THE REPUBLIC OF TURKEY
BAHCESEHIR UNIVERSITY

A SERIOUS GAME STUDY ON RAISING AWARENESS TOWARDS SOCIAL MEDIA SECURITY

Master's Thesis

HAKAN ARPACI

ISTANBUL, 2020

REPUBLIC OF TURKEY

BAHCESEHIR UNIVERSITY

GRADUATE SCHOOL OF SOCIAL SCIENCES

GAME DESIGN MASTER PROGRAM

A SERIOUS GAME STUDY ON RAISING AWARENESS TOWARDS SOCIAL MEDIA SECURITY

Master's Thesis

HAKAN ARPACI

Supervisor: İBRAHİM ALTUĞ IŞIGAN

ISTANBUL, 2020

THE REPUBLIC OF TURKEY
BAHCESEHIR UNIVERSITY

INSTITUTE OF SOCIAL SCIENCES
BUSINESS ADMINISTRATION MASTER'S PROGRAM

Name of the thesis: A Serious Game Study on Raising Awareness Towards Social Media Security
Name/Last Name of the Student: Hakan Arpacı
Date of the Defense of Thesis:

The thesis has been approved by the Graduate School of Social Sciences.

Assoc. Prof. Burak KÜNTAY
Graduate School Director

I certify that this thesis meets all the requirements as a thesis for the degree of Master of Business Administration.

Asst. Prof. Dr. Güven ÇATAK
Program Coordinator

This is to certify that we have read this thesis and we find it fully adequate in scope, quality and content, as a thesis for the degree of Master of Arts.

Examining Comittee Members ________Signature____ _____

Thesis Supervisor ----------------------------------
Asst. Prof. İbrahim Altuğ IŞIĞAN

Thesis Co-supervisor ---------------------------------
Assoc. Prof. Barbaros BOSTAN

Member ----------------------------------
Asst. Prof. Dr. Güven ÇATAK

ACKNOWLEDGEMENTS

I would like to acknowledge and thank the following important people who have supported me, not only during the course of this study, but throughout my Master Degree.

Firstly, I would like to express my gratitude to my supervisor Asst. Prof. İbrahim Altuğ Işığan, for this unwavering support, guidance and insight throughout this study.

I would also like to thank Co-founder at HRİKa Solutions, Murat Aytun who provides me serious game and the platform.

Special thanks to all my close friends and my family. You have all encouraged and believed in me. You have all helped me to focus on what has been a hugely rewarding and enriching process.

And finally, I acknowledge my wife, Ceren, who always supported and motivated me throughout this entire process.

ÖZET

SOSYAL MEDYA GÜVENLİĞİNE KARŞI FARKINDALIĞI ARTTIRMAYA YÖNELİK CİDDİ OYUN ÇALIŞMASI

Hakan Arpacı

Oyun Tasarımı Yüksek Lisans Programı

Tez Danışmanı: Yard. Prof. İbrahim Altuğ Işığan

Mayıs 2020, 61 Sayfa

Teknolojinin gelişmesi ile birlikte bilgi güvenliği çok önemli bir konu haline gelmiştir. Buna bağlı olarak, sosyal medya platformlarının kullanımının yaygınlaşması hem bireylere hem de şirketlere zarar verebilen güvenlik riskleri ve tehditlerini de beraberinde getirebilmektedir. Günümüzde, hem işgücü hem de teknoloji meraklı popülasyonu temsil eden Y Jenerasyonu sosyal medya güvenliğine karşı en korunmasız grup olarak kabul edilebilir. Sosyal medya şirketleri ve BT departmanları sistem geliştirmelerini sağlamaktadır; fakat, insan tabanlı faktorleri azaltmak için farkındalık arttırmak gereklidir. Geleneksel yöntemlerle ve yetersiz uygulamalı örneklerle tasarlanmış birçok eğitim programı olmasına rağmen, güçlü öğrenme tekniklerini düşük bütçe ile sağlayabilen ciddi oyunlar gibi alternatif çözümler keşfedilebilmektedir.

Bu çalışmada, HRİKa Çözümler tarafından geliştirilen ve özel ayarların yetersiz düzenlenmesi, riskli talepler ve davetler, uygun olmayan iletişim ve hassas bilginin ortaya çıkması gibi sosyal medya güvenliği kazanımlarını öğretmeyi hedefleyen "Sentinel – Social Media" isimli bir çeşit ciddi oyun önerilmektedir.

Çalışmanın amacı, "Sentinel – Social Media" oyunu oynayan Y jenerasyonu beyaz yaka çalışanlarının öğrenme kazanımına önemli derecede etkisini göstermektir. Çalışma, öğrenme kazanımlarına yönelik etkinin incelenmesi için tek grup öntest sontest tasarımı ile hazırlanmıştır. Ek olarak, katılımcıların oyun deneyim puanları da analiz edilecektir.

Keywords: bilgi güvenliği, sosyal medya güvenliği, farkındalık, risk, tehdit, zaafiyet, ciddi oyun, oyun tabanlı öğrenme

ABSTRACT

A SERIOUS GAME STUDY ON RAISING AWARENESS TOWARDS SOCIAL MEDIA SECURITY

Hakan Arpacı

Game Design Master Program

Thesis Supervisor: Asst. Prof. Altuğ Işığan

May 2020, 61 Pages

Information security is becoming a very significant topic with the advancement of technology. Accordingly, increasing the usage of social media platforms could bring about security risks and threats which may damage both individuals and corporates. Today, Generation Y who represents both workforce and tech-savvy population could be acceptable as the most vulnerable group towards social media security. Many system enhancements are provided by social network companies and IT departments; yet, raising awareness is necessary in order to decrease human-based factors. Although many training programs which most of are designed by traditional methods and insufficient for practical examples are concerned, an alternative solutions could be discovered such as serious games which ensure more powerful learning techniques with a minimum cost.

In this study, it is proposed that “Sentinel – Social Media” is a kind of serious game developed by Hrika Solutions and aims to teach social media security objectives which includes; insufficient configuration of privacy setting, risky solicitation or invitation, inappropriate communication and disclosure of sensitive information.

The aim of the study is show the significant effect on the learning gains of white collar Generation Y workers who play “Sentinel-Social Media”. The study was prepared as one-group pretest-posttest design in order to investigate the effectiveness on learning gains. In addition to this, a game experience scores will be analyzed of the participants.

Keywords: information security, social media security, awareness, risk, threat, vulnerability, serious game, game based learning

CONTENTS

TABLES

FIGURES

ABBREVIATIONS

SE: Standard Error

GEQ: Game Experience Questionnaire

IS: Information Security

1. INTRODUCTION

1.1 BACKGROUND, MOTIVATION AND RESEARCH PROBLEM OF THE STUDY

References to information security in daily press and in popular periodicals are now numerous, but the variety of ideas as to raising an awareness towards information security is correspondingly extensive.

In recent years, human life have been influenced significantly through the development of internet and information technology. Such enhancements could bring about a secure environment for information, mainly personal and business areas. However, advanced technology may not meet the requirements of security; besides the technological faces, the human aspects of information security which are the lack of awareness, negligence, apathy and resistance should be taken into consideration. (Safa, et al., 2016)

Information security awareness becomes a part of today's digital world. People are connecting a lot of platforms which most of them are bound to each other and sharing information related to both personal and business. Shared data could be abused by people who desired to damage an individual or public. To illustrate this point, sharing a travel photo of user can give an idea to a thief that the user is away from home. In addition to this, a sensitive information about a company can make the network accessible and a hacker may acquire customer data. The examples could be increased but the idea is that the information security should be considered, especially related to human factors.

In business world, many organization set up rules and regulations regarding information security in order to assure the employees to be aware of. Awareness becomes an integral part of an information security management plan of the organizations. Many of them are planning training programs which mostly lack of focused learning and critical thinking. Therefore, it is not guaranteed that each person has understood and accorded the content of those programs; thus, it is necessary to support the programs through games, simulations and so on. (Khan, et al., 2011)

Social media platforms are one of the most popular information sharing environments among both people and organizations. In this digital age, most of the people become social media addicts and a lot of time is consumed for browsing different mediums throughout a day. According to a survey, internet users are logging in an average of 2 hours 22 minutes per day on social media and messaging platforms. (Salim, 2019) Especially, generation Y (called "millennials" as well) who are born between 1980 and 1995 exists within the structure of business life increasingly from day to day. (Cilliers, 2017) That generation has enormous power of using technology, the internet and social media platforms certainly. A study according to the relationship between social media and the workplace has demonstrated that 81% of millennials using Facebook every day and 25% of them accessing social media with mobile phones. (Rai, 2012) In addition to this, they are becoming business leaders who are increasing labor demand and working capacity. Therefore, it is necessary to enhance the awareness of such people about the risks and threats of technology except the advantages such as information security.

In social media, sharing personal and private information brings about risks and threats for both individuals and organizations because such information could be misused by some people who use technology in order to access unauthorized data. This phenomenon is expected to be prevented through system developments which are not effective completely and information security awareness programs covering many subtitles with traditional learning materials that are unable to present practices. (TOSUN, et al., 2020)

Security education is difficult because security concepts and models are mostly abstract and technical. Practical tools and materials could increase the effectiveness of learning. Moreover, lack of educator about social media security awareness could be stated as one of the problems regarding that issue. Therefore, it becomes a requirement to discover different sources or materials for having social media awareness. (Yasin, et al., 2015)

Serious games are becoming popular solution towards such educational problems. Serious game concept has been conducted in the field of marketing, business, medical applications and education. Many studies have concluded that game based learning does make a positive effect on the learning performance. Learners could explore multiple alternative ways without a fear of negative consequences or failure.

There are several researches about serious game design towards social media security awareness, which aimed to show the design framework and which focus on viruses and malwares with a target of children and teenagers. However, none exist in detail about the objectives which are insufficient configuration of privacy setting, risky solicitation or invitation, inappropriate communication and disclosure of sensitive information. In addition to the existing studies, it is also very important to include the relationship between social media and the workforce because the alternative ways has to be discovered in order to raise an awareness towards social media security in business areas. Generation Y is the common ground when the social media security and workforce collaboration is criticized. Taking into consideration above factors, it is aimed to find out the effectiveness of social media security awareness game on the learning gain of Gen Y. Accordingly, the research problem of this study was defined as "*Is there any significant difference between pre-test and post-test scores of those who play Sentinel - Social Media?*"

As a conclusion, this study aims to analyze the effectiveness of a serious game towards social media security awareness for 23 white collar millennials. Pretest and posttest were implemented in order to evaluate the learning gains of the subjects. In addition, game experience questionnaire was applied for the assessment of game experience score into seven components; immersion, flow, competence, positive and negative effects.

1.2 OVERVIEW OF THE STRUCTURE OF THE STUDY

The structure of the study is organized into the subcategories; literature review, data and methods, findings, discussion and conclusion. The national and international literature which are mostly recent and previously published and focused on information security awareness, social media security awareness, the important role of millennials in corporate companies and serious game concept are examined in literature review. In methodology part, the population and sample selection is clarified and the experimental procedure is explained. Regarding data collection, learning difficulties and misconceptions for social media security are discussed and game design specifications are clearly demonstrated. In addition to this, evaluation part including aim of the research and data collection methods is conducted. Findings section involves the result of analyzed data. Lastly, a final discussion related to the contribution of the study in both the scientific field as much as the business world composes the conclusion.

2. LITERATURE REVIEW

2.1 INFORMATION SECURITY AWARENESS

Information security can be defined as an emerging scientific discipline which needs multi domain strategy in order to operate the global security threat landscape. The attacks for stealing personal data are more sophisticated and increasingly continuing issue and the magnitude of effect they bring about create a new mastery. It is becoming more important to have scientific and practical knowledge to decrease the risk of encountering information security crime. In addition, information security awareness is not provided in most computer science curriculum in higher education or schools. A considerable amount of people are victimized relatively through malicious criminals even if major enterprises to extend awareness and propaganda to eliminate vulnerabilities have been made. Only a handful of private programs by the academia and renowned organizations obtain certification and basic skills in information security, resulting in a breakout to complement today's social need. (Raman, et al., 2014)

2.2 SOCIAL MEDIA SECURITY AWARENESS

Unawareness of certain threats or characteristics of social media cause a lot of risks which stem from the users’ actions in social media. The attackers often misuse personal data through phishing, identity thefts, reputation damage, leaking information and blurring of the audience in social media. Scams and phishing are the most common risks to convince the users. (Hekkala, et al., 2012)

It can be asserted that people can build identities, coordinate their relationships and interact with virtual environment through different kinds of information systems. Today, social network sites have become a crucial and important part of daily communication practices for millions of people. In addition to this, social network sites have the opportunity of maintain the identities of organizations and companies which mostly are corporate. Considerable amount of information are exchanged among individuals and organizations through social media. Therefore, information security is an increasingly significant issue of interest. (Hekkala, et al., 2012)

Nowadays, popular social networks such as Facebook, Twitter and LinkedIn have become one of the most affecting media and an important part of the online activities. The main purpose of these online social networks is to offer the users to connect, share and increasingly interact with their contacts through a wide variety of communication tools. It is necessary to create several accounts on various sites on which the users disclose personal information with varying degress of sensitivity in order to make use of the ensured functionalities and to stay tuned with their related members. The information which consists of different attributes like name, age, educational history, hobbies, photos and lists of contacts is stored within users' profile(s). (Raad, et al., 2016)

Such personal data can reveal information about the private lives and social relationships of the users. Even if the well-known social media companies make a great investments for personal data protection, the protection policies may fail to meet the requirements of the security of user data. Therefore, the attitudes and behaviors which means of awareness of the social media users have a great factor for the protection of personal data. (Raad, et al., 2016)

The survey results of Hootsuite and WeAreSocial companies in January 2019 demonstrated that the population of Turkey is 82.44 million and 59.36 million is the active internet users. The number of people accessing internet with mobile devices is 56 million and 84% of these people access the internet every day regularly. The same report also indicated that the number of social media users actively in Turkey is 52 million. The number of people who connect social media with mobile devices is 44 million. Turkey uses social media 2 hours 46 minutes daily on average. (TOSUN, et al., 2020) In addition to this, the average of social media accounts per person is 9.7. (wearesocial, 2020) Those figures clearly show that the usage of internet and social media in Turkey is at high rate. Therefore, the density of such usage of internet and social media in Turkey brings about a requirement to follow the developments about information security in the world and Turkey. Apart from this, raising an information security awareness about both internet and social media becomes very significant in order to inform the individuals about risks and threats that may be encountered in internet environment. (TOSUN, et al., 2020)

2.3 THE IMPORTANT ROLE OF GENERATION Y IN CORPORATE COMPANIES

Businesses are changing with the wave of emerging young professionals who have been started to join the workforce (often referred to as “Generation Y” or “Millennials”). It is predicted that they will engage about half of the workforce as of 2020, and approximately one third of it by 2025. (Oliver Wyman, 2016) Therefore, it is necessary to meet the specific needs of the young people for most corporates through raising awareness.

Generation Y is representing a group of people who born between 1980 and 1995. The group has grown up with the advancement of technology which mostly based on computers and the Internet. (Cilliers, 2017) This population has constituted relationships with technology and strongly understand its various uses. One of studies about the sensitivity of generations towards technology indicates that when the older generations are compared, this generation is considerably eager to use social networking sites and to create profiles. Another study focusing on the activities surrounding this generation demonstrates that 70% of them uses social networking sites and about 65% has an online profile. It is also discovered that the daily usage which includes sending messages or sharing information to friends is 63%. (Cabral, 2011)

It is mostly misunderstood that all members of Generation Y are qualified for the usage of computers and cell phones and even social media. It can be accepted at a certain level, but in most cases, they do not have enough knowledge about information security and this may give rise to serious problems. Information security awareness is not an innate ability because nobody is born with the ability of using the internet and social media. It is a skill that must be acquired in order to avoid from the risks and threats that can be faced with. (Nyikes & Baimakova, 2016) It should be emphasized that using the technology does not mean to be protected and education is one of the best option to raise an awareness.

The term “information security” represents the protection of information and information systems from the harmful actions such as; unauthorized access, disclosure, modification and destruction in order to ensure integrity, confidentiality and availability. Integrity means to protect against inappropriate modification or destruction and covers guaranteed information authenticity. Confidentiality infers to guard authorized limitations on access and disclosure and to protect personal privacy. Availability connotes to provide timely and trusted access to use of information. (Hekkala, et al., 2012)

Actually, as the technology conducted and advanced the vast majority of operations, information security has become a well-established part of business. It could be admitted that the human factor has an important role in information security. Therefore, companies which make great investments to protect IT systems and to decrease security risks should guaranteed that the employees have an adequate security awareness. (Ahmmed, 2019)

Today, the responsibility of information security is not only belonging to task management and information technologies department but also to people individually. This issue could be accepted for social media security as well. Therefore, many training programs which could be beneficial for preventing security vulnerabilities are planned through the related functions of companies. However, those programs are mostly designed by traditional learning methods and lack of practice. It is difficult to learn social media security awareness through the reflected powerpoint slides. Moreover, traditional training sessions which are mostly preferred in companies are estimated to be insufficient and difficult to complete because of the cost and logistics. Therefore, new learning methods should be considered in order to maintain more effective and easily accessible. (Ahmmed, 2019)

2.4 SERIOUS GAME CONCEPT

It has been considered that the traditional classroom teaching techniques are not sufficient to achieve problem solving skills and intended learning objectives. In this digital age where people, especially young people, mostly live online rather than offline, better mechanisms are needed to encourage interest in training programs such as information security. It is stated that the scientific community could not focused on the quality of research, while the quality of teaching is given little importance. The receptivity and retention of concepts could be improved significantly through activity based learning. (Raman, et al., 2014)

Most of the instructors who teach security subjects use the traditional way of teaching in the classroom and using some technologies such as website and presentation file to teach the learner. It is an obviously fact that traditional teaching ways are passive and not interactive. The learners may not imagine real situation or how it related to real life, therefore; it becomes hard to be interested enough in the subject. In addition to this, perception and imagination are required for the abstract nature of information security concept but one teaching way cannot be coherent for all learners. Therefore, it is necessary to integrate an additional mechanism to stimulate learner interest and engagement in such a course in this digital era where people are familiar with digital media. (Visoottiviseth, et al., 2018)

Apart from powerful learning tools that may cause an "instructional revolution", games and simulations begin to demonstrate having enormous potential. Analysis games in education are made and frameworks that allow learning methodologies to integrate game design process are constructed in order to have better learning experience. The effectiveness can be improved through increasing critical thinking while approaching problem solving and virtual environment that enable using visual and audial materials. A concrete experience within which pupils can interiorize domain specific concepts can be provided by games. Critical thinking skills of students could be developed and the feedback which is one of the most powerful element in active learning can be given immediately through games and simulations. (Cone, et al., 2007)

It could be advocated that the modern meaning of "serious games" has been suggested by Abt in 1970 and many researchers and professionals modified since then. The widely accepted definition was propounded by Zyda who introduced serious games as a mental contest that allows users to play with a computer in compliance with specific rules which includes entertainment to support education, corporate training, public policy, health and similar areas. However, it is a fact that the definition still continues to debate and limited by the authors based on their own needs. (Le Compte, et al., 2015)

Fundamentally, all serious games take advantage of in-game mechanisms in order to evaluate player performance and progress, for a proper response to the action of player. The games could produce a large set of user data which could help for monitoring and assessment objectives because they are interactive and complex software systems that usually integrate logical rules for assessing system responses. The level of the performance can be monitored through the actions of the user towards game challenges or contents. Positive and negative feedbacks can support the performance of the user as well as game flow. (Hauge, et al., 2014)

2. DATA AND METHODS

3.1 LEARNING DIFFICULTIES AND MISCONCEPTIONS

3.1.1 Learning Difficulties

Information security is unique because the concept of information security brings wide range of domains which are demonstrated in the table below. Therefore, it could be asserted that information security courses are not enough to learn through a two-hour lecture. It can be recommended that this kind of a course should be supported through a well-organized implementation tool such as courseware, serious game and so on. (Armstrong & Armstrong, 2007)

Table 3. 1: The Domains of Information Security

Access control systems and methodologies	Security architecture
Communications and network security	Operations security
Security management	Business continuity planning
Application software security	Law, investigation and ethics
Cryptography	Physical security

In any kind of organization in modern business environments, information security awareness is very essential but complex issue because the connections between consciousness and unconsciousness are complicated. The situation becomes more complex when it is considered that the possibilities of the collective consciousness and collective unconsciousness. (Anttila & Savola, 2007)

Awareness is difficult to define or locate, it includes some disagreements depending upon someone’s philosophical paradigm. Some have even disputed that it is intrinsically impossible to test an awareness empirically. (Anttila & Savola, 2007)

3.1.2 Misconceptions

Social media security is one of the most important issue when the information security is considered. It is directly related to the protection of personal data and being aware of the risks and threats that could be confronted every time using social media. Therefore, there are also misconceptions related to social media security which are depends on information security as well.

Most of people who are learning information security overgeneralize and build misconceptions by supposing that encryption is enough for additional properties beyond confidentiality such as; personal data protection, preventing manipulation and cyber-attacks, and ensuring availability. For instance, when asked how encryption can assist the security of a social media application, it is incorrectly stated that encryption prevented theft of the data and alteration; thus, confidentiality is protected. (Thompson, et al., 2018)

Some people advocated that the internet has vulnerabilities and it is mostly generalized by those people that it is not necessary to take precautions in order for maintaining information security. For example, cryptography can protect personal data and confidentiality in most of the applications while sending messages over insecure channels through using tools such as; encryption, digital signatures, hashing, virtual private networks (VPN) and so on. (Thompson, et al., 2018)

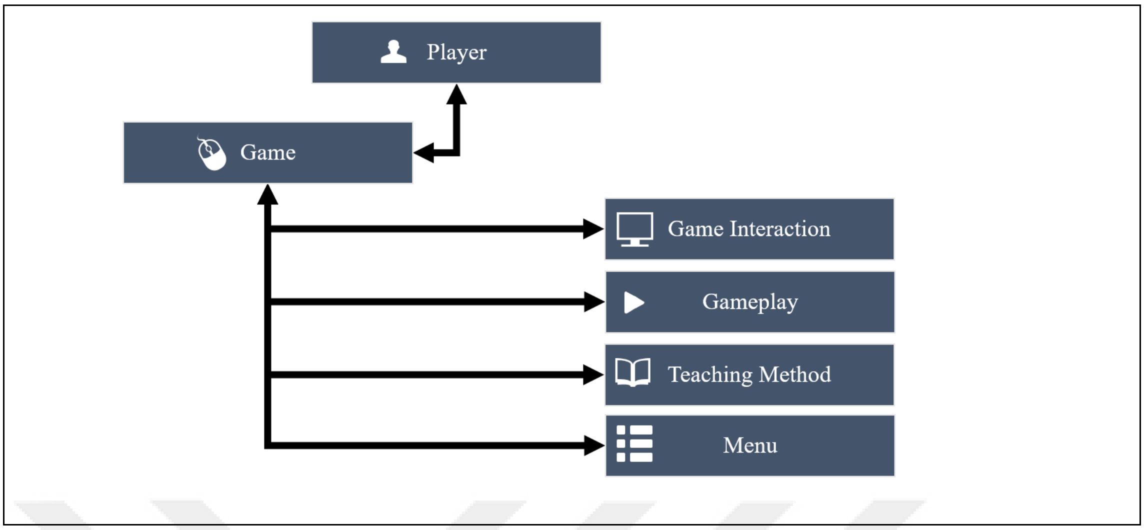
The internet can provide many services depending on each other through using personal data and the only requirement is creating awareness about information security.

In the context of information security, the term threat means a potential security breach, while the risk implies the possibility of an enemy taking advantage of this threat with potentially occurring loss (Bishop, 2003). On the contrary, in colloquial contexts, the idea of risk refers to any dangerous situation - if someone is driving without a seat belt, it may indicate that it is a risk. This concept of daily risk excludes the idea of taking into account the possibility of a threat occurring in the context of this driving, where a threat may include a drunk driver. (Thompson, et al., 2018)

3.2 GAME DESIGN SPECIFICATION

Sentinel – Social Media is a serious game and aims to raise an awareness about social media security. The game was developed by Hrika Solutions which mostly serves human resources solutions through serious games, web based games, web applications and etc.

Figure 3. 1: System architecture of “Sentinel – Social Media”

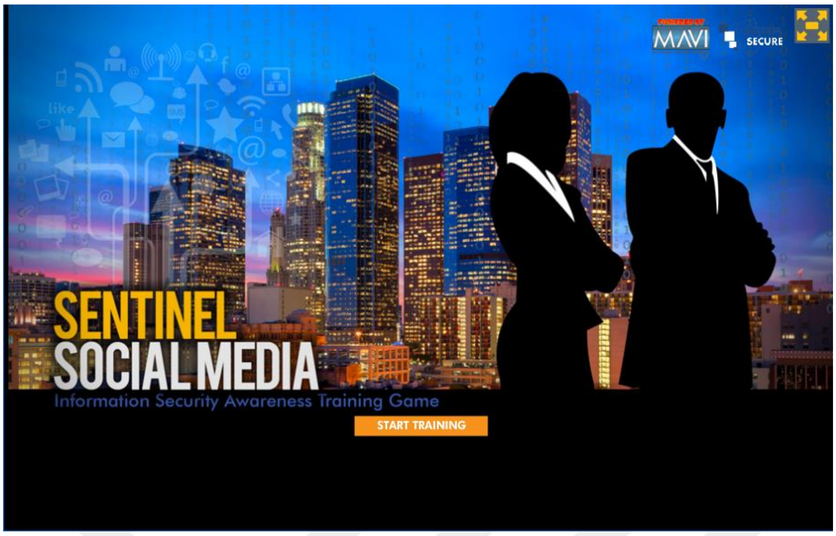


Sentinel – Social Media is a flash based game and it includes many resources to bind the story and objectives. It could be briefly demonstrated in Figure 3.1 that Sentinel – Social Media includes four main modules which are game interaction, teaching method, gameplay and the menu. The teaching system receives the interaction signal between the player and the system to perform the task in the game. Menu helps the player to pause the game, to check the objectives and to display missing elements. There are several screen captures that demonstrate the game and the structure.

The narrative of the game is basically that a social media security vulnerabilities for a company are founded and a sentinel who is protagonist of story is charged with a mission to investigate those vulnerabilities through examining the social media accounts (Facebook, LinkedIn and Twitter) of a sales manager who is the prime suspect of the company. The user is asked to examine social media risks and threats and categorize them in terms of the options below.

i. Insufficient configuration of privacy setting
ii. Risky solicitation or invitation
iii. Inappropriate communication
iv. Disclosure of sensitive information

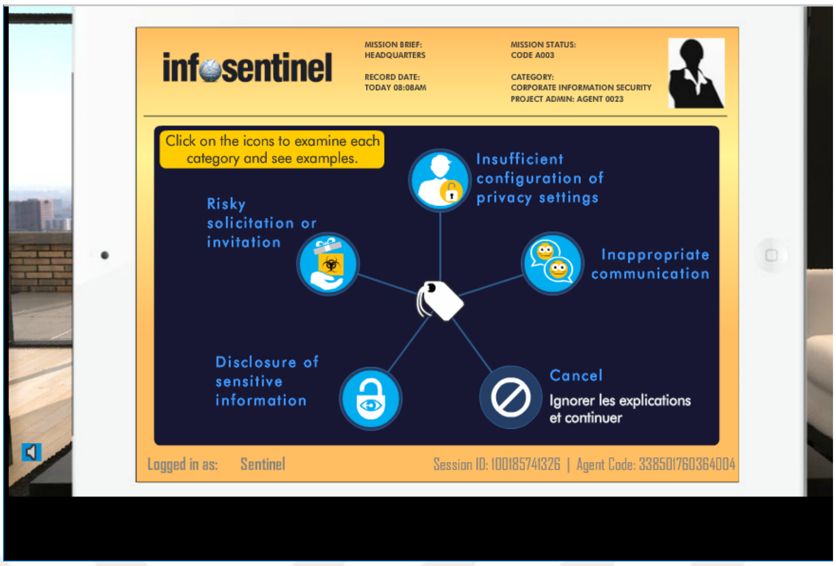
Figure 3. 2: Start Screen



In the beginning of the game, a visual presentation with a good sound raising the tension and the start screen appears. The user can click “Start Training” button to begin the game.

An incoming message is appearing and the user is asked to click the message. By doing this, the mission of the sentinel introduces by a well-designed video and the main categories for the examination of social media posts.

Figure 3. 3: Security vulnerability categories



infosentinel

MISSION BRIEF:
HEADQUARTERS

RECORD DATE:
TODAY 08:08AM

MISSION STATUS:
CODE A003

CATEGORY:
CORPORATE INFORMATION SECURITY
PROJECT ADMIN: AGENT 0023

Click on the icons to examine each category and see examples.

Insufficient configuration of privacy settings
Risky solicitation or invitation
Inappropriate communication
Disclosure of sensitive information
Cancel

Ignorer les explications et continuer

Logged in as: Sentinel

Session ID: 100185741326 | Agent Code: 338501760364004

In this screen, the user is wanted to click each category described below in order to understand the security vulnerabilities. Thus, the objectives of the game and the meaning of classification is clearly understood. Those four categories are described below.

Insufficient configuration of privacy settings: This category is related to the privacy setting of social network platform. The user can discover the insufficient setting and sign as this category.

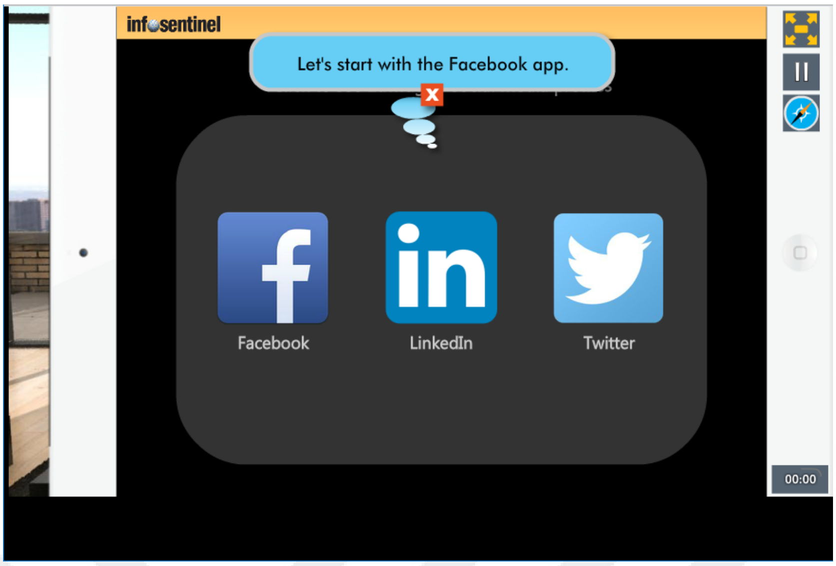
Risky solicitation or invitation: In social media platforms, it could be easy to send a request or invitation to each other which may cause a risk if it is wanted to misuse.

Inappropriate communication: This category indicates that the social media post could smear or insult someone or be a false information spreading among friends.

Disclosure of sensitive information: Social media users do not have enough attention to share the sensitive information both professional and personal lives. The sentinel tries to explore such sensitive information that could be bring about harmful actions.

The game continues with a screen that the user is asked to accept the mission. Thus, the playing starts.

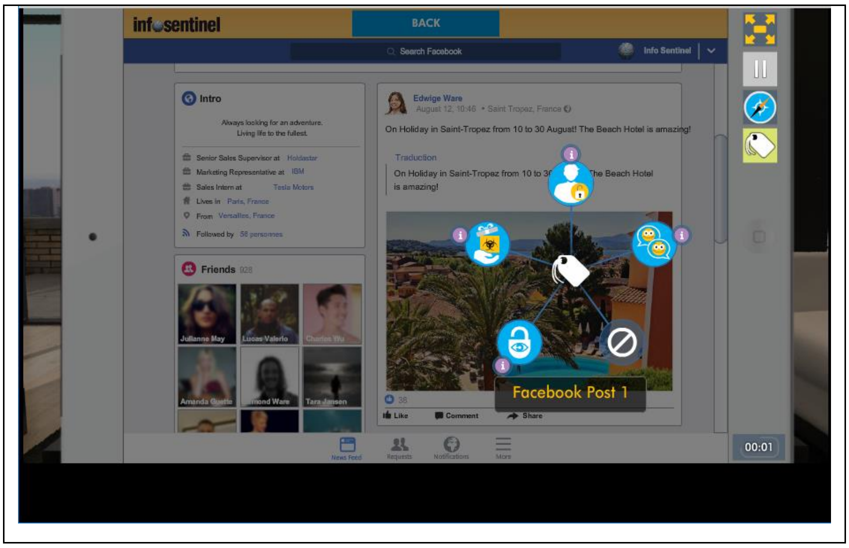
Figure 3. 4: Social media platforms



Let's start with the Facebook app.

The game presents 3 option to proceed. The user is free to choose social media platform to investigate first; yet, a feedback is also appears to help the user making a decision. The platform screens are explained orderly below.

Figure 3. 5: Facebook screen



Intro

Always looking for an adventure.
Living life to the fullest.

Senior Sales Supervisor at Holdastar
Marketing Representative at IBM
Sales Intern at Tesla Motors
Lives in Paris, France
From Versailles, France
Followed by 58 personnes

Edwige Ware
August 12, 10:46 • Saint Tropez, France

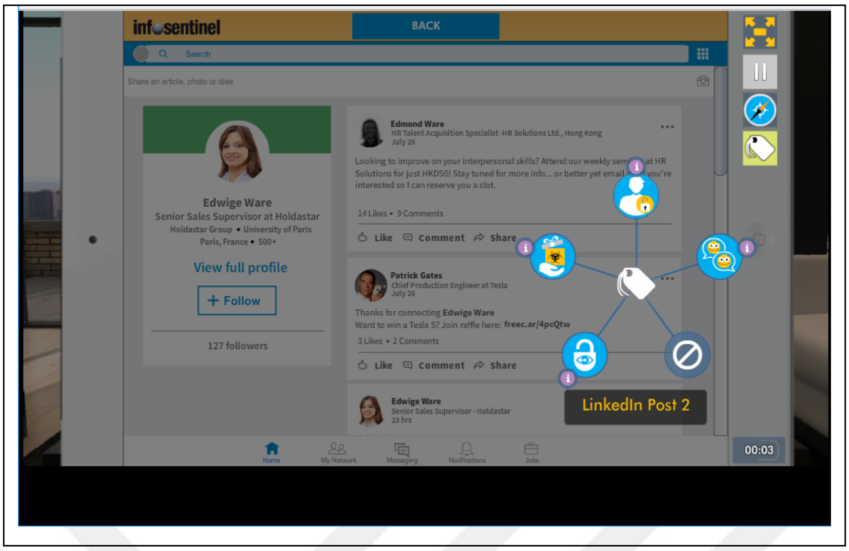
On Holiday in Saint-Tropez from 10 to 30 August! The Beach Hotel is amazing!

Traduction

On Holiday in Saint-Tropez from 10 to 3 The Beach Hotel is amazing!

Facebook screen is designed as similar as the real platform. The game user can analyze the profile and classify the posts or risky elements. It is not necessary to categorize all items that are shown in page; therefore, the player can also have more attention and understand the reason for an element including risk or not.

Figure 3. 6: LinkedIn screen



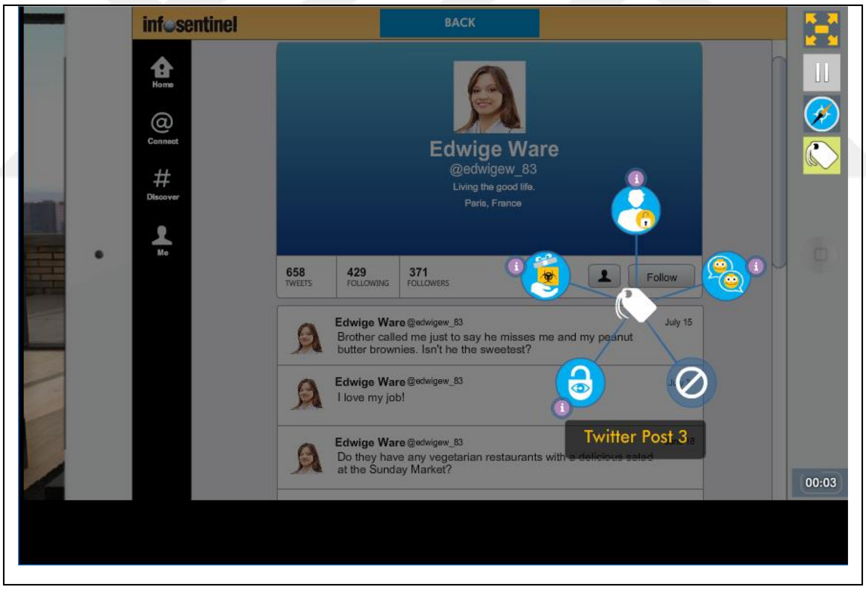
Edwige Ware
Senior Sales Supervisor at Holdastar
Holdastar Group • University of Paris
Paris, France • 500+
127 followers

Edmond Ware
HR Talent Acquisition Specialist -HR Solutions Ltd., Hong Kong
July 26
Looking to improve on your interpersonal skills? Attend our weekly semi at HR Solutions for just HKD50! Stay tuned for more info... or better yet email you're interested so I can reserve you a slot.
14 Likes • 9 Comments

Patrick Gates
Chief Production Engineer at Tesla
July 26
Thanks for connecting Edwige Ware
Want to win a Tesla S? Join raffle here: freec.ar/4pcQtw
3 Likes • 2 Comments

Edwige Ware
Senior Sales Supervisor - Holdastar
23 hrs

Figure 3. 7: Twitter screen



Edwige Ware
@edwigew_83
Living the good life.
Paris, France

658 TWEETS
429 FOLLOWING
371 FOLLOWERS

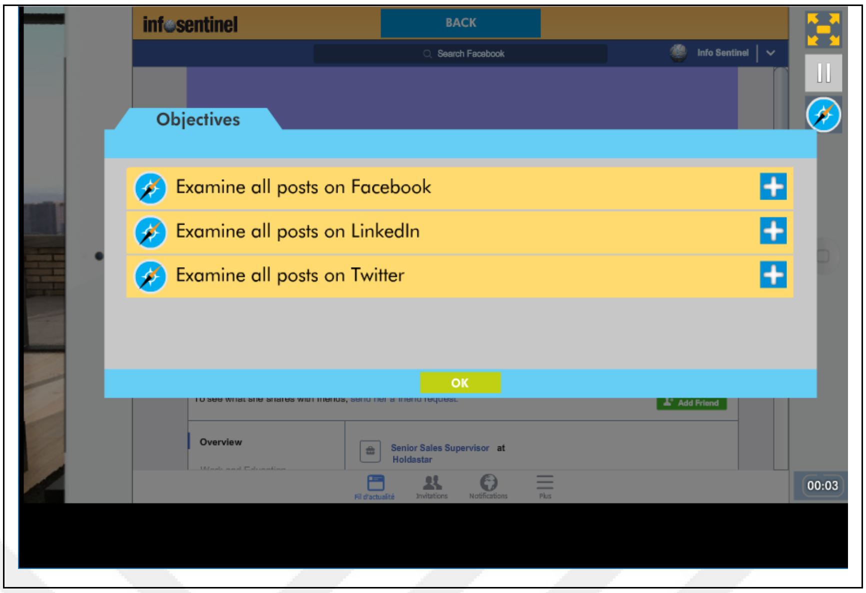
Edwige Ware @edwigew_83 July 15
Brother called me just to say he misses me and my peanut butter brownies. Isn't he the sweetest?

Edwige Ware @edwigew_83
I love my job!

Edwige Ware @edwigew_83
Do they have any vegetarian restaurants with a delicious salad at the Sunday Market?

LinkedIn and Twitter screens are also close to same to real one. Profile elements are shown consistently and the player can back to main screen.

Figure 3. 8: Objectives screen



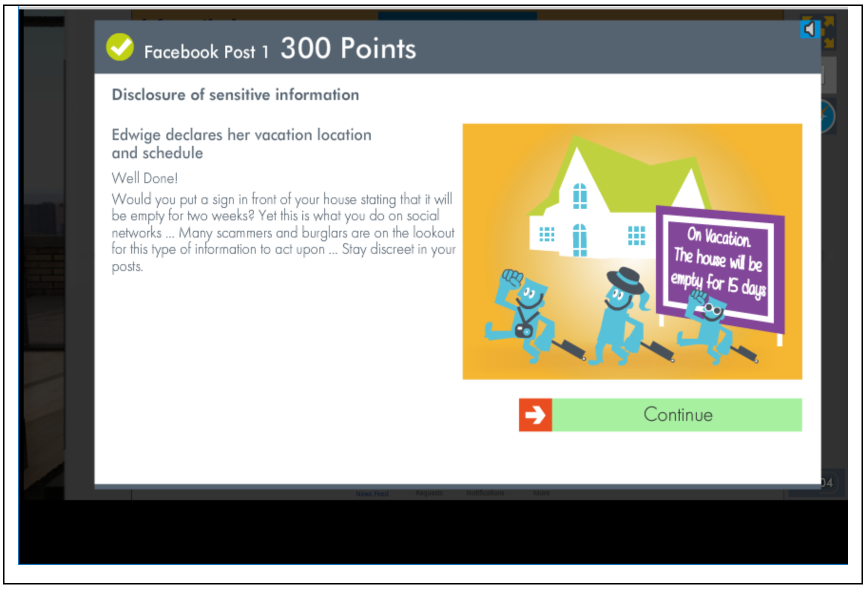
Objectives

- Examine all posts on Facebook
- Examine all posts on LinkedIn
- Examine all posts on Twitter

OK

The user can display the objectives and control the performance of playing the game. It enables the player to have an information about the number of items that should be labeled and the completion of each social media platform.

Figure 3. 9: Positive feedback screen



Facebook Post 1 300 Points

Disclosure of sensitive information

Edwige declares her vacation location and schedule

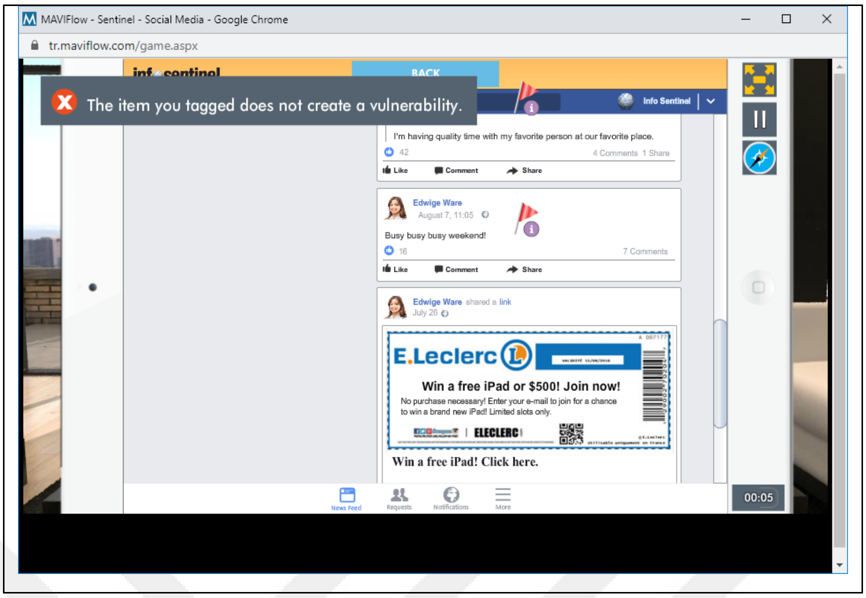
Well Done!

Would you put a sign in front of your house stating that it will be empty for two weeks? Yet this is what you do on social networks ... Many scammers and burglars are on the lookout for this type of information to act upon ... Stay discreet in your posts.

Continue

When the player tags an element as the right category, an immediate positive feedback is shown with an inspired text and image. The player can truly aware of the risk and threats through the description of those feedbacks.

Figure 3. 10: Negative feedback screen


MAVIFlow - Sentinel - Social Media - Google Chrome

tr.maviflow.com/game.aspx

The item you tagged does not create a vulnerability.

I'm having quality time with my favorite person at our favorite place.

Edwige Ware August 7, 11:05

Busy busy busy weekend!

Edwige Ware shared a link July 26

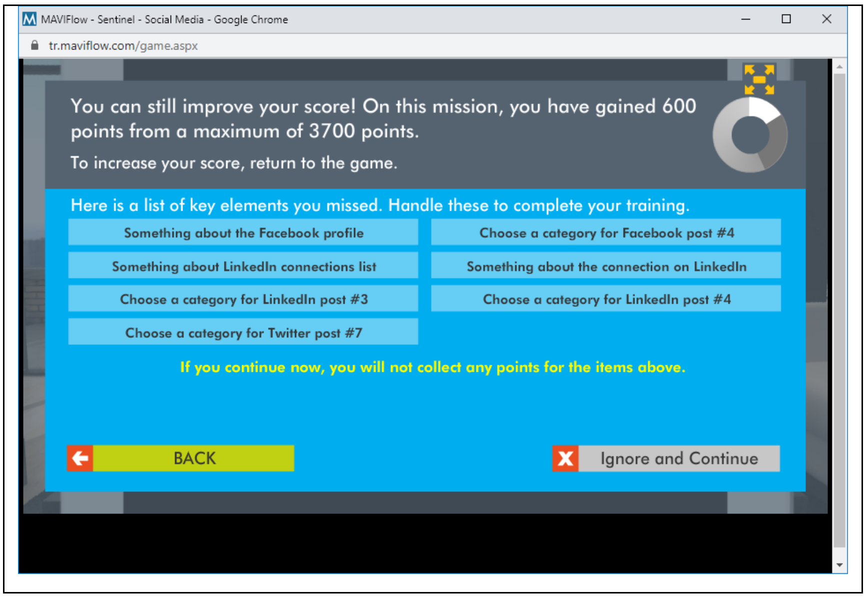
Win a free iPad or $500! Join now!

No purchase necessary! Enter your e-mail to join for a chance to win a brand new iPad! Limited slots only.

Win a free iPad! Click here.

The user could not find the right label for an element, a negative feedback appears with a simple and short way. Thus, the player can take the message of to be more careful; yet, the motivation loss may be decreased.

Figure 3. 11: General feedback screen


MAVIFlow - Sentinel - Social Media - Google Chrome

tr.maviflow.com/game.aspx

You can still improve your score! On this mission, you have gained 600 points from a maximum of 3700 points.

To increase your score, return to the game.

Here is a list of key elements you missed. Handle these to complete your training.

- Something about the Facebook profile
- Choose a category for Facebook post #4
- Something about LinkedIn connections list
- Something about the connection on LinkedIn
- Choose a category for LinkedIn post #3
- Choose a category for LinkedIn post #4
- Choose a category for Twitter post #7

If you continue now, you will not collect any points for the items above.

There is also a general feedback screen in the game. The player performance and the objectives are signified clearly to the user. The player could see the missing points and turn back to the mission in order to complete.

3.3 EVALUATION

3.3.1 Aim of the Evaluation Studies

The aim of the evaluation of this study is to be able to analyze that Sentinel - Social Media which is an information-security simulation game has an impact of raising an awareness for information security about social media platforms to those with little or no knowledge of the subject is presented. In addition, the possible suggestions which may occur during the evaluation will be obtained thus the lecturers can use the game as a learning tool.

3.3.2 Research Problems

The main objectives of this study can be clarified as asking the following questions.

- Is there any significant difference between pre-test and post-test scores of those who play “Sentinel - Social Media”?
- Is there any significant difference between learning gain scores and game experience scores of those who play “Sentinel – Social Media”?

3.3.3 Methodology

3.3.3.1 Population

The population of the study is whole Y generation of white collar workers in Turkey. According to labor market report in 2019 by Turkish Employment Agency, approximately 2.605.000 employees (20% of total employees) in Turkey are counted white collar workers and almost 43.417 of them (6% of white collar workers) are representing Y generation. (İŞKUR, 2019)

3.3.3.2 Sample

The sample of the study is 23 Y generation white collar workers in Turkey. The game participants will be selected from those who are meeting the criteria and are volunteered to take part in the study.

Table 3. 2: Demographic information of the sample

Category	Subcategory	Frequency	Ratio
Age	23-30	21	91%
	30-35	1	4%
	35-40	1	4%
Gender	Female	13	57%
	Male	10	43%
Education	Undergraduate	13	57%
	Postgraduate	10	43%
English Level	Advanced	16	70%
	Intermediate	7	30%
Job Sector	Accountancy, banking and finance	7	30%
	Information technology	5	22%
	Recruitment and HR	4	17%
	Engineering	2	9%
	Others	2	9%
	Marketing, advertising and PR	1	4%
	Science and pharmaceuticals	1	4%
	Teacher training and education	1	4%
Social Media Usage	1-2 hours	14	61%
	3-4 hours	8	35%
	More than 4 hours	1	4%
Device	Mobile Phone	22	96%
	Computer (desktop / laptop)	1	4%

According to the table, gender distribution of the sample is nearly equal with 13 female subjects and 10 male subjects. Moreover, 10 subjects have postgraduate grade and 13 subjects have undergraduate grade.

All of the subjects will be working in different sectors such as; accountancy, banking, finance, engineering, IT etc. The number of social media usage is mostly 1-2 hours with 14 subjects, 3-4 hours with 8 subjects and more than 4 hours with one subject.

The age discrimination of the subjects is shown in the table above. The subjects should be born in 1981 – 1996 years interval in order to be Y generation member. As seen, the most of the users are 23-30 years old and two users are distributed one by one for 30-35 years and 35-40 years.

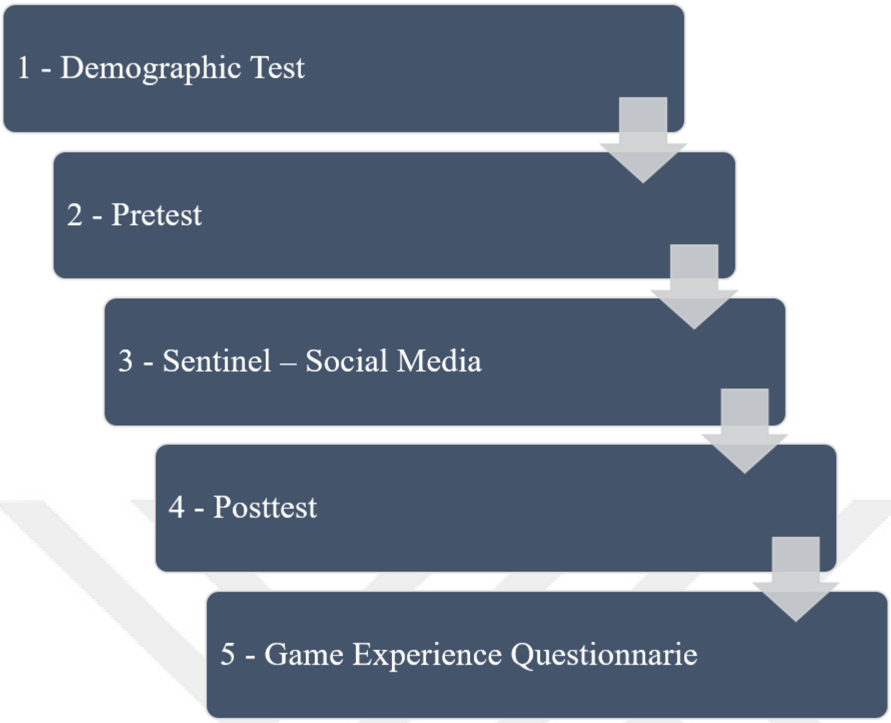
The job sectors of the subjects are mainly represented white collar employees who use digital communication in the business life. Thus, those sectors could be counted as one of the most threatened targets. Especially, information technology and accountancy, banking and finance are the most preferred target sectors for the hackers or attackers. Therefore, when the design and the objectives of “Sentinel – Social Media” is considered, it is recommended to be presented those employees in order to meet the requirements.

According to demographic data the subjects stated that each one has enough English language level because the instruments and the game are in English. In addition, all users except one pointed out that mobile devices are preferred in order to follow social media accounts. One user chooses to follow by computer (laptop/desktop).

3.3.3.3 Experimental procedure

This study employed Quasi-Experimental research design approach. 23 participants who are white collar workers between 24-39 ages representing Y generation were involved in this study. All the participants were required to play Sentinel – Social Media and also required to take pre-test and post-test in order to assess their achievement performance. In addition, a demographic test will be given to the subjects before pre-test section and GEQ will be given after post-test section.

Figure 3. 12: Experimental procedure


1 - Demographic Test
2 - Pretest
3 - Sentinel – Social Media
4 - Posttest
5 - Game Experience Questionnarie

All the participants will be informed through a well-designed e-mail in order to explain the experiment process step by step. The e-mails will be sent one by one because each person will be given a unique code to create an account on system before playing the game.

The whole experimental process is shown in Figure 3.12 above. First of all, the subjects are exposed to fill online demographic test which is designed as classical demographic survey questions related to age, gender, education level, language level, job sector, social media usage and the device type.

The pre-test includes 10 multiple choice questions to assess the participants’ knowledge in social media security principles and threats. The post-test also consists of 10 multiple choice questions each was designed as an equivalent of pre-test questions with that measures the knowledge in social media security awareness. The pre-test and post-test scores are analyzed by using two approaches; descriptive analysis and hypothesis evaluation.

3.3.4 Data Collection Tools and Methods

3.3.4.1 Qualitative data

Qualitative data will be mainly collected through the feedback and comments of those who will be subjected to playing the game after the experiment.

3.3.4.2 Quantitative data

Quantitative data will be collected through demographic survey, pretest, posttest and game experience questionnaire during the experiment.

Pretest consists of 10 multiple choice questions and each has 4 options. The questions were prepared according to the objectives of the game. It is aimed to assess the prior knowledge of the subjects about social media security risks and threats.

Similarly, posttest was prepared to include 10 multiple choice questions and each has 4 options. However, after the experiment, it was realized that one question (Question – 4) had been mistaken and it was canceled in evaluation part. Therefore, posttest includes 9 questions which aids to assess social media security awareness of the subjects after the experiment.

Game experience questionnaire is 5 items likert scale and is developed for FUGA project aiming to measure human experience of media enjoyment. The questionnaire consists of fourteen questions which represent seven components which are; competence, sensory and imaginary immersion, flow, tension, challenge, negative affect and positive affect. Component scores will be computed as the average value of its items.

Those questions are categorized under the following options:

- Not at all (1)
- Slightly (2)
- Moderately (3)
- Fairly (4)
- Extremely (5)

The Cronbach’ s Alpha score of the questionnaire varied between 0.693 and 0.80.

Quantitative data is necessary to test hypothesizes of the research to conclude about the functionality and success of Sentinel – Social Media. Data will be obtained from the pretest and posttest to calculate the users’ progress playing the game.

4. FINDINGS

4.1 TABULATION OF DATA

It is shown in the tables below that the pretest and posttest scores of each subjects are classified according to the correct and wrong answers.

4.1.1 Pretest Scores

The pretest scores are shown in the table below. Pretest consists of 10 questions and each correct answer is pointed as “1”. The wrong answers are shown with the symbol “-“ as this way makes easy to read the distribution of the answers.

Table 4. 1: Pretest scores of subjects

ID	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	TOTAL
1001	-	1,00	-	-	1,00	1,00	1,00	-	1,00	-	5,00
1002	1,00	1,00	1,00	1,00	1,00	-	1,00	1,00	1,00	1,00	9,00
1024	1,00	1,00	1,00	-	-	-	1,00	1,00	1,00	1,00	7,00
1016	1,00	1,00	1,00	1,00	-	-	1,00	1,00	1,00	1,00	8,00
1003	-	1,00	1,00	-	1,00	-	1,00	1,00	1,00	-	6,00
1004	-	-	-	-	1,00	-	1,00	1,00	1,00	1,00	5,00
1013	1,00	1,00	1,00	-	1,00	1,00	1,00	1,00	1,00	-	8,00
1009	1,00	1,00	1,00	1,00	1,00	1,00	1,00	-	1,00	-	8,00
1005	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	1,00	-	9,00
1006	1,00	1,00	1,00	1,00	1,00	1,00	-	1,00	1,00	1,00	9,00
1008	-	1,00	1,00	-	1,00	-	1,00	1,00	-	-	5,00
1007	1,00	1,00	1,00	1,00	1,00	1,00	1,00	-	1,00	-	8,00
1015	1,00	1,00	1,00	-	1,00	-	1,00	1,00	1,00	-	7,00
1018	-	1,00	1,00	1,00	1,00	-	1,00	-	1,00	-	6,00
1011	1,00	1,00	1,00	1,00	-	1,00	1,00	1,00	1,00	-	8,00
1012	-	1,00	1,00	-	1,00	1,00	1,00	1,00	1,00	1,00	8,00
1014	1,00	-	1,00	-	-	-	1,00	1,00	1,00	-	5,00
1022	1,00	1,00	1,00	-	1,00	-	1,00	-	-	-	5,00
1017	-	1,00	1,00	1,00	-	1,00	1,00	1,00	1,00	-	7,00
1019	1,00	1,00	1,00	1,00	-	-	1,00	1,00	1,00	-	7,00
1020	1,00	1,00	1,00	-	-	1,00	1,00	1,00	1,00	1,00	8,00
1021	1,00	1,00	1,00	-	1,00	-	1,00	1,00	-	-	6,00
1023	1,00	1,00	1,00	-	-	1,00	1,00	-	1,00	-	6,00
										AVERAGE	**6,96**

4.1.2 Posttest Scores

The posttest scores are shown in the table below. In the beginning of the study, posttest consists of 10 questions which shows to be equal to pretest question number. However, in the end of the study, it has been figured out that Q4 was mistaken and it was dropped from the posttest. In order to maintain the each correct answer is scored as the result of "10/9". The wrong answers of the subjects are shown with the symbol "-" as this way makes easy to read the distribution of the answers.

Table 4. 2: Posttest scores of subjects

ID	Q1	Q2	Q3	Q5	Q6	Q7	Q8	Q9	Q10	TOTAL
1001	1,11	1,11	1,11	1,11	-	1,11	1,11	1,11	1,11	8,89
1002	1,11	1,11	1,11	1,11	1,11	-	1,11	1,11	1,11	8,89
1003	1,11	1,11	-	1,11	1,11	1,11	1,11	1,11	1,11	8,89
1004	1,11	-	-	1,11	1,11	1,11	1,11	1,11	1,11	7,78
1005	1,11	-	-	1,11	1,11	1,11	1,11	1,11	1,11	7,78
1006	1,11	1,11	-	1,11	1,11	1,11	1,11	1,11	1,11	8,89
1007	1,11	-	-	1,11	1,11	-	1,11	1,11	1,11	6,67
1008	1,11	1,11	1,11	1,11	1,11	1,11	1,11	-	1,11	8,89
1009	-	-	-	1,11	1,11	1,11	1,11	1,11	1,11	6,67
1011	1,11	1,11	1,11	1,11	1,11	-	1,11	-	1,11	7,78
1012	1,11	1,11	-	1,11	-	-	1,11	1,11	1,11	6,67
1014	1,11	1,11	-	1,11	-	1,11	1,11	1,11	-	6,67
1015	1,11	1,11	1,11	1,11	1,11	1,11	1,11	1,11	-	8,89
1016	-	1,11	-	1,11	-	1,11	1,11	-	1,11	5,56
1017	1,11	-	1,11	1,11	-	-	1,11	1,11	1,11	6,67
1018	1,11	1,11	-	1,11	-	-	1,11	1,11	1,11	6,67
1019	1,11	-	1,11	1,11	1,11	1,11	1,11	1,11	1,11	8,89
1020	1,11	1,11	-	1,11	1,11	-	1,11	1,11	1,11	7,78
1021	1,11	1,11	-	1,11	-	-	1,11	1,11	1,11	6,67
1022	1,11	1,11	1,11	1,11	-	-	1,11	1,11	1,11	7,78
1023	1,11	1,11	1,11	1,11	1,11	-	1,11	1,11	1,11	8,89
1013	1,11	1,11	-	1,11	1,11	1,11	-	1,11	1,11	7,78
1024	1,11	1,11	1,11	1,11	-	1,11	1,11	1,11	1,11	8,89
									AVERAGE	**7,78**

4.1.3 Game Experience Scores

Game experience scores are obtained into 7 categories; sensory and imaginative immersion, negative affect, tension, competence, flow, challenge and positive affect. Each category is evaluated by unique two items and the total demonstrates game experience scores for “Sentinel – Social Media”.

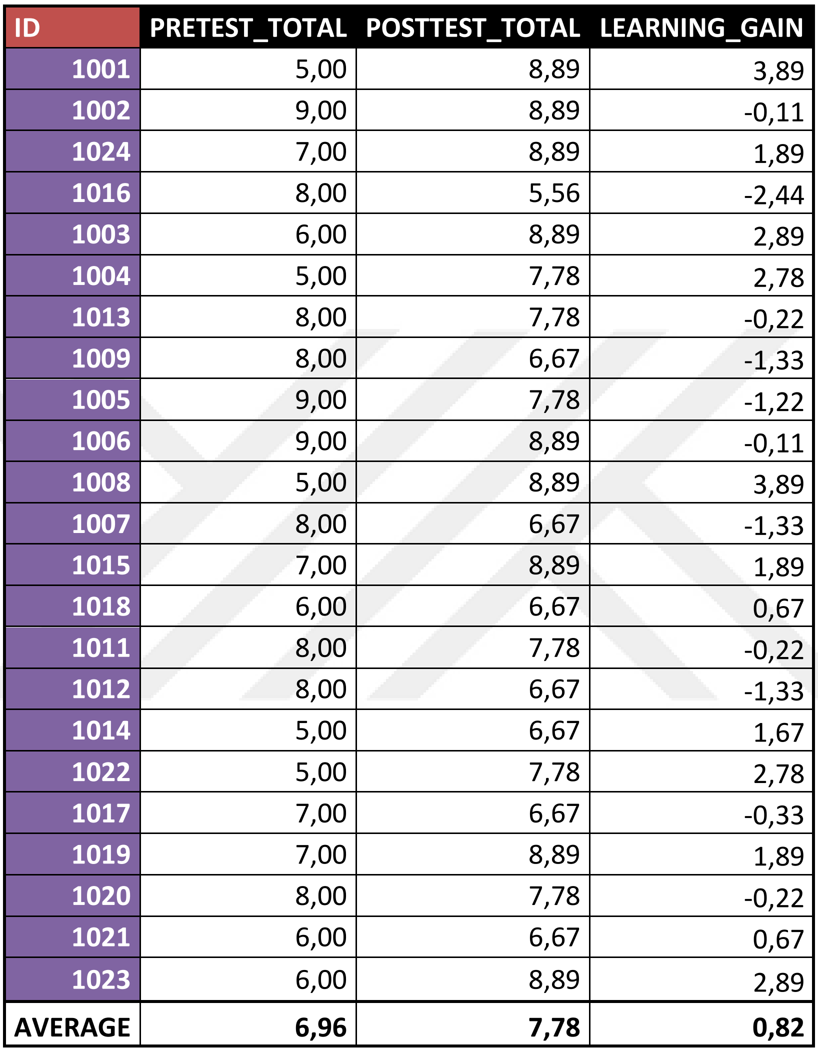
Table 4. 3: Game experience scores of subjects

	Sensory and Imaginative Immersion		Negative affect		Tension		Competence		Flow		Challenge		Positive affect		
ID	**Q1**	**Q4**	**Q3**	**Q7**	**Q6**	**Q8**	**Q2**	**Q9**	**Q5**	**Q10**	**Q12**	**Q13**	**Q11**	**Q14**	**TOTAL**
1001	4	4	3	2	2	2	4	5	2	1	5	5	5	5	**88**
1002	3	3	2	1	1	1	4	3	3	3	3	2	4	3	**65**
1003	5	5	1	1	1	1	5	5	5	3	5	2	3	5	**86**
1004	5	4	3	4	3	3	4	4	3	3	4	4	4	5	**97**
1005	5	5	1	1	1	1	5	5	5	5	5	5	5	5	**98**
1006	3	3	4	4	4	1	3	4	2	3	4	4	2	2	**82**
1007	4	4	2	4	1	1	5	3	4	3	5	3	5	5	**88**
1008	5	5	2	1	3	1	4	4	3	2	5	3	4	3	**83**
1009	3	3	3	4	3	3	4	4	3	3	4	3	3	4	**87**
1011	4	4	3	3	2	2	3	4	4	3	3	1	3	4	**79**
1012	4	4	2	1	1	1	3	2	3	2	4	3	4	4	**68**
1013	4	3	2	1	1	1	1	1	1	1	1	1	3	4	**43**
1014	5	4	1	1	3	1	4	4	3	4	4	3	5	5	**84**
1015	3	2	3	2	1	1	4	4	2	2	4	1	3	3	**64**
1016	5	5	1	1	1	1	5	5	3	1	3	3	5	5	**78**
1017	4	3	2	1	1	1	3	4	3	3	3	2	3	3	**66**
1018	5	5	3	4	3	1	1	5	1	4	2	5	5	5	**88**
1019	4	4	2	2	2	2	3	3	3	3	4	3	4	4	**78**
1020	5	5	1	1	1	1	4	4	4	4	5	5	5	5	**90**
1021	4	4	1	1	3	3	3	2	3	3	5	5	4	4	**82**
1022	5	4	1	1	1	1	4	4	4	3	4	3	3	4	**77**
1023	5	5	1	1	1	1	4	5	3	5	5	4	5	5	**90**
1024	4	3	4	4	2	3	3	2	3	3	3	4	3	2	**81**

4.2 LEARNING

4.2.1 Learning Gain

Table 4. 4: Learning gain scores of subjects



ID	PRETEST_TOTAL	POSTTEST_TOTAL	LEARNING_GAIN
1001	5,00	8,89	3,89
1002	9,00	8,89	-0,11
1024	7,00	8,89	1,89
1016	8,00	5,56	-2,44
1003	6,00	8,89	2,89
1004	5,00	7,78	2,78
1013	8,00	7,78	-0,22
1009	8,00	6,67	-1,33
1005	9,00	7,78	-1,22
1006	9,00	8,89	-0,11
1008	5,00	8,89	3,89
1007	8,00	6,67	-1,33
1015	7,00	8,89	1,89
1018	6,00	6,67	0,67
1011	8,00	7,78	-0,22
1012	8,00	6,67	-1,33
1014	5,00	6,67	1,67
1022	5,00	7,78	2,78
1017	7,00	6,67	-0,33
1019	7,00	8,89	1,89
1020	8,00	7,78	-0,22
1021	6,00	6,67	0,67
1023	6,00	8,89	2,89
AVERAGE	**6,96**	**7,78**	**0,82**

The data obtained from sample group was analyzed to determine whether or not there is a significant difference between pretest and posttest scores of students. In order to determine which tests can be used to compare pretest and posttest mean scores, it is required to look at the normal distribution of the scores obtained in both tests.

Table 4. 5: Tests of Normality for Learning Gain scores

Descriptives				
			Statistic	Std. Error
LEARNING_GAIN	Mean		0,8235	0,38309
	95% Confidence Interval for Mean	Lower Bound	0,0290	
		Upper Bound	1,6180	
	5% Trimmed Mean		0,8264	
	Median		0,6700	
	Variance		3,375	
	Std. Deviation		1,83722	
	Minimum		-2,44	
	Maximum		3,89	
	Range		6,33	
	Interquartile Range		3,11	
	Skewness		**0,118**	**0,481**
	Kurtosis		**-1,101**	**0,935**

4.2.2 The Difference Between Pretest and Posttest Scores

Table 4. 6: Descriptives of Pretest & Posttest Scores

Descriptives				
			Statistic	Std. Error
PRETEST_TOTAL	**Mean**		6,9565	0,29137
	95% Confidence Interval for Mean	**Lower Bound**	6,3523	
		Upper Bound	7,5608	
	5% Trimmed Mean		6,9517	
	Median		7,0000	
	Variance		1,953	
	Std. Deviation		1,39734	
	Minimum		5,00	
	Maximum		9,00	
	Range		4,00	
	Interquartile Range		2,00	
	Skewness		**-0,135**	**0,481**
	Kurtosis		**-1,307**	**0,935**
POSTTEST_TOTAL	**Mean**		7,7800	0,22068
	95% Confidence Interval for Mean	**Lower Bound**	7,3223	
		Upper Bound	8,2377	
	5% Trimmed Mean		7,8336	
	Median		7,7800	
	Variance		1,120	
	Std. Deviation		1,05834	
	Minimum		5,56	
	Maximum		8,89	
	Range		3,33	
	Interquartile Range		2,22	
	Skewness		**-0,345**	**0,481**
	Kurtosis		**-1,144**	**0,935**

Although the distribution from a visual display is concerned as the ability to describe, it has been founded by researchers that it is difficult to understand the shape of distribution when numerical statistics are compared such as the mean and median. Therefore, the measurement of skewness and kurtosis become more important. (Doane & Seward, 2011)

According to descriptive analysis of pretest and posttest, it could be claimed that test scores are approximately normally distributed with a skewness of -,135 (SE = ,481) and a kurtosis of -1,307 (SE = ,935) for the pretest scores and a skewness of -,345 (SE = ,481) and a kurtosis of -1,144 (SE = ,935).

Even if the distribution of data is not normal and non-parametric test will be used or if the distribution of data is normal and parametric test will be used.

As a result, we need to use parametric tests in order to determine whether there is a significant difference between pretest and posttest means. For this, Paired Samples T-test in parametric tests was used.

Table 4. 7: Paired Sample Statistics of Learning Gain Scores

Paired Samples Statistics					
		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	**PRETEST_TOTAL**	6,9565	23	1,39734	0,29137
	POSTTEST_TOTAL	7,7800	23	1,05834	0,22068

Paired Samples Test									
		Paired Differences					**t**	**df**	**Sig. (2-tailed)**
		Mean	**Std. Deviation**	**Std. Error Mean**	**95% Confidence Interval of the Difference**				
					Lower	**Upper**			
Pair 1	**PRETEST_TOTAL - POSTTEST_TOTAL**	-0,82348	1,83722	0,38309	-1,61795	-0,02900	-2,150	22	**0,043**

According to the result of Paired Samples T-test, there is a significant difference between pretest and posttest scores, t (22) = -2,15, p < .05, with the mean scores in posttest higher than the pretest scores as seen the table above. For these reasons, the null hypothesis which is claiming that there is no significant difference between pre-test and post-test scores of those who play Sentinel – Social Media was rejected and the alternative hypothesis which is claiming that there is a significant difference between pre-test and post-test scores of those who play Sentinel – Social Media was accepted. The meaningful difference is in the direction of posttest scores.

4.2.3 The Relationship Between Learning Gain and Game Experience Scores

In order to examine the relationship between learning gain and game experience scores, it is necessary to analyze the descriptives of data.

The descriptives table demonstrates that learning gain scores are approximately normally distributed with a skewness of ,073 (SE = ,687) and a kurtosis of -1,554 (SE = 1,191) for the subjects who are satisfied to play the game and a skewness of -,126 (SE = ,687) and a kurtosis of -,897 (SE = 1,334) for the users who are not satisfied to play the game. Therefore, independent samples test was applied to analyze the data.

Table 4. 8: Descriptives of Pretest & Posttest Scores

Descriptives					
				Statistic	Std. Error
LEARNING_GAIN	Satisfactory	Mean		1,1646	0,54206
		95% Confidence Interval for Mean	Lower Bound	-0,0164	
			Upper Bound	2,3457	
		5% Trimmed Mean		1,1518	
		Median		0,6700	
		Variance		3,820	
		Std. Deviation		1,95444	
		Minimum		-1,33	
		Maximum		3,89	
		Range		5,22	
		Interquartile Range		3,61	
		Skewness		**0,073**	**0,616**
		Kurtosis		**-1,554**	**1,191**
	Unsatisfactory	Mean		0,3800	0,52642
		95% Confidence Interval for Mean	Lower Bound	-0,8109	
			Upper Bound	1,5709	
		5% Trimmed Mean		0,4033	
		Median		-0,1650	
		Variance		2,771	
		Std. Deviation		1,66470	
		Minimum		-2,44	
		Maximum		2,78	
		Range		5,22	
		Interquartile Range		2,47	
		Skewness		**-0,126**	**0,687**
		Kurtosis		**-0,897**	**1,334**

According to the group statistics of learning gain scores compared with the game experience, it could be seen that the mean of the satisfaction is higher with 13 users than the 10 users who preferred the game is not satisfied.

Table 4. 9: Group Statistics of Learning Gain

Group Statistics					
1		N	Mean	Std. Deviation	Std. Error Mean
LEARNING_GAIN	Satisfactory	13	1,1646	1,95444	0,54206
	Unsatisfactory	10	0,3800	1,66470	0,52642

It is obviously shown in the independent samples test results table below that significance value with a number of ,380 is higher than confidence interval (p >,05) for the Levene' s test for equality of variances, thus, equal variances is assumed. In regard to the t-test for equality of means, the significance value with a number of ,321 is higher than confidence interval (p>,05) which means that there is not a significant difference between the learning gain scores and game experience scores.

Table 4. 10: Independent Samples Test Results

Independent Samples Test									
	Levene's Test for Equality of Variances		t-test for Equality of Means						
								95% Confidence Interval of the Difference	
	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	Lower	Upper
Equal variances assumed	0,803	0,380	1,016	21	0,321	0,78462	0,77221	-0,82128	2,39051
Equal variances not assumed			1,038	20,727	0,311	0,78462	0,75562	-0,78803	2,35727

Therefore, it could be said that the learning gain scores do not depend upon the game experience scores of the users.

5. DISCUSSION AND CONCLUSION

Advanced technology brings about new risks and threats as well as various advantages. The most considerable one of those is information security awareness. Accordingly, increasing social media usage and high percentage of unawareness towards sharing personal data could make people vulnerable for the security risks and threats.

Due to information security awareness, in the business world companies are embarking on a quest for creative ways to discover a solution for raising an awareness to the employees. On the contrary of traditional learning methods which are ineffective for active participants and unadaptable for having practices, serious games become prominent for using as a learning material recently. “Sentinel – Social Media” is one of the most useful serious games through social media security framework and specific learning objectives.

This study mainly aimed that a serious game named “Sentinel – Social Media” has a significant influence on social media security awareness on those who play the game. The study sample was chosen from the people who represented Generation Y in today’s digital age and white collars of business which means the main consumers of digital communication.

The findings from both descriptive analysis and hypothesis evaluation suggested that H01 was substantiated. It showed that there is a significant improvement in terms of social media security awareness between pretest and post test scores of those who play “Sentinel – Social Media”. Thus, it could be concluded that a meaningful difference on learning gain of the participants are observed after playing the serious game. This finding suggests that serious games could be beneficial learning materials in order to raise an awareness towards social media security. Hence, this study concludes that “Sentinel – Social Media” has potential to increase learning gain of player regarding social media security.

Furthermore, the game experience scores of the subjects were collected in order to analyze the effectiveness of game experience towards learning gain. According to the evaluation of the data, it is obviously demonstrated that there is not a significant difference on learning gain of the game experience score of the users. This mean that, game experience does not have a role on learning gain.

In addition to all considerations above, it is essential to ascertain the limitations, strengths and recommendations in order to make the research beneficial for the future contributions. Those are determined through the researcher during the whole process of study.

One of the main limitations of the study is that there is no singular company who specializes in developing a serious game conducted social media security in Turkish. Therefore, language barrier could be prevent a clear understanding of materials when the learning gain is observed. Moreover, “Sentinel – Social Media” is flash based game and it may be broken by the web browsers which withdraw the support for flash. For this reason, some participants could not play the game and not complete the posttest as well. Final limitation could be the number of the participants. Increasing the number of subjects could ensure more effective results in order to generalize the study.

Online platforms were very helpful during the study. The participants played the game by Maviflow which is a learning management system supplied by HRİKa Solutions and completed the tests through online test tools. Thus, it was easy to complete entire experimental process for the participants and to follow the procedure for the researcher.

Future work will focus on improving different experimental design for this kind of study. It could be more effective to implement the game with appropriate set of skills for different level of expertise, and therefore cover a larger range of participants. Research will also be conducted on alternative contents in serious games. Finally, a proof of concept will be designed for a case study in order to refine and validate the framework.

As a conclusion, “Sentinel – Social Media” is an effective serious game for raising an awareness towards social media security. Research conducted could be a good evidence for both using “Sentinel – Social Media” as a learning material or reinforcer and the importance of serious games with a specific objectives. Researchers in the future can investigate the effectiveness of serious games in security related objectives or different subjects.

REFERENCES

Books

Hauge et al. 2014. Implications of Learning Analytics for Serious Game Design Proceedings - *IEEE 14th International Conference on Advanced Learning Technologies*, ICALT 2014, pp. 230-232, IEEE Computer Society

Le Compte, A., Elizondo, D. & Watson, T., 2015. A renewed approach to serious games for cyber security.*7th International Conference on Cyber Conflict: Architectures in Cyberspace,* pp. 203-216, NATO CCD COE Publications

Periodicals

Cabral, J., 2011. Is Generation Y Addicted to Social Media?. The Elon Journal of Undergraduate Research in Communications, **2** (1), pp. 5-14.

Cilliers, E., 2017. The challenge of teaching generation Z. PEOPLE: International Journal of Social Sciences, **3** (1), pp. 188-198.

Cone, B. D., Irvine, C. E., Thompson, M. F. & Nguyen, T. D., 2007. A video game for cyber security training and awareness. computers & security **26** (1), pp. 63-72.

Doane, D. P. & Seward, L. E., 2011. Measuring Skewness: A Forgotten Statistic?. Journal of Statistics Education, **19** (2), pp. 1-18.

Khan, B., Alghathbar, K. S., Nabi, S. I. & Khan, M. K., 2011. Effectiveness of information security awareness methods based on psychological theories. African Journal of Business Management, **5** (26), pp. 10862-10868.

Raad, E., Bouna, B. A. & Chbeir, R., 2016. Preventing sensitive relationships disclosure for better social media preservation. International Journal of Information Security, **15** (2), p. 173–194.

Rai, S., 2012. Engaging young employees (Gen Y) in a social media dominated world Review and Retrospection. Procedia - Social and Behavioral Sciences, **37** (1) pp. 257-266.

Safa, N. S., Solms, R. V. & Furnell, S., 2016. Information security policy compliance model in organizations. Computer & Security, **56** (1), pp. 70-82.

Tosun et al. 2020. A swot analysis to raise awareness about cyber security and proper use of social media: İstanbul Sample. International Journal of Curriculum and Instruction, **12** (special issue), pp. 271-294.

Yasin et al. 2015. Improving Software Security Awareness Using A Serious Game. The Instution of Engineering and Technology, **13** (2), pp. 1-12.

Other Sources

Ahmmed, N. M. A., 2019. An Evaluation of Targeted Security Awareness for End Users, University of Plymouth.

Anttila, J. & Savola, R., 2007. Fulfilling the Needs for Information Security Awareness and Learning in Information Society.

Armstrong, C. J. & Armstrong, H. L., 2007. Mapping information security curricula to professional accreditation standards. West Point, NY, USA, IEEE.

Hekkala, R., Väyrynen, K. & Wiander, T., 2012. Information Security Challenges Of Social Media For Companies, ECIS.

Nyikes, Z. & Baimakova, K. V., 2016. An Examination of the Relationship between Security Awareness and Digital Competence. Bitola, FICT.

Oliver Wyman, 2016. What role for HR in 2020-2025? https://www.oliverwyman.com/content/dam/oliverwyman/global/en/2016/june/What%20role%20for%20HR%20in%202020-2025.pdf [retrieval date April 2020].

Raman, R., Lal, A. & Achuthan, K., 2014. Serious Games based approach to cyber security,

Salim, S., 2019. Digital Information World. [Çevrimiçi] https://www.digitalinformationworld.com/2019/01/how-much-time-do-people-spend-social-media-infographic.html [retrieval date May 2020].

Thompson et al. 2018. Student Misconceptions about Cybersecurity Concepts: Analysis of Think-Aloud Interviews. *Journal of Cybersecurity Education, Research and Practice*, 2018.

Visoottiviseth et al. 2018. Lord of Secure: the Virtual Reality Game for Educating Network Security. *Nakhonpathom, 2018 Seventh ICT International Student Project Conference* (ICT-ISPC).

wearesocial, 2020. wearesocial. https://wearesocial.com/digital-2020 [retrieval date April 2020].

İŞKUR, 2019. *İŞKUR.* https://media.iskur.gov.tr/34629/turkiye.pdf [retrieval date May 2020].

APPENDICES

APPENDIX-1: Demographic Test

1 - Gender?

a. Female

b. Male

2 – Age?

a. 23 – 30

b. 30 – 35

c. 35 – 40

d. 40+

Educational Qualification?

a. High School

b. Undergraduate

c. Postgraduate

English language level?

a. Beginner

b. Pre-Intermediate

c. Intermediate

d. Advanced

Which job sector are you working for?

a. Accountancy, banking and finance

b. Business, consulting and management

c. Creative arts and design

d. Energy and utilities

e. Engineering

f. Environment and agriculture

g. Healthcare

h. Hospitality and events management

i. Information technology

j. Law

k. Leisure, sport and tourism

l. Marketing, advertising and PR

m. Media and internet

n. Recruitment and HR

o. Science and pharmaceuticals

p. Teacher training and education

q. Transport and logistics

r. Others

How many hours do you use social media in a day?

a. Never use

b. 1 – 2 hours

c. 3 – 4 hours

d. More than 4 hours

With which device do you use the social media more than others?

a. Computer (desktop / laptop)

b. Tablet PC

c. Mobile Phone

APPENDIX-2: Pre Test

Which of the following is not a risk about social media security?

a. To give to charities who ask for money
b. To accept friend requests without being selective
c. To make personal account public
d. To share an information from a trusted source

Which of the following is an example for disclosure of sensitive information?

a. A photo of you that includes your ID card on a table
b. A link in your post that connects to a harmful webpage
c. A document about best places to travel in your post
d. A music file that you melodized last night

Which of the following has higher risk than others?

a. Profile picture
b. Personal information
c. Username
d. Common posts

Which of the following could be accepted as confidential information in social media?

a. Sharing a logo of the company you are working for
b. Sharing a news content on the website of the company you are working for
c. Sharing an e-mail content about celebration of your birthday of the company you are working for
d. Sharing the campaign announcement of the company you are working for

Which one is true regarding the posts on social media when you think information security?

a. My social media posts don't hurt me.
b. My social media posts are securely stored.
c. There is no threat to my social media posts.
d. My social media posts make me traceable and follow-up.

Which of the following does not threat personal information?

a. Social media photos
b. Social media friends
c. Social media username
d. Social media invitations

Which of the following can be threatened from the posts in our social media account?

a. Social media posts do not threat anyone.
b. Social media posts just threat me.
c. Social media posts can threat me and all other people in my account.
d. Only public accounts can be threatened.

Which of the following is TRUE when you faced with a scam shared by your friend?

a. Click the post to understand why your friend shared it.
b. Do nothing and continue to look other posts.
c. Sharing the post in order to be aware your other friends.
d. Tag the post as a spam and inform your friend and the platform.

Which of the following is TRUE regarding social media security?

a. Sharing your locations with dates when you are in travel.
b. Sharing your company e-mail which celebrates your anniversary.
c. Sharing your travel memories with only your close friends.
d. Sharing a post that you found on your friend's account and link to get free travel campaign.

Which of the following categories is related for the responsibility for spreading false information, or for smearing or insulting others?

a. Disclosure of sensitive information
b. Risky solicitation or invitation
c. Insufficient configuration of privacy settings
d. Inappropriate communication

APPENDIX-3: Post Test

Which of the following is a risk about social media security?

a. To accept friend requests after selection and control
b. To share the holiday plan at the weekend
c. To click sharing links after making sure
d. To make personal account private

Which of the following is an example for disclosure of sensitive information?

a. A post about common news that could be fake in your country
b. A photo of you in which your desktop screen at back
c. A post about book list that you read last month
d. A video link of your best football player from trusted source

Which of the following has more risk than others?

a. Personal (direct) message
b. E-mail address
c. School experience
d. Hobbies

Which of the following could be accepted as a threat in social media? (CANCELED)

a. Using the same password on all personal social media accounts
b. Making social media posts on public
c. Communicate / interact with people you don't know through your personal social media accounts
d. Making social media posts only visible to your own friends and not contain personal, sensitive data through your personal social media accounts

Which of the following is correct for the posts on social media and other internet platforms?

a. Social media platforms make us traceable and traceable.
b. Nobody can reach the social media posts we make.
c. The social media posts we make are exclusively for us.
d. There is no threat from social media platforms.

Which of the followings is usually not kept private on social media?

a. Photos
b. Username
c. Shared posts
d. Invitations

How should you make your social media account private and secure?

a. By tagging friends always
b. By using security applications
c. Doing password protect
d. Going offline discontinuously

What should be done when you see a social media post offering free iPhone by your friend?

a. Click the link to get free iPhone
b. Tag the post as a spam and inform your friend and the platform.
c. Setup an antivirus application to your computer or mobile device
d. Share the post in your account in order to get your friends iPhone too

Which of the following is TRUE regarding social media security?

a. All social media sharings should be public
b. All social media sharings should be private
c. Sensitive sharings on social media should be private
d. Sensitive sharings on social media should be public

Which of the following is an example for inappropriate communication if social media security is concerned?

a. Sharing a widely spreading post that is not from trustworthy source
b. Sharing a campaign post of well known mobile phone
c. Sharing a historical place information to travel
d. Sharing a post to request to donate blood for a best friend's operation

APPENDIX-4: Game Experience Questionnaire

Instruction: Please indicate how you felt after you finished playing the game for each of the items, on the following scale:

Items	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
I was interested in the game's story.					
I felt successful.					
I felt bored.					
I found it impressive.					
I forgot everything around me.					
I felt frustrated.					
I found it tiresome.					
I felt irritable.					
I felt skilful.					
I felt completely absorbed.					
I felt content.					
I felt challenged.					
I had to put a lot of effort into it.					
I felt good.					

THE REPUBLIC OF TURKEY
BAHCESEHIR UNIVERSITY

A SERIOUS GAME STUDY ON RAISING AWARENESS TOWARDS SOCIAL MEDIA SECURITY

Master's Thesis

HAKAN ARPACI

ISTANBUL, 2020