Cyber Security Behavior of IT Students: An Example of EMU

Sijuwonuola Tolu Lawal

Submitted to the
Institute of Graduate Studies and Research
in partial fulfillment of the requirements for the degree of

Master of Science
in
Information and Communication Technologies in Education

Eastern Mediterranean University
February 2021
Gazimağusa, North Cyprus

Approval of the Institute of Graduate Studies and Research

Prof. Dr. Ali Hakan Ulusoy
Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science in Information and Communication Technologies in Education.

Prof. Dr. Ersun İşçioğlu
Chair, Department of Computer Education and Instructional Technologies

We certify that we have read this thesis and that in our opinion it is fully adequate in scope and quality as a thesis for the degree of Master of Science in Information and Communication Technologies in Education.

Prof. Dr. Ersun İşçioğlu
Supervisor

Examining Committee

1. Prof. Dr. Ersun İşçioğlu

2. Asst. Prof. Dr. Fahme Dabaj

3. Asst. Prof. Dr. Damla Karagözlü

ABSTRACT

Due to technological innovations, the world has changed and everything such as information is easily accessible in electronic and digital format. This has revealed the importance of the concept of cyber security. The main purpose of this thesis is to examine the cyber security behaviors of Eastern Mediterranean University (EMU) Information Technology (IT) undergraduate students. In the study, cyber security behaviors were examined according to 5 sub-dimensions: malware, password usage, phishing, social engineering, and online scam. In addition, this study determines the relationship between cyber security behavior of IT students and their gender. Cyber Security Behavior (CSB) Scale (Muniandy, Muniandy, & Samsudin, 2017) was used as a data collection tool in the research. The study was carried out using the quantitative research method and survey model. Participants of the study consisted of 255 IT undergraduate students who enrolled at EMU in the spring semester of 2018-2019.

The results of this research show that IT undergraduate students have generally low cyber security behaviors. In addition, when all sub-dimensions were evaluated, it was determined that IT undergraduate students had low cyber security behaviors in the sub-dimensions of malware, password usage, social engineering, and online scam. Only, IT undergraduate students had high cyber security behavior in the phishing sub-dimension. In addition, IT undergraduate students had the lowest cyber security behavior in the social engineering sub-dimension, and the highest cyber security behavior in the phishing sub-dimension. Subsequently, the findings of this research show that a significant difference exists between IT students' cyber security behavior

and their gender. Male IT undergraduate students demonstrated higher cyber security behaviors than female's IT undergraduate students in 6 Items, while female IT students demonstrated higher cyber security behaviors than male IT students in 2 Items out of 50 items.

Keywords: cyber security, cyber security behavior, malware, phishing, online scam, social engineering.

ÖZ

Özellikle teknoloji alanında yaşanan yenilikler nedeniyle tüm dünyada hızlı değişimler oluşmaktadır. Günümüzde bilgiye elektronik ve dijital formatta kolayca erişilebilir bir ortam oluşmuştur. Bu gelişmeler, siber güvenlik kavramının önemini de ortaya çıkartmıştır. Bu tez çalışmasının temel amacı, Doğu Akdeniz Üniversitesi (DAÜ), Bilgi Teknolojileri (BT) lisans programı öğrencilerinin siber güvenlik davranışlarının incelenmesidir. Çalışmada, öğrencilerin siber güvenlik davranışları, 5 alt boyuta (kötü amaçlı yazılım, parola kullanımı, kimlik avı, sosyal mühendislik ve çevrimiçi dolandırıcılık) göre incelenmiştir. Ayrıca bu çalışmada bir diğer amaç olarak, BT öğrencilerinin siber güvenlik davranışları ile cinsiyetleri arasındaki ilişki de araştırılmıştır. Araştırmada veri toplama aracı olarak, Siber Güvenlik Davranış (CSB) Ölçeği (Muniandy, Muniandy ve Samsudin, 2017) kullanılmıştır. Çalışma nicel araştırma yöntemi temel alınarak ve tarama modelinden yararlanılarak gerçekleştirilmiştir. Çalışmanın katılımcılarını, DAÜ'de 2018-2019 bahar döneminde kayıt yaptıran 255 BT lisans öğrencisi oluşturmuştur.

Çalışma sonucunda, BT lisans öğrencilerinin genel olarak düşük siber güvenlik davranışlarına sahip olduğu belirlenmiştir. Ayrıca, tüm alt boyutlar açısından değerlendirildiği zaman, BT lisans öğrencilerinin kötü amaçlı yazılım, parola kullanımı, sosyal mühendislik ve çevrimiçi (e-) dolandırıcılık alt boyutlarında düşük siber güvenlik davranışlarına sahip oldukları, kimlik avı alt boyutunda ise siber güvenlik davranışlarının yüksek olduğu tespit edilmiştir. Ek olarak, BT lisans öğrencilerinin sosyal mühendislik alt boyutunda en düşük siber güvenlik davranışına sahip olduğu, çevrimiçi (e-) dolandırıcılık alt boyutunda ise en yüksek siber güvenlik

davranışına sahip olduğu görülmüştür. Ayrıca, bu araştırmanın bulguları arasında, BT lisans öğrencilerinin siber güvenlik davranışları ile cinsiyetleri arasında da bir fark olduğunu ortaya koyulmuştur. Toplam 50 maddeden oluşan CSB ölçeğinin, 2 maddesinde kadın BT lisans öğrencilerinin daha yüksek siber güvenlik davranışı sergilediği belirlenirken, 6 Madde de erkek BT lisans öğrencilerinin daha yüksek siber güvenlik davranışları gösterdiği tespit edilmiştir.

Anahtar Kelimeler: siber güvenlik, siber güvenlik davranışı, kötü amaçlı yazılım, kimlik avı, çevrimiçi dolandırıcılık, sosyal mühendislik.

DEDICATION

Those close to your heart have a great influence on the performance of your work because of the effort, motivation and prayer they put into it

My dedication goes to God for the strength, my mother for the prayers, my family for the support and my friend for the belief.

ACKNOWLEDGEMENT

This thesis becomes a reality with the kind support and help of many individuals and one special friend. My sincere thanks goes to all of them.

My deep gratitude goes to my supervisor for his immeasurably support and guidance in the preparation of this thesis.

A big thank you to my mother for her love and prayers. I would also love to appreciate my sisters for their support as well.

I also want to appreciate the love of my life for the undying love and trust. Waking up with me at night just to encourage me to do more. I would never have done this alone if not for her support.

TABLE OF CONTENTS

LIST OF TABLES

Chapter 1

INTRODUCTION

The internet is considered as one of the many advancements developed through technological innovations. According to Sternstein (2016), the internet has affected various sectors in our everyday lives. Emeka and Nyeke (2016) defined the internet as a huge computing network connecting millions of smaller machines, on various websites in millions of companies, political agencies, educational institutions, families, friends and others. Moreover, the internet has made access to millions of information easier (Černá & Poulová, 2012).

The Internet is a worldwide community with active users all around the world actively engaged in using the internet for multiple purposes. In academia, the internet plays a crucial role in the teaching and learning process (Virtič, 2012; Trojovská & Trojovsky, 2012). More so, the internet is considered as a revolutionary prospect in tertiary institutions, particularly in countries where accessing information by the mass population remains a problem (Agbo & Igwebuike, 2016). Moreover, it is without a doubt that the emergence of the internet has brought a modernized way of creating and sharing information into digital format with nearly infinite amount of information, freely distributed, and open to people in various parts of the world (Kortjan, 2013; Kumar & Kaur, 2006). Nevertheless, the internet, which is considered as a global computer network that communicates through a set of agreed upon rules for

exchanging information between users known as the protocol, is known as the backbone of cyber security (Ivwighreghweta & Igere, 2014).

Von Solms and Van Niekerk (2013) referred to cyber security as a set of resources, procedures, principles, protocols, activities, best practices, and innovations utilized to ensure the security of the users and their information in the cyberspace. Abomhara and Køien (2015) also referred to cyber security as synonymous with network security or internet security that concern the protection of data on electronic or digital devices such as smartphones, computers, servers and also internet, while, Hill (2015), gave a detailed definition of cyber security as a protection of devices or internet against unauthorized access and hackers that may damage or alter files, information, data, etc. connected to the internet. Various benefits of cyber security as outlined by researchers are protecting devices from cyber-threats, identifying and preventing fraudulent activities, protecting sensitive information, and creating awareness for users on the various cyber threats (Cavelty, 2010; Tarter, 2017; Rahman, Malaysia, Sairi, Zizi, & Khalid, 2020).

Every device needs to be protected at all time to ensure that sensitive information cannot be accessed by people with ill intent. In cyber security, information refers to any data considered sensitive or insensitive and varies from one user to another or from device to device (Hill, 2015). According to Gunduz and Das (2020), computer system usage and reliance on internet and other smart devices, are always susceptible to cyber-attacks, which makes awareness on cyber-security and threats associated with cyber security useful and crucial when dealing with information systems.

According to Leszczyna (2018), when the cyber security of a device or system is low, the system is considered as compromised and has higher risks of exposure to being infected by virus, hacked, accessed by unauthorized users, or exposed to cyber threats. Moreover, when such situations arise, it is assumed that the cyber security behavior of the user is insufficient, hence they are defenseless and not able to protect themselves against such malicious threats (Rubio, Alcaraz, Roman, & Lopez, 2019).

According to Bergner (2011) as quoted from Ossorio (2006), behavior is considered as an observable and apparent activity carried out by humans, animals, or other living things, which shows how they act or interact in situations.

Cyber security behavior as defined by various researchers is characterized as the knowledge, security practices and measures utilized by users in a cyber-environment that ensures their data or information is protected, and that cyber-threats online are mitigated or neutralized to ensure their safety (Aliyu, Abdallah, Lasisi, Diyar, & Zeki, 2010; Hamudin & Ariffin, 2014; Muniandy, Muniandy, & Samsudin, 2017). Practicing good cyber security behavior online ensures that user passwords are strong and protected from key loggers, the system is hostile to infection, and firewalls are set up to enable the detection of threats and preventing them (Ramendran, 2014). Ertan, Denny, and Jensen (2020) measured the cyber security behavior of users based on their adherence to security policies, phishing or email behaviors, and password behavior. In addition, researchers Shah and Argawal (2020) stated that good cyber security behaviors are practiced by ensuring safety of devices and add-on utilities; staying away from dangerous behaviors and practices; and ensuring preventive behaviors and practices are adhered to. Moreover, Flores, Farid, and Samara (2019) indicated that cyber security behavior of students should be measured in respect to

online scam, phishing, malware, password usage, social engineering, malware and data handling.

The Cyber Security Behavior (CSB) includes malware, password usage, phishing, social engineering, and online scam according to Muniandy, Muniandy, and Samsudin (2017). Idika and Mathur (2007) defined malware based on the earlier definition provided by Vasudevan and Yerraballi (2006) as malicious software such as trojans, worms, virus etc., attached to applications, emails, files, for the purpose of causing harm to the device, stealing information, stealing funds, or disrupting the functionality of the system. In reference to cyber security behavior, passwords are considered as the first action of defense against attackers, therefor password usage are the security practices or measures taken by users when creating or using their passwords on devices or websites to ensure security of their information such as including alpha numeric cases in passwords to ensure it is strong or using passwords longer than 7 characters (Kovačević, Putnik, & Tošković, 2020). Workman (2008) defined phishing as tactical attempt made by hackers pretending to be real business by sending emails or luring their victims to click on hyperlinks as a means of getting their victims to give them their sensitive information. Social engineering in terms of cyber security are mental manipulations of victims by attackers of attackers posing as people of authority so they can infiltrate their victims data, carry out certain illegal actions, or trick their victim into proving them with certain private information (Abass, 2018). In cyber security, online scams or internet fraud as defined in the works of Buchanan and Whitty (2014) are fraudulent criminal activities carried out by scammers under false pretenses by establishing a form of relationship either business, friendship, or romance with their victims by creating fake account with fake pictures for the purpose of luring their victims, offering false services, and gaining the trust of their victims before

manipulating them into sending monetary gifts or hacking into their accounts to steal vital information.

Senthilkumar and Easwaramoorthy (2017) conducted a study in Tamil Nadu on college students for investigating their cyber security behavior based on several security threats. The findings of their research demonstrated that majority of college student at Tamil Nadu have moderately high levels of cyber security behavior in regards to identifying and protecting themselves against multiple dangerous cyber issues.

Researchers Rabon and Syiemlieh (2018) examined the behavior and awareness of high school students on cyber-crimes in Social Networking Sites (SNS). The aim of their research was to discover if a relationship exists between sports and non-sports students based on the awareness and behaviors on cyber-crimes in SNS. Their results indicated that non-sports students have higher levels of awareness and behaviors towards cyber-crimes than the sports students counter parts.

Flores, Farid, and Samara (2019) conducted a research on the cyber security behavior of University students at United Arab Emirates (UAE). The aim of their research was to discover the level of cyber security behavior of the students based on malware, password usage, data handling, phishing, social engineering and online scam by utilizing the E- Security Behavior Survey Instrument (EBSI). At the end of their research, it was discovered that University students at UAE exhibit positive cyber security behaviors when it concerned phishing, social engineering, and online scam, but exhibited poor cyber security behavior when it concerned malware, password usage, and data handling.

Additionally, academicians and researchers have conducted various research on the cyber security behaviors of instructors, perceptions of students' internet security, and knowledge of cyber-crimes in Turkish Republic of Northern Cyprus (TRNC), however limited research has focused on the cyber security behaviors of students. Furthermore, this research is conducted to add to the literature of cyber security behavior of students because there is a gap on this topic in the literature.

1.1 Aim of Study

This thesis is aimed at investigating IT students' cyber security behaviors at Eastern Mediterranean University.

1.2 Research Questions

This research is intended on providing answers for the following questions:

1. How is the cyber security behavior of IT students in terms of malware, password usage, phishing issues, social engineering, and online scam.
2. Is there any relationship between cyber security behavior of IT students and their gender?

1.3 Significance of the Study

This research is important to students that want to gain knowledge about their behavior and how aware they are of their cyber security levels so they can adequately identify and prevent cyber-attacks. The importance of knowing the behavior of students to cyber security is a critical issue, hence there is a need for them to be aware of how to keep themselves safe from hackers and people with malicious intent ready to access their sensitive information and use it.

In addition, this research is important to the field by providing more useful and helpful information for future researchers on the cyber security behaviors of students in the

literature, therefore, contributing to the field of cyber security, and the field of information and communication technologies especially in a place like North Cyprus.

Moreover, it is important to the Faculty at the University especially Eastern Mediterranean University because it will enhance their knowledge on the cyber security behaviors of the students and offer measures such as training and more courses into their curriculum to increase their cyber security behavior levels and to protect their data from attackers.

1.4 Limitation of the Study

This research was limited to only the bachelor's degree students enrolled in the 2018-2019 Spring semester in IT department at Eastern Mediterranean University.

1.5 Definition of Key Terms

Cyber security: cyber security is concerned with the safety and protection of people and data within the cyber environment or internet, and the measure taken to counter malicious attacks (Cavelty, 2010).

Cyber security behavior: this is the behavior of users in the cyberspace that may be beneficial to them by protecting them, or consequential by leaving them exposed to attack (Guo, 2013).

Malware: Malware also known as malicious software are applications downloaded or attached to email attachments with the ability to compromise the protection of the system or device (Sharp, 2009; Denning, 1990).

Phishing: Phishing attacks are cyber-attacks conducted by attackers, hackers, or people with malicious intent with the intent of tricking or manipulating their victims

into giving them their personal and sensitive information (Sun, Yu, Lin, & Tseng, 2016; Frye, 2007).

Social engineering: social engineering which is similar to phishing attacks is concerned with manipulating or influencing the victims decisions so they can make bad or consequential choices that leave them vulnerable and open to attacks online (Rains, 2020).

Online scam: online scams are usually a combination of catfishing, criminal, and swindling activities carried out by fraudsters that gain illegal access into organizations financial account for the purpose of stealing their funds and accessing their data, or by pretending to establish a romantic relationship with their victims with the intention of defrauding them (Whitty, 2013).

Chapter 2

LITERATURE REVIEW

This chapter of this thesis discusses literature related to cyber security, behavior, and cyber security behavior. Also, in this section.

2.1 Cyber Security

Cyber security, which is a term synonymous with internet security or e-security has become a major topic of discussion in various sectors. Due to the internet and web 2.0 technologies making information easily and readily accessible, the increase in cyber-crime and exposure to cyber-threats has also become more rampant, hence there is a growing demand to know the cyber security levels of users and the protection of their devices (Erçağ & Karabulut, 2017). Pandey and Misra (2016) stated that the increase in cyber-crime has affected and instilled fear, unease, and heightened the awareness levels of people all over the world, especially in America where citizens are more worried about their information or identity being stolen, falling victim to internet fraud, or experiencing any sort of cyber-crime, cyber-threats or cyber-terrorism. Moreover, cyber security are protocols, instruments, technological innovations, practices, and teaching set-up to ensure safety of users and information within cyber space (Yılmaz & Sağıroğlu, 2013).

Additionally, the history of cyber security can be traced back to the early 1970's when Bob Thomas, a computer program researcher at that time invented a program called the Creeper to surf through the ARPANET (now known as the internet), which left

digital footprints (Chadd, 2020). Later on, Ray Tomlinson another programmer designed a program called Reaper to terminate the original Creeper program, hence Reaper was considered as the first ever antivirus software as a form of providing cyber security (Chadd, 2020).

Years after the Creeper was determined as the first case of cyber-threats or cyber-attacks, other malicious software's or cyber-threats were created to infiltrate the computer systems of user with the intent of stealing sensitive information or weakening the defense mechanisms such as firewalls, or antivirus software put in place by the user to prevent unauthorized access into their computers or other electronic devices by hackers (Green, 2015). Some of the various approach used in coercing information from users, stealing from users, or gaining unauthorized access include malwares, bots, virus, phishing, social engineering, network intrusion, IP spoofing, spywares (Hamudin & Ariffin, 2014; SecureWorks, 2017; Jameel, 2016).

Moreover, when considering the easiest and weakest channels in maintaining good cyber security practices, humans and passwords were considered as the weakest channels and therefore the easiest to attack (Jameel, 2016; Gratian, Bandi, Cukier, Dykstra, & Ginther, 2018). The findings from various academicians show that when it concerns being exposed to cyber security threats, students were considered as the most vulnerable because every day they communicate making use of internet, web 2.0 technologies, or even connect to open-access Wi-Fi's, which leaves their electronic devices, smart devices, or computer systems open, accessible, and susceptible to malicious attacks (Rezgui & Marks, 2008; Mensch & Wilkie, 2011).

Nevertheless, in the 21st century information and communication technologies remain vital components for communication and interaction, however, most websites, links, email attachments, or even open Wi-Fi connections may not be 100% secure and may contain virus, malwares, and spywares that can be used to steal data from people, hence, the need to determine the knowledge level of people and their behaviors towards cyber security issues are critical (Jameel, 2016).

2.2 Behavior

Popescu (2014) definition of behavior as cited in the earlier works of Doron and Parot (1999) is based on interaction and environment, hence behavior refers to the reaction and interaction of living things(humans, animals) when put in a certain situation or environment. In reference to cyber security, behavior is concerned with students knowledge towards a particular threat and how they act when they encounter such cyber threats. From the findings of Sarathchandra, Haltinner, and Lichtenberg (2016) majority of University students tend to stay away from content or interactions that they find suspicious on the internet or social media, which shows that they have good cyber security behaviors.

2.3 Cyber Security Behavior

Scholars have referred to cyber security behaviors as the behavior of humans in a cyber space environment concerning taking security risks and also managing problems that involve security risks in respect to their awareness on cyber security of their devices, practicing safe and secure internet usage, and how they utilize security technologies (Venard, 2019; Smith, 1989; Whitman & Mattord, 2011).

Muniandy, Muniandy, and Samsudin (2017) developed a scale for measuring the cyber security behavior of students towards malware, password usage, phishing, social engineering and online scam attacks.

2.3.1 Malware

Malwares are the most known cyber security threats that occur by exploring the vulnerabilities of a system. Malwares are software used and created by hackers or people with ill intent to gain illegal access to accounts or stealing private information for their criminal activities. Malwares are software created that have been manipulated by criminals to cause harm to devices, steal private information, or gain unauthorized access to their victims devices (Milošević, 2013). The most known form of malware attacks are: spyware, ransomware, worms, virus etc., that are attached to downloadable files, email attachments, or illegal websites, so that when the user downloads the files of visit the websites, the attackers get access to their data (Kleczynski, 2018).

As technologies evolved and measures were taking to prevent malware attacks, the type of malware programs and the medium of their attack also changed. It can be noted that malware in the late 20th century such as Jerusalem, brain, Morris worm, Michelangelo, CIH, and Melissa that were spread and distributed through floppy disks, attached email files, or websites are not the same as the evolved malware in the 21st century such as Code Red, Nimda, Anna Kournikova, sircam, Sony rootkits, Mpack, Thanatos, Wannacry, etc., that target Internet of Things (IoT), cryptocurrencies, emails, databases and any channel that can be attacked, however, the only thing that remains the same is the intention behind these software, which is to cause harm (Landesman, 2021).

2.3.2 Password Usage

In the aspect of cyber security, when compared to facial recognition, thumbprint recognition, voice recognition, and password usage, passwords remain the most used means of authentication and security protection used by people all over the world, however, passwords are considered one of the easiest forms of security measures to infiltrate (Shen, Yu, Xu, Yang, & Guan, 2016). The first use of password as a form of security and authentication was in 1961, and it was used for the Compatible Time Sharing System (CTSS) (Foster, 2020; Morris & Thompson, 1979).

It is a known fact that due to the convenience of usage, most users prefer using text based passwords for security protection and authentication of their devices and account information such as emails, banks, desktops, laptops, notebooks, and mobile devices, however, the problem is created when users set easy passwords like their date of birth, pet names, nicknames, favorite food, favorite colors, or short numerical passwords that are easy to guess or access by key-loggers and other types of attackers (Shen, Yu, Xu, Yang, & Guan, 2016). Moreover, Lorenz, Kikkas, and Klooster (2013) explained that based on cyber security, a major factor that improves the security of user passwords is by creating passwords with an average length of 15 characters that comprises of numbers, special keys, and alphabet's, hence making the passwords impenetrable to key-loggers and other hackers. Nevertheless, notwithstanding the amount of education and training provided to users by government, schools, and organizations, users still practice unsafe password usage behaviors (Cavelty, 2010).

2.3.3 Phishing

In terms of security, phishing refers to techniques or approaches used by attackers and criminals to prey on the vulnerabilities of their victims so they can gather their information and use it for various malicious purposes (Rader & Rahman, 2015). The

term phishing was first used in the late 90s of the 20th century to refer to criminals involved in hacking people's accounts just to steal their information and password credentials (Kay, 2004).

Gupta, Singhal, and Kapoor (2016) described that phishing attacks are usually carried out when criminals trick the users who have little knowledge on these attacks into believing that they just won a sum of money, car, gift, house or lottery by sending them messages via emails, text, or website links, so the victims can click on a link created by the criminals that redirects them to a website which resembles that of an authentic organization, so that when the victims enter their sensitive credentials, it is then stolen by the attackers. However, it should be noted that victims of phishing attacks are not only users who have bad cyber behavior practices, even companies that have vast knowledge on these kinds of attacks and how to prevent them fall victim unfortunately. Collins (2017) states that all humans are susceptible to phishing attacks. Also, the various kinds of phishing attacks used by hackers include: deceptive phishing, spear phishing, CEO fraud, vishing, smishing, and pharming (Bisson, 2020).

Moreover, the most expensive phishing attack to ever happen recently in history was on Facebook and Google within a time frame of 2013 to 2015, two tech giants, where a hacker known as Evaldas Rimasauskas tricked them into believing that he was from a company in Taiwan they frequently do business with by providing them with falsified documents, after which he defrauded them of a sum of $100,000,000 USD (Graphus, 2020). Nevertheless, in the aspect of cyber security behavior, bad cyber security behavior practiced by users is what increases or leads to phishing issues.

2.3.4 Social Engineering

In the aspect of cyber security, social engineering are attacks performed by criminals within the cyber space, whereby the hackers attackers prey on the weakest and most vulnerable defense of the security system which are the humans, and trick them into disclosing private information (Bhusal, 2020). Moreover, in the researches conducted by Abass (2018) and (2020), social engineering attacks were classified into 2 which are: the technologically based deception attacks which targets the users by pretending to be a website the user is interacting with; and the human based deception attack where the hackers target their victims and use the weakness provided by the human behavior to their own advantage.

Additionally, various researchers have come up with various techniques to prevent social engineering issues, which are: filtering spam emails for easy identification of spoof email; being cautious about the information shared with others; getting trained on how to detect hacking issues such as Trojans and viruses (Breda, Barbosa, & Morais, 2017; Gupta, Singhal, & Kapoor, 2016). More so, to prevent social engineering attacks online, it is advised that users practice good and efficient cyber security behavior online (Abass, 2018).

2.3.5 Online Scam

According to the FBI, online scams are fraudulent activities carried out by fraudsters via the internet with the intent of manipulating their victims so they can defraud them, hacking into their victims emails to steal sensitive information they can use for fraudulent activities, or intercepting bank transfers to redirect the money into their own accounts (FBI, 2021).

Furthermore, according to information gotten from PR Newswire (2020), in 2020 alone over €36,000,000,000 was lost to internet scam, which shows that the rate at which internet scam activities are conducted is increasing at an alarming rate. Moreover, various kinds of scams used by attackers include: romance scams, Nigerian prince scam, tech support scam etc (Rijnetu, 2019; Johansen, 2019).

2.4 Related Research

This section of this research highlights related research works and their cyber security behavior.

Case and King (2013) carried out a longitudinal investigation for 5 years on the cyber security behaviors and perceptions of undergraduate students to find out if students were at risk of cyber security attacks. Their results showed that during the duration of their research, spam and phishing issued reduced.

Rahim, Ramanchandram, Abdullah, and Mohammad (2017) investigated on certain factors that determine the cyber security behavior of students in Malaysia. The benefit of their study was to determine the factors that affect the level of cyber security behavior in undergraduate students at Universiti Utara Malaysia. At the end of their study, it was determined that factors such as self-efficacy, password management, perceived security, perceived privacy, how an individual perceives cyber-threats, and individual susceptibility to attack, affect the cyber security behavior of undergraduate students.

Furthermore, Hadlington (2017) researched on the human factors that influence in risky cyber security behavior of users in the aspect of internet addiction, impulsivity, and attitudes. The benefit of the research was to establish if a relation exists between

internet addiction, impulsivity, attitudes, and risky cyber security behaviors of the users. At the end of the research, it was determined that internet addiction is a major factor that influences and determines user cyber security behaviors; having a good attitude towards cyber security usage was not related to users dangerous cyber security behaviors; and in the aspect of impulsivity 2 factors were discovered as good predictors of cyber security behaviors which were both attentiveness and acting on user impulsiveness.

Gratian, Bandi, Cukier, Dykstra, and Ginther (2018) researched on determining the relationship between human traits and cyber security behavior. Their research investigated on how demographic characteristics and actions such as taking risks, and decision-making abilities of the user affects their cyber security behaviors in the aspect of securing their devices, creating their passwords, updating, their security softwares, and proactive awareness. A total of 369 people participated in in their study and consisted of faculty members, staff, and students while utilizing the Security Behavior Intention Scale (SeBIS). At the end of their research, it was determined that human traits such as taking risks regarding finances, making rational decisions, gender and extraversion were major predictors of having good cyber security behaviors.

Karagozlu (2020) conducted a research on the factors that determine the cyber security behavior of Pre-Service teachers especially in the Faculty of Education, while focusing on 2 Universities in the Turkish Republic of Northern Cyprus (TRNC). The research was aimed at investigating the behaviors of Pre-Service teachers towards cyber security. The participants of the research comprised of 144 enrolled students and utilized a scale. At the end of the research, it was determined that Pre-Service teachers practice good cyber security behaviors when it concerns detecting scammers, and they

were also able to protect themselves from cyber-attacks, thereby ensuring the safety of their data.

Furthermore, Matyokurehwa, Rudhumbu, Gombiro, and Mlambo (2021) based their study on the awareness and behavior of students in Zimbabwean Universities towards cyber security. Their research aimed at determining the cyber security awareness and behavior of the students with respect to the Cyber Security Awareness Scale (CSA). Also, 322 students participated in their study. At the end of their study, it was determined that malware, Internet of Things (IoT), and social engineering issues are dependent on the cyber security behavior and awareness levels of the students.

Chapter 3

METHODOLOGY

In this chapter, the focus is to describe the research design method utilized for this thesis, the participants of the research, the data collection tool used in gathering the data, how the data analysis was carried out, and the validity and reliability of this research.

3.1 Research Design

A quantitative research method together with survey research was applied in this thesis. Based on the definition provided by Babbie (2020), quantitative analysis is usually concerned with the collection of numerical statistical data and the deduction of meaningful information to explain the derived results gotten from mathematical statistical analysis. More so, the statistical data analyzed with the use of quantitative research method could be gotten from surveys (Aliaga & Gunderson, 2000). Based on the definition provided by Ponto (2015), survey research is concerned with gathering of data from participants or respondents that share same interests based on their response to questions provided. Also, surveys can exist in the form of survey questionnaire, open-ended interviews etc (Kelley, Clark, Brown, & Sitzia, 2003; Ponto, 2015). Additionally, survey research utilized in the form of a questionnaire was applied to this research for evaluating the IT students cyber security behavior.

3.2 Participants

The people who participated in this research were 255 undergraduate students from the IT department enrolled in the Spring 2018-2019 academic semester at Eastern

Mediterranean University. Mentioned in Table 3.1 below are the participants' demographic information such as gender, age, academic year, access to internet and hours spent on device.

Table 3.1: Profile of participants

	Frequency (N)	Percentage (%)
Gender		
Female	120	47.1
Male	135	52.9
Total	255	100
Age		
18-20	47	18.4
21-25	95	37.3
26-30	91	35.7
31+	22	8.6
Total	255	200
Academic Year		
1st Year	103	40.4
2nd Year	75	29.4
3rd Year	58	22.7
4th Year	19	7.5
Total	255	100
Access to Internet		
Yes	239	93.7
No	16	6.3
Total	255	100
Hours Spent on Device		
Less than 1 hour	37	14.5
2-5 hours	85	33.3
6-10 hours	77	30.2
11+ hours	56	22.0
Total	255	100

As seen in Table 3.1, the result shows that 255 IT students participated voluntarily where 52.9% (135 students) represents male students and 47.1% (120) represents the female students.

Also illustrated in Table 3.1, the finding reveals that 18.4% (47 students) were between the age ranges of 18-20 years, 37.3% (95 students) belonged to the age range of 21-25, 35.7% (91 students) age ranged between 26-30, while 8.6% (22 students) belonged to the age range of 31 and above.

Moreover, Table 3.1 also highlights that 40.4% (103 students) were in their first year of study, 29.4 % (75 students) were second year students, 22.7 % (58 students) where third year students, while 7.5% (19 students) were in their fourth year of study.

Additionally, Table 3.1 shows that 93.7 % (239 students) confirm that they have accessibility to the internet, on the other hand, 6.3% (16 students) responded that they do not have access to the internet.

Subsequently, Table 3.1 reveals the amount of time spent on devices by the participants. 14.5% (37 students) said they spend less than 1 hour on their device, 33.3% (87 students) responded that they spend between 2-5 hours on their device, 30.2% (77 students) confirmed that they spend 6-10 hours on their devices, while 22.0% (56 students) spend at least 11 hours on their devices.

3.3 Data Collection Tool

The instrument used for collecting the participants' data was a survey that comprised of two sections. The first section was the demographic sections designed by the researcher that contained basic questions focusing on participants' traits such as

gender, age, academic year, access to internet and hours spent on devices. On the other hand, the second part of the survey was the Cyber Security Behavior Scale (CSB) developed by Muniady, Muniady, and Samsudin (2017) that comprised of 50 Items was ranked on a 5-point Likert type ranging from 5(strongly agree), 4 (agree), 3(don't know), 2 (disagree) and 1 (strongly disagree). Moreover, the CSB was further categorized into 5 sub-dimensions which are malware, password usage, phishing issues, social engineering issues, and online scam issues. Additionally, the malware sub-dimension comprised of 10 Items aimed at measuring the behavior of students towards malware. The password usage sub-dimension consisted of 10 Items that measures the students' behavior on the aspect of how they use, manage and often change their password. Also, phishing issues sub-dimensions contained 10 Items, which measure the students behavior of phishing attacks. Social engineering issues sub-dimensions contains 10 Items and is aimed at measuring students' behavior towards the dangers of social engineering. Finally, the sub-dimension related to online scam issues comprised of 10 Items aimed at finding out how students behave when they encounter online scammers (Muniandy, Muniandy, & Samsudin, 2017). For more details on the CSB Scale, see Appendix B.

3.4 Data Analysis

For this research, the entirety of the data was gathered and analyzed using descriptive analysis together with the statistical analysis software package known as IBM SPSS 23. In addition, Frequency (n), Percentages (%), and t-test were utilized to perform the analysis of the data. Nonetheless, frequency and percentages were used to represent the results for individual research Items. Kaur, Stoltzfus, and Yellapu (2018) referred to descriptive analysis as the representation of mathematical expressions in a way that shows the dependent or independent variables and their relation with the sample or

population, which is usually represented in terms of frequency, measures of central tendency, and often times their standard deviation.

3.5 Validity and Reliability

The research conducted by Muniady, Muniady, and Samsudin (2017) revealed a general Cronbach alpha value of 0.762 for all the Items combined, and for the sub-dimensions the Cronbach alpha values for individual sub-dimensions. Table 3.2 below represents the Cronbach alpha values from the malware, password usage, phishing, social engineering, and online scam sub-dimension together with the total Cronbach alpha value from the original CSB Scale.

Table 3.2: CSB reliability measurement (Muniandy, Muniandy, & Samsudin, 2017)

Cyber security Sub-dimensions	Cronbach alpha
Malware	0.841
Password usage	0.702
Phishing	0.703
Social engineering	0.859
Online scam	0.702
Total	0.762

Table 3.2 above shows the Cronbach alpha values gotten from Muniady, Muniady, and Samsudin (2017) research whereby in respect to the various sub-dimensions, the Cronbach alpha values were revealed as 0.841 for malware, 0.702 for password usage, 0.703 for phishing, 0.859 for social engineering and 0.702 for online scam. Moreover, the general Cronbach alpha value gotten from their research indicated a value of 0.762, which proved the reliability of the CSB Scale and the consistency of each Item. As seen in Table 3.3 below, the Cronbach alpha values from the malware, password usage,

phishing, social engineering, and online scam sub-dimension together with the total Cronbach alpha value from the CSB reliability measurement for IT students.

Table 3.3: CSB reliability measurement for IT students

Cyber security Sub-dimensions	Cronbach alpha
Malware	0.674
Password usage	0.790
Phishing	0.793
Social engineering	0.771
Online scam	0.790
Total	0.764

As shown in Table 3.3, the Cronbach alpha values for each sub-dimensions for this research was 0.674 for malware, 0.790 for password usage, 0.793 for phishing, 0.771 for social engineering, and 0.790 for online scam issues. Additionally, an internal consistency and reliability coefficient (Cronbach alpha value for all 50 Items) was discovered as 0.764. Consequently, as explained in the works of Kelley, Clark, Brown and Sitzai (2003) high Cronbach alpha values are acceptable.

Chapter 4

RESULTS AND DISCUSSIONS

This chapter presents all the findings of the analysis with detailed explanation. The information provided below demonstrates the cyber security behavior of IT students based on the research questions.

4.1 Cyber Security Behavior of IT Students in Respect to Malware, Password Usage, Phishing, Social Engineering and Online Scam

Table 4.1 below represents the cyber security behavior of IT students in reference to the malware sub-dimension. Additionally, Items M1, M2, M3, M4, M5, M6, M7, M8, M9, and M10 are abbreviated representations of malware issues from Item 1 to Item 10 in the original survey (see Appendix B).

Table 4.1: IT students' cyber security behavior on malware

Items	SD		D		DK		A		SA		Mean	Std. Dev
	n	%	n	%	n	%	n	%	n	%		
M1	64	26.8	84	35.1	48	20.1	34	14.2	9	3.8	**2.33**	1.13
M2	30	12.6	58	24.3	88	36.8	50	20.9	13	5.4	2.82	1.07
M3	23	9.6	38	15.9	94	39.3	56	23.4	28	11.7	3.12	1.11
M4	26	10.9	44	18.4	99	41.4	55	23.0	15	6.3	2.95	1.05
M5	16	6.7	39	16.3	71	29.7	79	33.1	34	14.2	3.32	1.11
M6	18	7.5	43	18.0	91	38.1	72	30.1	15	6.3	3.10	1.01
M7	22	9.2	28	11.7	73	30.5	80	33.5	36	15.1	3.33	1.15
M8	18	7.5	42	17.6	66	27.6	71	29.7	42	17.6	3.32	1.17
M9	30	12.6	43	18.0	70	29.3	68	28.5	28	11.7	3.09	1.20
M10	22	9.2	32	13.4	65	27.2	69	28.9	51	21.3	**3.40**	1.22

Based on the results gotten from Table 4.1, results from Item M1 (willing to open email attachments from strangers) showed that majority of the students behaved negatively towards opening email attachments received from unknown senders. As a result, 61.9% of the students confirmed that they are not willing to open email attachments received from unknown senders. However, 18% of the students responded that they are willing to open email attachments from people they do not know. Also, an arithmetic mean value of 2.33 and a standard deviation 1.13 indicates that when opening email attachments, students are not willing to open the attachment if they do not know the sender. Additionally, the results show that majority of the students have knowledge on malware and how malware attacks can be conducted via the attachment of malicious software to receivers email. Additionally, a different result from the findings of this research is that of Garba, Siraj, Othman, and Musa (2020) where their study revealed that majority of the students lack knowledge on how to identify malware attacks especially when it concerns opening emails from unknown senders, which can pose as a threat to the student's cyber security.

According to Table 4.1, Item M10 (apply security patches as soon as possible) result indicates that 50.2% of the students responded positively towards being able to apply security patches as soon as possible when necessary. On the other hand, 22.6% of the students disagreed on applying security patches as soon as possible. Subsequently, an arithmetic mean value of 3.40 and a standard deviation of 1.22 demonstrate that when a security patch is made available, the students are able to apply them to their devices when needed to prevent malware attacks. The results also reveals that students know how to apply security patches to ensure their devices are always protected.

As understood from the results given in the malware sub-dimension, out of the 10 Items presented, 8 Items (M2, M3, M4, M5, M6, M7, M8, M9) shows that students cyber security behavior on malware attacks are low, which means that they may not know of the precautions taken to prevent malware attacks, therefore their devices are not well protected and are susceptible to malware attacks. Also, 2 Items (M1, M10) indicates that the students know how to protect themselves from malware attacks.

In summary, based on the findings from the malware sub-dimension, it can be concluded that students demonstrate low cyber security behavior regarding malware issues. A reason for this may be because IT students are not properly trained or their courses are not sufficient enough for them to identify malware threats. Conclusively, similar findings to this research is that of Teer, Kruck and Kruck (2007) in the aspect of students' usage of computers, where they discovered that students do not possess adequate knowledge on how to detect and prevent malware attacks in respect to their usage of firewalls, antivirus, and how to open emails with multiple attachments.

Table 4.2 below shows the cyber security behavior of IT students based on the password usage sub-dimension. Items labeled PU1, PU2, PU3, PU4, PU5, PU6, PU7, PU8, PU9, and PU10 are abbreviated representations of password usage issues from Item 11 to Item 20 in the original survey (see Appendix B).

Table 4.2: IT students' cyber security behavior on password usage

Items	SD		D		DK		A		SA		Mean	Std. Dev
	n	%	n	%	n	%	n	%	n	%		
PU1	7	2.9	19	7.9	52	21.8	76	31.8	85	35.6	**3.89**	1.07
PU2	47	19.7	22	9,2	53	22.2	93	38.9	24	10.0	**3.10**	1.29
PU3	10	4.2	27	11.3	64	26.8	72	30.1	66	27.6	3.66	1.12
PU4	8	3.3	22	9.2	56	23.4	87	36.4	66	27.6	3.76	1.06
PU5	12	5.0	25	10.5	62	25.9	74	31.0	66	27.6	3.66	1.14
PU6	19	7.9	33	13.8	69	28.9	82	34.3	36	15.1	3.35	1.13
PU7	28	11.7	33	13.8	63	26.4	77	32.2	38	15.9	3.27	1.23
PU8	21	8.8	26	10.9	65	27.2	85	35.6	42	17.6	3.42	1.16
PU9	20	8.4	30	12.6	71	29.7	78	32.6	40	16.7	3.37	1.15
PU10	27	11.3	32	13.4	83	34.7	63	26.4	34	14.2	3.19	1.18

Results from Table 4.2 shows that in reference to the results for Item PU1 (password does not follow keyboard pattern) 67.4% of IT students agree that when creating their passwords, they ensure that it does not follow a sequential pattern. Nevertheless, 10.8% of IT students disagreed and responded that their passwords follow specific keyboard patterns. In addition, an arithmetic mean value of 3.89 together with a standard deviation of 1.07 explains that when students create their passwords, they do not follow sequential or specific keyboard patterns. Conclusively, the results for PU1 prove that students have effective password usage and maintain appropriate cyber security behaviors when it involves creating strong and secure passwords by avoiding sequential patterns on their keyboards, which makes it harder for key-loggers to get their password information. Moreover, Aljohani and Elfadil (2020) findings which

was dissimilar to the findings of PU1 shows that students have neutral behaviors and awareness levels when it concerns creating passwords that do not follow a sequence.

Subsequent results in Table 4.2 based on Item PU2 (Sharing password with other people) shows that 48.9% of the students agree that they disclose their password information to other people. However, 28.9% of the students do not support the idea of sharing their passwords with other people. Moreover, an arithmetic mean value of 3.10 with a standard deviation of 1.29 indicates that most IT students feel comfortable sharing their passwords with other people, therefore showing that they have low cyber security behaviors, hence it is easy for their data to accessible or stolen by people with malicious intent.

The findings of the password usage sub-dimension demonstrates that out of the 10 Items in the sub-dimension, only 4 Items (PU1, PU3, PU4, and PU5) indicate high cyber-security behaviors among IT students regarding their password usage practice and knowledge on how to protect and keep their passwords safe. Nevertheless, 6 Items (PU2, PU6, PU7, PU8, PU9, and PU10) show that IT students exhibit low cyber-security behaviors when it concerns keeping their passwords safe, not using personal information such as names or birthdays, changing their passwords frequently, and never writing down the details of their passwords.

Conclusively, the findings of the password usage sub-dimension shows that although a percentage of IT students know how to keep their passwords safe, majority of them have low cyber-security behavior when it concerns the safe-keeping and security of their passwords, which makes their information open and accessible by key-loggers and hackers. Moreover, the results of Kovačević, Putnik, and Tošković (2020) similar

to the findings in the password usage sub-dimension proves that students do not have adequate knowledge of how to create adequate password.

Table 4.3 below, shows the cyber security behavior of IT students based on the phishing issues sub-dimension. The Items labeled PH1, PH2, PH3, PH4, PH5, PH6, PH7, PH8, PH9, and PH10 are abbreviated representations of the phishing issues from Item 21 to Item 30 in the original survey (see Appendix B).

Table 4.3: IT students' cyber security behavior on phishing

Items	SD		D		DK		A		SA		Mean	Std. Dev
	n	%	n	%	n	%	n	%	n	%		
PH1	8	3.3	16	6.7	39	16.3	61	25.5	115	48.1	**4.08**	1.10
PH2	10	4.2	21	8.8	51	21.3	113	47.3	44	18.4	3.67	1.01
PH3	30	12.6	25	10.5	43	18.0	76	31.8	65	27.2	3.51	1.33
PH4	22	9.2	31	13.0	52	21.8	91	38.1	43	18.0	3.43	1.19
PH5	37	15.5	29	12.1	42	17.6	83	34.7	48	20.1	**3.32**	1.34
PH6	17	7.1	24	10.0	51	21.3	91	38.1	56	23.4	3.61	1.16
PH7	14	5.9	19	7.9	60	25.1	82	34.3	64	26.8	3.68	1.13
PH8	13	5.4	26	10.9	57	23.8	89	37.2	54	22.6	3.61	1.11
PH9	9	3.8	19	7.9	68	28.5	85	35.6	58	24.3	3.69	1.04
PH10	15	6.3	22	9.2	52	21.8	79	33.1	71	29.7	3.71	1.17

From the results in Table 4.3, Item PH1 (upgrading phishing knowledge by reading phishing materials) demonstrates that majority of the students illustrated as 73.6% agreed that they upgrade the knowledge on phishing issues by reading relevant phishing materials. However, 10% of the students responded negatively stating that

they do not read relevant materials on phishing to increase their phishing knowledge. Furthermore, an arithmetic mean value of 4.08 and a standard deviation of 1.10 shows that when students read phishing materials, it increases their knowledge on phishing so they may be able to detect and prevent phishing attacks with ease.

Also gotten from Table 4.3, Item PH5 (trusting email messages announcing contest wins) shows that 54.8% of the students reported that they believe emails informing them they have won prizes in a contest. On the other hand, 27.69% disagree by indicating that they do not trust any emails they receive indicating that they have won a prize from a contest. With an arithmetic mean value of 3.32 and a standard deviation of 1.34, the result of Item PH5 shows that most IT students believe any email they receive informing them they have won a contest. However, the sender of the email may indirectly trick them into revealing sensitive information, which indicates that when it concerns trusting emails received stating that they have won a contest, IT students practice bad cyber security behaviors which makes them easily susceptible and fall prey to phishing attacks that may be as a result of being naive, lack of adequate training, and lack of well-informed courses for identifying and protecting them against any kind of phishing attacks.

As understood from the results given in the phishing sub-dimension, out of the 10 Items presented, 6 Items (PH1, PH6, PH7, PH8, PH9, PH10) shows that students behavior toward phishing issues are somewhat high, which means that they have sufficient knowledge on how to identify phishing attacks. However, 4 Items (PH2, PH3, PH4, PH5) shows that when it concerns knowing how to protect themselves from phishing attacks IT students have low cyber security behaviors. A contributing factor

to this response may be lack of understanding in regards to the question asked or inadequate training.

In summary, results of the phishing sub-dimension shows that majority of IT students know how to identify phishing issues, however, some students still lack knowledge on how to adequately identify and protect themselves from phishing attack Chandarman and Van Niekerk (2017) findings proved otherwise, stating that majority of students in their research did not know what phishing was and they could not identify phishing attacks.

Table 4.4 below represents the cyber security behavior of IT students in reference to the social engineering sub-dimension. More so, Items SE1, SE2, SE3, SE4, SE5, SE6, SE7, SE8, SE9, and SE10 are abbreviated representations of the social engineering issues from Item 31 to Item 40 in the original survey (see Appendix B).

Table 4.4: IT students' cyber security behavior on social engineering

Items	SD		D		DK		A		SA		Mean	Std. Dev
	n	%	n	%	n	%	n	%	n	%		
SE1	21	8.8	22	9.2	53	22.2	48	20.1	95	39.7	**3.73**	1.31
SE2	46	19.2	26	10.9	54	22.6	105	43.9	8	3.3	**3.01**	1.21
SE3	17	7.1	20	8.4	89	37.2	70	29.3	43	18.0	3.43	1.10
SE4	7	2.9	22	9.2	78	32.6	95	39.7	37	15.5	3.56	0.96
SE5	29	12.1	40	16.7	72	30.1	70	29.3	28	11.7	3.12	1.19
SE6	28	11.7	42	17.6	67	28.0	75	31.4	27	11.3	3.13	1.18
SE7	22	9.2	26	10.9	75	31.4	66	27.6	50	20.9	3.40	1.20
SE8	14	5.9	21	8.8	67	28.0	90	37.7	47	19.7	3.56	1.08
SE9	16	6.7	30	12.6	74	31.0	74	31.0	45	18.8	3.43	1.13
SE10	13	5.4	32	13.4	65	27.2	77	32.2	52	21.8	3.51	1.13

As reported by the results in Table 4.4, based on Item SE1 (not interested in reading social engineering issues), 59.8% of the students support the idea of not being interested in reading social engineering issues. However, 18% of the students disagreed, and showed interest in reading about social engineering issues. An arithmetic mean value of 3.73 and a standard deviation of 1.31 explains that students are not interested in reading social engineering issues. Moreover, the results show that the students are not interested in reading social engineering issues, which can be because of laziness or lack of interest in reading about social engineering issues.

Also, according to Table 4.4, Item SE2 (willing to give my username and password to any one claiming to be the administrator) results shows that 47.2% of the students responded positively, indicating that they are willing to give out their username and

password to anyone claiming to be the administrator. On the other hand, 30.1% of the students disagreed on the idea of giving out their username and password to anyone claiming to be the administrator. More so, an arithmetic mean value of 3.01 and a standard deviation of 1.21 demonstrate that most IT students trust anyone claiming to be the administrator and they give out their information and logging in details to them, which, means that when it concerns willingly giving sensitive information to anyone claiming to be the system administrator, IT students practice unsafe cyber security behaviors, hence their information is open to social engineering threats.

As understood from the results given in the social engineering sub-dimension, out of 10 Items presented, 9 Items (SE1, SE2, SE3, SE4, SE5, SE6, SE7, SE9, SE10) show that IT students have low cyber security behaviors when it concerns identifying and protecting themselves against social engineering threats. The results also show that IT students do not have adequate knowledge when it concerns social engineering threats. However, only 1 Item (SE8) shows that when it concerns being questioned by someone, IT students are not intimidated.

In summary, based on the findings from the social engineering sub-dimension, it can be concluded that IT students demonstrate low cyber security behaviors regarding social engineering threats. A reason for this may be that IT students are not properly trained to identify and prevent social engineering attacks.

As indicated in Table 4.5 below, it shows the cyber security behavior of IT students based on the online scam sub-dimension. The Items labeled OS1, OS2, OS3, OS4, OS5, OS6, OS7, OS8, OS9, and OS10 are abbreviated representations of the online scam issues from Item 41 to Item 50 in the original survey (see Appendix B).

Table 4.5: IT students' cyber security behavior on online scam

Items	SD		D		DK		A		SA		Mean	Std. Dev
	n	%	n	%	n	%	n	%	n	%		
OS1	10	4.2	24	10.0	56	23.4	47	19.7	102	42.7	**3.87**	1.20
OS2	5	2.1	22	9.2	67	28.0	114	47.7	31	13.0	3.60	0.90
OS3	33	13.8	33	13.8	65	27.2	72	30.1	36	15.1	**3.19**	1.25
OS4	15	6.3	21	8.8	61	25.2	93	38.9	49	20.5	3.59	1.10
OS5	22	9.2	22	9.2	61	25.2	86	36.0	48	20.1	3.49	1.18
OS6	32	13.4	33	13.8	63	26.4	78	32.6	33	13.8	3.20	1.23
OS7	15	6.3	30	12.6	55	23.0	84	35.1	55	23.0	3.56	1.16
OS8	21	8.8	38	15.9	77	32.2	72	30.1	31	13.0	3.23	1.13
OS9	12	5.0	27	11.3	76	31.8	77	32.2	47	19.7	3.50	1.08
OS10	12	5.0	30	12.6	66	27.6	83	34.7	48	20.1	3.52	1.10

As reported by the results in Table 4.5, based on Item OS1 (establish trusted relationship with online strangers) 62.4% of the students agreed that they have a trusting online relationship with strangers. However, 14.2% of the students disagreed to the idea of establishing trusted online relationship with people they do not know. An arithmetic mean value of 3.87 and a standard deviation value of 1.20 explains that it is easy for IT students to develop a trusting online relationship with people who they nothing about. This result means that it is easy for IT students to form trusting relationships with strangers online, therefore, they can easily fall prey to online scammers and have low cyber security behaviors.

Based on Table 4.5, Item OS3 (respond to text messages announcing contests involving huge sum of money) result shows that 45.2% of the students responded

positively to responding to text messages announcing contests involving huge sum of money. Furthermore, 27.6% of the students disagreed indicating that they do not respond to text messages announcing contests involving huge sum of money. Also, an arithmetic mean value of 3.19 and standard deviation of 1.25 demonstrate that IT students respond positively to text messages announcing contests involving huge sum of money without checking if the text messages are real. The finding also reveals students may easily fall prey to online scammers when it involves messages involving a huge sum of money, hence they have low cyber security behaviors.

As understood from the results given in the online scam sub-dimension, out of the 10 Items presented, 6 Items (OS1, OS3, OS6, OS8, OS9, OS10) shows that students cyber security behavior towards online scam is low which means that they may not be adequately skilled in identifying online fraudsters or preventing themselves from falling victims to these fraudsters. However, 4 Items (OS2, OS4, OS5, OS7) shows that when it concerns trusting the identity provided by strangers online, paying for services offered by online sites, or ability to identify latest online scams, IT students have high cyber security behaviors. A major reason for the low cyber security behavior from IT students may be because they do not have sufficient training in preventing online scam attacks or the courses thought are not sufficient.

To summarize, based on the findings from the online scam sub-dimension, it can be inferred that IT students have low cyber security behaviors when it concerns online scam issues. A reason for this may be because IT students are not aware of techniques online scammers use in tricking their victims, and they do not how to prevent online fraud from occurring.

Consequently, due to the unsafe cyber security behavior practices in malware, password usage, phishing, social engineering and online scam issues by IT students, it can be deduced that IT students have low cyber security behaviors, hence, they do not possess sufficient knowledge on how to prevent these attacks. Similarly, the findings of Muniandy, Muniandy and Samsudin (2017) show that based on the malware, password usage, phishing, social engineering and online scam sub-dimensions, the students had insufficient cyber security behaviors.

4.2 Relation between Cyber Security Behavior and Students Gender

The results inferred in this section of the thesis reveals if any relation was found between IT students cyber security behavior and their gender at EMU. A statistical analysis known as independent sample T-test was utilized for finding the relation between male and female genders and cyber security behavior of students. A total of 8 Items out of 50 Items were found as significantly different in reference to IT students gender.

Table 4.6 below represents the 8 Items that are significantly different for IT students gender and cyber security behavior.

Table 4.6: Cyber security behavior of IT students based on gender

Items	Gender	Frequency (N)	Mean	SD	t	Df	P
M3	Female	120	2.98	1.06	-2.09	253	0.037
	Male	135	**3.26**	1.10			
PU2	Female	120	3.35	1.12	2.36	253	0.019
	Male	135	**2.98**	1.37			
PU4	Female	120	3.62	1.08	-2.15	253	0.032
	Male	135	**3.90**	0.99			
PH4	Female	120	3.66	1.23	-2.47	253	0.014
	Male	135	**3.30**	1.19			
PH7	Female	120	**3.87**	1.04	2.24	253	0.026
	Male	135	3.57	1.16			
PH8	Female	120	**3.80**	0.98	2.38	253	0.018
	Male	135	3.47	1.18			
OS1	Female	120	4.07	1.14	2.56	253	0.011
	Male	135	**3.69**	1.21			
OS3	Female	120	3.40	1.20	2.40	253	0.017
	Male	135	**3.03**	1.25			

As indicated in Table 4.6, the results for M3 (very sure of the status of the antivirus software on PCs) was significantly different in IT students ($p<0.05$) for female (mean= 2.98, SD= 1.06) and male (mean=3.26, SD=1.10) gender $t(253) = -2.09$, $P=0.037$. The results show that the gender of IT students affects their cyber security behavior in respect to knowing the status of their antivirus software. Further explanations of this

is that when it concerns the status of their antivirus software male IT students exhibit higher cyber security behaviors than female IT students.

Also shown in Table 4.6, PU2 (sharing password with other people) was significantly different in IT students ($p<0.05$) for female (mean= 3.35, SD= 1.12) and male (mean= 2.98, SD=1.37) genders, t (253) = 2.36 and P (0.019). Results indicates that the gender of IT students is related to their behavior towards sharing their passwords with other people. Furthermore, when it concerns sharing their passwords with other people, female IT students had lower cyber security behaviors than male IT students.

In addition, results in Table 4.6 for PU4 (passwords consist of lower case, upper case, numbers and special characters) reveals a significant difference in IT students ($p<0.05$) for female (mean=3.62, SD=1.08) and male (mean=3.90, SD=0.99) genders, t (253) =-2.15, P=0.032. The findings revealed that the gender of IT students affects their cyber security behavior in respect to how they set up passwords that consist of lower case, upper case, numbers and special characters combined. This result shows that when it concerns creating strong passwords that consists of lower case, upper case, numbers and special characters, male IT students exhibit higher cyber security behaviors than female IT students.

As indicated in Table 4.6, the results for PH4 (willing to click hyperlinks in email messages) was significantly different for IT students ($p<0.05$) in female (mean=3.66, SD=1.23) and male (mean=3.30, SD=1.19) genders, t (253) = 2.47, P=0.014. It was revealed in the finding that the gender of IT students affects their cyber security behavior in respect to their willingness to click hyperlinks in email messages. Further

explanations on this Item indicate that, when it comes to clicking hyperlinks in emails, female IT students exhibit lower cyber security behaviors than male IT students.

Furthermore, results in Table 4.6, for PH7 (padlock symbol is more necessary to transmit private information) reveals a significant difference in IT students ($p<0.05$) for female (mean=3.87, SD=1.04) and male (mean=3.17, SD=1.16) genders, t (253) =2.24, P=0.026. The results indicate that the gender of IT students' affects their cyber security behavior in respect to their necessity for transmitting sensitive information through padlock symbol. The findings revealed that when it concerns padlock symbol being present while sending or receiving sensitive information, female IT students' exhibit high cyber security behaviors than male IT students.

Moreover, as seen in Table 4.6, the results for PH8 (I prefer typing URL in a new browser rather than clicking hyperlinks) was significantly different in IT students ($p<0.05$) for female (mean=3.80, SD=0.98) and male (mean=3.47, SD=1.18) genders, t (253) = 2.38, P=0.018. The results indicated that the gender of IT students affects their cyber security behavior in respect to their preference for typing URL in a new browser rather than clicking hyperlinks. Subsequently, results indicate that female IT students have higher security behaviors than male IT students when it concerns avoiding phishing attacks by their preference of typing the URL in a new browser rather than clicking hyperlinks.

More so as highlighted in Table 4.6, the findings for OS1 (established trusted online relationship with strangers) was found to be significantly different in IT students ($p<0.05$) for female (mean=4.07, SD=1.14) and male (mean=3.09, SD=1.21) genders, t (253) =2.56, P=0.01. As indicated in the results, the gender of IT students affects

their cyber security behavior in respect to their ability to establish trusted online relationship with strangers. Additional results revealed that when it concerns the establishment of trusted online relationship with strangers, female IT students possess lower cyber security behaviors than male IT students do.

Based on the illustrations in Table 4.6, results for OS3 (respond to SMS announcing contests involving huge sum of money) was seen as significantly different in IT students ($p<0.05$) for female (mean=3.40, SD=1.20) and male (mean=3.03, SD=1.25) genders, t (253) =2.40, P=0.017. The results indicated that, the gender of IT students affects their cyber security behavior in respect to responding to SMS announcing contests involving huge sum of money online. Further explanations for this Item shows that when it concerns responding to SMS announcing contests involving huge sum of money, female IT students have lower cyber security behaviors than male IT students do.

In summary, out of 50 Items, 42 Items were not significantly different for gender, whereas 8 Items were significantly different between gender of IT students. Based on the 8 Items with significant differences, in 6 Items (M3, PU2, PU4, PH4, OS1, OS3) male IT students had higher cyber security behavior than female IT students, while in 2 Items (PH7, PH8) female IT students possessed higher cyber security behavior than male IT students

Conclusively, the findings by Fatokun, Hamid, Norman and Fatokun (2019), determine that gender is a determinant factor in the investigation of students cyber security behaviors, whereby male students possess higher cyber security behaviors than female students.

Chapter 5

CONCLUSION

The main aim of this research was to discover the cyber security behavior of IT student in terms of malware, password usage, phishing, social engineering and online scam attacks. In addition, this research also aimed at investigating if a relationship between cyber security behavior and the gender of IT students exists.

The results of the research shows that the IT students' have low cyber security behaviors in general. However, when considering the responses to the Items in respect to the sub-dimensions, in malware sub-dimension 8 Items (M2, M3, M4, M5, M6, M7, M8, M9) shows that students cyber security behavior on malware attacks are low, while 2 Items (M1, M10) showed that IT students have high cyber security behavior when it concerns malware issues. In password usage sub-dimension, 6 Items (PU2, PU6, PU7, PU8, PU9, and PU10) indicated that IT students had low cyber security behavior, and 4 Items (PU1, PU3, PU4, and PU5) showed that IT students had high cyber security behavior when it concern password usage issues. In phishing sub-dimension, 6 Items (PH1, PH6, PH7, PH8, PH9, PH10) indicated that IT students had high cyber security behavior, while 4 Items (PH2, PH3, PH4, PH5) showed that IT students had low cyber security behavior when it concern phishing issues. In social engineering sub-dimension 9 Items (SE1, SE2, SE3, SE4, SE5, SE6, SE7, SE9, SE10) indicated that IT students had low cyber security behavior, while 1 Item (SE8) showed that IT students had high cyber security behavior when it concern social engineering

attacks. In online scam sub-dimension 6 Items (OS1, OS3, OS6, OS8, OS9, OS10) indicated that IT students had low cyber security behavior, while 4 Item (OS2, OS4, OS5, OS7) showed that IT students had high cyber security behavior when it concern social engineering attacks.

Additionally, in this research, it was discovered that out of 50 Items, 42 Items did not show significant difference between the cyber security behaviors of female and male IT students, however, 8 Items were significantly different. In these 6 Items very sure of the status of anti-virus software on my personal computer; sharing password with other people; passwords consists of lowercase, uppercase, numbers and special characters; willing to click hyperlinks in email messages; establish trusted relationship with online friends; respond to text messages announcing contests involving huge sum of money (M3, PU2, PU4, PH4, OS1, OS3), male IT students had higher cyber security than female IT students. On the other hand, in these 2 Items Padlock symbols a must when transmitting confidential information, and I prefer to type URL in a new browser rather than click it on hyperlink (PH7, PH8), female IT students possessed higher cyber security behavior than male IT students.

In summary, the result of this thesis shows that Eastern Mediterranean University IT students exhibit low cyber security behaviors in general, and low cyber security behaviors respect to malware, password usage, social engineering, and online scam cyber-attacks, while exhibiting high cyber security behavior in respect to phishing.

REFERENCES

Abass, I. A. (2018). Social engineering threat and defense: a literature survey. *Journal of Information Security*, *9*(04), 257.

Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks. . *Journal of Cyber Security and Mobility*, 65-88.

Agbo, A. D., & Igwebuike, E. U. (2016). Assessment of internet awareness and use by the undergraduate students of College of Agricultural and Science Education in Michael Okpara University of Agriculture Umudike. *American Journal of Educational Research, 4(2), 200-203, 4*(2), 200-203.

Aliaga, M., & Gunderson, B. (2000). *Interactive Statistics.* Prentice Hall.

Aliyu, M., Abdallah, N. A., Lasisi, N. A., Diyar, D., & Zeki, A. M. (2010). Computer security and ethics awareness among IIUM students: An empirical study. *Proceeding of the 3rd International Conference on Information and Communication Technology for the Moslem World (ICT4M) 2010.* (pp. A52-A56)). IEEE.

Aljohani, W., & Elfadil, N. (2020). Measuring Cyber Security Awareness of Students: A Case Study at Fahad Bin Sultan University. *International Journal of Computer Science and Mobile Computing, 9*(6).

Babbie, E. R. (2020). *The practice of social research.* Cengage learning.

Bergner, R. M. (2011). What is behavior? And so what?. *New ideas in psychology, 29*(2), 147-155.

Bhusal, C. S. (2020). Systematic Review on Social Engineering: Hacking by Manipulating Humans. *Available at SSRN, 3720955.*

Bisson, D. (2020). *6 Common Phishing Attacks and How to Protect Against Them*. Retrieved 2021, from The State of Security: https://www.tripwire.com/state-of-security/security-awareness/6-common-phishing-attacks-and-how-to-protect-against-them/

Breda, F., Barbosa, H., & Morais, T. (2017). Social engineering and cyber security. . *Proceedings of the International Conference on Technology, Education and Development*, (pp. 6-8.). Valencia, Spain .

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: causes and consequences of victimhood. *Psychology, Crime & Law*, *20*(3), 261-283.

Case, C. J., & King, D. L. (2013). Cyber security: A longitudinal examination of undergraduate behavior and perceptions. *ASBBS E-Journal*, *9*(21).

Cavelty, M. D. (2010). Cyber-security. . *The routledge handbook of new security studies*, 154-162.

Černá, M., & Poulová, P. (2012). Utilization of Web Portals at Selected Universities: Comparative Study. *Proceedings of the 9 th International Scientific Conference on Distance Learning in Applied Informatic*, (pp. 63-72).

Chadd, K. (2020). *The history of cybersecurity*. Retrieved 2021, from Avast: https://blog.avast.com/history-of-cybersecurity-avast#:~:text=Cybersecurity%20proper%20began%20in%201972,protocols%20for%20remote%20computer%20networking.

Chandarman, R., & Van Niekerk, B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. . *The African Journal of Information and Communication, 20*, 133-155.

Cision PR NewsWire. (2020). *€36 Billion Lost in Online Scams: Online scams to grow by 40% in 2020*. Retrieved 2021, from Cision PR NewsWire: https://www.prnewswire.com/news-releases/36-billion-lost-in-online-scams-301160799.html

Collins, N. (2017). *Who's Most Likely to Get Phished?* Retrieved 2021, from Pacific Standard: https://psmag.com/environment/who-gets-phished

Denning, P. J. (1990). *Computers under attack; intruders, worms, and viruses.* New York ACM Press.

Doron, R., & Parot, F. (1999). Dictionary of psychology. *Bucharest: Humanitas*, 320-321.

Emeka, U. J., & Nyeche, O. S. (2016). Impact of internet usage on the academic performance of undergraduates students: A case study of the university of Abuja,Nigeria. *International Journal of Scientific & Engineering Research, 7*(10), 1018-1029.

Erçağ, E., & Karabulut, M. (2017). Perceptions on self-efficacy of students studying at secondary education in the TRNC on Internet security. *Revista de Educación a Distancia (RED)*(54).

Ertan, A. C., Denny, D., & Jensen, R. (. (2020). Cyber Security Behaviour In Organisations. *arXiv preprint arXiv:, 2004*, 1768.

Fatokun, F. B., Hamid, S., Norman, A., & Fatokun, J. O. (2019). The impact of age, gender, and educational level on theCybersecurity behaviors of tertiary institution students: An empirical investigation on Malaysian universities. *Journal of Physics: Conference Series, 1339*(1), 012098.

FBI. (2021). *Scams and Safety*. Retrieved 2021, from FBI: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/internet-fraud

Flores, P., Farid, M., & Samara, K. (2019). Assessing E-Security Behavior among Students in Higher Education. *2019 Sixth HCT Information Technology Trends (ITT)* (pp. 253-258). IEEE.

Foster, B. (2020). *User practice in password security: An empirical study of real-life passwords in the wild. ,*. Retrieved 2021, from Mobile Iron:

https://www.mobileiron.com/en/blog/the-history-of-passwords-and-making-passwords-history

Frye, D. W. (2007). Email, Instant Messaging and Phishing. *Network Security Policies and Procedures*, 131-152.

Garba, A. A., Siraj, M. M., Othman, S. H., & Musa, M. A. (2020). Study on Cybersecurity Awareness Among Students in Yobe State University, Nigeria: A Quantitative Approach. *International Journal on Emerging Technologies , 11*(5), 41-49.

Graphus. (2020). *5 Costly phishing attacks in recent history*. Retrieved 2021, from Graphus: https://www.graphus.ai/blog/5-costly-phishing-attacks-in-recent-history/

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. ,. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security,, 93*, 345-358.

Green, J. A. (Ed.). (2015). *Cyber warfare: a multidisciplinary analysis.* Routledge. Retrieved from Routledge.

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer networks, 107094*, 169.

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security, 32*, 242-251.

Gupta, S., Singhal, A., & Kapoor, A. (2016). A literature survey on social engineering attacks: Phishing attack. *2016 international conference on computing, communication and automation (ICCCA)* (pp. 537-540). IEEE.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), e00346.

Hamudin, N., & Ariffin, A. (2014). Cyber crime target – Malaysians among most vulnerable to phishing worldwide. *The Sun*, 6.

Hill, J. F. (2015). Problematic Alternatives: MLAT Reform for the Digital Age. . *Harvard Law School: National Security Journal, 1*.

Idika, N., & Mathur, A. P. (2007). A survey of malware detection techniques. *Purdue University, 48*.

Ivwighreghweta, O., & Igere, M. A. (2014). Impact of the internet on academic performance of students in tertiary institutions in Nigeria. . *Information Impact: Journal of Information and Knowledge Management, 5*(2), 47-56.

Jameel, F. (2016). Network security challenges in smart grid. *2016 19th International Multi-Topic Conference (INMIC)* (pp. 1-7). IEEE.

Johansen, A. G. (2019). *Internet scams: What they are and how to avoid them*. Retrieved from Norton: https://us.norton.com/internetsecurity-online-scams-internet-scams.html

Karagozlu, D. (2020). Determination of cyber security ensuring behaviours of pre-service teachers. *Cypriot Journal of Educational Science., 15*(6), 1698-1706.

Kaur, P., Stoltzfus, J., & Yellapu, V. (2018). Descriptive statistics. *International Journal of Academic Medicine, 4*(1), 60-63.

Kay, R. (2004). *Sidebar: The Origins of Phishing*. Retrieved 2021, from Computer World: https://www.computerworld.com/article/2575094/sidebar--the-origins-of-phishing.html

Kelley, K., Clark, B., Brown, V., & Sitzia, J. (2003). Good practice in the conduct and reporting of survey research. *International Journal for Quality in Health Care, Vol. 15*(3), pp. 261–266.

Kleczynski, M. (2018). *Breaking Down Malware: Why It's Still One Of The Biggest Threats Facing Businesses*. Retrieved 2020, from Forbes: https://www.forbes.com/sites/forbestechcouncil/2018/09/28/breaking-down-malware-why-its-still-one-of-the-biggest-threats-facing-businesses/?sh=53b533f1fe1a

Kortjan, N. (2013). A cyber security awareness and education framework for South Africa (Doctoral dissertation, Nelson Mandela Metropolitan University).

Kovačević, A., Putnik, N., & Tošković, O. (2020). Factors Related to Cyber Security Behavior. *IEEE Access, 8*.

Kumar, R., & Kaur, A. (2006). Internet use by teachers and students in engineering colleges of Punjab, Haryana, and Himachal Pradesh States of India: An analysis.

Landesman, M. (2021). *A Brief History of Malware*. Retrieved 2021, from Lifewire: https://www.lifewire.com/brief-history-of-malware-153616#:~:text=Scammers%20have%20been%20using%20a,known%20as%20Brain%2C%20was%20released.

Leszczyna, R. (2018). Cybersecurity and privacy in standards for smart grids–A comprehensive survey. . *Computer Standards & Interfaces, 56*, 62-73.

Lorenz, B., Kikkas, K., & Klooster, A. (2013). "The four most-used passwords are love, sex, secret, and god": password security and training in different user groups. *International Conference on Human Aspects of Information Security, Privacy, and Trust.* (pp. 276-283). Berlin, Heidelberg.: Springer.

Matyokurehwa, K., Rudhumbu, N., Gombiro, C., & Mlambo, C. (. (2021). Cybersecurity awareness in Zimbabwean universities: Perspectives from the students. *Security and Privacy, 4*(2), e141.

Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. *Academy of Information and Management Sciences Journal, 14*(2), 91-116.

Milošević, N. (2013). History of malware. *arXiv preprint arXiv:1302.5392.*

Morris, R., & Thompson, K. (1979). Password security: A case history. . *Communications of the ACM, , 22*(11), 594-597.

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cyber security behaviour among higher education students in Malaysia. *Journal of Information Assurance & Cyber Security., 2017*, 1-13.

Ossorio, P. G. (2006). *The behavior of persons.* Descriptive Psychology Press.

Pandey, R. K., & Misra, M. (2016). Cyber security threats—Smart grid infrastructure. *2016 National Power Systems Conference (NPSC)* (pp. 1-6). IEEE.

Ponto, J. (2015). Understanding and evaluating survey research. *Journal of the advanced practitioner in oncology, 6*(2), 168.

Popescu, G. (2014). Human behavior, from psychology to a transdisciplinary insight. *Procedia-Social and Behavioral Sciences, 128*, 442-446.

Rabon, M., & Syiemlieh, C. (2018). Awareness about Cybercrimes through Social Networking Sites among the higher secondary students. *Research journal of social sciences, 9*(9).

Rader, M., & Rahman, S. (2015). Exploring historical and emerging phishing techniques and mitigating the associated security risks. . *arXiv preprint arXiv:1512.00082.*

Rahim, N. F., Ramanchandram, R., Abdullah, S. S., & Mohammad, A. (2017). Factors Affecting Personal Information Security Behaviour Among Undergraduates At Universiti Utara Malaysia. *Journal Of Business and Hospitality Management (JBHM), 3*(1), 25-39.

Rahman, A., Malaysia, N. A., Sairi, M. T., Zizi, I. K., & Khalid, F. (2020). The Importance of Cybersecurity Education in School. *International Journal of Information and Education Technology, 10*(5), 378-382.

Rains, T. (2020). *Cybersecurity Threats, Malware Trends, and Strategies.* Packt Publishing.

Ramendran, C. (2014). Beware 'Zeus'–Police warn of danger of e-banking via smartphones and tablets. *theSun*, *25*, 1.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security, 27*(7-8), 241-253.

Rijnetu, I. (2019). *Here are the Top Online Scams You Need to Avoid Today*. Retrieved 2021, from HeimdalSecurity: https://heimdalsecurity.com/blog/top-online-scams/

Rubio, J. E., Alcaraz, C., Roman, R., & Lopez, J. (2019). Current cyber-defense trends in industrial control systems. Computers & Security. *Computers & Security, 87*(101561).

Sarathchandra, D., Haltinner, K., & Lichtenberg, N. (2016). College students' cybersecurity risk perceptions, awareness, and practices. *2016 Cybersecurity Symposium* (pp. 68-73). IEEE.

SecureWorks. (2017). *Cyber Threat Basics, Types of Threats, Intelligence & Best Practices*. Retrieved 2020, from Secure Works: https://www.secureworks.com/blog/cyber-threat-basics

Senthilkumar, K., & Easwaramoorthy, S. (2017). A Survey on Cyber Security awareness among college students in Tamil Nadu. *IOP Conference Series: Materials Science and Engineering*. *263*, p. 042043. IOP Publishing.

Shah, P., & Agarwal, A. (. (2020). Cybersecurity behaviour of smartphone users in India: an empirical analysis. *Information & Computer Security.*

Sharp, R. (2009). *An Introduction to Malware.*

Shen, C., Yu, T., Xu, H., Yang, G., & Guan, X. (2016). User practice in password security: An empirical study of real-life passwords in the wild. *Computers & Security, 61*, 130-141.

Smith, M. (1989). Computer security-threats, vulnerabilities and countermeasures. *Information Age, 11*(4), 205-210.

Sternstein, A. (2016). *This Cyber 'Safeguard'Is Hurting US Defenses. .* Defense One.

Sun, J. C., Yu, S. J., Lin, S. S., & Tseng, S. S. (2016). The mediating effect of anti-phishing self-efficacy between college students' internet self-efficacy and anti-phishing behavior and gender difference. *Computers in Human Behavior, 59*(2), 49-257.

Tarter, A. (2017). Importance of cyber security. . In *Community Policing-A European Perspective* (pp. 213-230). Springer, Cham.

Teer, F. P., Kruck, S. E., & Kruck, G. P. (2007). Empiracal study of students' computer security practices/perceptions. *Journal of Computer Information Systems, 47*(3), 105-110.

Trojovská, E., & Trojovsky, P. (2012). On Creating Animations in System Maple. *Proceedings of the 9th International Scientific Conference on Distance Learning in Applied Informatics (DIVAI 2012)*, (pp. 311-318).

Vasudevan, A., & Yerraballi, R. (2006). Spike: engineering malware analysis tools using unobtrusive binary-instrumentation. *Proceedings of the 29th Australasian Computer Science Conference, 48*, pp. 311-320.

Venard, B. (2019). The determinants of individual cyber security behaviours: Qualitative research among french students. *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)* (pp. 1-4). IEEE.

Virtič, M. P. (2012). The role of internet in education. *Proceedings of DIVAI 2012-9th International Scientific Conference on Distance Learning in Applied Informatics, Štúrovo, Slovakia*, (pp. 243-249).

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security, 38*, 97-102.

Whitman, M. E., & Mattord, H. J. (2011). *Principles of information security.* Cengage Learning.

Whitty, M. T. (2013). The scammers persuasive techniques model: Development of a stage model to explain the online dating romance scam. *British Journal of Criminology, 53*(4), 665-684.

Workman, M. (2008). Wisecrackers: A theory-grounded investigation of phishing and pretext social engineering threats to information security. *Journal of the American Society for Information Science and Technology, 59*(4), 662-674.

Yılmaz, S., & Sağıroğlu, Ş. (2013). Cyber Security Risk Analysis, Threat and Readiness Levels. *Proceedings of the 6th International Information Security and Cryptology Conferenceç*, (pp. 158-166.).

APPENDICES

Appendix A: Demographic Information of Students

Dear student,
To answer the questions in this section please put a tick " √ " in the appropriate box that best suits the answer you have selected.

Note: only one answer can be selected for a question.
PART 1: Demographics

1. Gender:
   - ☐ Female
   - ☐ Male
1. Age range:
   - ☐ 18-20
   - ☐ 21-22
   - ☐ 26-30
   - ☐ 31+
2. What is your academic class level(grade)?
   - ☐ 1st Year
   - ☐ 2nd Year
   - ☐ 3rd Year
   - ☐ 4th Year
3. Do you have access to internet connection?
   - ☐ Yes
   - ☐ No

4. How many hours do you spend on your mobile devices or computers?
   - ☐ Less than 1 hour
   - ☐ 2-5 hours
   - ☐ 6-10 hours
   - ☐ 11+ hours

Appendix B: Cyber Security Behavior Scale (CSB)

The following questions stated below will be answered with the given 5 points likert Scale, with 5 specifying that you strongly agree (SA), 4 specifying that you agree(A), 3 specifying that you don't know(DK) option, 2 specifying that you Disagree(D) and 1 stating that you strongly disagree(SD) with the idea.

		Item Abbr	SA	A	DK	D	SD
1	Willing to open email attachments from strangers	M1					
2	Interesting subject line causes the opening of email attachment	M2					
3	Very sure of the status of Anti-virus software on my personal computer	M3					
4	Interested to open attachments with multiple extensions	M4					
5	Sense something is wrong if my computer is extremely slow	M5					
6	Download freeware on the internet	M6					
7	Scan removable drives prior to using it on my personal computer	M7					
8	Installed Anti-virus software, firewall and anti- spyware	M8					
9	Willing to download materials from unsecured sites	M9					
10	Apply security patches as soon as possible	M10					
11	Password does not follow keyboard pattern	PU1					
12	Sharing password with other people	PU2					
13	Different passwords for different applications	PU3					
14	Passwords consists of lowercase, uppercase, numbers and special characters	PU4					
15	Passwords longer than 8 characters	PU5					
16	Passwords based on personal information	PU6					
17	Never change password	PU7					
18	Usage of "remember my password" option	PU8					

19	Used to write down my password	PU9					
20	Never use “Hint” to recover forgotten password	PU10					
21	Upgrading phishing knowledge by reading phishing materials	PH1					
22	Not a target of phishing Attack due to my Student status	PH2					
23	Willing to provide any confidential information to any type of email	PH3					
24	Willing to click Hyperlinks in email messages	PH4					
25	Trusting any email messages announcing contests or prizes	PH5					
26	URL must be “https” if I am transmitting confidential information	PH6					
27	Padlock symbols a must when transmitting confidential information	PH7					
28	I prefer to type URL in a new browser rather than click it on hyperlink	PH8					
29	Receiving suspicious email will make me to contact relevant party for verification	PH9					
30	Check URL spelling before any type of transaction.	PH10					
31	Not interested in reading social engineering issues	SE1					
32	Willing to give my user name and password to any one claiming to be the administrator	SE2					
33	Not a target of social engineering attack due to my status as a student	SE3					
34	Not willing to respond to text, calls or email from friendly or non-threatening strangers	SE4					
35	Willing to give my information to those who speak with authority	SE5					
36	Willing to give my password to anyone at the help Desk	SE6					
37	Check the identity and authorization of someone before talking on any issue	SE7					
38	I am not intimidated with questions by someone	SE8					
39	I will not communicate with stranger even though his/her look warrant sympathy	SE9					
40	I wouldn’t give out my confidential information under any circumstances	SE10					
41	Establish trusted relationship with online friends	OS1					

42	Ignore emails from well-known organization or establish announcing something unusual or too good	OS2					
43	Respond to Text messages announcing contests involving huge sum of money	OS3					
44	Never trusted stranger identity information given on the internet	OS4					
45	Never consider any amount of money given for services rendered on the internet	OS5					
46	Willing to deposits money requested by online friends	OS6					
47	Aware and able to identify latest online scam	OS7					
48	Trust pictures posted by strangers online	OS8					
49	Never received gifts of packages from internet friends	OS9					
50	Wouldn’t hesitate to have a face-to-face with my internet friend	OS10					

Appendix C: Consent Form for IT Students

Dear Students,
I am a Masters student from the Department of Information and Communication Technologies in Education, at the Eastern Mediterranean University conducting my Master's thesis on "Cyber Security Behavior of IT Students: An Example of EMU".
The purpose of this thesis is to determine your behavior towards cyber security threats such as malware, password usage issues, phishing threats, social engineering threats, and online scam and how you behave in certain situations.

At the end of answering the questions provided in the survey, your response will aid me in answering the following objectives:

1. How is the present condition of the cyber-security behavior of I.T Students with respect to malware, password usage, phishing, social Engineering and online scam?

2. Is there any relationship between gender and cyber security behavior of I.T students?

This survey given to you will take approximately 15 to 20 minutes of your time to complete and consists of 2 sections.
After reading the questions carefully, you are allowed to pull out from the investigation whenever. All information you have given will be kept private between my supervisor and I, and may only be utilized for this research. For additional requests or questions, please reach out to my thesis supervisor or me without hesitating. If you intentionally accept these terms and conditions and willingly agree to partake in this survey, please, fill the suitable fields underneath.

Sijuwonuola Tolu Lawal
M.S Candidate
Information and Communication
Technologies in Education
Department of CITE
Eastern Mediterranean University
Email: sybiesky@gmail.com
Phone: +903926303123

Assoc. Prof. Dr. Ersun ISCIOGLU
Master's Thesis Supervisor
Department of CITE
Eastern Mediterranean University
Email: ersun.iscioglu@emu.edu.tr
Phone: +903926303123

I have read and understood the agreements of this consent form and posed essential inquiries and got answers to my questions. I acknowledge partaking in this study willfully.

Name and Surname:

Date:

Appendix D: Ethics Committee Approval Form

Doğu Akdeniz Üniversitesi
Eastern Mediterranean University
"Virtue, Knowledge, Advancement"
99628, Gazimağusa, KUZEY KIBRIS / Famagusta, North Cyprus, via Mersin-10 TURKEY
Tel: (+90) 392 630 1995
Faks/Fax: (+90) 392 630 2919
E-mail: bayek@emu.edu.tr
Etik Kurulu / Ethics Committee

Reference No: ETK00-2019-0102 26. 04.2019

Subject: Application for Ethics.

RE: Sijuvvonuola Tolu

Faculty of Education

To Whom İt May Concern:

On the date of **26.04.2019**, (Meeting number **2019/13-08**), EMU's Scientific Research and Publication Ethics Committee (BAYEK) has granted, Sijuvvonuola Tolu from the, Faculty of Education to pursue with his MA thesis work **"I.T. Students Cyber Security Behavior: An Example of Emu."** under the supervision of Assoc. Prof. Dr. Ersun İşçioğlu. This decision has been taken by the majority of votes.

Regards,

Prof. Dr. Fatma Güven Lisaniler
Director of Ethics Committee

FGL/ns.

Appendix E: Turnitin Report

Turnitin Originality Report

Thesis_New3 by Siju Lawal

From Siju_Lawal (SCHOOL OF COMPUTING AND TECHNOLOGY)

- Processed on 30-Mar-2021 11:15 +03
- ID: 1546224250
- Word Count: 13515

Similarity Index
9%
Similarity by Source

Internet Sources:
7%
Publications:
4%
Student Papers:
2%

sources:
1

1% match (Internet from 21-Nov-2020)

https://ibimapublishing.com/articles/JIACS/2017/800299/
2

1% match (student papers from 22-Mar-2021)

Class: SCHOOL OF COMPUTING AND TECHNOLOGY
Assignment: Tengu_Njoh
Paper ID: 1539190287
3

1% match (publications)

Carlos Arriaga Costa, Orlando Petiz Pereira. "Values and trust in human capital: University students' perceptions, 2015-2017", Revista Galega de Economía, 2019
4

< 1% match (Internet from 06-Jun-2020)

https://mafiadoc.com/perceptions-of-students-and-teachers-about-the-use-_59df37971723dd9068428e92.html
5

< 1% match (Internet from 03-Oct-2020)

https://supportessays.com/subjects/thesis/
6

< 1% match (Internet from 25-Jul-2018)

http://ibimapublishing.com/articles/JIACS/2017/800299/800299.pdf