önlem Alma Stratejileri: Trabzon Teknokent Örneği" isimli yüksek lisans tez çalışması incelenmiş olup çalışmanın Bilimsel Araştırma ve Yayın Etiği yönünden bir sakıncasının olmadığına oy birliği ile karar verildi.

4. Gündem dışı görüşülecek bir konu olmaması üzerine Akd.Bşk.Yrd. (Fakülte Dekanı) Prof.Dr. İ.Hakkı DEMİRCİOĞLU tarafından 2'nci Etik Kurulu toplantısı sonlandırılmıştır. 09 Haziran 2023

(İMZALI)
Prof.Dr. İ.Hakkı DEMİRCİOĞLU
Akd.Bşk.Yrd. (Fakülte Dekanı)

(İMZALI) J.Alb.Dr. Adnan ABDULVAHİTOĞLU Öğr. Üyesi	(KATILMADI) Prof.Dr. G.İbrahim ÖĞÜNÇ Adli Bil.Enst.Md.	(İMZALI) Dr.Öğr.Üyesi Ali YILDIRIM Öğr. Üyesi
(İMZALI) Öğr.Gör.Dr. Kürşad GÜÇ Öğr. Gör.	(İMZALI) J.Huk.Yzb. Hakan BULDU Dis. ve Huk.İş.Ş.Md.	

EK-2. Kurum Uygulama İzni

TRABZON
TEKNOLOJİ GELİŞTİRME BÖLGESİ (TEKNOKENT)
Teknoloji ve yeniliğe Karadeniz'den yelken açın

Sayı : 2023-237
Konu : Tez Çalışması Hakkında

27 Nisan 2023

T.C. İÇİŞLERİ BAKANLIĞI
JANDARMA VE SAHİL GÜVENLİK AKADEMİSİ
GÜVENLİK BİLİMLERİ ENSTİTÜSÜ

71398025814 T.C. Kimlik Nolu Elif KURT **"Siber Suç Korkusu ve Önlem Alma Stratejileri: Trabzon Teknokent Örneği"** Başlıklı Tezi için oluşturduğu anket çalışmasını Teknokent'te yer alan firma çalışanları ile yapabilir. Bilgilerinize saygılarımızla arz ederiz.

JSGA'lı, Her Zaman Yurt, Ulus ve Cumhuriyete Aşk ve

Sadakatle Bağlı Tevazu, Fedakârlık ve Feragat Örneğidir