UNIVERSITY of RWANDA

Research and Postgraduate Studies (RPGS) Unit

ASSESSING THE CYBERSECURITY AWARENESS LEVEL OF UNDERGRADUATE STUDENTS AT MAKERERE UNIVERSITY

BY
SIXBERT SHEMA HABURUKUNDO

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTERS OF SCIENCE IN INFORMATION SYSTEM.
OPTION: INTERNET TECHNOLOGY

SUPERVISORS:

FREDERIC NZANYWAYINGOMA, PhD
Ass Prof. FIONA SSOZI

KIGALI, RWANDA,

24th May 2024

Declaration

I, HABURUKUNDO SHEMA SIXBERT (Reg No: 217022650) state that this research, "Assessing the cybersecurity awareness level of undergraduate students at Makerere university", done for the degree award of masters of Science in Information Systems (option: internet technology), has never been submitted or presented anywhere else for award of any other degree.

Sign: …… Date.....

HABURUKUNDO SHEMA SIXBERT (Reg No: 217022650)

Declaration by Supervisors

This research thesis has been presented for examinations with our approval as supervisors:

Sign..... Date.....

Frederic Nzanywayingoma, PhD

UNIVERSITY OF RWANDA

Sign.....Date.....

Ass Prof. Fiona Ssozi

MAKERERE UNIVERSITY

Acknowledgement

I would like to express my gratitude to a collective effort of magnificent people who helped me during this research project. Special thanks to EQIP project student exchange program for the opportunity to go to do my research at Makerere University. I thank my supervisors, Dr. Frederic Nzanywayingoma and Prof. Fiona Ssozi for their enlightenment and scholarly advice that made this research successful.

I would like also to express my sincere gratitude to my family and friends for their support and prayers. I acknowledge also my student colleagues for our team work during class activities, I am really thankful for them.

Also I acknowledge the University of Rwanda (UR), College of Science and Technology (CST), School of ICT for giving the opportunity to gain knowledge through their wonderful Lecturers.

Abstract

The constant development of technology and increase in internet connectivity have made access to information become easier. However, people becoming endlessly connected especially students have created new opportunities for cybercrimes such as phishing attacks, zeroday attacks, cyberbullying etc. and those cyber-attacks have made cybersecurity awareness an urgent matter. This study focuses on assessing the cybersecurity awareness level of undergraduate students at Makerere University because in most cases students engage in digital misconduct due to lack of awareness on cybersecurity. The study used a sample of 400 students from nine colleges and the school of law as the tenth at Makerere University. Data was collected using questionnaire and data was collected using convenience sampling technique. Quantitative analysis was done using the analytic hierarchy process (AHP). And IBM SPSS Statistics was used during data analysis. Different statistical test were conducted, where Cronbach's Alpha technique was used to do the reliability test, Pearson correlation coefficient technique was used to do the validity test and to test the correlation and homogeneity between variables, the Bartlett's test and the Kaiser–Meyer–Olkin (KMO) test were conducted. Awareness was assessed using three variables as dimensions: knowledge (what does a person know), attitude (how do they feel about the topic) and behavior (what do they do). The results found showed that the level of awareness is 67.4% which falls under the average or satisfactory criteria which means that action is potentially required. Those dimensions were assessed on six focus areas: (a) password security, (b) cyberbullying, (c) phishing, (d) malware, (e) identity theft, (f) downloading, sharing, and use of pirated content. In the end the research presents recommendations based on the data collected to tackle the problem.

Keywords: awareness level, cybersecurity, undergraduate students, Makerere University

Table of Contents

List of Figures

List of Table

CHAPTER 1: INTRODUCTION

1.1 Background

More than 5.3 billion people were using internet globally by 2022 (ITU, 2023). According to DATAREPORTAL by January 2022 Uganda had a population of 47.77 million and there were 13.92 million internet users, The number of internet users increased by 1.8 million (+15.1%) between 2021 and 2022 and internet penetration was 29.1%; there were 2.8 million social media users equivalent to 5.9% of the total population; also there were 27.67 million mobile connections equivalent to 57.9% of the total population. The number of mobile connections in Uganda decreased by 698 thousand (-2.5%) between 2021 and 2022. With this increase of internet and electronic devices connectivity it has also created the opportunities for cyber-attacks such as unauthorized access, malware attack, zeroday attack, data breach, denial of service (DoS), social engineering or phishing etc. (Iqbal et la., 2020). Cyber-attacks exploit that increase in connectivity and complexity of critical infrastructure systems, put the Nation's security, health, economy, and public safety at risk. Critical infrastructure is defined in the U.S. Patriot Act of 2015 as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." (NIST, 2018). In that case if cyber-attacks are not taken seriously they can ruin a company's ability to innovate, to get and keep customers.

This research focus on undergraduates students at Makerere University to assess their level of awareness on cybersecurity. This is because cyber-attacks have increased at a high rate in recent years, for example in 2010, there were less than 50 million unique malware executable known to the security community. By 2012, they were double around 100 million, and in 2022, there were more than 1300 million malicious executable known to the security community, and this number is likely to grow according to the statistics of AV-TEST institute in Germany. In 2020, cybercrime magazine estimated that over the next five years the cost of cybercrimes was going to grow by 15% per year reaching $ 10.5 trillion USD annually by 2025, up from $ 3 trillion USD in 2015 globally.

According to the above statistics you can't ignore the fact that even university students are among the victims of the cyber-attacks or cybercrimes and they are future leaders of different organizations. Therefore to assess their level of awareness on cybersecurity is a very important issue. These days securing the confidentiality and the integrity of the information in the system of complex networks is very important and challenging. And mostly students are connected to these networks. In accordance with (Senthilkuma & Sathishkumar, 2017), curiosity and revenge maybe the primary reasons for students to get involved in cyber-crimes and most of the time students are not aware of the implications of cybercrime and girls are the most found victims of the cyber-crime. Many reports shows that universities and colleges are hacked into their information systems with the attempts of stealing valuable intellectual property and their property and their research data such as patents awarded to the professors and students, and also the personal information about the students ,staff and faculty. (Senthilkuma & Sathishkumar, 2017).

This research concentrate on undergraduates students at Makerere University to assess their level of awareness on cybersecurity, which include password management, cyberbullying, social engineering (including phishing, online scams and frauds), malware, identity theft, and general secure behavior (e.g., downloading and sharing "pirated" film and TV content, using pirated software). So that Makerere University can set policies to increase the cybersecurity awareness level of students and to see where to put much strength for the safety of its cyberspace.

1.2 Problem statement

Nowadays the internet is being used mostly in every aspect of people's life. People are connected in order to do: online banking, business establishment, virtual healthcare, video calls, education etc. Though being endlessly connected have increased risks. Therefore as people, cybersecurity risks guide to creating threats to finances, identity, and privacy. For example (Adamu, et al, 2020) did a research in Nigerian universities with the objective to see how students in this developing country are aware of cyber-attacks, the means they use to protect themselves from the attacks and to see if cybersecurity is part of programs they take at the university. The results showed that students have basic knowledge about cybersecurity but they are not aware of how to protect their data. And it appeared that many universities did not have active programs for cybersecurity to enhance student's knowledge on ways to protect themselves from cyber threats (Adamu, et al, 2020). In 2021, Talal and Asifa did a research to evaluate and investigate the level of cybersecurity awareness and user compliance among undergraduate students at Majmaah University, they found that many of the participants were unaware of the cybersecurity fundamentals and did not know ways to manage their data, although 92% of them did a formal program of security awareness (Talal & Asifa, 2021).

The persistent psychological need to remain connected via an increasing variety of electronic devices further exposes individuals to online risks (Mochiko, 2016). In the Silicon Valley in California, USA, student's attitude toward cybersecurity was evaluated by Moallem. The author mainly focus in most advanced technological places in the world by evaluating the cybersecurity level among students because their behavior is extremely diverse. Even though college students were aware that their activities were monitored and observed, they were not conscious of the safety of their information and across university networks their data were not securely transmitted (Moallem, 2018). Therefore to increase the awareness of cybersecurity in high education institutions it is needed because nowadays computer and internet have become important resources in every day's work and studies.

1.3 study objectives

1.3.1 General objective

This thesis has an objective of assessing the level of awareness on cybersecurity among undergraduate students at Makerere University. And provide a recommendation.

1.3.2 Specific objectives

- To identify the attitude, knowledge, and behavior the undergraduate students at Makerere University have on cybersecurity.
- To identify means undergraduate students at Makerere University use to prevent themselves from cyber-attacks.

- To provide an appropriate solution to increase awareness level among undergraduate students at Makerere University.

1.4 Research questions

- What attitude, knowledge, and behavior do the undergraduate students at Makerere University have on the six focus areas?
- What are means do the undergraduate students at Makerere University use to protect themselves against cyber-attacks?

1.5 Scope of the study

This study focus on the undergraduate students at Makerere University. I have chosen undergraduate students because they come at the University with different backgrounds and some of them have little knowledge about cybersecurity and some of them don't have any knowledge at all. This thesis will assess their level of awareness on cybersecurity and then propose a solution.

1.6 Significance of the study

The study's findings will help Makerere University to know how much efforts it should put in cybersecurity awareness and set policies to protect its cyberspace.

This study also will provide a strategy to be used in order to increase the level of awareness among university students not only at Makerere University But also in other universities in Uganda especially undergraduates students who start universities without much skills about cybersecurity so that they can be aware of cyber-attacks, due the fact that some of them start to use computers when they start university studies.

The purpose of this thesis fall under the computer Misuse Act, 2011 which is an Act to make provision for safety and security of electronic transactions and information systems; to prevent unlawful access, abuse or misuse of information systems including computers and to make provision for securing the conduct of electronic Transactions in a trustworthy electronic environment and to provide for other related matters. (GOU, "The Computer Misuse Act," 2011, Preamble). This suggest that anyone found breaking the requirement of the Act is regarded as a criminal and legal proceedings could be set in motion against such a person. So this means that if the level of awareness is good undergraduate students won't be found violating this Act.

CHAPTER 2: LITERATURE REVIEW.

2.0 Introduction

This chapter reviews literature from different authors following the objectives of the study. It addresses the research gap and the Information security awareness measurement framework.

2.1 Cybersecurity definition

Cybersecurity is a set of technologies and processes designed to protect computers, networks, programs and data from attack, damage, or unauthorized access. (Steven, 2017) and also the process of protecting cyberspace from attacks by criminals and other adversaries is called cybersecurity. (Eric, 2017). According to (Eric, 2017) ICT devices and components form a highly interdependent system of networks, infrastructure, and resident data known as cyberspace. The likelihood of cyber-attack depend on three factors: threats (who is attacking), vulnerabilities (what weakness they are attacking) and impact (how the attack affects the victims). (Eric, 2017) defined these factors as follow:

The threats: are people who perform cyber-attacks generally fall into one or more of five categories: criminals intent on monetary gain from crimes such as theft or extortion; spies involved in espionage stealing classified or proprietary information used by government or private entities; nation-state adversaries who develop capabilities and undertake cyber-attacks in support of a country's strategic objectives; "hacktivists" who perform cyber-attacks for nonmonetary .reasons; and terrorists who engage in cyber-attacks as a form of non-state or state sponsored warfare. (Eric, 2017)

The vulnerabilities, attackers and defenders are engaged in a cybersecurity arms race. Attackers constantly probe ICT systems for weaknesses. Defenders can often protect against them, but three are particularly challenging: inadvertent or intentional acts by insiders with access to a system; supply chain vulnerabilities, which can permit the insertion of malicious software or hardware during Development or acquisition; and previously unknown, or Zero-day, vulnerabilities with no established fix. (Eric, 2017)

The impacts, a successful attack can compromise the confidentiality, integrity, and availability of an ICT system, the information it handles, and things to which it is connected. Cyber theft or cyber espionage can result in exfiltration of financial, proprietary, or personal information from which the attacker can benefit, often without the knowledge of the victim. Denial-of service attacks can slow or prevent legitimate users from accessing a system. Botnet malware can give an attacker command of a network of "zombie" computers or devices for use in cyber-attacks on other systems. Attacks on industrial control systems can result in the destruction of the equipment they Control, such as generators, pumps, and centrifuges. (Eric, 2017)

2.2 Literature review

A survey in Middle East was done by Al-Janabi and Al-Shourbaji on security awareness, studying on security awareness among academic staff, researchers and students and focusing on educational setting. They found that the participants in the Middle East were not significantly aware of cybersecurity essentials. In that case, the overall management plan for security should add trainings and security awareness for all users and administrators (Al-Janabi & Al-Shourbaji, 2016). There

is a security assessment on a group of students at the College of Business and Economics at California State University, Los Angeles, USA done by Slusky and Partow-Navid. They found that the main problem was not the absence of the required information about cybersecurity awareness, as they were expecting it, rather the approach student were using to deal with that information in practical circumstances. Their findings were used to help the college to design its syllabus which added additional information security trainings (Slusky & Partow-Navid, 2012).

A study on the relationship between the awareness of phishing (a form of social engineering which uses emails to maliciously solicit information from computer users, such as login or financial account details) and users falling victim to phishing was done by (Rajan, 2010). The study concluded that despite of having knowledge and understanding the importance of being ware of phishing, people still fall for phishing attacks. This is due to wrong behaviors regarding online security. (Dodge & Ferguson, 2006) simulated phishing emails to give rise to user awareness. The study was done on students at the United States Military academy to assess their awareness level for the purpose of awareness program. Doing that exercise, it increased the awareness. In 2007 a similar study was done on higher education stuff in the Western Cape Province of South Africa by (Steyn, et al, 2007), during their study found that email security should be prioritized for awareness activities and education. According to (Mishra, 2014) people believe that anti-virus programs prevent their computers from being compromised and also some people believe that firewalls are the same as anti-virus applications. Both studies found that correct attitudes and correct awareness in addition to knowledge in promoting online security behavior are essentials.

A research by (Pramod & Raman, 2014) about smartphones usage by students in higher education, discovered that students in higher education know about security concerns but they don't really understand all the security risks and the importance of security practices. A recommendation of training and awareness campaigns was given by (Pretorius & Van, 2015) after finding the vulnerabilities in industrial control systems caused by unpatched software, insecure password management, and outdated or uninstalled anti-virus and malware protection. These research showed how there can be a disorder between cyber security attitudes, knowledge and behavior.

(Lennon, 2015) discovered over a 10 year period cyber-espionage campaign to attack government, businesses and journalist in south Asia and India. The campaign was employing both social engineering and malware. In April 2014 the Heartbleed was broadcasted and made the news as biggest security vulnerability in IT history (Mitre, 2014). In that month Internet Explorer was not recommended to the users because of extreme vulnerability in the browser where without knowing malware could be installed over webpages browsed (Rosenblatt, 2014). Botnet activity and a number of distributed denial of services (DDoS) attacks were globally recorded in September 2014, within an hour of the ShellShock/BashDoor vulnerability being disclosed (TroyHunt, 2014). These attacks showed the importance of awareness in terms of patching and updating machines, and additionally the importance of awareness in terms of social engineering and phishing, so that to protect against ronsomware, sophisticated attacks and other attacks.

(Mensch & Wilkie, 2011) did an experimental research on college students and they found that installation of security tools and applications create a wrong sense of security in connection to personal information protection. (Janssen, 2014) said that if a person's identity is stolen online

may stand heavy consequences such as financial charges and damaged credit scores. If identity information data held by universities were sold on cyber black market, they would possibly be worth billions of dollars (Wlasuk, 2012).

(Kim, 2014) discovered that many college students in the United States did not do information security awareness training, and they seem to understand the importance of the trainings. The study also found that students learning about security happened little by little, and to develop a continuous secure behavior they needed to do more focused information security awareness training. This also showed the likely separation between having sufficient knowledge and understanding and having a good secure practice.

(Kaur & Mustafa, 2013) did an investigation on small and medium enterprise's employees about information security awareness, and they found that employees were affected by attitude, behavior and knowledge. The research discovered that attitude and behavior had significant relationships with security awareness, but knowledge did not. (Bada & Sasse, 2014) and (Aliyu et al., 2010) both studies on Malaysian students and IT, found that computer ethics and security were affected by attitudes and perception. A study on e-commerce customers about knowledge, attitudes and practices by (Bakar et al., 2013) found that there were small knowledge about legal provisions and encouragement for better behavior and attitudes was needed to reduce the odds of the customers falling victims to cyber criminals. The baseline of cybersecurity insight levels are attitudes, skills and knowledge and the relationships between these are needed to guide the training (Peltier, 2005).

(Aliyu et al., 2010) found that Malaysian university students were big violators of security and computer ethics as they were frequently careless when browsing and posting contents and all the time involved in illegal use via sharing and downloading of fake software, TV series and films. Based on some factors such as laziness and economic standing, the students were found not to practice safe computing at all.

The general conclusion that come out from the literature is that education and trainings are major initiatives drives to produce cybersecurity awareness and reduce bad online security behavior. The research examined in the literature also proposed that knowledge, self-insight of skills, real skills and behaviors, and attitudes, are all suitable to evaluating cybersecurity awareness, and knowledge only is not enough to guarantee cybersecurity awareness.

2.3 Cybersecurity in Africa

In 2018**,** Africa had a population of 1.24 billion and yet it had 7,000 certified security professionals, or one for every 177,000 people. Between 2000 and 2016 Africa's ICT sector expanded by 7,000 percent with increase in internet penetration of approximately 28% (Kwasi, et al, 2018)**.** (Nir, 2019) quoted Bulent Teksoz from Symantec Middle East where he said that "Cybercrime is shifting towards the emerging economies. This is where the cyber criminals believe the low-hanging fruit is" ironically African economies have become a major source and additionally victims of cyber-attacks. Serianu firm, a pan-African based cybersecurity and business consulting firm reported that in 2017 African economies lost $ 3.5 billion on cybercrimes and in that same year, annually Nigeria and Kenya lost an estimation of $649 million and $210million respectively

on cybercrimes. On the report of South Africa Banking Risk Information Center (SABRIC), annually South Africa loses $175 million on cybercrimes. (Nir, 2019).

Hamadoun Toure, an ex-secretary general of the International Telecommunication Union (ITU) discussing on increasing cyber victimization in African, he said that "At the moment, cybercriminals see Africa as a safe haven to operate illegally with impunity". Symantec had spotted 24million malware events that targeted Africa in 2016. Symantec reported that in 2013 there was a high increase in rate of cybercrime in Africa than any other region in the world. In 2016 financial institutions in Ghana experienced more than 400, 000 incidents linked to malware, 44 million related to spam emails and 280,000 connected to botnets. (Nir, 2019).

Business software alliance reported that two African countries Libya and Zimbabwe in 2017 were the ones with the highest software piracy rates in the World where the percentages of unlicensed software in the two countries were 90% in Libya and 89% in Zimbabwe. Because pirated software cannot be updated from producers, they increase the spread of malware. (Nir, 2019).

Lack of skills is another problem among internet user in Africa in order to safeguard themselves from high growing cyber-threats. Like in any other developing countries African internet users don't have much experience and they are not technically sharp. A high percentage of them are receiving computer machines and being connected for the first time. And most of them also don't understand English language. This is a significant point because most of the instructions and contents for security products are available in English language only. Cybersecurity products are built in English language so many African internet users cannot access them.

Even though cyber-attacks attacking African economies are rising, there are numerous positive and encouraging gestures. Enforcement measures and cybersecurity legislation in the continent step by step are improving. Many private sector enterprises have risen in order to help and to build up cybersecurity space of the continent.

2.4 Cybersecurity in Uganda

Since the daybreak of internet space in Uganda, various cybercrimes have been registered. Cybercrimes have involved the hacking of email accounts and many website scams that were aiming Ugandans and citizens of other countries. Illegal online transfers of funds, hacking of bank accounts, cyberbullying, email scams, sending malware to others and stealing of people's information are the most common cybercrimes in Uganda and are reported on large scale (Scott & Marry, 2020). In accord with (Paul, 2017) operating strategies of cyber criminals are evolving year by year, they are developing new techniques and tools in order to take advantage of the changes in consumers and business behavior. And as banking, e-commerce and more services are becoming available via mobile apps, mobile phones continue to be vulnerable to cybercriminals. The poor password practices in the Internet of Things (IoT) devices have made cybercriminals jump into IoT in order to take over those devices for their own objectives.

In 2013, the police annual report stated that cybercrimes cost Uganda around UGX. 18 billion. Kaspersky labs released another figure and put the figure at UGX. 25 billion. These figures were in the same range with the figure released by an auditing firm Deloitte. In 2016 the report shows that the country made of a loss of UGX.122 billion to cybercrimes. Cybersecurity researchers in

2017 revealed that Uganda lost close to UGX. 15 billion to cybercriminals in 2017 alone. During the time of review unreported or unresolved cybersecurity incidents were 95.6% and only 4.4% of the cases which were reported were followed through to a successful prosecution (Scott & Marry, 2020).

In Uganda cybercrimes have gone beyond the individual level, companies have been also targeted years ago. The country's largest company in telecommunications MTN Uganda was a victim in one of the scams that made the company and even the government to lose millions of Ugandan shillings (Ndagire, 2020).

Although those cases happened and many more others, in 2018 Uganda was ranked the first in Africa and 40th in the world by the Estonia's E-government Academy Foundation Company in Global Nation Cybersecurity Index with the index of 49.35 (Osekeny, September 24, 2018). The readiness of countries to prevent themselves against cyber threats and management of cyber incidents is what the National Cybersecurity Index measures. Uganda coming first in Africa and 40th in world put Uganda ahead many developed and developing countries. For example Uganda is ahead Israel which was 42nd globally and even china which was 62nd globally. In Africa Uganda came ahead Mauritius which was 2nd and 43rd globally, Nigeria which was 3rd in Africa and 45th globally and South Africa which was 75th globally (Osekeny, September 24, 2018). If Uganda can outperform these countries it means Uganda has learned from the mistakes of other countries and set measures to protect its cyber space.

The Ugandan government created and ratified a number of cyber laws supported by earlier laws, for example the official Secret Acts, 1964 (Section 4 (1) (d)) and the Secret Organisations Act, 2005, to give a base for the country to create protection in a digital age which include the Computer Misuse Act, 2011, the Electronic Transaction Act, 2011 and the Electronic Signature Act, 2011.

Uganda also put in place The Communications Sector Computer Emergency Response Team (CERT), the National Information Security Framework (NISF) and the National Information Security Strategy (NISS), 2011 to supervise a strong readiness in cybersecurity (ict.go.ug).

2.5 Identifying research gap

Studies on the level of awareness on cybersecurity among college students have been conducted for example (Moallem, 2018), (Adamu, et al, 2020), (Talal & Asifa, 2021), (Phuong & Andrea, 2021), (Mohammed, 2022), etc. these studies have been conducted in different countries and different universities but in Uganda there are no found researches about the level of awareness on cybersecurity among university students. As Uganda is developing it's cyber space it raises also the problem of security in that cyber space which brings the curiosity of knowing how college students are aware of cyber-attacks or cyber threats they can face online as they are a big number of technology users in nowadays.

(Mohammed, 2022) did an assessment about cybersecurity awareness among college students at Imam Abdulrahman Bin Faisal University. His assessment was based on essential three points: password security, browser security, and social media. Mohammed found that students understand the importance of cybersecurity awareness. Even though practically when it comes to password security, students' levels of cybersecurity are still lacking. For example students did not pay much

attention to using strong and correct passwords to protect their accounts or websites (Mohammed, 2022); (Adamu, et al, 2020) did a research in Nigerian universities with the objective to see how students in this developing country are aware of cyber-attacks, the means they use to protect themselves from the attacks and to see if cybersecurity is part of programs they take at the university. The results showed that students have basic knowledge about cybersecurity but they are not aware of how to protect their data. And it appeared that many universities did not have active programs for cybersecurity to enhance student's knowledge on ways to protect themselves from cyber threats (Adamu, et al, 2020); (Phuong & Andrea, 2021) did a study of comparing the level of cybersecurity awareness, knowledge and behavior via using smart phones among university students in general particularly between Vietnam and Hungry. Without any barriers between the countries, Phuong and Andrea found that university students in different fields of study were lacking not only cybersecurity fundamental knowledge, but also, good practices in their daily experience while using their smartphones, beyond the differences in respondent's country (Phuong & Andrea, 2021).

This research focus on undergraduate students at Makerere University. It will help to know the level of awareness on cybersecurity among undergraduate students as it was not done before because there are no found literature about level of awareness on cybersecurity among college students in the context of Uganda. After finding the level of awareness among undergraduate students at Makerere University this research will give a recommendation to the Makerere University of based on the findings.

2.6 Information security awareness measurement Framework

This research was conducted using the adapted model by (Kruger & Kearney, 2006). The model adapt a social psychology theory called the Theory of Planned Behavior (TPB) as an aid that offer three elements to measure a favorable or unfavorable manner to a particular object; these are cognition, affect, and behavior (Kruger, et al., 2010). The elements were used to build three similar dimensions known as Knowledge (what does a person know), attitude (how do they feel about the topic), and behavior (what do they do) (Sari, 2012). The focus areas were adapted from (Chandarman & Van, 2017). The focus area used are approach related to cybersecurity. There are a total of six focus areas used, (a) password security, (b) cyberbullying, (c) phishing, (d) malware, (e) identity theft, (f) downloading, sharing, and use of pirated content (Chandarman & Van, 2017). I have chosen this framework because it is a widely applied model which has met with some degree of success in predicting cybersecurity awareness level (Sari & Candiwan, 2014; Chandarman & Van, 2017; Balqis & Candiwan, 2020). And also because the TPB details the determinants of an individual's decision to enact a particular behavior (Mark & Christopher, 1998). The framework was adopted from (Sari & Candiwan, 2014) and (Chandarman & Van, 2017).

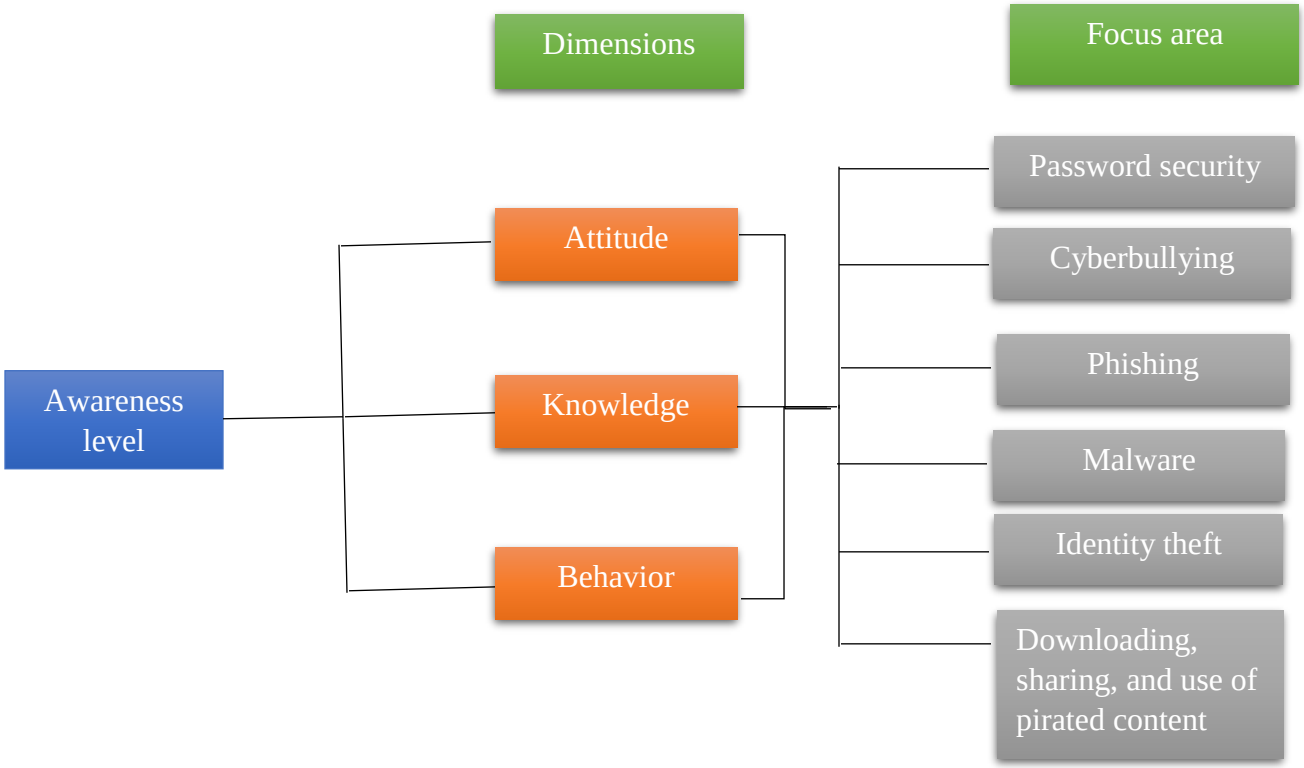

Figure 1. Information security awareness measurement framework (Sari & Candiwan, 2014) and (Chandarman & Van, 2017).

2.6.1 Focus areas

This section discuss about the focus areas of the research.

2.6.1.1 Password security

In computer security, authentication is one of the most important areas, and the text-based passwords tradition usage has been well studied. But, this kind of authentication system has disadvantages. Many different authentication systems that have purpose of setting security and usability have been suggested. The suggestions were from graphical password to location based authentication (Forget, 2012), (Goldberg, et al, 2002) and (Thorpe, et al, 2013). No matter how, no one of these systems could defeat the simplicity and affordability of typing sequence of keyboard characters to permit authenticating users (Bonneau, et al, 2012). Sadly, in terms of usability, text-based password authentication is quite problematic. A good password needs to be "easy to remember and hard to guess" at the same time as suggested by (Wiedenbeck, et al, 2005).

In information systems, passwords are observed as one of the most remarkable risk factors in terms of security because they are vulnerable to attacks (Carstens, et al, 2004). User practice and behavior are the main cause of this vulnerability. The memorability issue is the main problem which cause the other problems associated to passwords for example, sharing, reusing and choosing weak passwords. These problems are known as the human factor problems in password authentication domain (Herley, 2009) and (Summers & Bosworth, 2004). It is frequently said that passwords

should contains a mixture of keyboard characters and should not contain meaningful words from dictionaries (Yan, et al, 2004).

There are various details to password security that need to be considered. These involves the way in which passwords are stored. A secured password storage is important in protecting passwords from malicious threats. There are different methods of storing passwords such as, hashing, plain text, salted hashing and rainbow tables. Another issue to be taken seriously is password theft, password can be stolen through social engineering, brute forcing, keylogging etc.

(Katha, 2016) discussed different aspects of password security as follow:

Password storage

A password can be composed of characters, numbers and other special characters. Passwords can be entirely numbers which are called passcodes and re frequently used as Personal Identification Numbers (PINs) in ATMs and net baking operations. Online passwords are stored in many different ways, some are considered to be more secured than others and some are considered to be very vulnerable to attacks. Below are some few most popular ways to store passwords.

- **Plain Text Passwords**: This is the simplest form of storing a password. Somewhere on the server of the site, there is a database which stores passwords and usernames in plain text. If the password is 'PassText321'then in the database, the password is stored as 'PassText321'. This is the worst form of storing passwords in terms of security. The passwords are immediately compromised when they are stored in human readable form, if the site is hacked. The hacker can read all the passwords with virtually no extra effort.
- **Encrypted Passwords:** Encrypted form of passwords are stored in the database on the servers of many sites. A special key is used in encryption to convert password into a random string of text. The advantage is that, the hacker cannot obtain the passwords if he/she does not have the key, only randomly encrypted strings are obtained. When a server is hacked and the key is retrieved, all the passwords are decrypted and compromised. Encryption is reversible is a fact, for example, a message can be coded and decoded poses a security threat.
- **Hashed Passwords:** Hashing is a function that will turn the password into a random long string of letters and numbers. Hashes have the advantage of being irreversible over encryption. There is no existing algorithm to reverse the hashed password to its original password because, the hacker is supposed to hash a combination of numbers one by one to find hashes that match with the one that are stored on the server. One way to do this is rainbow tables, which are computationally very fast. Hackers can also use a brute force attack, where every possible combination of letters and numbers are tried, hashed and matched with the hash retrieved from the database. MD5, SHA-1, SHA-256, and SHA-512 are types of hashing algorithms.
- **Salted Hashes:** To make hashes more secure, 'salt 'can be added to the hash. This means that, a random string of characters is either prefixed or post fixed to the password before hashing it. Every password has a different salt. Even though the salts are saved on the database, using a rainbow table, it is very complicated to crack the passwords as the salted

passwords are long, unique and complex. Salted hashes can be brute forced but the time taken is significantly longer. Using two salts, one public and one private can also protect the password against offline attacks (Manber, 1996).

Password Theft

Passwords can be leaked in a number of ways. An attacker can hack into the database of the site which stores the user credentials and uncover a huge number of passwords. On a personal level thefts can also occur. A user can write down the password somewhere and it can make its way to malicious hands. Or a user can set a very simple and obvious password that is easy to guess. Social engineering, phishing or keyloggers can also compromise passwords (Gayathiri, 2012). Passwords can very commonly be uncovered by brute forcing or offline dictionary attacks.

Password strength

A brute force attack tries every possible combination in a given character set and tries to match it against the original password. So more the number of possible combinations, more the time it will take for the algorithm to generate the guesses. On an average, almost half of the total number of combinations is tried before striking on the right one. A strong password take a long time to break. So it is logical to conclude that greater the length of a password, the better it can stand against a brute force attack. Let the length of the password that is to be cracked be N. Let say the password consist of alphabets only in lower cases. This forms the character set. The possible candidates for each character of the password are 26. For a more generic case, let the character set consist of k characters. Then the number of possible passwords can be Nk. So, the length of the password can increase by either increasing N or by increasing k. If the length of the password is 6 and it is made up of only lower case alphabets then the number of possible passwords is 266 which are 308915776. If it were made of upper and lower case characters then the character set size would be 52 and the possibilities would be 526, which is 1.9770 x 1010. If the password size is 7 then the possibilities would become 267 and 527

It very clear from this literature that passwords should be taken seriously. Easy passwords can be broken and data can be compromised. Organizations should take strong measures to ensure that their data are secured sufficiently by making sure that correct schemes are implemented to protect against hacks. And also the role played by users in securing their data is encouraged.

2.6.1.2 Cyberbullying

Cyberbullying is a type of bullying that happens in the digital domain/medium of electronic text (Wong-Lo & Bullock, 2011). Online bullying, electronic bullying, or cyberbullying are new methods of bullying implying actions of bullying interpreted as using technology to harass people, for example on Facebook, twitter, email, etc. chat rooms, mobile phone texting and cameras, picture messages (including sexting), instant messages (IM), and/or blogs (Miller & Hufstedler, 2009; Beale & Hall, 2007). The frequent common sites in which cyberbullying were email (21%), online chat rooms (20%), social networking sites (20%) and mobile phones (19%). Other websites (8%) and other forms of texting, such as Twitter (6%), were also reported. Through free-text response, 12% of participants also reported MSN Messenger as a cyberbullying tool (Charles, et al, 2013).

All teens surveyed use the Internet on a regular basis Teens using social networking sites Usage per day	95% 80% 48%
Students visit sites for information: movies, TV shows, music groups, sports stars, or health information and use social networking sites	81%
Visit websites to get news	62%
Watched a video on a video-sharing site such as YouTube or Google Video	57%
Looked online for health, dieting or physical fitness information	31%
Got information about a college, university or other school they are considering attending	55%
Purchased something online like books, clothes or music	49%
Teens who use social media, reported that they have witnessed someone being mean or cruel to another online, with 12 saying this is a 'frequent' occurrence.	88%
Students who are online revealed that they have created online content of some kind	64%

Table 1. Tools cyberbully can use (Charles, et al, 2013).

Past generations, once they had arrived home from school, they were safe from the peer pressures, abuse and judgment (at that time the class bully would never call you house back then). But today cyberspace has no limit, and students have only their intelligence to defend themselves from harassment, teasing and threats that can reach them online anytime (Mustacchi, 2009). Associate professor of criminal justice at the university of Wisconsin-Eau Claire and co-author with Hinduja of Bullying beyond the Schoolyard: Preventing and Responding to Cyberbullying, Patchin said that "Cyberbullying is tailor-made for the relational aggression and rumors that girls typically engage in" (Adams, 2010).

Reasons for Cyberbullying

Causes for cyberbullying are: prejudice, envy and injustice for disability, gender, pride, religion, shame, guilt, and anger. (Hoff & Mitchell, 2009; Jones, et al, 2011). Table 2 shows other reasons for cyberbullying. These certain whys that can explain the use of cyberbullying by those who could not confront their victims face to face.

Reasons for cyberbullying
Anonymity Approval
Boredom Feel Better
Instigate Jealousy
No perceived consequences Projection of feelings
Protection Reinvention of self
Revenge

Table 2. Reasons for cyberbullying (Charles, et al, 2013).

(Mesh, 2009) stated that cyberbullying occur mostly common from relationship problems (break-ups, envy, intolerance, and ganging up); victims face negative effects especially on their social wellbeing; and reactive behavior from schools and students is mostly inappropriate, absent, or

ineffective (Hoff & Mitchell, 2009). According to (Sahim, 2012) there is a significant correlation between a cyber-victim and loneliness among adolescents.

The virtual world put together distance and intimacy in a special way that brings up new questions about personal development and social life of young people (Cowie & Colliety, 2010). Educators should teach children and young people skills to control risks successfully, to be aware of how they can defend themselves and to support vulnerable peers who are being mistreated online. According to (Rivers & Noret, 2010) virtual interactions should not be considered fantasy since they are real to the young people engaged with them.

2.6.1.3 Phishing

Phishing is a social engineering technique which use many methods to influence the target of the attack to tell personal information, such as username, password, financial information, or email address. And the given information is used to mischief the victim by the attacker (Stavroulakis & Stamp, 2010). The term phishing is acquired from the word "fishing", the idea of the terminology is that an attacker uses "bait" to direct the victim and then "fishes" for the personal information they want to steal. For the first time phishing attack was reported in 1995, when a hacker convinced the victims to share the details of their AOL accounts (Jakobsson & Myers, 2006) and (Rekouche, 2011). In the media for the first time the word "phishing" was printed in 1997 (Rader & Rahman, 2013).

The Anti-Phishing Work Group (APWG) announced that since 2016 and in the third quarter of 2019, phishing rates rose to their highest levels (APWG, 2019). Graph 1 show the trends in phishing websites from 2013 to 2019. Moreover, phishing attacks continue to be highly used, such as the most common infection vector called spear phishing is used to distribute malware, in 2018 it was used by 71% of the groups and in 2019 it was used by 65% of the groups, Graph 2 shows (Symantec, 2018). In addition, the number of Uniform Resource Locators (URLs) phishing increased by 20% from 2017 to 2018, nowadays, the two-thirds of these phishing websites are using a Secure Sockets Layer (SSL). This is the highest rate since 2015, which shows that HTTPS is no longer a good indication of a site's safety (APWG, 2019).

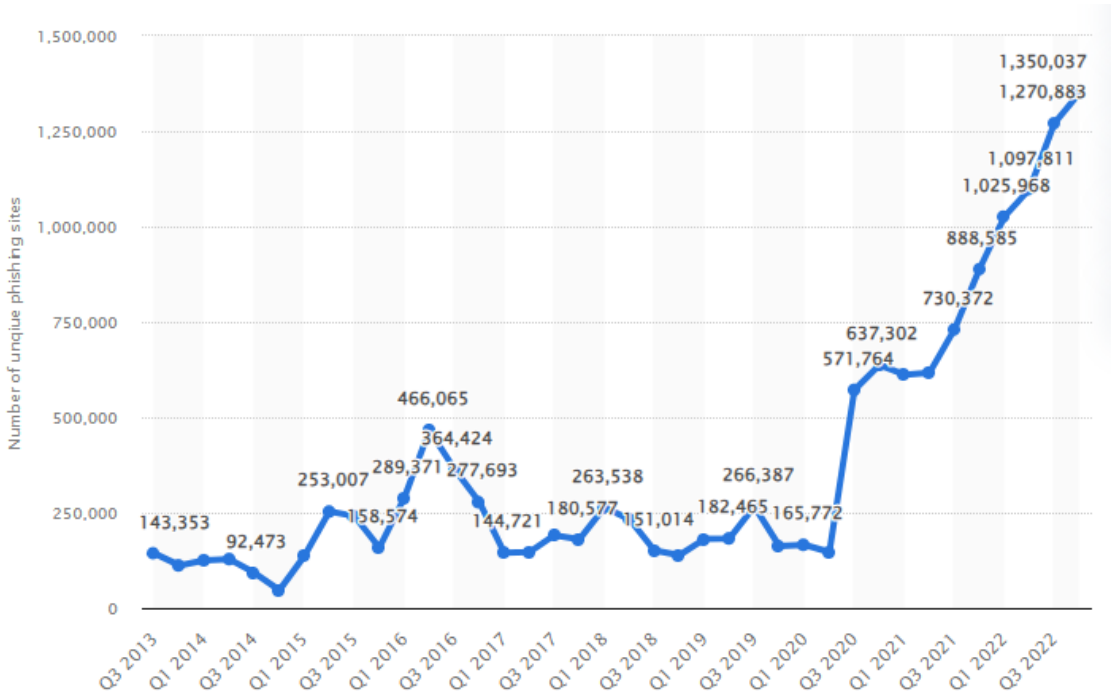

Figure 2. Number of unique phishing sites detected worldwide from 3rd quarter 2013 to 34th quarter 2022 (statista, 2023)

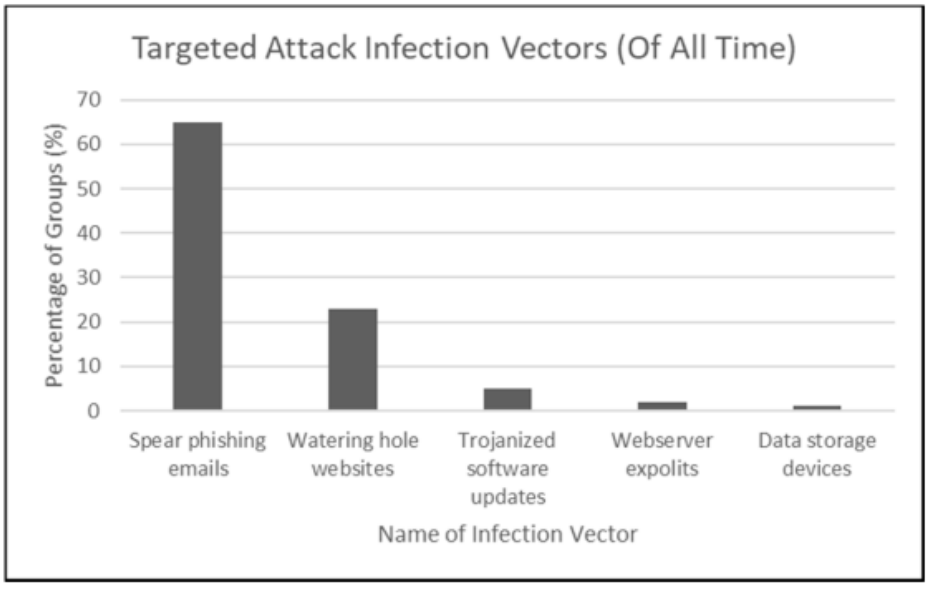

Figure 3. Targeted attack infection vectors (Anti-Phishing Working Group).

Software as a service (SaaS) and webmail have been the main focus of phishers in recent years, they are considered to be 33% of the attacks against different industry sectors (APWG, 2019). IBM found that 27% of phishing attacks were targeting webmail services. X-Force analyzed the attacks

against businesses and found that 29% of the attacks were breaches of a phishing email (IBM, 2019).

FBI receive around 100 complaints in 2018, from the most known targeted industries being healthcare, education and air travel, which was followed by a total net loss of approximately USD 100 million combined. The scam used the phishing emails to target the employees in order to get their login credentials. And these were used to get access to the payroll system and after that the phishers implemented rules so that employees no longer get notifications about changes in their accounts. The phishers were able to change account owner's direct debit information to channel the funds into their own accounts which in this case involved a prepaid card (IBM, 2019).

Industries such as healthcare and education where people are playing online games the consequences of phishing attacks are high felt. An example, there was a phishing scam that had a purpose of stealing the user login credentials for steam (a PC gaming platform) by giving a "free skin giveaway", it shown in Figure 2, the scam was started by the feedback left on user's profile, which once clicked, direct the victim to the phishing website with information about the giveaway and even a fake scrolling chart bar to give an impression of legitimacy. The victim was asked to login via Steam which took them to a fake login screen where credentials were taken. The attack extended to generating a real Steam guard code (i.e., two-factor authentication), which gave the phisher permission to the victim's account to sell items and further promote the scam (see figure 2) (ICC, 2018). Massive multiple online games (MMOs) are also a common target for phishers as "lot box" style goods can be sold on the online black market. An example is of this type of phishing scam recently targeted the MMO Elder Scrolls online (Threatpost, 2019).

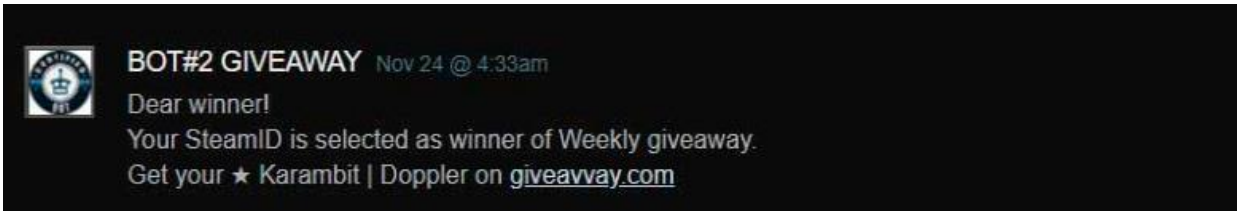

Figure 4. Example of Steam phishing attempts

Phishing is a current and crucial global issue. Phishing remains the first infection vectors for malware (Symantec, 2018), the primary methodology of infiltration used in breaches, and is the number one methodology used in social engineering attacks (Verizon, 2019). As shown in Figure 1, phishing sites that were discovered by the end of 2019, they were at the highest levels since 2016 so there is a worrying in that number as technology continues to evolve. The scope of phishing vectors will keep up growing, and malicious players no doubt will discover ways to use new these new vectors in more advanced, progressive phishing attacks (for example, the latest evolution of QRishing).

2.6.1.4. Malware

Nowadays, almost everyone is using internet in his or her daily life. This because almost in everything we need to use internet, for example in social interactions, health related transactions, online banking, and marketing. Because internet has developed rapidly, crimes are being committed online rather than in real world. Malicious software are being used to launch cyber-

attacks on the machine of the victim by cybercriminals. A malware is any software which on purpose execute malicious payloads on victim's devices such as smartphones, computers, computer networks, etc. There are different kinds of malware including worm, virus, Trojan horse, ransomware and rootkit. Victim's devices are affected differently based on the type and family of the malware, for example damaging the targeted system, stealing of confidential data, remote code execution.

Before, malware were written with simple goals, therefore it was easier to detect them. These types of malware can be defined as tradition or simple malware. But nowadays to detect a malware is very hard because the malware can be running in the kernel mode and it is more damaging and harder to detect compared to traditional malware. They are defined as new generation malware or next generation malware. These malwares bypass easily protection software that run in the kernel mode like firewall, antivirus software, etc. normally, tradition malwares are made of on process and they don't use complex techniques to hide themselves. On the contrary, new generation malwares use various new and existing processes and uses some complicated techniques to hide themselves and be patient in the system. Table 3 below shows the comparison between tradition and new generation malware (Ömer& Refik, 2020).

Comparison parameter	Traditional	New generation
Implementation level	Simple coded	Hard coded
State of behavior	Static	Dynamic
Proliferation	Each copy is similar	Each copy is different
Through spread	Uses .exe extension	Uses also different extension
Permanence in the system	Temporary	Persistent
Interaction with the process	A few processes	Multiple processes
Use concealment techniques	none	Yes
Attack type	General	Targeted
Defensive challenge	Easy	Difficult
Targeted devices	General computers	Many different devices

Table 3. Traditional versus new generation malware

Approximately 1 million malware are created everyday according to scientific and business reports, in 2019, (Morgan, 2019) estimated that by 2021 the world will be paying $6 trillion annually on cybercrimes (Morgan, 2019). The latest studies show that mobile malwares are on the rise. McAfee report on mobile threats says that there is a vast increase in backdoor, banking Trojans for mobile and fake applications (Samani & Davis, 2019). Another rise in malware is found in cloud computing, internet of things (IoT), social media, health industry and cryptocurrencies. There was an estimation that by the end of 2019, ransomware malware would be costing globally $1.5 billion stated by cybersecurity ventures (Morgan, 2019).

The first malware existed was a virus, many studies done theoretically are focused on virus detection. The detection of virus is impossible according to early studies (Cohen, 1986), (Cohen, 1992), (Chess & White, 2000), and NP-complete (Cohen, 1987), (Adleman, 1990), (Spinellis, 2003), (Zuo, et al, 2005). Cohen F. stated that detecting a computer virus is undecidable because the detection process contains contradictions itself (Cohen, 1986), (Chess & white, 2000), (Cohen,

1987). If the decision-making problem is seen as a detection problem, D (decision-maker) will have to decide whether P is a virus or not. According to Cohen, it cannot be decided whether P is a virus because if P is a virus, it will be marked by D as a virus and will not be able to make changes to other programs, as it will not act as a virus. If D decision maker did not identify P as a virus, P will interact with other programs to spread and become infected. This decision process involves contradiction, and therefore it is not possible to identify P as a virus. There is no software that can detects all viruses without false positives (FPs) since viruses are polymorphic and can be found in different forms (Chess & white, 2000). (Adleman, 1990) said that detecting is quite unmanageable and nearly impossible. This is because according to Gödel numberings of the partial recursive functions, it is not possible to create detecting mechanism. To reliably identifying a bounded-length mutating virus is NP-complete explained in (Spinellis, 2003). According to the author, virus detector for certain virus strain can be used to solve the satisfiability problem. Since NP-complete is known to be satisfiability, then the malware detection is NP-complete. Zuo et al. claim that there exist computer viruses whose detecting procedures have sufficiently large time complexity, and there are undecidable viruses which have no minimal detecting procedure (Zuo, et al, 2005).

Malware detecting techniques and algorithm

Malware detection is a process of examining the parts of the program and making a decision if the analyzed program is a malware or not. There are 3 stages of detecting a malware and there are: malware analysis, feature extraction, and classification.

a. Malware analysis

The content and behaviors of a malware need to be analyzed in order to understand it. The process of determining the functionality of a malware is called malware analysis and through that process three questions need to be answered (Alosefer, 2012), (Sikorski, & Honig, 2012). How malware works, which machines and programs are affected, and which data is being damaged and stolen etc. there are two techniques of analyzing malware: static and dynamic (Alosefer, 2012). Static analysis inspect the malware without running the actual code (Idika & Mathur, 2007). On contrary, dynamic analysis inspect the malware behavior when running its code. Malware analysis starts basically with static analysis and ends with dynamic analysis. Reverse engineering is used in malware analysis (Eilam, 2011). Figure 3 shows reverse engineering process.

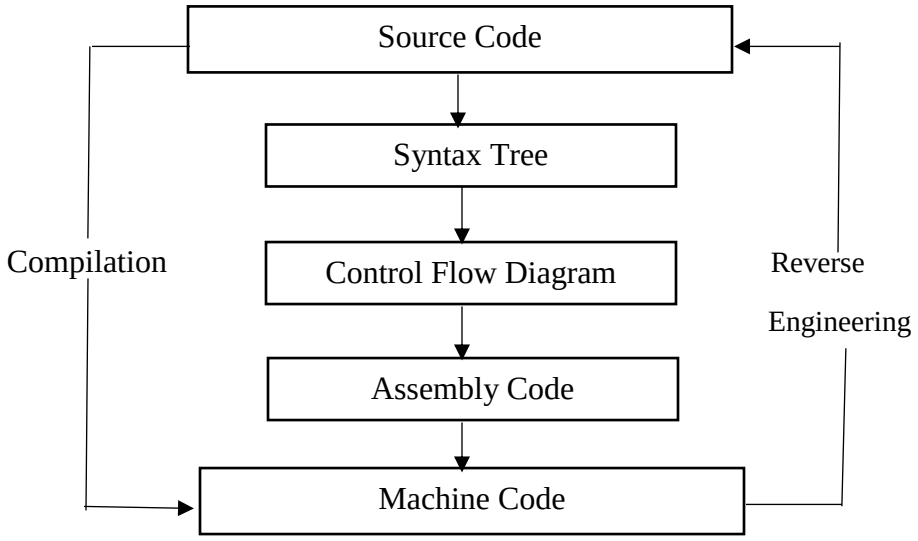

Figure 5. Flow chart of reverse engineering process.

b. Malware feature extraction

Data mining techniques are used to extract malware features. A process of extracting meaningful information which has been unknown before from large datasets or databases is called data mining. In last few years, data mining new models and datasets have been created (Souri, & Hosseini, 2018). To create malware datasets and features different algorithm are used such as, n-gram and graph model.

c. Malware classification

Machine learning (ML) is a set of algorithm that perfectly approximate the outputs of the applications without being exactly programmed. In malware detection ML algorithms have been used for many years (Gandotra, 2018). Here are well-known ML algorithms: Bayesian network (BN), naive Bayes (NB), C4.5 decision tree variant (J48), logistic model trees (LMT), random forest tree (RF), k-nearest neighbor (KNN), multilayer perceptron (MLP), simple logistic regression (SLR), support vector machine (SVM), and sequential minimal optimization (SMO). In behavior based detection is when those algorithms are used. Even though each algorithm has its own advantages and disadvantages, you cannot conclude that one algorithm is more efficiently than the other one. But one algorithm can perform better than the other in terms of data distribution, dependences between features and number of features.

Even though there have been different new methods and approaches to detect malwares, no one method can detect all new generation and complicated malwares. This indicate that building an effective method that will detect malware is a very challenging job, and there is a vast gap to fill in new researches and methods.

2.6.1.5 Identity theft

An act of acquiring personal information of a person for criminal activities is called identity theft as defined by various researchers (Dadkhah, et al, 2018). Studies view identity theft as using personal information of a victim intentionally, with no legal authority, with the purpose of doing

criminal activities (Irshad & Soomro, 2018). FBI's internet crime complaint center's (IC3), identity theft was ranked number seven with around 16 thousand victims with a loss of around $58 million and this only was documented in the USA as reported in the internet crime 2016 (FBI, 2016). In 2017 identity theft was ranked number six with around 17 thousand victims with a loss of $66 million in the USA only (FBI, 2017). This show that there is an increase in number of victims and the loss in money every year. The annual summary of the Federal Trade Commission (FTC) in 2016, ranked identity theft on the third place with the number of complaints around 399 thousand (FTC, 2017). Again in 2018 identity theft became the third with the number of complaints around 444 thousand out of 3 million reports. Even though it has lost in ranking the number of identity theft was increased by 11.3% in 2018.

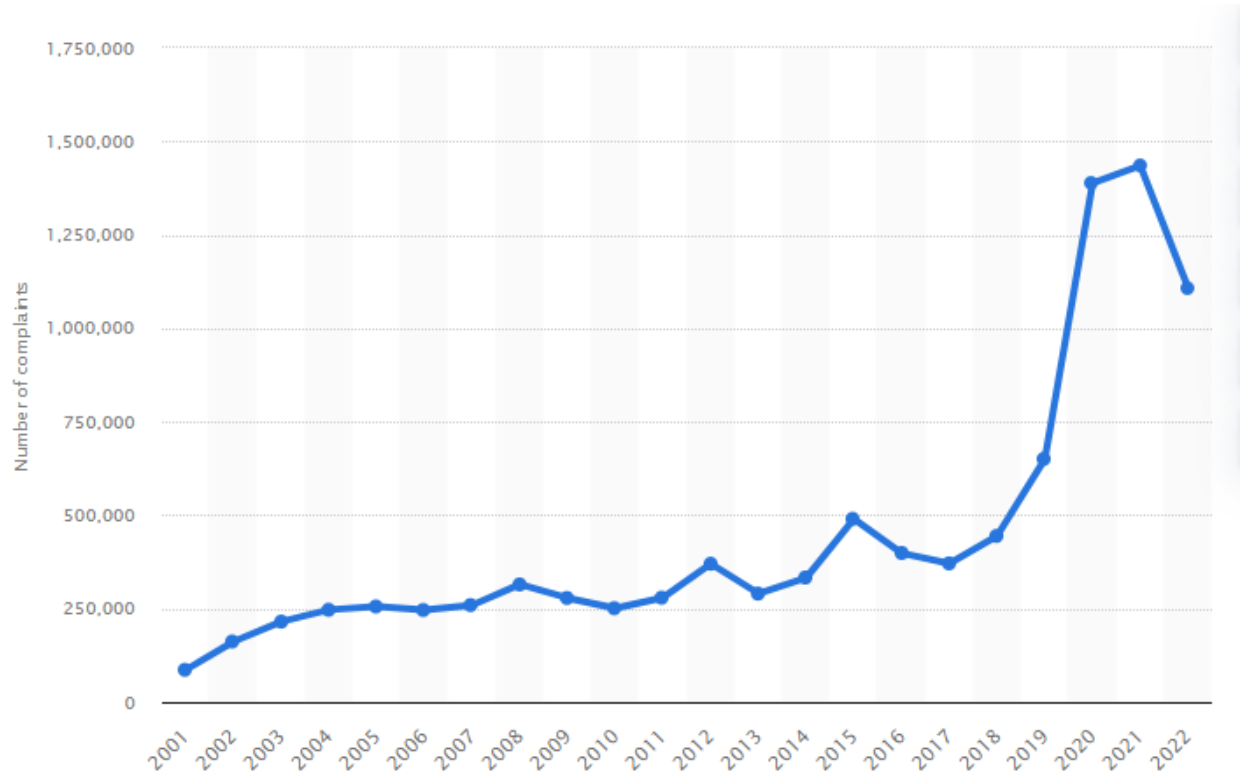

Figure 6. Number of consumer complaints relating to identity theft lodged with the U.S. Federal Trade Commission from 2001 to 2022.

The Germany cybercrime watchdog in January 2014, the federal office of information security found that 16 million email addresses and passwords were stolen (ENISA, 2014). Three major global cyber hacks happened that same year, plus the largest ever recorded in theft resulted in 2 billion credit card and customer records from large US retailers (Banjo, 2014), (Finkle & Hosenball, 2014), (Perlroth & Gelles, 2014). Generally these latest criminal activities and the growth of darknet, proof show that hijacked computer networks and malware represent the most significant attacks in relation to current identity theft (Ablon, et al, 2014).

The crimes that require the duplication of digital information or the hijacking of online accounts with the aim of doing identity fraud against a person or an organization is described as online

identity theft which is a subset of online fraud (Wall, 2013). The frequently used technique is phishing in the mission of online identity theft. Social engineering techniques are mostly used where an attacker request personal details as a legitimate request of companies. Social media has increased the phishing attacks. These platform display a pool of 2.5 billion of users that motivate identity theft offenders (Burnap et al, 2013), (Sloan et al, 2013), (Burnap et al. 2014). Graph 4 shows the number social media users worldwide in billions from 2018 to 2027. (Cohen & Felson, 1979) suggested there is an increased likelihood of victimization when individuals are placed in high risk situations, are attractive targets, lack a capable guardian and are in the reach of a motivated offender.

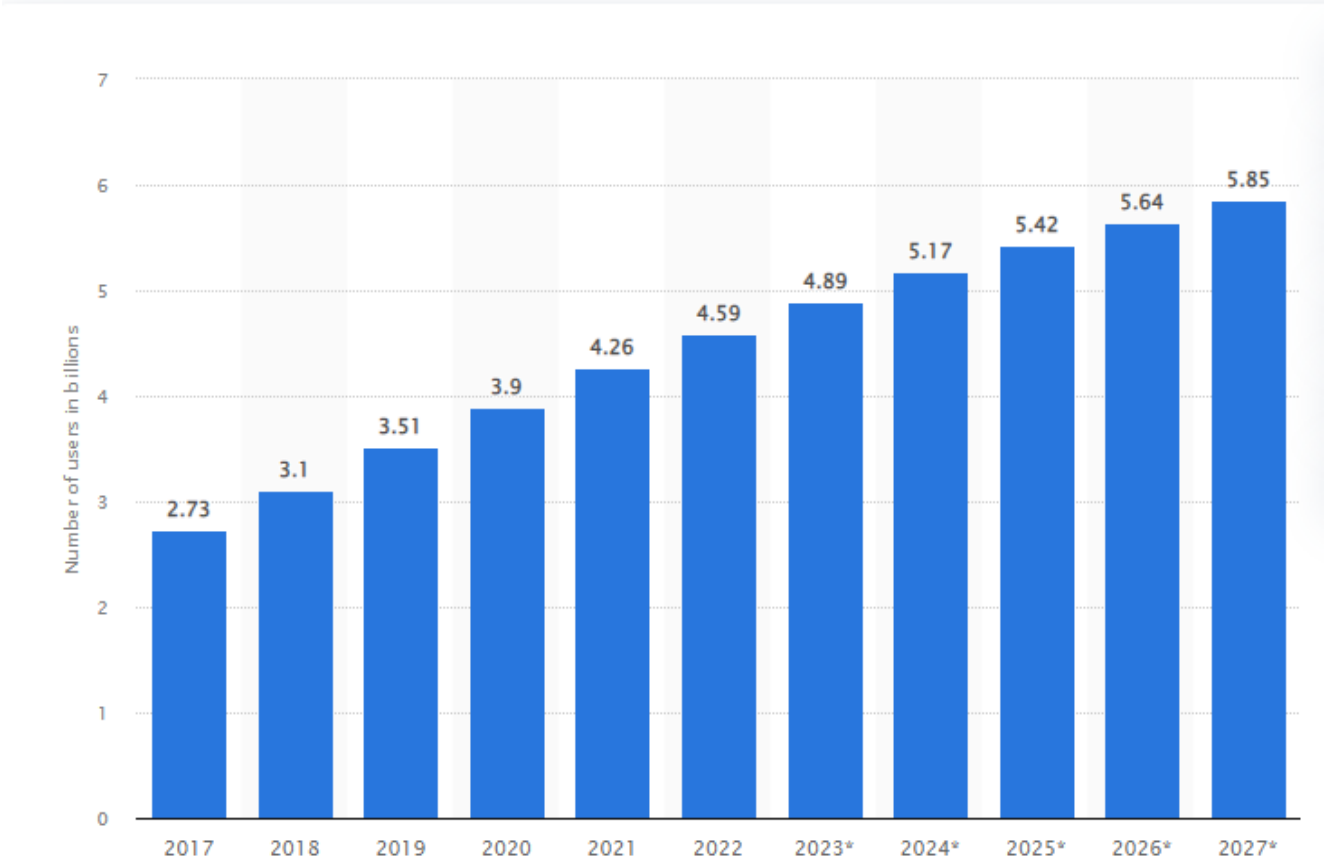

Figure 7. Number of social media users worldwide from 2018 to 2027 in billions (Statista, 2022).

2.6.1.6 Downloading, sharing, and use of pirated content

Digital content can be used, copied and distributed legally or illegally by People without spending any additional cost or time, this brings a problem among copyrights promoters, industry representative and officials from the governments. One of the copyrights issues is unauthorized peer to peer (P2P) file sharing websites. Internet users, uses P2P file sharing sites to bypass central

controlled server based services in order to allow them to download digital content from other user's computers directly (Wang & McClung, 2011). These sites have been used frequently by many people especially young people in order to download or distribute digital copyrighted material illegally for the past decade. Colombia University's American assembly in 2013 reported that 13% of US internet users have used P2P file sharing sites and 20% of them were young people under 30 years (Karaganis & Renkema, 2013). The institute for policy innovation reported that every year, the US economy loses $58 billion in total output, around 373 thousand jobs are lost and $2.6 billion in annual tax revenue due to illegal downloading.

The Centrum Cyfrowe (Digital Centre) team conducted a research and found that 33% of poles (polish people) have been engaged in some type of informal sharing of digital content. The frequently used technologies were streaming channels (25%), physical carriers (19%), downloading from websites (12%), using P2P protocol (11%), and sharing links via e-mail or messenger services (6%). The research also showed that in the category of age 15-24, the mostly used forms of having access on pirated files are P2P services (about 28%), downloading from websites (about 32%), peer exchange through external carriers (over 40%), and streaming (over 60%) (Filiciak et al., 2012). According to NI Direct (the official government website for Northern Ireland citizens), the dangers of downloading and file sharing apart from breaking copyright, which the law views as theft, other possible dangers include (NI Direct, 2022):

- **Viruses** Computers can be at risk from corrupted programs by downloading files or software.
- **Theft**: file sharing can allow other computers to view all the files on your computer, which means that your personal information might be stolen.
- **Unsuitable images**: A child can be put at risk of violent, pornographic or age-inappropriate content, if they are using an illegal download site
- **Exposure to potentially dangerous strangers**: it's possible to chat on some file sharing sites, which could leave your child open to grooming, bully.

CHAPTER 3. RESEARCH METHODOLOGY

3.0 Research Methodology

This chapter, describe the methodology and technique used during the study. It contains also data collection part and sampling techniques used in data collection.

This research used quantitative research methodology. Quantitative research covers a scope of methods concerned with the systematic research of social occurrence, using numerical or statistical data. Therefore, quantitative research involves measurement and assumes that the phenomena under study can be measured (Watson, 2015). The Analytic Hierarchy Process (AHP) method was used in the analysis of data. The Analytic Hierarchy Process (AHP) is a method of measurement through pairwise comparisons and relies on the judgments of experts to derive priority scales (Saaty, 2008). It contains three parts: the ultimate goal or problem you're trying to solve, all of the possible solutions, called alternatives, and the criteria you will judge the alternatives on (Bahurmoz, 2006). Thomas L. Saaty developed AHP model as a decision support model which would be used to break down complex multi-criteria or multi-factor problems into a hierarchy (Kusumadewi, et al, 2006). I have chosen AHP because it is widely used by decision makers and researchers and also because it is a simple and powerful tool (Rosaria de F.S.M. & Roberto, 2015). Therefore it can be used to evaluate the decision making of undergraduate students at Makerere University to protect themselves from cyber-attacks. The figure 8 below shows the AHP diagram of this research.

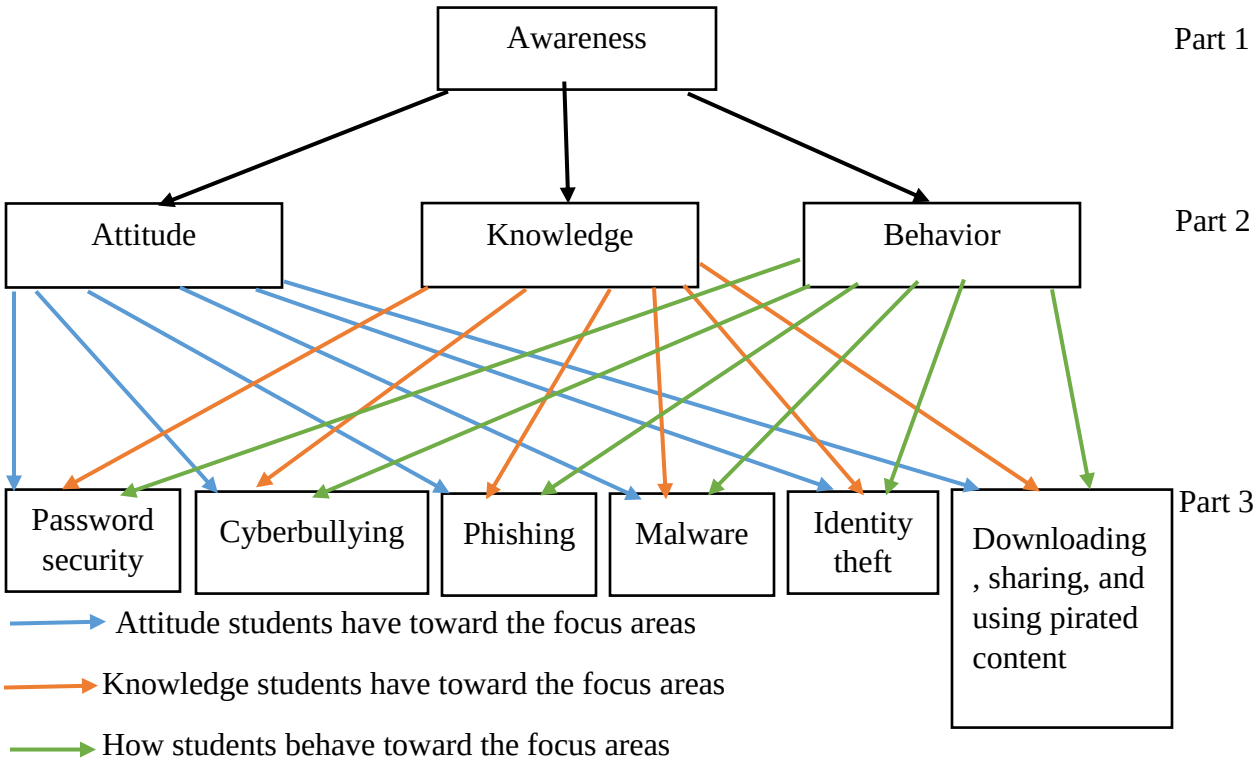

Figure 8. AHP diagram of this research

In the AHP at the top of hierarchy is the goal of decision making. The next level is for criteria and it can be broken down into sub-criteria. And the last level is for alternatives. Via pairwise comparisons and judgments from decision makers, priorities of alternatives and criteria weights are calculated. The importance of the AHP method is explained in table 4 below.

Intensity of importance	**Definition**
1	Equal importance
3	Somewhat more important
5	Much more important
7	Very much more important
9	Absolutely more important
2,4,6,8	Intermediate values

Table 4. Level of Importance in AHP (Balqis & Candiwan, 2020)

The data is collected by a questionnaire, the questionnaire used a nominal scale type and dichotomous scaling method. The population of this research is 31000 undergraduate students at Makerere University. To determine the sample in this research Yamane equation (Yamane, 1967) was used and it is show below:

$$n = \frac{N}{1 + Ne^2}$$

Where n is the sample size, N is the population size and e is margin of error. This research used a confidence level of 95% so the margin error is 5%. By substituting the population size and margin of error values to the equation we get:

$$n = \frac{31000}{1+(31000*0.05^2)} = 394.904 == 395 \text{ samples}$$

According to the Website of Makerere University, Makerere University has 9 colleges and school of law as the 10th on campus. Which are:

1. College Of Agricultural And Environmental Sciences (CAES)
2. College of Business and Management Sciences (CoBAMS)
3. College of Computing and Information Sciences (CoCIS)
4. College Of Education And External Studies (CEES)
5. College Of Engineering, Design, Art And Technology (CEDAT)
6. College of Health Sciences (CHS)
7. College of Humanities and Social Sciences (CHUSS)
8. College of Natural Sciences (CoNAS)
9. College of Veterinary Medicine, Animal Resources and Biosecurity (CoVAB)
10. School of Law (SoL)

Therefore to facilitate further calculation process the number of respondents in this study is 400 undergraduate students in order to pick 40 undergraduate students in each college. This study has 32 questions about cybersecurity awareness to test knowledge, behavior and attitude of

undergraduate students at Makerere University. There are some questions which are answered as 3-point scale consisting of yes||, do not know|| and no||, while other questions only requires answers on a 2-point scale consisting of yes|| or no||. This study follows an exploratory approach, using non-probability sampling. The study use convenience sampling technique. Therefore a convenience sample of students was taken among the 10 colleges at Makerere University.

We have a total of six focus areas, (I) password security, (II) cyberbullying, (III) phishing, (IV) malware, (V) identity theft, (VI) downloading, sharing, and use of pirated content (Chandarman & Van, 2017). Various question indicators were made for this study about the framework and the mentioned focus areas above. To weight each dimension and focus area in accord with the level of importance AHP approach is also used. To evaluate subjective factors pairwise comparison is used and these are determined by professional opinions and judgment (Kruger & Kearney, 2006). Preference scale is used during comparisons, which grant numerical values to different preference levels (Kruger & Kearney, 2006).

Dimensions	**Weighting values**
Knowledge	30%
Attitude	20%
Behavior	50%

Table 5. Dimension weighting value (Kruger & Kearney, 2006).

According to (Kruger & Kearney, 2006) the dimension of behavior need more attention followed by the dimensions of knowledge and attitude. Based on the fixed weights, weighting is carried out before calculation. Weighting is done on each dimension (behavior, attitude and knowledge) and focus areas (password security (I), cyberbullying (II), phishing (III), malware (IV), identity theft (V), downloading, sharing, and use of pirated content (VI)). The focus areas were weighted assuming that each focus area has the same level of importance or equally important. After determining the level of importance for each focus area, then the value of importance will be calculated and normalized to get a weighting value (%) for each focus area. Manual calculations and formulas in Microsoft excel are used to do normalization. The next step is to determine the average for each focus area. By assuming that each focus area has the same level of importance that is how weighting values are obtained. AHP approach uses paired comparisons to give subjective evaluations of factors based on professional opinions and considerations in order to get the weight of importance (Sari & Candiwan, 2014). The value of cybersecurity awareness in each dimension, focus area and total weight is calculated based on the weighting values. A preference scale is used in comparisons which offer numerical values to different preference level (Sari & Candiwan, 2014).

Criteria	**Value (%)**	**Action**
Good	77.78 - 100	Action is not needed
Average or satisfactory	55.56 - 77.77	Action is potentially required
Poor	33.33 – 55.55	Action is required

Table 6. Awareness criteria (Sari & Candiwan, 2014).

The score of each focus area and dimensions are calculated and they are grouped according to the awareness criteria as it is shown in table 6. The interval value is determined by the value of the

continuing line in which the maximum value is 100% and the minimum score is 33.33% (Sari & Candiwan, 2014). After calculating the predetermined weights, the results are obtained in the form of cybersecurity awareness criteria in each focus area and dimension. Every result of cybersecurity awareness criterion has actions that need to be carried out at a later stage when cybersecurity awareness is on certain criteria.

CHAPTER 4. RESULTS

4.0. Introduction

This chapter presents, analyzes and interprets data generated through a quantitative approach to assess the cybersecurity awareness level of undergraduate students at Makerere University. A Survey questionnaire was distributed from 5th May to 09th May 2023. The questionnaire used a nominal scale type and dichotomous scaling method. Quantitative methods were used in this study to discuss findings from the data.

4.1. Reliability, validity and feasibility test of the questionnaire

All 400 samples of the respondents were used to perform the reliability, validity and feasibility test of the questionnaire. This study used IBM SPSS statistics 28.0.1.1 software to perform all the tests.

4.1.1. The Reliability test

This study used the Cronbach's Alpha technique to check the reliability from each subject. The question is said to be reliable if r count > r table. The question is declared to be unreliable if the r count ≤ r table. Below is the equation of the Cronbach alpha test.

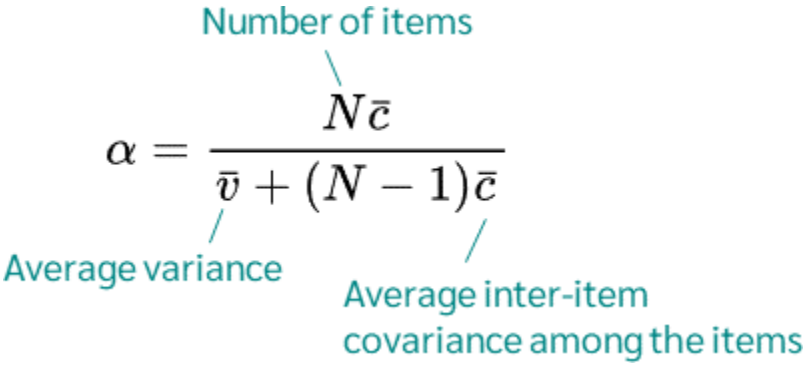

Figure 9. The Cronbach Alpha equation.

With a confidence level of 95%, the Cronbach Alpha test was done and gave 0.564 which is poor. The test was recalculated with question DQ9 excluded, resulting in 0.618 which is acceptable. A general accepted rule is that alpha value of 0.6-0.7 indicates an acceptable level of reliability (Hulin, et al, 2001). This indicates that every statement used in the variable is reliable.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.564	.626	49

Table 7. The Cronbach's Alpha Value before excluding question DQ9.

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
.618	.640	48

Table 8. The Cronbach's Alpha Value after excluding question DQ9.

4.1.2. The Validity test

Validity test in this research used Pearson correlation coefficient technique. By using the r table value with n = 400 and the significance level of 5%, the r-value of the table obtained is 0.098. Table 9 below shows the results of the validity tests that have been conducted on the questionnaire. The validity test results show that all questionnaire items are valid.

Variable or dimension	Question item	r-table	r-value	Category
Attitude	AQ1	0.098	0.556	Valid
	AQ2	0.098	0.593	Valid
	AQ3	0.098	0.320	Valid
	AQ4	0.098	0.384	Valid
	AQ5	0.098	0.383	Valid
	AQ6	0.098	0.554	Valid
Knowledge	KQ1	0.098	0.383	Valid
	KQ2	0.098	0.417	Valid
	KQ3	0.098	0.507	Valid
	KQ4	0.098	0.469	Valid
	KQ5	0.098	0.411	Valid
	KQ6	0.098	0.613	Valid
Behavior	BQ1	0.098	0.430	Valid
	BQ2	0.098	0.145	Valid
	BQ3	0.098	0.504	Valid
	BQ4	0.098	0.145	Valid
	BQ5	0.098	0.553	Valid
	BQ6	0.098	0.410	Valid

Table 9. The Validity test results.

4.1.3. The Feasibility test

At this stage the correlation between variables using Bartlett's test and the Kaiser–Meyer–Olkin (KMO) test is tested. This test is done to assess the feasibility of a variable analyzed using factor analysis (Koepp, et al, 2012). The table 10 shows that the significance value of Bartlett's test of sphericity is 0.001, the p-value (0.001) < (0.05), which means there is a correlation between variables. Also the KMO value is 0.772, the KMO value is found between 0.5-1, which means that

the variables are homogeneous. The two test have been met so that the variables can be predicted and further analysis can be carried out.

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.772
Bartlett's Test of Sphericity	Approx. Chi-Square	4111.420
	df	1275
	Sig.	<.001

Table 10. KMO and Bartlett's test results.

4.2. Results from data collected from the sample

4.2.1. Demography and Background characteristic of the respondents on cybersecurity awareness

This section provide information about the background characteristics of the respondents on cybersecurity awareness. The objective of this study is to assess the cybersecurity awareness level of undergraduate students at Makerere University. The questions about how often do they use internet, how long have they been using internet, how computer skilled are they, what purpose do they use their computers, if they can be cyber-attack targets based on their student status, which of the cyber-attacks they are aware of, the tools they use to protect themselves from cyber-attacks, if they have heard of the term cybersecurity before and if they desire to study security, were considered important because everyone can be a victim of cyber-attacks not matter how experienced they are and it is even worse when someone being attacked is not aware of cyber-attacks or doesn't have means to protect himself or herself from cyber-attacks.

4.2.2. Demography of respondents

The table below shows gender distribution, having 60% of male and 40% of female students.

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	240	60.0	60.0	60.0
	Female	160	40.0	40.0	100.0
	Total	400	100.0	100.0	

Table 11. Gender distribution

The table below shows year of study distribution. In all 400 respondents, Year 1 students were 11.8%, Year 2 students were 37.3%, Year 3 students were 35%, Year 4 students were 15.5% and Year 5 were 0.5%.

Year of study

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Year 1	47	11.8	11.8	11.8
	Year 2	149	37.3	37.3	49.0
	Year 3	140	35.0	35.0	84.0
	Year 4	62	15.5	15.5	99.5
	Year 5	2	.5	.5	100.0
	Total	400	100.0	100.0	

Table 12. Year of study distribution

The table below shows the range of age distribution. 83.8% were between 18 and 24 years old, 15.5% were between 25 and 35 years old and 0.8% were 36 years old and above.

Age range

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-24	335	83.8	83.8	83.8
	25-35	62	15.5	15.5	99.3
	36 and above	3	.8	.8	100.0
	Total	400	100.0	100.0	

Table 13. The range of age distribution

4.2.3. Background characteristics of the respondents on computer usage experience and cybersecurity

This section we are to provide information about the background characteristics of the respondents on computer usage experience and cybersecurity.

The table below shows how often respondents use internet. 32% of them use internet on hourly bases, 65% of them use internet on daily bases, 1.5% of them use internet on weekly bases, and also 1.5% of them use internet on monthly bases. 32% of the respondents, every hour they are checking something on the internet and 65% of the respondent at least once or twice a day they use the internet. This give the confidence that the population would be fit for the survey.

How often do you use internet?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Hourly	128	32.0	32.0	32.0
	Daily	260	65.0	65.0	97.0
	Weekly	6	1.5	1.5	98.5
	Monthly	6	1.5	1.5	100.0
	Total	400	100.0	100.0	

Table 14. Internet usage frequency

The table below shows for how long the respondents have been using internet. 72% of the respondents said they have been using internet for 5 years and above.

For how long have you been using the internet?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Weeks	7	1.8	1.8	1.8
	Months	10	2.5	2.5	4.3
	1 to 4 years	95	23.8	23.8	28.0
	5 years and above	288	72.0	72.0	100.0
	Total	400	100.0	100.0	

Table 15. The time respondents have been using internet

The table below shows how computer skilled respondents think they are. 8.3% of them consider themselves as beginners, they are just starting to use computers; 77.3% of them consider themselves as intermediate, they are not highly skilled not also lowly skilled and 14.5% of them consider themselves as advanced, they are highly skilled.

How computer skilled are you?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Beginner	33	8.3	8.3	8.3
	Intermediate	309	77.3	77.3	85.5
	Advance	58	14.5	14.5	100.0
	Total	400	100.0	100.0	

Table 16. Computer skills

The table below shows for what purpose the respondents use their computers. The highest percentage is 16.6% for the purpose of education as they are students.

For what purpose do you use your computer?

		Responses		
		N	Percent	Percent of Cases
Computer usage purpose	Word typing	308	15.3%	77.0%
	Internet Browsing	285	14.2%	71.3%
	Internet communications	281	14.0%	70.3%
	Education	334	16.6%	83.5%
	Gaming	136	6.8%	34.0%
	Business	114	5.7%	28.5%
	Entertainment	290	14.4%	72.5%
	Sending & Receiving Emails	265	13.2%	66.3%
Total		2013	100.0%	503.3%

a. Dichotomy group tabulated at value 1.

Table 17. Computer usage purpose

The table below shows if the respondents think they are targets of cyber-attacks due to their student status. 28.7% said they strongly disagree which means that they know that they targets of cyber-attacks like anyone else while 7.5% said they strongly agree which means they think that they are not targets of cyber-attacks due their student status.

I think I'm not a target of cyber-attacks due to student status.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Disagree	115	28.7	28.7	28.7
	Disagree	116	29.0	29.0	57.8
	Neither Agree or Disagree	64	16.0	16.0	73.8
	Agree	75	18.8	18.8	92.5
	Strongly Agree	30	7.5	7.5	100.0
	Total	400	100.0	100.0	

Table 18. Respondents concern if they can be cyber-attacks targets due to their student status

The table below shows some of the known cyber terms to the respondents.

Which of the following are you aware of?

		Responses		
		N	Percent	Percent of Cases
Cyber terms	Password security	327	29.1%	81.8%
	Cyberbullying	187	16.7%	46.8%
	Phishing	96	8.6%	24.0%
	Malware	133	11.9%	33.3%
	Identity theft	147	13.1%	36.8%
	Downloading, sharing, and using pirated content	214	19.1%	53.5%
	None of them	18	1.6%	4.5%
Total		1122	100.0%	280.5%

a. Dichotomy group tabulated at value 1.

Table 19. Cybersecurity terms

The table below shows that 91.8% of the respondents have heard of the term cybersecurity in their lives while 4% of them was their first time because they answered “NO”. And 4.3% of the respondents don’t know where they stand on the topic.

Have you ever heard or known about the term of “Cybersecurity”?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	367	91.8	91.8	91.8
	No	16	4.0	4.0	95.8
	I don't know	17	4.3	4.3	100.0
	Total	400	100.0	100.0	

Table 20. The respondents who knew the term cybersecurity

The table below shows if the respondents have desire to learn about online security 96.5% said yes which means they desire to learn more about cybersecurity and 3.5% of them said no which means they are not interested in learning about cybersecurity.

Do you desire to learn more on security?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	386	96.5	96.5	96.5
	No	14	3.5	3.5	100.0
	Total	400	100.0	100.0	

Table 21. The respondents who desire to learn more about online security

4.2.4. Findings on attitude dimension on focus areas

Attitude is how the respondents feel about the topic in our case they are focus areas: password security, cyberbullying, Phishing, Malware, Identity theft and downloading, sharing, and using pirated content. This section shows the findings of the attitude respondents have toward each focus area.

4.2.4.1. Password security

It is a waste of time to change passwords because you can still get hacked

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	94	23.5	23.5	23.5
	No	229	57.3	57.3	80.8
	I don't know	77	19.3	19.3	100.0
	Total	400	100.0	100.0	

Table 22. Attitude on password security

The highest percentage is 57.3% where respondents answered "NO", which means they don't think it is waste of time to keep changing their passwords to keep their online accounts secure. 23.5% of the respondents answered "YES", which means for them it is a waste of time to change their passwords because still they can get hacked into their accounts. 19.3% of the respondents answered "I DON'T KNOW", which means they don't know where they stand toward the topic.

4.2.4.2. Cyberbullying

Posting pictures and bad messages online about my college students makes it anonymous and is much better than saying it to their face.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	94	23.5	23.5	23.5
	No	234	58.5	58.5	82.0
	I don't know	72	18.0	18.0	100.0
	Total	400	100.0	100.0	

Table 23. Attitude toward cyberbullying

The highest percentage is 58.5% where the respondents answered "NO", which means they can't get involved in cyberbullying because they think it is wrong. 23.5 % answered "YES" which means they can get involved in cyberbullying. 18% answered "I DON'T KNOW", which means they don't know where they stand toward the topic.

4.2.4.3. Phishing

I am careful when opening email attachments and links.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	296	74.0	74.0	74.0
	No	74	18.5	18.5	92.5
	I don't know	30	7.5	7.5	100.0
	Total	400	100.0	100.0	

Table 24. Attitude toward phishing

The highest percentage is 74% where the respondents answered “YES”, which means they are careful when they are going to open an email attachments and links which are the biggest sources of phishing attacks which may lead to other cyber-attacks. 18% answered “NO” which means they don’t care whether the email attachments and links are malicious which may lead to phishing attacks. 7.5% answered “I DON’T KNOW”, which means they don’t know where they stand toward the topic.

4.2.4.4. Malware

I am aware of protecting my device (PC, smartphone, tablet, etc.) from virus/malware so I should install antivirus.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	325	81.3	81.3	81.3
	No	45	11.3	11.3	92.5
	I don't know	30	7.5	7.5	100.0
	Total	400	100.0	100.0	

Table 25. Attitude toward malware

The highest percentage is 81.3% where the respondents answered “YES”, which means they are concerned about their devices being affected by malwares or computer viruses so they install antivirus software in their PC, smartphones, tablets, etc. 11.3% of the respondents answered “NO”, which means they can be victims of malware attacks. 7.5% answered “I DON’T KNOW” which means they don’t know where they stand the topic.

4.2.4.5. Identity theft

I am concerned about someone stealing information about myself when I am online.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	328	82.0	82.0	82.0
	No	42	10.5	10.5	92.5
	I don't know	30	7.5	7.5	100.0
	Total	400	100.0	100.0	

Table 26. Attitude toward identity theft

The highest percentage is 82% where the respondents answered “YES”, which means they are worried about their identity being stolen online so they very careful about giving their information. 10% of the respondents answered “NO”, which means they are not careful when giving their information online so their identity may get stolen. 7.5% answered “I DON’T KNOW”, which means they don’t know where they stand toward the topic.

4.2.4.6. Downloading, sharing, and using pirated content

It is OK to download pirated movies and TV series because the companies that make them are rich and I really cannot afford it (I am a student).

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	182	45.5	45.5	45.5
	No	141	35.3	35.3	80.8
	I don't know	77	19.3	19.3	100.0
	Total	400	100.0	100.0	

Table 27. Attitude toward Downloading, sharing, and using pirated content

The highest percentage is 45.5% where the respondents answered “YES”, which means they think there is no problem in downloading pirated movies and TV series while those documents comes which computer viruses and also they are not concerned it is illegal. 35.3% of the respondents answered “NO”, which means they are concerned about pirated documents because they are dangerous and also illegal. 19.3% answered “I DON’T KNOW”, which means they don’t know where they stand toward the topic.

4.2.5. Findings on knowledge dimension

Knowledge is what the respondents know about the topic in our case they are focus areas: password security, cyberbullying, Phishing, Malware, Identity theft and downloading, sharing, and using pirated content. Below are the findings of the knowledge respondents have on each focus area.

4.1.5.1. Password security

If I don't maintain the security of my password, I could experience security problems in cyberspace.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	330	82.5	82.5	82.5
	No	32	8.0	8.0	90.5
	I don't know	38	9.5	9.5	100.0
	Total	400	100.0	100.0	

Table 28. Knowledge on password security

The highest percentage is 82.5% where the respondents answered “YES”, which means they know that they can experience cyber-attacks if they are not careful with the security of their passwords. 8% of the respondents answered “NO”, which means they do not know about password security. 9.5% of the respondents don’t know where they stand toward the topic.

4.2.5.2. Cyberbullying

I have been harassed while online by people I did not know.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	170	42.5	42.5	42.5
	No	208	52.0	52.0	94.5
	I don't know	22	5.5	5.5	100.0
	Total	400	100.0	100.0	

Table 29. Knowledge on cyberbullying

The highest percentage is 52% where the respondents answered “NO” which means they might know about cyberbullying or not. 42.5% of the respondents answered “YES”, which means they have experienced cyberbullying in their lives which means they know cyberbullying. 5.5% of the respondents answered “I DON’T KNOW”, which means they don’t know where they stand toward the topic.

4.2.5.2. Phishing

A phishing attack means that someone is trying to generate personal information from you, for example when you log in on a webpage, or sign a form on a webpage (eg. An appealing message on Facebook or e-mail). Based on this description do you think that you have been exposed to a phishing attack?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	196	49.0	49.0	49.0
	No	88	22.0	22.0	71.0
	I don't know	116	29.0	29.0	100.0
	Total	400	100.0	100.0	

Table 30. Knowledge on phishing

The highest percentage is 49% where the respondents answered “YES”, which means they know what a phishing attack is because they have been exposed toward one. 22% of the respondents answered “NO”, which they know what phishing attack or not. 29% of the respondents answered “I DON’T KNOW”, which means they don’t know where they stand toward the topic.

4.2.5.4. Malware

For protecting my device (PC, smartphone, tablet, etc.) From malware/virus so I should install antivirus.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	331	82.8	82.8	82.8
	No	28	7.0	7.0	89.8
	I don't know	41	10.3	10.3	100.0
	Total	400	100.0	100.0	

Table 31. Knowledge on Malware

The highest percentage is 82.8% where respondents answered “YES”, which means know about malware or computer viruses attacks. 7% of the respondents answered “NO”, which means they don’t know about malware attacks. 10% of the respondent don’t know where they stand toward the topic.

4.2.5.5. Identity theft

Do you know that, people steal other people's identities online in order to commit cybercrimes?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	346	86.5	86.5	86.5
	No	20	5.0	5.0	91.5
	I don't know	34	8.5	8.5	100.0
	Total	400	100.0	100.0	

Table 32. Knowledge on identity theft

The highest percentage is 86.5% where the respondents answered "YES", which means they have knowledge on online identity theft. 5% of the respondents answered "NO", which means they don't know about online identity theft. 8.5% answered "I DON"T KNOW", which means they don't know where they stand toward the topic.

4.2.5.6. Downloading, sharing, and using pirated content

Do you think downloading, using and sharing files for free over Internet is legal or not?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	165	41.3	41.3	41.3
	No	99	24.8	24.8	66.0
	I don't know	136	34.0	34.0	100.0
	Total	400	100.0	100.0	

Table 33. Knowledge on Downloading, sharing, and using pirated content

The highest percentage is 41.3% where the respondents answered "YES", which means they do not know that downloading, using and sharing files for free over the internet is a cyber-crime, they can be punished by the law. 24.8% of the respondent answered "NO", which means they know that it is a crime to download, use and share file for free over the internet. 34% of the respondents answered "I DON'T KNOW", which means they don't know where they stand toward the topic.

4.2.6. Findings on the behavior dimension

Behavior is what the respondents do about the topic in our case they are focus areas: password security, cyberbullying, Phishing, Malware, Identity theft and downloading, sharing, and using pirated content. Below are the findings of how the respondents behave toward each focus area.

4.2.6.1. Password security

I always keep my password secure to avoid security breaches in cyberspace

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	370	92.5	92.5	92.5
	No	30	7.5	7.5	100.0
	Total	400	100.0	100.0	

Table 34. Behavior toward password security

The highest percentage is 92.5% where the respondents answered "YES", which means the practice password security to avoid security breaches. 7.5% of the respondent answered "NO" which means they don't practice password security.

4.2.6.2. Cyberbullying

I have used the Internet to make fun of other people or say bad things about them because I knew no one would know it was I who did it

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	59	14.8	14.8	14.8
	No	341	85.3	85.3	100.0
	Total	400	100.0	100.0	

Table 35. Behavior toward cyberbullying

The highest percentage is 85.3% where the respondents answered "NO", which means they have not been involved in cyberbullying. 14.8% answered "YES", which means they have been involved in cyberbullying.

4.2.6.3. Phishing

You receive an email from your bank that your account needs to be verified because the bank has installed new software. You are required to click on a link provided and supply the necessary personal verification information. You must respond within the next 24 hours otherwise your bank account will be blocked and frozen. Do you call the bank to check if this is true?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	291	72.8	72.8	72.8
	No	109	27.3	27.3	100.0
	Total	400	100.0	100.0	

Table 36. Behavior toward phishing

The highest percentage is 72.8%, where the respondent answered "YES", which means they can't be tricked into a phishing attack. 27.3% answered "NO", which means they can get tricked into a phishing attack.

4.2.6.4. Malware

I install antivirus for protecting my device (PC, smartphone, tablet, etc.) from virus/malware that can cause malfunction of my device

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	302	75.5	75.5	75.5
	No	98	24.5	24.5	100.0
	Total	400	100.0	100.0	

Table 37. Behavior toward malware

The highest percentage is 75.5% where the respondents answered "YES", which means they protect their devices against malwares or computer virus attacks. 24.5% answered "NO", which means they don't protect their devices against malwares or computer virus attacks.

4.2.6.5. Identity theft

I am very protective of my personal information such as email, password, credit card PIN, etc. so that my identity cannot be stolen.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	364	91.0	91.0	91.0
	No	36	9.0	9.0	100.0
	Total	400	100.0	100.0	

Table 38. Behavior toward identity theft

The highest percentage is 91% where respondent answered "YES", which means they keep secure their personal information in order to not be stolen while they are online. 9% answered of the

respondents “NO”, which means they don’t keep their personal information secret which can lead to identity theft.

4.2.6.6. Downloading, sharing, and using pirated content

If you hear a song on the radio that you really like, do you go home and download the mp3 from mp3 free download websites or other file sharing service for free.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Yes	330	82.5	82.5	82.5
	No	70	17.5	17.5	100.0
	Total	400	100.0	100.0	

Table 39. Behavior toward Downloading, sharing, and using pirated content

The highest percentage is 82.5% where the respondents answered “YES”, which means they download, share and use pirated contents which is against the law here in Uganda and also which can compromise their devices such as PC, smartphones, etc. 17.5% of the respondent answered “NO”, which means they don’t download, share and use pirated contents.

4.3. Assessing the cybersecurity awareness level

By using the information security awareness measurement framework, awareness is divided into three dimensions: attitude, knowledge and behavior. Six focus areas: password security, cyberbullying, Phishing, Malware, Identity theft and downloading, sharing, and using pirated content to assess each dimension. To assess the awareness level the AHP model is uesd. In the AHP at the top of hierarchy is the goal of decision making in our case it is awareness. The next level is for criteria in our case they are dimensions (attitude, knowledge and behavior). And the last level is for alternatives which are the focus areas (password security (I), cyberbullying (II), phishing (III), malware (IV), identity theft (V), downloading, sharing, and use of pirated content (VI)) in our case. AHP approach uses paired comparisons to give subjective evaluations of factors based on professional opinions and considerations in order to get the weight of importance (Sari & Candiwan, 2014). The table below shows the dimension weighting and they were determined by professional opinions and judgment (Kruger & Kearney, 2006). Preference scale is used during comparisons, which grant numerical values to different preference levels (Kruger & Kearney, 2006).

Dimensions	**Weighting values**
Knowledge	30%
Attitude	20%
Behavior	50%

Table 40.Dimension weighting value (Kruger & Kearney, 2006).

The dimension of behavior need more attention followed by the dimensions of knowledge and attitude (Kruger & Kearney, 2006).

Focus Areas (16.67%)	Dimensions			
	Knowledge (30%)	**Attitude (20%)**	**Behavior (50%)**	**Total awareness/ focus area**
Password security	82.5%	57.3%	92.5%	82.3%
Cyberbullying	42.5%	58.5%	85.3%	67%
Phishing	49%	74%	72.8%	66%
Malware	82.8%	81.3%	75.5%	78.7%
Identity theft	86.5%	82%	91%	87.6%
Downloading, sharing, and use of pirated content	24.8%	35.3%	17.5%	22.7%
Total awareness/ Dimension	61.3%	64.7%	72.4%	67.4%

Table 41.cybersecurity awareness level of the respondents

The value of cybersecurity awareness in each dimension, focus area and total weight is calculated based on the weighting values. A preference scale is used in comparisons which offer numerical values to different preference level (Sari & Candiwan, 2014). The score of each focus area and dimensions are calculated and they are grouped according to the awareness criteria as it is shown in the table below. The interval value is determined by the value of the continuing line in which the maximum value is 100% and the minimum score is 33.33% (Sari & Candiwan, 2014). After calculating the predetermined weights, the results are obtained in the form of cybersecurity awareness criteria in each focus area and dimension. Every result of cybersecurity awareness criterion has actions that need to be carried out at a later stage when cybersecurity awareness is on certain criteria.

Criteria	**Value (%)**	**Action**
Good	77.78 – 100	Action is not needed
Average or satisfactory	55.56 - 77.77	Action is potentially required
Poor	33.33 – 55.55	Action is required

Table 42. Awareness criteria (Sari & Candiwan, 2014).

According to the cybersecurity awareness level obtained in Table 37. According to the dimensions the results are as follow. The total percentage of cybersecurity awareness is 67.4%. It indicates that the cybersecurity awareness level is in average or satisfactory criteria. In this level, the respondents need more assistance to improve their cybersecurity awareness.

Between the three dimensions the highest percentage of awareness is for the behavior dimension with a percentage of 72.4%. In this level the respondents need treatment as it falls under the average or satisfactory criteria. The high percentage of 72.4% is caused by the respondents 'high likelihood to answer positively to cybersecurity questions. All behavior percentages show a significant amount except the one for downloading, sharing, and use of pirated content which is 17.5%. The highest percentage is on the questionnaire item BQ1. The questionnaire item BQ1 shows that the respondents have a good practice of keeping their password secure to avoid online breaches.

The attitude dimension has a total percentage of 64.7%. In this level, also the respondents need treatment to improve as it falls under average or satisfactory criteria. This is because according to the survey, the percentage found on questionnaire item AQ1, AQ2 and AQ6 falls under the criteria of average, average and poor respectively. This suggest that the respondents don't change their passwords regularly, they tend to participate in cyberbullying and they are likely to download, share and use pirated contents which is illegal and can lead to cyber-attacks

The dimension of Knowledge is the one with the lowest percentage 61.3%, it also falls under average or satisfactory criteria. This shows that action is potentially required to boost the respondents' knowledge. Results from the calculations shows that the lowest percentage of knowledge items are KQ2, KQ3 and KQ6. It indicates that respondents don't have enough knowledge about cyberbullying, phishing attacks and they think that downloading, sharing file for free over internet is legal.

Per focus area the highest percentage is identity theft with percentage of 87.6%, followed by password security with percentage of 82.3%, malware with percentage of 78.7%, cyberbullying with percentage of 67%, phishing with percentage of 66%, and Downloading, sharing, and use of pirated content with percentage of 22.7%. Out of the total percentage of each focus area, the results shows that the focus area identity theft, password security and malware are in the good criteria of awareness, and taking action is not fully needed. But the percentage of cyberbullying and phishing are in the average criteria, so it can be said that action is potentially required. However the percentage of downloading, sharing, and use of pirated content is very poor, which means that it needs too much attention because its percentages are very low even in each dimension compared to other focus areas.

4.4. Research questions

4.4.1. What attitude, knowledge, and behavior do the undergraduate students at Makerere University have on the six focus areas?

The total percentage of the attitude that undergraduate students at Makerere University have on password security, cyberbullying, phishing, malware, identity theft and downloading sharing and use of pirated content is 64.7% which is in the average or satisfactory criteria of awareness criteria, so it state that the action is potentially required.

The total percentage of the knowledge that undergraduate students at Makerere University have on password security, cyberbullying, phishing, malware, identity theft and downloading sharing

and use of pirated content is 61.3% which is in the average or satisfactory criteria of awareness criteria, so it state that the action is potentially required.

The total percentage of the behavior that undergraduate students at Makerere University have on password security, cyberbullying, phishing, malware, identity theft and downloading sharing and use of pirated content is 72.4% which is in the average or satisfactory criteria of awareness criteria, so it state that the action is potentially required.

4.4.2. What are means do the undergraduate students at Makerere University use to protect themselves against cyber-attacks?

Which of the following do you use to protect yourself from cyber-attacks?

		Responses		
		N	Percent	Percent of Cases
Means	Turn on multifactor authentication	177	14.2%	44.3%
	Update your software and operating system	160	12.9%	40.0%
	Think before you click	162	13.0%	40.5%
	Use strong password	309	24.9%	77.3%
	Use antivirus software	177	14.2%	44.3%
	Use antispyware software	35	2.8%	8.8%
	Backup your data	223	17.9%	55.8%
Total		1243	100.0%	310.8%

a. Dichotomy group tabulated at value 1.

Table 43.Means to protect against cyber-attacks

Based on the results from the table 39, use of strong password is the mostly way used by students followed by backup of data, turn on multifactor authentication, use of antivirus software, think before you click, update your software and operating system and lastly use antispyware software.

4.5. Suggested solutions

Based on the findings of the study, as the cybersecurity awareness level of the respondents is in average or satisfactory criteria, as it states that potential action is required. Here are some information security awareness delivery methods that can be used to increase the level of cybersecurity awareness at Makerere University among undergraduate students. There are numerous information security awareness delivery models. And these models are capable of

increasing the awareness of students for a wide range of cybersecurity problems that ranges from spam and phishing to well organized attacks intending to manipulate or disable systems.

4.5.1. Conventional delivery methods

The conventional of delivering information security awareness include paper resources and electronic resources. Hardy copy or paper based security awareness delivery methods enclose posters and flyers that attract attention with slogans on relevant subjects (e.g. reminding students that their password are not to be shared) and newsletters (newsletters, memos and news clipping). To announce only one topic at any given time posters are commonly used. They are mostly displayed in gathering areas such as meeting rooms and canteens. They can be used to spotlight time sensitive topics and remind students of very particular actions that they can take to improve their online security. Newsletter can be a periodic (e.g. quarterly or monthly) channel of information security awareness. Newsletters can be in electronic or print format. Reinforcing information security awareness program is one of the primary purpose of newsletters. Compared to posters newsletters have an advantage of conveying a number of massages at the same time.

4.5.2 Instructor-led delivery methods

Different formal presentations (e.g. seminars and class room style workshops) assisted by information security experts can be used to improve information security awareness of students. These approach have a purpose to impact on the individual level through an expert (i.e. instructor-led) conducted at a large population. One of the advantages of instructor led delivery method is that the instructor is able to improve instructional methods appropriately, understand nonverbal student hints and give convenient answers to students' questions. This can be used to increase the level of awareness of the students especially on the focus area of downloading, sharing and using pirated contents as many of the respondents didn't know that it is illegal and it can compromise their devices. It can also be used on the focus area of cyberbullying as students tend to do or participate in cyberbullying, students need to know that legal measures can be taken against them.

4.5.3. Online delivery methods

There are different ways of online security awareness delivery models. Those methods include online synchronous and asynchronous discussion, e-mail broadcasting, information uploading, animation, blogging and multimedia. Generally these delivery methods are suitable for supporting multiple teaching methods over different geographical areas.

One of the online delivery method is the web based computer security awareness training (WBT), it offers flexible models that allow users to increase security awareness at their own pace and it is user friendly. It can provide the university the ability to train students to a wide standard. Alert security messages such as pre-logon messages and email messages are one of the ways for improving information security awareness. The flexibility to deliver one message to many is one of the strengths of email. Emails campaigns can be directed at students. Different mobile platforms that teach anytime and anywhere information security awareness have emerged. Social media is an ideal tool through which awareness on existing and emerging threats can be created. And the advantage of learning on mobile based on social media is that you can check if the receiver like the message or not. (Jemal, 2012).

4.5.4. Game-based delivery methods

Online games merge graphics, play and trainings ideas to generate compiling training experiences. Game based awareness delivery method give a benefit of challenge, motivation and engagement of the participants. They are very interactive so they can help the university's objective of security awareness while engaging students. One of the game based information security awareness delivery is CyberCIEGE. In the virtual world of CyberCIEGE, users pay virtual money to defend and operate their networks, and while they are under attack, they can watch the consequences of their choices. In this video game players buy and configure workstations, operating systems, servers, network devices and applications (NPS, 2023). Anti-Phishing Phil is another game based awareness training system, it has a purpose to teach users how to differentiate phishing URLs and legitimate ones, how to find cues in web browser and how to utilize search engines to identify legitimates sites (CMU, 2023).

4.5.5. Video-based delivery methods

Online video is a way that give visual and audio learning for the participants. Students can learn independently and study at their own speed and only what they need to learn. Students can also start and stop the training according to their schedule because it is not time dependent. The online video trainings is a flexible and an effective training choice as the videos can be watched and re-watched.

4.5.6. Simulation-based delivery methods

In simulation based information security awareness delivery methods, to test user's vulnerability to phishing attacks, users are sent simulated phishing emails and then follow up with trainings (Jagatic et al. 2007, Spagat 2009). After all, users are given materials that teach them about phishing attacks and phishing emails that were used to evaluate progresses in phishing detection capacities of the users. This delivery method can be used to teach students how to detect phishing emails.

For the sake of fighting students based vulnerabilities and raise the security awareness levels of the students a strong awareness program is needed to make sure that students understand their information security responsibilities, university policies and how to appropriately use and protect their devices (PC, smartphones, tables, etc.) and university assets. Also, to keep the students in row and refreshed any awareness program must be in progress and be a part of the university culture.

CHAPTER 5. CONCLUSION AND RECOMMENDATION

5.1. Conclusion

This research shows that the overall level of cybersecurity awareness for undergraduate students at Makerere University is at average or satisfactory criteria (67.4%), which states that action is potentially required. This means that the university need to put some effort to increase the level of cybersecurity. Some focus areas need to be addressed in order to have potential development. In the dimension of knowledge, cyberbullying, phishing and downloading, sharing, and use of pirated content need to be fixed and addressed to a get higher percentage. While in the dimension of attitude, there are password security, cyberbullying, phishing and downloading, sharing, and use of pirated content. And also in the dimension of behavior, there are cyberbullying, phishing and downloading, sharing, and use of pirated content.

5.2. Recommendation

Based on the results of this research, the following are recommended:

- Makerere University should raise knowledge, attitude and behavior on some cybersecurity factors such as cyberbullying, phishing and mostly on downloading, sharing, and use of pirated content.
- The delivery methods for cybersecurity awareness and training campaigns, can be text based, game based or video based.
- To develop a sustainable cybersecurity behavior among students security awareness should be taught at young age.
- The university should have many programs, campaigns and socializations related to cybersecurity especially in the matter of content piracy. Because the data from the research shows that there are many students who download and use content illegally and they don't know the consequences of content piracy.

5.3. Areas for further research

This research has limitations as other studies, the involved respondents did not represent larger population. As well, this research did not represents other broader cybersecurity subjects. For that reason, the next research can improve the method and framework with numerous developments, such as, detailed focus area and deeper qualitative researches in cybersecurity awareness.

References

1. International telecommunication union (ITU). (2023, March 07). Measuring digital development: Facts and Figures 2022. https://www.itu.int/en/ITUD/Statistics/Pages/facts/default.aspx#:~:text=Latest%20figures%20show%20that%20an,over%20own%20a%20mobile%20phone
2. DATAREPORTAL. (2023, March 7). DIGITAL 2022: UGANDA. https://datareportal.com/reports/digital-2022-uganda
3. National Institute of Standards and Technology (NIST). (2018). Framework for Improving Critical Infrastructure Cybersecurity version 1.1.
4. Iqbal, H. S., Kayes, A. S. M., Shahriar, B., Hamed, A., Paul, W. & Alex, N. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data. https://doi.org/10.1186/s40537-020-00318-5.
5. AV-TEST. (2022, August 08). Malware. https://www.av-test.org/en/statistics/malware/
6. Sausalito, C. (2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime magazine. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report2016/#:~:text=Cybersecurity%20Ventures%20expects%20global%20cybercrime,%243%20trillion%20USD%20in%202015.
7. Senthilkumar, K. & Sathishkumar, E. (2017). A Survey on Cyber Security awareness among college students in Tamil Nadu. IOP publishing. doi:10.1088/1757-899X/263/4/042043
8. Steven, A. (2017). Cybersecurity: The cold war online. Nature. 2017;547(7661):30
9. Eric, A., F. (2017). Cybersecurity Issues and Challenges. Congressional research service.
10. 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. Paper presented at the Information and Communication Technology for the Muslim World (ICT4M) 2010 International Conference, Jakarta, 13-14 December. https://doi.org/10.1109/ict4m.2010.5971884
11. Mochiko, T. (2016, November 22). Cybercrime “will rise” with internet of things. Business Live. https://www.businesslive.co.za/bd/life/gadgets-and-gear/2016-11-22cybercrime-will-rise-with-internet-of-things
12. Adamu, A., G., Maheyzah, B., S. & Siti, H. (2020). Cybersecurity awareness among university students: a case study.
13. Talal, A., & Asifa, T. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University.
14. Al-Janabi, S. & Al-Shourbaji, I. (2016). A study of cyber security awareness in educational environment in the middle east. J. Inf. Knowl. Manag. 1650007.
15. Slusky, L.& Partow-Navid, P. (2012). Students information security practices and awareness. J. Inf. Priv. Secur. 8, 3–26.
16. Rajan, M. (2010). Internet phishing hook, line and hopefully not sunk. MBA thesis, University of KwaZulu-Natal, Durban.

17. Dodge R. C., & Ferguson A. J. (2006). Using phishing for user email security awareness. In S. Fischer-Hübner, K. Rannenberg L. Yngström. & S. Lindskog (Eds.), Security and privacy in dynamic environments. Proceedings of the IFIP TC-11 21st International Information Security Conference (SEC 2006), 22-24 May, Karlstad, Sweden. https://doi.org/10.1007/0-387-33406-8_41
18. Steyn, T., Kruger, H. A., & Drevin, L. (2007). Identity theft – empirical evidence from a phishing exercise.
19. Mishra, U. (2014). Is anti-virus a necessary evil? https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2434470
20. Pramod, D., & Raman, R. (2014). A study on the user perception and awareness of smartphone security. International Journal of Applied Engineering Research, 9(23), 19133-19144.
21. Pretorius, B., & Van Niekerk, B. (2015). Cyber-security and governance for ICS/SCADA in South Africa. In J. Zaaiman, & L. Leenen (Eds.),Proceedings of the 10th International
22. Lennon, M. (2015). FireEye uncovers decade-long cyber espionage campaign targeting South East Asia. Security Week. Retrieved from http://www.securityweek.com/fireeye-uncovers-decade-long-cyber-espionage-campaign-targeting-southeast-asia
23. Mitre. (2014, April). The Heartbleed Bug. Retrieved from http://heartbleed.com/
24. Rosenblatt, S. (2014, April 28). Stop using Microsoft's IE browser until bug is fixed, US and UK warn. CNET. Retrieved from http://www.cnet.com/news/stop-using-ie-untilbug-is-fixed-says-us
25. TroyHunt. (2014). Everything you need to know about the Shellshock Bash bug. Retrieved from http://www.troyhunt.com/2014/09/everything-you-need-to-know-about.html
26. Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. Academy of Information & Management Sciences Journal, 14(2), 91-153.
27. Janssen, C. (2014). Techopedia. Retrieved from http://www.techopedia.com/it-dictionary
28. Wlasuk, A. (2012). Higher education – the perfect security storm. Security Week. Retrieved from http://www.securityweek.com/higher-education-perfect-securitystorm
29. Kim, E. B. (2014). Recommendations for information security awareness training for college students. Information Management & Computer Security, 22(1), 115-126. https://doi.org/10.1108/imcs-01-2013-0005
30. Kaur, J., & Mustafa, N. (2013). Examining the effects of knowledge, attitude and behavior on information security awareness: A case on SME. In IEEE (Ed.), 2013 International Conference on Research and Innovation in Information Systems (ICRIIS) (pp. 286-290). https://doi.org/10.1109/icriis.2013.6716723
31. Bada, M., & Sasse, A. (2014). Cyber security awareness campaigns why do they fail to change behaviour? Global Cyber Security Capacity Centre. Retrieved from http://discovery.ucl.ac.uk/1468954/1/Awareness%20CampaignsDraftWorkingPaper.pdf
32. 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. Paper presented at the Information and Communication Technology for the Muslim World (ICT4M) 2010

International Conference, Jakarta, 13-14 December. https://doi.org/10.1109/ict4m.2010.5971884
33. Bakar, E. A., Chang, L. L., & Saidin, A. Z. (2013). Knowledge, attitude and practices of consumers in e-commerce transactions. Paper presented at the Information and Communication Technology for the Muslim World (ICT4M) 5th International Conference. Rabat, 26-27 March. https://doi.org/10.1109/ict4m.2013.6518903
34. Peltier, T. R. (2005). Implementing an information security awareness program. Information Systems Security, 14(2), 37-49. https://doi.org/10.1201/1086/45241.14.2.20050501/88292.6
35. Kwasi, A., Nabeel, M., Aminata, A., & Garba, M., S. (2018). Assessing Cybersecurity Policy Effectiveness in Africa via a Cybersecurity Liability Index. SSRN.
36. Nir, K. (2019). Cybercrime and Cybersecurity in Africa. Journal of Global Information Technology Management, 22:2, 77-81. DOI: 10.1080/1097198X.2019.1603527. https://doi.org/10.1080/1097198X.2019.1603527
37. Kruger, H., A., & Kearney, W., D. (2006). A prototype for assessing information security awareness. Elsevier.
38. Kruger, H., A., Drevin, L., & Steyn, L. (2010). A vocabulary Test to Assess Information Security Awareness. South African Information Security Multi-conference in Port Elizabeth, South Africa.
39. Sari, P., K. (2012). Concept of Information Security Management for Higher Education. International Conference on Technology and Operation Management, 3rd. Bandung. 469-477.
40. Chandarman, R., & Van, N., B. (2017). Students' cybersecurity awareness at a private tertiary educational institution. The African Journal of Information and Communication (AJIC), 20, 133-155. https://doi.org/10.23962/10539/23572
41. Stavroulakis, P., & Stamp, M. (2010). (Eds.) Handbook of Information and Communication Security; Springer Science & Business Media: Berlin/Heidelberg, Germany.
42. Jakobsson, M., & Myers, S. (2006). Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft; Wiley: Hoboken, NJ, USA.
43. Rekouche, K. (2011). Early Phishing. arXiv 2011, arXiv:1106.4692.
44. Rader, M.A. & Rahman, S.M. (2013). Phishing Techniques and Mitigating the Associated Security Risks. Int. J. Netw.Secur. Appl. 2013, 5, 23–41. [CrossRef]
45. Symantec. (2015). ISTR Internet Security Threat Report 2015. https://docs.broadcom.com/doc/istr-24-2019-en
46. APWG (Anti-Phishing Working Group). (2019). Phishing Activity Trends Report: 3rd Quarter2019. 2019. https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf
47. Symantec. (2018). ISTR Internet Security Threat Report Volume 23. 2018. Available online: https://www.phishingbox.com/assets/files/images/Symantec-Internet-Security-Threat-Report-2018.pdf
48. APWG. (2019). Phishing Activity Trends Reports. https://apwg.org/trendsreports/
49. IBM. (2019) IBM X-Force Threat Intelligence Index 2019. https://www.securindex.com/downloads/8b9f94c46a70c60b229b04609c07acff.pdf

50. ICC (IC3)/Federal Bureau of Investigation (FBI). (2018). Internet Crime Report 2018. https://www.fbi.gov/news/stories/ic3-releases-2018-internet-crime-report-042219
51. Threatpost. (2019). Seals, T. Elder Scrolls Online Targeted by Cybercrooks Hunting In-Game Loot. . https://threatpost.com/elder-scrolls-online-cybercrooks-in-gameloot/150934/
52. Verizon. (2019). Data Breach Investigations Report. Comput. Fraud Secur.
53. Forget, A. (2012). A world with many authentication scheme. Ph.D. thesis, Carleton University, Ottawa, Ontario.
54. Goldberg, J., Hagman, J., & Sazawal, V. (2002). Doodling our way to better authentication. In: CHI Extended Abstracts on Human Factors in Computing Systems, pp. 868–869. ACM
55. Thorpe J., MacRae, B., & Salehi-Abari, A. (2013). Usability and security evaluation of geopass: A geographic location-password scheme. In: Proceedings of the Ninth Symposium on Usable Privacy and Security, SOUPS '13, pp. 1–14. ACM, New York, NY, USA. https://doi.org/10.1145/2501604.2501618
56. Bonneau, J., Herley, C., van Oorschot, P.C., & Stajano, F. (2012). The quest to replace passwords: a framework for comparative evaluation of web authentication schemes. In: Security & Privacy (SP), IEEE Symposium, pp. 553–567.
57. Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A., & Memon, N. (2005). Authentication using graphical passwords: effects of tolerance and image choice. In: Proceedings of the 2005 Symposium on Usable Privacy and Security, SOUPS '05, pp. 1–12. ACM, New York, NY, USA.
58. Carstens, D.S., McCauley-Bell, P.R., Malone, L.C., & DeMara, R.F. (2004). Evaluation of the human impact of password authentication practices on information security. Inf. Sci. J. 7, 67–85.
59. Herley, C., van Oorschot, P., & Patrick, A. (2009). Passwords: If we're so smart, why are we still using them? In: Dingledine, R., Golle, P. (eds.) Financial Cryptography and Data Security, FC 2009. Lecture Notes in Computer Science, vol. 5628, pp. 230–237. Springer, Berlin.
60. Summers, W., & Bosworth, E. (2004) Password policy: the good, the bad, and the ugly. In: Proceedings of the Winter International Symposium on Information and Communication Technologies, pp. 1–6. ACM.
61. Yan, J., Blackwell, A., Anderson, R., & Grant, A. (2004). Password memorability and security: empirical results. IEEE Priv. Secure. 2(5), 25–31.
62. Katha, C. (2016). Password Security: An Analysis of Password Strengths and Vulnerabilities. I. J. Computer Network and Information Security, 2016, 7, 23-30. DOI: 10.5815/ijcnis.2016.07.04
63. Manber, U. (1996). A simple scheme to make passwords based on one-way functions much harder to crack. Computers & Security 15.2: 171-176.
64. Gayathiri, C. (2012).Text Password Survey: Transition from First Generation to Second Generation‖ unpublished.

65. Wong-Lo, M., & Bullock, L. M. (2011). Digital aggression: Cyberworld meets school bullies. Part of a special issue: Cyberbullying By: Preventing School Failure, 55(2), 64-70. DOI: 10.1080/1045988X.2011.539429
66. Miller, J. D., & Hufstedler, S. M.. (2009). Cyberbullying knows no borders. Australian Teacher Education Association, Paper presented at the Annual Conference of the Australian Teacher Education Association (ATEA) (Albury, Jun 28-Jul 1, 2009). (ED524610)
67. Beale, A. V., & Hall, K. R. (2007). Cyberbullying: What school administrators (and parents) can do? Clearing House, 81(1), 8-12. DOI: 10.3200/TCHS.81.1.8-12.
68. Charles, E., N., Sharon, P., & Jessica, R. (2013). Cyberbullying: A Review of the Literature. Universal Journal of Educational Research 1(1): 1-9, 2013. DOI: 10.13189/ujer.2013.010101
69. Mustacchi, J. (2009). R U Safe? Educational Leadership, 66(6), 78-82.
70. Adams, C. (2010). Cyberbullying: How to make it stop. Instructor. 120(2), 44-49.
71. Hoff, D. L., & Mitchell, S. N. (2009). Cyberbullying: Causes, effects, and remedies. Journal of Educational Administration, 47(5), 652-665.
72. Jones, S. E., Manstead, A. S. R., & Livingstone, A. G. (2011). Ganging up or sticking together? Group processes and children's responses to text-message bullying. British Journal of Psychology, 102(1), 71-96.
73. Şahin, M. (2012). The relationship between the cyberbullying/cybervictmization and loneliness among adolescents. Children & Youth Services Review, 34(4), 834-837.
74. Rivers, I., & Noret, N. (2010). British Educational Research Journal, 36(4), 643-671.
75. Ömer A., & Refik, S. (2020). A Comprehensive Review on Malware Detection
76. Approaches. IEEE access.
77. Morgan, S. (2019). cybersecurity almanac: 100 facts, figures, predictions and statistics. Cisco and Cybersecurity Ventures. Accessed: Nov. 10, 2019. [Online]. Available: https://cybersecurityventures.com/cybersecurity-almanac-2019
78. Samani, R., & Davis, G. (2019). McAfee Mobile Threat Report Q1. [Online]. Available: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf
79. Cohen, F. (1986). ‘‘Computer viruses,’’ Ph.D. dissertation, Univ. SouthernCalifornia, Los Angeles, CA, USA.
80. Cohen, (1992). ‘‘A formal definition of computer worms and some related results,’’ Comput. Secur. vol. 11, no. 7, pp. 641–652.
81. Chess, D., M., & White, S., R. (2000). ‘‘An undetectable computer virus,’’ in Proc. Virus Bull. Conf., vol. 5.
82. Cohen, F. (1987). ‘‘Computer viruses: Theory and experiments,’’ Comput. Secur.,vol. 6, no. 1, pp. 22–35.
83. Adleman, L., M. (1990). ‘‘An abstract theory of computer viruses,’’ in Advances in Cryptology—CRYPTO. New York, NY, USA: Springer-Verlag.
84. Spinellis, D. (2003). ‘‘Reliable identification of bounded-length viruses is NPcomplete,’’ IEEE Trans. Inf. Theory, vol. 49, no. 1, pp. 280–284.
85. Zuo, Z., Zhu, Q., & Zhou, M. (2005). ‘‘On the time complexity of computer viruses,’’ IEEE Trans. Inf. Theory, vol. 51, no. 8, pp. 2962–2966.

86. Alosefer, Y. (2012) ‘‘Analysing Web-based malware behaviour through client honeypots,’ Ph.D. dissertation, School Comput. Sci. Inform., Cardiff Univ., Cardiff, U.K.
87. Sikorski, M. & Honig, A. (2012). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. San Francisco, CA, USA: No Starch Press.
88. Idika, N., & Mathur, P. (2007). ‘‘A survey of malware detection techniques,’’ Purdue Univ., West Lafayette, IN, USA, Tech. Rep., vol. 48.
89. Eilam, E., (2011). Reversing: Secrets of Reverse Engineering. Hoboken, NJ, USA:Wiley.
90. Souri, A., & Hosseini, R. (2018). ‘‘A state-of-the-art survey of malware detection approaches using data mining techniques,’’ Hum.-Centric Comput. Inf.Sci., vol. 8, no. 1, p. 3.
91. Gandotra, E., Bansal, D., & Sofat, S. (2104). ‘‘Malware analysis and classification: A survey,’’ J. Inf. Secur., vol. 5, no. 2, pp. 56–64.
92. Dadkhah, M., Lagzian, M., & Borchardt, G. (2018). “Identity Theft in the Academic World Leads to Junk,” Science and Engineering Ethics, vol. 24, no. 1, pp. 287–290. https://doi.org/10.1007/s11948-016-9867-x
93. Irshad, S., & Soomro, T., R., (2018). “Identity Theft and Social Media,” International Journal of Computer Science and Network Security, vol. 18, no. 1, pp. 43–55.
94. FBI. (2016). “Internet Crime Report (2016),” Internet Crime Complaint Center.
95. FBI. (2017). “Internet Crime Report (2017),” Internet Crime Complaint Center.
96. FTC. (2017). “FTC Releases Annual Summary of Consumer Complaints (2017),” FTC.
97. European Union Agency for Network and Information Security. (2014), 16 Million E-Identities and Passwords Theft. European Union Agency for Network and Information Security.
98. Banjo, S. (2014), ‘Hope Depot Hackers Exposed 53 Million Email Addresses’, The Wall Street Journal.
99. Perlroth, N. & Gelles, D. (2014), Russian Hackers Amass Over a Billion Internet Passwords. New York Times.
100. Finkle, J. & Hosenball, M. (2014), FBI Warns Retailers to Expect More Credit Card Breaches. Reuters.
101. Ablon, L., Libicki, M. C. & Golay, A. A. (2014), Markets for Cybercrime Tools and Stolen Data. Rand Corporation.
102. Wall, D. S. (2013), ‘Policing Identity Crimes’, Policing and Society, 23: 437–60.
103. Burnap, P., Rana, O. F., Avis, N., Williams, M. L., Housley, W., Edwards, A., Morgan, J. & Sloan, L. (2013), ‘Detecting Tension in Online Communities With Computational Twitter Analysis’, Technological Forecasting & Social Change.
104. Burnap, P., Williams, M. L. & Sloan, L. (2014), ‘Tweeting the Terror: Modelling the Social Media Reaction to the Woolwich Terrorist Attack’, Social Network Analysis and Mining, 4: 206.
105. Sloan, L., Morgan, J., Housley, W., Williams, M. L., Edwards, A., Burnap, P. & Rana, O. F. (2013), ‘Knowing the Tweeters: Deriving Sociologically Relevant Demographics from Twitter’, Sociological Research Online.
106. Cohen, L. and Felson, M. (1979), ‘Social Change and Crime Rate Trends: A Routine Activity Approach’, American Sociological Review, 44: 588–608.

107. Statista. (September 16, 2022). Number of social media users worldwide from 2018 to 2027. https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/
108. Wang, X., & McClung, S.R.(2011). Toward a detailed understanding of illegal digital downloading intentions: an extended theory of planned behavior approach. New Media Soc. 13 (4), 663–677.
109. Karaganis, J., & Renkema, L. (2013). Copy culture in the US & Germany. Retrieved from the American Assembly website: http://piracy.americanassembly.org/wpcontent/uploads/2013/01/Copy-Culture.pdf.
110. Filiciak, M., Tarkowski, A., & Hofmokl, J. (2012). Obiegi kultury. Społeczna cyrkulacja treści. Raport z badań. Warszawa: Centrum Cyfrowe.
111. NI Diret. (2022). Preventing your child from downloading and file sharing illegally. https://www.nidirect.gov.uk/articles/preventing-your-child-downloading-and-file-sharing-illegally
112. Watson, R. (April 1, 2015). Quantitative research. Nursing Standard (2014+); London Vol. 29, Iss. 31: 44. DOI:10.7748/ns.29.31.44.e8681. https://www.proquest.com/openview/058c84ecfd436cf965eacb1556000ab0/1?pq-origsite=gscholar&cbl=2042228
113. Bahurmoz, A. (2006). The Analytic Hierarchy Process: A Methodology for Win-Win Management. JKAU: Econ. & Adm., Vol. 20, No. 1.
114. Scott, N., R. & Mary, M. (2020). Routledge Companion to Global Cyber-Security Strategy.
115. Paul, K. (2017). "Cybercrime in Uganda: computer Security. www.forensicsinstitute.org/cybercrime-inuganda/
116. Ndagire, B. (2020, January 30). How fraudsters cheated govt, MTN in phone calls scam, Daily Monitor. www.monitor.co.ug/News/National/How-fraudsters-cheated-government-MTN-phonecalls-scam/688334-5437814-nfu2q6/index.html
117. Osekeny, J. (2018, September 24). Uganda Ranked 1st in Africa in the National Cyber Security Index. https://guru8.net/2018/09/uganda-ranked-1st-in-africa-in-the-national-cyber-security-index/
118. Kusumadewi, S., Hartati, S., Harjoko, A., & Wardoyo, R. (2006). Fuzzy MultiAttribute Decision Making (FUZZY MADM). Special Region of Yogyakarta: Graha Ilmu.
119. Balqis, R., C., & Candiwan. (2020). Analysis of College Students' Cybersecurity Awareness In Indonesia. DOI 10.24167/sisforma.v7i2.2706
120. Yamane, T. (1967). Statistics, an Introductory Analysis, 2nd Ed., New York: Harper and Row.
121. Kruger, H., A. & Kearney, W., D. (2006) A Prototype For Assessing Information Security Awareness Computers & Security, 25(4), 289–296.
122. Sari, P., K. & Candiwan. (2014). Measuring Information Security Awareness of Indonesian Smartphone Users, TELKOMNIKA (Telecommunication Computing Electronics and Control), 12(2), 493.

123. Moallem, A. (2018). Cyber Security Awareness among College Students. In International Conference on Applied Human Factors and Ergonomics; Springer: Berlin/Heidelberg, Germany. pp. 79–87.
124. Mohammed, A., A. (2022). Factors Affecting Cybersecurity Awareness among University Students.
125. Phuong, T., M. & Andrea, T. (2021). Cyber Security Awareness and Behavior of Youth in Smartphone Usage: A Comparative Study between University Students in Hungary and Vietnam.
126. Mark, C. & Christopher, J., A. (1998). Extending the Theory of Planned Behavior: A Review and Avenues for Further Research.
127. Rosaria de F.S.M., R & Roberto, C. (2015). Criteria in AHP: A Systematic Review of Literature
128. Saaty, T., L. (2008). Decision making with the analytic hierarchy process. Int J Serv Sci ;1:83-98
129. Naval Postgraduate School (NPS). (24th May 24, 2023). CyberCIEGE. https://nps.edu/web/c3o/cyberciege
130. Carnegie Mellon University (CMU). (24th May 24, 2023). Information Security Office. https://www.cmu.edu/iso/aware/phil/index.html
131. Jagatic, T., Nathaniel, A., J., Markus, J. & Filippo, M. (2007). Social phishing. Communications of the ACM, 50 (10), 94–100.
132. Spagat, E., (2009). Justice Department Hoaxes Employees. News Article [online]. Available from: http://news.yahoo.com/s/ap/20090129/
133. Jemal, A. (2012). User preference of cyber security awareness delivery methods.
134. Koepp, G.A.; Snedden, B.J.; Flynn, L.; Puccinelli, D.; Huntsman, B.& Levine, J.A. (2012). Feasibility Analysis of Standing Desks for Sixth Graders. ICAN Infant, Child, Adolesc. Nutr.89–92.
135. Hulin, C., Netemeyer, R., and Cudeck, R. (2001). Can a Reliability Coefficient Be Too High?
136. Ani, P. (2023). Number of unique phishing sites detected worldwide from 3rd quarter 2013 to 34th quarter 2022. https://www.statista.com/statistics/266155/number-of-phishingdomainnamesworldwide/#:~:text=In%20the%20fourth%20quarter%20of,increase%20from%20the%20preceding%20quarter.
137. Statista research department. (2023). Number of consumer complaints relating to identity theft lodged with the U.S. Federal Trade Commission from 2001 to 2022. https://www.statista.com/statistics/587351/indentity-theft-complaints-frequency-in-the-us/