CYBER HYGIENE DURING COVID-19 TO AVOID CYBER ATTACKS

BY

YVONNE LEE YI JIN

A REPORT
SUBMITTED TO
Universiti Tunku Abdul Rahman
in partial fulfillment of the requirements
for the degree of
BACHELOR OF INFORMATION SYSTEMS (HONOURS) BUSINESS INFORMATION SYSTEMS
Faculty of Information and Communication Technology
(Kampar Campus)

JAN 2022

UNIVERSITI TUNKU ABDUL RAHMAN

REPORT STATUS DECLARATION FORM

Title: CYBER HYGIENE DURING COVID-19 TO AVOID CYBER ATTACKS

Academic Session: JANUARY 2022

I YVONNE LEE YI JIN

(CAPITAL LETTER)

declare that I allow this Final Year Project Report to be kept in
Universiti Tunku Abdul Rahman Library subject to the regulations as follows:

1. The dissertation is a property of the Library.
2. The Library is allowed to make copies of this dissertation for academic purposes.

Verified by,

(Author's signature)

(Supervisor's signature)

Address:
D-210, PANGSAPURI MAKMUR,
JALAN PJS 8/9, TAMAN SRI SUBANG,
41650 PETALING JATA, SELANGOR.

Yap Seok Gee
Supervisor's name

Date: 21 APRIL 2022

Date: 22/4/2022

Universiti Tunku Abdul Rahman			
Form Title : **Sample of Submission Sheet for FYP/Dissertation/Thesis**			
Form Number: **FM-IAD-004**	Rev No.: **0**	Effective Date: **21 JUNE 2011**	Page No.: **1 of 1**

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

UNIVERSITI TUNKU ABDUL RAHMAN

Date: 21 April 2022

SUBMISSION OF FINAL YEAR PROJECT/DISSERTATION/THESIS

It is hereby certified that ______***Yvonne Lee Yi Jin***___________ (ID No: __***18ACB02825***__) has completed this final year project entitled "*Cyber Hygiene During Covid-19 To Avoid Cyber Attacks*" under the supervision of Ms Yap Seok Gee (Supervisor) from the Department of Information Systems, Faculty of Information And Communication Technology , and ____________________ (Co-Supervisor)* from the Department of _________________________, Faculty of __________________________.

I understand that University will upload softcopy of my final year project in pdf format into UTAR Institutional Repository, which may be made accessible to UTAR community and public.

Yours truly,

Yvonne.

____
(*Yvonne Lee Yi Jin*)

*Delete whichever not applicable

DECLARATION OF ORIGINALITY

I declare that this report entitled "**CYBER HYGIENE DURING COVID-19 TO AVOID CYBER ATTACKS**" is my own work except as cited in the references. The report has not been accepted for any degree and is not being submitted concurrently in candidature for any degree or other award.

Signature :

Name : Yvonne Lee Yi Jin

Date : 21 APRIL 2022

ACKNOWLEDGEMENTS

My current research cannot be accomplished only by my own efforts. Throughout the study process, I received a great deal of assistance and resources. As a result, I'd like to take this opportunity to thank the few people that helped and led me during the process.

I would like to express my sincere thanks and appreciation to my supervisor, Ms Yap Seok Gee who has given me this bright opportunity to engage in a research project about cyber hygiene. It is my first step to establish a deep study on cyber hygiene. A million thanks to you.

In addition, I would like to say thanks to Dr. Mobashar who has given me a lot of suggestions and comments on my research project. I really appreciate Dr. Mobashar for giving me support and guideline which help me in completing my project.

Furthermore, I would like to convey my appreciation to every respondent who has agreed to participate in this study. I would not have been able to finish my research study without their honest participation and assistance in distributing the questionnaire to their friends. As a result, I really appreciate of the time and effort put in by my responders in providing me with helpful information.

Finally, I must say thanks to my parents and my family for their love, support, and continuous encouragement throughout the course.

ABSTRACT

This project is a research study on cyber hygiene during COVID-19 to avoid cyber-attacks for academic purposes. Cyber security is crucial in today's cyber defence. Cyber security expenses have increased over the past decade while massive infringements of data and data leaks have also risen. In addition, we need to practice the best cyber hygiene behaviors in order to avoid cyber-attacks like phishing, data loss, and others. Therefore, we need a deeper understanding of how the various variables have an impact on cyber hygiene behaviour. In this study, we will further evaluate how the self-efficacy, cyber hygiene knowledge, and cyber hygiene awareness affect the cyber hygiene attitude and then lead to cyber hygiene behavior. Moreover, the Theory of Planned Behavior (TPB) was used in this study to help investigate the relationship between attitude, intentions, and behavior toward cyber hygiene. Five hypotheses were developed in hopes of identifying the relationship between the factors and cyber hygiene behavior. In order to gain deeper understanding, the questionnaire was created and delivered via the Google Form to the 160 responders. After received the responds from participants, we had run the analysis on all the variables by using SmartPLS 3.3 and calculate the PLS-SEM algorithm of the variables. After running the analysis, we discuss our key findings using the results for each path's t-statistic and p-value. Last but not least, the implications of this study are presented, with the hope that future researchers, policymakers, and practitioners can serve as a reference for further experimental approaches to improve the current state of cyber hygiene behavior.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

SE	Self-efficacy
CHK	Cyber Hygiene Knowledge
CHA	Cyber Hygiene Awareness
CHAtt	Cyber Hygiene Attitude
CHI	Cyber Hygiene Intention
CHB	Cyber Hygiene Behavior
TPB	Theory of Planned Behavior
CA	Composite Reliability
AVE	Average Variance Extracted

Chapter 1

Research Overview

1.0 Introduction

The purpose of this study is to observe the factors that lead to the cyber hygiene behavior of Malaysia Internet users to avoid cyber-attacks during COVID-19. This section will include the research background, problem statement, research objective, research question, the hypothesis of the study, and research significance.

1.1 Research Background

In the fourth quarter of 2019, the world began a new way of life as a result of the COVID-19 epidemic. COVID-19 (coronavirus disease) is a widespread epidemic. The pandemic has caused concern in businesses and individuals all around the world [1]. The number of infected people has risen to almost 60 million, with over a million people dying. Countries must adopt bans and segregate people to protect lives and limit the spread of the COVID-19 virus. As a result, computer systems and virtual worlds have evolved into essential instruments for human connection [2]. Most businesses, for example, need employees to work from home, students are transitioning to online learning, online sales are growing, and social networking activity is on the rise, all of which has resulted in a huge increase in internet users [2].

Information security and data privacy are always at a risk in a world increasingly driven by big data, online transactions, social networking, and automated procedures performed utilizing IT systems. Cybercriminals continue to expand the number of attacks and the amount of harm they do to victims as new tools and technologies are developed [3]. Cyber-attacks are growing more widespread for many types of business and individuals nowadays. Based on the study of [4], a cyber-attack is an attempt to steal, alter, or destroy any vital data stored on a computer or computer network. Any person or process that gains unauthorized access or use qualifies as an attacker. Cyber-attacks can be carried out by individuals or groups. A cyber-attacks is intended to get access to an individual's or company's information systems. In cyber-attacks, malicious code is used to alter computer data, logic, or code. As a result, data is destroyed and disrupted, as well as illegal activity such as identity and information theft [4].

As the COVID-19 pandemic spreads rapidly across the globe, cyber-attack have also increased during the pandemic period. According to [1], despite the obstacles faced by this pandemic, fraudsters continue to target unwary individuals and organizations in order to steal sensitive information via social engineering. Cybercriminals are keen to take opportunity of the current situation by targeting healthcare providers such as hospitals, as well as manufacturing and pharmaceutical companies, and even government institutions [5]. The cyber-attacks that happened during pandemic are phishing for access to data, fake landing pages purporting to be from the World Health Organization, with the latest up to date COVID-19 infection numbers, social engineering activities, websites link that have been infected with malware, and attachments of email which contains malware [5]. Since the students have changed their study mode from physical class to online class, cyber-attacks among student group also increases. Example cyber-attack is mobile malware. [6] said that Check Point researchers discovered that mobile device threats have surged by 50% during 2018. As more students migrate from desktops to smartphone, mobile security become more crucial than ever. Besides, a study on cybersecurity threats during COVID-19 pandemic found that hackers are utilizing platforms like WhatsApp and Facebook for scams to entice people into phishing sites that could divulge personal information [6].

Cyber hygiene is an adaptable knowledge and behavior that can reduce dangerous internet behaviors which jeopardize the social, financial, and personal information of an individual [7]. The acts and steps taken by computer and other device users to maintain system health and boost online security are referred to as cyber hygiene [8]. Humans must practice cyber hygiene to protect their identity and other facts that could be stolen or compromised. Actually, cyber hygiene is comparable to personal hygiene in the sense that people must take care of and cultivate good habits to keep sensitive data organized, protected, and secure from cyber-attacks. People can do cyber hygiene like install software updates, use antivirus software, use unique passwords, use two-factor authentication, and other good online safety practices [8]. Maintaining cybersecurity requires good cyber hygiene. Cybersecurity is employed to aid in the prevention of data leakage, identity theft, and cyber-attacks [9], whereas cyber hygiene is the most common set of practices for managing cybersecurity risks [10]. To address cyber-attacks, cyber hygiene should be implemented, emphasizing the necessity of regular, low-impact security actions while reducing the danger of being a victim of cyber-attacks [11]. From individuals to organizations, everyone needs to maintain cyber hygiene to prevent them from cyber threats [12]. There are two obvious reasons why it is beneficial to practice a regular cyber hygiene behavior which are maintenance and security. A well-maintained system is unlikely to be affected by cyber security risks. Although predicting threats can be challenging, but it is feasible to prepare and prevent threats through reasonable cyber hygiene practices [8]. In this moment, not only is it critical to keep excellent physical hygiene in order to protect ourselves from COVID-19, but it is also critical to maintaining good cyber hygiene in order to protect ourselves from cyber-attacks. With the rapid increase in cyber-attacks in the COVID-19 era, cyber hygiene has become increasingly crucial.

1.2 Problem Statement and Motivation

With more individuals online than ever before, the current globe atmosphere provides a fertile hunting ground for hackers and other nefarious cyber predators, as well as a consistent, unwitting potential victim supply [13]. A vast number of destructive scams and intrusions have been disclosed in the last month or two, affecting susceptible systems all around the world, frequently unreported [13]. A total of 838 cybersecurity incidents were reported to the Malaysian Cyber Security Agency between March 18 and April 7, while the Malaysian government enforced a movement control order (MCO) restricting unrestricted travel around the country. The number of reported events jumped by 82.5 percent from the same period last year, with the bulk of cases including cyberbullying, illegal system hacking, and fraud. Phishing and emails scams claiming to provide COVID-

19 information account for a significant number of fraud cases. According to a Cisco Systems study survey of Asia-Pacific countries, cybersecurity difficulties persisted in Malaysian enterprises in 2020, with 62% of respondents encountering cyber-attacks, according to the Malaysia Cybersecurity 2020 annual report. Since the commencement of the COVID-19 epidemic, cyber-attacks have escalated by 25% or more [14]. Local businesses have been the target of cyber intrusions such as distributed denial of service (DDoS) assaults, according to [13], while data breaches accounted for 18% of all reported occurrences during the MCO. Other cases of people or targeted individuals seeking unlawful data or meddling with company systems and causing mayhem to have been observed in huge enterprises [13]. Business are particularly vulnerable since many workers now work from home, and their devices such as network infrastructure, and laptops are less secure than they were at work in office. This can disclose security flaws, but there are practical steps that can be taken to protect the sensitive data and maintain secure systems while work in home [13].

To avoid cyber-attacks, individuals who practice excellent cyber hygiene would take the time to update software and generate unique passwords. However, there might raise a lot of cybersecurity problems for the users who have poor cyber hygiene behavior. One of the poor cyber hygiene behavior is users share their password freely, reuse passwords, and can quickly share private information through social networks [15]. When users sharing their photos and posted them using hashtag in social media like Facebook, Twitter, and Instagram, scammers can quickly scan the site to find this tag, and possibly find users personal information. Typically, the snapshot includes supplementary information such as the date and location. This can be used to deduce other personal facts, such as the user's date of birth and the city in which they grew up, as well as common security difficulties with a bank account and retirement savings [16]**.** This issue must be addressed since attackers will be able to quickly get access to the system and steal user information or identify technical flaws. It is therefore important to help Internet users improve their understanding and conduct in cyber hygiene. No matter how strong the security of the system, people are more vulnerable than computers. Users who exhibit bad cyber hygiene practices such as users who do not follow best cyber hygiene practices or leak too much personal information will easily be the target of attackers [15].

As far as the security of information systems is concerned, passwords are vulnerable to network attacks and are therefore considered to be one of the most important risk factors [17]. Despite massive government education campaigns aimed at preventing dangerous online behavior, many people continue to engage in risky password practices, such as sharing passwords, using the same password on multiple platforms, and choosing passwords that are easy to guess [18]. The Norton Report is based on a survey of over 1,000 people aged 18 and up who own at least one mobile phone that was performed between February 2015 and January 2016. According to the survey, Malaysians (particularly millennials) will share passwords frequently. Millennials account for 26% of those who exchange passwords with others, followed by Generation X (17%) and baby boomers with just 8% [19]. Email passwords were the most commonly exchanged (59%), followed by social media passwords (49%), and bank account passwords (34%) [19]. Individuals may suffer negative effects as a result of such behaviors, such as identity theft, bank account theft, fraud, and others. Individuals who use passwords incorrectly may be the target of a password attack by hackers aiming to obtain your password. According to [20], one of the most common types of corporate and personal data breaches is password theft. As long as hackers recognise that many passwords are badly crafted, password attacks will continue to be employed as a means of attack. Consequently, it is critical to identify measures to prevent unsafe cyber hygiene practices. This is particularly relevant because the passwords on all "safe" Internet systems are a default authentication technique [18]. Besides, the researcher discovered that the majority of people are aware of what constitutes proper password management [21]. Despite being aware of security threats, it was revealed that people took risks because they were excessively thinking that bad things would never happen to them, they could not see any immediate negative effects, or the made a convenience trade-off with security [21]. Aside from these specific motivations, there may be personal characteristics that separate those who engage in risky cyber hygiene behavior. To date, the psychological literature has paid little attention to individual differences in bad cyber hygiene behavior [18]. Investigating who is more likely to engage in dangerous online hygiene practices can aid in reducing the risk of risky behavior. This information can be used to better target and identify those who are more likely to engage in risky behavior [18]. To address this problem, researcher will examine self-efficacy in information security to determine how self-efficacy will reflect Internet users practicing good cyber hygiene behavior. Identifying the people who have high self-efficacy in information systems can aid in the development of future efficient and successful cyber hygiene education programs. The reason researchers examine self-efficacy is because there has little research on how self-efficacy will affect cyber hygiene behavior. Most of the past research is doing their research on observing how individual differences like personality characteristics, self-monitoring, and demographic characteristics influence the behavior of cyber hygiene. So, in the current study, the researcher will have a deep investigation on does self-efficacy affects people's cyber hygiene behavior.

Secondly, end-users face high-security risks when getting into trouble due to a lack of cyber hygiene behavior and cyber hygiene awareness [15]. One of the most well-organized crimes of the twenty-first century is phishing [22]. Phishing is a type of malware or a term that describes when someone sends bogus emails to unwitting victims in order to obtain personal information [22]. According to [23], the attacker used the creation of a fake Facebook website phishing.php file as an example to create his own fake websites, which will collect all forms of data and index.html pages, the attacker can enter the Facebook page without logging in. Attackers will look for text actions in order to find the link. According to the author of the paper, the main reason for phishing has greatly affected the ability of entirely innocent people to access different secret information held by one person. One of the reasons for this situation is inducement of phishing. Phishing has spread widely with the increase of unsuspected people, who are vulnerable to attackers. Important information includes their card number, mother's name and other secret records. Attacker can obtain more information through phishing because public information is easy to retrieve. Therefore, it is very important that almost all ordinary users should be aware of phishing so that no one will be trapped by attackers [23].

Moreover, students nowadays are avid Internet users in search of information. The current generation of academics is an active Internet user. Students with a higher level of education are also more sensitive to cybersecurity dangers, since they rely on the Internet for the majority of their daily communication and educational activities [24]. Internet is very effective and popular tool used by students for various other purpose such as education and entertainment [25]. Students also use it to supplement their studies. According to [26], they claimed that most Internet users in Malaysia are aged between 15-32 years old, and further include those pursuing higher education in Malaysia. However, [27] report that young adults, aged between 18-24 are more susceptible to cybersecurity threatened. Because students tends to use a lot of Internet, so it is important to educate them on how to practice good cyber hygiene when online. According to [28], they stated that the leakage of confidential or sensitive information is the most common concern of educational institutions. According to [29], the common serious risk for all universities is data loss. Universities are public institutions that provide education, research, and knowledge exchange. Universities also process a lot of sensitive data at the same time, including student assessment data, diploma data, personal informaation, projects, contract information. copyrights, bank accounts, and so on. Many outsider and organizations may be interested in these information. This information is being utilized for nefarious purpose. Internal threats and multiple external threats are both possible [29]. Besides, most students make considerable use of digital technology, yet they are frequently unaware of the dangers to which they are exposed. In fact, while the Internet allows youngsters to engage, it also exposes them to a range of online hazards, including content risks such as pornograhic images, commercial risk such as abuse of personal information, and contact risk such as communicating with unknown individuals and cyberbullying [30]. According to [6], lack of cyber-hygiene awareness could jeopardize both the safety of students and the overall security of the educational system. A lack of cyber hygiene raises the possibility of a cyber-attack. Based on the research of [6], this problem need to be solved because education is one of the most vulnerable areas for cyber-attack, accounting for over 64% of all malware infections, demostrating the need for enhanced cyber-hygiene in the classroom. 30% of students were victims of phishing which is a type of cyber-attack in which cyber-criminals pose as legitimate firms in order to acquire information such as usernames and passwords. The dilemma is aggravated further by the pandemic’s abrupt shift to distant learning. As students increasingly use their PCs and insecure network to attend online classes, threat vectors in the education sector are growing too [6]. So, if the students do not grasp basic cyber hygiene behavior and connect to insecure networks, disclose passwords or usernames, or do not check people’s identities, they are vulnerable to a variety of threats [6]. Hence, the lack of cyber hygiene awareness among users has prompted the current study to be conducted among Malaysians to evaluate whether awareness of cyber hygiene will affect to their cyber hygiene behavior.

Additionally, lack of cyber hygiene behavior led to cyber threats and cyber-attacks [12] . For example, a cyber-attacks called WannaCry Ransomware was launched a large-scale attack on Microsoft Windows operating systems which include Windows 8, 2003 and XP users [12]. This problems occurred due to many users have not updated their software security version. Outdated software is more vulnerable to attacks and malicious software. It cannot protect businesses from the last threats if the software has not been updated for months [8]. Therefore, unlicensed Windows software makes systems with outdated software versions more vulnerable to this attack. According to [31], encryption ransomware and locker ransomware are the two types of ransomware. Encryption ransomware encrypts files and demands a ransom payment for file decryption, whereas Locker ransomware locks the victim out of the operating system and can prohibit access to the target desktop Ransomware, program malware, and files. In the last few years, in the healthcare sector had happened several cybersecurity incidents which including WannaCry ransomware [32]. This problem need to solve to avoid ransomware attacks to the users’ desktop, applications, and files. By practicing a good cyber hygiene, it can help people to know the types of ransomware along with some of the actions to overcome the attacks. This may help protecting themselves from becoming one of the victim of cyber-attacks.

Furthermore, users are lack of cyber hygiene knowledge about how to protect themselves from the cyber-attacks. According to [8], the common cyber hygiene problems are loss of data and misplaced data. It is vulnerable to hacker attacks when there is not back up or maintained for hard drives and online cloud storage. This might cause all the information loss when the cyberattacks come in. A poor cyber hygiene behavior may cause people lose their data in other ways. Information may not be destroyed or disappear forever, but because there are too many places to store data, misplaced files are becoming more and more common in modern enterprises [8]. According to [15], the end user is the weakest link in cybersecurity. End-users are the target of 95% of attacks in personal computing environments [15]. This can happen because the security personnel who are keeping the hardware and the software up to date cannot secure the personal computer devices. Good cyber hygiene can, however, encourage safe conduct and protect against attacks. If the users did not practice a good cyber hygiene bahavior, then their device software will be easily hack by attackers [12]. When an attacker gains device-level software access rights, it will perform many technical and fraudulent activities such as malware injection, denial of service, misidentification, privilege escalation to control the data present in the system [12]. In conclusion, most of the users do not know how to follow the best cyber hygiene practices and lack knowledge on what is cyber hygiene that can help them avoid cyber attacks. Users frequently lack knowledge of the procedures that must be performed to maintain cyber hygiene, which can result in inappropriate attitudes and behavior. So, we need to help users improve their cyber hygiene knowledge and behavioral attitude. In the current study, we will explore the cyber hygiene knowledge of Malaysians to observe whether users with a good knowledge of cyber hygiene will have appropriate cyber hygiene behavior in their daily life, which will help formulate a more effective cyber hygiene practices.

Lastly, many studies use cyber hygiene behavior theory to describe their framework, which leads to many various sources of elements that might contribute to cyber hygiene behavior, such as personal, social, technological, environmental, and so on. In other words, the lack of a clear image explains why attitudes and intention influence behavior. For an example, self-efficacy is proved to be a significant feature that may impact information security behavior. However, it was discovered that self-efficacy was not an essential factor in information security behavior in another study. As a result, researchers in this study will apply theory of planned behavior to explain the new framework and redefine previously assumed significant links.

1.3 Project Objectives

1.3.1 General Objectives

General objectives of this study is to identify the elements that influence cyber hygiene behavior in order to prevent cyber-attacks during COVID-19. In addition, the goal of this study was to investigate the relationship between variables and cyber hygiene behavior.

1.3.2 Specific Objectives

SO1: To investigate the relationship between self-efficacy and cyber hygiene attitude.

SO2: To investigate the relationship between cyber hygiene knowledge and cyber hygiene attitude.

SO3: To investigate the relationship between cyber hygiene awareness and cyber hygiene attitude.

SO4: To investigate the relationship between cyber hygiene attitude and cyber hygiene intention.

SO5: To investigate the relationship between cyber hygiene intention and cyber hygiene behavior.

1.4 Research Questions

These research questions was aimed to be answered by the present study:

1.4.1 General Questions

GQ1: What elements influence cyber hygiene behavior during COVID-19 in order to avoid cyber-attacks?

GQ2: What is the relationship between these elements and cyber hygiene behavior?

1.4.2 Specific Questions

SQ1: Is self-efficacy significantly explaining Internet users' cyber hygiene attitude?

SQ2: Is cyber hygiene knowledge significantly explaining Internet users' cyber hygiene attitude?

SQ3: Is cyber hygiene awareness significantly explaining Internet uses' cyber hygiene attitude?

SQ4: Is cyber hygiene attitude significantly explaining Internet users' cyber hygiene intention?

SQ5: Is cyber hygiene intention significantly explaining Internet users' cyber hygiene behavior?

1.5 Research Hypothesis

H1: Self-efficacy has a significant relationship with cyber hygiene attitude.

H2: Cyber hygiene knowledge has a significant relationship with cyber hygiene attitude.

H3: Cyber hygiene awareness has a significant relationship with cyber hygiene attitude.

H4: Cyber hygiene attitude has a significant relationship with cyber hygiene intention.

H5: Cyber hygiene intention has a significant relationship with cyber hygiene behavior.

1.6 Research Significance

Significance of the findings are revealed in this research, which aims to contribute to cyber hygiene behavior and various parties interested in the relevant literature area.

The goal of this research is to look at the elements that determine Malaysian Internet users' cyber hygiene behavior to avoid cyber-attacks during COVID-19. The use of Internet appears to be on the rise during COVID-19 pandemic, as evidenced by figures from [33]. When it comes to cyber world, many users lack of cyber hygiene behavior, as most studies have shown. By doing this research, Internet users will have better understanding of why they need engage in cyber hygiene behavior, as well as an opinion and perspective on the future of cyber hygiene. If Internet users have misconceptions about what cyber hygiene is, this research will assist them in changing their minds about what it is. However, the relationship between attitude-intention-behavior are still in the dark, thus the goal of this research was to determine the factors that led to cyber hygiene behavior and the relationship between attitude, intention, and behavior, so that they could better understand themselves in future.

This study will provide fresh insights on factors that influence cyber hygiene behavior in order to prevent cyber-attacks, particularly during the COVID-19 pandemic. Through this research, the community will further realize cyber hygiene behavior as a preventive measure against various cyber-attacks. This study provides a clear presentation of the cyber hygiene behavior, giving them insights into which factors have a significant relationship with cyber hygiene behavior. Besides, this study will provide related organizations or education an overview of what factor they need to take note in order to improve cyber hygiene behavior during COVID-19 to help Internet users avoid cyber-attacks. The findings of this study will provide more advice and tactics in cyber hygiene for the government, education, and small-and-medium businesses. It can assist them in communicating more effectively in order to ehance future cyber world and make recommendations based on the data gathered.

1.7 Conclusion

Chapter 1 has covered the aim of the study which provides a clear direction for the research's future progress. Besides, this chapter explores the definition of cyber hygiene as well as the understudied cyber hygiene problem statement. Researchers will discuss literature reviews in the following chapter. In the following chapter, the conceptual framework and variables are also defined.

Chapter 2

Literature Review

2.0 Introduction

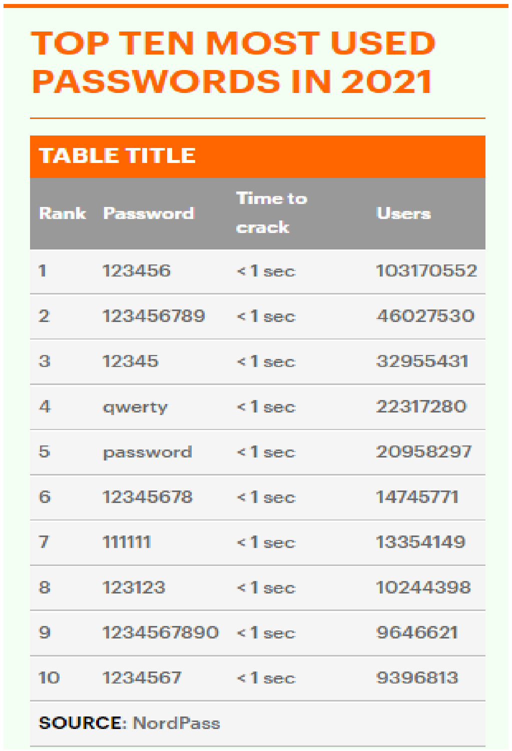
In this chapter, the researcher discusses and draws relationship between multiple variables related to the cyber hygiene behavior which including self-efficacy, cyber hygiene knowledge, cyber hygiene awareness, cyber hygiene attitude and cyber hygiene intention, by referring at literature and past study of other researchers. Based on the data gathered, a conceptual framework incorporating relevant theories and phenomena is created to aid in the formulation of methodological research designs.

2.1 Previous Findings on Cyber Hygiene Research

Through its Rangkaian Komputer Malaysia (Rangkom) project, the Malaysian Institute of Microelectronic Systems (MIMOS) introduced the Internet in Malaysia in 1987. RangKom is a pilot program that has successfully connected a number of Malaysian universities [34]. Rangkom became an Internet Service Provider (ISP) in 1991, serving a limited number of people. MIMOS founded JARING, Malaysia's first internet service provider, in 1992 [34]. Between October and November 1995, one out of every thousand Malaysians had Internet connection, equating to 20,000 Internet users out of a population of 20 million. The percentage of people who use the Internet climbed to 2.6 percent of the overall population in 1998. Since the year 2000, Malaysians have been using the internet at an increasing rate [34]. As there are many and many Internet users nowadays, and most of the users are lack cyber hygiene knowledge and awareness which will lead them to cyber-attacks. The goal of the previously identified cyber hygiene study is to understand the unique human variables that may affect cyber hygiene, as well as to provide a survey to explore end user's cyber hygiene habits in order to enhance their awareness of users and help design more effective practices.

Based on [17], authentication is one of the most important areas in cybersecurity. However, the security issues in textual password authentication are mostly caused by the limitations of human memory, human perception, and subsequent responses [17]. According to [35], in the past 40 years traditional textual passwords have been the most commonly used authentication method because it has many advantages such as easy to use, easy to implement and easy to remember. However, in the past decade, technological advancements and user error management practices have led to an increase in security vulnerabilities [35]. In fact, most people are be advised to use the strong password to protect their information and prevent from the cyber-attacks [17]. In order to increase the strength of the password when people creating a password, they are usually required to abide by a set of rules called password guidelines. Strong passwords are those that have at least eight characters. Upper and lower characters, numbers, and special characters should be included among these eight characters [15]. [17] pointed that the eight characters passwords should include at least one number or one upper case letter and should not contain any username in the password. Strong password practices are impractical because they are complicated and long alphanumeric passwords are unmemorable, and it is impossible for the human brain to remember many complex passwords that must be created for each account to avoid security failures [15]. Based on [36], password strength can only be estimated. The human brain tends to follow various patterns to help remember passwords, because human memory is mainly realized through associations. This brings a problem. If the passwords is difficult to remember, then people are likely to be written down in a piece of paper, this literally posing a security risk which anyone can use it [36]. Password misappropriation may also threaten other information systems [37]. This is because many people often reuse the same password, and this will make hackers more easily access other accounts. Other studies have shown that even if users know importance having good or wrong password practices, they still have little incentive to comply because they have few threats and do not want to feel inconvenienced [38]. Moreover, there are some methods are used to overcome the limitation of the solution in the research. Based on [17], these methods aim to guide user behavior by implementing strict passwords creation guidelines, active password checkers or password validity period to ensure a high level of security. Other than that, users tend to use the path of least resistance. In order to solve these limitations is through fear appeals [38]. Generally, fear appeals are persuasive messages designed to better help people realize the threat and persuade them to take proactive action. Fear appeals can be implemented to help increase users' awareness of the cost and dangers of reusing passwords [38].

According to [39], phrases such as "123456", "password", and "qwerty" still remain the world's most common passwords. NordPass recently released its annual report on the most widely used passwords, and the research showed that passwords vary significantly by different area and gender. Researcher also surveyed that many users still use their names, as well as vehicle brands, sports teams as their password. This study reveals that many people still do not comprehend the dangers of having weak passwords which will bring cyber-attacks to them. Based on the Figure 2.1 below, it is the table of top ten most used passwords in 2021 by people.



TOP TEN MOST USED PASSWORDS IN 2021

TABLE TITLE

Rank	Password	Time to crack	Users
1	123456	< 1 sec	103170552
2	123456789	< 1 sec	46027530
3	12345	< 1 sec	32955431
4	qwerty	< 1 sec	22317280
5	password	< 1 sec	20958297
6	12345678	< 1 sec	14745771
7	111111	< 1 sec	13354149
8	123123	< 1 sec	10244398
9	1234567890	< 1 sec	9646621
10	1234567	< 1 sec	9396813

SOURCE: NordPass

Figure 2. 1 Top Ten Most Used Passwords In 2021

From the Figure 2.1, we can see that "123456" ranked in number 1 which is the password that has been used most commonly in global and has 103170552 users using this as their password. The second most used password is "123456789" with 46027530 users and the third most used password is "12345" with 32955431. The phrases "password" and "qwerty" are also included in the top ten list of the most used passwords in the year 2021. Because there are some common qualities, hackers may be able to crack passwords by knowing someone’s location and gender. For example, based on the Figure 2.2, researchers noticed that women will used more positive and loving phrases such as “iloveyou” with 222,287 women use it compared to men. In other hand, men are more likely to create passwords that related to sports like “Hockey” which has been used by 26,055 men users.

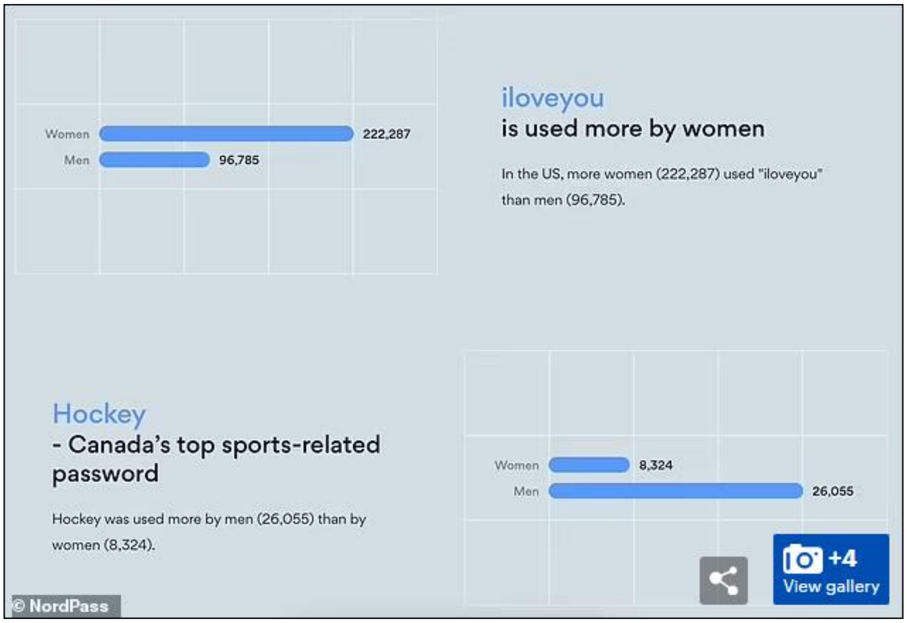


Figure 2. 2 Password That Women and Men More Likely to Use

NordPass CEO Jonas Karklys stated that passwords are becoming weaker and that individuals are not practicing basic password hygiene. He also said that as we spend more time online, it is critical to strengthen our cybersecurity and it is vital to recognize that passwords are the gateway to our digital life [39]. In the previous study, researchers advised people to use a password manager, which allows users to establish a unique password for each website they visit without having to remember any information. By using password manager, users do not have to remember the complex and long passwords they create. Other than using password manager, researchers also stated that to protect users from safe browsing , consumers must guarantee that their online accounts are secured with a difficult and long password that also serves as two-factor authentication [39].

Furthermore, the research show that many organizations are still using old systems such as Windows XP which has long since stopped supporting them and this allowing adversary to easily break through defenses [32]. Organizations have becoming attractive targets for cybercrime due to large amounts of valuable data and weak security [32]**.** Their weak security posture is mainly due to the lack of adequate network security budgets, which results in limited access to technology and expertise [32]. [40] said that in most Internet of Things (IoT) applications, the device may be left unattended and may be placed in a location that is easily accessible by attackers. This had increased the possibility for attacker to capture the device under the control of attacker such as modify the program or replace it with malicious device. With the increasing popularity of technology, the role of humans in basic security processes will continue to expand. [41] demonstrate that human users are the most effective link for identifying deception-based attacks such as application cloaking, spear-spoofing, and other types of semantic social engineering. Researchers have created a framework for human security sensors with practical implementation in the form of a Microsoft Windows prototype and reported a semantic social engineering attack against them [41]. According to their findings, the group has successfully identified an attack if a single user correctly detected the attack and could communicate internally. So, this had concluded that humans are no longer considered as threats in cybersecurity. They are an effective technique to limit the risk of persons contributing to e-health systems through training and awareness initiatives [42]. While training can assist lessen a person's risk, it is ineffective. There hasn't been enough research done on the effectiveness of various distribution techniques. A side-by-side evaluation of alternative information security awareness dissemination strategies is also absent. As a result, it is critical to comprehend the effective transfer of training throughout a business [42]. Moreover, [43] conducted the first effectiveness evaluation with the solution, Cyber Essentials, and found that its security control measures seem to be good mitigation of the threats designed for it. This result may also be applicable to other small and medium-sized enterprise programs that share/include the same security controls around the world.

2.2 Theory of Planned Behavior (TPB)

The Theory of Planned Behavior (TPB), a related conceptual framework, is the subject of this section.

According to [44], the theory of planned behavior seeks to describe and predict human behavior. It is an extension of rational action theory, which is crucial when dealin with people's incapacity to regulate their will due to the original model's flaws. The basic feature of the idea of planned conduct, like the original theory of rational action, is a person's desire to undertake a specified activity. The goal of this hypothesis is to identify the motivators that influence conduct. Motivators reveal how much effort people are willing to put in, as well as how much effort they intend to put in to complete the task. The greater the general purpose to undertake a specific action, the more probable it will carried out. It should be noted, however, that behavioral purpose can only be identified when the activity is under voluntary control [44].

Due to the limits of the original model in dealing with behaviour that people do not have complete control over, the theory of planned behaviour, an extension of the theory of rational action, became necessary. The hypothesis is depicted as a structural diagram in Figure 2.3. Potential feedback effects of conduct on antecedent variables are not specified for illustration reasons [45]. An important aspect of the notion of planned behavior is an individual's motivation to undertake a specific activity. A hypothetical purpose describes the motivations that drive activity by indicating how much effort someone is willing to try and how much work they intend to put in to attain that behavior. The stronger the desire to do something, the more likely it is to occur [45]. According to rational action theory, when the activity or scenario provides the person entire control over the performance of the behavior, intention alone is sufficient to anticipate behavior. Increased perceived behavioral control should become more effective as volitional control over conduct declines. Both intention and perception of behavioral control can play a role in behavioral prediction, however, one may be more relevant than the other in a given situation and only one of the two predictors may be required [45].

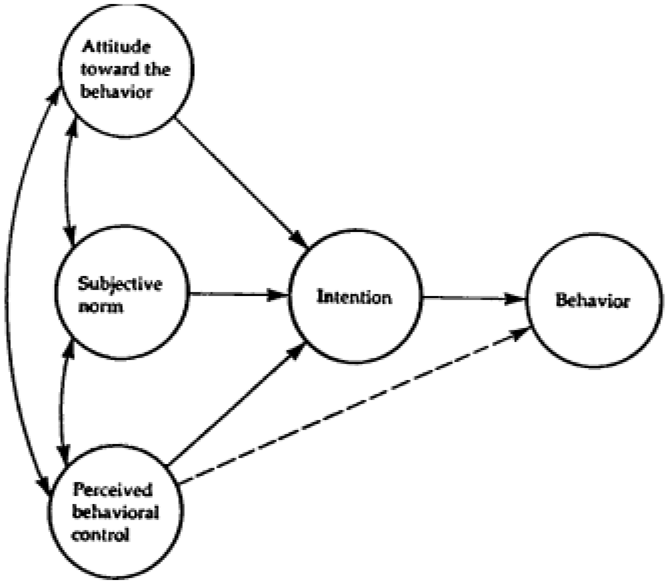


Figure 2. 3 Theory of Planned Behavior

According to [46], intention is regarded to be the immediate cause of action. Intent includes both the purpose and the likelihood of engaging in a behavior. The strength of this intention-behavior relationship is influenced by the degree to which intention and behavior measures coincide, the temporal stability of the intention, and the degree to which the conduct in question is premeditated. Planned behavior theory has been used to predict online safety behaviors in a few published research. Previously, researchers used the theory of planned behavior models to anticipate the intent to employ anti-spyware and other preventive steps to remove potentially harmful software ("malware"). The planned behavior model theory's findings support the expected association between attitudes and intentions [46].

Based on the work of [45], the theory of planned behaviour offers three fundamentally distinct intention drivers. The first is a person's attitude toward conduct, which is their judgement of whether a certain behaviour is good or bad. The second predictor is a social component known as the subjective norm, which refers to an individual's feeling of societal pressure to do or not do something. The third antecedent to intention is the degree of perceived behavioral control, which is related to the perceived ease of behavior execution and is considered to represent prior experience as well as projected challenges and obstructions. As a result, a theory of planned behavior may discover that in certain applications, the only attitude has a substantial effect on intention, in others, attitude plus perceived behavioral control are sufficient to explain intention, and in still others, all three predictors are significant [45].

The attitude toward the behavior is common to influence the intention. In this study, there will have 3 factors that will be used to help determine the relationship between attitude, intention, and behavior of cyber hygiene. Self-efficacy, cyber hygiene knowledge and cyber hygiene awareness can assist researcher to decide how people's attitude toward a particular thing, person or stituation.

2.3 Variables Review

2.3.1 Dependent Variable - Cyber Hygiene Behavior (CHB)

According to [47], it begins by noting that all behavior can be regarded as an individual's endeavor to cause a state of affairs. Cyber hygiene behavior is the behavior that individuals do on a daily basis to ensure the health and safety of devices, data, and networks. Recognizing the high cost of online injury, researchers are increasingly focusing on internet users' action and behaviors to keep their devices safe. Past cyber security behavior research has solely focused on extremely particular areas of cyber behavior. For example, researchers evaluated the level of safety compliance among 416 employees of four Malaysian companies [48]. According to the researchers, employees' loyalty to the organization had minimal influence on their attitudes toward desirable cybersecurity compliance actions.

Cyber hygiene is the proactive reduction of vulnerabilities in order to maintain system security. Cyber hygiene procedures include scanning computers for malware, updating, backing up data, and using secure passwords [49]. Cyber hygiene behavior is comparable to putting on armor before a battle. During combat, armor defends the body and minimized its vulnerability to attack. For examples, use of secure passwords, and software upgrades [49].

Previous research has discovered that the response rate to phishing spams is extremely high [15]. Phishing is a technique that designed to steal users' private personal information by disguising as a trusted source like website to the users [50]. According to [51], the payment services industry is the most popular target for phishers, accounting for 41.10 percent of all attacks in April 2011. The banking sector, the most well-known victim of phishing assaults, accounted for only 33.20 percent of all phishing attacks. A 6.50 percent pf phishing attack was launched against the auction sector. Other areas where phishing attacks were recorded included social networking, online gaming, online media, other internet corporations, and other organizations, which accounted for 14.20 percent of all reported phishing assaults. By analyze user behavior, it can defend the weakest links and detect counterfeit websites. According to [51], they have used novel paradigm analysis of user behavior to detect phishing sites. They had proved that this is an accurate method, discussed how to design and implement methods that are difficult to circumvent, and discussed its unique advantages in protecting users from phishing attacks. Image matching is a basic problem in computer vision [51]. Phishers are now responding by assembling phishing pages with non-HTML components, allowing existing system counterfeiters to create a phony page completely of graphics, even if the real page just contains textual content. Because their HTML code only comprises HTML img/> components, content-based anti-phishing program cannot assess suspicious pages in this situation [51]. This is the disadvantages of existing system because it cannot prevent phishing effectively, has low accuracy, high error rate. To overcome these limitations, [51] had proposes a phishing detection method based on the similarity between phishing and the appearance of real pages insteas of only doing text-based analysis. Take the first snapshot of suspicious webpage and compare it with the original webpage. Other than that, they also propose an image-based phishing detection schema which using color ratios and color modes to compare the images [51]. By comparing the results it can help users to identify phishing pages and original pages , so this can reduce the risk of phishing occurred toward people. Hence, there are some tips that can be used to prevent fraud. In this case, users should take it seriously to avoid situations such as throwing money to an unknown site or being arranged to engage in any fraudelent incident [23]. Users need to keep good cyber practices like keep the personal information confidential. Things like bank account numbers, phone numbers, addresses, and passwords. Other than that, researchers state that do not get lost in emails from unkown sites that ask for personal information and give you a strict deadline [23].

According to the research of [15], the research shows the broad and up-to-date research on conceptual cyber hygiene, threats and user behavior, covering safety software, phishing scams, identity verification, and social networking, Web Browsing, Wi-Fi host use, and USB drive utilization. In their study, they presented the latest data about user behavior and knowledge about password usage and phishing, as well as findings of how user variables such as gender, attack history, age, training, and expertise affect good or poor cyber hygiene. This research provides comprehensive data on end-user cyber hygiene in today's cyber threat world [15]. Furthermore, the researchers discovered that 81 percent of users received some form of safety training, which is higher than prior studies' findings of 43 percent of adults and 19 percent of college-age users. They believe that users have already received training in cyber hygiene. For example, the tutorials at work will have a better understanding of cyber hygiene. Researchers discovered that Internet users are not following good cyber hygiene practices when it comes to defending against phishing attacks or protecting their passwords. [15] stated that future research would concentrate on establishing more effective training programs as well as strategies to persuade younger users to act more securely while browsing the Internet. Aside from that, research has shown that when people receive more rewards for such actions, they are more likely to follow safe behaviors, however, when they pay more for the behaviors that follow safe behaviors, they are less likely to follow safe behaviors. As a result, [15] argue that future research should concentrate on how training may effectively explain advantages and costs. [52] pointed out that when users realized the consequences of unsafe behavior, their behavior will be more protective. [18] investigated the categories of persons who are more inclined to disclose passwords. According to the findings, young people were more eager to disclose passwords than older people. Younger folks may have more opportunities to exchange passwords than older adults because they have more online family and friends. According to the experts, educational programmes must target young people. Nonetheless, Internet illiteracy continues to be a major global issue. Organizations and educational institutions must first design adequate training programmes in order to compare and evaluate levels of awareness across various populations [48]. [52] had introduced a user behavior model that emphasizes factors related to users' perception of risk and choices based on that perception. Users may model their own behavior based on what they think other people do. The potential deterrent to dangerous behavior is that others may "blame" him or her for the problem caused, especially if one's behavior is much higher than the risk of others.

2.3.2 Independent Variable - Self-efficacy (SE)

Constant vigilance is essential for the ever-changing cybersecurity threat landscape [53]. One method for reducing consumers' potential sensitivity to cybersecurity threats is to develop a mechanism to identify the most and least vulnerable individuals. Users will be able to utilize this information to forecast the length and expens of increasing cybersecurity breaches. As a result, users must be able to quickly identify potential cybersecurity weaknesses using rigorous measures that can predict future performance. According to the past researchers, self-efficacy is a strong predictor of performance behavior. Valid self-efficay measures the best predict future performance have also been recommended to be adjusted to gauge areas of interest. According to [53], in order to improve someone's ability to protect themselve online, the trainer can maximize training efficiency by constantly modifying and comparing exact measures to establish which specific characteristics mak users more or less vulnerable to cybersecurity assaults.

People's belief in their ability to mobilize the motivation, cognitive resources, and action plans required to exercise control over a certain situation is known as self-efficacy [54]. People who have a high level of self-efficacy are more confident in their capacity to mobilize the motivation, action plans, and cognitive resources required to execute tasks successfully. People's motivation and conduct, as well as their level of effort, the commencement and persistence of coping efforts in the face of adversity, and self-regulation, are all influenced by their self-efficacy. People are more willing to participate in a specific activity if they believe they can succeed, according to [55]. Their views are inextricably linked to their self-esteem.

Self-efficacy is a significant component that influences personal information security practices, according to the majority of articles. They looked explored how self-efficacy affected a number of dependent variables, such as the motivation to implement information security, self-reported security behaviors, attitudes about information security policy, and the use of security software and features. For example, [54] discovered that students' self-efficacy had a significant impact on their desire to practice information security. End-user intentions to implement proposed personal computer security measures against malware are positively influenced by self-efficacy [54].

2.3.3 Independent Variable - Cyber Hygiene Knowledge (CHK)

Knowledge is defined as remembering specific and general themes, remembering structures, contexts, or patterns, or recalling processes or procedures. To take the appropriate action in a particular scenario, knowledge is essential. This includes understanding the potential impact and understanding what can be done to mitigate them [55]. Knowledge is a necessary precondition for adopting appropriate action in any given situation. In order to grasp cyber-attacks and the hazards associated with them, users must first understand cyberthreats and understand how to protect themselves from cyber-attacks [55].

Cyber hygiene knowledge refers to an individual’s knowledge about the cyber hygiene practices that can help them away from the cyber-attacks. There are still significant discrepancies between specialists and non-specialists when it comes to basic cyber hygiene such as upgrading software, backup software. Knowing more about cyber hygiene can have an impact on their attitude [18].

To create an effective cyber hygiene behavior on purpose, the user mush have knowledge. According to [53] research, users’ cyber security behavior increases as their level of cybersecurity education increases. It was revealed that users with good phishing threat avoidance knowledge avoided more phishing attempts, but users without such expertise avoided less phishing attempts. Furthermore, gaining a better grasp of the consequences of cyber attacks may lead to more cautious and conscientious online behavior [53]. To raise users' cyber hygiene behavior, they must first understand that cyber threats exist and these threats may be avoided. Users will not do proactive cyber security behavior to avoid cyber threats if they detect it but believe it cannot be averted.

Cyber security vulnerabilities are widely known, most people know that they are at risk of cyber-attacks, but they do not know how to practice a good cyber hygiene such as how to protect passwords. Individual variances exist in the cyber hygiene behaviors of users. Due to low cyber hygiene knowledge, most of end-users always post personal information on social networking sites which will cause their personal information been stolen and lead to cyber-attacks [15]. Based on the survey of [56], 59% and 62% of users are respond that they are releasing information regarding their real name and email address. About 45% of users had released their date of birth but along with their name. Personal data may be used in assaults in social engineering where fraudulent e-mails contain personal information to improve the likelihood of an answer [15]. The shortcomings of older users in adhering to normal standards, as well as their greater likelihood of exposing personal information such as passwords, may be attributed to the use of technology, as well as a lack of familiarity and understanding. In the research of [12] stated that they have research on a concept of "building cyber defense: a survey of leading cyber reference architectures and frameworks", and discussed the necessity of establishing agile structures in the field of cyber hygiene and cyber security to develop notification procedures. The fraudulent activities have made them aware of these attacks, so that they have enough time to reduce the impacts of the attacks [12]. According to [57]**,** although people are more aware of security breaches, but many of people do not take some basic cyber hygiene to protect their data. Only 56% of people use a password to safeguard their PCs, while only 45% use a PIN to secure their mobile devices. Nowadays, much of the existing cybersecurity knowledge tends to focus on defending the complex digital systems of large organizations. There is little attention to providing ordinary users with the in-depth knowledge and skills needed to protect their personal information or small business systems. According to [58], by practicing good cyber hygiene habits, it is necessary to combine knowledge with correct attitudes and mindful behaviors to protect valuable information and data in businesses and communities. Users frequently lack comprehension of the required cybersecurity measures, which may be the source of incorrect attitudes and behaviors [15].

2.3.4 Independent Variable - Cyber Hygiene Awareness (CHA)

The term awareness refers to users being aware of what is going on around them. According to [48], cybersecurity awareness is defined as the extent to which users understand the importance of information security, as well as their responsibilities and actions for implementing acceptable levels of information security controls to protect an organization's data and networks. The researchers attribute app usage and messaging on social media and internet pages to a general lack of knowledge of cyber hazards. They also emphasize that hackers attempt to prey on the most susceptible consumers, those who lack cybersecurity expertise and awareness [48]. Because the human component has been demonstrated to be the primary source of cyber breaches, academic instituions and commercial enterprises are increasingly offering cyber awareness training programmes focused on improving individual cybercrime knowledge [59]. However, raising awareness requires a thorough understanding of cyber awareness. As the world becomes more connected through the internet, programmes that enhance civic consciousness and the abilities of economic and public-sector actors will be the most successful in raising cyber expertise [48]. Such adjustments may be successful if the reasons for the lack of cybersecurity knowledge are identified. Nonetheless, a fundamentally global problem remains a lack of cyber awareness. Organizations and educational institutions must design relevant training programs to help improving users' awareness to cyber hygiene.

Furthermore, [24] urge that cybersecurity education should be included in Malaysian students' curricula so that they have the information to protect themselves from cyber-attacks. The researchers were unwavering in their belief that all Internet users must accept proper best practices. While improving cyber security may not eliminate the need for educational and training incidents, Internet users need to be aware and safeguarded to better understand these cyber threats [24]. For three reasons, the researchers believe the current study is crucial to understanding higher education students' cybersecurity behaviour: they are Malaysia's future workforce, they are the country's largest group of internet users, and the findings will define the next actions for all parties. are acceptable. According to the researcher, one of the many initiatives that concerned parties may do to safeguard these groups of individuals from emerging cybersecurity dangers is to provide necessary knowledge to improve students' understanding of such issues [24]. As a result, cyber security awareness training is critical for protecting Internet users from potential cybercrime and emerging cyber dangers [24]. [60] performed a field survey among 342 students in the accounting department of Universiti Teknologi MARA (UiTM) using a standardized questionnaire that contains demographic information as well as the seven most common cybercrimes. They discovered that female students are more aware and have affirmative insights than male students. They also discovered that students between the ages of 18 and 23 have poorer perception and awareness than those between the ages of 24 and above. The study provides empirical evidence of the necessity to enhance rules and processes for senior management of organizations to protect younger generations, hence lowering the high risk of becoming victims.

2.3.5 Independent Variable - Cyber Hygiene Attitude (CHAtt)

The term attitude refers to a person’s point of view, which may impact online behavior. These attitudes are formed as a result of a person’s learning experiences, observations, and social characteristics, all of which may impact how they choose specific events in their online activities [61]. The degree to which a person favorably or negatively assesses the behavior in question is referred to as attitude toward behavior [45]. Even if a person has a complete grasp of cyberattacks and cybersecurity controls, they must be able to explain the development of cyber hygiene behaviors. This is why, according to the behavioral literature, attitudes play a major role in explaining behavior [55].

Attitude or perceptions of things or people play a role in explaining behavior as well. Attitudes are classified into three types which are cognitive, behavioral, and affective [55]. A person’s intuition about something or someone forms the emotive component. Trait-based assessments are used to create cognitive components. The behavioral component is associated with attitudes impacted by previous activities and experiences. A behavioral component is not included because people’s attitudes are formed solely by their actions or experiences in certain situations. This only happens when individuals have a weak or ambiguous attitude, or when they are unable to explain their behavior in any other reasonable manner [55].

2.3.6 Independent Variable - Cyber Hygiene Intention (CHI)

The idea of intended behavior defines intention as an endeavor to attain a predetermined behavior rather than actual implementation [45]. Expected intentions have an impact on performance to the extent that a person has behavioral control, and when a person obtains behavioral control, their performance should improve, inspiring them to strive. Interaction theory has a minimal scientific basis, despite its intuitive appeal. According to [62], intention is intrinsic because it is the desire or goal to act in a specific way. While the goal is to stay in a place where the individual has not yet practised or translate their dreams into reality. Intent is defined by an individual’s attitude toward the behavior and personal sentiments. When given the opportunity to act, intention become acts [62].

2.4 Proposed Conceptual Framework

The conceptual framework of the current study is developed based on Theory of Planned Behavior (TPB). The framework includes independent variables which are self-efficacy, cyber hygiene knowledge, cyber hygiene awareness, cyber hygiene attitude, and cyber hygiene intention. The dependent variable for this framework is cyber hygiene behavior.

Figure 2.4 depicts a structure outlining the relationship between cyber hygiene behaviors and its determinants. The relationship is represented by the corresponding hypothesis.

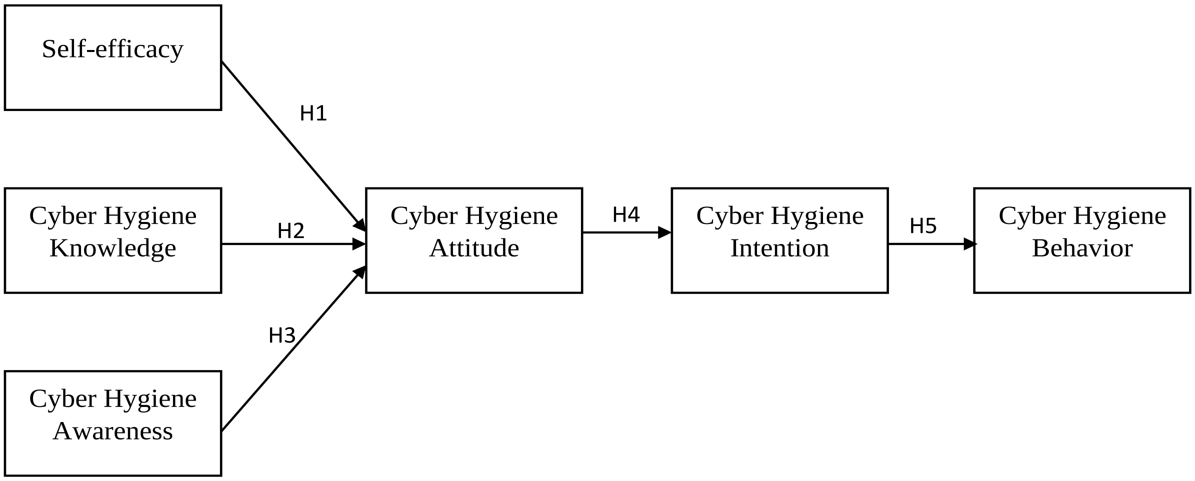


Figure 2. 4 Conceptual Framework

2.5 Hypothesis Development

2.5.1 Self-efficacy and Cyber Hygiene Attitude

In past research, researchers had tested that self-efficacy can be a strong predictor of performance behavior [53]. “When confronted with problems, persons who have substantial doubts about their own abilities relax their efforts or give up completely, whereas those who have a strong feeling of efficacy fight harder to meet challenges” [53]. Positive cyber security behavior has been connected to feelings of self-efficacy. According to [63], individual with higher information security self efficacy utilize more security protection software, and individuals with higher information security self-efficacy display more security-conscious care behaviors. They also discovered that self-efficacy in information security predicts the usage of cybersecurity programmes, tools, and upgrades. Most notably, high information security self-efficacy predicted the use of security software as well as security or internet use such as the use of multiple strong passwords and always backups of essential data [53]. So, researchers considered self-efficacy as important factors in this research model. In the current study, researchers will make a hypothesis as below to investigate whether users with high level of self-efficacy will change their attitude to practice good cyber hygiene behavior. So, the first hypothesis is:

H1: Self-efficacy has a significant relationship with cyber hygiene attitudes.

2.5.2 Cyber Hygiene Knowledge and Cyber Hygiene Attitude

The first step towards changing one’s behavior is to get knowledge. We do not simply need to inform. we also need to encourage people to change their attitudes [64]. Attitude can be influenced by behavior, and intention can be influenced by attitude. As a result, an individual’s perception, and consequently the acquisition of knowledge is influenced by their attitudes. The interaction of these three aspects: knowledge, attitude, and behavior is dynamic and reciprocal at times [64]. As a result, the second hypothesis is:

H2: Cyber hygiene knowledge has a significant relationship with cyber hygiene attitude.

2.5.3 Cyber Hygiene Awareness and Cyber Hygiene Attitude

According to [65], the researchers have done an essay with the topic of the erroneous reasoning at the heart of the conscious movement. The notion that changes awareness automatically result in changes in action. This premise is simply too concise and basic, given how illogical and baffling most people's behavior decisions are. Unsurprisingly, raising awareness is a component of the equation, but it is far from the only answer to major, widespread changes in attitudes and, crucially behavior. Moreover, [66] have investigated whether educating students about potential web hazards by directly learning about their behavior during online activities will result in greater privacy awareness and willingness to decrease their susceptibility to privacy threats. Researchers have noticed that students with limited technological expertise were generally unaware of privacy threats and has a sluggish attitude toward privacy protection. Individuals can effectively value their privacy and decrease their eposure while browsing the web by being aware of privacy dangers and change their attitude by learning how to control their personal information through the use of privacy-enhancing tools [66]. So, in the current study, researchers make a hypothesis as below to investigate whether users with high level of awareness will change their attitude to practice good cyber hygiene. Third hypothesis is:

H3: Cyber hygiene awareness has a significant relationship with cyber hygiene attitude.

2.5.4 Cyber Hygiene Attitude and Cyber Hygiene Intention

In the past research, researchers have conducted a survey with 30 organizations to examine a knowledge-sharing strategy. Researchers have drawn an result which attitude toward information sharing has a favorable and significant impact on behavioral intention [67]. According to [68], previous researchers developed a model that represents the factors that drive the adoption of home technology and concluded that attitude toward IT use and intention to use technology have a substantial link. Besides, another researchers identified a positive and significant connection between attitude and intention by looking at the interactions between website delay, the breadth of users' information search results, and familiarity [69]. A positive association was discovered between attitudes and behavioural intentions, according to [55]. This suggests that having a more positive mindset increases the likelihood of adopting cybersecurity practises. Therefore, forth hypothesis is:

H4: Cyber hygiene attitude has a significant relationship with cyber hygiene intention.

2.5.5 Cyber Hygiene Intention and Cyber Hygiene Behavior

Behavioral intents were chosen over self-reported behaviors since people may not be able to recollect their actions precisely. Actual cybersecurity activities do not match self-reported cybersecurity behaviors according to recent studies. The advantage of basing judgements on intention is that it lends itself well to questionnaires. This involves the adoption of measurements that allow participants to convey their level of commitment to a particular action. Early study also shows that behavioral purpose explains a significant portion of behavior with a 0.90 intent-behavior correlation. Behavioral intent is a strong predictor of actual conduct, according to other systematic literature research on cyber hygiene habits [55]. According to the theory of planned behavior, behavior is the combined consequence of intention and perceived behavioral control [45]. As a result, the last hypothesis for the current study is:

H5: Cyber hygiene intention has a significant relationship with cyber hygiene behavior.

2.6 Conclusion

The basic ideas and frameworks used to explain the link between dependent and independent variables are thoroughly clarified in this chapter. Besides, previous findings of cyber hygiene also included in this chapter. From this part, we have reviewed what the other researchers have done to solve the problem and what is the limitations of their solution. The next chapter will go through research methods.

Chapter 3
Research Methodology

3.0 Introduction

The methods used in this study will be discussed in this chapter. The research design and data collection methods will be described in this chapter too. In addition, survey instruments such as questionnaires and pilot tests, as well as sampling design processes such as target population, sampling methodologies, sampling scale, measurement methods, and techniques are built in this chapter. Data processing, data analysis tools are also covered in Chapter 3.

3.1 Design for the Research

A descriptive design and a quantitative research method were used in this study. By using quantitative approach, researchers able to describe the averages, correlations, and frequencies by measuring variables, hypotheses about variable relationships are put to the test, and using quantitative approach help researchers to see how effective new treatments, procedure, or items are [70]. Moreover, descriptive research focuses on describing the population, phenomenon, or circumstance under examination. It focuses on the how, when, what, and where of study issues as opposed to the why. This is because it is necessary to thoroughly appreciate the implications of research topic before delving into why it exists [71]. The type of descriptive research will be used in current study is correlative survey which are used to determine whether two variables are positively, negatively, or neutrally connected. This is true if two variables, such as X and Y are proportional, inversely proportional, or unrelated [71]. In the current study, researcher will do survey research. This is a common method of data collection in research design. In survey research, a researcher creates a survey or questionnaire and distribute it to respondents. It is commonly used to extract rapid data from primary sources as well as conduct rigorous quantitative and qualitative research [71]. As the COVID-19 pandemic worsens, researcher will use Google Forms to conduct an online survey to get responses from participants.

3.2 Data Collection Methods

According to [72], one of the most critical steps of research is data collection. Data collection is the systematic gathering and analysis of information on variables that allows people to answer specific research questions, test hypotheses, and evaluate results. All data collection attempts to collect high-quality evidence, which is then turned into rich data analysis, enabling the construction of convincing and trustwothy answers to the questions addressed. Data collecting is aa difficult process that takes careful planning, hard labor, endurance, patience, and so on in order to be completed properly [72].

The primary data source is the original data source from which the researcher gets data for a specific study goal or project [73]. Data can be gathered in a variety of ways. Interviews, self-administered surveys, experiments, and field observations are the most prevalent methodologies. Primary data collection is both costly and time-consuming when compared to secondary data collecting. However, raw data collecting may be the only option for other types of research. In this study, researcher will distribute the questionnaires to collect the primary data. Researcher prepared a self-administered surveys with closed-ended questions and distribute it to participants via online. Questionnaires allow reseachers to obtain the most up-to-date information and responses in a short amount of time.

The secondary data is any dataset not obtained by the author, or more precisely “it is an analysis of data collected by others” [74]. Ancillary data could contain preciously gathered data that is being examined for re-use for new inquiries for which it was not initially collected. Academic books, journals, online information databases for articles, and textbooks are the sources of secondary data [75]. According to [76], this could be a time and cost-saving strategy because ealier data has been established and the researcher can simply apply the results and data. As a result, data cleaning, data processing, and other operations can be eliminated because they use genuine data from the present study. In current study, researcher utilize the online article and journal such as Journal of Information Security as secondary data. The majority of the research was sourced from Science Direct, Research Gate, and Scopus. These data were mostly gathered via Internet seaarch engines which include Elsevier, Google Scholar, and UTAR library online databases for information compatibility.

3.3 Design of the Sampling

3.3.1 Target Population

The intervention's target population will be the groups that will be researched and conclusions are taken. The target population was defined as the group of people who were deemed eligible to participate in the study's data analysis [62]. Target population for this research is students from Universiti Tunku Abdul Rahman (UTAR), Malaysia. This university was chosen because of its cost-effectiveness, closeness, and availability of study subjects. The reasons researchers choose students as target population is because students are also considered as one of the heavy Internet users during COVID-19.

Some previous studies have specifically targeted university students as a target group, such as study about different disciplines require varying levels of cyber knowledge [48], age and level education on cyber hygiene culture [77].

A sampling frame is a list of real people from whom samples can be drawn [78]. A sampling frame is a list or directory of respondents who have been chosen for a sample and who have specific information about themselves [62]. So, there was no sampling frame available because the target demographic was students who will practice cyber hygiene behavior in their daily life.

3.3.2 Sampling Technique

Because no sampling frame was available for this study, a non-probability sampling approach was used. In this study, convenience sampling was used. Convenience sampling is a non-probability sampling method that is often employed in survey sample selection. This sampling approach is low-cost, quick, and simple to use [77]. When using convenience sampling, researchers look for persons who have spare time and are willing to complete the questionnaire. Because the researchers need to collect data over a long period of time and have not yet gotten financing for the project, they are employing this technique. As a result, researchers will disseminate online surveys via Google Forms, with links to the forms sent to specified groups or meeting platforms. People can complete the questionnaire in their spare time, based on their willingness to assist. This allows Internet users to readily contribute information, making the data collection process more efficient and productive.

3.3.3 Sample Size

The total number of people who will be polled from the study's target demographic is referred to as the sample size. At least five times the number of variables evaluated should be observed [79]. As a result of the calculation formula used in this study [80] , the calculated sample size is as follows:

The smallest sample size = Number of indicators x 5

There were a total of 160 respondents (32 x 5)

As a result, at least 160 respondents were needed for this investigation.

3.4 Instruments

3.4.1 Survey Design

A questionnaire that is well-structured has questions that are easy to understand. This type of questionnaire is beneficial in research since it aids in data collection. A self-administered questionnaire is used in this investigation. A 5-point Likert scale is used to answer the questionnaire, which includes some fixed items. As a result, responders can select their responses fast and directly. It also saves time for respondents and leads to solid conclusions.

This study's questionnaire is divided into seven sections: A, B, C, D, E, F, and G. On the cover, there is an introduction, a study purpose, a research topic, and some private and personal information about the respondents. Part A of the survey includes demographic information such as gender, age, and educational level, as well as some general questions to learn more about the respondents' demographics. Parts B, C, D, E, and F, respectively, inquire about respondents' opinions on independent factors such as self-efficacy, online hygiene knowledge, awareness, attitude toward internet hygiene, and readiness to practice internet hygiene. Influence people's online hygiene habits. To further grasp respondents' perspectives and thoughts on the topic, statements concerning cyber hygiene activities are listed in Section G.

3.4.2 Pilot Test

According to [81], a pilot study is defined as a small study designed to test research methods, sample recruitment strategies, data collection instruments, and other research techniques in advance of a larger study. A pilot study is one of the most significant stages of a research project, and it used to discover potential issue areas and flaws in research tools and methods before they are implemented in a larger study. It also assits members of the research team in familiarizing themselves with the protocol’s procedures and in deciding between two competing research methodologies, such as employing interviews rather than self-administered questionnaires.

Following the completion of the pre-test questionnaire, the pilot study was conducted online. Google Forms have been shared on social media sites like Facebook and Instagram and will be distributed via Microsoft Teams, allowing researchers to reach a large number of UTAR students quickly. The Internet has made it possible to collect data online in a more powerful, effective manner, and time-saving [82]. Besides, online data collection refers to information obtained through sending emails, text messages, and other electronic messages. Respondents have enough time to complete the questionnaire or survey when data is collected online. As a result, the data acquired is usually more accurate [82]. According to [83], internal pilot research with a sample size of 10% is appropriate. As a consequence, a total of 30 responses were collected, with no comments from respondents. This demonstrates that the responders can understand all of the questions in the questionnaire.

After that, the researchers used the SmartPLS 3.3 analytic tool to conduct reliability tests on the measurement items used in the study to determine their stability and internal consistency. The Cronbach’s alpha value and composite reliability is used to calculate it. The levels of composite realibility of 0.7 and higher are generally regarded as acceptable [84]. Moreover, Cronbach’s alpha is a statistic that is widely used by researchers to illustrate the tests and scales produced or utilized for research projects are appropriate for their intended purpose [85]. Cronbach's alpha should be between 0 and 1.00, according to [86] , and items with values close to 1.00 are thought to have excellent internal consistency. Results from standardized tests should be greater than 0.80 or 0.85; anything less than 0.7 is considered inadequate. In addition, the convergence efficacy of each latent variable was assessed using average variance extraction (AVE) [87]. According to [88], The researchers indicated that the AVE should be more than 0.5 in an acceptable model to reflect the convergent validity of a certain construct.

Cronbach's alpha, composite reliability, and average variance extraction (AVE) values obtained from the pilot test are shown in Table 3.1. Cronbach's alpha values range from

0.77 to 0.95, composite reliability ranges from 0.80 to 0.95, and AVE ranges from 0.5 to 0.80. As a result, the survey is trustworthy, with strong internal consistency and convergent validity.

Table 3. 1 Reliability and Convergent Validity Analysis for Pilot Test

Variable’s name	Number of items	Cronbach’s Alpha	Composite Reliability	Average Variance Exxtracted (AVE)
Self-efficacy	4	0.777	0.844	0.577
Cyber Hygiene Knowledge	5	0.948	0.959	0.797
Cyber Hygiene Awareness	6	0.813	0.879	0.594
Cyber Hygiene Attitude	6	0.907	0.930	0.696
Cyber Hygiene Intention	5	0.904	0.931	0.734
Cyber Hygiene Behavior	5	0.817	0.872	0.593

3.4.3 Fieldwork

The online survey, which was conducted using Google Forms, had received 160 replies from respondents. Google Forms is preferred by researchers since it is free and does not require any technical skills. At the same time, it is a helpful tool for creating data automatically, which helps to remove human and human error.

Furthermore, social media platforms such as Instagram, WeChat, and WhatsApp are utilized to disseminate information about Google Forms links. The survey was distributed to various groups that include UTAR students. Besides, the Microsoft Team platform has also been used for collecting the responses. This is because Microsoft Team is the main online teaching platform for UTAR students, so researchers are able to approach the UTAR students easier. With just a few taps on their phone screen, respondents can engage in the survey at any time and from anywhere.

To ensure the data collected is correct, the questionnaire structure must be simple and comprehensive. As a result, simple and unambiguous questions in English were created to make the questions easier to understand by respondents. Respondents can contact the researcher if they have any concerns because the researcher's contact information is included in the questionnaire. This is to guarantee that respondents comprehend everything and can respond without hesitation.

3.5 Constructive Measurements

3.5.1 Scale Measurement

The four most regularly utilized scales in the study are ordinal scales, ratio scales, nominal scales, and interval scales. In this study, the researchers employed three types of measures: 5-point Likert scales, ordinal scales, and nominal scales. Nominal scales are scales that cannot be numbered but must be included in the classification. An ordinal scale, on the other hand, is a measure that arranges data in ascending or descending order. So, in Part A, nominal scales for gender are utilized, while ordinal scales for age and education level are employed. All questions in Parts B, C, D, E, and F are answered on a 5-point Likert scale: strongly disagree, disagree, neutral, agree, and strongly agree. On a scale of 1 to 5, respondents could assess their agreement or disagreement with each statement using the Likert scale. Statements for cyber hygiene behavior, on the other hand, were graded as follows: 1-never, 2-rarely, 3-sometimes, 4-very often, and 5-always.

Table 3. 2 5-Point Likert Scale Measurement (Agreement and Disagreement)

Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
1	2	3	4	5

Table 3. 3 5-Point Likert Scale Measurement (Behavior)

Never	Rarely	Sometimes	Very Often	Always
1	2	3	4	5

3.5.2 Origin of Construct

The following literature has been adapted from several measurement structures:

Table 3. 4 Origin of Construct

Construct	Source
Self-efficacy	He et al. (2014) Rhee et al. (2009)
Cyber Hygiene Knowledge	Pew Research Gate (2017)
Cyber Hygiene Awareness	Zwilling, et al. (2020) Aljohani & Elfadil (2020) Alharbi & Tassaddiq (2021)
Cyber Hygiene Attitude	Kok, et al. (2020) Alharbi & Tassaddiq (2021)
Cyber Hygiene Intention	Alharbi & Tassaddiq (2021)
Cyber Hygiene Behavior	Cain, et al. (2018) Talib, et al. (2014)

3.5.3 Operational Definition

The numerous indicators for each structure that have been applied to the questionnaire are shown in Table 3.5.

Table 3. 5 Operational Definition

Independent Variables	**Questions**
Self-efficacy	• I feel confident managing files in my computer. • I feel confident learning advanced skills to protect my information and information system. • I am able to use anti-virus software without much effort. • I set up password on my phone.
Cyber Hygiene Knowledge	• Installing anti-virus software can prevent yourself from "phishing" attack. • Password with minimum 8 characters including upper and lower characters, numbers, and special characters is considered as strong and secure password. • Using the URL that starts with "https://" is more secure than using the URL "http://" (without "s"). • Password "WTh!5Z" is more secure to password "123456". • It is generally not safe to use the public Wi-Fi network (such as in an airport or café) for sensitive activities such as online banking. • Using a virtual private network (VPN) minimizes the risk of using an unsecured Wi-Fi network.
Cyber Hygiene Awareness	• I read the user agreements for free program/software before clicking "I accept".

	• All my passwords include minimum 8 characters including upper and lower characters, numbers, and special characters. • I regularly check the browser history and find suspicious activities. • I use two-factor authentication when possible. • I use multiple passwords for everything that needs a password.
Cyber Hygiene Attitude	• It is annoying to have different complex password for different accounts. • It is hard to remember the different passwords for every different accounts. • I believe only public accounts are targeted by hackers and cybercriminals. • I feel that only simple and easy to guess passwords are at risk of being victims of cybercrime. • My first impression when checking if a website address is secure by seeing if it contains "https://" and/or showing a padlock is positive. • Locking a device when I am no longer using it is something I find useful and easy.

Cyber Hygiene Intention	• I intend to set a long and strong password. • I will be going to keep my computer and phone locked with a pin, or a password longer than 6 numbers. • I will be going to change my password periodically and use a different passwords for each of the accounts. • I intend to participate in the training class about cyber hygiene in the future. • I will sign out the accounts when away from the computer or device.
Dependent Variables	**Questions**
Cyber Hygiene Behavior	• I use the same password for multiple account. • I set my passwords with minimum 8 characters including upper and lower characters, numbers, and special characters. • I share personal information on social media. • I performed an anti-virus scan regularly. • I back up my important files every time.

3.6 Data Processing

The collecting and translation of datasets into relevant, useable information is known as data processing in research. It guarantees that the raw data is relevant and helpful to the study.

3.6.1 Questionnaire Check

Questionnaire checking aids researcher in avoiding spelling errors, misspellings, and questionnaire misconceptions [76]. Respondents were asked a simple and understandable questions as part of the procedure. As a result, as soon as the data was returned, the researchers double-checked the questionnaires. Researchers can learn about faults and blunders this way and avoid them during the data collection procedure.

3.6.2 Editing of Data

Data editing aids in the correction of issues discovered earlier in data inspections by altering data inspections to improve the readability of the results before they are registered into the system [76]. Researchers can take action at this point if they receive questionnaires that are incomplete or inconsistent. In order to increase the data’s dependability and authenticity, researchers must eliminate survey sets filled out by respondents that contain inaccuracies. In the current study, the researcher employed an online questionnaire and specified certain parameters to allow respondents to skip any questions before continuing, eliminating invalid responses.

3.6.3 Encoding of Data

Data encoding is the process of converting linguistic data into variables and categories so that it may be fed into a computer for analysis. Researchers will be able to conduct

SmartPLS more readily and simply after completing this step. In this study, the researchers assigned male respondents a score of 1 and female respondents a score of 2. In addition, for Sections B, C, D, E, and F, researchers assigned a score of 1 to Strongly Disagree, 2 to Disagree, 3 to Neutral, 4 to Agree, and 5 to Strongly Agree. In section G, the researcher will Never be 1, Rarely be 2, Sometimes be 3, Very Often be 4, and Always be 5.

3.6.4 Transcription of Data

The transcribing process begins once the data has been encoded. This may be accomplished using software that delivers and transcribes the encoded data in the questionnaire's opening sentence into several results [89]. To convey encoded data straight from the questionnaire to the system, the researchers employed a keyboard technique. The system can automatically execute the data after it has been recorded.

3.6.5 Cleansing of Data

The process of discovering, assessing, and resolving missing replies is known as data cleansing [89]. SmartPLS will allow researchers to detect incorrect figures supplied by each respondent. As a result, researchers must reverse the process and go back in time to find survey editing and coding issues. Because if there is no value, the researcher will come to an ambiguous or doubtful conclusion. If the value is still ambiguous after investigation, the investigator can use list deletion of neutral values or pairwise deletion to skip the treatment. The researchers in this study employed neutral values as a remedy for omissions.

3.7 Data Analysis Tool

3.7.1 Structural Equation Modeling (SEM)

Structural equation modelling (SEM) is a strong multivariate approach for testing and evaluating multivariate causal links in scientific research. Because SEMs test for direct and indirect effects on pre-assumed causal links, they differ from other modelling methods [90]. Models can be tested using either variance-based or covariance-based approaches, and there are two types of SEM. The Partial Least Squares SEM (PLS-SEM) method, also known as variance-based SEM (VB-SEM), allows users to approximate complex models with a high number of constructs, indicator variables, and structural paths. Furthermore, covariance-based SEM (CB-SEM) is frequently employed to support or disprove a notion. CB-SEM is an approach that uses a maximum likelihood (ML) estimate procedure to reproduce the covariance matrix without the focus on explained variance like PLS-SEM does. When the subject lacks a solid theoretical framework, especially when there is minimal prior knowledge of causation, PLS-SEM is the method of choice [90]. The emphasis is on discovery rather than confirmation in this case. So, PLS-SEM will be used in this study.

3.7.2 SmartPLS Version 3.3

In this study, researcher use the SmartPLS version 3.3 to help analyze the data. SmartPLS is a turning point in latent variable modelling. By using SmartPLS, researcher able to get deep insights into the data easily. Researcher can develop a path model in minutes due to the powerful modelling environment. Path models such as PLS-SEM can be employed instead of covariance-based structural equation modelling (SEM). SmartPLS' flexibility, which is unrestricted by rules and regulations, allows researchers to investigate causal mechanisms utilizing undistributed data [91]. Only a small sample size and the residual distribution are required for PLS-SEM. As a result, for the PLS-SEM technique, which uses tiny sample sizes, SmartPLS is the optimum statistical tool. SmartPLS appears to be the greatest choice for this inquiry because both situations qualify as PLS-SEM.

3.7.3 Analysis for the Descriptive

Descriptive analysis is the practice of employing tools like tables, bar charts, pie charts, and graphs to describe demographic data from respondents in a study [92]. This study allows researchers to get a more complete picture of demographics and have a better understanding of respondents. Section A is made up of 5 questions, all of which are presented in a pie chart since it is more intuitive and easier to understand, and the proportions of each part are mentioned explicitly.

By classifying data and noting how many data points exist in each class, frequency distribution summarizes and compresses it. According to [93], a frequency distribution is a table that shows how frequently each variable value appears in a set of scores. Frequency distributions are usually expressed as percentages. The frequency distribution table in Section A clearly displays the highest frequencies of outcomes often used to represent demographic data.

3.7.4 Indicator Validity

3.7.4.1 Outer Loadings

The significance of each item or variable in a PLS analysis is determined using outer loading in the reflection measurement model. Outer loadings of 0.7 or above were deemed to be extremely satisfactory [94]. Manifest variables with a load value of less than 0.5 should be eliminated, even though a load value of 0.5 is deemed acceptable [95].

3.7.5 Internal Consistency Reliability

3.7.5.1 Cronbach’s Alpha Reliability

To guarantee that each question in each independent variable was reliable and valid, the researchers conducted reliability tests. Cronbach's alpha rule is used to determine it.

Cronbach's alpha is a measure of a variable's dependability. The higher the value, the more reliable the variable [96]. The question is regarded as genuine and real when the reliability score is greater than 0.7. The link strength for various degrees of alpha coefficient values is shown in Table 3.6.

Table 3. 6 Cronbach's Alpha Power Association

Alpha Coefficient	**Power of Association**
$\alpha \geq 0.9$	Very Good
$0.8 \leq \alpha < 0.9$	Good
$0.7 \leq \alpha < 0.8$	Acceptable
$0.6 \leq \alpha < 0.7$	Questionable
$0.5 \leq \alpha < 0.6$	Poor
$\alpha < 0.5$	Unacceptable

3.7.5.2 Composite Reliability

Composite reliability is calculated by adding all of the actual score variances and covariances in the composite of construct-related indicator variables and dividing the total variance in the composite. Composite reliability is also a dependability indicator which consider the items' varied factor loadings. The levels of composite reliability of 0.7 and higher are generally regarded as acceptable [84]. However, composite reliability is seen to be a better indicator of internal consistency than Cronbach's alpha since it considers standardized variable loadings [68].

3.7.6 Convergent Validity

3.7.6.1 Average Variance Extracted (AVE)

The Average Variance Extracted (AVE) of each latent variable is determined to determine convergent validity [87]. According to [88], researcher stated that AVE should be more than 0.5 in an acceptable model to reflect the convergent validity of a specific construct. In a reflective model, AVE represents the average commonality for each latent variables. The AVE should also be bigger than the cross-loadings, implying that the factors should explain at least half of the variance in their respective indicators. When the AVE is less than 0.5, it signifies that the error variance exceeds the explained variance [88]. According to [97], AVE 0.4 is acceptable too. Because if the AVE is less than 0.5 but the composite reliability is greater than 0.6, the construct's convergent validity is still sufficient.

3.7.7 Discriminant Validity Test

3.7.7.1 Fornell-Larcker Criterion

The four-step in reflective measurement model assessment is to assess discriminant validity which how distinct a construct is experimentally from other components in the structural model. [97] provided the standard metric and advocated comparing the AVE of each construct to the square inter-construct correlation of that same construct and all other reflectively assessed constructs in the structural model [98]. The shared variances of all model constructs should not be larger than their AVEs. According to [88], the square toot of the AVE of each construct should be greater than the construct's highest correlation with every other construct in the model. As a way of measuring discriminant validity for reflective models, cross-loadings, the outer loading of each indicator on a construct should be greater than the sum of all its cross-loadings with other constructs [88].

3.7.8 Structural Model Measurement

To discover multicollinearity concerns, variance inflation factors (VIF), and path coefficients, the model uses a path model technique. As long as the VIF score is greater than 10 (considered detrimental), any multicollinearity problem can be found. In addition, path coefficients based on the t-statistics, and R-squared are assumed. P-values less than 0.05, t-statistics greater than 1.96, and R-squared values of 0.25 (low), 0.50 (mid), and 0.7 (high) are all acceptable.

3.8 Project Timeline

The completion of each task in a project is represented by a timeline in Gantt charts. These timelines demonstrate how tasks are related to one another. Gantt charts are important because they show the activities and progress of a project [99]. The work on a job cannot begin until the linked task is done. Researchers may use this data to better identify project barriers and make key decisions about how to proceed.

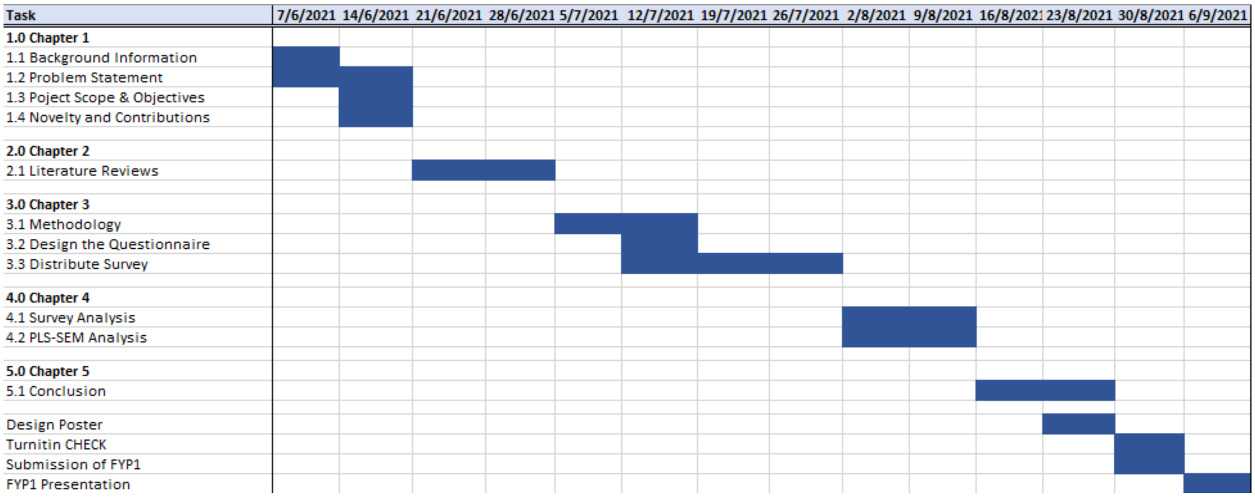
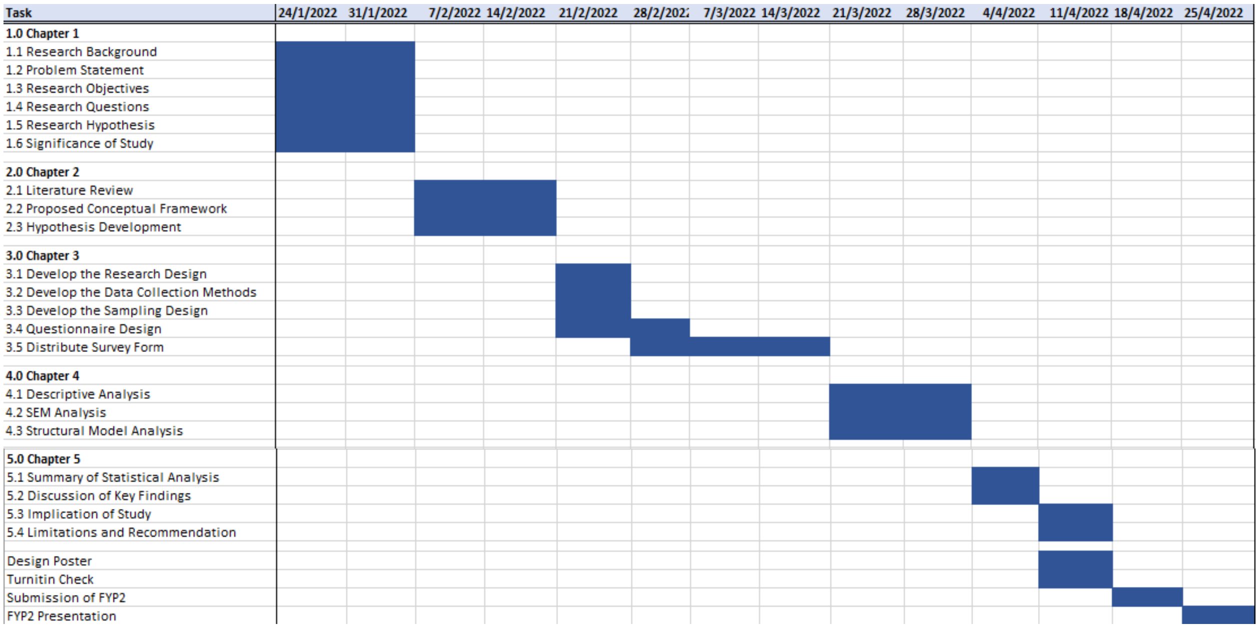


Figure 3. 1 Gantt Chart for FYP1



Task	24/1/2022	31/1/2022	7/2/2022	14/2/2022	21/2/2022	28/2/202	7/3/2022	14/3/2022	21/3/2022	28/3/2022	4/4/2022	11/4/2022	18/4/2022	25/4/2022
1.0 Chapter 1														
1.1 Research Background	■	■												
1.2 Problem Statement	■	■												
1.3 Research Objectives	■	■												
1.4 Research Questions	■	■												
1.5 Research Hypothesis	■	■												
1.6 Significance of Study	■	■												
2.0 Chapter 2														
2.1 Literature Review			■	■										
2.2 Proposed Conceptual Framework			■	■										
2.3 Hypothesis Development			■	■										
3.0 Chapter 3														
3.1 Develop the Research Design					■									
3.2 Develop the Data Collection Methods					■									
3.3 Develop the Sampling Design					■									
3.4 Questionnaire Design					■	■								
3.5 Distribute Survey Form						■	■	■						
4.0 Chapter 4														
4.1 Descriptive Analysis									■	■				
4.2 SEM Analysis									■	■				
4.3 Structural Model Analysis									■	■				
5.0 Chapter 5														
5.1 Summary of Statistical Analysis											■			
5.2 Discussion of Key Findings											■			
5.3 Implication of Study												■		
5.4 Limitations and Recommendation												■		
Design Poster												■		
Turnitin Check												■		
Submission of FYP2													■	
FYP2 Presentation														■

Figure 3. 2 Gantt Chart for FYP2

3.9 Conclusion

In conclusion, the method for performing the study is discussed in Chapter 3. The research design describes quantitative and descriptive investigations. It also outlines the data collection methodologies and sample design procedure, as well as the instruments for performing research and data processing. Descriptive analysis, internal consistency reliability, convergent validity, discriminant validity test, and structural model measurement were used as analytical tools. The findings of the statistical analysis will be shown in the following chapter.

Chapter 4
Data Analysis

4.0 Introduction

The results of the analysis received from the respondents are discussed in Chapter 4. Demographic data will be described using descriptive and frequency analyses, while the research question's aims will be discussed in this chapter. The SmartPLS software is the principal instrument for data analysis.

4.1 Descriptive Analysis

4.1.1 Demographic Analysis

Each respondents was asked five demographic questions in the survey, including their age, gender, level of education, primary use of the Internet, and experience on cyber-attacks. Based on frequency analysis, this section gives a demographic analysis of respondents.

4.1.1.1 Age

Table 4. 1 Respondent's age

	Frequency (f)	Percentage (%)	Cumulative Percentage (%)
18 - 28 years old	160	100.0	100
29 - 39 years old	0	0	0
40 and above years old	0	0	0
Total	**160**	**100.0**	

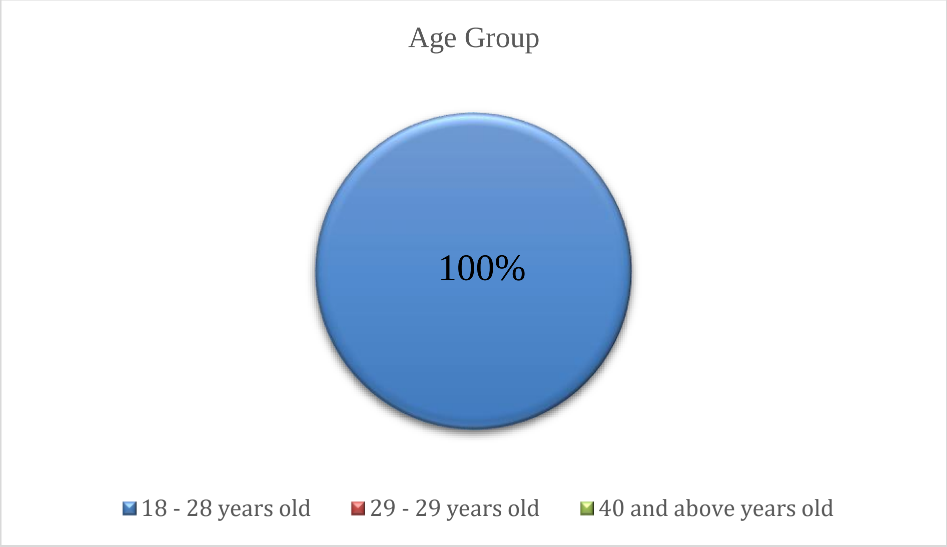


Figure 4. 1 Respondent's age

The respondents' age are shown in Table 4.1 and Figure 4.1. All the respondents were between the ages of 18 and 28 years old, accounting for 100% of the total (160). The majority of the respondents were between the ages of 18 and 28 years old, which is the typical age range for youthful internet users.

4.1.1.2 Gender

Table 4. 2 Respondent's gender

	Frequency (f)	Percentage (%)	Cumulative Percentage (%)
Male	73	45.6	45.6
Female	87	54.4	100.0
Total	**160**	**100.0**	

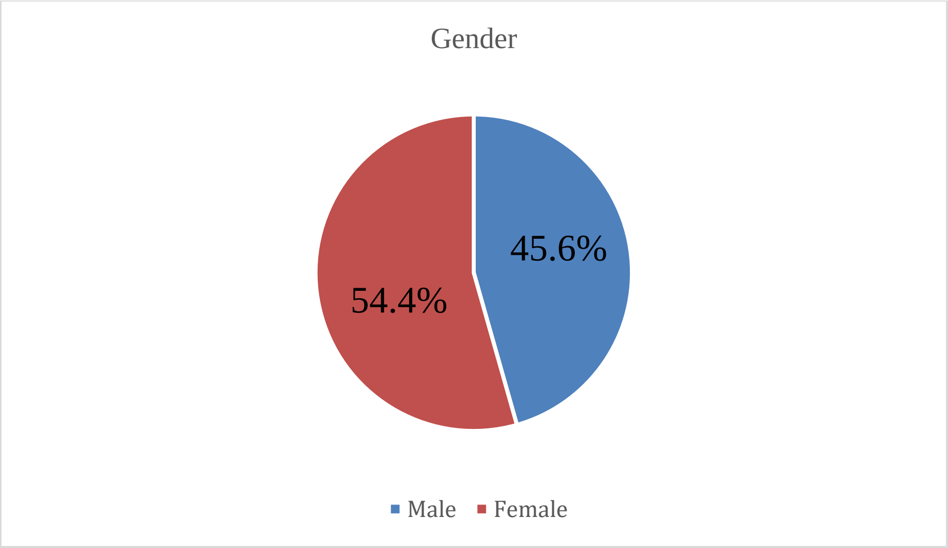


Figure 4. 2 Respondent's gender

The majority of respondents (54.4%) were female, while 45.6% were male, as shown in Table 4.2 and Figure 4.2. That is, 87 females and 73 males were among the 160 people who responded.

4.1.1.3 Education Level

Table 4. 3 Respondent's education level

	Frequency (f)	Percentage (%)	Cumulative Percentage (%)
Secondary School	0	0	0
STPM	0	0	0
Foundation/Diploma	82	51.2	51.2
Bachelor's Degree	78	48.8	100.0
Master	0	0	100.0
PhD	0	0	100.0
Total	**160**	**100.0**	

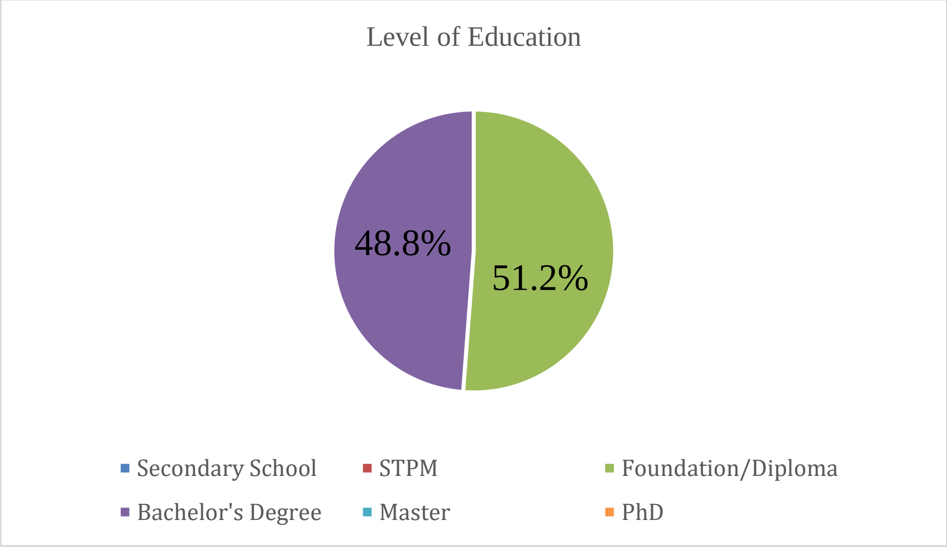


Figure 4. 3 Respondent’s education level

The respondents' educational levels are shown in Table 4.3 and Figure 4.3. The biggest percentage of respondents (51.2% or 82 respondents) had a foundation or diploma education, followed by a bachelor's degree (48.8% or 78 respondents). Because the study's target demographic was limited to UTAR students, the majority of responses fell somewhere between these two educational levels.

4.1.1.4 Main Use of the Internet

Table 4. 4 Respondent’s main use of the Internet

	Frequency (f)	Percentage (%)	Cumulative Percentage (%)
Education	27	16.9	16.9
Entertainment	67	41.9	58.8
Searching job	0	0	58.8
Online shopping	33	20.6	79.4
Gathering information	33	20.6	100.0
Total	**160**	**100.0**	

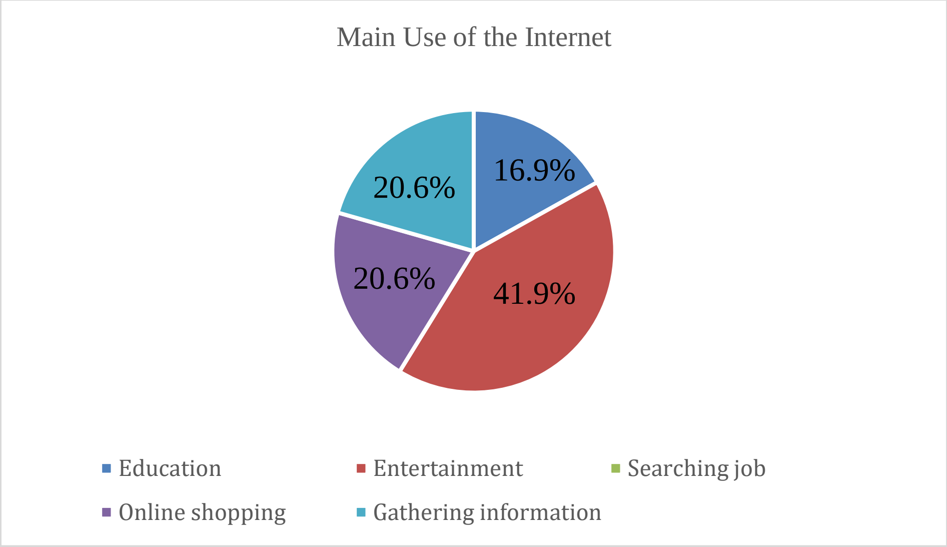


Figure 4. 4 Respondent’s main use of the Internet

Respondents were asked about their primary use of the Internet in question 4 of the survey. Figure 4.4 and Table 4.4 show the outcomes. The majority of respondents (41.9% or 67 respondents) use the Internet for entertainment, followed by online shopping (20.6% or 33 respondents), gathering information (20.6% or 33 respondents), and education (16.9% or 27 respondents). None of the respondents used the Internet to look for work as their primary purpose.

4.1.1.5 Cyber-Attacks Experience

Table 4. 5 Respondent’s cyber-attacks experience

	Frequency (f)	Percentage (%)	Cumulative Percentage (%)
Yes	52	32.5	32.5
No	108	67.5	100.0
Total	**160**	**100.0**	

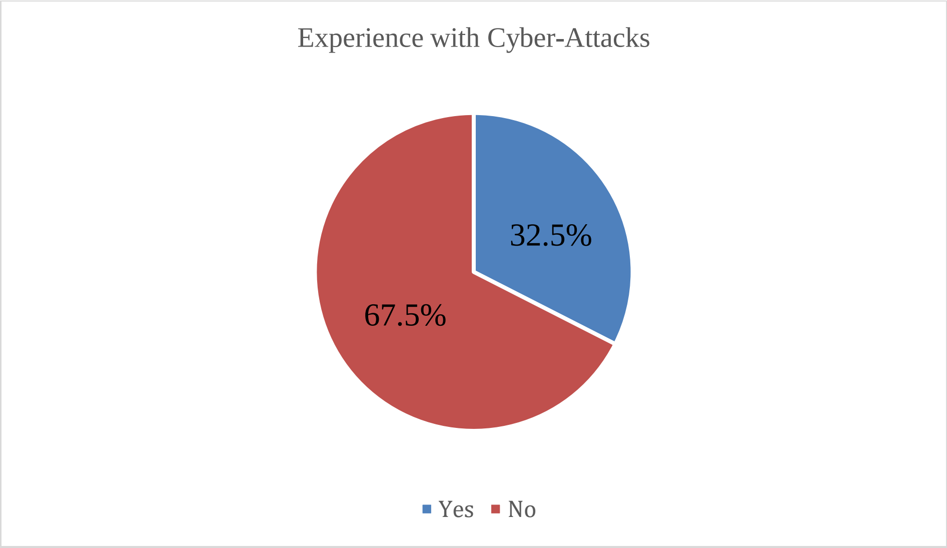


Figure 4. 5 Respondent’s cyber-attacks experience

Figure 4.5 and Table 4.5 reveal whether or not respondents have been the victim of cyber-attacks. The majority of respondents (67.5%, or 108 respondents) have no prior experience with cyber-attacks, whereas 32.5%, or 52 respondents, have experience with cyber-attacks.

4.1.2 Measurement of Structure's Central Trend

The mean scores for six interval-scale structures were calculated using a measure of central tendency. The SmartPLS result yielded a total of 32 items with particular average scores. All items/questions were rated on a 5-point Likert scale which are 1-Strongly disagree, 2-Disagree, 3-Neutral, 4-Agree, and 5-Strongly agree. However, for the cyber hygiene behavior was rated on 1-Never, 2-Rarely, 3-Sometimes, 4-Very often, and 5-Always.

Table 4. 6 Central Trend Measurement of Structure: Self-efficacy

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean	Standard Deviation
I feel confident managing files in my computer.	0.62%	18.13%	18.75%	47.50%	15.00%	3.581	0.971
I feel confident learning advanced skills to protect my information and information system.	0.62%	21.25%	13.12%	53.12%	11.88%	3.544	0.974
I am able to use anti-virus software without much effort.	2.50%	11.88%	18.12%	53.75%	13.75%	3.644	0.944
I set up password on my phone.	1.25%	6.25%	6.25%	66.88%	19.37%	3.969	0.786

For each item of self-efficacy, Table 4.6 displays the mean, standard deviation, and percentage.

The majority of respondents (47.50%) agreed that they were confident in their ability to manage files on their computer, while 18.75% neither agreed nor disagreed. While 53.12% of respondents said they were confident in their ability to develop advanced skills to protect their information and information systems, 21.25% said they disagree. Meanwhile, 53.75% of respondents say that they are able to use anti-virus software without much effort, while 18.12% of respondents neither agreed nor disagreed. Finally, 66.88% of respondents agree that they set up passwords on their phones, with 19.37% strongly agreeing.

The item with the largest mean (mean = 3.969) was “I set up a password on my phone” followed by “I am able to use anti-virus software without much effort” (mean = 3.644). “I feel confident managing files in my computer” (mean = 3.581) was the item with the third-highest average. The smallest mean (mean = 3.544) was for “I feel confident learning advanced skills to protect my information and information systems”.

The item with the largest standard deviation, 0.974, was “I feel confident learning advanced skills to protect my information and information systems”. “I am able to use anti-virus software without much effort” was the item with the second highest standard deviation (0.944). “I feel confident managing files in my computer” (standard deviation = 0.971) was the item with the third largest standard deviation. The standard deviation for “I set up password on my phone” was the smallest (standard deviation = 0.786).

Table 4. 7 Central Trend Measurement of Structure: Cyber Hygiene Knowledge

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean	Standard Deviation
Installing anti-virus software can prevent yourself from “phishing” attack.	1.25%	6.88%	11.88%	51.88%	28.12%	3.987	0.887
Password with minimum 8 characters including upper and lower characters, numbers, and special characters is considered as strong and secure password.	1.25%	1.25%	10.00%	54.38%	33.12%	4.169	0.752
Using the URL that starts with “https://” is more secure than using the URL “http://” (without “s”).	1.25%	5.62%	16.25%	47.50%	29.38%	3.981	0.891
Password "WTh!5Z" is more secure to password "123456".	0.62%	1.88%	7.50%	48.75%	41.25%	4.281	0.735

It is generally not safe to use the public Wi-Fi network (such as in an airport or café) for sensitive activities such as online banking.	0.62%	6.25%	11.25%	47.50%	34.38%	4.088	0.869
Using a virtual private network (VPN) minimizes the risk of using an unsecured Wi-Fi network.	0.62%	6.88%	14.37%	48.75%	29.38%	3.994	0.877

For each item of cyber hygiene knowledge, Table 4.7 displays the mean, standard deviation, and percentage.

There were as much as 51.88% of the respondents agreed that installing anti-virus software can prevent themselves from “phishing” attack, and 28.12% strongly agree with this statement. Password with minimum 8 characters including upper and lower characters, numbers, and special characters is considered as strong and secure password have been agreed by 54.38% of the respondents, and 33.12% of them strongly agreeing with that statement. 47.50% of them agreed that using the URL that starts with “https://” is more secure than using the URL “http://” (without “s”), while 29.38% of respondents strongly agreed. 48.75% of the respondents agreed that password "WTh!5Z" is more secure to password "123456", while 41.25% of respondents are strongly agreeing. It is generally not safe to use the public Wi-Fi network (such as in an airport or café) for sensitive activities such as online banking is agreeing by 47.50% of respondents, while 34.38% of them strongly agreed with that statement. Finally, there are 48.75% agreed, and 29.38% strongly agreed that using a virtual private network (VPN) minimizes the risk of using an unsecured Wi-Fi network.

The item with the largest mean value (mean = 3.981) is “Password "WTh!5Z" is more secure than password "123456" ”, followed by “Password with minimum 8 characters including upper and lower characters, numbers, and special characters is considered as strong and secure password” (mean = 4.169). “It is generally not safe to use the public Wi-Fi network (such as in an airport or café) for sensitive activities such as online banking” came in third (mean = 4.088), followed by “Using a virtual private network (VPN) minimizes the risk of using an unsecured Wi-Fi network” (mean = 3.994). With a mean of 3.987, “Installing anti-virus software can prevent yourself from “phishing” attack” ranked fifth, while “Using the URL that starts with “https://” is more secure than using the URL “http://” (without “s”)” has the smallest mean which is 3.981.

The item with the largest standard deviation of 0.891 was “Using the URL that starts with “https://” is more secure than using the URL “http://” (without “s”)”. The item with the second largest standard deviation of 0.887 was “Installing anti-virus software can prevent yourself from “phishing” attack”. Then followed by “Using a virtual private network (VPN) minimizes the risk of using an unsecured Wi-Fi network” has the third-highest standard deviation (standard deviation = 0.877). The item “It is generally not safe to use the public Wi-Fi network (such as in an airport or café) for sensitive activities such as online banking” have the standard deviation of 0.869. The item “Password with minimum 8 characters including upper and lower characters, numbers, and special characters is considered as strong and secure password” has its standard deviation of 0.752. The item with lowest standard deviation is “Password "WTh!5Z" is more secure to password "123456" ”, the standard deviation value is 0.735.

Table 4. 8 Central Trend Measurement of Structure: Cyber Hygiene Awareness

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean	Standard Deviation
I read the user agreements for free program/software before clicking "I accept".	2.50%	26.25%	16.88%	38.12%	16.25%	3.494	1.072
All my passwords include minimum 8 characters including upper and lower characters, numbers, and special characters.	1.25%	18.12%	26.88%	37.50%	16.25%	3.544	0.980
I regularly check the browser history and find suspicious activities.	2.50%	28.12%	21.88%	36.25%	11.25%	3.356	1.033
I use two-factor authentication when possible.	1.25%	10.62%	12.50%	52.50%	23.13%	3.906	0.886
I use multiple passwords for everything that needs a password.	3.12%	18.75%	26.25%	40.00%	11.88%	3.513	0.962

For each item of cyber hygiene awareness, the above Table 4.8 displays the mean, standard deviation, and percentage.

The majority of respondents (38.12%) agreed, while 26.25% did not agree that they read the user agreements for free program/software before clicking “I accept”, and 16.88% of them neither agreeing nor disagreeing. 37.50% agreed and 26.88% neither agreed nor disagreed, and 18.12% disagreed that all their passwords include minimum 8 characters including upper and lower characters, numbers, and special characters. 36.25% of the respondents agreed that they regularly check the browser history and find suspicious activities, 28.12% of them did not agree with that statement. 52.50% agreed and 23.13% strongly agreed that they use two-factor authentication when possible. Finally, 40.00% of the respondents agreed that they use multiple passwords for everything that needs a password, while the remaining 26.25% neither agreeing nor disagreeing with that statement.

The item with the highest mean (mean = 3.906) was “I use two-factor authentication when possible”, followed by “All my passwords include minimum 8 characters including upper and lower characters, numbers, and special characters” (mean = 3.544). “I use multiple passwords for everything that needs a password” (mean = 3.513) was the item with the third-highest mean. The mean score for “I read the user agreements for free program/software before clicking "I accept"” was 3.494. The item “I regularly check the browser history and find suspicious activities” (mean = 3.356) has the lowest mean score.

The item “I read the user agreements for free program/software before clicking "I accept"” has the highest standard deviation (standard deviation = 1.072), followed by “I regularly check the browser history and find suspicious activities” (standard deviation = 1.033). The item “All my passwords include minimum 8 characters including upper and lower characters, numbers, and special characters” ranked the third largest standard deviation, which is 0.980. Then followed by “I use multiple passwords for everything that needs a password” (standard deviation = 0.962). The item “I use two-factor authentication when possible” has the lowest standard deviation, which is 0.886.

Table 4. 9 Central Trend Measurement of Structure: Cyber Hygiene Attitude

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean	Standard Deviation
It is annoying to have different complex password for different accounts.	1.25%	25.62%	19.38%	40.00%	13.75%	3.394	1.049
It is hard to remember the different passwords for every different accounts.	1.25%	22.50%	16.88%	41.25%	18.12%	3.525	1.066
I believe only public accounts are targeted by hackers and cybercriminals.	5.62%	14.38%	26.25%	43.12%	10.63%	3.388	1.037
I feel that only simple and easy to guess passwords are at risk of being victims of cybercrime.	4.38%	13.75%	20.62%	48.75%	12.50%	3.513	1.019
My first impression when checking if a website address is secure by seeing if it contains "https://" and/or showing a padlock is positive.	3.12%	16.88%	16.25%	50.63%	13.12%	3.538	1.018

Locking a device when I am no longer using it is something I find useful and easy.	0.62%	9.38%	11.25%	61.25%	17.50%	3.856	0.836

For each item of cyber hygiene attitude, Table 4.9 displays the mean, standard deviation, and percentage.

There were as much as 40.00% of the respondents agreed and 25.62% disagreed that it is annoying to have different complex password for different accounts. 41.25% of the respondents agreed that it is hard to remember the different passwords for every different accounts, while 22.50% of them did not agree. 43.12% of respondents agreeing and 26.25% of them neither agreeing nor disagreeing that they believe only public accounts are targeted by hackers and cybercriminals, while 14.38% of them did not agree with that item. 48.75% of them agreed that they feel that only simple and easy to guess passwords are at risk of being victims of cybercrime, while 20.62% o them neither agreeing nor disagreeing with that statement. 50.63% of the respondents agreed and 16.88% of them disagreed that their first impression when checking if a website address is secure by seeing if it contains "https://" and/or showing a padlock is positive. Finally, 61.25% of the respondents agreed that locking a device when they are no longer using it is something they find useful and easy, while 17.50% of them strongly agreed with that statement.

The item with highest mean (mean = 3.856) was “Locking a device when I am no longer using it is something I find useful and easy”, followed by “My first impression when checking if a website address is secure by seeing if it contains "https://" and/or showing a padlock is positive” (mean = 3.538), followed by “It is hard to remember the different passwords for every different accounts” (mean = 3.525), followed by “I feel that only simple and easy to guess passwords are at risk of being victims of cybercrime” (mean = 3.513), followed by “It is annoying to have different complex password for different accounts” (mean = 3.394). “I believe only public accounts are targeted by hackers and cybercriminals” (mean = 3.388) is the item with lowest mean.

The item that has the highest standard deviation (standard deviation = 1.066) is “It is hard to remember the different passwords for every different accounts”. The item with second highest standard deviation (standard deviation = 1.049) is “It is annoying to have different complex password for different accounts”. Then followed by “I believe only public accounts are targeted by hackers and cybercriminals” (standard deviation = 1.037). The standard deviation of the item “I feel that only simple and easy to guess passwords are at risk of being victims of cybercrime” is 1.019. The standard deviation of the item “My first impression when checking if a website address is secure by seeing if it contains "https://" and/or showing a padlock is positive” is 1.018. The item “Locking a device when I am no longer using it is something I find useful and easy” has the lowest standard deviation (standard deviation = 0.836).

Table 4. 10 Central Trend Measurement of Structure: Cyber Hygiene Intention

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree	Mean	Standard Deviation
I intend to set a long and strong password.	0.62%	13.75%	15.62%	51.88%	18.13%	3.731	0.934
I will be going to keep my computer and phone locked with a pin, or a password longer than 6 numbers.	1.88%	11.25%	13.75%	53.75%	19.38%	3.775	0.948
I will be going to change my password periodically and use a different passwords for each of the accounts.	1.88%	21.87%	18.75%	42.50%	15.00%	3.469	1.048
I intend to participate in the training class about cyber hygiene in the future.	1.25%	17.50%	20.00%	46.25%	15.00%	3.562	0.985
I will sign out the accounts when	1.88%	12.50%	13.75%	53.12%	18.75%	3.744	0.963

away from the computer or device.		

For each item of cyber hygiene intention, Table 4.10 displays the mean, standard deviation, and percentage.

A whopping 51.88% of respondents agreed, with 18.13% strongly agreed that they intend to set a long and strong password. 53.75% of respondents agreed that they will be going to keep their computer and phone locked with a pin, or a password longer than 6 numbers, with 19.38% strongly agreed and 13.75% neither agreeing nor disagreeing. Only 42.50% of respondents agreed that they will be going to change their password periodically and use a different passwords for each of the accounts, while 21.87% of them disagreed. 46.25% of the respondents agreed, 20.00% neither agreed nor disagreed, and 17.50% of respondents disagreed that they intend to participate in the training class about cyber hygiene in the future. Finally, 53.12% of respondents agreed that they will sign out the accounts when away from the computer or device, 18.75% strongly agreed, and 13.75% neither agreed nor disagreed.

The item with the highest mean (mean = 3.775) is “I will be going to keep my computer and phone locked with a pin, or a password longer than 6 numbers”, followed by “I will sign out the accounts when away from the computer or device” (mean = 3.744). The item with third-highest mean (mean = 3.731) was “I intend to set a long and strong password”, followed by “I intend to participate in the training class about cyber hygiene in the future” (mean = 3.562). “I will be going to change my password periodically and use a different passwords for each of the accounts” (mean = 3.469) is the item with the lowest mean.

The item that has the highest standard deviation (standard deviation = 1.048) is “I will be going to change my password periodically and use a different passwords for each of the accounts”. The item with second highest standard deviation (standard deviation = 0.985) is “I intend to participate in the training class about cyber hygiene in the future”. The item with third highest standard deviation (standard deviation = 0.963) is “I will sign out the accounts when away from the computer or device”, followed by “I will be going to keep my computer and phone locked with a pin, or a password longer than 6 numbers” (standard deviation = 0.948). The item “I intend to set a long and strong password” has the lowest standard deviation (standard deviation = 0.934).

Table 4. 11 Central Trend Measurement of Structure: Cyber Hygiene Behavior

	Never	Rarely	Sometimes	Very Often	Always	Mean	Standard Deviation
I use the same password for multiple account.	0.62%	20.62%	34.38%	25.00%	19.38%	3.419	1.040
I set my passwords with minimum 8 characters including upper and lower characters, numbers, and special characters.	0.00%	14.38%	41.88%	28.12%	15.62%	3.450	0.921
I share personal information on social media.	3.75%	24.38%	43.75%	20.62%	7.50%	3.038	0.948
I performed an anti-virus scan regularly.	3.75%	15.00%	26.25%	29.38%	25.62%	3.581	1.132
I back up my important files every time.	3.75%	8.75%	22.50%	28.13%	36.88%	3.856	1.123

For each item of cyber hygiene behavior, Table 4.11 displays the mean, standard deviation, and percentage.

There were as much as 34.38% of the respondents describe that sometimes they use the same password for multiple account, while 25.00% of them very often will do that behavior. 41.88% of the respondents describe that sometimes they set their passwords with minimum 8 characters including upper and lower characters, numbers, and special characters, while 28.12% very often and 15.62% always do that behavior. 43.75% of the respondents describe that they sometimes will share personal information on social media, while 24.38% of them rarely do that. 29.38% of the respondents very often performed an anti-virus scan regularly, while 26.25% sometimes, and 25.62% always do that. Finally, 36.88% of the respondents describe that they always back up their important files every time, while 28.13% of them describe they very often do that.

The item with greatest mean value was “I back up my important files every time” (mean = 3.856), followed by “I performed an anti-virus scan regularly” (mean = 3.581). “I set my passwords with minimum 8 characters including upper and lower characters, numbers, and special characters” (mean = 3.450) is the item with third-highest mean. The item with second lowest mean value is “I use the same password for multiple account” (mean = 3.419). The statement “I share personal information on social media” (mean = 3.038) is the statement with lowest mean among all.

The item “I performed an anti-virus scan regularly” has the highest standard deviation (standard deviation = 1.132). The item with second highest standard deviation (standard deviation = 1.123) is “I back up my important files every time”. The item “I use the same password for multiple account” is the item with third highest standard deviation (standard deviation = 1.040). The item “I share personal information on social media” (standard deviation = 0.948) has the second smallest standard deviation. The item “I set my passwords with minimum 8 characters including upper and lower characters, numbers, and special characters” has the lowest standard deviation (standard deviation = 0.921).

4.2 SEM Analysis

Internal consistent reliability measurement models include Cronbach's Alpha and composite reliability (CR). After that, a convergent validity measurement model, such as average variance extraction (AVE), is used in this study. Furthermore, discriminant validity incorporates Fornell-Lacker criteria, and cross-loading is evaluated at this stage to see how concepts connect to other metrics.

To identify multicollinearity concerns, the Variance Inflation Factor (VIF), and path coefficients, the path model approach is applied [100]. Aside from that, the path coefficient develops the hypothesis using beta, t-value, and R square.

4.2.1 Analysis of Reliability and Validity

The measuring model for the current research is shown in Table 4.12. CHAtt1, CHAtt2, CHB1, and CHB3 will be deleted because their outer loadings are less than 0.5. Table 4.12 shows that all of the items are more than the acceptable value of 0.5. With the exception of SE4 and CHB2, the results reveal that when the outer load is larger than 0.7, these items are rated outstanding.

Composite reliability (CR) is a superior measure of internal consistency since it uses normalized loadings of variables [97]. The purpose of composite reliability is to determine the variables' dependability [101]. Composite reliability is recommended for values above 0.7 [102]. Table 4.12 shows that all elements have values more than 0.8, indicating that the composite reliability is dependable. CHK had the highest composite reliability rating of 0.942, while CHB had the lowest composite reliability score (0.858). As a result, the findings show that each variable reaches excellent composite reliability.

CHK and CHI both had the value of 0.926 and 0.910 for their Cronbach's alpha, which were judged to be excellent association strengths. Second, CHAtt, CHA, and SE have Cronbach's alpha values of 0.849, 0.886, and 0.849, respectively, with a reliability above 0.8 deemed good. Furthermore, Cronbach's alpha values for CHB were 0.748 respectively. Cronbach's alpha scores for all variables ranged from 0.748 to 0.926, all of which were higher than the 0.7 criteria. As a result, all variables are regarded as trustworthy.

In a partial least squares analysis, [97] examined the convergence validity of the average variance extraction criterion for each latent variable. Furthermore, when the average variance extraction value was larger than the permitted threshold of 0.5, convergent validity was proven. All constructions were over 0.5 in Table 4.12, with CHAtt at 0.688, CHA at 0.686, CHB at 0.672, CHI at 0.735, CHK at 0.729, and SE at 0.696. This meant that all of the constructs passed the convergent validity test. As a result, all of the items had enough convergent validity.

Table 4. 12 Analysis of Convergent Validity and Internal Consistency Reliability

Construct	Items	Outer Loading	Cronbach's Alpha	Composite Reliability	Average Variance Extracted
Self-efficacy	SE1	0.904	0.849	0.900	0.696
	SE2	0.879			
	SE3	0.863			
	SE4	0.671			
Cyber Hygiene Knowledge	CHK1	0.869	0.926	0.942	0.729
	CHK2	0.880			
	CHK3	0.863			
	CHK4	0.767			
	CHK5	0.858			
	CHK6	0.881			
Cyber Hygiene Awareness	CHA1	0.820	0.886	0.916	0.686
	CHA2	0.866			
	CHA3	0.854			
	CHA4	0.771			
	CHA5	0.827			
Cyber Hygiene Attitude	CHAtt3	0.811	0.849	0.898	0.688
	CHAtt4	0.863			
	CHAtt5	0.853			

	CHAtt6	0.788			
Cyber Hygiene Intention	CHI1	0.884	0.910	0.933	0.735
	CHI2	0.877			
	CHI3	0.868			
	CHI4	0.874			
	CHI5	0.782			
Cyber Hygiene Behavior	CHB2	0.661	0.748	0.858	0.672
	CHB4	0.882			
	CHB5	0.895			
Note: CHAtt1, CHAtt2, CHB1, and CHB3 were deleted due to low outer loading					

4.2.2 Analysis of Discriminant Validity

The degree to which a construct can be discriminated from other constructs in the same model is known as discriminant validity. Cross-loading methods of measuring metrics and Fornell-Larcker criterion can be used to examine discriminative validity tests [97].

To measure the discriminant validity of the structural model, researcher used Fornell-Larcker criterion. To establish discriminant validity, [97] advocated using the square root of the AVE in each latent of the variable. When compared to other latent elements, the AVE values for each variable were higher than the highest squared correlation of the latent variables [68]. The discriminant validity of all items is well established, as shown in Table 4.13, and the latent variables have good values. As we can see that the AVE of all the latent variables were greater than 0.5 minimum treshold in Table 4.12, and in Table 4.13 shows that the square root of AVE is greater than the correlations between latent variables. As a result, we may infer that all of the measures utilized in this study have good discriminant validity. For example, the latent variable Cyber Hygiene Intention’s AVE is found to be 0.735 (from Table 4.12) hence its square root becomes 0.858. The number is larger than the correlation values in the column of Cyber Hygiene Intention (0.551 and 0.560) and the number also larger than the values in the row of Cyber Hygiene Intention (0.782, 0.628, and 0.641). A similar finding is made for the latent variables: Self-efficacy, Cyber Hygiene Knowledge, Cyber Hygiene Awareness, Cyber Hygiene Attitude, and Cyber Hygiene Behavior. All the latent variable's square root number is found larger than their AVE values and correlation valus in column and row. Hence, the outcome suggests that discriminant validity is well established.

Table 4. 13 Fornell-Larcker Criterion Analysis for Checking Discriminant Validity

	CHAtt	CHA	CHB	CHI	CHK	SE
Cyber Hygiene Attitude	**0.829**					
Cyber Hygiene Awareness	0.544	**0.828**				
Cyber Hygiene Behavior	0.600	0.559	**0.820**			
Cyber Hygiene Intention	0.782	0.628	0.641	**0.858**		
Cyber Hygiene Knowledge	0.511	0.393	0.355	0.551	**0.854**	
Self-efficacy	0.633	0.572	0.461	0.560	0.488	**0.834**

Cross-loadings of each indicator shown in Table 4.14. Cross-loading was used to test the reliability of each item, and it was discovered that the factor loading values for each structure were quite high, exceeding the cut-off value of 0.70 [103]. When compared to other loading levels, bold numbers represent the highest value cross-loading. In cross-loading, all values represent each item's contribution to the construction. When compared to other latent variables, indicators have higher values on their related latent variable. With this we can confirms the model discriminant validity by ensuring the manifest variables in each construct represent the assigned latent variables. For example, CHAtt3 has a variance of 0.811, which indicates it accounts an 81.1% share in the construction. Furthermore, each structure with the highest cross-loading value among its own latent variables was found to have discriminant validity.

Table 4. 14 Cross Loadings

Items	Cyber Hygiene Awareness	Cyber Hygiene Attitude	Cyber Hygiene Behavior	Cyber Hygiene Intention	Cyber Hygiene Knowledge	Self-efficacy
CHA1	**0.820**	0.446	0.395	0.464	0.313	0.463
CHA2	**0.866**	0.401	0.469	0.500	0.286	0.457
CHA3	**0.854**	0.406	0.449	0.466	0.189	0.457
CHA4	**0.771**	0.513	0.492	0.584	0.497	0.493
CHA5	**0.827**	0.460	0.494	0.559	0.295	0.483
CHAtt3	0.397	**0.811**	0.444	0.615	0.409	0.498
CHAtt4	0.339	**0.863**	0.532	0.644	0.409	0.483
CHAtt5	0.518	**0.853**	0.557	0.686	0.416	0.511
CHAtt6	0.533	**0.788**	0.455	0.643	0.456	0.599
CHB2	0.557	0.349	**0.661**	0.421	0.130	0.453
CHB4	0.443	0.552	**0.882**	0.598	0.343	0.353
CHB5	0.410	0.549	**0.895**	0.540	0.368	0.357
CHI1	0.604	0.670	0.555	**0.884**	0.524	0.531
CHI2	0.474	0.713	0.641	**0.877**	0.515	0.485
CHI3	0.522	0.652	0.529	**0.868**	0.408	0.422
CHI4	0.633	0.653	0.585	**0.874**	0.436	0.479
CHI5	0.463	0.663	0.421	**0.782**	0.475	0.485
CHK1	0.344	0.473	0.335	0.494	**0.869**	0.400
CHK2	0.219	0.406	0.253	0.423	**0.880**	0.417
CHK3	0.329	0.533	0.336	0.493	**0.863**	0.421
CHK4	0.267	0.317	0.161	0.314	**0.767**	0.386
CHK5	0.434	0.417	0.346	0.521	**0.858**	0.455
CHK6	0.408	0.439	0.348	0.537	**0.881**	0.426
SE1	0.584	0.519	0.396	0.504	0.357	**0.904**
SE2	0.541	0.513	0.433	0.491	0.355	**0.879**
SE3	0.523	0.601	0.404	0.522	0.417	**0.863**
SE4	0.228	0.461	0.295	0.328	0.511	**0.671**

4.3 Structural Model

Table 4.15 shows the results where the VIF values range from 1.0 to 2.5, and there is no evidence of multicollinearity. In addition, the path coefficients aid in determining the degree of the effect and demonstrate that the variables have a direct relationship. Between 0.1 and 1 is the recommended range. Thus, SE, CHK, and CHA appear to have a direct influence upon CHAtt, CHAtt appear to have a direct influence upon CHI, and CHI also appear to have a direct influence upon CHB.

After assessing the measurement models in PLS, structural models were created, and the significance of the provided model assumptions was tested by examining the internal models. As shown in Table 4.15, the value of VIF exhibits no signs of multicollinearity concerns. Next, the link between two variable can be determined using the T-statistics and the P-value. When the T-statistics value is greater than 1.96 and the P-value is less than 0.05, the alternative hypothesis is accepted. The acceptable T-statistics outcomes in this study were 3.424, 2.327, 21.709, 9.382, with P-values of 0.001, 0.020, 0.000, and 0.000 respectively.

Table 4. 15 Path Analysis for Structural Model

Path	VIF	Path Coefficient	T-Statistics	P-Values	Results
Self-efficacy --> Cyber Hygiene Attitude	1.693	0.388	3.424	0.001	Accept
Cyber Hygiene Knowledge --> Cyber Hygiene Attitude	1.347	0.231	2.327	0.020	Accept
Cyber Hygiene Awareness --> Cyber Hygiene Attitude	1.526	0.232	1.509	0.132	Reject
Cyber Hygiene Attitude --> Cyber Hygiene Intention	1.000	0.782	21.709	0.000	Accept
Cyber Hygiene Intention --> Cyber Hygiene Behavior	1.000	0.641	9.382	0.000	Accept

Cyber Hygiene Attitude: R-square = 0.489; Adjusted R-square = 0.480
Cyber Hygiene Intention: R-square = 0.611; Adjusted R-square = 0.609
Cyber Hygiene Behavior: R-square = 0.411; Adjusted R-square = 0.408

Figure 4.6 depicts the framework, which displays the outer loaded values for items inside the independent variables (SE, CHK, CHA, CHAtt, and CHI) as well as the dependent variable (CHB). Because the dependability of an item is determined by numbers between 0 and 1, with values closer to 1 suggesting a higher level of reliability, any number greater than 0.7 is regarded as preferred. The outer load value should be more than 0.5, according to [98], which indicates that values between 0.5 and 1 do not need to be culled.

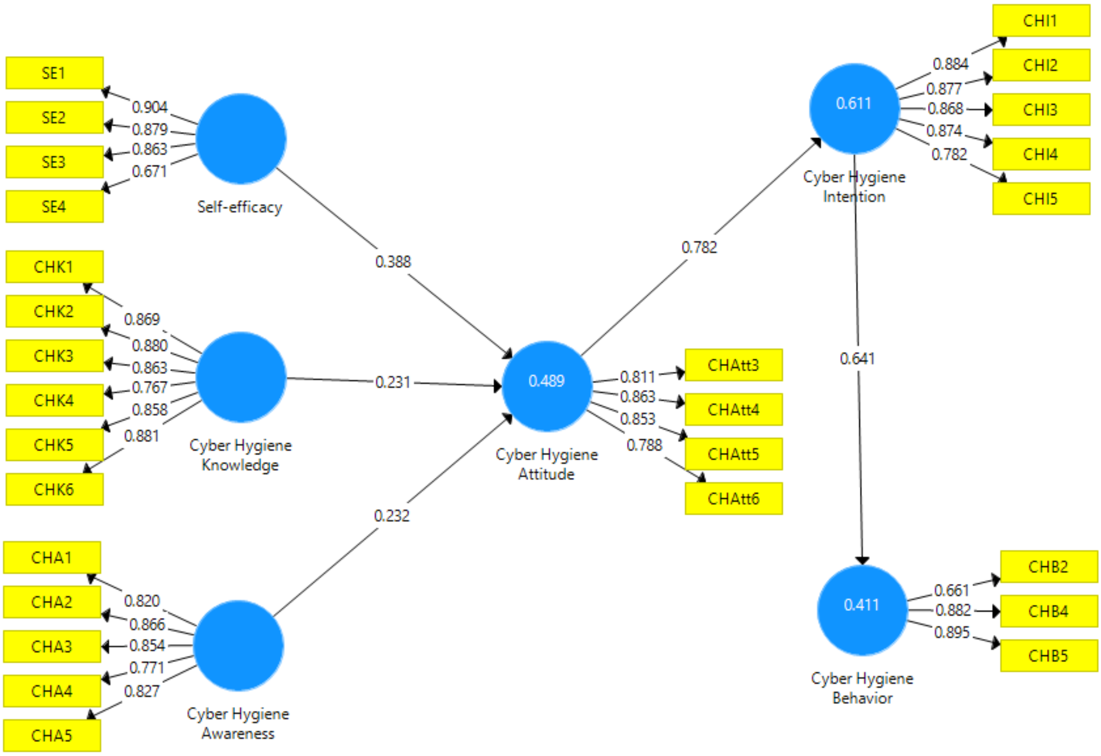


Figure 4. 6 Finalized Framework Structural Model

4.4 Conclusion

In the nutshell, the questionnaire data was compiled and PLS-SEM findings was analyzed using SmartPLS. There are three parts to the study: descriptive analysis, SEM analysis, and structural modeling. The results and interpretation of the analysis will be utilized in the following chapter to continue the entire study's discussion, ramifications, and conclusions.

Chapter 5

Implications, Findings, And Conclusions

5.0 Introduction

This chapter summarizes and discusses the prior chapter's findings, as well as descriptive and inferential analysis. The theory will also be backed up by reasoning or proof. Consequences and suggestions are also documented. The limitations of this study will also be addressed at the end of this chapter as the ultimate conclusion of this investigation.

5.1 Statistical Analysis Summary

5.1.1 Descriptive Analysis

5.1.1.1 Respondent Demographics

According to the analysis of respondents' demographic profiles, the majority of respondents were women (54.4%). All of those who responded were between the ages of 18 and 28 years old. This is due to the fact that the majority of UTAR students are in this age bracket. Additionally, the bulk of responders (51.2%) were having their level of education on foundation/diploma. Finally, 41.9% of respondents use the Internet for entertainment purposes and 67.5% of them do not have experience with cyber-attacks.

5.1.1.2 Central Trend Measurement of Structures

In terms of self-efficacy, the highest mean was 3.969 for “I set up a password on my phone”, while the lowest was 3.544 for “ I feel confident learning advanced skills to protect my information and information system”. “I feel confident learning advanced skills to protect my information and information system” had the largest standard deviation of 0.974, while “I set up a password on my phone” had the lowest standard deviation (standard deviation = 0.786).

For the cyber hygiene knowledge, the item “Password "WTh!5Z" is more secure to password "123456"” has the largest mean, which is 4.281, while the smallest mean 3.981 is the item “Using the URL that starts with “https://” is more secure than using the URL “http://” (without “s”)”. Besides, with a standard deviation of 0.891, the item “Using the URL that starts with “https://” is more secure than using the URL “http://” (without “s”)” had the largest standard deviation, while the “Password "WTh!5Z" is more secure to password "123456"” (standard deviation = 0.735) had the smallest standard deviation in the construct of cyber hygiene knowledge.

In the construct of cyber hygiene awareness, “I use two-factor authentication when possible” is the item with highest mean (mean = 3.906). The item with the lowest mean is “I regularly check the browser history and find suspicious activities” (mean = 3.356). On the other hand, the item “I read the user agreements for free program/software before clicking "I accept"” has the largest standard deviation, which is 1.072. The item with smallest standard deviation is “I use two-factor authentication when possible”, which is 0.886.

In terms of cyber hygiene attitude, the statement of “Locking a device when I am no longer using it is something I find useful and easy” is the item with highest mean (mean = 3.856). The item with lowest mean is “I believe only public accounts are targeted by hackers and cybercriminals” (mean = 3.388). On the other hand, the item that has the highest standard deviation (standard deviation = 1.066) is “It is hard to remember the different passwords for every different accounts”. The item has the lowest standard deviation (standard deviation = 0.836) was “Locking a device when I am no longer using it is something I find useful and easy”.

In the construct of cyber hygiene intention, the item with largest mean (mean = 3.775) was “I will be going to keep my computer and phone locked with a pin, or a password longer than 6 numbers”. The item “I will be going to change my password periodically and use a different passwords for each of the accounts” has the smallest mean among all (mean = 3.469). Additionally, the item which has largest standard deviation (standard deviation = 1.048) is “I will be going to change my password periodically and use a different passwords for each of the accounts". The item has the smallest standard deviation (standard deviation = 0.934) was "I intend to set a long and strong password".

In the aspect of cyber hygiene behavior, "I back up my important files every time" is the statement which has largest mean (mean = 3.856), while the item "I share personal information on social media" has the smallest mean among all (mean = 3.038). Moreover, statement with largest standard deviation (standard deviation = 1.132) is "I performed an anti-virus scan regularly". The statement that has the lowest standard deviation (standard deviation = 0.921) was "I set my passwords with minimum 8 characters including upper and lower characters, numbers, and special characters".

5.1.2 SEM Analysis Summary

5.1.2.1 Analysis of Reliability and Validity

The 32 items of internal reliability and validity of the 6 constructs in the questionnaire were assessed using composite reliability, Cronbach's alpha coefficient, and extracted average variance extracted (AVE). Cronbach's alpha coefficient for self-efficacy (4 items) is 0.849, cyber hygiene knowledge (6 items) is 0.926, cyber hygiene awareness (5 items) is 0.886, cyber hygiene attitude (4 items) is 0.849, cyber hygiene intention (5 items) is 0.910, and cyber hygiene behavior (3 items) is 0.748. All the value is above 0.7, so all constructs are considered to be reliable. The composite reliability to self-efficacy (4 items) is 0.900, cyber hygiene knowledge (6 items) is 0.942, cyber hygiene awareness (5 items) is 0.916, cyber hygiene attitude (4 items) is 0.898, cyber hygiene intention (5 items) is 0.933, and cyber hygiene behavior (3 items) is 0.858. As a result, the findings show that each variable reaches excellent composite reliability since all the values are exceed the threshold of 0.7. The AVE for self-efficacy (4 items) is 0.696, cyber hygiene knowledge (6 items) is 0.729, cyber hygiene awareness (5 items) is 0.686, cyber hygiene attitude (4 items) is 0.688, cyber hygiene intention (5 items) is 0.735, and cyber hygiene behavior (3 items) is 0.672. This meant that all of the constructs passed the convergent validity test. So, all items had sufficient convergent validity. In the measurement model, CHAtt1, CHAtt2, CHB1, and CHB3 were deleted due to low outer loading.

5.1.2.2 Analysis of Discriminant Validity

In this study, we may infer that all of the measures utilized have good discriminant validity. All the latent variable’s square root number is found larger than their AVE values and correlation valus in column and row. Hence, the outcome suggests that discriminant validity is well established. Furthermore, any structure with the highest cross-loading value among its own latent variables was found to have discriminative validity.

5.1.3 Summary of Structural Model

Multicollinearity issues are absent in this study because all the VIF values for the path are between the range of 1.0 and 2.5. In addiditon, all independent variables have a direct relationship upon dependent variables due to the path coefficient is between 0.1 and 1. Lastly, all the T-statistics and P-values are greater than 1.96 and less than 0.05, except for the independent variables of cyber hygiene awareness.

5.2 Discussion of Key Findings

5.2.1 Findings on General Question

GQ1: What elements influence cyber hygiene behavior during COVID-19 in order to avoid cyber-attacks?

Items including self-efficacy, cyber hygiene knowledge, cyber hygiene awareness, cyber hygiene attitude, and cyber hygiene intention all obtain an outer loading that is greater than 0.5 acceptable value. As a result, researchers infer that all elements contribute to the desire to cyber hygiene behavior during COVID-19 to avoid cyber-attacks. To the researcher’s knowledge, just a few researchers have focused on cyber hygiene behavior during COVID-19.

GQ2: What is the relationship between these elements and cyber hygiene behavior?

Only one association are not supported, as indicated in Table 5.1, notably the relationship between cyber hygiene awareness and cyber hygiene attitude. The remaining linkages reveal a statistically significant relationship between cyber hygiene behavior. Cyber hygiene knowledge were found to be a key determinant of cyber hygiene attitude, accounting for around 72.9% of the variance. Meanwhile, cyber hygiene intention which mediates the cyber hygiene behavior, is influenced by cyber hygiene attitude. From a content-specific standpoint, researcher clearly identified the factors impacting Internet users' cyber hygiene behavior in this study. The findings add to researchers' knowledge of the elements that influence Internet users' cyber hygiene behavior.

Table 5. 1 Results of Hypotheses Test

Hypothesis	T-Statistics	P-Values	Results
H1: Self-efficacy has a significant relationship with cyber hygiene attitude.	3.424	0.001	Supported
H2: Cyber hygiene knowledge has a significant relationship with cyber hygiene attitude.	2.327	0.020	Supported
H3: Cyber hygiene awareness has a significant relationship with cyber hygiene attitude.	1.509	0.132	Not Supported
H4: Cyber hygiene attitude has a significant relationship with cyber hygiene intention.	21.709	0.000	Supported
H5: Cyber hygiene intention has a significant relationship with cyber hygiene behavior.	9.382	0.000	Supported

5.2.2 Relationship Between Self-efficacy and Cyber Hygiene Attitude

SQ1: Is self-efficacy significantly explaining Internet users' cyber hygiene attitude?

H1: Self-efficacy has a significant relationship with cyber hygiene attitude.

Self-efficacy and cyber hygiene attitude have a substantial positive association, according to the data in Chapter 4, with a T-statistic of 3.424 and 0.001 for its p-value, which is significant at an alpha value of 0.05. Self-efficacy and cyber hygiene attitude had a path coefficient of 0.388, which was between the recommended value of 0.1 and 1. As a result, this hypothesis is accepted.

Self-efficacy in information security is favorably connected with attitudes toward cyber cleanliness, according to the findings of this study. [53] believes that self-efficacy is positively related to attitude and that it can be a significant predictor of performance behavior. It has also been recommended that valid measures of self-efficacy should be adjusted to evaluate areas of interest in order to best predict future performance. Besides, self-efficacy is a key predictor of safe behaviors in cyber hygiene, and it is related to an individual's confidence in executing safe actions. As a result, an individual's attitude to comply with proactive cyber security behavior training may be influenced by self-efficacy [53]. Therefore, Internet users need to be have strnger self-efficacy in order to increase their attitude in cyber hygiene and take a good behavior on cyber hygiene. Finally, p-values and t-statistics show that it is a substantial positive link between cyber hygiene attitude and self-efficacy.

5.2.3 Relationship Between Cyber Hygiene Knowledge and Cyber Hygiene Attitude

SQ2:Is cyber hygiene knowledge significantly explaining Internet users' cyber hygiene attitude?

H2: Cyber hygiene knowledge has a significant relationship with cyber hygiene attitude.

The association between cyber hygiene knowledge and cyber hygiene attitude is significant, according to the findings, because its p-value is 0.020, which is lower than its alpha value of 0.05. Furthermore, with a path coefficient of 0.231 and a T statistic of 2.327, which was greater than the threshold of 1.96. So, cyber hygiene knowledge was positively connected with cyber hygiene attitude.

The findings agree with previous research. For example, the good correlations between knowledge-attitude, knowledge-practice, and attitude-practice found in the past study confirm the link between knowledge, attitude, and practice in cyberthreats prevention. It has been found that having enough knowledge can lead to a positive mindset and beneficial habits. Knowledge is a necessary precondition for adopting appropriate action in any situation. In other domains, such as nutrition and HIV prevention, research has shown that having the proper knowledge is a critical first step in changing one's behavior. Understanding cyberthreats and the dangers connected with them is essential when it comes to cybersecurity [55]. Finally, this research suggests that there is a strong link between cyber hygiene knowledge and cyber hygiene attitudes.

5.2.4 Relationship Between Cyber Hygiene Awareness and Cyber Hygiene Attitude

SQ3: Is cyber hygiene awareness significantly explaining Internet uses' cyber hygiene attitude?

H3: Cyber hygiene awareness has a significant relationship with cyber hygiene attitude.

With a t-statistics value of 1.509, which was less than the acceptable value of 1.96, and its p-value is 0.132, which was above the threshold alpha value of 0.05, path analysis tested by Bootstrapping revealed that there was no significant relationship between cyber hygiene awareness and cyber hygiene attitude. The hypothesis was rejected due to a failed t-statistic and p-value, despite the path coefficient value of 0.232, which was between 0.1 and 1.

This research outcome conflict with past research outcome. According to [104], the findings reveal that there is a link between users' attitudes and their awareness of information security. The findings reveal that attitudes are determinants of confidentiality, implying that while implementing procedures to preserve information confidentiality, personnel must have the right attitude. The data also reveal that only attitudes are drivers of usablity, implying that users may posses the essential attitudes [104]. Besides, individuals can effectively value their privacy and decrease their eposure while browsing the web by being aware of privacy dangers and change their attitude by learning how to control their personal information through the use of privacy-enhancing tools [66]. However, in this research, the results show that the cyber hygiene awareness and cyber hygiene attitude does not have significant relationship.

5.2.5 Relationship Between Cyber Hygiene Attitude and Cyber Hygiene Intention

SQ4: Is cyber hygiene attitude significantly explaining Internet users' cyber hygiene intention?

H4: Cyber hygiene attitude has a significant relationship with cyber hygiene intention.

With a path coefficient of 0.782, a t-statistic of 21.709, and a p-value of 0.000, the study's findings revealed a substantial positive association between cyber hygiene attitude and cyber hygiene intentions. The assumption is accepted because the path coefficient values are within the approved range of 0.1 to 1, the t-statistic is greater than 1.96, and the p-value is less than an alpha value of 0.05.

The findings of this study are supported by several past studies. For example, cybersecurity controls are also seen favorably. Although cognitive attitudes were higher than affective attitude, affective attitudes were nonetheless strong enough to explain a person's intention to undertake cybersecurity practices. The scales created to assess these two attitudes had a high level of internal consistency, indicating that they were suitable for those measurements [55]. Both attitudes and behavioral intentions had a favorable connection as expected. This suggests that having a more positive mindset increases the likelihood of adopting cybersecurity practices. The research discussed in past research is unique in that it incorporates not only cognitive but also affective attitudes. Decision about conduct are also influenced by feelings. Previous research has found a beneficial link between cognitive attitudes and behavioral intentions [105]. In conclusion, the hypothesis of cyber hygiene attitude has a significant relationship between cyber hygiene intention is accepted in this current research.

5.2.6 Relationship Between Cyber Hygiene Intention and Cyber Hygiene Behavior

SQ5: Is cyber hygiene intention significantly explaining Internet users' cyber hygiene behavior?

H5: Cyber hygiene intention has a significant relationship with cyber hygiene behavior.

With a path coefficient of 0.641, a t-statistic value of 9.382, which is larger than the threshold of 1.96, a p-value of 0.000, which is above the alpha value of 0.05, the results in Chapter 4 show that there is a significant positive association between cyber hygiene intention and cyber hygiene behavior.

This outcome is also in line with the [45]. He believes that behavior can be realistically predicted when focusing on stated intent. The mean intent-behavior correlation was r = 0.53 in numerous meta-analyses, including Sheeran's meta-analysis. In one interpretation of this relationship, intent might predict or explain around 28% of the behavioral variation. Additionally, feelings and ideas may not be as predictive of behavior as intentions. In many instances, people's intentions are a good (but far from perfect) prediction of behavior [106]. Behavioral purpose can explain a substantial number of future behavior changes on average. The average attitude toward behavioral correlation was r = 0.53 in several research, and in many cases, the correlation exceeded r = 0.70 [106]. Hence, in this study, the hypothesis of cyber hygiene intention has a significant relationship with cyber hygiene behavior that developed by researchers is accepted.

5.3 Implications of Study

The factors that influence cyber hygiene behavior are proposed in this study. The current study's findings have a lot of ramifications for people who want to learn how to enhance cyber hygiene behavior during COVID-19 to avoid cyber-attacks. Organizations and related actors might use the findings of the study to influence their future actions in order to increase their cyber hygiene behavior. For starters, self-efficacy has been discovered to be a significant factor affecting cyber hygiene attitude which will then lead to affect in cyber hygiene behavior. Organizations or school must understand that the people with stronger self-efficacy, the more likely that person will undertake a task. When self-efficacy and self-sufficiency are poor, people avoid work [107]. Furthermore, organizations or school must guarantee that cyber hygiene knowledge is an factors that need to be take in consideration. As the results show above, researchers have tested that cyber hygiene knowledge has a significant relationship with cyber hygiene attitude then which will then lead to cyber hygiene behavior. The first approach is to educate Internet users, but organizations or schools also need to figure out how to modify their attitudes and behaviors when it comes to cyber hygiene. Based on the results, researchers may give some recommendations to those cybersecurity organizations or schools in order to increase the young users' knowledge of cyber hygiene which will lead them to have a good cyber hygiene attitude which will then lead them to practice good cyber hygiene behavior during COVID-19 to avoid cyber-attacks. University can take these results into consideration and implement new courses regarding cyber hygiene for the students.

Next, cyber hygiene awareness also gives the related organizations know that the awareness regarding cyber hygiene is not used in helping Internet users practice good cyber hygiene behavior. Based on the results, there show cyber hygiene awareness has no significant relationship with cyber hygiene attitude. So, those organizations can reduce their effort in organizing cybersecurity awareness for the younger because this is not useful in helping them to increase their attitude and behavior in practicing good cyber hygiene. In addition, cyber hygiene attitudes also become the things that need to take attention in this cyber world. This research shows that cyber hygiene attitude is positively related to cyber hygiene intention. This study demonstrates that attitude is a significant component in changing behavioral intentions which this results also compatible with the results done by past researchers. As a result show above, this study prove that cyber hygiene attitude will positively relate to the cyber hygiene intentions. So, it is recommended that people focus on the mindset component to help them progress from a weak link to a strong link in cybersecurity. Lastly, this research finds that cyber hygiene intention is also one of the important factor to affect the cyber hygiene behavior. In this study, researchers have made a results on cyber hygiene intention has a significant relationship with cyber hygiene behavior. So, it is important for organizations or schools increase the young Internet users' attitude on cyber hygiene which will lead them to have a strong intention in cyber hygiene behavior. People who have intentions of doing something will have the biggest chance they will take the correct actions during using the Internet.

Self-efficacy and cyber hygiene knowledge were revealed to be influencing factors in cyber hygiene attitudes in this study. Simultaneously, cyber hygiene intention is influenced by cyber hygiene attitude, which in turn influences cyber hygiene behavior. Furthermore, this research discovered that cyber hygiene attitude and intention are essential elements in determining cyber hygiene behavior.

In the field of research, the majority of previous studies have focused on cybersecurity behaviors, with only a few studies focusing on cyber hygiene behaviors. As a result, this study investigates the various elements that lead to cyber hygiene behavior, thus filling a gap in the present literature and providing further insights to help improve the cyber hygiene behavior during COVID-19 to avoid cyber-attacks.

5.4 Limitations of Study and Recommendations for Future Research

There are number of limitations of this study. Several constraints must be acknowledged and brought out by researchers during the research process in order to acknowledge and learn. However, these restrictions have no bearing on the significance of the findings, which serve as a foundation for future research.

First, this research takes an individualistic approach, dismissing the significance of environmental, technological, and social influences. Although personal factors are the most crucial in influencing a person's attitude, intention, and behavior, it has been suggested that the environment, technological, and social might have an impact on how people understand and respond to specific events. Therefore, future research should include the environmental, technological, and social factors to study in deep how individuals will be influenced by this three factors and how individuals actively change their attitude, intention and behavior based on the environment, technological and social factors. Besides, the study could also look into whether young and old Internet users are consistent in their proactive activities in different contexts.

Second, due to time limits, this research can only look at a small number of people (160 respondents). It is possible that such a small sample size is not indicative of the entire population of Malaysian Internet users. Hence, for better and more reliable results, future research should increase the sample size to better represent the population. On the other hand, researchers only target the UTAR students on the Kampar campus as the respondents for this study. It is impossible that UTAR students can represent all Internet users in Malaysia. So, researchers should expand the target population to students from other universities in Malaysia or other heavy Internet users such as employees in the population in future research to get a more accurate and reliable result.

Another flaw was uncovered during data analysis. The researchers discovered that a professional license was required to run the data because the study employed SmartPLS software, therefore a 30-day free trial was the only way to save money.

Forth, the surveys are conducted online, researchers cannot guarantee that the responses received are genuine. This is because convenience sampling introduces voluntary response bias into the study. Respondents may simply pass through the question, and their minds are constantly filling in agree or neutral. As a result, respondents in a rush who need to complete work fast may choose to answer questions at random or based on their own interpretation of the question. This is a subjective activity that is not acknowledged, and as a result, it will impair the correctness of the overall results. In order to overcome this limitation, future researchers must collect surveys using more methods, such as face-to-face interviews. A face-to-face interview can let the respondents answer and clarify more questions at the same time. To increase accuracy, researchers can obtain complete information, experience, thoughts, and perception from respondents. Researchers may receive unexpected responses from respondents through face-to-face interviews.

Finally, there is a limitation that finding respondents during the data collection process is difficult and time-consuming. Because the data is collected through online Google Form, as most students are now taking classes online. The researchers found it challenging to track the actual responses of respondents after it went live. This is due to the absence of physical confrontation, which minimizes the amount of effort required to complete the questionnaire. As a result, the findings of research studies may not fully reflect cyber hygiene behavior, intention, and attitude. Despite the widespread perception of internet platforms as more convenient, most people overlook, ignore, or even refuse to engage in questionnaires provided on social media. Therefore, researchers have to send questionnaires to the masses one by one or in small groups which ultimately time consuming and will drags down the overall data collection efficiency. In my recommendation, future researchers should distribute surveys through online or brick-and-mortar means, as this is a more genuine and approachable manner to get replies from the general public. This method is relatively effective at obtaining high-quality data while also allowing researchers to communicate more effectively with event participants.

5.6 Conclusion

In conclusion, this study can be used as a foundation for further research and understanding of cyber hygiene behavior during COVID-19 to avoid cyber-attacks. The results of the variable analysis are summarized in this paper, along with a discussion of the main findings. Besides, implications have been developed in order to give Internet users greater insights and recommendations for improving their cyber hygiene behavior when surfing the Internet. Lastly, limitations and recommendations are presented for researchers to improve future studies.

REFERENCES

[1] A. M. Abukari and E. K. Bankas, "Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond," *International Journal of Scientific & Engineering Research,* vol. 11, no. 4, 2020.

[2] R. Khweiled, M. Jazzar and D. Eleyan, "Cybercrimes during COVID -19 Pandemic," *I.J. Information Engineering and Electronic Business,* no. 2, pp. 1-10, 2021.

[3] A. Bendovschi, "Cyber Attacks - Trends, Patterns and Security Countermeasures," *Procedia Economics and Finance,* no. 28, pp. 24-31, 2015.

[4] J. M. Biju, N. Gopal and A. J. Prakash, "Cyber Attacks and Its Different Types," *International Research Journal of Engineering and Technology* , vol. 6, no. 3, pp. 4849-4852, 2019.

[5] Dekra, "Are You Dealing With A Higher Volume Of Cyber-Attacks Due To Covid-19," [Online]. Available: https://www.dekra.com/en/cyber-attacks-due-to-covid-19/. [Accessed 5 March 2022].

[6] Mctracy, "Why Student Cyber Hygiene Is Critical In The Education Industry," 2021. [Online]. Available: https://www.responsivetechnologypartners.com/2021/09/13/why-student-cyber-hygiene-is-critical-in-the-education-industry/. [Accessed 27 February 2022].

[7] A. R.Neigel, V. L.Claypoole, G. E.Waldfogle, S. Acharya and G. M.Hancock, "Holistic cyber hygiene education: Accounting for the human factors," *Computer & Security,* vol. 92, 2020.

[8] G. H. Tandon, "cyber hygiene," June 2019. [Online]. Available https://www.researchgate.net/publication/333532052_cyber_hygiene.

[9] N. Sundaresan, P. Seemma and M.Sowmiya, "Overview of Cyber Security,' *International Journal of Advanced Research in Computer and Communicatior Engineering*, vol. 7, no. 11, p. 4, 2018.

[10] M. Trevors and C. M. Wallen, "Cyber Hygiene: A Baseline Set of Practices,' 2017.

[11] Enisa, "Review of Cyber Hygiene," *European Union Agency For Network anc Information Security*, p. 24, 2016.

[12] D. Singh, N. P. Mohanty, S. Swagatika and S. Kumar, "Cyber-hygiene: The key Concept for Cyber Security in Cyberspace," *Test Engineering & Management*, vol. 83, p. 8, 2020.

[13] J. Devanesan, "Cybersecurity is top concern, as online threats mount in Malaysia by 82.5%," 2020. [Online]. Available https://techwireasia.com/2020/04/cybersecurity-is-top-concern-as-online-threats-mount-in-malaysia-by-82-5/. [Accessed 23 March 2022].

[14] G. Mathews, "Cyber Sphere is Here to Stay. How to Cope & Stay Safe?," 2022 [Online]. Available: https://www.espc2go.com/news/cyber-sphere-is-here-to-stay-how-to-cope-stay-safe/#:~:text=The%20study%20revealed%20that%2060,important%20than%20before%20the%20pandemic.. [Accessed 23 March 2022].

[15] A. Cain, M. Edwards and D. J. Still, "An exploratory study of cyber hygiene behaviors and knowledge," *Journal of Information Security and Applications*, vol 42, pp. 36-45, 2018.

[16] TechXplore, "The dangers of sharing personal information on social media,' 2020. [Online]. Available: https://techxplore.com/news/2020-05-dangers-personal-social-media.html.

[17] M. Yildirm and L. Mackie, "Encouraging users to improve password security anc memorability," *International Journal of Information Security (2019),* vol. 18, no 12, 2019.

[18] M. Whitty, J. Doodson, S. Creese and D. Hodges, "Individual Differences ir Cyber Security Behaviors: An Examination of Who Is Sharing Paawords,' *CYBERPSYCHOLOGY, BEHAVIOR, AND SOCIAL NETWORKING,* vol. 18, no 1, 2015.

[19] L. K. Kay, "Dirty, Dirty Boy: Malaysians Lack 'Cyber-Hygiene'," 2016. [Online] Available: https://www.digitalnewsasia.com/dirty-dirty-boy-malaysians-lack-cyber-hygiene. [Accessed 13 March 2022].

[20] OneLogin, "Six Types of Password Attacks & How to Stop Them," 2021 [Online]. Available: https://www.onelogin.com/learn/6-types-password-attacks [Accessed 13 March 2022].

[21] M. Glassman and M. Vandenwauver, "The psychology of password management A tradeoff between security and convenience," *Behaviour and Informatior Technology,* no. 29, pp. 233-244, 2010.

[22] I. Vayansky and S. A. Kumar, "Phishing – challenges and solutions," *Computer Fraud & Security,* no. 1, pp. 15-20, 2018.

[23] P. Syiemlieh, M. Golden, Khongsit and U. Sharma, "Phishing-An Analysis on the Types, Causes, Preventive Measuresand Case Studies in the Current Situation,' *IOSR Journal of Computer Engineering (IOSR-JCE),* pp. 01-08, 2015.

[24] L. Muniandy, B. Munianday and Z. Samsudin, "Cyber Security Behaviour among Higher Education Students in Malaysia," *Journal of Information Assurance & Cybersecurity,* vol. 2017, no. 2017, p. 13, 2017.

[25] C. B. Devi and N. R. Roy, "Internet Use among University Students: A Case Study of Assam University Silchar," *Pratidhwani – A Journal of Humanities and,* vol. I, no. II, pp. 183-202, 2012.

[26] A. f. M. Ayub, W. Hamid and M. Nazawi, "Use of internet for academic purposes among students in Malaysian institutions of higher education," *The Turkish Online Journal of Educational,* vol. 13, no. 1, pp. 232-241, 2014.

[27] Y. Rezgui and A. Marks, "Information security awareness in higher education: An exploratory study," *Computers & Security,* vol. 27, pp. 241-253, 2008.

[28] R. Sani, "Curbing cyber threats in online learning," 13 May 2020. [Online].

[29] P. Biolcheva and M. Molhova, "Data Loss Prevention in Higher Education," Italy, 2021.

[30] I. Corradini and E. Nardelli, "Awareness In The Online Use of Digital Technologies of Italian Students," Spain, 2018.

[31] N. Shah and M. Farik, "Ransomware-Threats, Vulnerabilities And Recommendations," *International Journal of Scientific & Technology Research,* vol. 6, no. 6, pp. 307-309, 2017.

[32] S. Panda, E. Panaousis, G. Loukas and C. Laoudias, "Optimizing Investments in Cyber Hygiene for Protecting Helathcare Users".

[33] M. Beech, "COVID-19 Pushes Up Internet Use 70% And Streaming More Than 12%, First Figures Reveal," 2020. [Online]. Available: https://www.forbes.com/sites/markbeech/2020/03/25/covid-19-pushes-up-internet-use-70-streaming-more-than-12-first-figures-reveal/?sh=105da9be3104. [Accessed 10 April 2022].

[34] G. A. Supayah and J. Ibrahim, "An Overview of Cyber Security in Malaysia," *Kuwait Chapter of Arabian Journal of Business and Management Review ,* vol. 6 no. 4, pp. 12-20, 2016.

[35] L. Bosnjak and B. Brumen, "Examining Security and Usability Aspects of Knowledge-based Authentication Methods," Croatia, 2019.

[36] K. Curran, J. Doherty, A. Mccann and G. Turkington, "Good Practice For Strong Passwords," *The EDP Audit, Control, and Security Nesletter,* vol. 44, no. 5, pp 1-13, 2011.

[37] D. Charoen, "Password Security," *International Journal of Security (IJS),* vol. 8, no. 1, 2014.

[38] J. L. Jenkins, M. Grimes and P. B. Lowry, "Improving Password Cybersecurity Through Inexpensive and Minimally Invasive Means: Detecting and Deterring Password Reuse Through Keystroke-Dynamics Monitoring and Just-in-Time Fear Appeals," *Information Technology for Development,* vol. 20, no. 2, pp. 196-213, 2013.

[39] R. Morrison, "Password:'123456' and 'password' Are Still Among The Most Popular Passwords in the world.," 2021. [Online]. Available: https://www.dailymail.co.uk/sciencetech/article-10209349/Passwords-123456-password-popular.html. [Accessed 14 March 2022].

[40] M. Abomhara and G. M. Køien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," *Journal of Cyber Security,* vol 4, pp. 65-88, 2015.

[41] R. Heartfield and G. Loukas, "Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework," *Computers & Security,* 2018.

[42] A. Ghazvini and Z. Shukur, "Awareness Training Transfer and Information Security Content Development for Healthcare Industry," *(IJACSA) International Journal of Advanced Computer Science and Applications,* , vol. 7, no. 5, 2016.

[43] J. M. Such, P. Ciholas, A. Rashid, J. Vidler and T. Seabrook, "Basic Cyber Hygiene: Does it Work?," *Computer,* vol. 52, no. 4, pp. 21-31, 2019.

[44] J. L. T. Yi, T. W. Sen and N. T. C. Yao, "The Relationship Between Fear Of Failure, Creative Process Engagement, And Self-Rated Creatvity Among Malaysian Undergraduates," Faculty of Arts and Social Science University Tunku Abdul Rahman, Kampar, 2020.

[45] I. Ajzen, "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes,* vol. 50(2), no. DOI: 10.1016/0749-5978(91)90020-T, pp. 179-211, 1991.

[46] S. Burns and L. Roberts, "Applying the Theory of Planned Behaviour to Predicting Online Safety Behaviour," *Crime Prevention and Community Safety,* vol. 15, no. 1, pp. 48-64, 2013.

[47] R. M. Bergner, "What is Behavior? And so What?," *New Ideas in Psychology,* vol. 29, no. 2, pp. 147-155, 2011.

[48] M. Zwilling, G. Klien, D. Lesjak, L. Wiechetek, F. Cetin and H. N. Basim, "Cyber Security Awareness, Knowledge and Behavior: A Comparative Study," *Journal of Computer Information Systems*, 2020.

[49] D. Kelley, "Investigation of Attitudes Towards Security Behaviors," *McNair Research Journal SJSU,* vol. 14, no. 10, 2018.

[50] A. Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Countermeasures," *Procedia Economics and Finance,* vol. 28, pp. 24-31, 2015.

[51] M. Rajalingam, S. A. Alomari and P. Sumari, "Prevention of Phishing Attacks Based on Discriminative Key," *International Journal of Computer Science and Security (IJCSS),* vol. 6, no. 1, 2012.

[52] K. Aytes and T. Conolly, "A Research Model for Investigating Human Behavior Related to Computer Security," *AMCIS 2003 Proceedings,* p. 260, 2003.

[53] C. Conetta, "Individual Differences in Cyber Security," *McNair Research Journal SJSU,* vol. 15, no. 4, 2019.

[54] C. Yoon, J.-W. Hwang and R. Kim, "Exploring factors that influence students behaviors in information security," *Journal of Information Systems Education* , vol. 23, no. 4, pp. 407-416, 2012.

[55] L. C. d. Kok, D. Oosting and M. Spruit, "The Influence of Knowledge and Attitude on Intention to Adopt Cybersecure Behaviour," *Information & Security*, vol. 46, no. 3, pp. 251-266, 2020.

[56] S. Talib, S. Furnell and N. L. Clarke, "An Analysis of Information Security Awareness within Home and Work Environments," *Conference Paper,* 2014.

[57] tenable, "New Study: Many Consumers Lack Understanding of Basic Cyber Hygiene," 18 December 2017. [Online]. Available https://www.tenable.com/blog/new-study-many-consumers-lack-understanding-of-basic-cyber-hygiene.

[58] M. Gibbs, "Why Cyber Awareness Isn’t Enough," 2 May 2019. [Online] Available: https://www.cybintsolutions.com/why-cyber-awareness-isnt-enough/.

[59] R. Dodge, C. Carver and A. J. Ferguson, "Phishing for user security awareness," *Computers & Security,* vol. 26, no. 1, pp. 73-80, 2007.

[60] R. A. Rahman and N. B. Omar, "Perception and Awareness of Young Internet Users towards Cybercrime: Evidence from Malaysia," *Journal of the Social Sciences*, vol. 11, no. 4, pp. 395-404, 2015.

[61] M. Anyunes, C. Silva and F. Marques, "An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context," *Appl.Sci.*, vol. 11, no. 11269, pp. 2-18, 2021.

[62] G. W. Nie, H. S. Ying, L. Serene and W. L. Jian, "Determinants of Food Delivery Apps (FDA) Adoption Reluctance Among Generation Y in Malaysia," Faculty of Business and Finance Department of Marketing, Kampar, 2021.

[63] H.-S. Rhee, C. Kim and Y. U. Ryu, "Self-efficacy in information security: Its influence on end users' information security practice behavior," *Computers & Security,* vol. 28, no. 8, pp. 816-826, 2009.

[64] D. R.-A. "Knowledge, Attitude, Then Behavior," 2020. [Online]. Available https://respons-ability.net/knowledge-attitude-behavior/. [Accessed 14 March 2022].

[65] S. Gorman and J. M.Gorman, "Does Raising Awareness Change Behavior?," 2018. [Online]. Available: https://www.psychologytoday.com/us/blog/denying-the-grave/201806/does-raising-awareness-change-behavior. [Accessed 15 March 2022].

[66] D. Malandrino, V. Scarano and R. Spinelli, "How Increased Awareness Can Impact Attitudes and Behaviors toward Online Privacy Protection," *2013 International Conference on Social Computing,* pp. 57-62, 2013.

[67] G.-W. Bock, R. W.Zmud and Y.-G. Kim, "Behavioral Intention Formation In Knowledge Sharing: Examine the Roles of Extrinsic Motivators, Social-Psychological Forces, and Organizational Climate," *MIS Quarterly,* vol. 29, no. 1, pp. 87-111, 2005.

[68] S. I. Tamrin, A. A. Norman and S. Hamid, "Intention to share: the relationship between cybersecurity behaviour and sharing specific content in Facebook," *InformationResearch,* vol. 26, no. 1, 2021.

[69] S. I. Tamrin, A. A. Norman and S. Hamid, "Intention to Share: The Relationship Between Cybersecurity Behaviour and Sharing Specific Content in Facebook," *Information Research,* vol. 26, no. 1, 2021.

[70] S. McCombes, "Research Design | A Step-by-Step Guide with Examples," 2021. [Online]. Available: https://www.scribbr.com/methodology/research-design/. [Accessed 18 March 2022].

[71] F. B. "Descriptive Research Designs: Types, Examples & Methods," 2021. [Online]. Available: https://www.formpl.us/blog/descriptive-research. [Accessed 19 March 2022].

[72] S. M. S. Kabir, "Methods of data collection," *Basic Guidelines for Research: An Introductory Approach for All Disciplines*, pp. 201-275, 2016.

[73] N. J. Salkind, "Primary Data Source," *Encyclopedia of Research Design*, 2010.

[74] F. S. Martins, J. A. C. d. Cunha and F. A. R. Serra, "Secondary Data in Research – Uses and Opportunities," *Revista Ibero-Americana de Estratégia*, vol. 17, no. 4, pp. 01-04, 2018.

[75] U. Sekaran and R. Bougie, "Research Methods For Business: A Skill Building Approach," *Business & Management Special Topics*, 2016.

[76] Zikmund, Babin, Carr and Griffin, "Business Research Methods," *Eight Edition*, 2010.

[77] C. Ugwu, C. Ani, M. Ezema, C. Asogwa, U. Ome, A. Obayi, D. Ebem, A. Atanda and E. Ukwandu, "Towards Determining the Effect of Age and Educational Level on Cyber-Hygiene," 2021.

[78] S. McCombes, "Sampling Methods | Types and Techniques Explained," 2019. [Online]. Available: https://www.scribbr.com/methodology/sampling-methods/ [Accessed 19 March 2022].

[79] J. F. Hair, "Multivariate Data Analysis: An Overview," *In: Lovric M. (eds) International Encyclopedia of Statistical Science. Springer, Berlin, Heidelberg.*, 2011.

[80] D. Pathavi, M. R. R. Adam and Y. Bustaman, "Analysis of Factors Affecting the Green Purchase Intention of Electric Motorcycle: Case Study of Selis," *International Conference on Global Innovation and Trends in Economy 2020*, vol. 3, no. 1, pp. 458-476, 2020.

[81] Z. A. Hassan, P. Schattner and D. Mazza, "Doing A Pilot Study: Why Is It Essential?," *Malaysian Farm Physician,* vol. 1, no. 2, pp. 70-73, 2006.

[82] QuestionPro, "Online Data Collection using Research Panel," [Online]. Available: https://www.questionpro.com/online-data-collection-research-panel.html#:~:text=The%20advantage%20of%20online%20data,received%20is%20usually%20more%20accurate.. [Accessed 21 March 2022].

[83] M. A. Hertzdog, "Considerations in determining sample size for pilot studies," *Research in nursing & health,* vol. 31, no. 2, pp. 180-191, 2008.

[84] S. R. M. D. "Learn About Structural Equation Modeling in SmartPLS with Data From the Customer Behavior in Electronic Commerce Study in Ecuador," 2019 [Online]. Available: https://methods.sagepub.com/base/download/DatasetHowToGuide/sem-customer-behavior-electronics-ecuador#:~:text=Average%20of%20variance%20extracted%20(AVE,variance%20due%20to%20measurement%20error.. [Accessed 15 August 2021].

[85] K. S. Taber, "The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education," *Res Sci Educ,* vol. 48, pp. 1273-1296, 2017.

[86] C. S. Wells and J. A. Wollack, "An Instructor's Guide to Understanding Test Reliability," *Testing & Evaluation Services University of Wisconsin,* 2003.

[87] K. Kwong and K. Wong, "Partial Least Squares Structural Equation Modeling (PLS-SEM) Techniques Using SmartPLS," *Marketing Bulletin,* vol. 24, no. 1, 2013.

[88] T. Taylor and S. Geldenhuys, "Using Partial Least Squares to Measure Tourism Students' Satisfaction with Work-Integrated Learning," in *Tourism - Perspectives and Practices*, S. Sabah, Ed., intechopen, 2019.

[89] N. K. Malhotra and M. Peterson, Basic marketing research: A decision-making, 3rd ed., Pearson Education, 2009.

[90] Y. Fan, J. Chen, G. Shirkey, R. John, S. R. Wu, H. Park and C. Shao, "Applications of structural equation modeling (SEM) in ecological studies: an updated review," *Ecological Processes*, 2016.

[91] T. Sander and P. L. Teh, "SmartPLS for the human resources field to evaluate," Riga, 2014.

[92] M. G. Larson, "Descriptive Statistics and Graphical Displays," *Circulation,* vol. 114, pp. 76-81, 2006.

[93] J. Katzer, K. Cook and W. Crouch, Evaluating Information: A Guide for Users of Social Science Research, 4 ed., Jenson Books Inc, 1998.

[94] J. Henseler, C. M. Ringle and R. R. Sinkovics, "The use of partial least squares path modeling in international marketing," *New Challenges to International Marketing,* pp. 277-319, 2009.

[95] W. W. Chin, " The partial least squares approach to structural equation modeling.," *Modern methods for business research,* pp. 295-336, 1998.

[96] J. R. A. Santos, "Cronbach's alpha: A tool for assessing the reliability of scales," *Journal of Extension,* vol. 37, no. 2, pp. 1-5, 1999.

[97] Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *Journal of marketing research,* pp. 39-50, 1981.

[98] J. F. Hair, J. J. Risher, M. Sarstedt and C. M. Ringle, "When to use and how to report the results of PLS-SEM," *European Business Review,* vol. 31, no. 1, pp. 2-24, 2019.

[99] D. Ramos, "The Advantages and Limitations of Gantt Charts in Project Management," smartsheet, 03 May 2021. [Online]. Available https://www.smartsheet.com/content/gantt-chart-pros-cons. [Accessed 14 April 2022].

[100] N. Guenole and A. Brown, "The consequences of ignoring measurement invariance for path coefficients in structural equation models," *Front Psychol,* vol 5, p. 980, 2014.

[101] L. Terry and K. Kelly, "Sample size planning for composite reliability coefficients: accuracy in parameter estimation via narrow confidence intervals," *British Journal of Mathematical and Statistical Psychology,* vol. 65, no. 3, pp 371- 401, 2012.

[102] D. Alarcón and J. A. Sánchez, "Assessing convergent and discriminant validity in the ADHD-R IV rating scale: User-written commands for Average Variance Extracted (AVE), Composite Reliability (CR), and Heterotrait-Monotrait ratio of correlations (HTMT)," Universidad Pablo de Olavide, 2015.

[103] M. R. A. Hamid, W. Sami and M. H. M. Sidek, "Discriminant Validity Assessment: Use of Fornell & Larcker criterion versus HTMT Criterion," *Journal of Physics*, 2017.

[104] J. Kaur and N. Mustafa, "Examining the effects of knowledge, attitude anc behaviour on information security awareness: A case on SME," Malaysia, 2013.

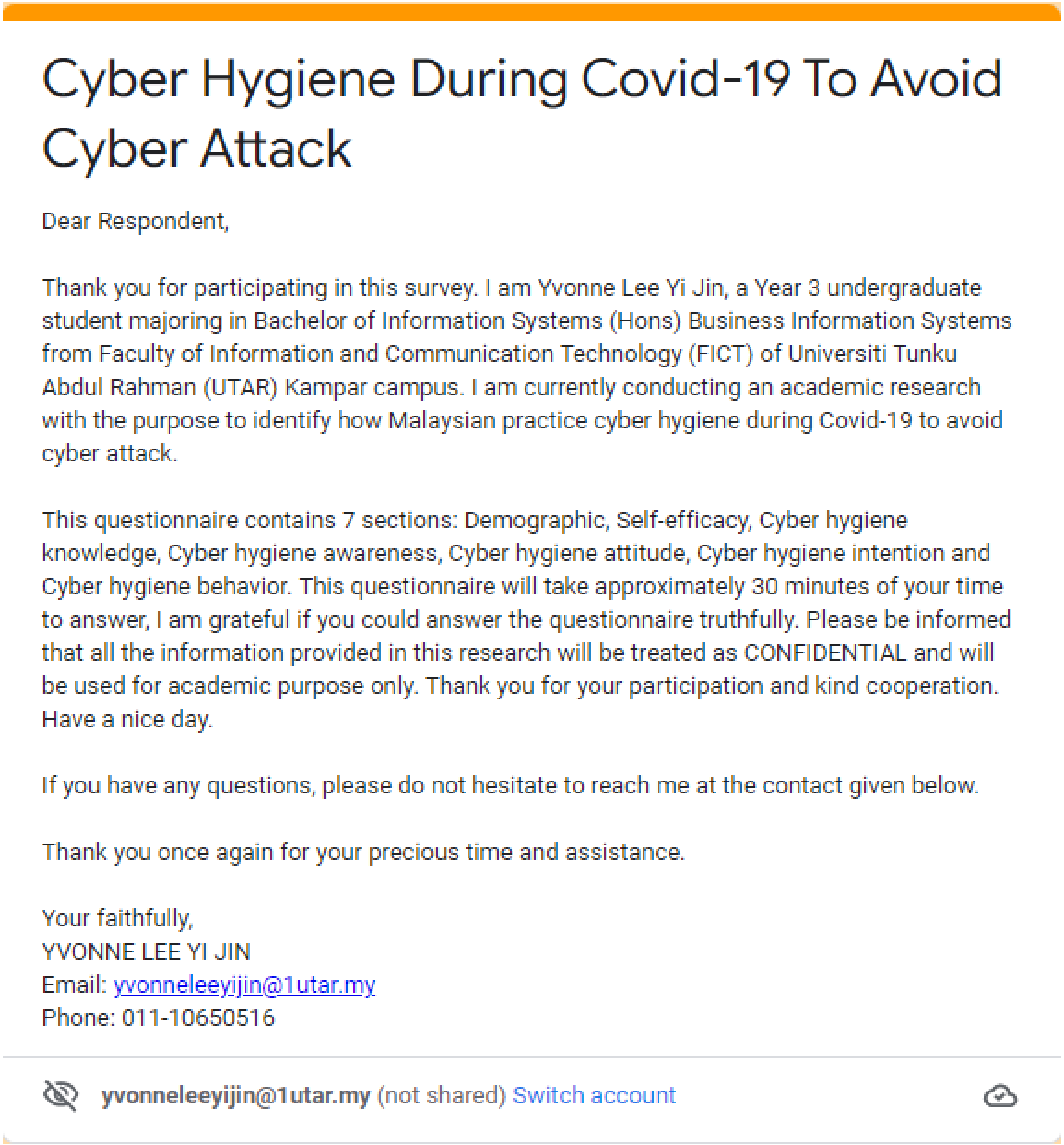
[105] J. Shropshire, M. Warkentin and S. Sharma, "Personality, attitudes, anc intentions: Predicting initial adoption of information security behavior,' *Computers & Security,* vol. 49, pp. 177-191, 2015.

[106] J. Sauro, "Do Attitudes Predict Behavior?," 2019. [Online]. Available https://measuringu.com/attitudes-behavior/. [Accessed 4 April 2022].

[107] S. Kalhoro, M. Rehman, V. A. Ponnusamy and F. B. Shaikh, "Extracting Key Factors of Cyber Hygiene Behavior Among Software Engineers," vol. 9, pp 99339-99363, 2021.

APPENDIX

A.1 Questionnaire Sample



Cyber Hygiene During Covid-19 To Avoid Cyber Attack

Dear Respondent,

Thank you for participating in this survey. I am Yvonne Lee Yi Jin, a Year 3 undergraduate student majoring in Bachelor of Information Systems (Hons) Business Information Systems from Faculty of Information and Communication Technology (FICT) of Universiti Tunku Abdul Rahman (UTAR) Kampar campus. I am currently conducting an academic research with the purpose to identify how Malaysian practice cyber hygiene during Covid-19 to avoid cyber attack.

This questionnaire contains 7 sections: Demographic, Self-efficacy, Cyber hygiene knowledge, Cyber hygiene awareness, Cyber hygiene attitude, Cyber hygiene intention and Cyber hygiene behavior. This questionnaire will take approximately 30 minutes of your time to answer, I am grateful if you could answer the questionnaire truthfully. Please be informed that all the information provided in this research will be treated as CONFIDENTIAL and will be used for academic purpose only. Thank you for your participation and kind cooperation. Have a nice day.

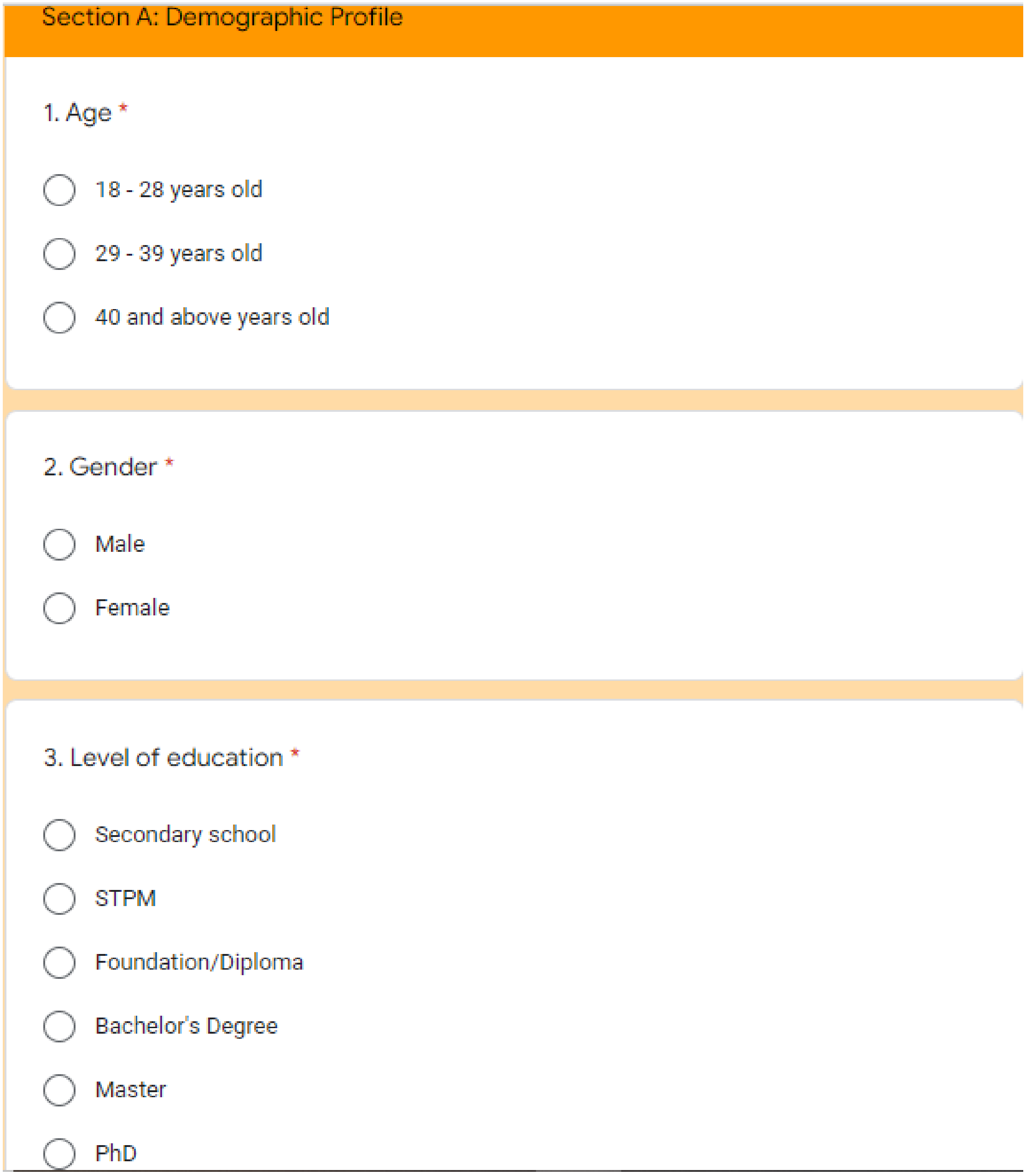
If you have any questions, please do not hesitate to reach me at the contact given below.

Thank you once again for your precious time and assistance.

Your faithfully,
YVONNE LEE YI JIN
Email: yvonneleeyijin@1utar.my
Phone: 011-10650516

yvonneleeyijin@1utar.my (not shared) Switch account

APPENDIX



Section A: Demographic Profile

1. Age *

○ 18 - 28 years old

○ 29 - 39 years old

○ 40 and above years old

2. Gender *

○ Male

○ Female

3. Level of education *

○ Secondary school

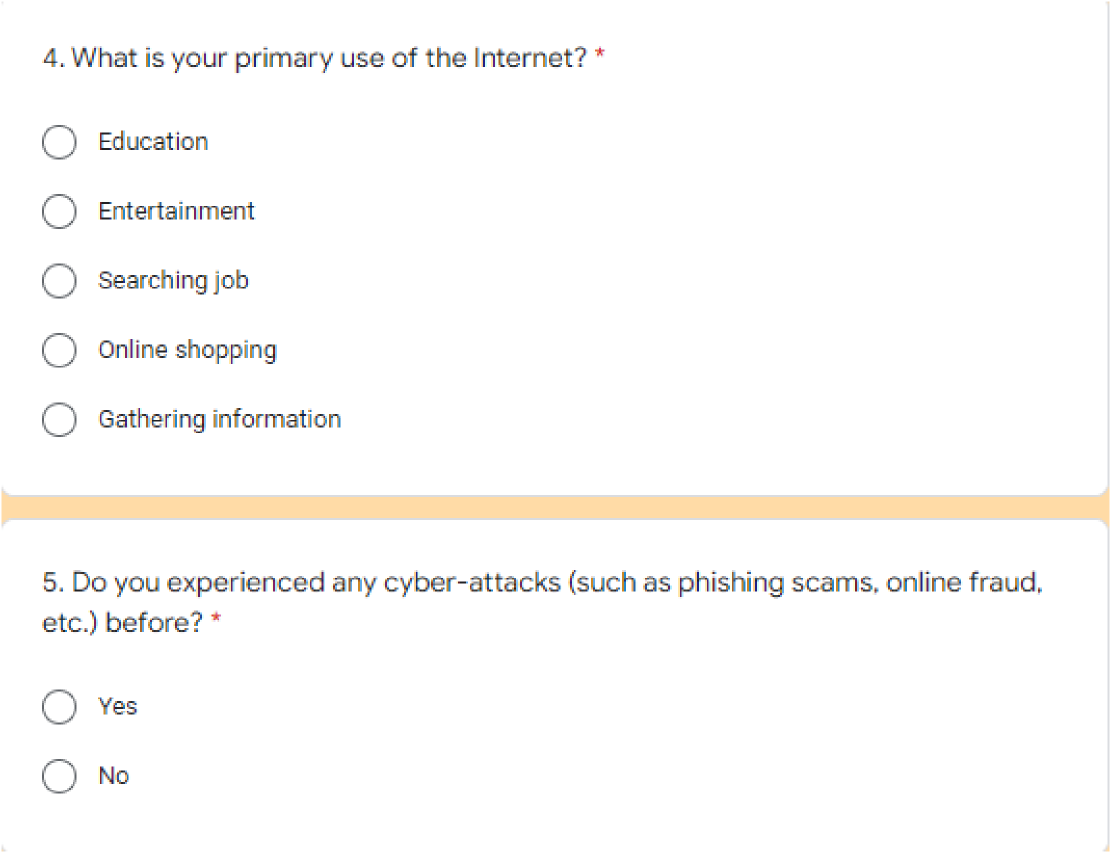
○ STPM

○ Foundation/Diploma

○ Bachelor's Degree

○ Master

○ PhD



4. What is your primary use of the Internet? *

○ Education

○ Entertainment

○ Searching job

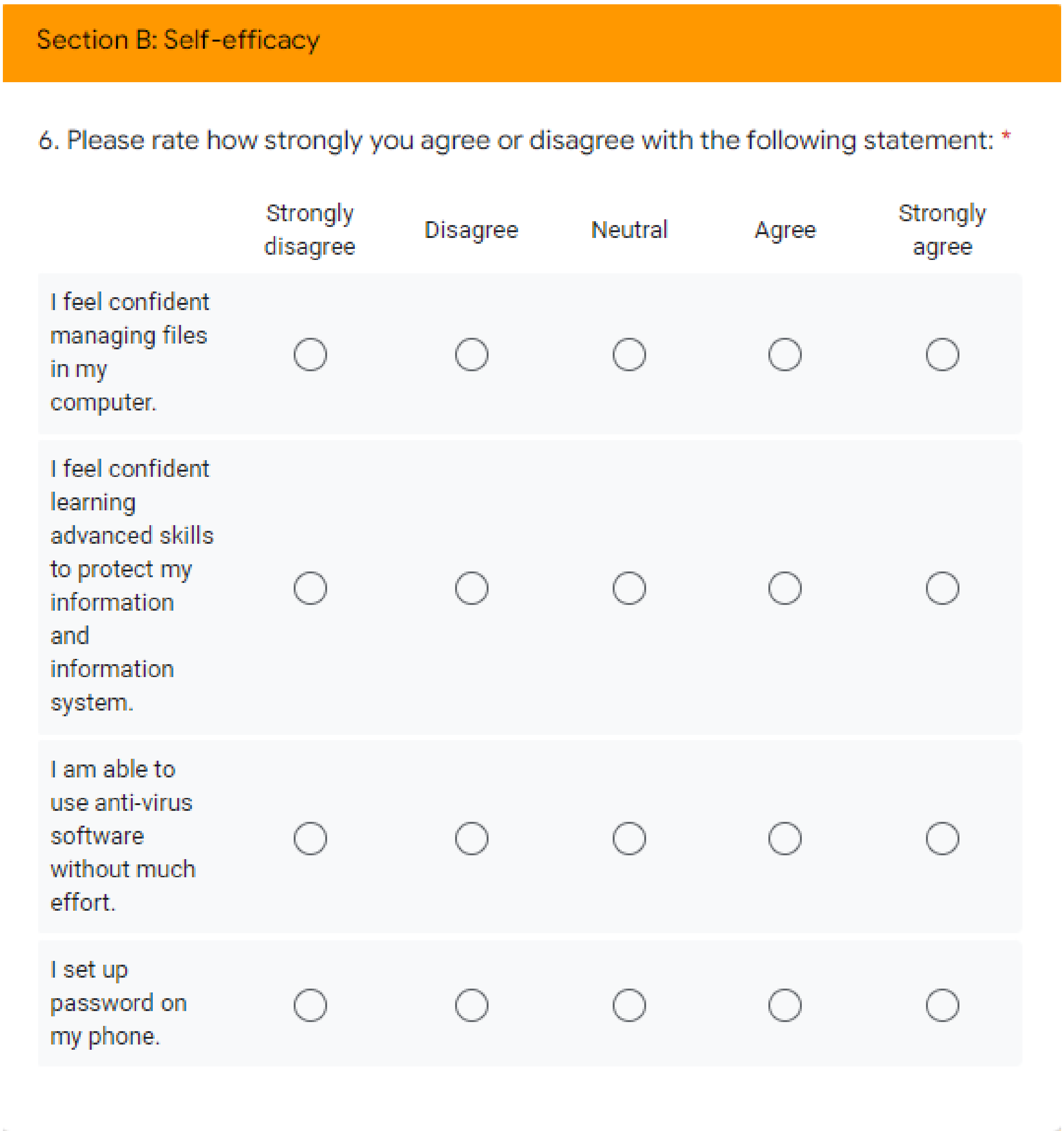
○ Online shopping

○ Gathering information

5. Do you experienced any cyber-attacks (such as phishing scams, online fraud, etc.) before? *

○ Yes

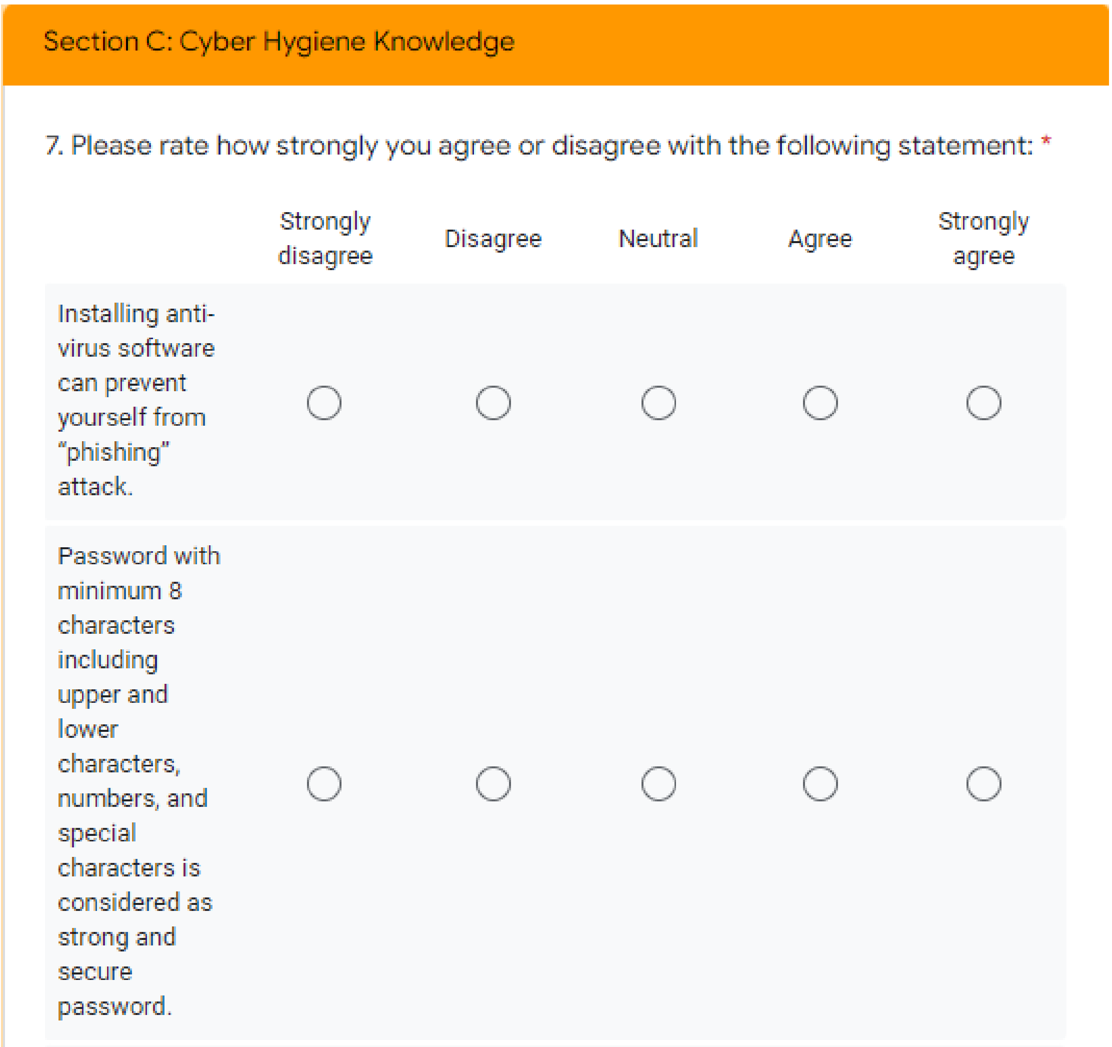
○ No



Section B: Self-efficacy

6. Please rate how strongly you agree or disagree with the following statement: *

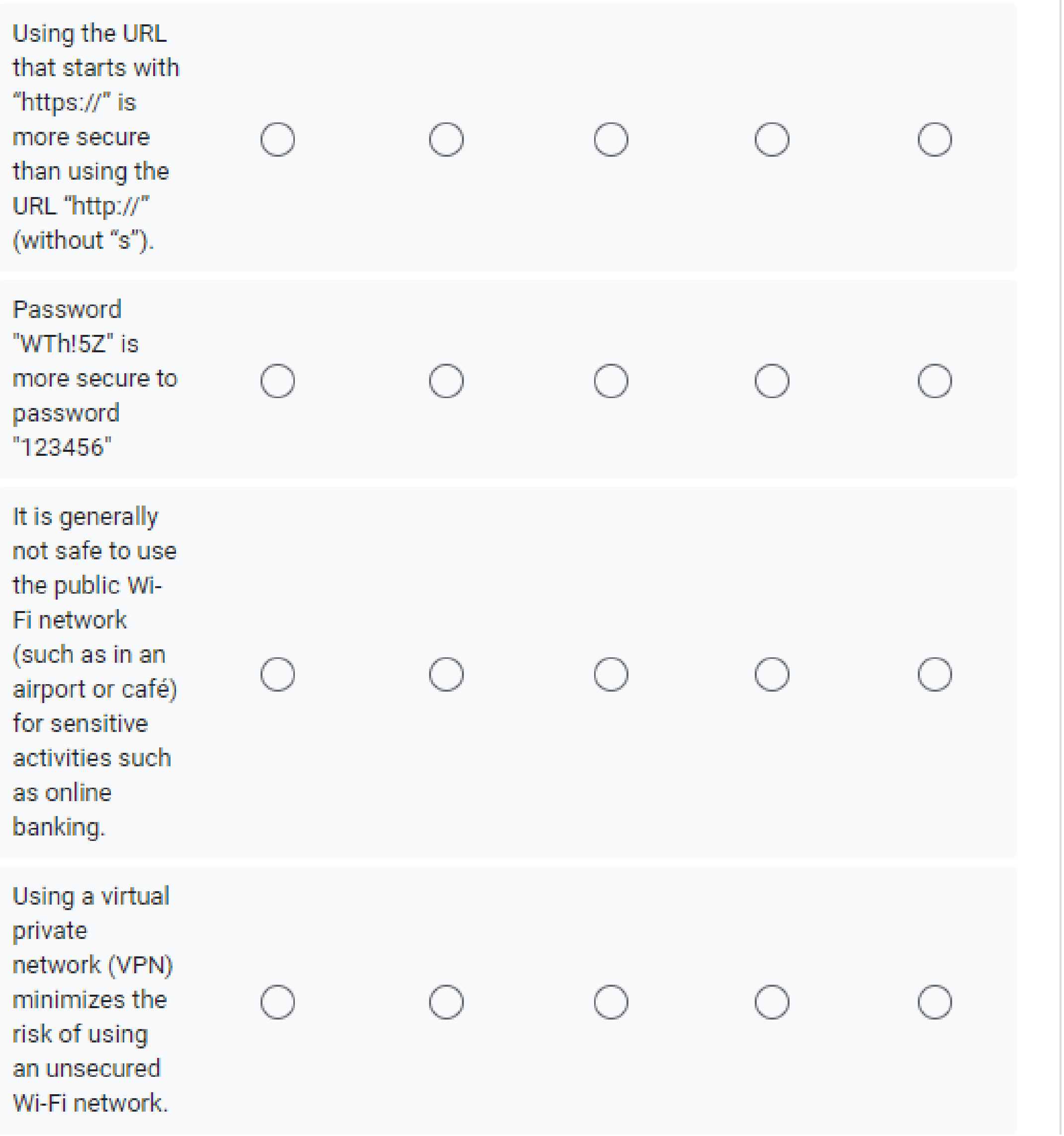
	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
I feel confident managing files in my computer.	○	○	○	○	○
I feel confident learning advanced skills to protect my information and information system.	○	○	○	○	○
I am able to use anti-virus software without much effort.	○	○	○	○	○
I set up password on my phone.	○	○	○	○	○



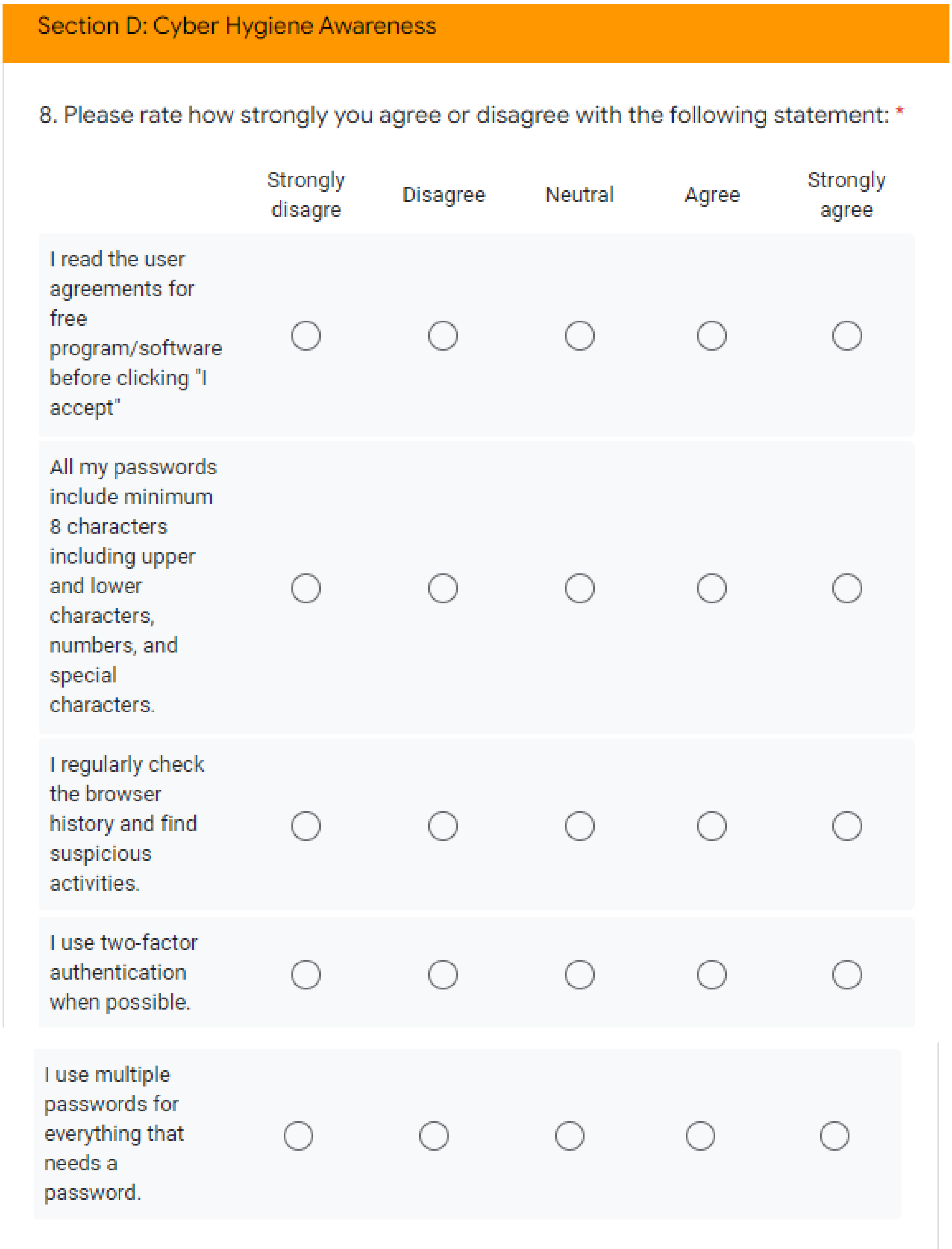
Section C: Cyber Hygiene Knowledge

7. Please rate how strongly you agree or disagree with the following statement: *

	Strongly disagree	Disagree	Neutral	Agree	Strongly agree
Installing anti-virus software can prevent yourself from “phishing” attack.	○	○	○	○	○
Password with minimum 8 characters including upper and lower characters, numbers, and special characters is considered as strong and secure password.	○	○	○	○	○



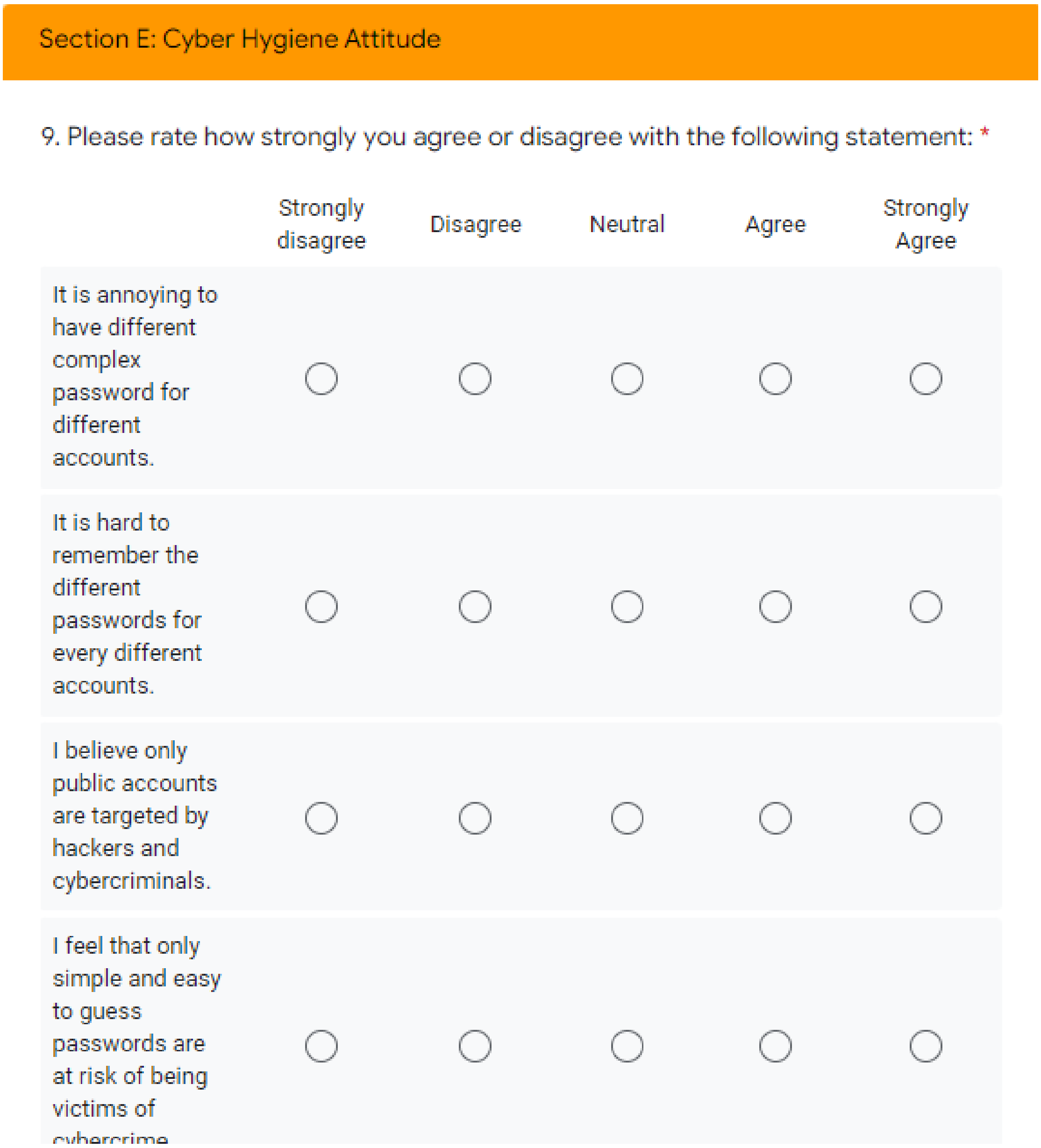
Using the URL that starts with “https://” is more secure than using the URL “http://” (without “s”).	○	○	○	○	○
Password "WTh!5Z" is more secure to password "123456"	○	○	○	○	○
It is generally not safe to use the public Wi-Fi network (such as in an airport or café) for sensitive activities such as online banking.	○	○	○	○	○
Using a virtual private network (VPN) minimizes the risk of using an unsecured Wi-Fi network.	○	○	○	○	○



Section D: Cyber Hygiene Awareness

8. Please rate how strongly you agree or disagree with the following statement: *

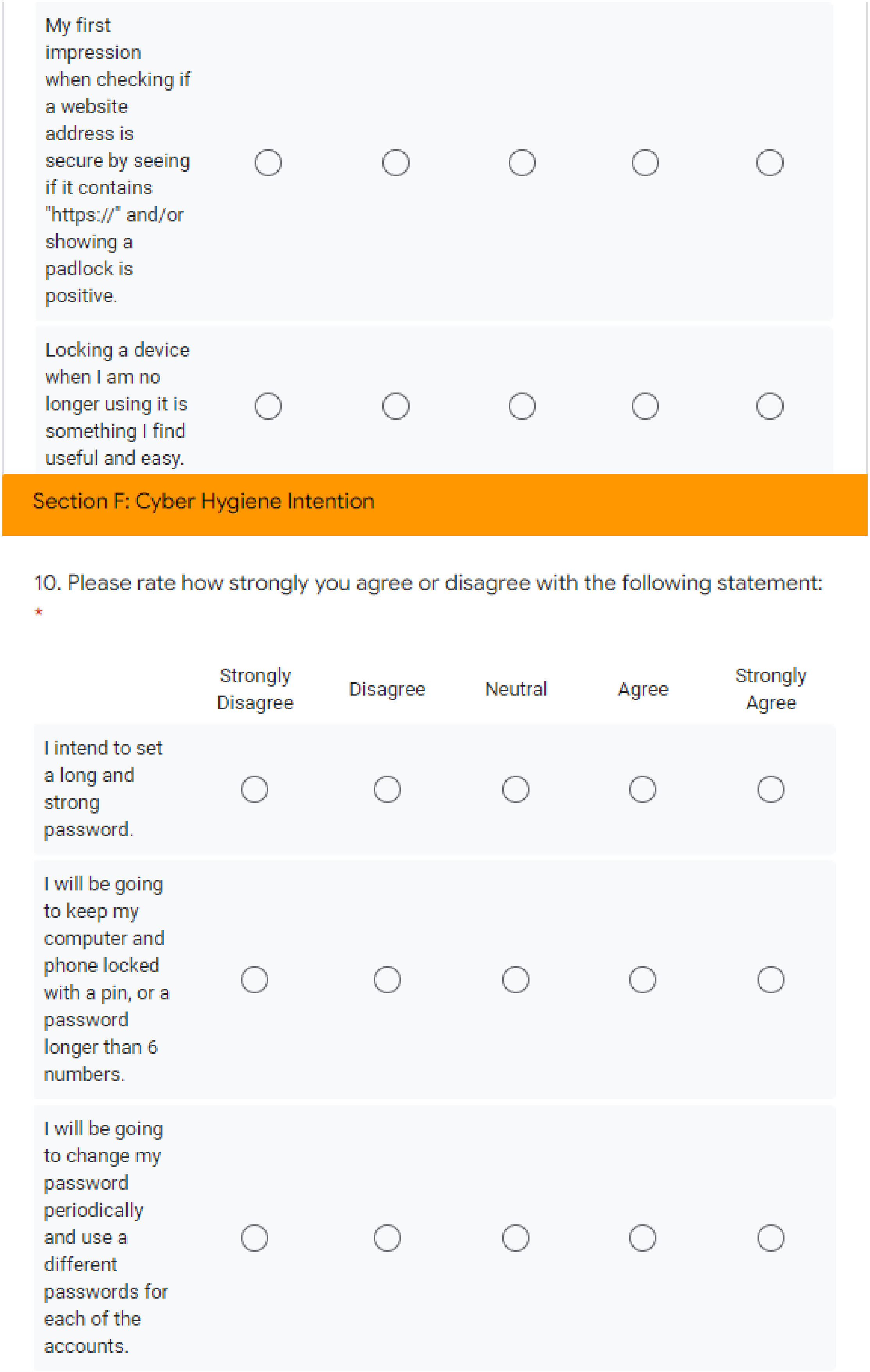
	Strongly disagre	Disagree	Neutral	Agree	Strongly agree
I read the user agreements for free program/software before clicking "I accept"	○	○	○	○	○
All my passwords include minimum 8 characters including upper and lower characters, numbers, and special characters.	○	○	○	○	○
I regularly check the browser history and find suspicious activities.	○	○	○	○	○
I use two-factor authentication when possible.	○	○	○	○	○
I use multiple passwords for everything that needs a password.	○	○	○	○	○



Section E: Cyber Hygiene Attitude

9. Please rate how strongly you agree or disagree with the following statement: *

	Strongly disagree	Disagree	Neutral	Agree	Strongly Agree
It is annoying to have different complex password for different accounts.	○	○	○	○	○
It is hard to remember the different passwords for every different accounts.	○	○	○	○	○
I believe only public accounts are targeted by hackers and cybercriminals.	○	○	○	○	○
I feel that only simple and easy to guess passwords are at risk of being victims of cybercrime	○	○	○	○	○

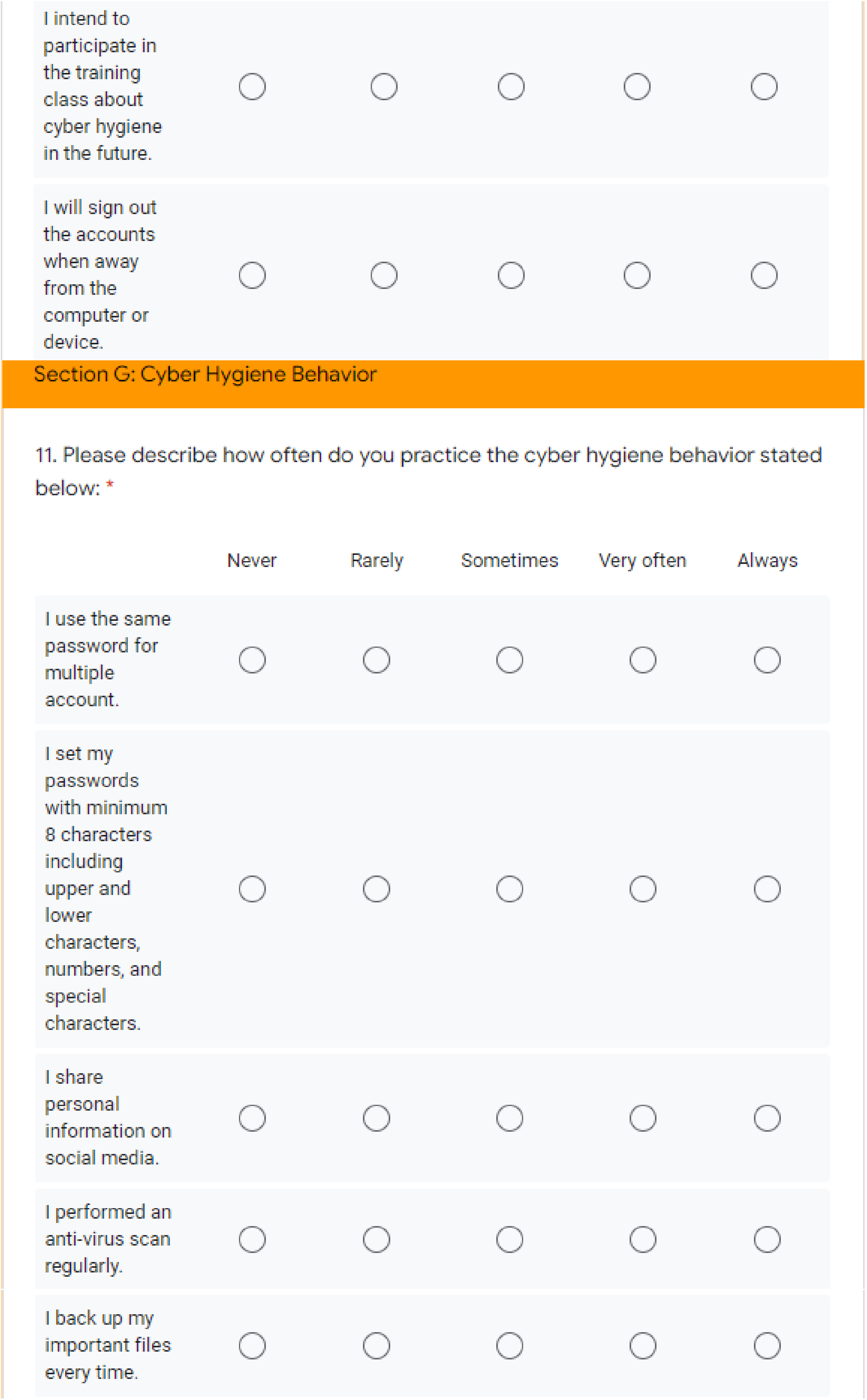


My first impression when checking if a website address is secure by seeing if it contains "https://" and/or showing a padlock is positive.	○	○	○	○	○
Locking a device when I am no longer using it is something I find useful and easy.	○	○	○	○	○

Section F: Cyber Hygiene Intention

10. Please rate how strongly you agree or disagree with the following statement:
*

	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I intend to set a long and strong password.	○	○	○	○	○
I will be going to keep my computer and phone locked with a pin, or a password longer than 6 numbers.	○	○	○	○	○
I will be going to change my password periodically and use a different passwords for each of the accounts.	○	○	○	○	○



I intend to participate in the training class about cyber hygiene in the future.	○	○	○	○	○
I will sign out the accounts when away from the computer or device.	○	○	○	○	○

Section G: Cyber Hygiene Behavior

11. Please describe how often do you practice the cyber hygiene behavior stated below: *

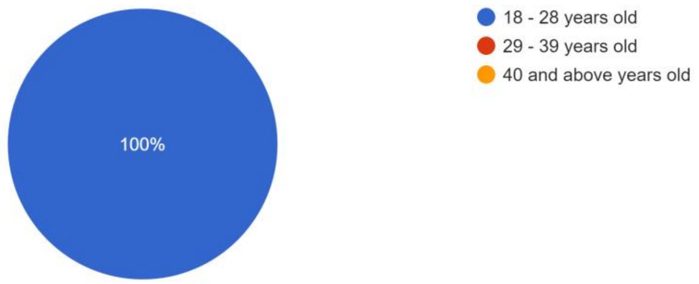
	Never	Rarely	Sometimes	Very often	Always
I use the same password for multiple account.	○	○	○	○	○
I set my passwords with minimum 8 characters including upper and lower characters, numbers, and special characters.	○	○	○	○	○
I share personal information on social media.	○	○	○	○	○
I performed an anti-virus scan regularly.	○	○	○	○	○
I back up my important files every time.	○	○	○	○	○

A.2 Questionnaire Results

Section A: Demographic Profile

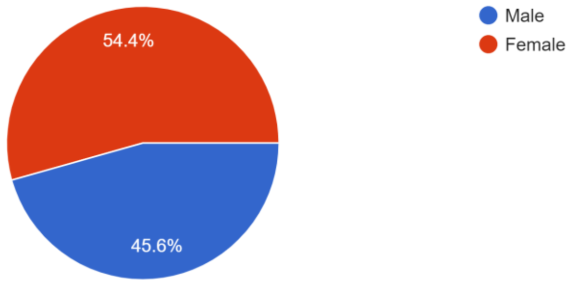
1. Age

160 responses



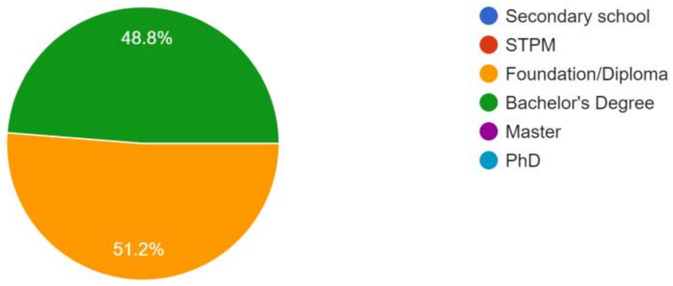
2. Gender

160 responses



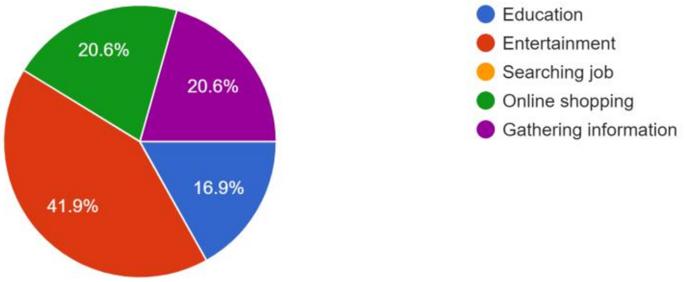
3. Level of education

160 responses



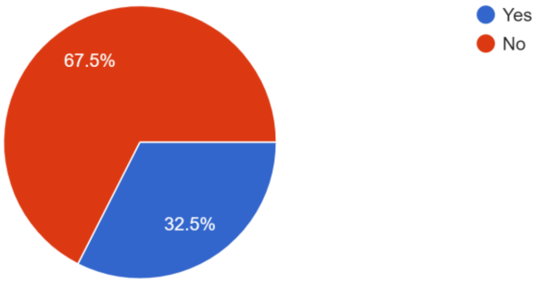
4. What is your primary use of the Internet?

160 responses



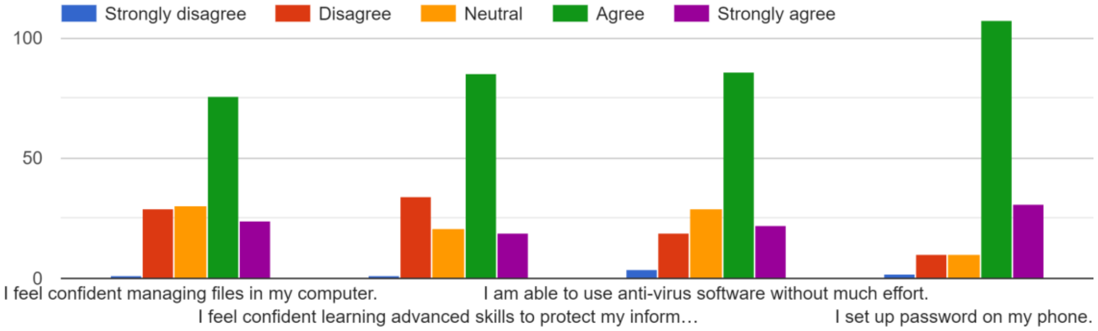
5. Do you experienced any cyber-attacks (such as phishing scams, online fraud, etc.) before?

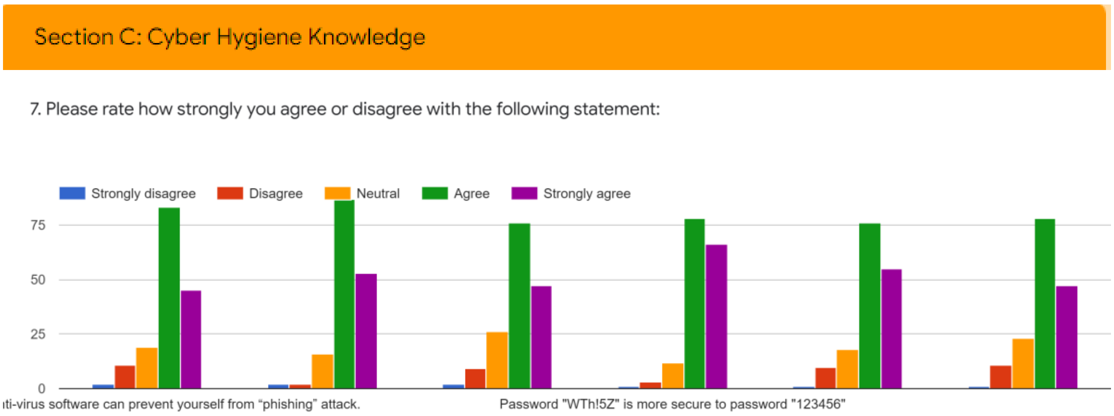
160 responses



Section B: Self-efficacy

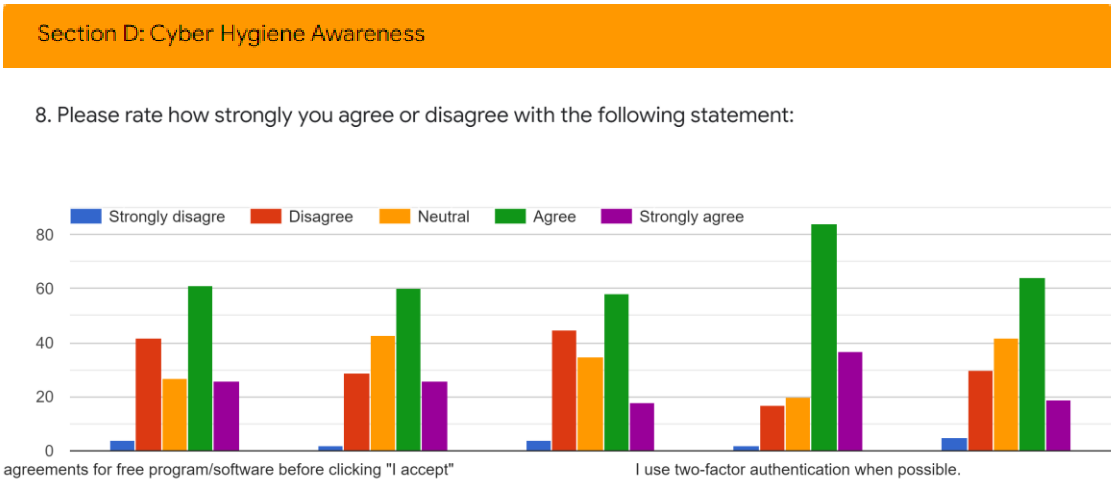
6. Please rate how strongly you agree or disagree with the following statement:





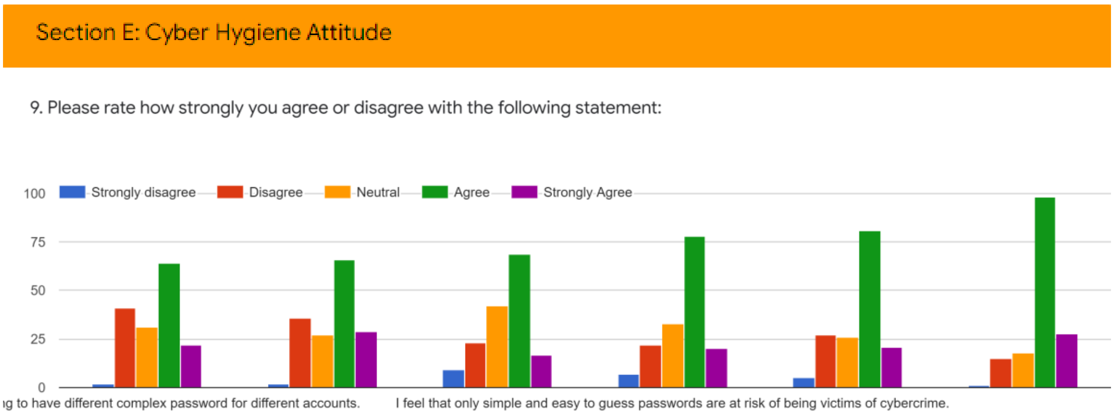
Section C: Cyber Hygiene Knowledge

7. Please rate how strongly you agree or disagree with the following statement:



Section D: Cyber Hygiene Awareness

8. Please rate how strongly you agree or disagree with the following statement:

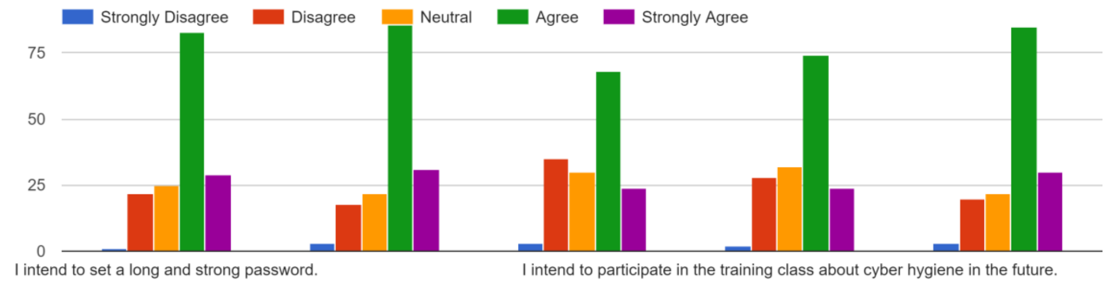


Section E: Cyber Hygiene Attitude

9. Please rate how strongly you agree or disagree with the following statement:

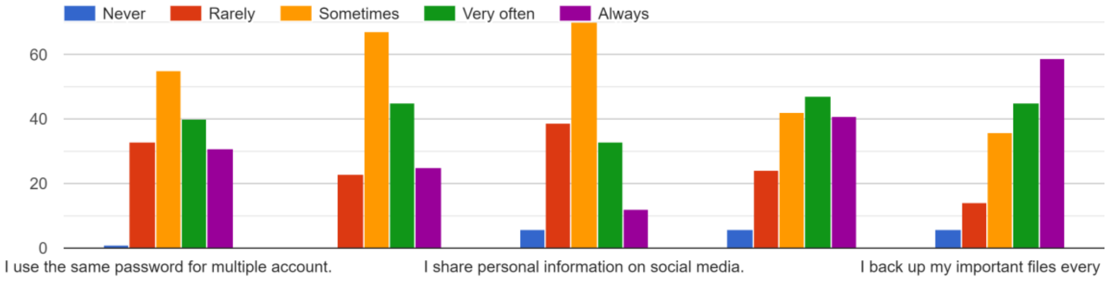
Section F: Cyber Hygiene Intention

10. Please rate how strongly you agree or disagree with the following statement:



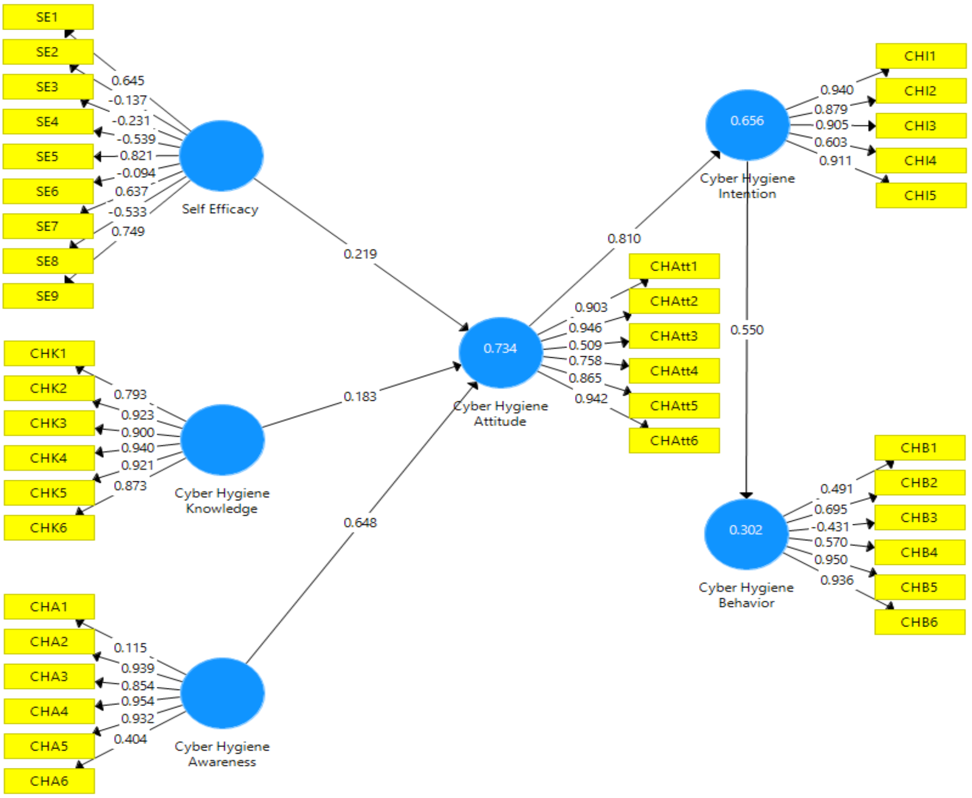
Section G: Cyber Hygiene Behavior

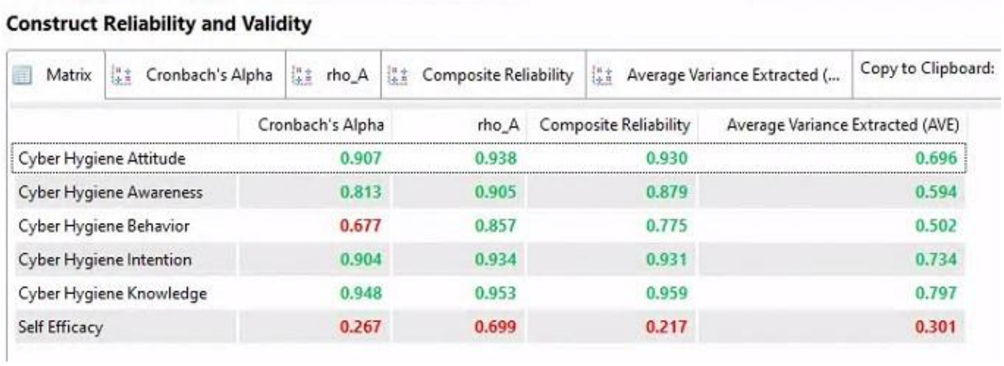
11. Please describe how often do you practice the cyber hygiene behavior stated below:



A.3 PLS-SEM Results (Pilot Test - 30 Respondents)

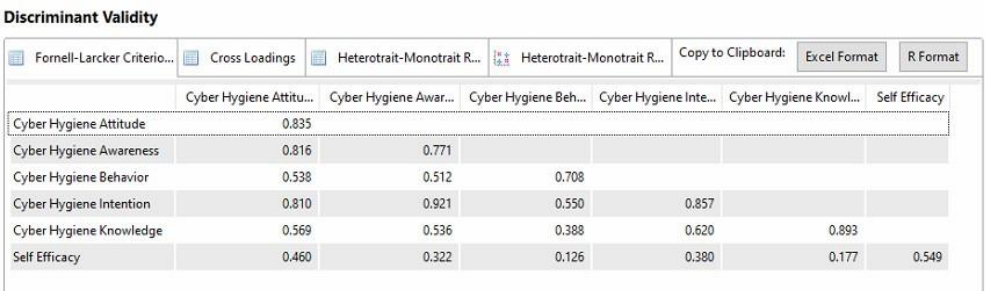
Test 1 (Eliminate item CHA7, CHB7):





Construct Reliability and Validity

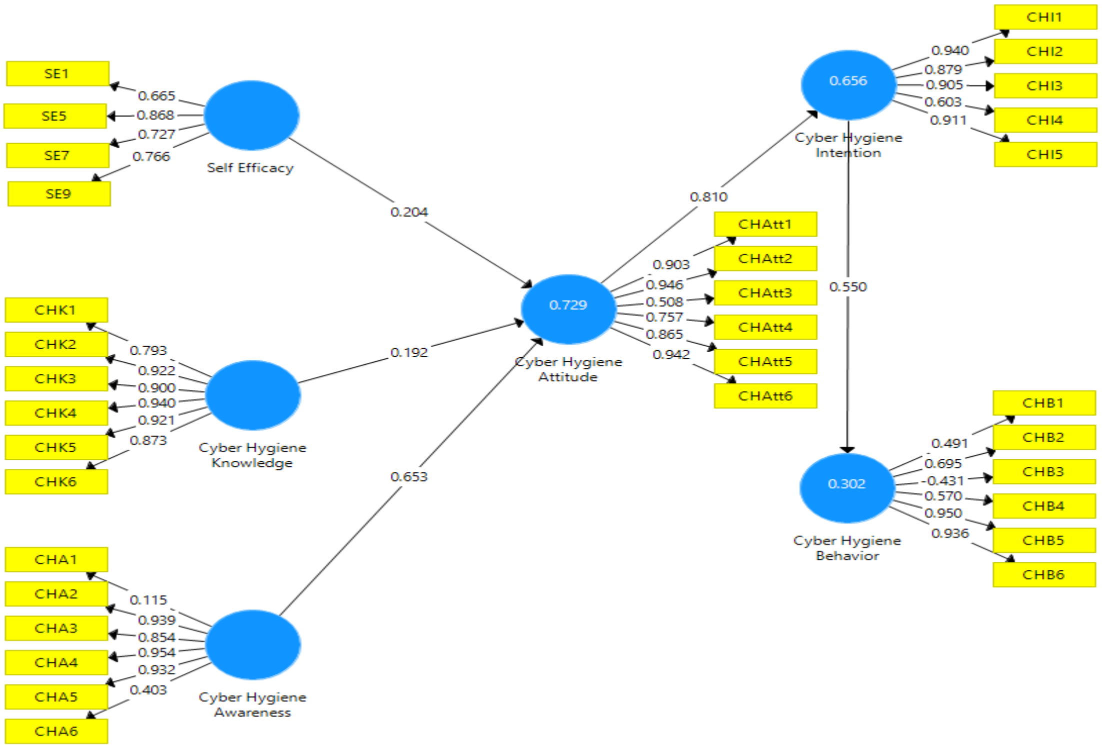
	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Cyber Hygiene Attitude	0.907	0.938	0.930	0.696
Cyber Hygiene Awareness	0.813	0.905	0.879	0.594
Cyber Hygiene Behavior	0.677	0.857	0.775	0.502
Cyber Hygiene Intention	0.904	0.934	0.931	0.734
Cyber Hygiene Knowledge	0.948	0.953	0.959	0.797
Self Efficacy	0.267	0.699	0.217	0.301

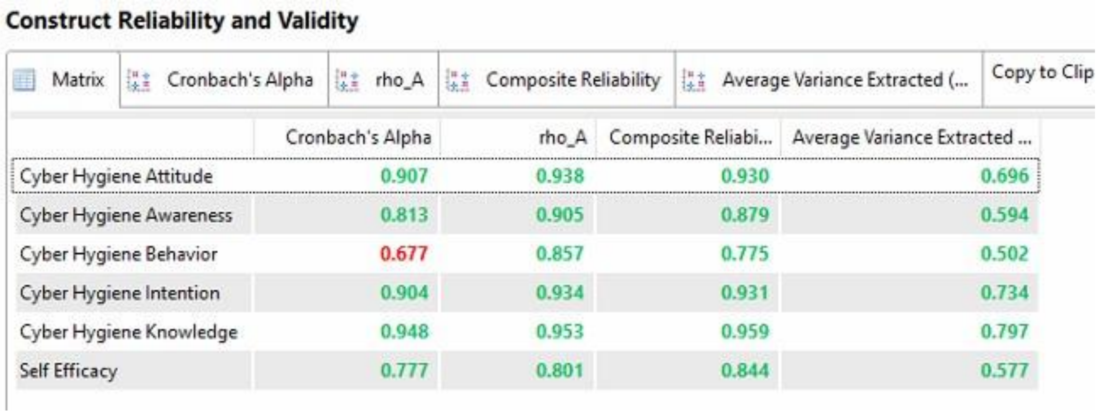

Fornell-Larcker Criterio...
Cross Loadings
Heterotrait-Monotrait R...
Heterotrait-Monotrait R...
Copy to Clipboard:
Excel Format
R Format

Discriminant Validity

	Cyber Hygiene Attitu...	Cyber Hygiene Awar...	Cyber Hygiene Beh...	Cyber Hygiene Inte...	Cyber Hygiene Knowl...	Self Efficacy
Cyber Hygiene Attitude	0.835					
Cyber Hygiene Awareness	0.816	0.771				
Cyber Hygiene Behavior	0.538	0.512	0.708			
Cyber Hygiene Intention	0.810	0.921	0.550	0.857		
Cyber Hygiene Knowledge	0.569	0.536	0.388	0.620	0.893	
Self Efficacy	0.460	0.322	0.126	0.380	0.177	0.549

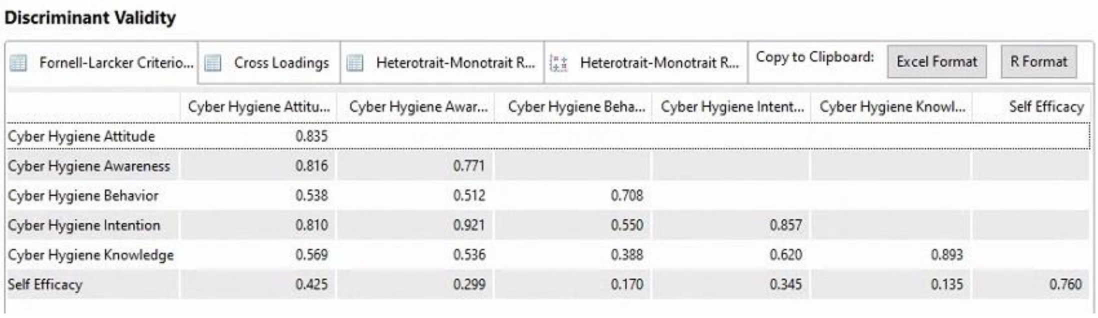
Test 2 (Eliminate item SE2, SE3, SE4, SE6, SE8, CHA7, CHB7):





Construct Reliability and Validity

	Cronbach's Alpha	rho_A	Composite Reliabi...	Average Variance Extracted ...
Cyber Hygiene Attitude	0.907	0.938	0.930	0.696
Cyber Hygiene Awareness	0.813	0.905	0.879	0.594
Cyber Hygiene Behavior	0.677	0.857	0.775	0.502
Cyber Hygiene Intention	0.904	0.934	0.931	0.734
Cyber Hygiene Knowledge	0.948	0.953	0.959	0.797
Self Efficacy	0.777	0.801	0.844	0.577

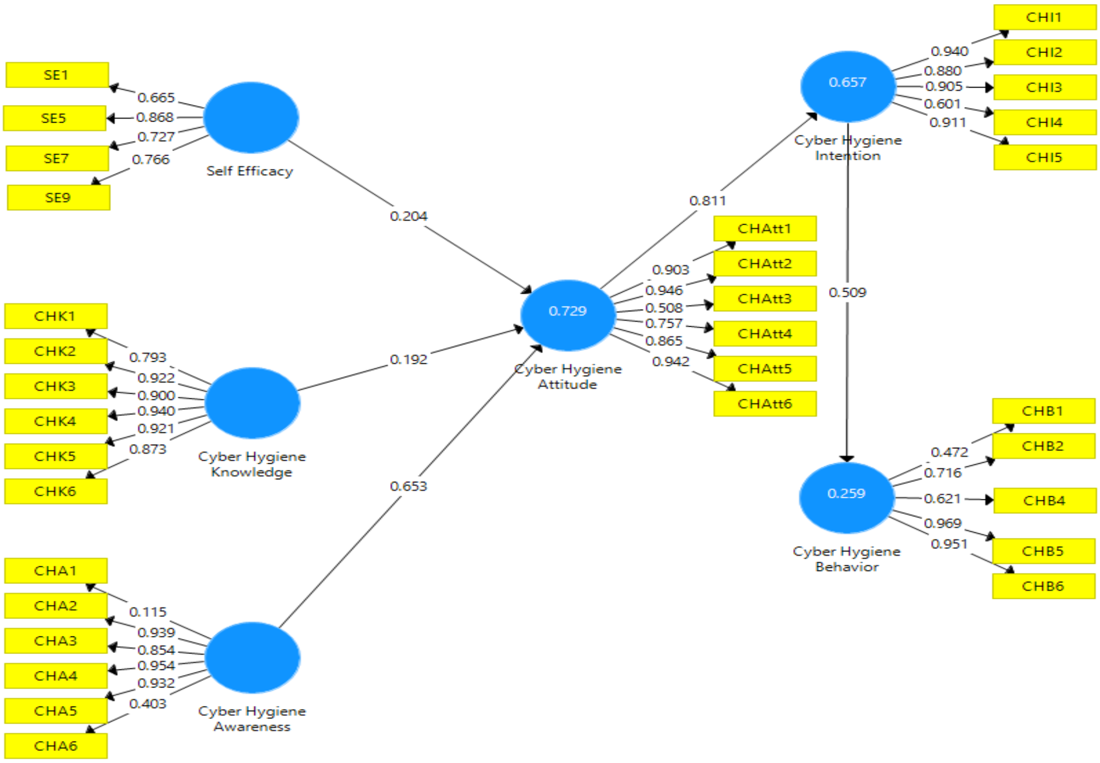


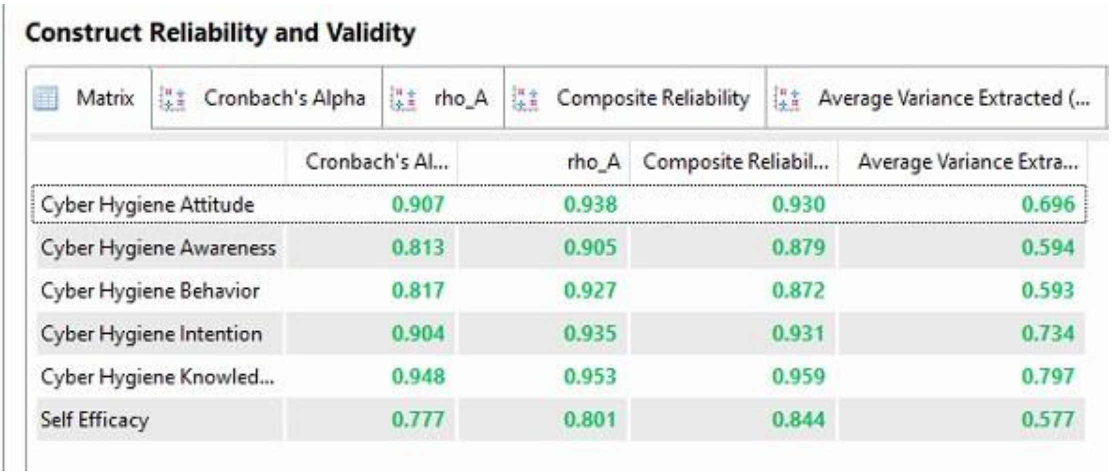
Discriminant Validity

Fornell-Larcker Criterio...
Cross Loadings
Heterotrait-Monotrait R...
Heterotrait-Monotrait R...
Copy to Clipboard:
Excel Format
R Format

	Cyber Hygiene Attitu...	Cyber Hygiene Awar...	Cyber Hygiene Beha...	Cyber Hygiene Intent...	Cyber Hygiene Knowl...	Self Efficacy
Cyber Hygiene Attitude	0.835					
Cyber Hygiene Awareness	0.816	0.771				
Cyber Hygiene Behavior	0.538	0.512	0.708			
Cyber Hygiene Intention	0.810	0.921	0.550	0.857		
Cyber Hygiene Knowledge	0.569	0.536	0.388	0.620	0.893	
Self Efficacy	0.425	0.299	0.170	0.345	0.135	0.760

Test 3 (Eliminate item SE2, SE3, SE4, SE6, SE8, CHA7, CHB3, CHB7)

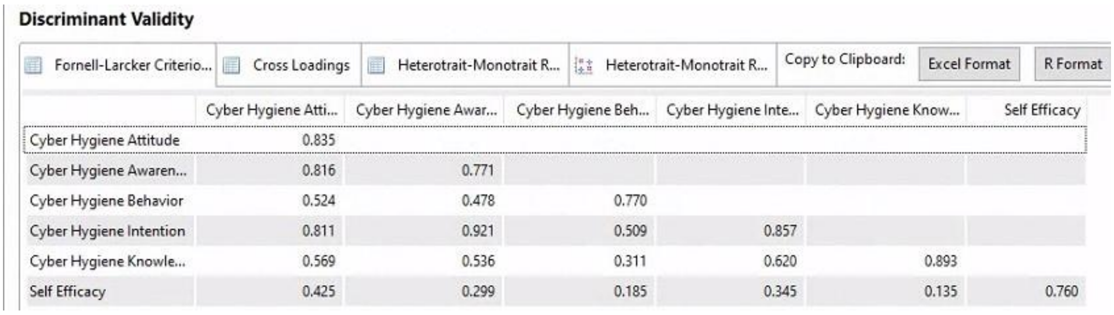




Construct Reliability and Validity

Matrix | Cronbach's Alpha | rho_A | Composite Reliability | Average Variance Extracted (...

	Cronbach's Al...	rho_A	Composite Reliabil...	Average Variance Extra...
Cyber Hygiene Attitude	0.907	0.938	0.930	0.696
Cyber Hygiene Awareness	0.813	0.905	0.879	0.594
Cyber Hygiene Behavior	0.817	0.927	0.872	0.593
Cyber Hygiene Intention	0.904	0.935	0.931	0.734
Cyber Hygiene Knowled...	0.948	0.953	0.959	0.797
Self Efficacy	0.777	0.801	0.844	0.577



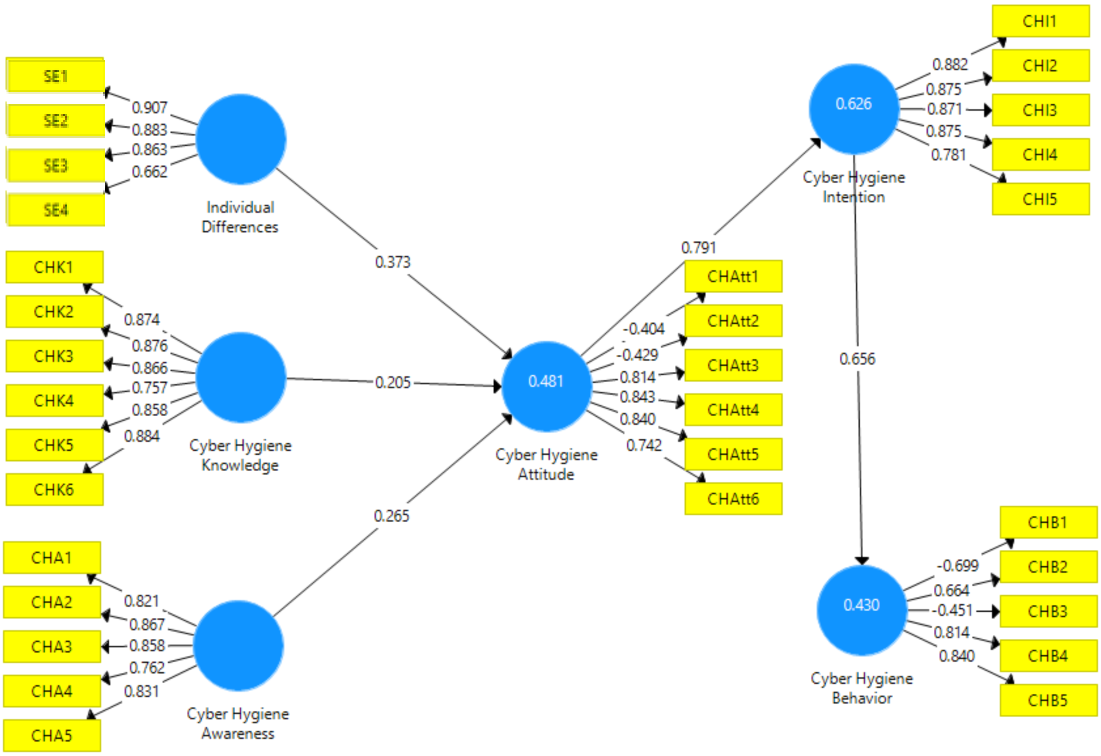
Discriminant Validity

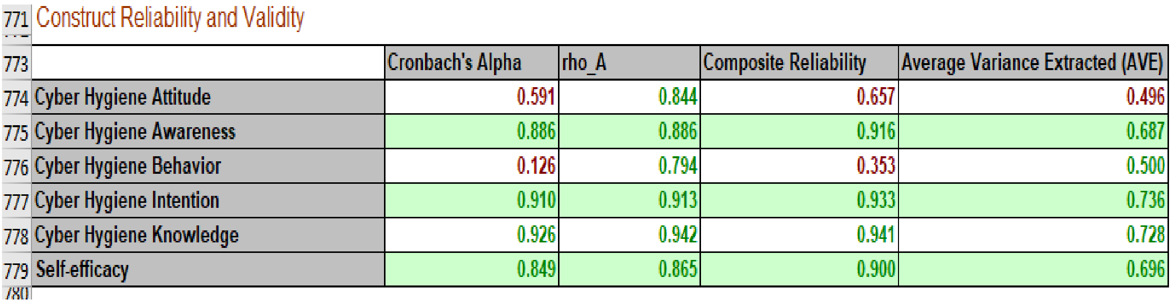
Fornell-Larcker Criterio... | Cross Loadings | Heterotrait-Monotrait R... | Heterotrait-Monotrait R... | Copy to Clipboard: | Excel Format | R Format

	Cyber Hygiene Atti...	Cyber Hygiene Awar...	Cyber Hygiene Beh...	Cyber Hygiene Inte...	Cyber Hygiene Know...	Self Efficacy
Cyber Hygiene Attitude	0.835					
Cyber Hygiene Awaren...	0.816	0.771				
Cyber Hygiene Behavior	0.524	0.478	0.770			
Cyber Hygiene Intention	0.811	0.921	0.509	0.857		
Cyber Hygiene Knowle...	0.569	0.536	0.311	0.620	0.893	
Self Efficacy	0.425	0.299	0.185	0.345	0.135	0.760

A.4 PLS-SEM Results (160 Respondents)

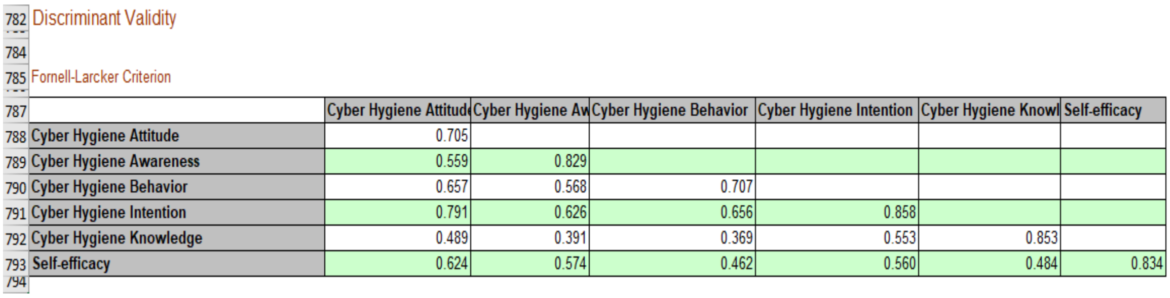
Test 1 (Include all items):





Construct Reliability and Validity

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Cyber Hygiene Attitude	0.591	0.844	0.657	0.496
Cyber Hygiene Awareness	0.886	0.886	0.916	0.687
Cyber Hygiene Behavior	0.126	0.794	0.353	0.500
Cyber Hygiene Intention	0.910	0.913	0.933	0.736
Cyber Hygiene Knowledge	0.926	0.942	0.941	0.728
Self-efficacy	0.849	0.865	0.900	0.696

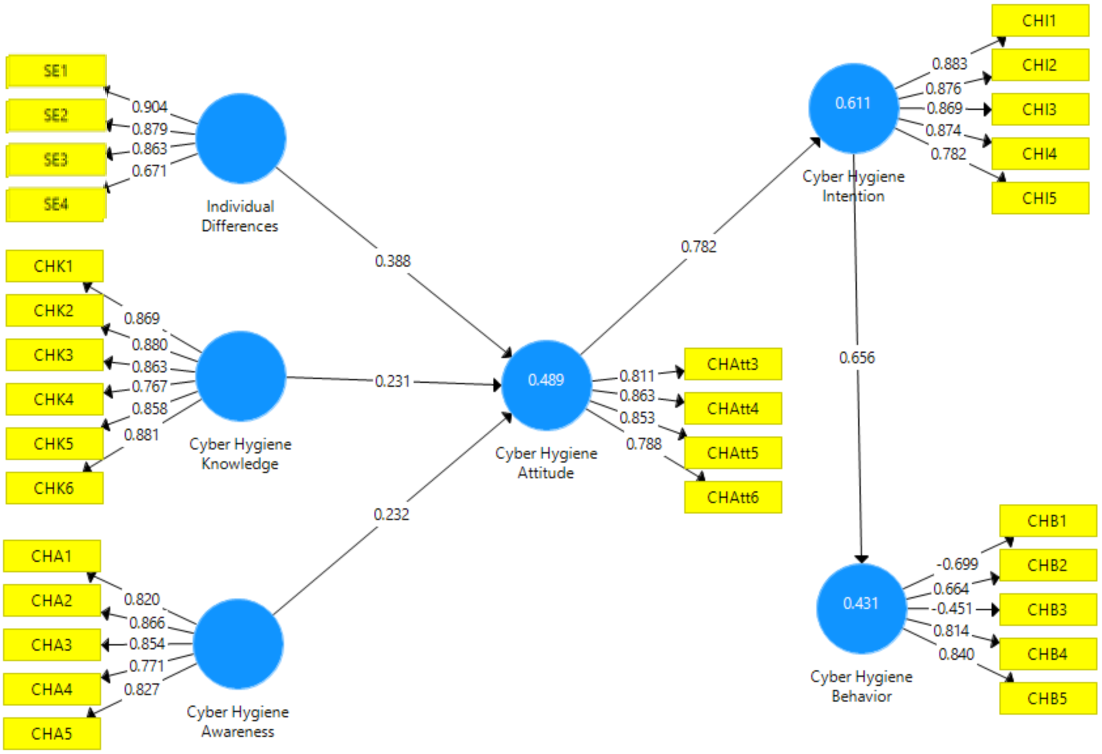


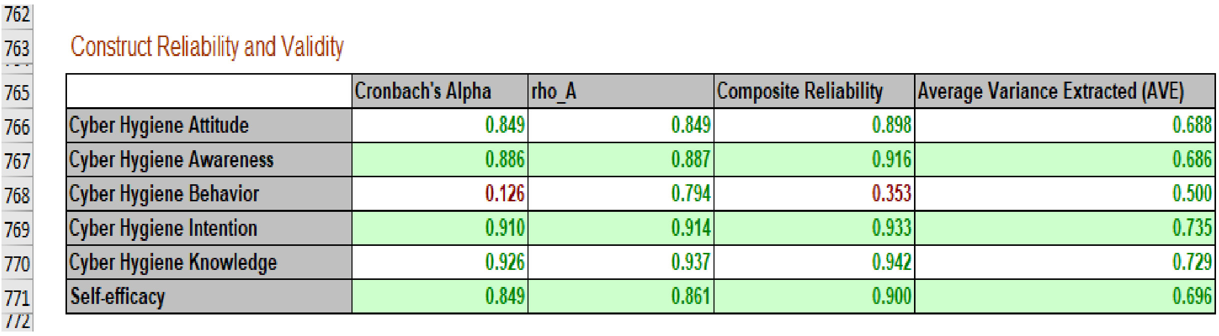
Discriminant Validity

Fornell-Larcker Criterion

	Cyber Hygiene Attitud	Cyber Hygiene Aw	Cyber Hygiene Behavior	Cyber Hygiene Intention	Cyber Hygiene Knowl	Self-efficacy
Cyber Hygiene Attitude	0.705					
Cyber Hygiene Awareness	0.559	0.829				
Cyber Hygiene Behavior	0.657	0.568	0.707			
Cyber Hygiene Intention	0.791	0.626	0.656	0.858		
Cyber Hygiene Knowledge	0.489	0.391	0.369	0.553	0.853	
Self-efficacy	0.624	0.574	0.462	0.560	0.484	0.834

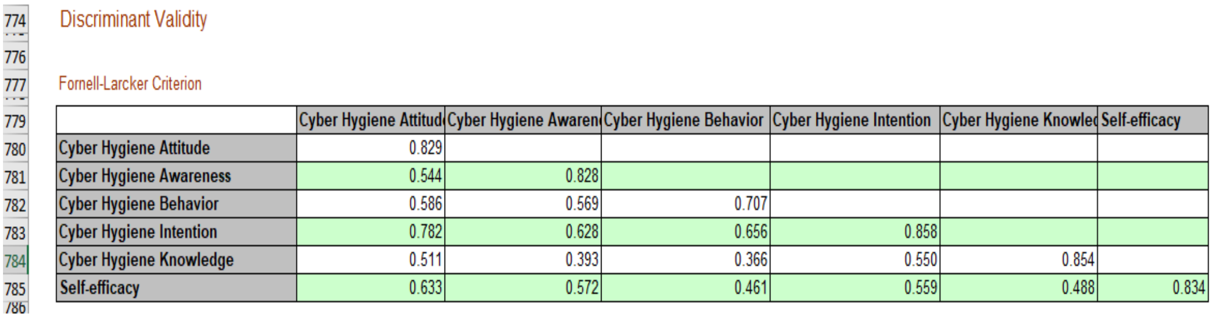
Test 2 (Eliminate item CHAtt1, CHAtt2):





Construct Reliability and Validity

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Cyber Hygiene Attitude	0.849	0.849	0.898	0.688
Cyber Hygiene Awareness	0.886	0.887	0.916	0.686
Cyber Hygiene Behavior	0.126	0.794	0.353	0.500
Cyber Hygiene Intention	0.910	0.914	0.933	0.735
Cyber Hygiene Knowledge	0.926	0.937	0.942	0.729
Self-efficacy	0.849	0.861	0.900	0.696

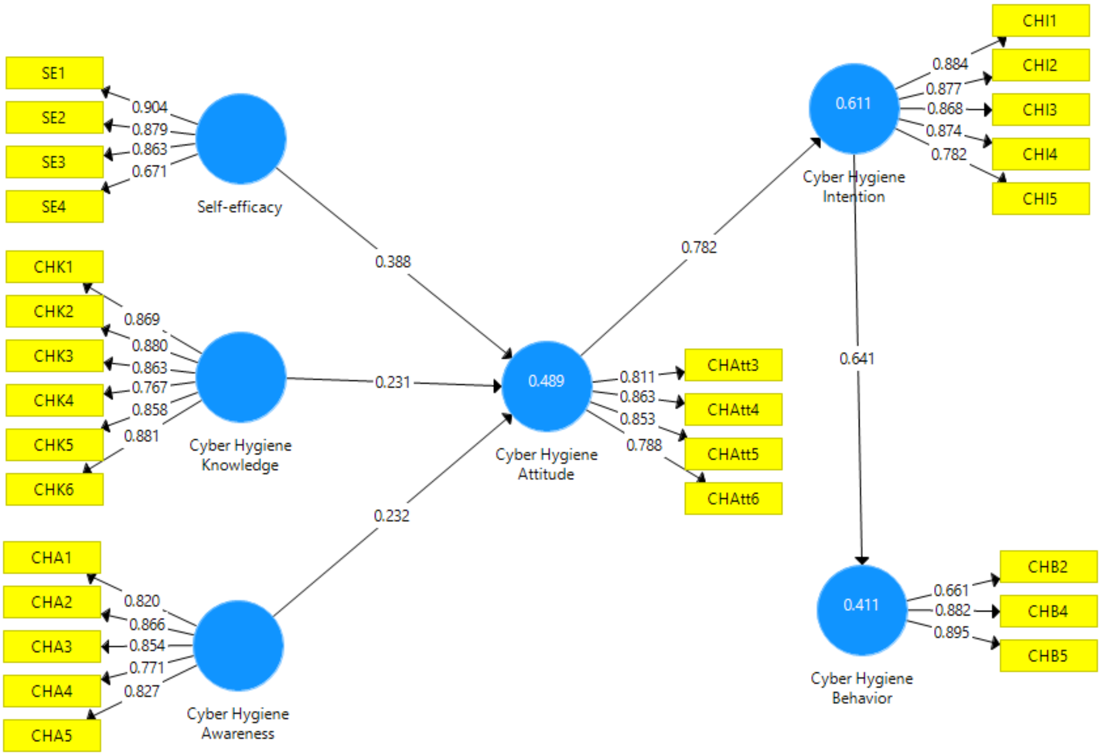


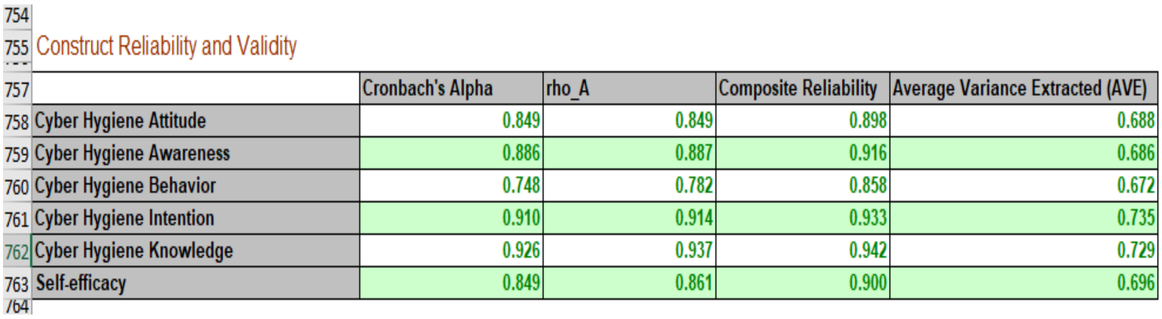
Discriminant Validity

Fornell-Larcker Criterion

	Cyber Hygiene Attitud	Cyber Hygiene Awaren	Cyber Hygiene Behavior	Cyber Hygiene Intention	Cyber Hygiene Knowle	Self-efficacy
Cyber Hygiene Attitude	0.829					
Cyber Hygiene Awareness	0.544	0.828				
Cyber Hygiene Behavior	0.586	0.569	0.707			
Cyber Hygiene Intention	0.782	0.628	0.656	0.858		
Cyber Hygiene Knowledge	0.511	0.393	0.366	0.550	0.854	
Self-efficacy	0.633	0.572	0.461	0.559	0.488	0.834

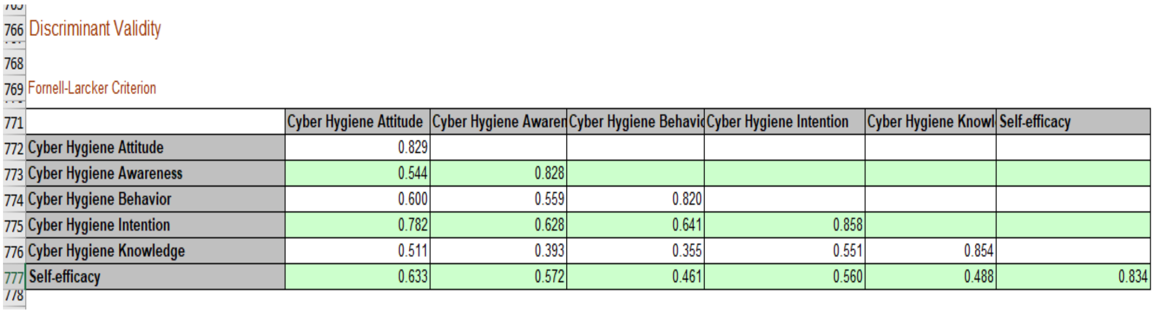
Test 3 (Eliminate CHAtt1, CHAtt2, CHB1, CHB3):





Construct Reliability and Validity

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Cyber Hygiene Attitude	0.849	0.849	0.898	0.688
Cyber Hygiene Awareness	0.886	0.887	0.916	0.686
Cyber Hygiene Behavior	0.748	0.782	0.858	0.672
Cyber Hygiene Intention	0.910	0.914	0.933	0.735
Cyber Hygiene Knowledge	0.926	0.937	0.942	0.729
Self-efficacy	0.849	0.861	0.900	0.696

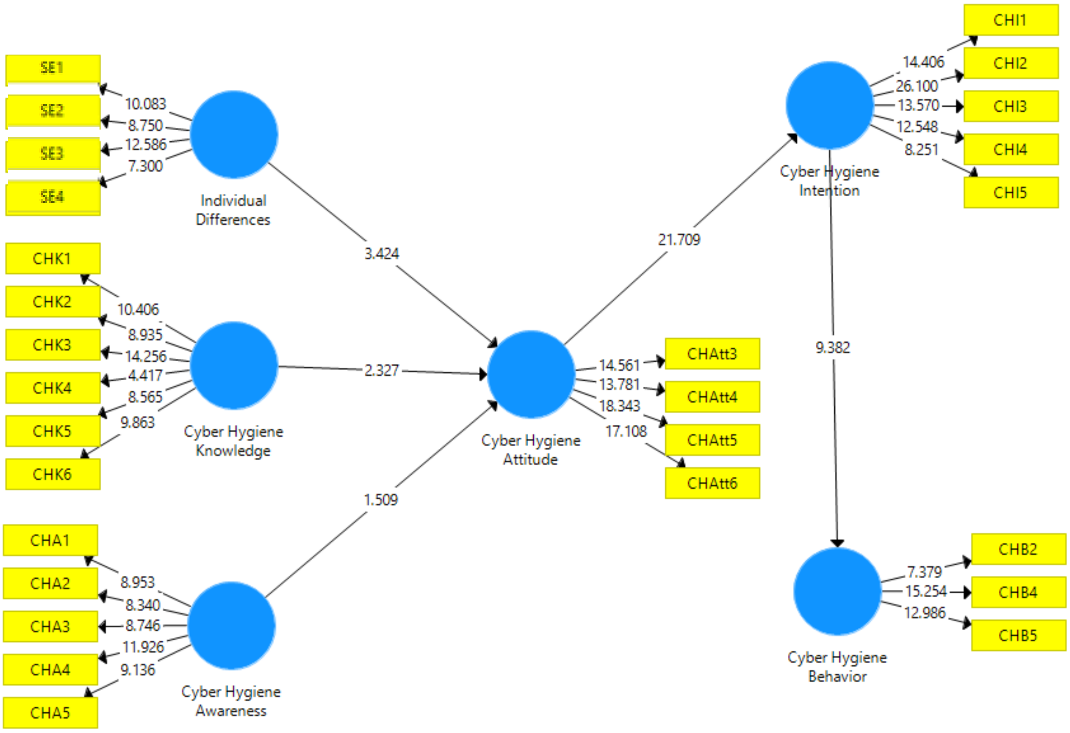


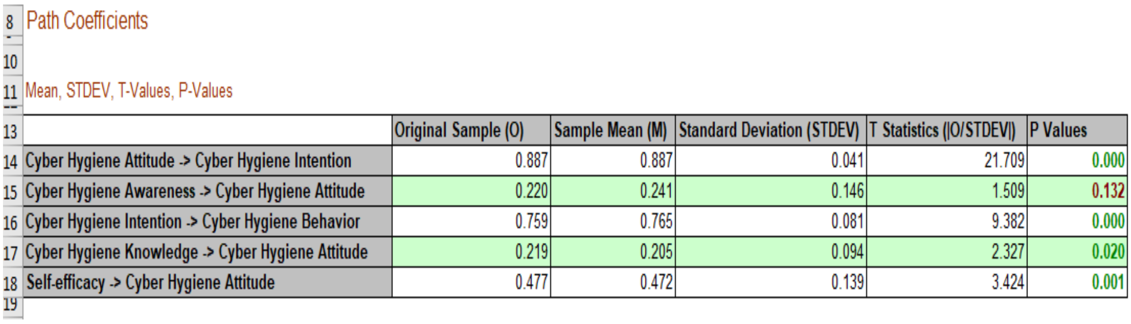
Discriminant Validity

Fornell-Larcker Criterion

	Cyber Hygiene Attitude	Cyber Hygiene Awaren	Cyber Hygiene Behavic	Cyber Hygiene Intention	Cyber Hygiene Knowl	Self-efficacy
Cyber Hygiene Attitude	0.829					
Cyber Hygiene Awareness	0.544	0.828				
Cyber Hygiene Behavior	0.600	0.559	0.820			
Cyber Hygiene Intention	0.782	0.628	0.641	0.858		
Cyber Hygiene Knowledge	0.511	0.393	0.355	0.551	0.854	
Self-efficacy	0.633	0.572	0.461	0.560	0.488	0.834

A.5 Path Analysis for Final Model





Path Coefficients

Mean, STDEV, T-Values, P-Values

	Original Sample (O)	Sample Mean (M)	Standard Deviation (STDEV)	T Statistics (|O/STDEV|)	P Values
Cyber Hygiene Attitude -> Cyber Hygiene Intention	0.887	0.887	0.041	21.709	0.000
Cyber Hygiene Awareness -> Cyber Hygiene Attitude	0.220	0.241	0.146	1.509	0.132
Cyber Hygiene Intention -> Cyber Hygiene Behavior	0.759	0.765	0.081	9.382	0.000
Cyber Hygiene Knowledge -> Cyber Hygiene Attitude	0.219	0.205	0.094	2.327	0.020
Self-efficacy -> Cyber Hygiene Attitude	0.477	0.472	0.139	3.424	0.001

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Y3S3	**Study week no.:** 1-2
Student Name & ID: Yvonne Lee Yi Jin 18ACB02825	
Supervisor: Ms Yap Seok Gee	
Project Title: Cyber Hygiene During COVID-19 to Avoid Cyber Attacks	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

Reviewing back the content that had been done in my FYP1. Found the problem or any contents that is missed out during my FYP1.

2. WORK TO BE DONE

Complete the content for Chapter 1. Reorganized the subtopics in Chapter 1.

3. PROBLEMS ENCOUNTERED

Project objectives are not clear enough. Confusing on the general objectives and specific objectives.

4. SELF EVALUATION OF THE PROGRESS

Keep working up and seek help from supervisor.

Supervisor's signature

Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Y3S3	**Study week no.:** 3-4
Student Name & ID: Yvonne Lee Yi Jin 18ACB02825	
Supervisor: Ms Yap Seok Gee	
Project Title: Cyber Hygiene During COVID-19 to Avoid Cyber Attacks	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

Refined the problem statement and research objectives. Added the research questions that need to be answered in the study.

2. WORK TO BE DONE

Evaluate present study with some previous study. Add on the review on each variables and the Theory of Planned Behavior. Develop conceptual framework based on the variables and develop hypotheses.

3. PROBLEMS ENCOUNTERED

There is a lack of research papers regarding the variables I used for my study. Some of the resources need to pay the fees. Confusing the relationship between variables is a problem to develop a hypothesis.

4. SELF EVALUATION OF THE PROGRESS

Read deeper and get the idea from the research papers. Understand how cyber-attacks can be avoided by practicing good cyber hygiene.

Supervisor's signature

Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Y3S3	**Study week no.:** 5-6
Student Name & ID: Yvonne Lee Yi Jin 18ACB02825	
Supervisor: Ms Yap Seok Gee	
Project Title: Cyber Hygiene During COVID-19 to Avoid Cyber Attacks	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

Determine how the past researchers have done to resolve the problems of cyber hygiene and highlight how the solutions' weaknesses/limitations can be resolved. Done proposed the conceptual framework for my research. Done develop 5 of the hypothesis based on the conceptual framework.

2. WORK TO BE DONE

Develop the research design, data collection methods, sampling design, and questionnaire design based on pilot test done in FYP1.

3. PROBLEMS ENCOUNTERED

Found some of the questions in my survey is not so good and not so related to the study.

4. SELF EVALUATION OF THE PROGRESS

Discussed with the supervisor whether I can still change my questions in my survey form.

Supervisor's signature

Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Y3S3	**Study week no.:** 7-8
Student Name & ID: Yvonne Lee Yi Jin 18ACB02825	
Supervisor: Ms Yap Seok Gee	
Project Title: Cyber Hygiene During COVID-19 to Avoid Cyber Attacks	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

Done designing the questionnaire. Define the target population who will be able to become one of my respondents to help me complete my study.

2. WORK TO BE DONE

Start to distribute the survey form to 160 respondents from UTAR.

3. PROBLEMS ENCOUNTERED

Hard to find the respondents to fill up the survey since it only can be sent online to the participants. Need to wait the respondents help to fill up the survey only can proceed to next chapter.

4. SELF EVALUATION OF THE PROGRESS

Keep sending email, or private message to participants via social media or Microsoft Teams.

Supervisor's signature

Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Y3S3	**Study week no.:** 9-10
Student Name & ID: Yvonne Lee Yi Jin 18ACB02825	
Supervisor: Ms Yap Seok Gee	
Project Title: Cyber Hygiene During COVID-19 to Avoid Cyber Attacks	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

Successfully collected 160 responses from the target population.

2. WORK TO BE DONE

Analyse the result of questionnaire from respondents. Calculate the Cronbach's Alpha, AVE value, Fornell-Larcker criterion using SmartPLS 3.

3. PROBLEMS ENCOUNTERED

Unable to activate the student free license in the SmartPLS 3 using my own computer. On the other hand, student free license only able to support 30 responses.

4. SELF EVALUATION OF THE PROGRESS

Try to reinstall the software again and seek the help from SmartPLS software support team. Apply the 30-days trial version for the professional accounts so that I able to run my analysis.

Supervisor's signature

Student's signature

FINAL YEAR PROJECT WEEKLY REPORT

(Project II)

Trimester, Year: Y3S3	**Study week no.:** 11-12
Student Name & ID: Yvonne Lee Yi Jin 18ACB02825	
Supervisor: Ms Yap Seok Gee	
Project Title: Cyber Hygiene During COVID-19 to Avoid Cyber Attacks	

1. WORK DONE

[Please write the details of the work done in the last fortnight.]

Done analyze all the questionnaires results. Done analyze for SEM analysis with the help of SmartPLS.

2. WORK TO BE DONE

Summarize the statistical analysis and SEM analysis. Discuss on the major finding and determine which hypothesis is supported. Define the implication of the study, limitations of the study and recommendations for future research. Design the poster.

3. PROBLEMS ENCOUNTERED

Do not know what implications of the study means in the research paper. Having no idea on what content should include inside poster.

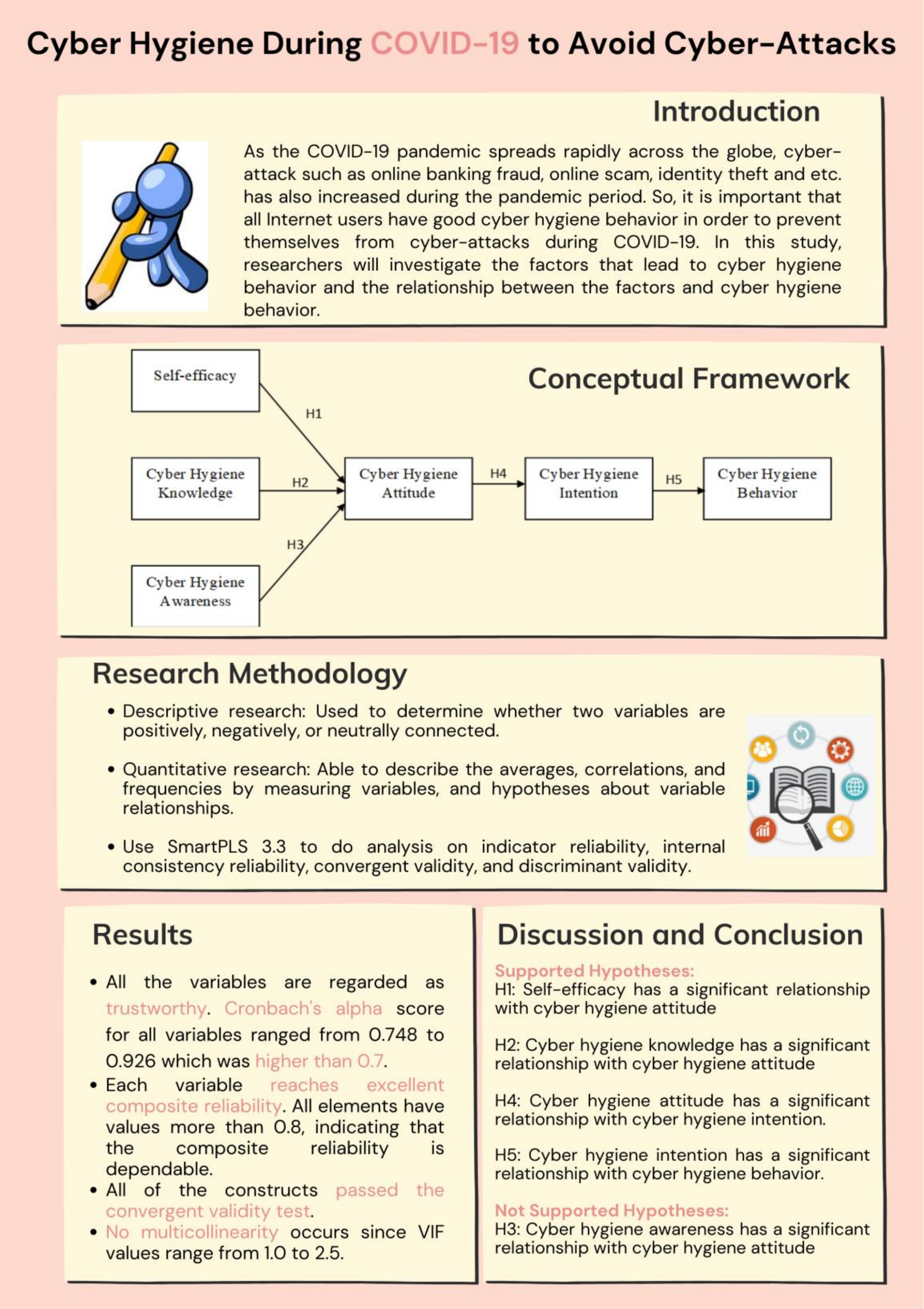
4. SELF EVALUATION OF THE PROGRESS

Seek some information regarding implications of the study from the Google search.

Supervisor's signature

Student's signature

POSTER



Cyber Hygiene During COVID-19 to Avoid Cyber-Attacks

Introduction

As the COVID-19 pandemic spreads rapidly across the globe, cyber-attack such as online banking fraud, online scam, identity theft and etc. has also increased during the pandemic period. So, it is important that all Internet users have good cyber hygiene behavior in order to prevent themselves from cyber-attacks during COVID-19. In this study, researchers will investigate the factors that lead to cyber hygiene behavior and the relationship between the factors and cyber hygiene behavior.

Conceptual Framework

Research Methodology

- Descriptive research: Used to determine whether two variables are positively, negatively, or neutrally connected.
- Quantitative research: Able to describe the averages, correlations, and frequencies by measuring variables, and hypotheses about variable relationships.
- Use SmartPLS 3.3 to do analysis on indicator reliability, internal consistency reliability, convergent validity, and discriminant validity.

Results

- All the variables are regarded as trustworthy. Cronbach's alpha score for all variables ranged from 0.748 to 0.926 which was higher than 0.7.
- Each variable reaches excellent composite reliability. All elements have values more than 0.8, indicating that the composite reliability is dependable.
- All of the constructs passed the convergent validity test.
- No multicollinearity occurs since VIF values range from 1.0 to 2.5.

Discussion and Conclusion

Supported Hypotheses:
H1: Self-efficacy has a significant relationship with cyber hygiene attitude

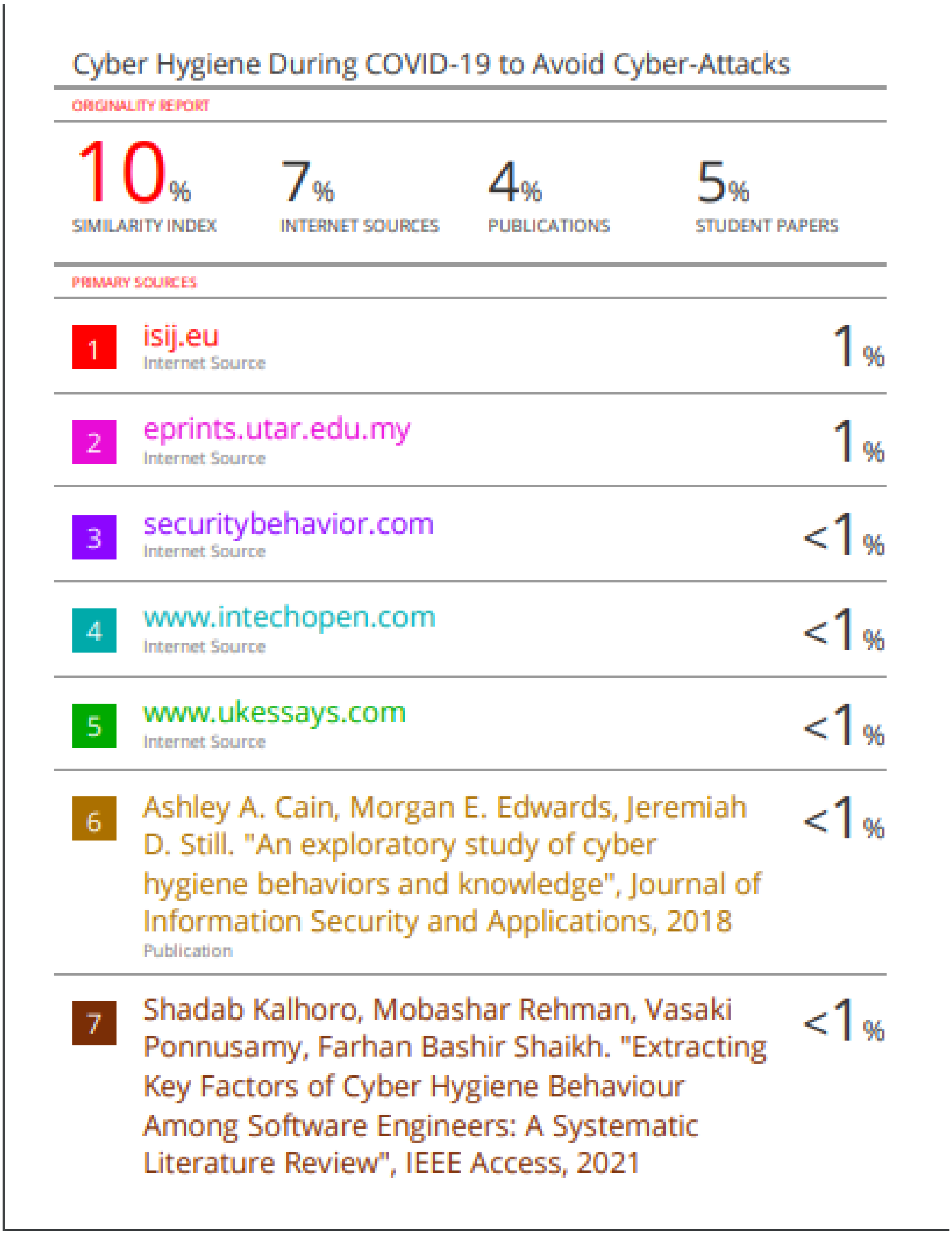
H2: Cyber hygiene knowledge has a significant relationship with cyber hygiene attitude

H4: Cyber hygiene attitude has a significant relationship with cyber hygiene intention.

H5: Cyber hygiene intention has a significant relationship with cyber hygiene behavior.

Not Supported Hypotheses:
H3: Cyber hygiene awareness has a significant relationship with cyber hygiene attitude

PLAGIARISM CHECK RESULT



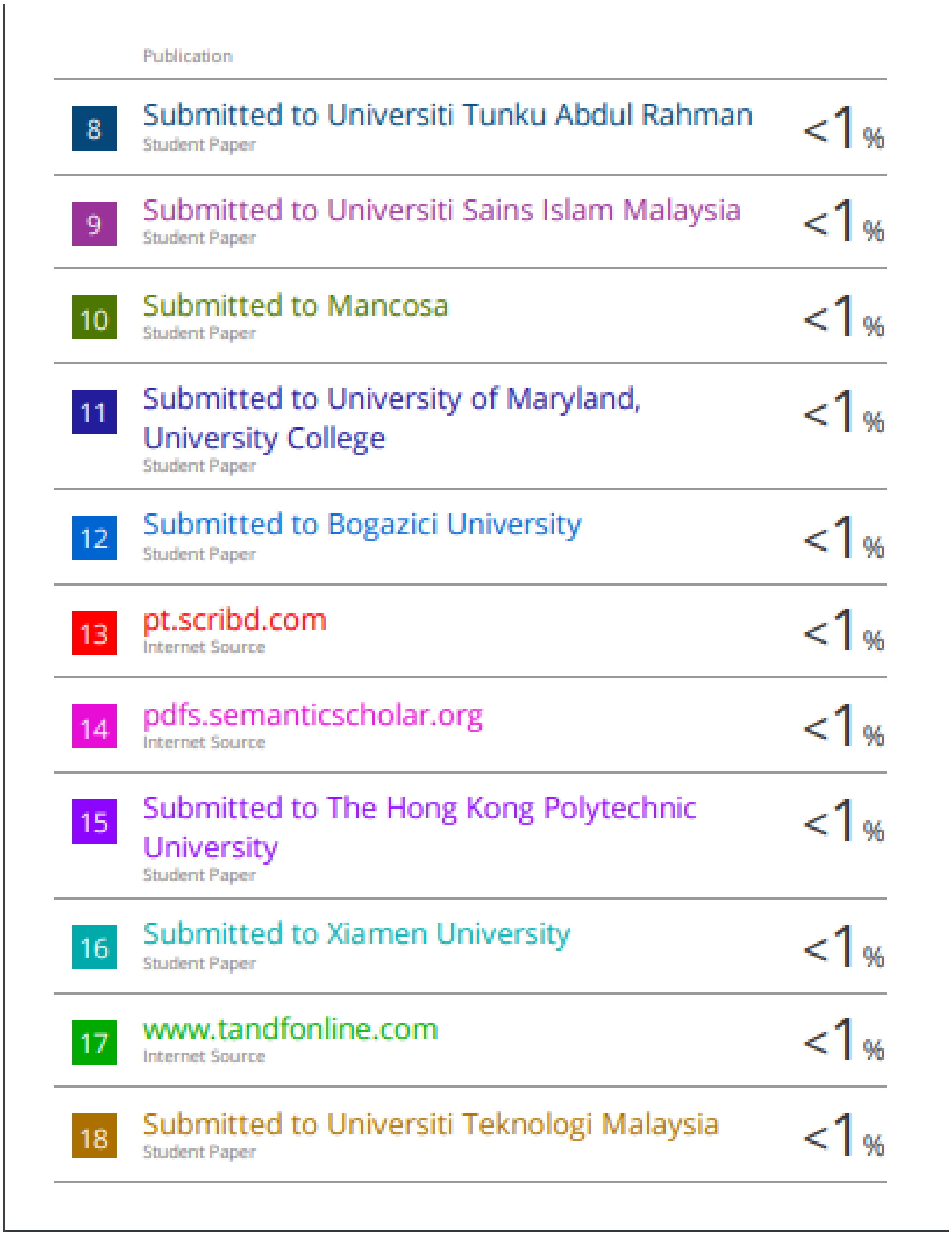
Cyber Hygiene During COVID-19 to Avoid Cyber-Attacks

ORIGINALITY REPORT

10%	7%	4%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

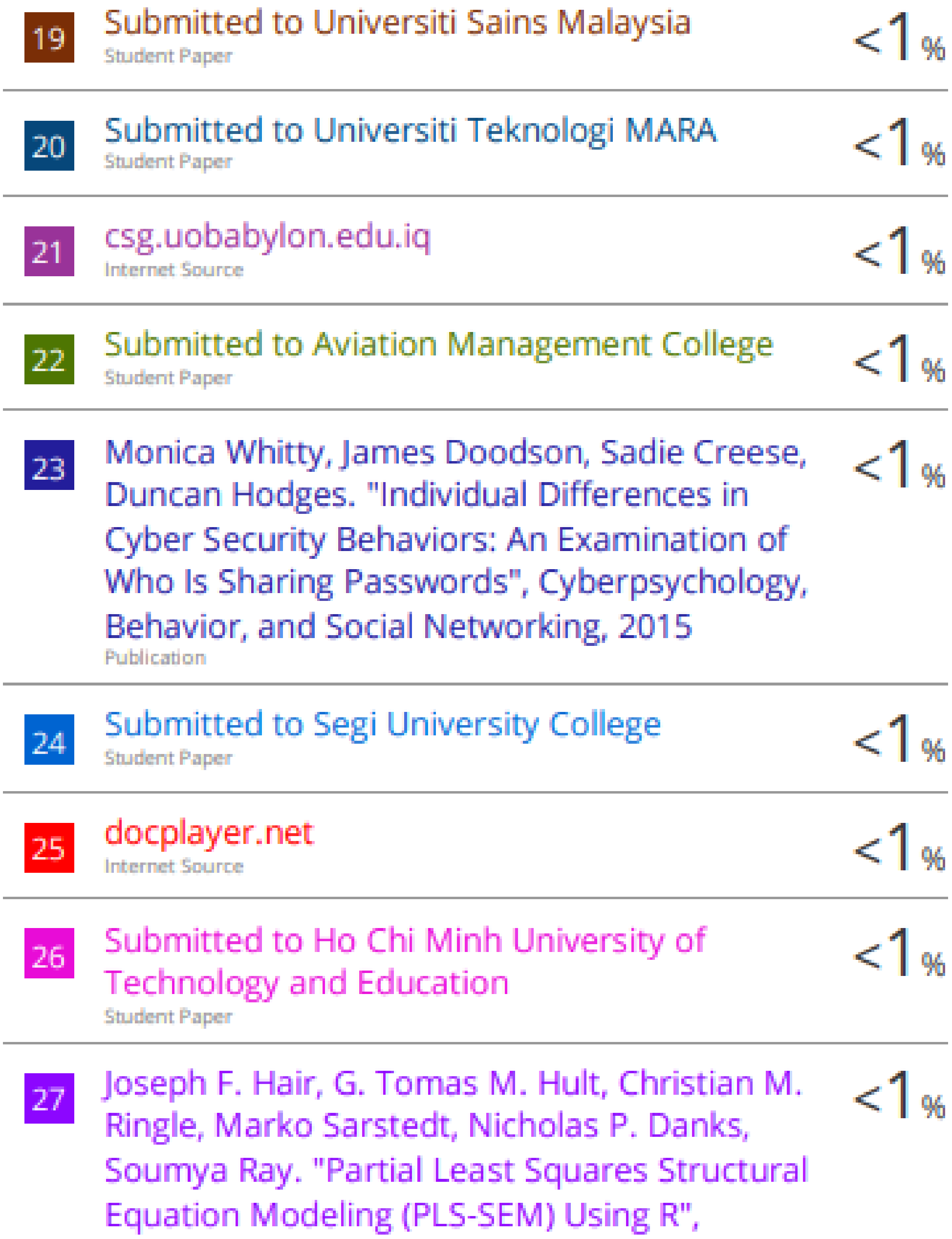
PRIMARY SOURCES

1	isij.eu Internet Source	1%
2	eprints.utar.edu.my Internet Source	1%
3	securitybehavior.com Internet Source	<1%
4	www.intechopen.com Internet Source	<1%
5	www.ukessays.com Internet Source	<1%
6	Ashley A. Cain, Morgan E. Edwards, Jeremiah D. Still. "An exploratory study of cyber hygiene behaviors and knowledge", Journal of Information Security and Applications, 2018 Publication	<1%
7	Shadab Kalhoro, Mobashar Rehman, Vasaki Ponnusamy, Farhan Bashir Shaikh. "Extracting Key Factors of Cyber Hygiene Behaviour Among Software Engineers: A Systematic Literature Review", IEEE Access, 2021	<1%

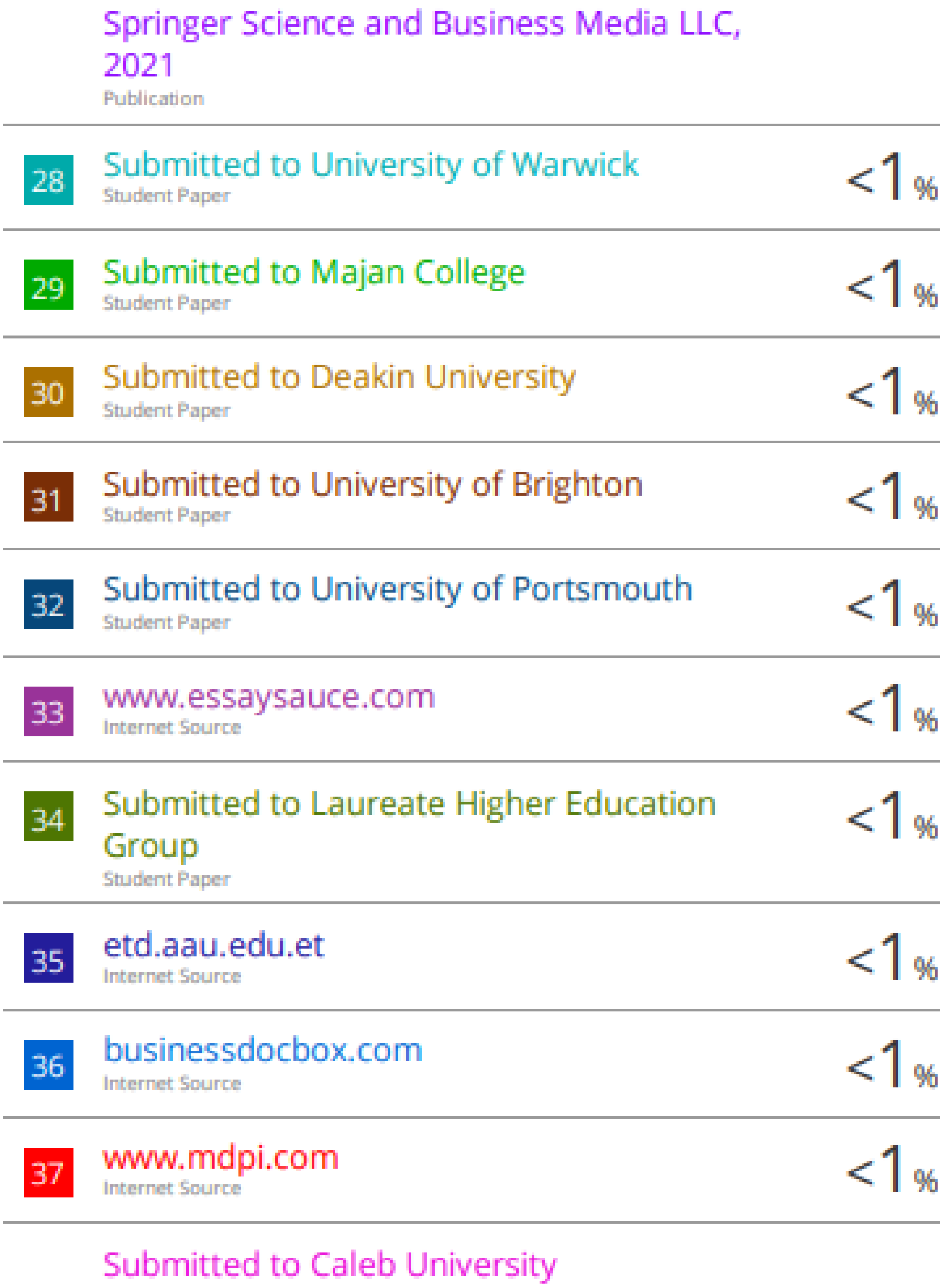


Publication

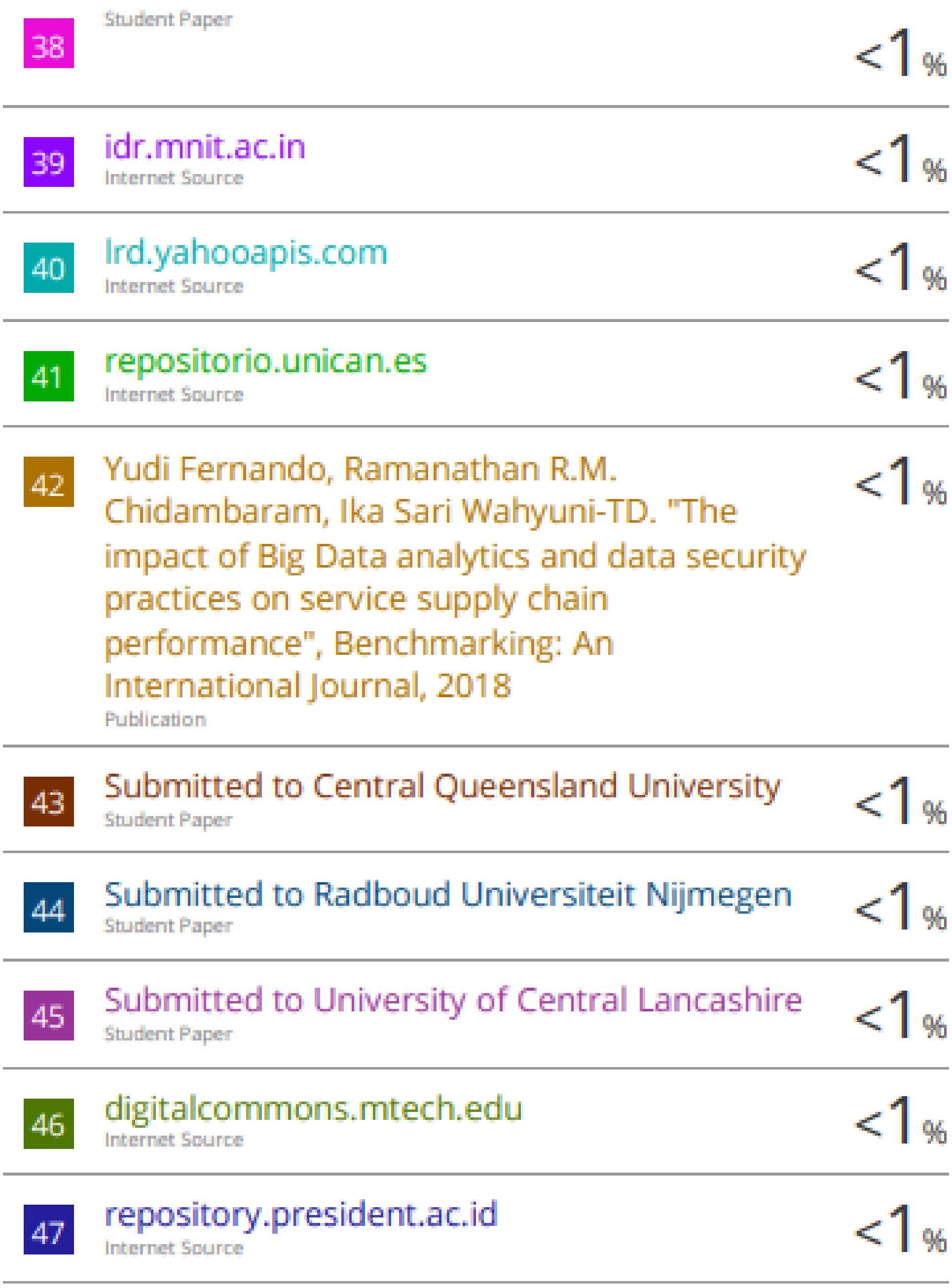
8	Submitted to Universiti Tunku Abdul Rahman Student Paper	<1 %
9	Submitted to Universiti Sains Islam Malaysia Student Paper	<1 %
10	Submitted to Mancosa Student Paper	<1 %
11	Submitted to University of Maryland, University College Student Paper	<1 %
12	Submitted to Bogazici University Student Paper	<1 %
13	pt.scribd.com Internet Source	<1 %
14	pdfs.semanticscholar.org Internet Source	<1 %
15	Submitted to The Hong Kong Polytechnic University Student Paper	<1 %
16	Submitted to Xiamen University Student Paper	<1 %
17	www.tandfonline.com Internet Source	<1 %
18	Submitted to Universiti Teknologi Malaysia Student Paper	<1 %



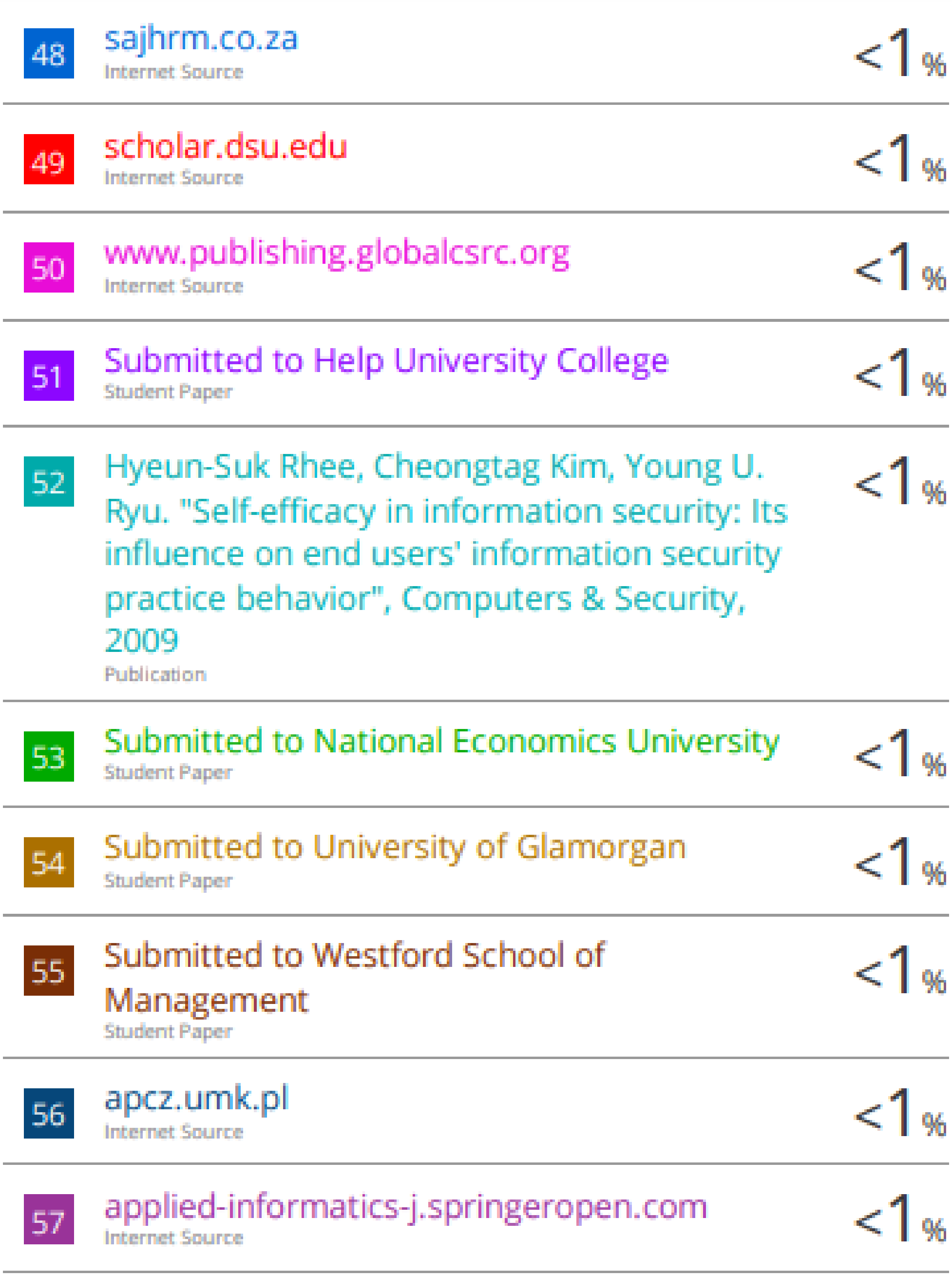
19	Submitted to Universiti Sains Malaysia Student Paper	<1 %
20	Submitted to Universiti Teknologi MARA Student Paper	<1 %
21	csg.uobabylon.edu.iq Internet Source	<1 %
22	Submitted to Aviation Management College Student Paper	<1 %
23	Monica Whitty, James Doodson, Sadie Creese, Duncan Hodges. "Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords", Cyberpsychology, Behavior, and Social Networking, 2015 Publication	<1 %
24	Submitted to Segi University College Student Paper	<1 %
25	docplayer.net Internet Source	<1 %
26	Submitted to Ho Chi Minh University of Technology and Education Student Paper	<1 %
27	Joseph F. Hair, G. Tomas M. Hult, Christian M. Ringle, Marko Sarstedt, Nicholas P. Danks, Soumya Ray. "Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R",	<1 %



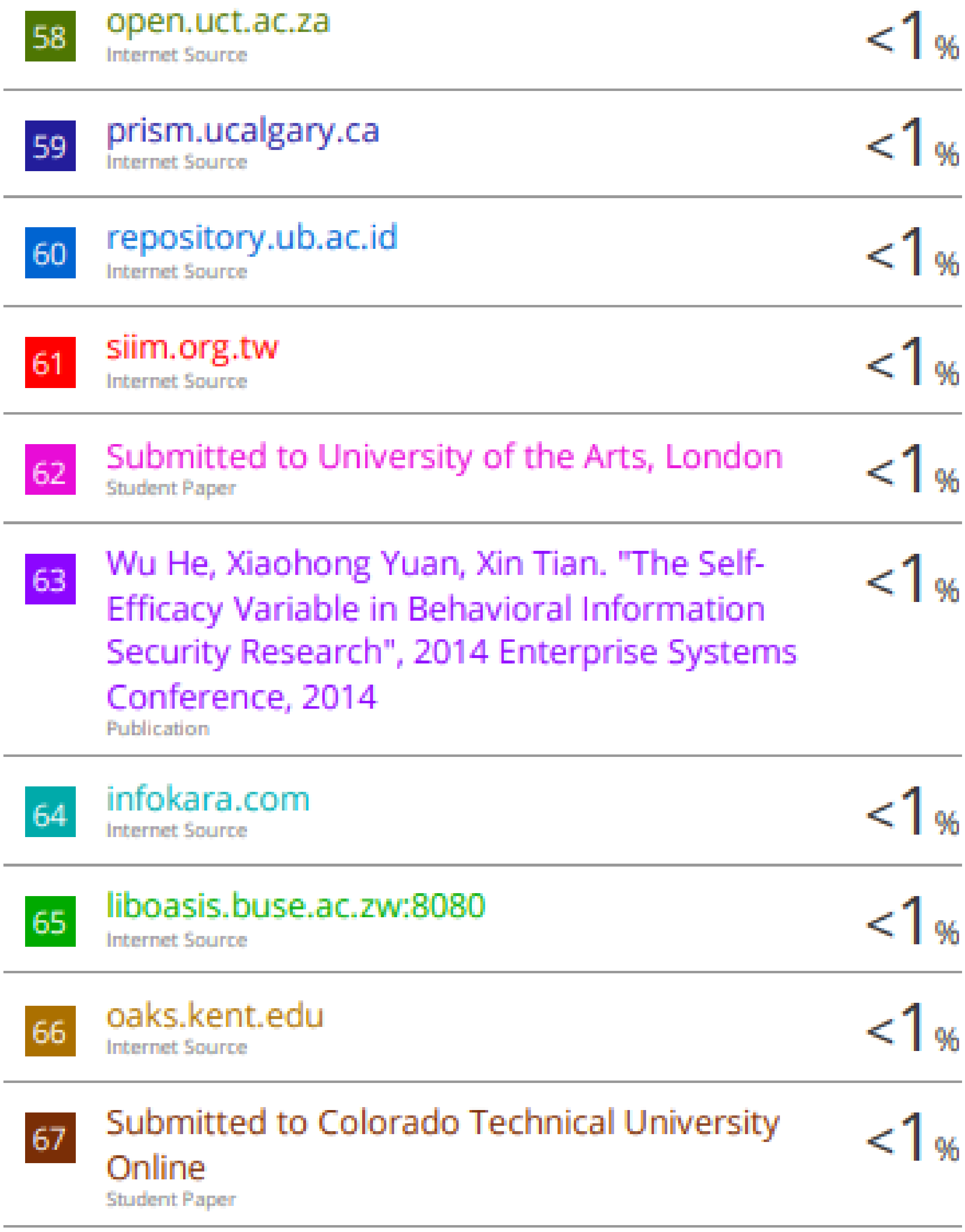
	Springer Science and Business Media LLC, 2021 Publication	
28	Submitted to University of Warwick Student Paper	<1 %
29	Submitted to Majan College Student Paper	<1 %
30	Submitted to Deakin University Student Paper	<1 %
31	Submitted to University of Brighton Student Paper	<1 %
32	Submitted to University of Portsmouth Student Paper	<1 %
33	www.essaysauce.com Internet Source	<1 %
34	Submitted to Laureate Higher Education Group Student Paper	<1 %
35	etd.aau.edu.et Internet Source	<1 %
36	businessdocbox.com Internet Source	<1 %
37	www.mdpi.com Internet Source	<1 %
	Submitted to Caleb University	



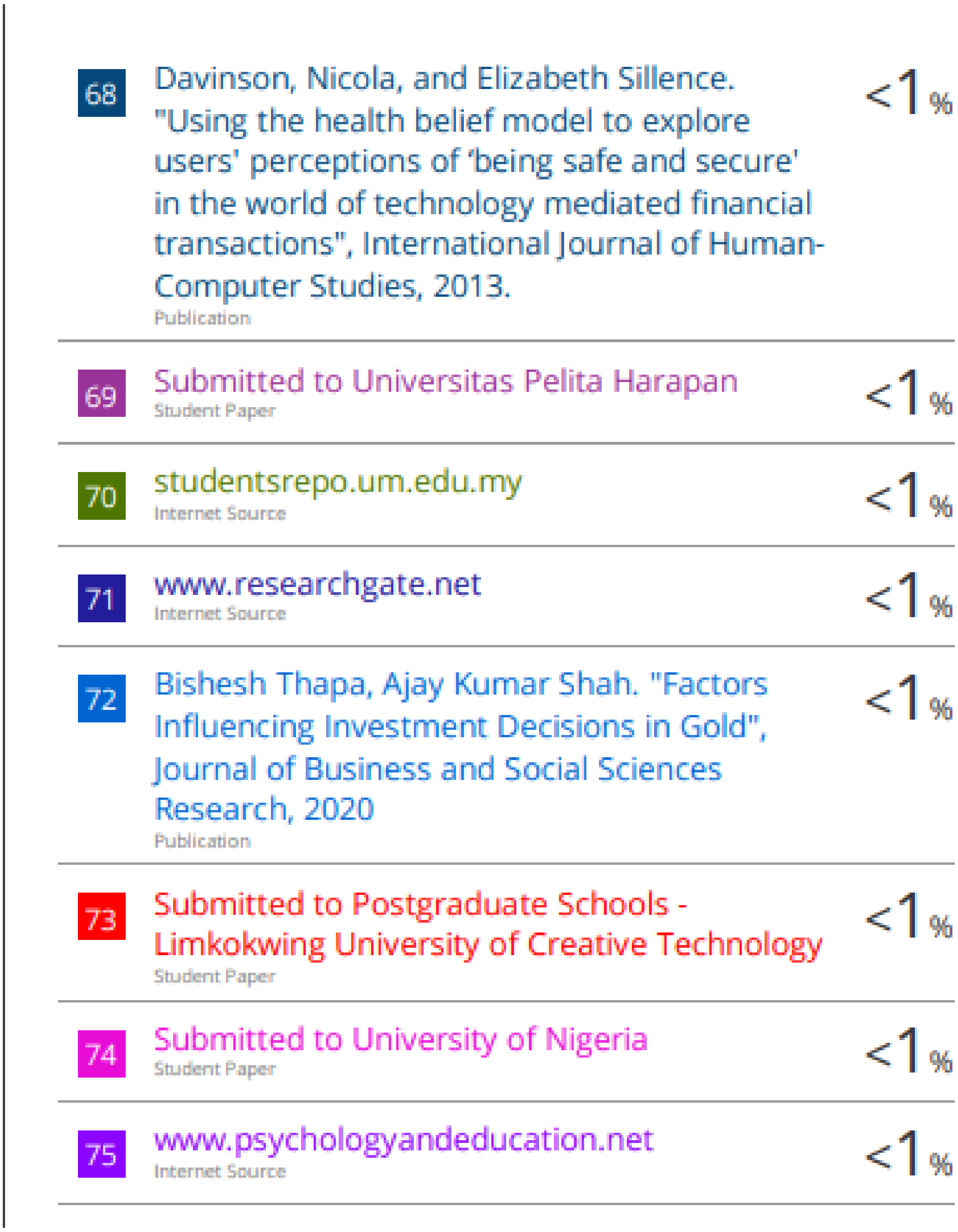
38	Student Paper	<1%
39	idr.mnit.ac.in Internet Source	<1%
40	lrd.yahooapis.com Internet Source	<1%
41	repositorio.unican.es Internet Source	<1%
42	Yudi Fernando, Ramanathan R.M. Chidambaram, Ika Sari Wahyuni-TD. "The impact of Big Data analytics and data security practices on service supply chain performance", Benchmarking: An International Journal, 2018 Publication	<1%
43	Submitted to Central Queensland University Student Paper	<1%
44	Submitted to Radboud Universiteit Nijmegen Student Paper	<1%
45	Submitted to University of Central Lancashire Student Paper	<1%
46	digitalcommons.mtech.edu Internet Source	<1%
47	repository.president.ac.id Internet Source	<1%



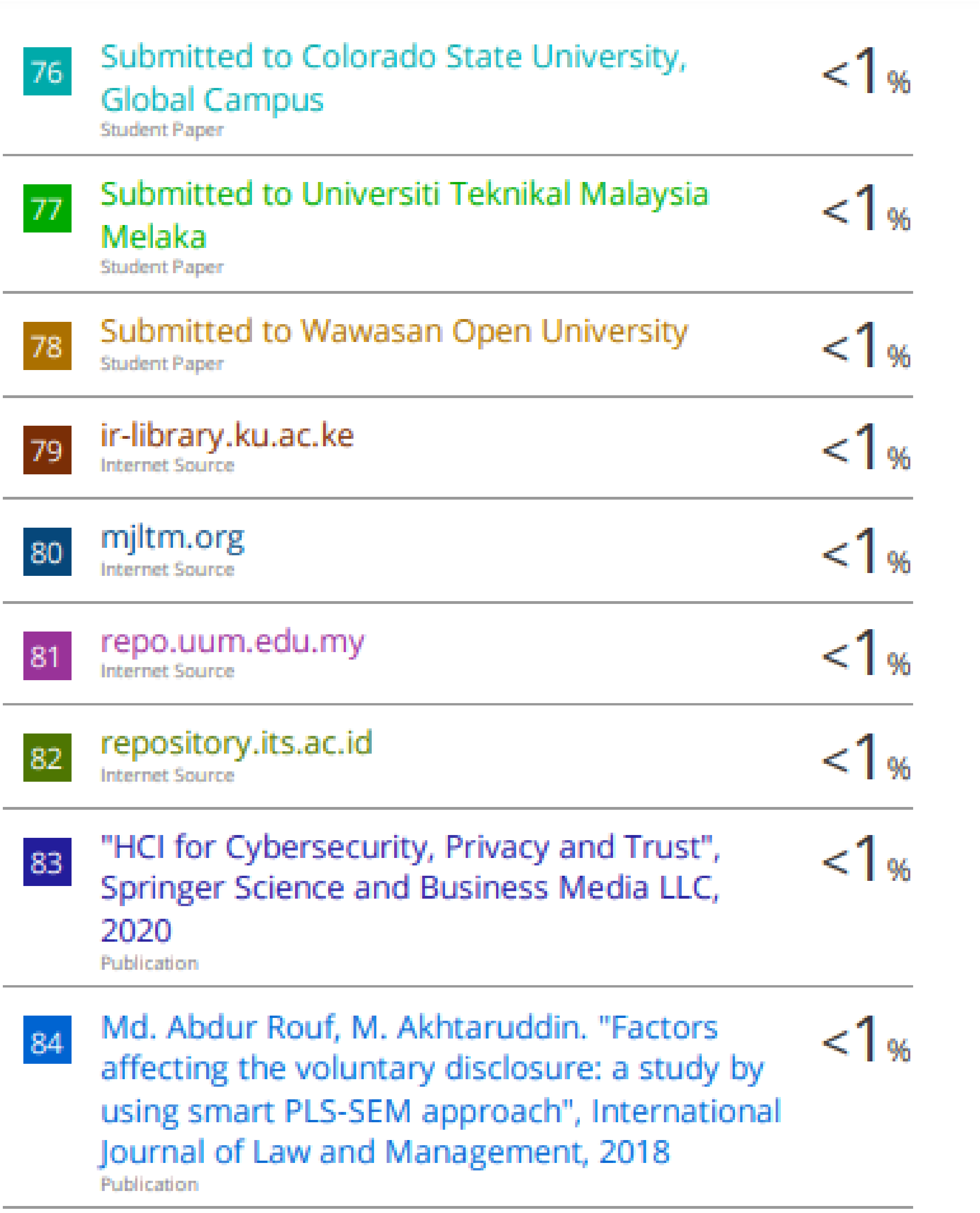
48	sajhrm.co.za Internet Source	<1 %
49	scholar.dsu.edu Internet Source	<1 %
50	www.publishing.globalcsrc.org Internet Source	<1 %
51	Submitted to Help University College Student Paper	<1 %
52	Hyeun-Suk Rhee, Cheongtag Kim, Young U. Ryu. "Self-efficacy in information security: Its influence on end users' information security practice behavior", Computers & Security, 2009 Publication	<1 %
53	Submitted to National Economics University Student Paper	<1 %
54	Submitted to University of Glamorgan Student Paper	<1 %
55	Submitted to Westford School of Management Student Paper	<1 %
56	apcz.umk.pl Internet Source	<1 %
57	applied-informatics-j.springeropen.com Internet Source	<1 %



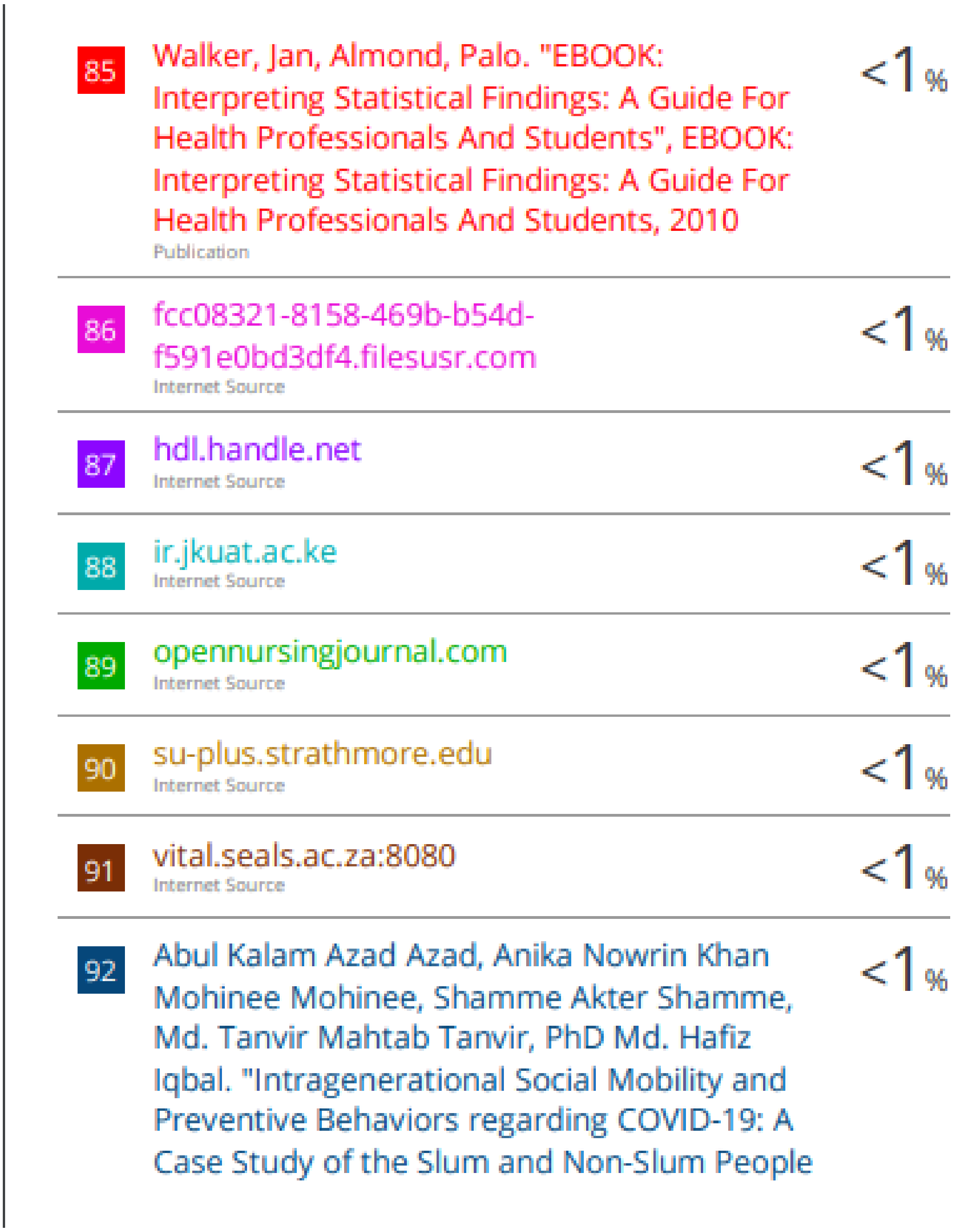
58	open.uct.ac.za Internet Source	<1 %
59	prism.ucalgary.ca Internet Source	<1 %
60	repository.ub.ac.id Internet Source	<1 %
61	siim.org.tw Internet Source	<1 %
62	Submitted to University of the Arts, London Student Paper	<1 %
63	Wu He, Xiaohong Yuan, Xin Tian. "The Self-Efficacy Variable in Behavioral Information Security Research", 2014 Enterprise Systems Conference, 2014 Publication	<1 %
64	infokara.com Internet Source	<1 %
65	liboasis.buse.ac.zw:8080 Internet Source	<1 %
66	oaks.kent.edu Internet Source	<1 %
67	Submitted to Colorado Technical University Online Student Paper	<1 %



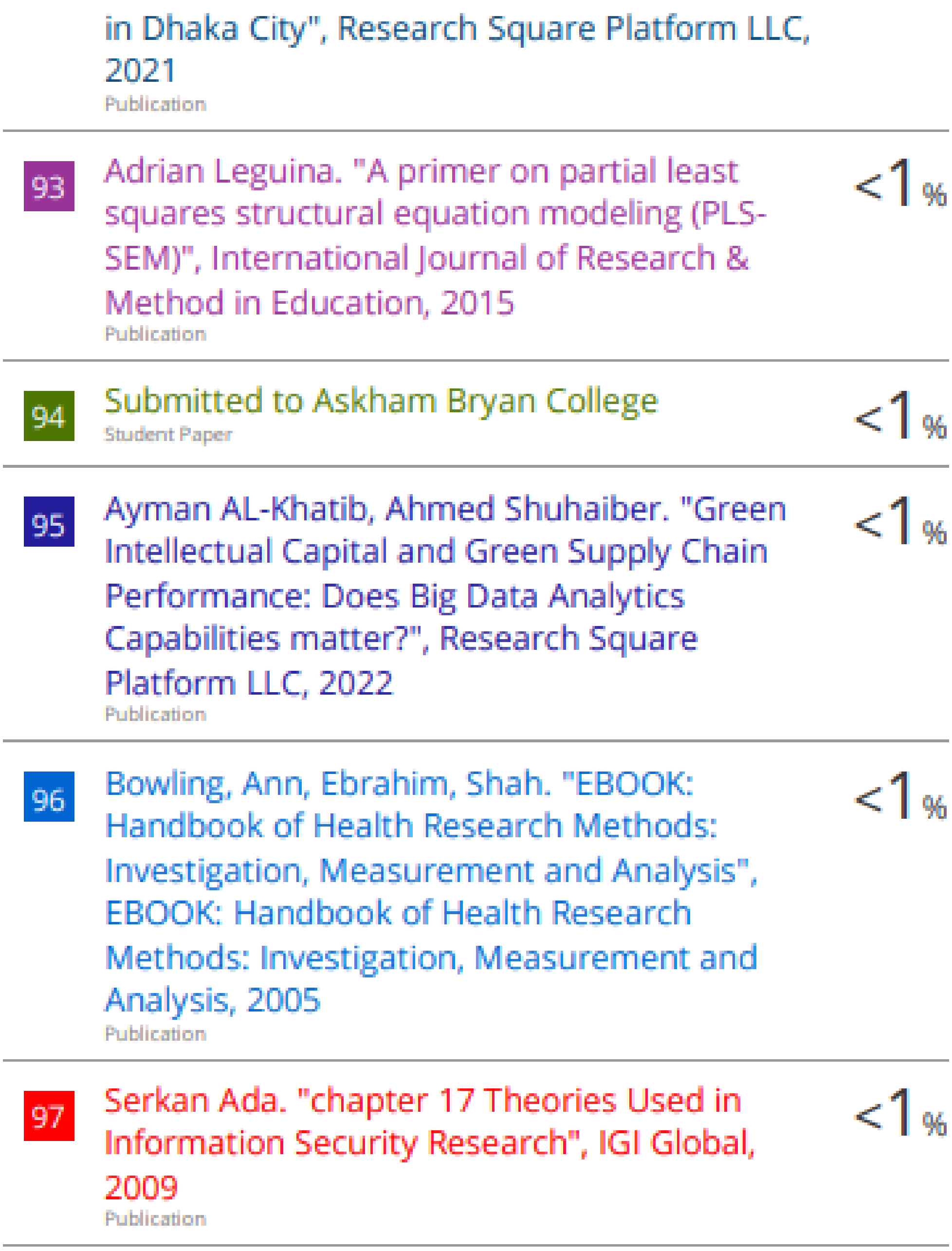
68	Davinson, Nicola, and Elizabeth Sillence. "Using the health belief model to explore users' perceptions of 'being safe and secure' in the world of technology mediated financial transactions", International Journal of Human-Computer Studies, 2013. Publication	<1 %
69	Submitted to Universitas Pelita Harapan Student Paper	<1 %
70	studentsrepo.um.edu.my Internet Source	<1 %
71	www.researchgate.net Internet Source	<1 %
72	Bishesh Thapa, Ajay Kumar Shah. "Factors Influencing Investment Decisions in Gold", Journal of Business and Social Sciences Research, 2020 Publication	<1 %
73	Submitted to Postgraduate Schools - Limkokwing University of Creative Technology Student Paper	<1 %
74	Submitted to University of Nigeria Student Paper	<1 %
75	www.psychologyandeducation.net Internet Source	<1 %



76	Submitted to Colorado State University, Global Campus Student Paper	<1 %
77	Submitted to Universiti Teknikal Malaysia Melaka Student Paper	<1 %
78	Submitted to Wawasan Open University Student Paper	<1 %
79	ir-library.ku.ac.ke Internet Source	<1 %
80	mjltm.org Internet Source	<1 %
81	repo.uum.edu.my Internet Source	<1 %
82	repository.its.ac.id Internet Source	<1 %
83	"HCI for Cybersecurity, Privacy and Trust", Springer Science and Business Media LLC, 2020 Publication	<1 %
84	Md. Abdur Rouf, M. Akhtaruddin. "Factors affecting the voluntary disclosure: a study by using smart PLS-SEM approach", International Journal of Law and Management, 2018 Publication	<1 %



85	Walker, Jan, Almond, Palo. "EBOOK: Interpreting Statistical Findings: A Guide For Health Professionals And Students", EBOOK: Interpreting Statistical Findings: A Guide For Health Professionals And Students, 2010 Publication	<1 %
86	fcc08321-8158-469b-b54d-f591e0bd3df4.filesusr.com Internet Source	<1 %
87	hdl.handle.net Internet Source	<1 %
88	ir.jkuat.ac.ke Internet Source	<1 %
89	opennursingjournal.com Internet Source	<1 %
90	su-plus.strathmore.edu Internet Source	<1 %
91	vital.seals.ac.za:8080 Internet Source	<1 %
92	Abul Kalam Azad Azad, Anika Nowrin Khan Mohinee Mohinee, Shamme Akter Shamme, Md. Tanvir Mahtab Tanvir, PhD Md. Hafiz Iqbal. "Intragenerational Social Mobility and Preventive Behaviors regarding COVID-19: A Case Study of the Slum and Non-Slum People	<1 %



in Dhaka City", Research Square Platform LLC, 2021
Publication

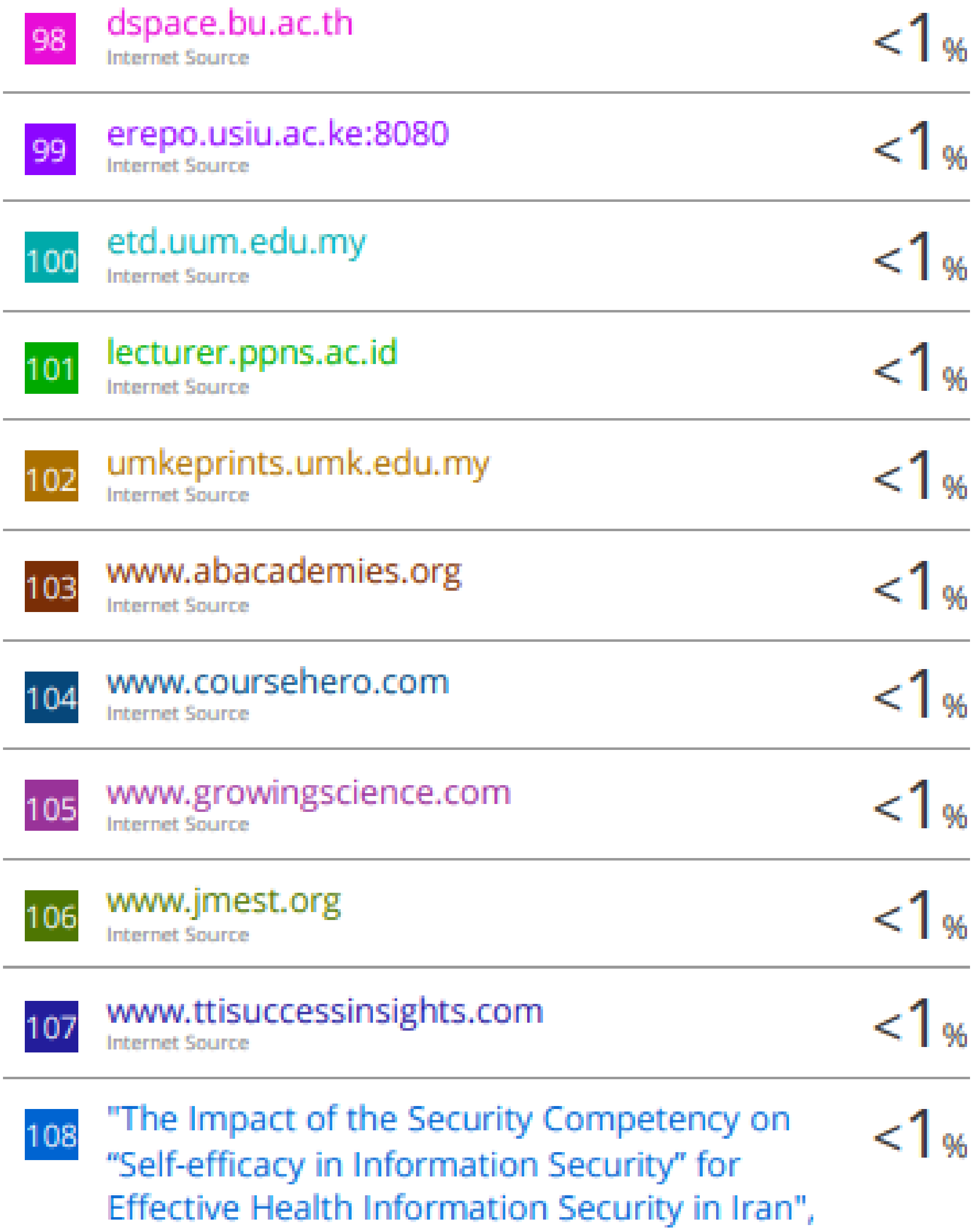
93 Adrian Leguina. "A primer on partial least squares structural equation modeling (PLS-SEM)", International Journal of Research & Method in Education, 2015
Publication
<1%

94 Submitted to Askham Bryan College
Student Paper
<1%

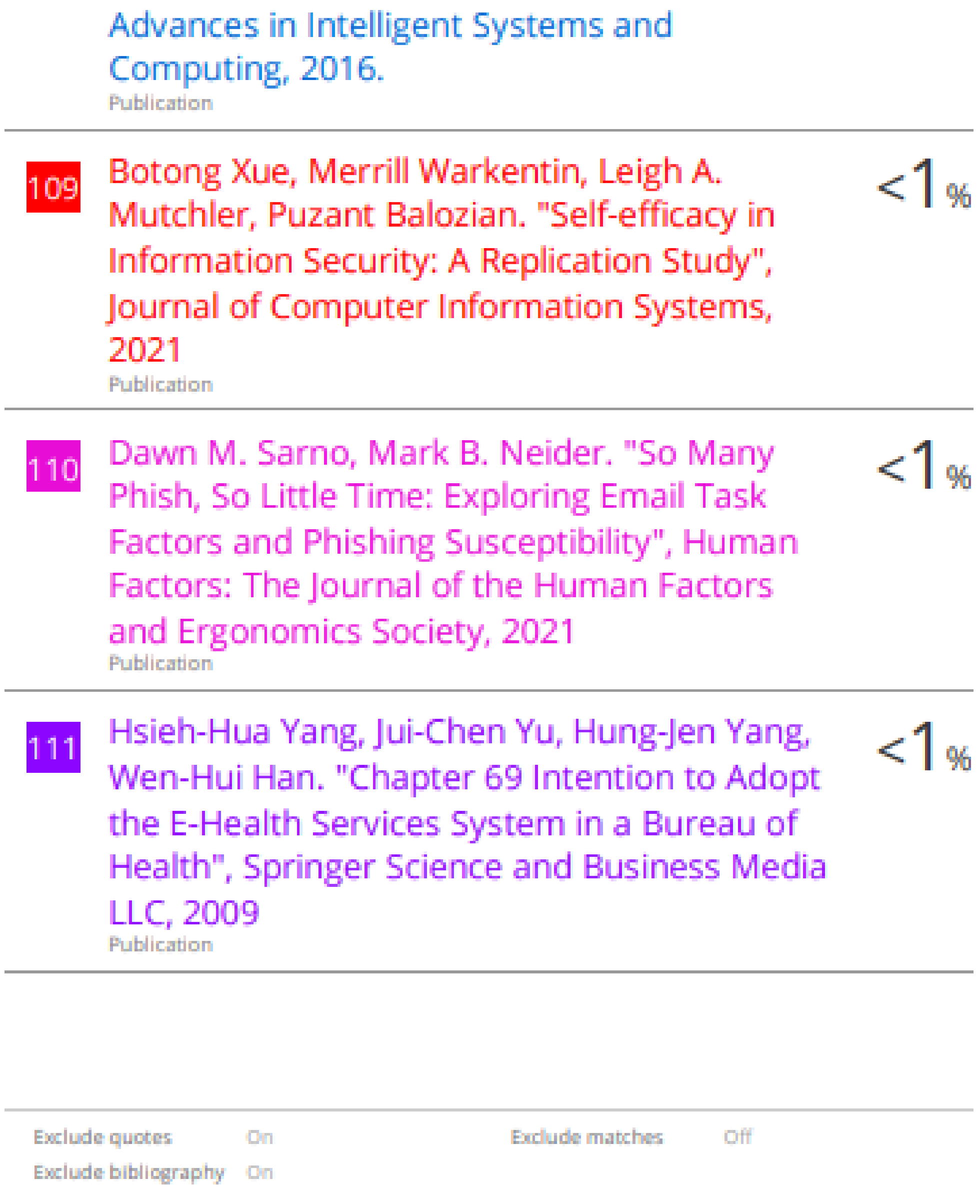
95 Ayman AL-Khatib, Ahmed Shuhaiber. "Green Intellectual Capital and Green Supply Chain Performance: Does Big Data Analytics Capabilities matter?", Research Square Platform LLC, 2022
Publication
<1%

96 Bowling, Ann, Ebrahim, Shah. "EBOOK: Handbook of Health Research Methods: Investigation, Measurement and Analysis", EBOOK: Handbook of Health Research Methods: Investigation, Measurement and Analysis, 2005
Publication
<1%

97 Serkan Ada. "chapter 17 Theories Used in Information Security Research", IGI Global, 2009
Publication
<1%



98	dspace.bu.ac.th Internet Source	<1 %
99	erepo.usiu.ac.ke:8080 Internet Source	<1 %
100	etd.uum.edu.my Internet Source	<1 %
101	lecturer.ppns.ac.id Internet Source	<1 %
102	umkeprints.umk.edu.my Internet Source	<1 %
103	www.abacademies.org Internet Source	<1 %
104	www.coursehero.com Internet Source	<1 %
105	www.growingscience.com Internet Source	<1 %
106	www.jmest.org Internet Source	<1 %
107	www.ttisuccessinsights.com Internet Source	<1 %
108	"The Impact of the Security Competency on "Self-efficacy in Information Security" for Effective Health Information Security in Iran",	<1 %



Advances in Intelligent Systems and Computing, 2016.
Publication

109 Botong Xue, Merrill Warkentin, Leigh A. Mutchler, Puzant Balozian. "Self-efficacy in Information Security: A Replication Study", Journal of Computer Information Systems, 2021
Publication
<1%

110 Dawn M. Sarno, Mark B. Neider. "So Many Phish, So Little Time: Exploring Email Task Factors and Phishing Susceptibility", Human Factors: The Journal of the Human Factors and Ergonomics Society, 2021
Publication
<1%

111 Hsieh-Hua Yang, Jui-Chen Yu, Hung-Jen Yang, Wen-Hui Han. "Chapter 69 Intention to Adopt the E-Health Services System in a Bureau of Health", Springer Science and Business Media LLC, 2009
Publication
<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

PLAGIARISM CHECK RESULT

Universiti Tunku Abdul Rahman			
Form Title : Supervisor's Comments on Originality Report Generated by Turnitin for Submission of Final Year Project Report (for Undergraduate Programmes)			
Form Number: FM-IAD-005	Rev No.: 0	Effective Date: 01/10/2013	Page No.: 1of 1

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

Full Name(s) of Candidate(s)	Yvonne Lee Yi Jin
ID Number(s)	18ACB02825
Programme / Course	Bachelor's Degree of Information Systems (Hons) Business Information Systems
Title of Final Year Project	Cyber Hygiene During COVID-19 to Avoid Cyber Attacks

Similarity	**Supervisor's Comments (Compulsory if parameters of originality exceeds the limits approved by UTAR)**
Overall similarity index: 10 % **Similarity by source** Internet Sources: 7 % Publications: 4 % Student Papers: 5 %	
Number of individual sources listed of more than 3% similarity: 0	

Parameters of originality required and limits approved by UTAR are as Follows:

(i) Overall similarity index is 20% and below, and

(ii) Matching of individual sources listed must be less than 3% each, and

(iii) Matching texts in continuous block must not exceed 8 words

Note: Parameters (i) – (ii) shall exclude quotes, bibliography and text matches which are less than 8 words.

Note Supervisor/Candidate(s) is/are required to provide softcopy of full set of the originality report to Faculty/Institute

Based on the above results, I hereby declare that I am satisfied with the originality of the Final Year Project Report submitted by my student(s) as named above.

Signature of Supervisor

Name: Yap Seok Gee

Date: 22/04/2022

Signature of Co-Supervisor

Name: ______________

Date: ______________

UNIVERSITI TUNKU ABDUL RAHMAN

FACULTY OF INFORMATION & COMMUNICATION TECHNOLOGY (KAMPAR CAMPUS)

CHECKLIST FOR FYP2 THESIS SUBMISSION

Student Id	18ACB02825
Student Name	Yvonne Lee Yi Jin
Supervisor Name	Ms Yap Seok Gee

TICK (√)	**DOCUMENT ITEMS** Your report must include all the items below. Put a tick on the left column after you have checked your report with respect to the corresponding item.
	Front Plastic Cover (for hardcopy)
✓	Title Page
✓	Signed Report Status Declaration Form
✓	Signed FYP Thesis Submission Form
✓	Signed form of the Declaration of Originality
✓	Acknowledgement
✓	Abstract
✓	Table of Contents
✓	List of Figures (if applicable)
✓	List of Tables (if applicable)
	List of Symbols (if applicable)
✓	List of Abbreviations (if applicable)
✓	Chapters / Content
✓	Bibliography (or References)
✓	All references in bibliography are cited in the thesis, especially in the chapter of literature review
✓	Appendices (if applicable)
✓	Weekly Log
✓	Poster
✓	Signed Turnitin Report (Plagiarism Check Result - Form Number: FM-IAD-005)
✓	I agree 5 marks will be deducted due to incorrect format, declare wrongly the ticked of these items, and/or any dispute happening for these items in this report.

*Include this form (checklist) in the thesis (Bind together as the last page)

I, the author, have checked and confirmed all the items listed in the table are included in my report.

____

(Signature of Student)
Date: 21 April 2022