

CYBER SECURITY AWARENESS  
AMONG STUDENTS IN UMP

NUR MADIHAH BINTI MAZLAN

Bachelor of Computer Science  
(Computer Systems and Networking) with Honours

UNIVERSITI MALAYSIA PAHANG

**UNIVERSITI MALAYSIA PAHANG**

**DECLARATION OF THESIS AND COPYRIGHT**

Author's Full Name : NUR MADIHAH BINTI MAZLAN

Date of Birth

Title : CYBER SECURITY AWARENESS AMONG STUDENTS  
IN UMP

Academic Session : 2022/2023

I declare that this thesis is classified as:

- CONFIDENTIAL (Contains confidential information under the Official Secret Act 1997)\*
- RESTRICTED (Contains restricted information as specified by the organization where research was done)\*
- OPEN ACCESS I agree that my thesis to be published as online open access (Full Text)

I acknowledge that Universiti Malaysia Pahang reserves the following rights:

1. The Thesis is the Property of Universiti Malaysia Pahang
2. The Library of Universiti Malaysia Pahang has the right to make copies of the thesis for the purpose of research only.
3. The Library has the right to make copies of the thesis for academic exchange.

Certified by:

\_\_\_\_\_  
(Student's Signature)

\_\_\_\_\_  
(Supervisor's Signature)

\_\_\_\_\_  
Date: 14/02/2023

\_\_\_\_\_  
Syahrizal Azmir bin Md. Sharif  
Date: 14/02/2023

NOTE : \* If the thesis is CONFIDENTIAL or RESTRICTED, please attach a thesis declaration letter.

## THESIS DECLARATION LETTER (OPTIONAL)

Librarian,  
*Perpustakaan Universiti Malaysia Pahang,*  
Universiti Malaysia Pahang,  
Lebuhraya Tun Razak,  
26300, Gambang, Kuantan.

Dear Sir,

### CLASSIFICATION OF THESIS AS RESTRICTED

Please be informed that the following thesis is classified as RESTRICTED for a period of three (3) years from the date of this letter. The reasons for this classification are as listed below.

Author's Name  
Thesis Title

Reasons            (i)  
  
                              (ii)  
  
                              (iii)

Thank you.

Yours faithfully,



---

(Supervisor's Signature)

Date:

Stamp:

Note: This letter should be written by the supervisor, addressed to the Librarian, *Perpustakaan Universiti Malaysia Pahang* with its copy attached to the thesis.



## SUPERVISOR'S DECLARATION

I hereby declare that I have checked this thesis and in my opinion, this thesis is adequate in terms of scope and quality for the award of the Bachelor of Computer Science (Computer Systems and Networking) with Hons.

A handwritten signature in black ink, appearing to be 'SA', is positioned above a horizontal line.

---

(Supervisor's Signature)

Full Name : Syahrizal Azmir bin Md. Sharif

Position : Lecturer

Date : 14/02/2023



## STUDENT'S DECLARATION

I hereby declare that the work in this thesis is based on my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at Universiti Malaysia Pahang or any other institutions.

A handwritten signature in black ink, appearing to be 'Nur Madihah', is written above a horizontal line.

(Student's Signature)

Full Name : Nur Madihah binti Mazlan

ID Number : CA19037

Date : 14/02/2023

CYBER SECURITY AWARENESS  
AMONG STUDENTS IN UMP

NUR MADIHAH BINTI MAZLAN

Thesis submitted in fulfillment of the requirements  
for the award of the Bachelor of Computer Science  
(Computer Systems and Networking) with Honours

Faculty of Computing  
UNIVERSITI MALAYSIA PAHANG

FEBRUARY 2023

## **ACKNOWLEDGEMENTS**

On I would like to express my thankfulness to all who have given me the motivation to complete this thesis. Special appreciations to my supervisor, Mr. Syahrizal Azmir bin Md. Sharif for guiding and giving me opinions in all the time during finishing my thesis and during process of writing this thesis. Truly thanks for gave a consolation and advice to improve all the mistaken.

Moreover, I also would like to recognize will all my instructors and friends, who give me their full of help and support to me during completing this thesis. A special gratitude goes to my course mates, who help me in finishing this thesis by investing energy for talking and gave a counsel to fix all the mistakes.

Not to forget, I would congratulate myself for being able to complete this research study within the deadline given. This research study has opened a new perspective for me to explore and improve my knowledge about new thing. Gaining support from people I mentions above, has helped me in various type of way to ensure that this research study able to be completed.

## ABSTRAK

Pelbagai kebimbangan keselamatan dalam talian berhadapan dengan pengguna internet, yang memerlukan pelaksanaan langkah keselamatan. Pelajar di UMP diwajibkan peka terhadap isu keselamatan siber. Pelajar prasiswazah dan siswazah adalah sasaran untuk kajian ini, yang bertujuan untuk mengukur tahap pengetahuan mereka mengenai keselamatan maklumat. Untuk mencapai matlamat penyelidikan ini, kami menggunakan pendekatan Teori Model Motivasi Perlindungan (PMT). Tinjauan terhadap (N=148) responden telah dijalankan menggunakan PMT untuk memastikan sejauh mana pengetahuan tentang faktor PMT meramalkan objektif keselamatan. Niat keselamatan dalam talian paling baik diramalkan dengan mengatasi ciri-ciri penilaian, terutamanya keberkesanan diri dan keberkesanan tindak balas. Penilaian ancaman adalah satu lagi peramal penting. Model PMT tradisional menggabungkan kerentanan ancaman dan keterukan ancaman.



## **ABSTRACT**

A range of online security concerns confront internet users, necessitating the implementation of safety measures. Students at UMP are required to be aware of cyber security issues. Undergraduate and graduate students are the target audience for this study, which aims to gauge their degree of knowledge regarding information security. To accomplish the goal of this research, we are utilizing the Protection Motivation Model Theory (PMT) approach. A survey of (N=148) respondents was conducted using PMT to ascertain the extent to which knowledge of PMT factors predicted security objectives. Online safety intentions were best predicted by coping appraisal characteristics, particularly self-efficacy and response efficacy. Threat assessment was another important predictor. The traditional PMT model incorporates threat susceptibility and threat severity.

## TABLE OF CONTENT

|                                    |            |
|------------------------------------|------------|
| <b>DECLARATION</b>                 |            |
| <b>TITLE PAGE</b>                  |            |
| <b>ACKNOWLEDGEMENTS</b>            | <b>ii</b>  |
| <b>ABSTRAK</b>                     | <b>iii</b> |
| <b>ABSTRACT</b>                    | <b>iv</b>  |
| <b>TABLE OF CONTENT</b>            | <b>v</b>   |
| <b>LIST OF TABLES</b>              | <b>ix</b>  |
| <b>LIST OF FIGURES</b>             | <b>x</b>   |
| <b>LIST OF ABBREVIATIONS</b>       | <b>xi</b>  |
| <b>CHAPTER 1 INTRODUCTION</b>      | <b>1</b>   |
| 1.1 Introduction                   | 1          |
| 1.2 Problem Statement              | 3          |
| 1.3 Objective                      | 4          |
| 1.4 Scope                          | 4          |
| 1.5 Significance of Research       | 5          |
| 1.6 Thesis Organization            | 6          |
| <b>CHAPTER 2 LITERATURE REVIEW</b> | <b>7</b>   |
| 2.1 Introduction                   | 7          |
| 2.2 Overview of Cyber Security     | 8          |
| 2.2.1 Concept of Cyber Security    | 9          |
| 2.2.2 Impact of Cyber Security     | 9          |

|                              |  |           |
|------------------------------|--|-----------|
| 2.2.3                        | Prevention of Cyber Security   | 10        |
| 2.3                          | Preview existing theoretical framework   | 11        |
| 2.3.1                        | Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behaviour using PMT | 11        |
| 2.3.2                        | Mobile Information Security Awareness among Students in Higher Education using KAB and TPB model           | 15        |
| 2.3.3                        | A Review and Insight on the Behavioural Aspects of Cybersecurity using TPB                                 | 18        |
| 2.4                          | Comparison of existing theoretical framework   | 20        |
| 2.5                          | Conclusion of the theories   | 24        |
| <b>CHAPTER 3 METHODOLOGY</b> |  | <b>25</b> |
| 3.1                          | Introduction   | 25        |
| 3.2                          | Project Management Framework (PMT Model)   | 26        |
| 3.2.1                        | Related Work with Protection Motivation Theory (PMT)   | 28        |
| 3.3                          | Research Design  | 36        |
| 3.3.1                        | Quantitative Method  | 36        |
| 3.4                          | Research Approach – Questionnaire Method   | 37        |
| 3.4.1                        | Sampling and Data Collection   | 37        |
| 3.4.2                        | Data Analysis and Result   | 37        |
| 3.4.3                        | Participants   | 38        |
| 3.5                          | Research Requirement   | 39        |
| 3.5.1                        | Input and Output   | 39        |
| 3.5.2                        | Constraint and Limitation  | 39        |
| 3.5.3                        | Case Study   | 39        |
| 3.6                          | Proposed Model   | 40        |
| 3.6.1                        | Threat Appraisal   | 40        |

|  |                                    |           |
|--|------------------------------------|-----------|
| 3.6.2                                    | Coping Appraisal                   | 41        |
| 3.7                                      | Proof of Initial Concept           | 42        |
| 3.7.1                                    | Pilot Questionnaire                | 42        |
| 3.8                                      | Expected Outcome                   | 43        |
| 3.9                                      | Hardware and Software Requirements | 44        |
| 3.9.1                                    | Hardware Requirement               | 44        |
| 3.9.2                                    | Software Requirement               | 44        |
| 3.10                                     | Gantt Chart                        | 45        |
| <b>CHAPTER 4 RESULTS AND DISCUSSION</b>  |                                    | <b>46</b> |
| 4.1                                      | Introduction                       | 46        |
| 4.2                                      | Analysis and Results               | 47        |
| 4.2.1                                    | Socio Demographic Characteristic   | 47        |
| 4.2.2                                    | Descriptive Analysis               | 50        |
| 4.2.3                                    | Reliability Test                   | 58        |
| 4.2.4                                    | Spearman's RHO Test                | 59        |
| 4.2.5                                    | Hypothesis Testing                 | 64        |
| 4.3                                      | Discussion                         | 66        |
| <b>CHAPTER 5 CONCLUSION</b>              |                                    | <b>68</b> |
| 5.1                                      | Introduction                       | 68        |
| 5.2                                      | Limitations                        | 68        |
| 5.3                                      | Future Work                        | 69        |
| 5.4                                      | Summary                            | 69        |
| <b>REFERENCES</b>                        |                                    | <b>70</b> |
| <b>APPENDIX A LIST OF QUESTIONNAIRES</b> |                                    | <b>72</b> |

|                                       |           |
|---------------------------------------|-----------|
| <b>APPENDIX B GANTT CHART</b>         | <b>80</b> |
| <b>APPENDIX C NON-PARAMETRIC TEST</b> | <b>81</b> |

## LIST OF TABLES

|  |    |
|--|----|
| Table 2-1 Comparison of existing theoretical framework   | 20 |
| Table 3-1 Questionnaire of Security Measure  | 30 |
| Table 3-2 Questionnaire of Smartphone  | 34 |
| Table 3-3 Hardware Requirement   | 44 |
| Table 3-4 Software Requirement   | 44 |
| Table 4-1 Summarize of Demographic result  | 49 |
| Table 4-2 Statistics of Security Intentions  | 51 |
| Table 4-3 Statistics of Threat Severity  | 52 |
| Table 4-4 Statistics of Threat Susceptibility  | 53 |
| Table 4-5 Statistics of Self-Efficacy  | 54 |
| Table 4-6 Statistics of Response Efficacy  | 56 |
| Table 4-7 Reliability Statistics   | 58 |
| Table 4-8 Correlation between threat severity and individual's intention to cyber security       | 60 |
| Table 4-9 Correlation between threat susceptibility and individual's intention to cyber security | 61 |
| Table 4-10 Correlation between self-efficacy and individual's intention to cyber security        | 62 |
| Table 4-11 Correlation between response efficacy and individual's intention to cyber security    | 63 |
| Table 4-12 Summary of Hypothesis test result   | 64 |

## LIST OF FIGURES

|  |    |
|--|----|
| Figure 2-1 KAB Model                                 | 16 |
| Figure 2-2 PMT Model                                 | 21 |
| Figure 2-3 KAB Model                                 | 21 |
| Figure 2-4 TPB Model                                 | 21 |
| Figure 3-1 PMT Framework                             | 26 |
| Figure 3-2 General PMT Model                         | 27 |
| Figure 3-3 The Adjusted PMT Model                    | 28 |
| Figure 3-4 Research Model using PMT approach         | 40 |
| Figure 4-1 Proposed PMT Model                        | 46 |
| Figure 4-2 Pie chart of Age                          | 47 |
| Figure 4-3 Pie chart of Faculty                      | 48 |
| Figure 4-4 Pie chart of Highest Education Background | 48 |

## **LIST OF ABBREVIATIONS**

|      |                                     |
|------|-------------------------------------|
| PMT  | Protection Motivation Theory        |
| TPB  | Theory Planned Behaviour            |
| KAB  | Knowledge-Attitude-Behaviour        |
| ISA  | Information Security Awareness      |
| ISSP | Information Systems Security Policy |
| TAM  | Technological Acceptance Model      |



# CHAPTER 1

## INTRODUCTION

### 1.1 Introduction

In modern times, there's the internet, and there's technology that connects us to a modern culture that evolves through time. Nowadays, technology, particularly the internet, is required for almost every profession and work, whether it is a way to store data, e-mail, crucial data collection, or even a meeting. Furthermore, people's social lives are also influenced by the internet, which is seen as a necessary daily tool. As can be observed, many people are "obsessed" with publishing personal information on social media platforms, such as their habit and orientation, as well as where they travelled and photographs. Without a doubt, the entire globe faces numerous issues in terms of hacker or cracker exploitation, as well as spammers, in numerous situations of sectors such as Internet security, software privacy, email, and so on [1].

Cyber security is a technique for securing computers, databases, portable devices, communications devices, networks, and data from malicious attacks. Cyber security awareness entails being conscious of security in everyday situations. Being aware of the risks of accessing the web, reading email, and engaging in online activities is part of cyber security awareness. The creation of a particular strategy must surmount potential hurdles and threats from both in and out of the business in order to synchronise with the organization's policy. In Malaysia, a result of the boundless and confidential communication, users face a number of security risks. Everything that related to the cyber security not only applied through mobile, but it is also can be applied by using computer and other electronic devices. According to the Internet World Statistics (2020), there are almost 3 billion internet users worldwide, signifying a 57.7 percent rise in growth from 2000 [2].

In University Malaysia Pahang, there are more than 3,000 users among students that live their lives through their technology devices. The accessibility of broadband services and the corresponding network connectivity of modern gadgets allow the majority of students to stay connected at all times, as well as the numerous apps available [3]. Because massive quantities of confidential material are collected and transmitted through with a variety of devices, individual employees and students are great targets for cyberattacks.

## 1.2 Problem Statement

Nowadays, the number of cyber-attacks and cyber-criminal are rising not just globally but also domestically. Paradoxically, persons with such abilities frequently violate their own abilities by misusing them, and the odds of becoming a cyber-crime victim are even higher for those with less IT capabilities. When it comes to security concerns and problems in higher education, the first issue is the potential loss of university information and intellectual assets. This is not because of the stealing the data information from certain website require a high degree of technical skill to perform a computer crime. It can easily to steal by taking the system. This problem come from human careless which can lead to greatest risks to an organization's information security procedures [1].

In addition, the use of public free Wi-Fi by students is on the rise as they try to connect to their university network connection using their own devices. There is a rise in the quantity of devices linked to the university network grows, so does the number of possible attacks. This includes the propagation of harmful malware, ransomware, and identity theft, in which attackers seek to obtain access to the university network via their devices that have been compromised [2], [3]. Most students do not log out of apps after using them, do not use a password on their devices, possibly allow apps to access national and organizational data held on these devices, and install apps, open attachments, and click on web addresses from unverified senders.

Moreover, most of the smart Internet users are lacked awareness in information security threats. Many of them are higher education students which been categorized as heavy Internet users compared to the others. Meanwhile, most of the institutions in Malaysia is at risk because of its ignorance of cybersecurity. Thus, so much of their everyday contact and educational activities take place on the Internet, students in higher education are subject to cyber security concerns [4].

### **1.3 Objective**

Based on the problem statements, the objectives of the research are:

- i) To study the level of knowledge about information security awareness among the students in UMP
- ii) To propose a Protection Motivation Theory (PMT) model that improve information security awareness among UMP's students
- iii) To evaluate the individual's information security awareness in cyber security threats based on the proposed model

### **1.4 Scope**

- User Scope:
  - i. Undergraduate and postgraduate students of UMP aged 18 to 30 years old
  
- System Scope
  - i. Defined as students' general knowledge about information security awareness
  - ii. Defined depending on people's individual situations that will be explored in higher education to see if differences in circumstances lead to distinct outcomes
  
- Development Scope
  - i. Online Survey Method (Google Form)

## **1.5 Significance of Research**

### **i) Undergraduate and Postgraduate student**

Student will be exposed to the awareness of cyber security. Students will be more aware of the importance of keeping passwords private, not updating passwords on a regular basis, while using the same password for many apps. They also can practice to beware on opening email attachments from unknown people. Students also will be provided knowledge to upgrade their understanding about cyber security issues and can be protected from the threat of cybercrime and the proliferation of cybersecurity threats.

## **1.6 Thesis Organization**

### **a. Chapter 1**

In this chapter, the researcher is discussing about the introduction of cyber security awareness among students in UMP towards endemic. Then, the researcher explains about the problem statement that need to be developed. The problem statement, objective, scope, and significance of the research can all be found in this chapter of the thesis.

### **b. Chapter 2**

This section is described the literature review of Cyber Security awareness among students in UMP towards endemic. The researcher also discussed three theories that have been used to measure the level of awareness about information security. At the end of this chapter, the researcher is come out with the comparison between three theories that are related to this thesis.

### **c. Chapter 3**

In chapter 3, the researcher discussed about the methodology for Cyber Security Awareness among students in UMP towards endemic. In addition, the researcher also discusses about the model that has been proposed.

### **d. Chapter 4**

In chapter 4, the researcher does the implementation about the result that get from the respondents and explained in detail about the discussion for this survey. The process of calculating the result from the respondents is stated in this chapter.

### **e. Chapter 5**

This chapter is discussing about the conclusion for the implementation of the result and the limitation and future works also will be mentioned at the end of this chapter.

## **CHAPTER 2**

### **LITERATURE REVIEW**

#### **2.1 Introduction**

A research study of a few references on information cyber security awareness will be presented depth in this chapter, which is a literature review. There are five subtopics under this chapter. In subtopic 2.2 has been discussed in detailed about cyber security and information security awareness. In subtopic 2.3 will preview on existing theoretical framework. After that, the comparison of existing theoretical framework has been discussed under subtopic 2.4. Lastly, in subtopic 2.5, the summary for the best theoretical has been discussed for future used in cyber security awareness among students in UMP towards endemic.

## 2.2 Overview of Cyber Security

Cyber security is a global topic that poses governments face a challenging social economic challenge while simultaneously need public engagement. Since cybersecurity is among the most pressing issues facing governments today, public knowledge and visibility are still lacking [5]. A combination of technologies, methods, and procedures aimed at preventing assaults, damage, and unauthorised networking, devices, programmes, and data is known as cyber security. Information security awareness (ISA) is one of the two main elements of sensory perception, another factor is action. It is characterised as a person's passive participation and heightened interest in certain subjects [6]. Information security awareness helps to ensure the privacy, reliability, and authenticity of both individual and corporate information assets and resources. ISA also can be specific as which member of human understands the relevance protection of data, the suitable levels of information security, and acts in accordance with their own security responsibilities.

Despite the fact that practically everybody has heard about cybersecurity, people's actions and urgency do not indicate a good level of expertise. The Internet is frequently portrayed as a secure platform for sharing messages, performing commerce, and regulating the material reality. Cyberwarfare is already in progress, and better preparedness is essential. Cyber-attacks against universities and academic organisations have become valuable targets, with a number of high-profile incidents already occurring. Academic institutions are attractive target of cyber, cyberterrorists, and surveillance because they handle vast amounts of valuable data and sensitive personal information. The attack surface is wide, ranging from opportunists looking for a quick money to substantially financed legislature groups trying to steal proprietary information [7].



### **2.2.1 Concept of Cyber Security**

The notion of cyber-security has evolved to create and maintain a safe computer infrastructure for all users in response to the increasing threat of cyber-related offenses. A complete definition of cyber-security has yet to be developed by several international and national agencies. As a result, there is a gap in our knowledge of cyber-security, because real-world activities are coupled with an artificial environment that is connected globally [8].

In the cybersecurity industry, cyber security works to ensure that an organization's and users' system security is attained and maintained against security-related hazards. The general aims are said to include accessibility, honesty, and secrecy. It may be argued that cyber-security is a catch-all word for a variety of distinct and fragmented security threats, all of which have one thing in common: the usage of cyberspace and the Internet [8]. According to the Royal Malaysian Police, cybercrime has eclipsed drug trade as the most profitable burglary, with cybercrime accounting for 70% of all professional criminal offences [9].

### **2.2.2 Impact of Cyber Security**

The consequence of cyber security awareness is not a short term, they long last knowledge that everybody needs to practice. This is because by having cyber security awareness among students will not produce the cyber security threats. Cyber security impact can reveal students' personal information. They will do that activity with conscious when they think that by revealing their personal information is not a big deal. These cybersecurity vulnerabilities can have major consequences for higher education students, including loss of revenue, cyberbullying, asset destruction, identity fraud, and so on. It is necessary to raise a teenager's cybersecurity awareness, which is the most important aspect of this study [10].

### **2.2.3 Prevention of Cyber Security**

One of the smartest actions that students can do for personal system is to secure and hide their Wi-Fi networks. Millions of computers linked to the network and expose to becoming available everyday as technology advances.

Every application and programme require a unique login for each student. Students' personal information may be jeopardised if many individuals connect to use the same identities. By giving each member a unique login, the number of assault fronts can be decreased. Users are only allowed to log in once per day and will only utilize their own set of logins. You won't just receive better security; you'll also get friendly user interface.

## **2.3 Preview existing theoretical framework**

In this section, the theories providing the bases for this study as well as the model are presented. The Protection Motivation Theory (PMT) is described in Section 2.3.1. The Knowledge-Attitude-Behaviour (KAB) is described in Section 2.3.2 and in Section 2.3.3, the studied construct the Theory of Planned Behaviour (TPB).

### **2.3.1 Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behaviour using PMT**

In this thesis, the authors are more focused on implement the protection motivation theory (PMT) approach in order to improve information assurance behaviour study in the employment, researchers established the conceptual areas of the safety of employees behaviour and developed and evaluated determined based and to look at the impact of PMT safety behaviour influences, perceived organizational influence, as well as administrative cultural pressure calls to action on employees' present cybersecurity habits [11].

#### **2.3.1.1 Protection Motivation Theory (PMT)**

The Protection Motivation Theory (PMT) examines how people are driven to deal with threats or harmful behaviour warnings [11]. PMT is one of many hypotheses that can be used to explain why someone wants to take proactive cyber security measures. The PMT model has been used to analyse information security challenges when employees require incentives to secure their company's information systems because it stresses adopting defensive actions in relation to personal health issues. The PMT was used to explore how employees who perceive cyberthreats and develop coping behaviours from a range of perspectives. Because it is characterised as a previous constructor in the PMT Model, employee action experiences play a significant role in the conservation of resources theory.

The PMT can be used to describe how people judge the risk level posed by dangerous cyber-crime based on the results of this study. Numerous cyberattacks will be faced by students, including self-efficacy and response efficacy. They must, on the other hand, deal with and prevent the harm or lost opportunity of information that may result from a threat [11]. It can be one's trust in managing a disease system when dealing with

a cyber security issue. When coping with a cyber security issue, it can be one's personal conviction in managing a virus-infected machine. Similarly, if students do not believe they are dealing with true cybersecurity crime, they will be unconcerned about the gravity of the crime. Individuals' security experiences and views, as well as the training provided by the other people, all have a substantial impact on the perceived seriousness of information security. Their perceptions of the threat posed by a cyber-attack incidence and their perceptions of a lack of preventative measures and actions are referred to as perceived vulnerability. Students that have prior information security expertise in organizing cybersecurity breaches, on the other hand, are far less susceptible in blocking new cyber-attacks.

#### I. Employee's organizational environment

Peer behaviour, action's cues, and the employee's expertise all contribute to the employee's operational environment. Employees' cybersecurity actions are influenced by either internal or extrinsic motivators, such as peer behaviour. Employees prefer to behave similarly as their co-workers when it comes to cybersecurity. There are a variety of other types of action cues or social influence that might favourably affect user behaviour, such as delivering a lecture on cyber knowledge, giving out message of caution about possibilities for safety crimes, or a colleague's dedication to safety and security. As a result, we claim that peer behaviour provides social influence, which employees' signals are triggered to combat internet., and that the causal relation among peer behaviour and cues to action is positive. We anticipate:

**H1.** Peer behaviour has a direct beneficial effect on cues to action for employees' cybersecurity behaviours.

**H2.** Employees' cybersecurity action satisfaction is strongly influenced by cues to action.

#### II. Cybersecurity behaviour appraisal and the protection motivation theory

From a variety of viewpoints, the PMT has been used to investigate how employees perceive cybersecurity threats and create coping behaviours. As a result, we employ the PMT model is used to describe how a user's prior information security knowledge effects

their impression of seriousness and susceptibility, as well as to assess the impact of PMT on user behaviour. The following hypotheses emerge from this discussion:

**H3a.** Professionals' security orientation is positively related to their perception of cybercrime severity.

**H3b.** Personnel' cybersecurity expertise is linked to their perception of vulnerability as a result of cybercrime.

Individuals' imagined cybersecurity hurdles are based on their prior experience. When it comes to cybersecurity precautionary processes, the more expertise they have, the lower the barrier they will perceive. As a result, we anticipate:

**H3c.** Employees with more experience in information security see fewer barriers when doing cybersecurity activities.

More the cybersecurity expertise employees have, the more confident they are in the ability of cybersecurity policies to avert a danger. We believe that the more knowledge an individual has with information security, the better equipped he is to carry out appropriate response measures. As a result, we anticipate:

**H3d.** Employees' cybersecurity adventure improves their response-efficacy when confronted with cybersecurity events.

**H3e.** Employees' cybersecurity option is to try their consciousness when it comes to dealing with cybersecurity concerns.

### III. Employee cybersecurity behaviour

We suggest that these contradictory results could be explained by a variety of methodological approaches. First, the discrepancies could be related to a smaller sample size, which means there is less power to identify connections between PMT component forecasts and cyber-security defensive behaviours. Second, some of the PMT model's variables are interrelated, it's impossible to analyse each predictor's unique contribution without modelling the entire framework. Finally, the assessment of security behaviour utilised as a criteria measure varies widely between studies, with many focusing on

gauging future behavioural intentions rather than attempting to examine employees' existing behaviours.

**H4a.** Employees' perceptions of cybersecurity severity have a beneficial impact on their cybersecurity protection behaviour.

**H4b.** Employees' perceived vulnerability has a beneficial influence on their cybersecurity defences activity.

**H4c.** Employees' perceptions of hurdles have a detrimental effect on their cyber capability's behaviour.

**H4d.** Employees' reaction efficacy has a favourable bearing on their cyber measure's behaviour.

**H4e.** Employees' self-efficacy has a favourable impact on their cybersecurity protection behaviour.

#### IV. Information policy awareness and compliance

Data security professionals throughout the world have experienced turbulence as their implement network security technologies and methods to keep up with the current information security threats. Employees typically do not readily follow such rules and standards, even if an information systems security policy (ISSP) is in better position to help maintain the company's IS assets and protect the integrity, abuse, and loss of its information systems. It is proposed that the following hypothesis be tested:

**H5.** Employees' cybersecurity defence behaviour will improve as they become more knowledgeable of information security policies.

### **2.3.2 Mobile Information Security Awareness among Students in Higher Education using KAB and TPB model**

In this thesis, the authors are more focused on implement the knowledge-attitude-behaviour (KAB) model and Theory of Planned Behaviour (TPB) approaches in order to measure information security awareness among students in higher education.

#### **2.3.2.1 Knowledge-Attitude-Behaviour (KAB) model**

The KAB model looked at how health information campaigns knowledge (K) influenced health behaviour, as well as the expectation of attitude change (A) and subsequent desired behaviour (B) modifications, producing the K-A-B continuum [3]. Most effective information security initiatives are based on the KAB paradigm, which focuses primarily on the human being's knowledge aspect. Changes in attitude are launched as knowledge accumulates in a relevant behaviour, such as cybersecurity, health, the environment, education, and so on, according to the KAB model. It essentially discusses the role of knowledge in behaviour change and knowledge gain. In the KAB model, this accumulation of information leads to a shift in attitude and, eventually, a shift in conduct.

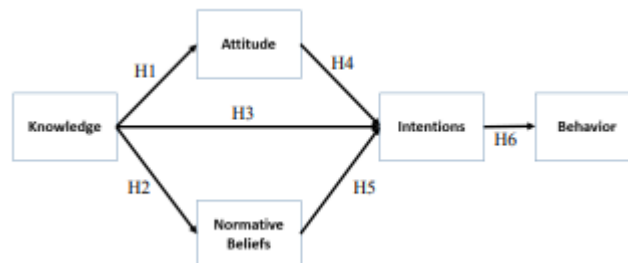
The basic concept of the KAB model regarding information security is that as knowledge about information security grows, so does one's attitude toward information security, and as a result, one's behaviour changes. According to the findings, having sufficient understanding did not necessarily change students' attitudes toward ISA, but there are also other factors that are expected to influence students' attitudes, including such personality and culture. For example, the loss of university information and knowledge assets. Even though the students having enough information about cyber security awareness, how it happens, but the current situation which they exposed to share everything without thinking the effect also can cause problems. It is also based on their personality, not all of them are easily to do this thing but most of them act based on their behaviours.

### 2.3.2.2 Theory of Planned Behaviour (TPB)

The TPB uses three criteria to predict behavioural intention: normative beliefs, disposition, and control beliefs. It asserts that intentions drive changes in behaviour. Attitudes and subjective norms influence intentions. Individuals' perceptions of social order to engage or not engage in a given conduct are referred to as subjective norms. As a result, the focus of this study is on five components: knowledge, attitude, normative views, intention, and behaviour [3]. The term "attitude" refers to how a person feels about and evaluates the conduct in question. Social pressure to engage in specific behaviours is captured by subjective norms. In PMT, perceived behavioural control is similar to self-efficacy except that it refers to a person's ability to accomplish a task. Security researchers have utilised TBP to predict safety compliance behavioural intention.

### 2.3.2.3 Proposed Model and Hypothesis

This work proposes and tests a research model that blends elements from the KAB and TPB models to increase understanding of mobile device security behaviours. The broad hypothesis is that information security intentions and behaviour are influenced by understandings, mindsets, and beliefs regarding information security.



**Figure 2-1 KAB Model**

Students between the ages of 18 and 30 are more susceptible to security concerns since they explore so much time online and on social media. They also have less familiarity with information assurances. The following are some hypotheses that have been proposed:

**H1.** Students' understanding of information security has a favourable impact on their attitudes toward information security awareness.



**H2.** Information security knowledge among students has a favourable impact on normative ideas regarding information security awareness.

**H3.** Students' knowledge of information security has a favourable impact on their information security intents.

**H4.** Students' attitudes regarding information security have a favourable impact on their information security intents.

**H5.** Students' attitudes toward information security have a beneficial impact on their intents to protect information.

**H6.** Information security awareness practises are positively influenced by students' intentions about information security.

#### **2.3.2.4 Summary of this research**

In a nutshell, the research demonstrates that students in higher education are increasingly using mobile communication devices. This widespread use of tech for mobile phones raises the risk of mobile cybersecurity threats, particularly among students in a university education who are still building their cybersecurity awareness. The goal of this study was to learn more about the individual elements that influence students' mobile security habits. The study's findings, which were based on existing constructs from the KAB and TPB models, imply that knowledge of dangers to security and intents to be security function influence students' mobile security behaviour. The study also highlighted the well-known "knowing vs doing" contradiction, wherein students' understanding of information security does not transition into practices for information safety and security.

### **2.3.3 A Review and Insight on the Behavioural Aspects of Cybersecurity using TPB**

In this thesis, the authors are more focused on implement the theory of planned behaviour (TPB) approach in order to improve for networks' defenders [12].

#### **2.3.3.1 Theory of Planned Behaviour (TPB)**

The theory of planned behaviour (TPB) is employing a prediction model that suggests subjective standards and attitudes have an impact on behavioural intent. People's positive attitudes, according to the TPB, are an excellent predictor of their actual conduct. The subjective norm is another way of looking at conduct. The perceived behavioural control refers to how easy or difficult it is to conduct an activity. In general, the more positive an individual 's lifestyle, social norm, and perceived behavioural control are toward an action, the more likely they are to display that behaviour. Beliefs are linked to attitude (behavioural, normative and control). Furthermore, several academics link social pressure to guidelines recommended. Understanding the functions of numerous behavioural elements and figuring out which ones are the most accurate predictors will be important in incorporating them into an intrusion prevention system or a prophylactic plan [12].

The author coupled the TPB with the Technological Acceptance Model (TAM) to discover that technological understanding is a determinant of a user's effort expectancy to employ anti-virus or anti-spyware software. Awareness of technology has a major impact on performance expectancy and attitudes about behaviour. They also discovered that TPB and TAM opinions are highly linked to awareness, and they urged managers to develop social activist groups and networks. Their job is to raise awareness about cybercrime [12]. The TPB has been commonly used to look into the ethical conduct of information systems and people's decisions to use appropriate information security protocols. The TPB has been used in various investigations of information security policy compliance and direct noncompliance. The TPB is considered based on amount of knowledge that has been get from students in UMP.

### **2.3.3.2 Summary of this research**

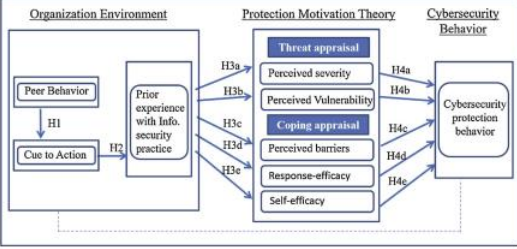

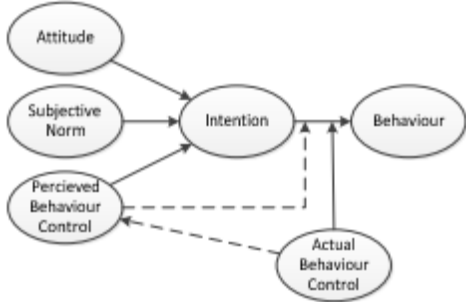
The study of cybersecurity's behavioural patterns is becoming highly prevalent. Human behaviour is unpredictable, which makes it an indispensable tool and supporter of security. The objective of this presentation is to underline the importance of social, interactions, surroundings, prejudices, impression, punishment, desire, disposition, typical, options, consequences, decision making, and other variables in comprehending cybercrime. Although each of these theories has its own set of limitations, they can be combined to strengthen a behavioural model. The habits and goals which is necessary to comprehend and imitate both the consumer and the perpetrator. Strengthening this area will undoubtedly assist in increasing readiness and preventing incidents. The concept can also help mitigate failure caused by social engineering or influence weapons. As a result, future research will enable a novel type of cyber ontology.

## 2.4 Comparison of existing theoretical framework

Based on the table below, it shows the comparison between three theories that have been discussed in 2.3 the comparison of existing theoretical framework is based on the advantages and disadvantages of using the theories to know the level of awareness between students in UMP.

**Table 2-1 Comparison of existing theoretical framework**

|               | <b>Protection Motivation Theory (PMT)</b>  | <b>Knowledge-Attitude-Behaviour (KAB)</b>  | <b>Theory of Planned Behaviour (TPB)</b>  |
|---------------|--|--|---|
| <b>Title</b>  | Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behaviour using PMT | Mobile Information Security Awareness Among Students in Higher Education using KAB model and TPB | A Review and insight on the behavioural aspects of cybersecurity                      |
| <b>Author</b> | Ling Lia, Li Xua, Ivan Asha, Mohd  | Tankiso Moletsane, Pitso Tsibolane   | Rachid Ait Maalem Lahcen, Bruce Caulkins, Ram Mohapatra <sup>1</sup> and Manish Kumar |
| <b>Model</b>  | Protection Motivation Theory (PMT) model and Conceptual Model  | Knowledge-Attitude-Behaviour (KAB) model and the Theory of Planned Behaviour (TPB)               | Technological Acceptance Model (TAM)  |

|                   |  |  |  |
|-------------------|--|--|--|
|                   |  <p style="text-align: center;"><b>Figure 2-2 PMT Model</b></p> |  <p style="text-align: center;"><b>Figure 2-3 KAB Model</b></p> |  <p style="text-align: center;"><b>Figure 2-4 TPB Model</b></p> |
| <b>Knowledge</b>  | √  | √  |  |
| <b>Attitude</b>   | √  | √  | √  |
| <b>Behaviour</b>  |  | √  | √  |
| <b>Method</b>     | Survey   | Survey   | Mathematical   |
| <b>Hypothesis</b> | <b>H1.</b> Peer behaviour has a direct beneficial effect on cues to action for employees' cybersecurity behaviours.                              | <b>H1.</b> Students' understanding of information security has a favourable impact on their  |  |

|                      |   |   |  |
|----------------------|---|---|--|
|                      | <p><b>H2.</b> Employees' cybersecurity action satisfaction is strongly influenced by cues to action.</p> <p><b>H3a.</b> Professionals' security orientation is positively related to their perception of cybercrime severity.</p> <p><b>H3b.</b> Personnel' cybersecurity expertise is linked to their perception of vulnerability as a result of cybercrime.</p> <p><b>H3c.</b> Employees with more experience in information security see fewer barriers when doing cybersecurity activities.</p> | <p>attitudes toward information security awareness.</p> <p><b>H2.</b> Information security knowledge among students has a favourable impact on normative ideas regarding information security awareness.</p> <p><b>H3.</b> Students' knowledge of information security has a favourable impact on their information security intents.</p> <p><b>H4.</b> Students' attitudes regarding information security have a favourable impact on their information security intents</p> |  |
| <b>Result/Output</b> | According to the findings of our research, employees in the United States have already been marshalling capabilities for digital  | This was a solitary case observational research with a modest sample size (n=397) that  | Network security, along with all of the technologies that go with it, isn't perfect. In reality, there is no such thing as the |

|                    |  |  |  |
|--------------------|--|--|--|
|                    | transformation in order to confront modern cybercriminals. Employees at a variety of companies have noticed issues created by cybercriminals as they devise and execute new security protocols, methods, technology, and equipment to keep up with market changes.   | looked at one South African public higher education institution. This has the capacity to redefine the results' generalizability. A more representative study could give more generalizable findings.  | perfect security. As a result, there is a constant need to develop and maintain new technological solutions. This is where modelling and simulation come in handy for saving time and money while developing testbeds or settings in which software inventions or techniques may be put to the test.   |
| <b>Limitations</b> | The response variable in the conceptual model is personality cybersecurity behaviour. Although numerous published research has used this method, it is prone to self-report bias. Future research should create measurements to compare the outcomes of genuine cybersecurity activity with self-reported cybersecurity behaviour. | According to the available literature, students in higher education are increasingly using mobile communication devices. This widespread use of mobile technology raises the risk of mobile cybersecurity threats, particularly among students in higher education who are still building their cybersecurity awareness. | The research of cybersecurity's behavioural patterns is becoming extremely valuable. Humans are an important component because of the unexpected complexity of human behaviours and enabler of cybersecurity. The habits and goals of both the user and the offender should be understood and imitated |

## **2.5 Conclusion of the theories**

In this chapter, three theories that have been applied to implement the cyber security information awareness have been reviewed and discussed in detail. Then, the comparison between the three theories have been discussed. For the information cyber security awareness will be used is based on the advantages of existing theories.



## **CHAPTER 3**

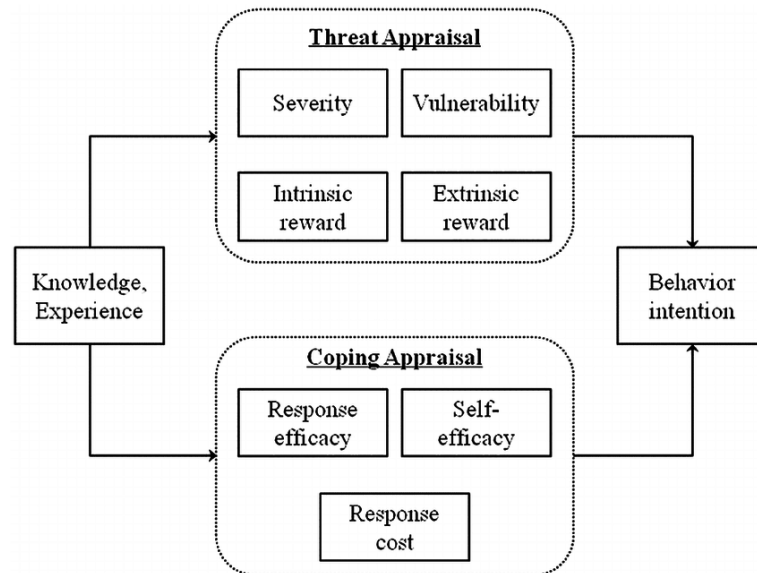
### **METHODOLOGY**

#### **3.1 Introduction**

This chapter will discuss the method that was selected and used to prove this study. Methodology is the way to strategize the method used in the research to complete the research. The approach, which includes a literature evaluation and data collecting, is discussed first. This chapter will also go over the software and hardware that were employed to make the study a success. In addition, this chapter will cover every aspect of the research, including the population and sample methodologies employed in the survey. Finally, this chapter describes the manner of analysis and data collecting method used in this study.

### 3.2 Project Management Framework (PMT Model)

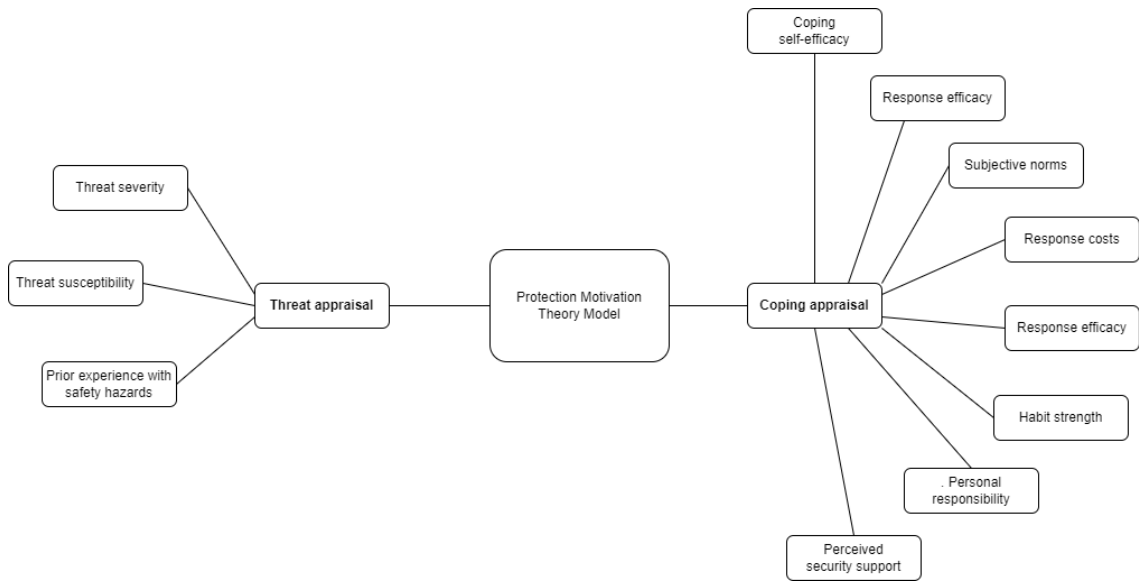
This research looks at cyber security and, more specifically, the desire to take online security measures, using the Protection Motivation Theory (PMT). The PMT model consists of threat and coping appraisal processes [13]. All the criteria used to evaluate the PMT were previously validated and adapted to the current research problem [14]. The PMT framework has been utilised in certain research to investigate specific online dangers such online harassing, malware attacks, and privacy issues. The PMT framework was used to test a complete security practises scale, which is a test that looks at the use of many security precautions in one scale instead than adopting distinct as a safety precaution practise, as was typically done in previous study, automated updating, password protection, 's compulsory, firewalls, and browser safety were used.



**Figure 3-1 PMT Framework**

The research demonstrated the utility of such a broad scale. As a result, rather than focusing on one single sort of crime or countermeasure, the present survey will take a broader approach and focus on perceptions of cyber security and online safety precautions in general. This makes sense because phishing can lead to fraudulent activity or hacking, malicious hackers can lead to online fraud, and certain remedies can often protect against multiple threats at once. The installation of a firewall, for example, can safeguard a computer from hacking, viruses, and spyware. Furthermore, implementing a

single precaution is insufficient to protect oneself from the variety of threats that may be encountered. As a result, a more inclusive strategy is required [14].



**Figure 3-2 General PMT Model**

The PMT model consists of threat and coping appraisal processes. For the threat appraisal, there are two elements which are threat severity and threat susceptibility. Threat appraisal is about the person determining the likelihood of the event or consequence occurring to them which is perception susceptibility and the intensity of the threat if it does perceived severity [15]. In threat severity, the respondent needs to know the level of computer and Internet virus dangerous would risks their online safety. In threat susceptibility will discuss about the probability of experiencing internet security hazards [16].

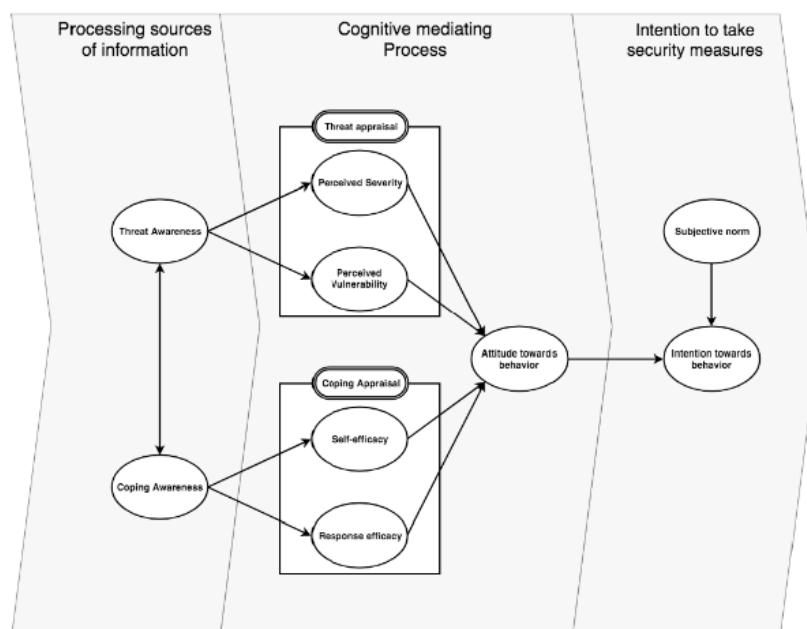
Furthermore, coping appraisal is about the individual’s assessments of their capacity to execute the actions that may avert the undesirable consequence individual assessments of the efficiency of that action in preventing the undesirable outcome and individual assessments of the cost of responding [15]. Coping appraisal has seven parts, including coping self-efficacy, which was linked to process or system and comfort when engaging preventive action, and response efficacy, which was used to evaluate the effectiveness of completing protective behaviours. Furthermore, subjective norms were assessed to see if they believed their friends and acquaintances, important others, or peers believed they should take precautions to protect oneself online. In addition, response

costs addressed the costs and repercussions of engaging in prevention programs, and pattern intensity indicated if taking protective activities online was a pattern for individuals. Next, individuals' beliefs of their own responsibility for keeping the Internet safe were linked to personal responsibility. Finally, perceived security support centred on participants' impressions of whether or not they needed assistance from everyone to install security software on their computers [16].

### 3.2.1 Related Work with Protection Motivation Theory (PMT)

#### 3.2.1.1 Investigating and Comparing the Predictors of the Intention towards Taking Security Measures Against Malware, Scams and Cybercrime in General

In the area of cybercrime, the PMT has been utilised to acquire a better understanding of the desire to execute defensive behaviour. It has been suggested that the PMT aids in the development of communication techniques to encourage people to take precautions against cybercrime. In its most basic form, the PMT can be broken down into three steps. The first one is the processing of information sources, next is the cognitive mediation process, and the last one is the intent to use specific protection techniques [17].



**Figure 3-3 The Adjusted PMT Model**

Different sources of information, spanning from ambient to intrapersonal sources, were provided in the original PMT model. While personality types and relevant qualifications are examples of intrapersonal information sources, social reinforcement and learning theory are sources of environmental information sources. Threat assessment and coping appraisal are two cognitive processes that determine attitude toward protective activity, and the cognitive mediating process distinguishes between them. Threat evaluation is the mental process by which a person assesses a potential threat and the risk it poses. It is made up of the threat's severity (perceived severity) and the possibility of being harmed by that threat (perceived vulnerability). Coping evaluation, on either side, is a psychological process in which a person evaluates potential protective techniques in terms of personal ability to put them into practise (self-efficacy), their effectiveness (response efficacy), and their concern about the cost of performing a recommended protective response (response cost) [17].

Threat evaluation is one of the two mechanisms involved in the mental conciliation process. There are two types of threat assessment: perceived severity and perceived vulnerability.

i. Threat Appraisal

According to the classic PMT model, perceived severity, or how serious someone feels that threats will have negative consequences, boosts motivation to defend oneself from those risks, a claim backed up by several research. As a result, the more dangerous a threat is seen to be, the more security measures are desired. According to the classic PMT model, perceived vulnerability, or someone's sense of their vulnerability to being harmed by a specific threat, enhances the attitude toward protective behaviour. This relationship has been studied extensively, but the conclusions are inconclusive. On the one hand, it was discovered that a sense of vulnerability enhances the need to defend [17]. As a conclusion, we can hypothesis that:

H1. Attitude toward preventative behaviour against cybercrime is positively correlated with perceived severity.

H2. The perception of vulnerability is a favourable determinant of commitment toward cybercrime prevention.

ii. Coping Appraisal

In the conventional PMT model, coping is measured in terms of response efficacy, self-efficacy, and response cost. Protective behaviour attitudes are assumed to be influenced by response efficacy and self-efficacy, whereas response cost is thought to be influenced by response cost. The efficacy of a protective measure against a specific cybercrime is defined as response efficacy [17]. Many scholars agree with the PMT's initial conclusion that there is a positive relationship between response efficacy and protective behaviour attitude: the more convinced an individual is that a particular protective that he or she will be well protected from cybercrime as a result of this measure., the more motivated he or she is to engage in that protective behaviour. Self-efficacy, or the belief in one's ability to carry out protective measures, has also been shown to have a large favourable impact on protective behaviour attitudes. Individuals who are confident in their ability are more prone to participate in this risk behaviour in order to attain a specified conduct. As a conclusion, we can hypothesis that:

H3. Self-efficacy is a favourable predictor of attitude toward cybercrime protective activity.

H4. Response efficacy is a favourable predictor of attitude toward cybercrime defensive behaviour.

**Table 3-1 Questionnaire of Security Measure**

| <b>Construct</b> | <b>Survey Item</b>  |
|------------------|---|
| Threat Awareness | How well do you understand the following concepts?<br>1 Malware<br>2 Scams<br>3 Hacking   |
| Coping Awareness | How well-versed in these remedies are you? (If you know of a software package that has multiple defences (for example, an autonomous password creator, anti-virus, and backup application in one, you can stuff the box with all of them. |

- 1 Install anti-virus, anti-spyware, anti-phishing, crypto locker, and backup software, for example.
- 2 Install any software that included with your computer system such as firewall, and defender
- 3 Update operating system software
- 4 Set up a secure Wi-Fi network
- 5 Create passwords for applications and your home network that are difficult to guess.
- 6 Verify the authenticity of the source and the document itself.
- 7 Be cautious about revealing personal information to others.

Malware\_Perceived\_severity

Which of the following assertions do you concur with the most?

- 1 I suppose malware is a significant issue.
- 2 I believe malware should be addressed seriously
- 3 I agree malware should be addressed seriously

Malware\_Perceived\_vulnerability

Which of the following assertions do you trust with the most?

- 1 It's conceivable that I'll get to be a malware victim.
- 2 I'm vulnerable to this type of malware.
- 3 There is a significant chance that I will become a target of malware.

Malware\_Self\_efficacy

Which of the following statements do you believe with the most?

- 1 Taking the appropriate anti-malware security protocols is simple
- 2 Taking the appropriate anti-malware security protocols is simple
- 3 I have the knowledge and abilities to take the appropriate malware security precautions.

Malware\_Response\_efficiency

Which of the following arguments do you concur that has the most?

1 Malware protection techniques are successful in preventing malware.

2 I can avoid viruses by taking security precautions.

---



### **3.2.1.2 Understanding Smartphone Security Behaviours: An Extension of the Protection Motivation Theory with Anticipated Regret**

Many people nowadays spend their entire lives glued to their smartphone. This has been made feasible by smartphone connections and the different smartphone apps that available for the preponderance of what people wish to do. The function of cautiousness as an intermediary between the threat characteristics of the PMT and security intentions/behaviours was added in this study's model for explaining level of security behaviours. In order to fully understand smartphone security behaviours, this study explores and proposes a study model that incorporates anticipated remorse and the PMT. The overall premise is that through the mediating role of expected regret, the PMT threat appraisal characteristics influence security intention and actual [18].

#### **i. Threat Appraisal Dimensions of the PMT**

Even though the threat assessment factor of the PMT has three aspects, but in this study, just perceived vulnerability and perceived severity will be used. The subjective possibility that a security threat will arise is referred to as perceived vulnerability. This is frequently based on a user's assessment of his or her vulnerability to certain dangers. In terms of smartphone security, this can be defined as the possibility that a person believes his or her smartphone is vulnerable to a security attack. The degree to which a user believes dangers with his or her cell phone will be detrimental can be characterised as perceived severity in the context of mobile security. Most likely, the impulse to take these safeguards comes from the desire to prevent potential remorse from passivity. This is because those who believe the risks and severity of a security breach are high are more likely to regret not taking preventative measures [18]. As a result, this research hypothesises that:

H1. Predicted regret will be strongly affected by specific vulnerability.

H2. Expected remorse will be influenced by perceived severity.

#### **ii. Coping Appraisal Dimensions of the PMT**

Self-efficacy, response efficacy, and response cost are three PMT coping appraisal dimensions. When compared to threat appraisal dimensions, the numerous qualities of coping appraisal have been shown to have a more direct favourable impact

on data privacy intentions across a variety of contexts. When an individual is confronted with a threat, the two efficacy dimensions (self-efficacy and reaction efficacy) are thought to be activated cognitive processes that encourage the individual to participate in activities that serve to reduce the threat. Self-efficacy is concerned with an individual's view of his or her talents and capacities to conduct a certain security behaviour, whereas response efficacy is concerned with the individual's belief in the action's perceived advantages.

Nonetheless, this research supports other findings that suggests that in order for people to adopt effective security practises to safeguard their smartphones, they must have a strong belief in their own abilities to protect them, as well as an understanding of the benefits of doing so [18]. As a result:

H3. According to this study, self-efficacy will better smartphone security intentions.

H4. Response efficacy will impact smartphone security intentions in a good way.

**Table 3-2 Questionnaire of Smartphone**

---

|  |
|--|
| <b>Self-efficacy</b>   |
| I am confident in securing my smartphone   |
| I have the means and skills to implement the security requirements on my phone   |
| Implementing the security features on my smartphone is simple  |
| I can enable security protocols on my smartphone by myself   |
| <b>Response efficacy</b>   |
| Security flaws can be avoided by installing security features on my smartphone   |
| Using security features on my smartphone is a good approach to keep hackers at the bay                                   |
| Hackers will not be able to steal my identity if I enable security features on my smartphone                             |
| The safeguards in place to prevent unauthorized access to sensitive financial or personal data on my phone are effective |
| <b>Response cost</b>   |

---

---

I find it inconvenient to use smartphone security features.

Taking security precautions on my smartphone would necessitate a significant amount of time and work.

It would take a long time for me to put security measures in place on my smartphone.

The cost of putting recommended security measures on my phone outweighs the advantages.

**Perceived vulnerability**

On my smartphone, I could be vulnerable to a significant data security vulnerability.

On my smartphone, I'm encountering an increasing number of information security concerns, and I'm concerned that my phone may be subject to a security issue.

If I do not follow appropriate smartphone security practises, I may become a victim of a malicious attack.

**Perceived severity**

For me, a security compromise on my smartphone would be a major issue.

Information loss as a result of hacking would be a major issue for me.

It would be a big concern for me if someone gained access to my personal information on my smartphone without my approval or knowledge.

---

### **3.3 Research Design**

A research methodology design is a method for gathering information and data in order to make informed decisions. This research will employ quantitative methodology, employing an online survey questionnaire as the data collection method.

#### **3.3.1 Quantitative Method**

Quantitative research approaches describe and measure the quantity of occurrences using statistics and maths. Methods for obtaining quantitative data are based on numbers and applied mathematics. Quantitative data gathering approaches employ random sampling and structured data collection devices. Communicating, analysing, comparing, and summarising quantitative study findings is usually straightforward. Interview, questionnaire, and observation are the most common quantitative methods. In the online approach, the targeted students will be given a link to a survey where they can fill out the answers. Because the link is based on an automated key issued by the sender, the selected individual can only access the questionnaire and answer the question once [1].

### **3.4 Research Approach – Questionnaire Method**

A survey is going to be conducted to focus on the UMP students in order to prove what has been discussed in literature review. Basically, there is a method to collect data that can be done which is a self-administered computer survey (online). This survey will be conducted based on students' information and understanding of cyber security knowledge.

#### **3.4.1 Sampling and Data Collection**

The population included in this research will be undergraduate and postgraduate student from University Malaysia Pahang (UMP). The selecting procedure will be based on the user's background knowledge of cyber security. Furthermore, all participants will be placed in naturalistic conditions to gather additional information and data.

The online questionnaire was prepared and distributed using Google Form, a web-based survey service that was chosen for the job because it is extremely secure and can handle big amounts of data [19]. The responses can be exported into a variety of statistical forms, including Microsoft Excel files. The online questionnaire link was sent to all students via the internet email system. The email invited all students to participate in the study voluntarily. Furthermore, the survey invitation stated unequivocally that all responses will be kept totally confidential and that no individuals will be identifiable from the data collected. The research's objective and details were described in the email. The email further suggested that by responding to the online form, the respondents were giving their approval at the same time.

#### **3.4.2 Data Analysis and Result**

The connection between threat and coping appraisal and intention was investigated using the PMT model, and how the factors perceived knowledge and website quality impacted these actions and motivations. To compile statistics of all answers to questions that have been answered, a quantitative approach and Microsoft Excel were employed. Additionally, content analysis was used to determine whether or not responses to open-ended questions seemed either positive or negative. Open-ended questions that merely sought to acquire a basic overview or insight into employee perceptions and behaviours in regard to computer crime or information security incidents were subjected

to content analysis. Finally, to highlight the links between information ideas and related behaviours, Microsoft Excel's cross-tabulation (pivot tables) capabilities was used.

In conclusion, the exploratory nature of this study warrants the use of both online questionnaires and literature reviews to collect data. Because it is more convenient for respondents, using an online questionnaire provides a better response rate than traditional paper-based surveys. The questionnaire's design is based on principles that have been demonstrated to be both practical and useful in other studies.

### **3.4.3 Participants**

In this research, the participants that will participate are undergraduate and postgraduate students from University Malaysia Pahang (UMP). For the undergraduate and postgraduate student, the range of age is around 18 to 30 years old. This research will also study based on the gender which is male and female. In addition, the level of their study background will be one of the main reasons to study this cyber security. We used to choose these participants because they are more exposed to devices such as online and offline devices.

### **3.5 Research Requirement**

#### **3.5.1 Input and Output**

The input for this research is student of UMP applying their information security awareness knowledge by answering the question. While the output for this research is the feedback and result of level of knowledge of students of UMP.

#### **3.5.2 Constraint and Limitation**

Cross-sectional survey, such as this one, cannot prove causality. Although the sample employed in this study was representative of the entire online population in the UMP, it was skewed toward young individuals with higher education levels than the old individual's population.

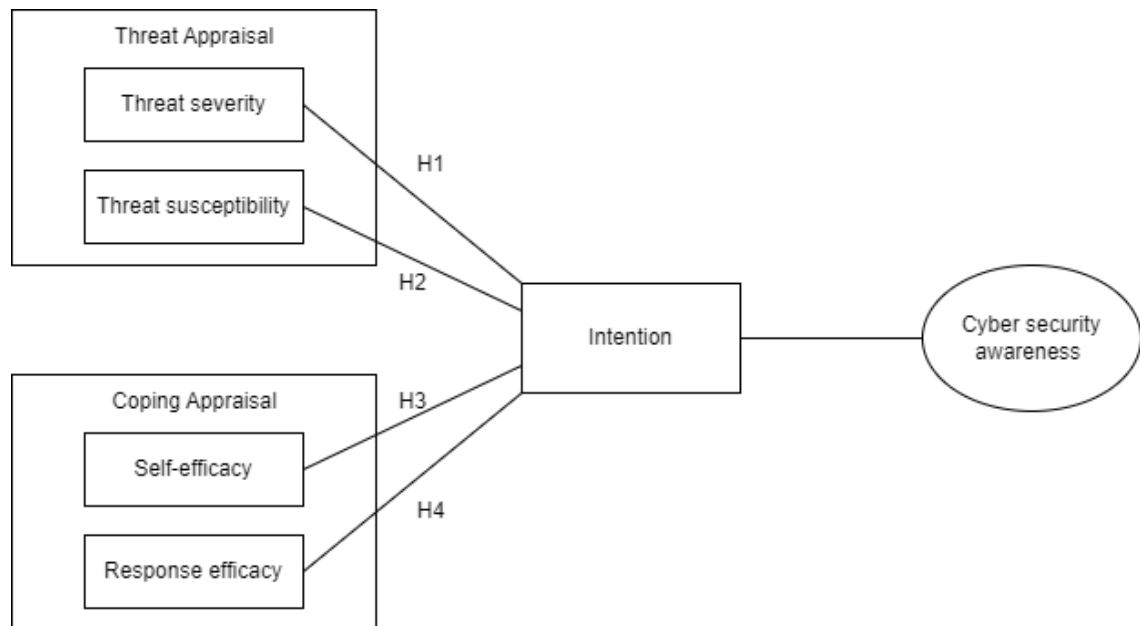
Furthermore, to determine the reasons that generate online safety behaviours, more research into danger appraisal and coping appraisal variables is needed. We did not add more variables regarding danger evaluation because this study evaluated the association between several variables and security intentions for the sake of parsimony.

#### **3.5.3 Case Study**

This research is based on analysis of cyber security awareness among student in UMP. To test the PMT model, the online survey will be distributed among them to get the collection of data which are some questionnaires that are related to the cyber security. The questionnaires will be created based on the impact of cyber security awareness on students' cybersecurity.

In the beginning of the process will be applied to the responses from the students and data collected to enable the creation of the predictive analysis. Our sample is representative of the UMP population based on the distribution of category, gender, age, and education background. The constraint and limitation for this method are user must have access to the internet to utilise the online survey from starting till the end of answering. In addition, only one account of email can answer the survey question.

### 3.6 Proposed Model



**Figure 3-4 Research Model using PMT approach**

#### 3.6.1 Threat Appraisal

Threat appraisal is defined by threat severity and threat susceptibility. Threat severity refers to how serious an individual considers the repercussions of a specific incident. Despite the fact that a cyber-attack could have serious consequences for internet and devices students, individuals may interpret the threat or the amount of the injury in terms of seriousness in different ways. According to research, the severity of malware risks as perceived motivates internet users to engage in malware avoidance behaviour. This outcome is in line with previous findings from more general cybersecurity investigations. According to earlier studies, being worried about security dangers contributed to a more favourable feeling toward acting, and threat severity has a beneficial impact on applying security procedures. We form the following hypothesis based on our findings:

H1: Threat severity of cyber security is strongly tied to the intention to adopt protective measures against cyber security.



The second threat appraisal notion is threat susceptibility, or a person's evaluation of the likelihood of encountering threatening events, such as becoming a cybersecurity victim. Individuals that perceive something as a danger are thought to adjust their behaviour in response to the level of risk they threat. A more intensely felt threat enhances the drive to escape the threat. For example, in the instance of e-mail security, threat susceptibility to malicious attachments has been linked to computer security behaviour. As a result, we anticipate that threat cybersecurity susceptibility will be linked to protection motivation in a similar way. We propose the following hypothesis:

H2: Threat susceptibility of cyber security is significantly associate to the intention to take precautionary measures against cyber security.

### **3.6.2 Coping Appraisal**

The second process evaluation looked at remedies that could be used in the event of a danger. This evaluation is based in part on how a person assesses their own ability to undertake the specified behaviour. In the context of this study, self-efficacy refers to the capacity to take precautions on the internet, such as installing virus protection and changing passwords on a regular basis. Previous research has found that a person's threat self-efficacy is a good predictor of their online security behaviour or desire to take precautions. Individuals who believe they can do a given conduct appear to be more inclined to do so. Considering this argument, the following hypothesis is proposed:

H3: Threat self-efficacy is highly associate to the intention to take protective measures against cybercrime.

It's also crucial that the proposed remedies are seen as effective in protecting internet users from online dangers, a concept known as response-efficacy. This will determine whether the proposed behaviour is followed. In the area of cybersecurity measures, the relationship between perceived response efficacy and intention has been shown multiple times. As a result of our focus on cybersecurity measures, we anticipate:

H4: Perceived response efficacy will influence the propensity to conduct cybersecurity prevention actions in a good way.

### **3.7 Proof of Initial Concept**

#### **3.7.1 Pilot Questionnaire**

Four to five undergraduate students were conducted a pilot test of the methods, stimuli, and instrument. The average age of the participants and their gender were determined based on the results of this test. During the pilot test, the feedback has been requested on the wording of items and manipulations in addition to doing early manipulation tests, but no significant changes to the procedures were required for the major data collection. The survey's usability was tested on a range of devices (mobile, desktop and tablet). To improve response rates, the questionnaires were kept short, with an expected completion time of 8 to 10 minutes.

The questionnaire consists of five sections. Each of every section will have five questions. The first section will be test about demographic which is about their information. As example, age, gender, background study and category. Second, participants will answer the first hypothesis question which related to the threat severity question. The next section is about the second hypothesis question which related to the threat susceptibility question. Moreover, the fourth section is discussing about the third hypothesis question which related to the self-efficacy question. Finally, is discussing about the fourth hypothesis question which related to the response-efficacy question.

### **3.8 Expected Outcome**

In this research, I anticipate that students will improve their awareness of cyber security issues by understanding and practicing what they have learned in their daily lives. As a result, they should participate in cyber security awareness training to protect Internet users from cybercrime and developing cyber dangers.

If the research proves my hypothesis to be correct, I suggest the government or authorities provide chances for higher education students to study about and comprehend evolving cyber security threats, despite the fact that previous studies have shown that academics are excessive Internet users.

### 3.9 Hardware and Software Requirements

This section will identify the main requirements that are needed to carry out this research. The hardware and software needed in order to implement this research will explained below:

#### 3.9.1 Hardware Requirement

**Table 3-3 Hardware Requirement**

| <b>Hardware</b> | <b>Version</b>  | <b>Purpose</b>   |
|-----------------|---|--|
| Laptop          | HP Laptop<br>AMD A6-9220 RADEON<br>R4, 5 COMPUTE CORES<br>2C+3G 2.50 GHz<br>RAM - 8.00 GB | To carry out the entire research process which are starting from finding until the implementations |
| Printer         | HP Deskjet Ink Advantage<br>2135 All-In-One Printer                                       | To print out all the related documents   |

#### 3.9.2 Software Requirement

**Table 3-4 Software Requirement**

| <b>Software</b>              | <b>Version</b>                 | <b>Purpose</b>   |
|------------------------------|--------------------------------|--|
| Microsoft Office Word        | LTSC Professional Plus<br>2021 | To document all the findings and generate thesis report        |
| Microsoft Office Excel       | LTSC Professional Plus<br>2021 | To generate Gantt chart and save all the data from respondents |
| Microsoft Office Power-Point | LTSC Professional Plus<br>2021 | To visualize report for presentation                           |
| IBM SPSS                     | Version 26                     | To calculate and analyse all the results from respondents      |
| Draw.io                      | Free online software           | To draw the flowchart  |
| Canva                        | Free online software           | To visualize the poster  |

### **3.10 Gantt Chart**

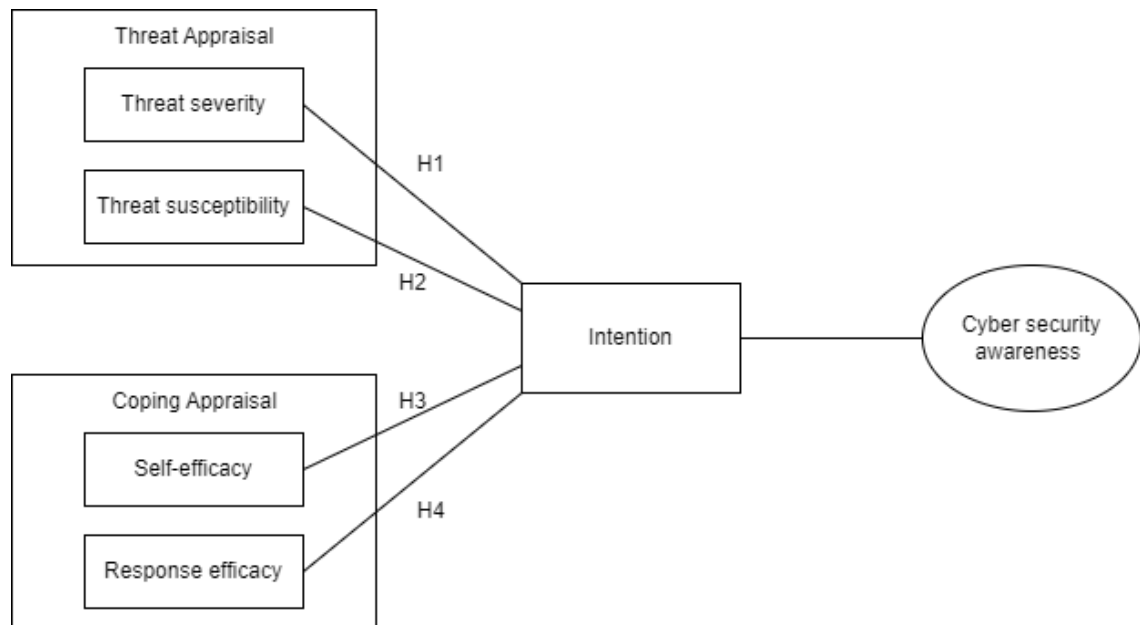
Gantt chart will show the flow of this research paper that started from March 2022 until the end of this research. This research is followed by the continuous meeting with supervisor in order to make sure that this research paper done within the timeframe given that is March until end of February 2023. **Refer to Appendix B.**

## CHAPTER 4

### RESULTS AND DISCUSSION

#### 4.1 Introduction

This chapter discusses the finding of this thesis. Survey have been conducted to investigate the level of awareness about cyber security. The respondents from this survey covered University Malaysia Pahang students from both campus with different educational level. The findings are presented under the following major headings: socio demographic characteristic, security intentions, threat severity, threat susceptibility, self-efficacy, response efficacy.

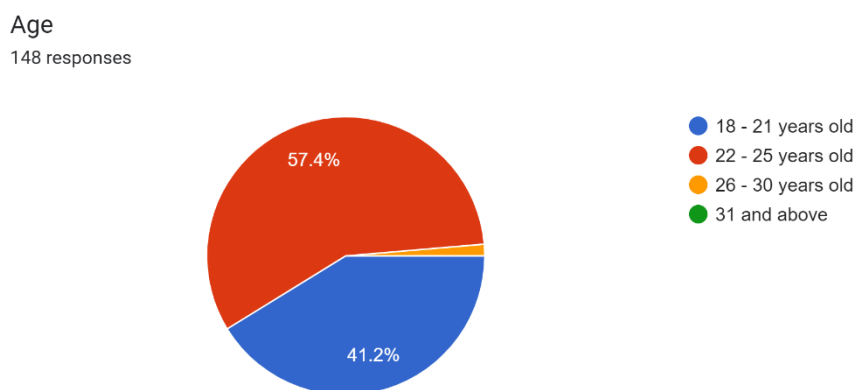


**Figure 4-1 Proposed PMT Model**

## 4.2 Analysis and Results

### 4.2.1 Socio Demographic Characteristic

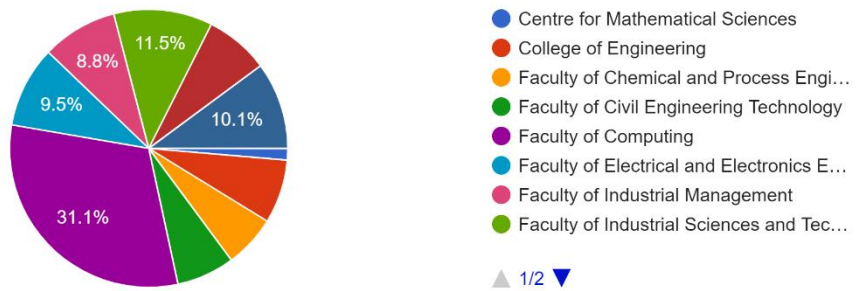
Respondents of all ages (18 and above) were represented, with slightly larger number in the lowest age bracket 18-21 and 22-25 categories accounting for 61(41.2%) and 85(57.4%) of the respondents, respectively. The oldest age bracket was 26-30 which accounted for 2(1.4%) of the respondents. The proportion of ages of males and females about 44.6% and 55.4% in all age groups.



**Figure 4-2 Pie chart of Age**

The survey indicates the faculty of a highest which is Faculty of Computing (FK) 46 (31.1%). Besides that, the second highest of respondents involved from Faculty of Industrial Sciences and Technology (FIST) 11.5% followed by Faculty of Mechanical and Automotive Engineering Technology (FTKMA) 10.1% and then from Faculty of Electrical and Electronics Engineering Technology (FTKKEE) 9.5%. Based on the result collected, 8.8% are from Faculty of Industrial Management (FIM). A further, 11(7.4%) were both from College of Engineering (CE) and Faculty of Manufacturing and Mechatronic Engineering Technology (FTKPM). Plus, Faculty of Civil Engineering Technology (FTKA) produce only 6.8% respondents followed by Faculty of Chemical and process Engineering Technology (FTKKP) 9(6.1%). The remaining 2(1.4%) of the respondents grouped under Centre of Mathematical Sciences (CMS). The proportion of campus of Gombang and Pekan about 44.6% and 55.4% in all faculty groups.

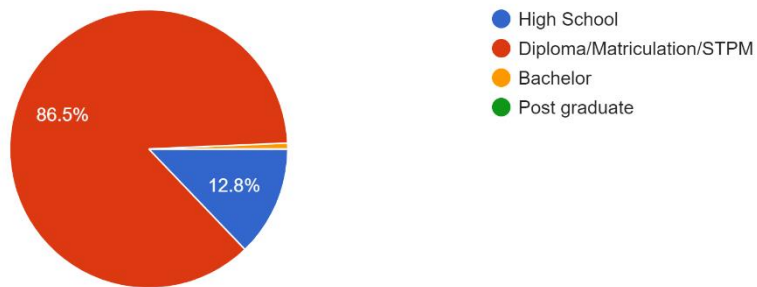
Faculty  
148 responses



**Figure 4-3 Pie chart of Faculty**

The findings of this study showed most of the respondents 148(100%) were undergraduate students. Based on the result collected majority of the respondents holding diploma, matriculation, and STPM (86.5%), while who are in high school level is 12.8%. The respondent for bachelor is 0.7%.

Highest Education Background  
148 responses



**Figure 4-4 Pie chart of Highest Education Background**



**Table 4-1 Summarize of Demographic result**

| <b>Category</b>                     | <b>N</b> | <b>%</b> |
|-------------------------------------|----------|----------|
| <b>Gender</b>                       |          |          |
| Male                                | 66       | 44.6     |
| Female                              | 82       | 55.4     |
| <b>Age</b>                          |          |          |
| 18 – 21 years old                   | 61       | 41.2     |
| 22 – 25 years old                   | 85       | 57.4     |
| 26 – 30 years old                   | 2        | 1.4      |
| <b>Campus</b>                       |          |          |
| Gambang                             | 66       | 44.6     |
| Pekan                               | 82       | 55.4     |
| <b>Faculty</b>                      |          |          |
| FK                                  | 46       | 31.1     |
| FIST                                | 17       | 11.5     |
| FTKMA                               | 15       | 10.1     |
| FTKEE                               | 14       | 9.5      |
| FIM                                 | 13       | 8.8      |
| CE                                  | 11       | 7.4      |
| FTKPM                               | 11       | 7.4      |
| FTKA                                | 10       | 6.8      |
| FTKKP                               | 9        | 6.1      |
| CMS                                 | 2        | 1.4      |
| <b>Current Academic Status</b>      |          |          |
| Undergraduate                       | 148      | 100      |
| Postgraduate                        | 0        | 0        |
| <b>Highest Education Background</b> |          |          |
| High school                         | 19       | 12.8     |
| Diploma/Matriculation/STPM          | 128      | 86.5     |
| Bachelor                            | 1        | 0.7      |

## 4.2.2 Descriptive Analysis

### 4.2.2.1 Security Intentions

Based on the results from the respondents, half of all the respondents have prior knowledge about cybersecurity which contribute around 52% of the respondents. The rest of the respondents were do not have and not sure about their knowledge in cybersecurity which are 33.8% and 14.2% respectively which produce ( $M=2.38$ ,  $SD=0.723$ ). Other than that, there are 54.7% were not have prior knowledge about information security while 25.0% were not sure about information security knowledge. The rest of the respondents were known with prior knowledge about information security which contribute 20.3% of the respondents which produce ( $M=1.95$ ,  $SD=0.673$ ).

There are two types of cybersecurity concepts that has been asked for the respondents which how aware are them of the malware and scams concepts. Based on the result for malware concept, there are 81(54.7%) of the respondents are aware followed by 27(18.2%) were not aware about this concept. 25 of the respondents were between aware and not aware which is neutral about malware which contribute 16.9%. There are 10.1% are totally aware about malware concept in cybersecurity. Other than that, there are 102(68.9%) of the respondents are aware about concept of scams in cybersecurity. 26 of the respondents were between aware and not aware which is neutral about scams which contribute 17.6% followed by 19(12.8%) were totally aware about this concept. There are 0.7% are not aware about scams concept in cybersecurity.

There are five (5) questions for security intentions that has been asked for the respondents to measure their awareness about these countermeasures. In table 4.2 shown about frequency summarisation of security intentions questions.

**Table 4-2 Statistics of Security Intentions**

|  | N(%)             |          |          |           | Mean     | Std. Deviation |               |
|--|------------------|----------|----------|-----------|----------|----------------|---------------|
|  | Totally disagree | Disagree | Neutral  | Agree     |          |                | Totally Agree |
| Malware  | 0(0)             | 27(18.2) | 25(16.9) | 81(54.7)  | 15(10.1) | 3.57           | 0.905         |
| Scams  | 0(0)             | 1(0.7)   | 26(17.6) | 102(68.9) | 19(12.8) | 3.94           | 0.574         |
| Install software such as anti-virus, anti-spyware, backup software in my personal computer and laptop                          | 0(0)             | 1(0.7)   | 6(4.1)   | 119(80.4) | 22(14.9) | 4.09           | 0.457         |
| Set up software that is included with your operating system such as firewall, defender to protect personal computer and laptop | 0(0)             | 26(17.6) | 29(19.6) | 77(52.0)  | 16(10.8) | 3.56           | 0.905         |
| Secure a Wi-Fi network   | 0(0)             | 1(0.7)   | 3(2.0)   | 120(81.1) | 24(16.2) | 4.13           | 0.441         |
| Set up difficult to guess passwords for accounts and home network  | 0(0)             | 1(0.7)   | 14(9.5)  | 112(75.7) | 21(14.2) | 4.03           | 0.514         |
| Share personal information on the Internet   | 0(0)             | 2(1.4)   | 2(1.4)   | 115(77.7) | 29(19.6) | 4.16           | 0.491         |

#### 4.2.2.2 Threat Severity

From the threat severity factor, it is generally found that the malware cause a system crash from time to time (M=3.91, SD=0.471), malware can reveals personal passwords to inline criminals (M=3.18, SD=0.839), where considerably as lower mean level of practice. Scams can steal someone’s personal information (M=4.49, SD=0.515) followed by scams can increase the nuisance phone calls, emails, and texts from various sources (M=4.28, SD=0.557). The scams can cause lasting mental and physical trauma for victims (M=3.84, SD=0.946).

**Table 4-3 Statistics of Threat Severity**

|   | N(%)             |          |          |           | Totally Agree | Mean | Std. Deviation |
|---|------------------|----------|----------|-----------|---------------|------|----------------|
|   | Totally disagree | Disagree | Neutral  | Agree     |               |      |                |
| Malware cause a system crash from time to time                                      | 0(0)             | 1(0.7)   | 21(14.2) | 117(79.1) | 9(6.1)        | 3.91 | 0.471          |
| Malware can reveals personal passwords to inline criminals                          | 0(0)             | 37(25)   | 52(35.1) | 55(37.2)  | 4(2.7)        | 3.18 | 0.839          |
| Scams can steal someone’s personal information                                      | 0(0)             | 0(0)     | 1(0.7)   | 73(49.3)  | 74(50.0)      | 4.49 | 0.515          |
| Scams can increase the nuisance phone calls, emails, and texts from various sources | 0(0)             | 1(0.7)   | 5(3.8)   | 94(63.5)  | 48(32.4)      | 4.28 | 0.557          |
| Scams can cause lasting mental and physical trauma for victims                      | 0(0)             | 22(14.9) | 13(8.8)  | 79(53.4)  | 34(23.0)      | 3.84 | 0.946          |

### 4.2.2.3 Threat Susceptibility

From the threat susceptibility factor, it is generally found that the risk is big that I become a victim of malware (M=2.20, SD=1.117), malware is extremely likely that my computer will be infected by malware in the future (M=2.42, SD=0.857). There is a good possibility that my personal devices will have malware (M=2.45, SD=0.875) followed by my chances of being a scams victim is high (M=2.16, SD=1.105), where considerably as lower mean level of practice. There is possible I been the victim of an online scam and lost money (M=2.44, SD=0.882).

**Table 4-4 Statistics of Threat Susceptibility**

|  | N(%)             |          |          |          | Mean | Std. Deviation |
|--|------------------|----------|----------|----------|------|----------------|
|  | Totally disagree | Disagree | Neutral  | Agree    |      |                |
| The risk is big that I become a victim of malware                                      | 53(35.8)         | 38(25.7) | 34(23.0) | 21(14.2) | 2.20 | 1.117          |
| Malware is extremely likely that my computer will be infected by malware in the future | 15(10.1)         | 73(49.3) | 47(31.8) | 9(6.1)   | 2.42 | 0.857          |
| There is a good possibility that my personal devices will have malware                 | 15(10.1)         | 71(48.0) | 45(30.4) | 14(9.5)  | 2.45 | 0.875          |
| My chances of being a scams victim is high   | 54(36.5)         | 40(27.0) | 34(23.0) | 17(11.5) | 2.16 | 1.105          |
| There is possible I been the victim of an online scam and lost money                   | 17(11.5)         | 68(45.9) | 47(31.8) | 13(8.8)  | 2.44 | 0.882          |

#### 4.2.2.4 Self-Efficacy

From the self-efficacy factor, it is generally found that the question of I feel comfortable taking measures to secure my primary home computer or personal laptop (M=4.09, SD=0.316), where considerably the highest mean level of practice. By taking the necessary security measures is entirely under my control (M=3.59, SD=0.699) followed by I have resources and the knowledge to take necessary security measures (M=3.89, SD=0.515). I feel nervous when I think about online security issues (M=3.42, SD=0.756) and I possess the knowledge and skills to take the necessary security measures against malware (M=3.85, SD=0.539).

**Table 4-5 Statistics of Self-Efficacy**

|  | N(%)             |          |          |           |               | Mean | Std. Deviation |
|--|------------------|----------|----------|-----------|---------------|------|----------------|
|  | Totally disagree | Disagree | Neutral  | Agree     | Totally Agree |      |                |
| I feel comfortable taking measures to secure my primary home computer or personal laptop | 0(0)             | 0(0)     | 1(0.7)   | 132(89.2) | 15(10.1)      | 4.09 | 0.316          |
| By taking the necessary security measures is entirely under my control                   | 0(0)             | 8(5.4)   | 55(37.2) | 75(50.7)  | 10(6.8)       | 3.59 | 0.699          |
| I have resources and the knowledge to take necessary security measures                   | 0(0)             | 2(1.4)   | 23(15.5) | 113(76.4) | 10(6.8)       | 3.89 | 0.515          |
| I feel nervous when I think about online security issues                                 | 0(0)             | 19(12.8) | 53(35.8) | 71(48.0)  | 5(3.4)        | 3.42 | 0.756          |

---

|  |      |        |          |           |        |      |       |
|--|------|--------|----------|-----------|--------|------|-------|
| I possess the knowledge and skills<br>to take the necessary security<br>measures against malware | 0(0) | 4(2.7) | 22(14.9) | 114(77.0) | 8(5.4) | 3.85 | 0.539 |
|--|------|--------|----------|-----------|--------|------|-------|

---

#### 4.2.2.5 Response Efficacy

From the response efficacy factor, it is generally found that the question of protective software would be useful for detecting and remove the malware (M=4.15, SD=0.357), where considerably the highest mean level of practice. Protective software would increase my performance in protecting myself from malware (M=3.84, SD=0.603) followed by protective software would enable me to search and remove malware faster (M=3.95, SD=0.486). Safety measures against scams are effective in preventing scams (M=3.94, SD=0.631) and protective software would be useful for detecting and removing scams issues (M=4.02, SD=0.412).

**Table 4-6 Statistics of Response Efficacy**

|   | N(%)             |          |          |           |               | Mean | Std. Deviation |
|---|------------------|----------|----------|-----------|---------------|------|----------------|
|   | Totally disagree | Disagree | Neutral  | Agree     | Totally Agree |      |                |
| Protective software would be useful for detecting and remove the malware            | 0(0)             | 0(0)     | 0(0)     | 126(85.1) | 22(14.9)      | 4.15 | 0.357          |
| Protective software would increase my performance in protecting myself from malware | 0(0)             | 1(0.7)   | 37(25.0) | 94(63.5)  | 16(10.8)      | 3.84 | 0.603          |
| Protective software would enable me to search and remove malware faster             | 0(0)             | 1(0.7)   | 18(12.2) | 116(78.4) | 13(8.8)       | 3.95 | 0.486          |
| Safety measures against scams are effective in preventing scams                     | 0(0)             | 1(0.7)   | 31(21.0) | 92(62.2)  | 24(16.2)      | 3.94 | 0.631          |



---

|   |      |      |         |           |         |      |       |
|---|------|------|---------|-----------|---------|------|-------|
| Protective software would be useful for detecting and removing scams issues | 0(0) | 0(0) | 11(7.4) | 123(83.1) | 14(9.5) | 4.02 | 0.412 |
|---|------|------|---------|-----------|---------|------|-------|

---

### 4.2.3 Reliability Test

The degree to which a test evaluates something accurately is measured by its test reliability. It is intimately related to test validity. Precision, or the degree to which measurements are error-free, can be thought of as a measure of test reliability. The concept of reliability is crucial for recognising and quantifying bias and distortion. If this study is free of bias and distortion, it would be considered reliable.

The proposed instrument underwent the process of accuracy and reliability checking to confirm the validity of the questionnaire and, ultimately, the results. A test's reliability is determined by how reliable and consistent its results are. To this end, a 100% of the sample size is used to determine the total number of responders who must take the reliability test.

**Table 4-7 Reliability Statistics**

| Cronbach's Alpha | Cronbach's Alpha Based on Standardized Items | N of Items |
|------------------|--|------------|
| 0.902            | 0.917  | 29         |

The Cronbach's Alpha,  $\alpha$  value of the sample size for 148 is 0.902 which produce the high level of internal consistency for the scale which normally ranges between 0 to 1 with the specific sample and excellent result. The average inter-item correlations and the amount of variables both enhance Cronbach's alpha coefficient. Furthermore, the Cronbach's alpha based on standardized items produce 0.917 value which employs the correlations among items. The number of items which more specific is the number of variables is 29 questions were selected to do the reliability statistics.

#### 4.2.4 Spearman's RHO Test

Correlation, often known as correlation analysis, is a phrase used to describe the connection or association among two (or more) quantitative measures. Researchers can use correlation analysis to gauge the degree to which two continuous, numerically measurable variables are related.

H1: Threat severity of cyber security is strongly tied to the intention to adopt protective measure against cyber security.

H2: Threat susceptibility of cyber security is significantly associate to the intention to take precautionary measures against cyber security.

H3: Threat self-efficacy is highly associate to the intention to take protective measures against cybercrime.

H4: Perceived response efficacy will influence the propensity to conduct cybersecurity prevention actions in a good way.

#### 4.2.4.1 Correlation between threat severity and individual's intention to cyber security

Calculation of relation between threat severity and intention analysed to the 148 students in UMP show the result of Spearman's coefficient ( $r_s$ ) = 0.433 as the hypothesis of this research. Referring to the result obtained on Table 4.3, Spearman Coefficient shows the positive correlation between threat severity and individual's security intention to cyber security. The p-value (quoted under Sig. (2-tailed)) is 0.000 (reported as  $p < 0.01$ ) which is less than 0.05, this indicates that threat severity and individual's security intention is a significant positive relation between each other. We would report that the results were significantly and moderately positively correlated  $r = 0.433$ ,  $N = 148$ ,  $p < 0.01$ .

**Table 4-8 Correlation between threat severity and individual's intention to cyber security**

|                |                     | Security Intentions     | Threat Severity |
|----------------|---------------------|-------------------------|-----------------|
| Spearman's rho | Security Intentions | Correlation Coefficient | 1.000           |
|                |                     | Sig. (2-tailed)         | .000            |
|                |                     | N                       | 148             |
|                | Threat Severity     | Correlation Coefficient | 0.433**         |
|                |                     | Sig. (2-tailed)         | .000            |
|                |                     | N                       | 148             |

\*\* . Correlation is significant at the 0.01 level (2-tailed).

#### 4.2.4.2 Correlation between threat susceptibility and individual's intention to cyber security

Calculation of relation between threat susceptibility and intention analysed to the 148 students in UMP show the result of Spearman's coefficient ( $r_s$ ) = -0.129 as the hypothesis of this research. Referring to the result obtained on Table 4.3, Spearman Coefficient shows the negative correlation between threat susceptibility and individual's security intention to cyber security. The p-value (quoted under Sig. (2-tailed)) is 0.118 (reported as  $p > 0.01$ ) which is more than 0.05, this indicates that threat susceptibility and individual's security intention is a significant negative relation between each other. We would report that the results were significantly and moderately negatively correlated  $r = -0.129$ ,  $N = 148$ ,  $p > 0.01$ .

**Table 4-9 Correlation between threat susceptibility and individual's intention to cyber security**

|                |                       | Security Intentions     | Threat Susceptibility |
|----------------|-----------------------|-------------------------|-----------------------|
| Spearman's rho | Security Intentions   | Correlation Coefficient | 1.000                 |
|                |                       | Sig. (2-tailed)         | .                     |
|                |                       | N                       | 148                   |
|                | Threat Susceptibility | Correlation Coefficient | -0.129                |
|                |                       | Sig. (2-tailed)         | .118                  |
|                |                       | N                       | 148                   |

#### 4.2.4.3 Correlation between self-efficacy and individual's intention to cyber security

Calculation of relation between self-efficacy and intention analysed to the 148 students in UMP show the result of Spearman's coefficient ( $r_s$ ) = 0.404 as the hypothesis of this research. Referring to the result obtained on Table 4.3, Spearman Coefficient shows the positive correlation between self-efficacy and individual's security intention to cyber security The p-value (quoted under Sig. (2-tailed)) is 0.000 (reported as  $p < 0.01$ ) which is less than 0.05, this indicates that self-efficacy and individual's security intention is a significant negative relation between each other. We would report that the results were significantly and moderately positively correlated  $r = 0.404$ ,  $N = 148$ ,  $p < 0.01$ .

**Table 4-10 Correlation between self-efficacy and individual's intention to cyber security**

|                |                     | Security Intentions     | Self-Efficacy |
|----------------|---------------------|-------------------------|---------------|
| Spearman's rho | Security Intentions | Correlation Coefficient | 1.000         |
|                |                     | Sig. (2-tailed)         | .000          |
|                |                     | N                       | 148           |
|                | Self-Efficacy       | Correlation Coefficient | 0.404**       |
|                |                     | Sig. (2-tailed)         | .000          |
|                |                     | N                       | 148           |

\*\* . Correlation is significant at the 0.01 level (2-tailed).

#### 4.2.4.4 Correlation between response efficacy and individual's intention to cyber security

Calculation of relation between response efficacy and intention analysed to the 148 students in UMP show the result of Spearman's coefficient ( $r_s$ ) = 0.496 as the hypothesis of this research. Referring to the result obtained on Table 4.3, Spearman Coefficient shows the positive correlation between response efficacy and individual's security intention to cyber security. The p-value (quoted under Sig. (2-tailed)) is 0.000 (reported as  $p < 0.01$ ) which is less than 0.05, this indicates that response efficacy and individual's security intention is a significant negative relation between each other. We would report that the results were significantly and moderately positively correlated  $r = 0.496$ ,  $N = 148$ ,  $p < 0.01$ .

**Table 4-11 Correlation between response efficacy and individual's intention to cyber security**

|                |                     | Security Intentions     | Response Efficacy |
|----------------|---------------------|-------------------------|-------------------|
| Spearman's rho | Security Intentions | Correlation Coefficient | 1.000             |
|                |                     | Sig. (2-tailed)         | .                 |
|                |                     | N                       | 148               |
|                | Response Efficacy   | Correlation Coefficient | 0.496**           |
|                |                     | Sig. (2-tailed)         | .000              |
|                |                     | N                       | 148               |

\*\* . Correlation is significant at the 0.01 level (2-tailed).

#### 4.2.5 Hypothesis Testing

There are two types of cyber security threats, malware and online scams. From the findings, the respondent's awareness in all aspects were considerably vulnerable and their awareness would certainly expose them to the cyber security threats. The research also finding the coping appraisal to track the students' awareness about cyber security. All the four aspects which are threat severity (TSE), threat susceptibility (TSU), self-efficacy (SE) and response efficacy (RE) were against individual's security intentions (SI).

**Table 4-12 Summary of Hypothesis test result**

|           | <b>Path</b> | <b>Coefficient</b> | <b>p-value</b> | <b>Result</b> |
|-----------|-------------|--------------------|----------------|---------------|
| <b>H1</b> | TSE → SI    | 0.433              | < 0.01         | Supported     |
| <b>H2</b> | TSU → SI    | -0.129             | > 0.01         | Not supported |
| <b>H3</b> | SE → SI     | 0.404              | < 0.01         | Supported     |
| <b>H4</b> | RE → SI     | 0.496              | < 0.01         | Supported     |

The result of the study, H1 is supported and threat severity of cyber security is strongly tied to the intention to adopt protective measure against cyber security. This can be seen when the p-value is less than 0.01 which the result of the correlation is significant at the 0.01 level. Students in UMP are aware about Malware threat may be harm for them. According to study, internet users are motivated to practise malware avoidance awareness because of how serious they consider the risks from malware. According to past research, being concerned about security risks made people feel more inclined to act, and the seriousness of the threat has a positive effect on following security protocols.

H2 is not supported and threat susceptibility of cyber security is not significantly associate to the intention to take precautionary measures against cyber security. This can be seen when the p-value is more than 0.01 which the result of the correlation is significant at the 0.01 level. It is believed that people who view something as a threat would alter their behaviour in proportion to the degree of risk they pose. Threats that are experienced more strongly increase the desire to flee them. Susceptibility to cyber hazards is the inability to prevent them; vulnerability to cyber threats is the inability to



withstand them; and resilience to cyber threats is the capacity to do so. Not everyone can have the ability to prevent cyber security with their intentions.

Thus, H3 is supported and threat self-efficacy is highly associate to the intention to take protective measures against cybercrime. This can be seen when the p-value is less than 0.01 which the result of the correlation is significant at the 0.01 level. A people's threat self-efficacy is a strong predictor of their internet security behaviour or intention to take safeguards, according to prior studies. People seem to be more likely to engage in a particular behaviour if they feel capable of doing so. The confidence in one's own capacity to use IT security or privacy skills [20]. People must be able to use their intentions to carry out security-related abilities.

Hence, H4 is supported and perceived response efficacy will influence the propensity to conduct cybersecurity prevention actions in a good way. This can be seen when the p-value is less than 0.01 which the result of the correlation is significant at the 0.01 level. The majority of coping evaluations were reliable indicators of security aims. The best predictors in particular are habit strength.

### 4.3 Discussion

In study, we proposed a model in which aspects of students' information security are related to cyber security protection action. We used a Protection Motivation Theory (PMT) framework to propose that information security affects students' awareness through students' appraisal about cyber security threats. The lack of knowledge of cyber security threats among youths between the ages of 18 and 25 is the primary cause of the rising cyber threat in Malaysia. Cyberbullying, asset damage, identity fraud, and other major consequences can result from these security concerns, which are particularly harmful to younger generations [11]. The most important component of this research is to raise teenagers' cybersecurity awareness.

To summarize our findings, we found that the socio-demographic variables significantly predicted security intentions as evidenced by the highest level of education. It is significant because most of respondents had only received a diploma in schooling. They might have come into contact with security purposes while participating in prior studies. Based on Figure 4.3, there are more than quarter of the respondents which is 31.1% of the respondents are made up Faculty of Computing students, who are more likely to study in the data and network security subject. They need to take the data and network security subject for one semester in order to complete their bachelor degree. From that, they learned more about network security to protect themselves while using the Internet network. The most significant predictors were coping appraisals, which include self-efficacy and response efficacy characteristics. This shows how crucial cognitive functions are to security preservation. The majority of coping assessments were effective predictors of security intentions. The best predictor is habit strength in particular. Therefore, in order to enhance Internet users' security intentions, it will be crucial to inform them of the seriousness of online threats as well as the effectiveness of security measures and make them aware of their obligation to defend themselves online.

By evaluating all the result from the respondents, the survey that have been done to this research can contribute a few impacts to the students in UMP. Students can learn more about network security from the survey. Data security is possible. since we know that, network security inhibits illicit access. Many sensitive pieces of information are stored on a network, including the personal data of university students. Anyone with network access might put this important data in danger. Network security needs to be

implemented as a result to protect them. Moreover, students who are aware of information security issues can also defend themselves against cyberattacks. The bulk of network attacks originate on the internet. In this field, there are experts, and then there are virus outbreaks. If they aren't careful, they might fool around with a lot of the network's information. If network protection is put in place, these assaults won't impact computers. In a nutshell, the survey can offer some information about cyber security that could endanger respondents as they use the Internet.

## **CHAPTER 5**

### **CONCLUSION**

#### **5.1 Introduction**

The purpose of this research is to analyse the UMP student's awareness about cyber security. The data collection is conducted by distributing online surveys among students in University Malaysia Pahang for both campuses which are Gambang and Pekan by using Google Forms. A sample size of 148 respondents was gathered and the results were validated by using IBM SPSS tool with Cronbach's Alpha and Spearman's Rho tests. The model of evaluation of student's awareness about cyber security is based on Protection Motivation Theory (PMT).

#### **5.2 Limitations**

Even if the results were encouraging, there are still certain limitations that can be discovered and investigated in other investigations. This study's primary limitation is the size of the sample that was used.  $N = 148$  was the total achieved acceptable sample size for this study, which is not enough. A sufficient sample size may not have been obtained for a number of reasons, including the following: (1) There is no effective way to contact students other than direct contact through WhatsApp, Telegram, and email; (2) The response rate for this particular project was very low, which may have been due to students conducting their own research or projects during this same semester. In addition, it maybe caused of students busy during their three months semester break which starting from July 2022 until end of October 2022.

The next drawback is that there aren't enough questions to cover all the topics. For instance, several of the questions don't go far enough to address the threat intensity,

threat susceptibility, self-efficacy, and response efficacy variables. The survey's questions were not particularly appropriate.

### **5.3 Future Work**

The advantages and difficulties were discussed in this research. However, the research project was only able to cover and analyse a small amount of data. The use of significantly bigger data sets is advised for use in future research projects. This survey needs more participants by remaining the question that have been asked, which is a problem. With this, the research will be improved. In addition, the survey's questions need to be more reliable in order to make the offered questions more pertinent to the suggested variables. The questions need to be more focused on specific problems and issues. It may also relevant to the current issues that happen in university life.

### **5.4 Summary**

In conclusion, this study, which focuses on University Malaysia Pahang student's cyber security awareness, demonstrates that the respondents generally do not really follow the recommended procedures that will shield them from security threats. All four factors in this study, namely, threat severity, threat susceptibility, self-efficacy and response efficacy show that students' awareness is unsatisfactory. These findings were consistent with those of other studies that assessed the students' knowledge of cyber security. The researcher was adamant that everyone using the internet needed to be made aware of the value of following best practises. Additionally, students in higher education use the Internet frequently and will make up the bulk of the labour force in the future.

Due to these reasons, it is essential that students are informed about cyber security issues. Internet users must be trained to raise their awareness of these situations so they can take pre-cautions when necessary, even though escalating cyber security incidents may not be completely prevented with education and training. Users must have the knowledge necessary to defend themselves. The best defence while browsing the Internet is self-defence.

## REFERENCES

- [1] A. Rahman Ahlan, Y. Arshad, and M. Lubis, "Implication of Human Attitude Factors toward Information Security Awareness in Malaysia Public University."
- [2] F. Liu, E. T. K. Lim, H. Li, C. W. Tan, and D. Cyr, "Disentangling utilitarian and hedonic consumption behavior in online shopping: An expectation disconfirmation perspective," *Information and Management*, vol. 57, no. 3, Apr. 2020, doi: 10.1016/j.im.2019.103199.
- [3] T. Moletsane and P. Tsibolane, "Mobile Information Security Awareness among Students in Higher Education : An Exploratory Study," in *2020 Conference on Information Communications Technology and Society, ICTAS 2020 - Proceedings*, Mar. 2020. doi: 10.1109/ICTAS47918.2020.233978.
- [4] L. Muniandy, B. Muniandy, and Z. Samsudin, "Cyber Security Behaviour among Higher Education Students in Malaysia," *Journal of Information Assurance & Cybersecurity*, pp. 1–13, Feb. 2017, doi: 10.5171/2017.800299.
- [5] H. de Bruijn and M. Janssen, "Building Cybersecurity Awareness: The need for evidence-based framing strategies," *Gov Inf Q*, vol. 34, no. 1, pp. 1–7, Jan. 2017, doi: 10.1016/j.giq.2017.02.007.
- [6] N. Choi, D. Kim, J. Goo, and A. Whitmore, "Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action," *Information Management and Computer Security*, vol. 16, no. 5, pp. 484–501, 2008, doi: 10.1108/09685220810920558.
- [7] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," *Future Internet*, vol. 13, no. 2. MDPI AG, pp. 1–40, Feb. 01, 2021. doi: 10.3390/fi13020039.
- [8] R. Munteanu, "EMERGING SECURITY ISSUES IN THE 21ST CENTURY: THE CONCEPT OF CYBER-SECURITY." [Online]. Available: [http://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=853225](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=853225).
- [9] "guidelines for developing comprehensive cyber security modules for school students. III. METHOD."
- [10] N. J. Jian, I. Farahana, and B. Kamsin, "Cybersecurity Awareness Among the Youngs in Malaysia by Gamification," 2021.

- [11] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior," *Int J Inf Manage*, vol. 45, pp. 13–24, Apr. 2019, doi: 10.1016/j.ijinfomgt.2018.10.017.
- [12] R. A. Maalem Lahcen, B. Caulkins, R. Mohapatra, and M. Kumar, "Review and insight on the behavioral aspects of cybersecurity," *Cybersecurity*, vol. 3, no. 1. Springer Science and Business Media B.V., Dec. 01, 2020. doi: 10.1186/s42400-020-00050-w.
- [13] L.-W. Wong, V.-H. Lee, G. W.-H. Tan, K.-B. Ooi, and A. Sohal, "The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities," *Int J Inf Manage*, vol. 66, p. 102520, Oct. 2022, doi: 10.1016/j.ijinfomgt.2022.102520.
- [14] L. de Kimpe, M. Walrave, P. Verdegem, and K. Ponnet, "What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context," *Behaviour and Information Technology*, 2021, doi: 10.1080/0144929X.2021.1905066.
- [15] M. Wilson, S. McDonald, D. Button, and K. McGarry, "It Won't Happen to Me: Surveying SME Attitudes to Cyber-security," *Journal of Computer Information Systems*, pp. 1–13, May 2022, doi: 10.1080/08874417.2022.2067791.
- [16] H. Y. S. Tsai, M. Jiang, S. Alhabash, R. Larose, N. J. Rifon, and S. R. Cotten, "Understanding online safety behaviors: A protection motivation theory perspective," *Comput Secur*, vol. 59, pp. 138–150, Jun. 2016, doi: 10.1016/j.cose.2016.02.009.
- [17] M. Martens, R. de Wolf, and L. de Marez, "Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general," *Comput Human Behav*, vol. 92, pp. 139–150, Mar. 2019, doi: 10.1016/j.chb.2018.11.002.
- [18] S. F. Verkijika, "Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret," *Comput Secur*, vol. 77, pp. 860–870, Aug. 2018, doi: 10.1016/j.cose.2018.03.008.
- [19] H. Chan and S. Mubarak, "Significance of Information Security Awareness in the Higher Education Sector," 2012.
- [20] N. Borgert and Elson, "The Study of Cybersecurity Self-Efficacy: A Systematic Literature Review of Methodology." [Online]. Available: <https://osf.io/vf6bn/>

## APPENDIX A LIST OF QUESTIONNAIRES

### Cyber Security Awareness among students in UMP

Assalamualaikum and Greetings Everyone!

My name is Nur Madihah binti Mazlan (Faculty of Computing), Bachelor of Computer Science (Computer System & Networking) from Universiti Malaysia Pahang (UMP) currently conducting a survey for my final year project under supervision Mr. Syahrizal Azmir bin Md. Sharif (Faculty of Computing). Specifically, my research is to predict the level of cyber security awareness of UMP students.

The research objective is to study the level of knowledge about information security awareness among the students in UMP. This research is solely for academic purposes. Therefore, I would really appreciate if you can spend your time to answer the questionnaire by completing ALL sections and items in the survey. Your contribution to this effort is very much appreciated.

If you have any questions, please contact me:  
Nur Madihah Binti Mazlan  
nrmdihah58@gmail.com

Thank you in advance for your valuable time and cooperation.



(not shared) [Switch account](#)



\* Required

Email Address \*

Your answer

#### DEMOGRAPHIC

Gender \*

- Male  
 Female

Age \*

- 18 - 21 years old  
 22 - 25 years old  
 26 - 30 years old  
 31 and above



Campus \*

- Gambang
- Pekan

Faculty \*

- Centre for Mathematical Sciences
- College of Engineering
- Faculty of Chemical and Process Engineering Technology
- Faculty of Civil Engineering Technology
- Faculty of Computing
- Faculty of Electrical and Electronics Engineering Technology
- Faculty of Industrial Management
- Faculty of Industrial Sciences and Technology
- Faculty of Manufacturing and Mechatronic Engineering Technology
- Faculty of Mechanical and Automotive Engineering Technology

Current Academic Status \*

- Undergraduate
- Postgraduate

Highest Education Background \*

- High School
- Diploma/Matriculation/STPM
- Bachelor
- Post graduate

## Security Intentions

This section describes about someone's awareness of taking any action with the aim to hurt someone else without justification.

Please read carefully how far you aware with the statement regarding intention based on your opinion.

Do you have prior knowledge about cybersecurity? \*

- Yes
- No
- Not sure

Do you have prior knowledge about Information Security? \*

- Yes
- No
- Not sure

How aware are you of the following concepts? \*

|         | Totally not aware     | Not aware             | Neutral               | Aware                 | Totally aware         |
|---------|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Malware | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Scams   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

How aware are you of these countermeasures? \*

|  | Totally not aware     | Not aware             | Neutral               | Aware                 | Totally aware         |
|--|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Install software such as anti-virus, anti-spyware, backup software in my personal computer and laptop                          | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Set up software that is included with your operating system such as firewall, defender to protect personal computer and laptop | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Secure a Wi-Fi network   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Set up difficult to guess passwords for accounts and home network  | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Share personal information on the Internet   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

## Threat Severity

This section is to analyze that respondents need to know the Malware and Scams is dangerous and would risks their online safety .

Malware is the malicious software that affects the normal functioning of your device. e.g. virus, worms, trojan horses, adware, botnets, ransomware.

A scam is the action whereby information or money is obtained by misleading a victim using information technologies. e.g. via mail, false websites.

Please read carefully how far you agree with the statement regarding threat severity based on your opinion.

To what extent do you agree with the following statements? \*

|   | Totally disagree      | Disagree              | Neutral               | Agree                 | Totally Agree         |
|---|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Malware cause a system crash from time to time                                      | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Malware can reveals personal passwords to inline criminals                          | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Scams can steal someone's personal information                                      | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Scams can increase the nuisance phone calls, emails, and texts from various sources | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Scams can cause lasting mental and physical trauma for victims                      | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

## Threat Susceptibility

This section will discuss about the someone's probability of experiencing internet security hazards.

Please read carefully how far you agree with the statement regarding threat susceptibility based on your opinion.

Please tell us how much you agree or disagree with each statement. \*

|  | Totally disagree      | Disagree              | Neutral               | Agree                 | Totally Agree         |
|--|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| The risk is big that I become a victim of malware                                      | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Malware is extremely likely that my computer will be infected by malware in the future | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| There is a good possibility that my personal devices will have malware                 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| My chances of being a scams victim is high   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| There is possible I been the victim of an online scam and lost money                   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

## Self-Efficacy

This section will explain about someone's capacity to take precautions on the internet which was linked to process or system and comfort when engaging online preventive action.

Please read carefully how far you agree with the statement regarding self-efficacy based on your opinion.

Please tell us how much you agree or disagree with each statement. \*

|  | Totally disagree      | Disagree              | Neutral               | Agree                 | Totally Agree         |
|--|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| I feel comfortable taking measures to secure my primary home computer or personal laptop | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| By taking the necessary security measures is entirely under my control                   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| I have resources and the knowledge to take necessary security measures                   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| I feel nervous when I think about online security issues                                 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

## Response Efficacy

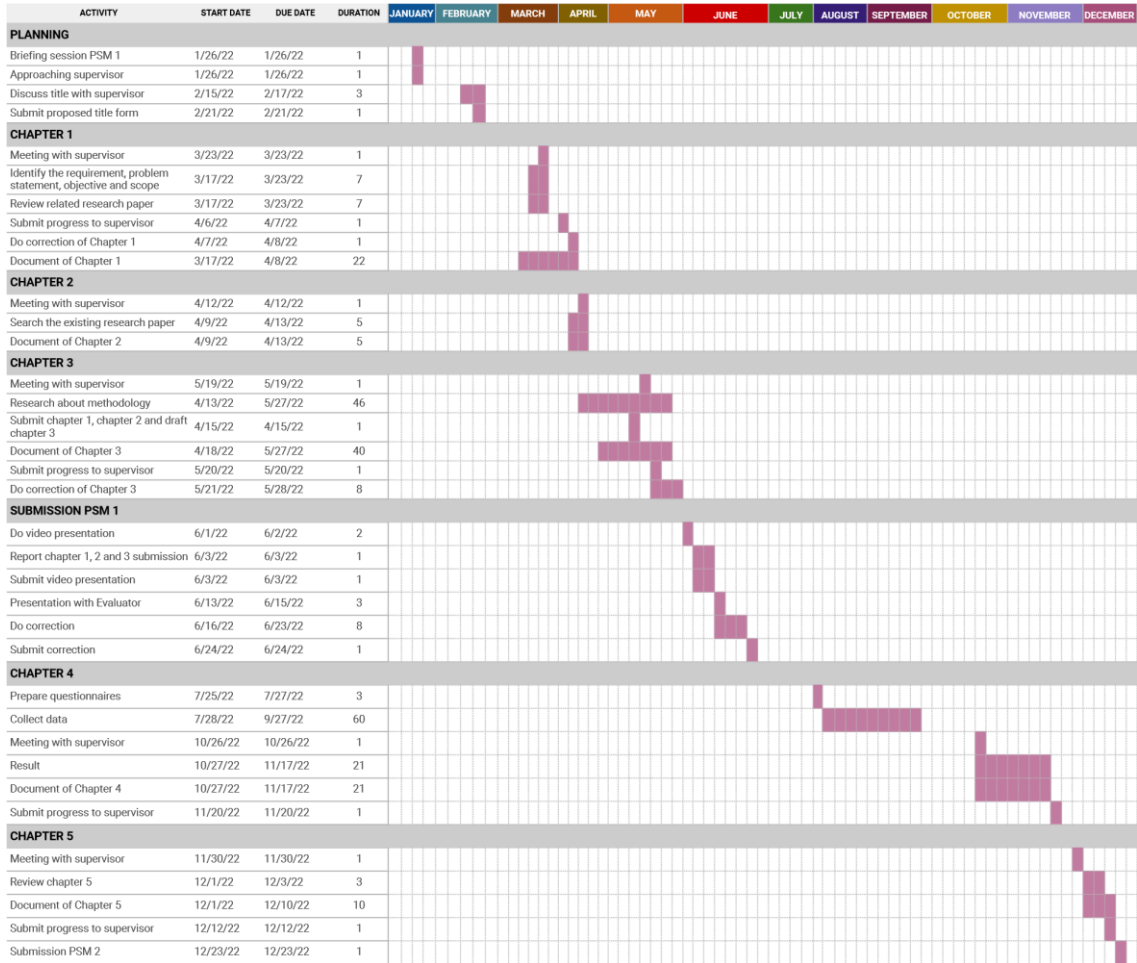
This section is to evaluate the effectiveness of completing protective measure against cybercrime and will concerned with the individual's belief in the action's perceived advantages.

Please read carefully how far you agree with the statement regarding response efficacy based on your opinion.

Please tell us how much you agree or disagree with each statement. \*

|   | Totally disagree      | Disagree              | Neutral               | Agree                 | Totally Agree         |
|---|-----------------------|-----------------------|-----------------------|-----------------------|-----------------------|
| Protective software would be useful for detecting and remove the malware            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Protective software would increase my performance in protecting myself from malware | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Protective software would enable me to search and remove malware faster             | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Safety measures against scams are effective in preventing scams                     | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Protective software would be useful for detecting and removing scams issues         | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

# APPENDIX B GANTT CHART





## APPENDIX C NON-PARAMETRIC TEST

### Case Processing Summary

|                       | Valid               |         | Cases Missing |         | Total |         |
|-----------------------|---------------------|---------|---------------|---------|-------|---------|
|                       | N                   | Percent | N             | Percent | N     | Percent |
|                       | Security Intentions | 148     | 100.0%        | 0       | 0.0%  | 148     |
| Threat Severity       | 148                 | 100.0%  | 0             | 0.0%    | 148   | 100.0%  |
| Threat Susceptibility | 148                 | 100.0%  | 0             | 0.0%    | 148   | 100.0%  |
| Self-Efficacy         | 148                 | 100.0%  | 0             | 0.0%    | 148   | 100.0%  |
| Response Efficacy     | 148                 | 100.0%  | 0             | 0.0%    | 148   | 100.0%  |

### Tests of Normality

|                       | Kolmogorov-Smirnov <sup>a</sup> |     |      | Shapiro-Wilk |     |      |
|-----------------------|---------------------------------|-----|------|--------------|-----|------|
|                       | Statistic                       | df  | Sig. | Statistic    | df  | Sig. |
| Security Intentions   | .162                            | 148 | .000 | .935         | 148 | .000 |
| Threat Severity       | .157                            | 148 | .000 | .967         | 148 | .001 |
| Threat Susceptibility | .151                            | 148 | .000 | .942         | 148 | .000 |
| Self-Efficacy         | .209                            | 148 | .000 | .917         | 148 | .000 |
| Response Efficacy     | .311                            | 148 | .000 | .822         | 148 | .000 |

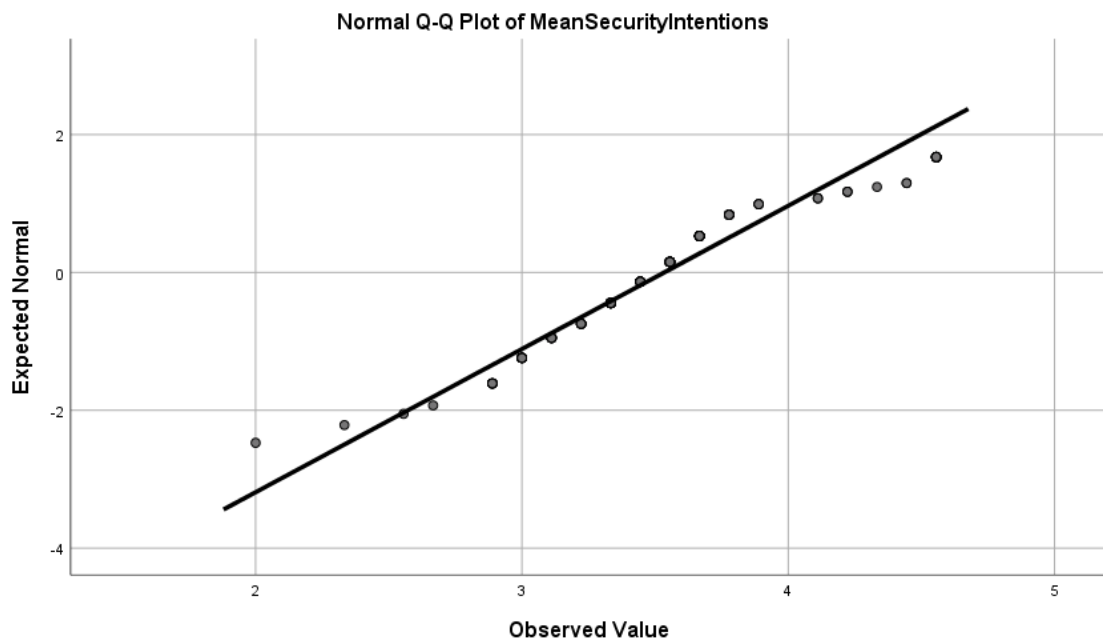
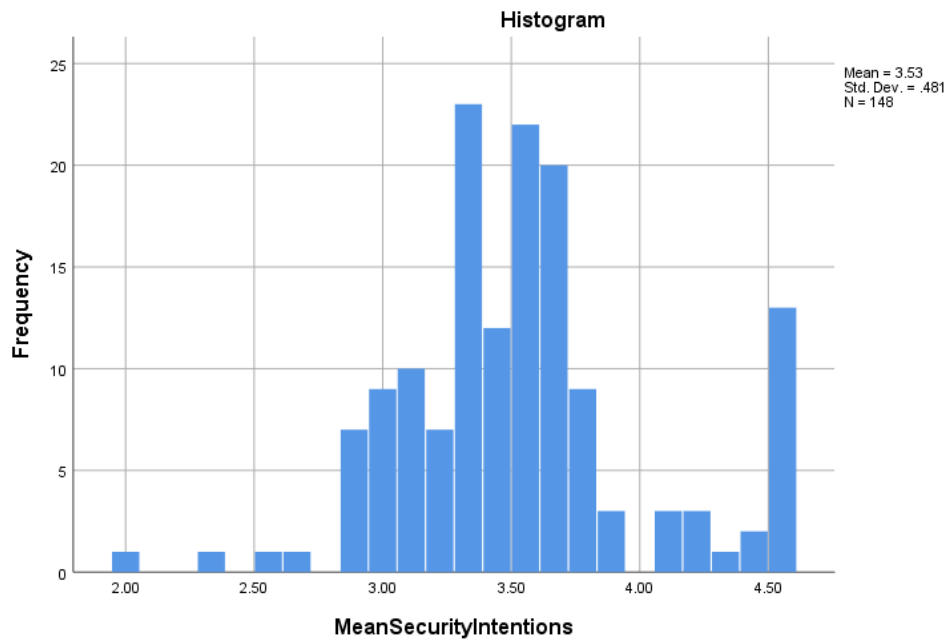
a. Lilliefors Significance Correction

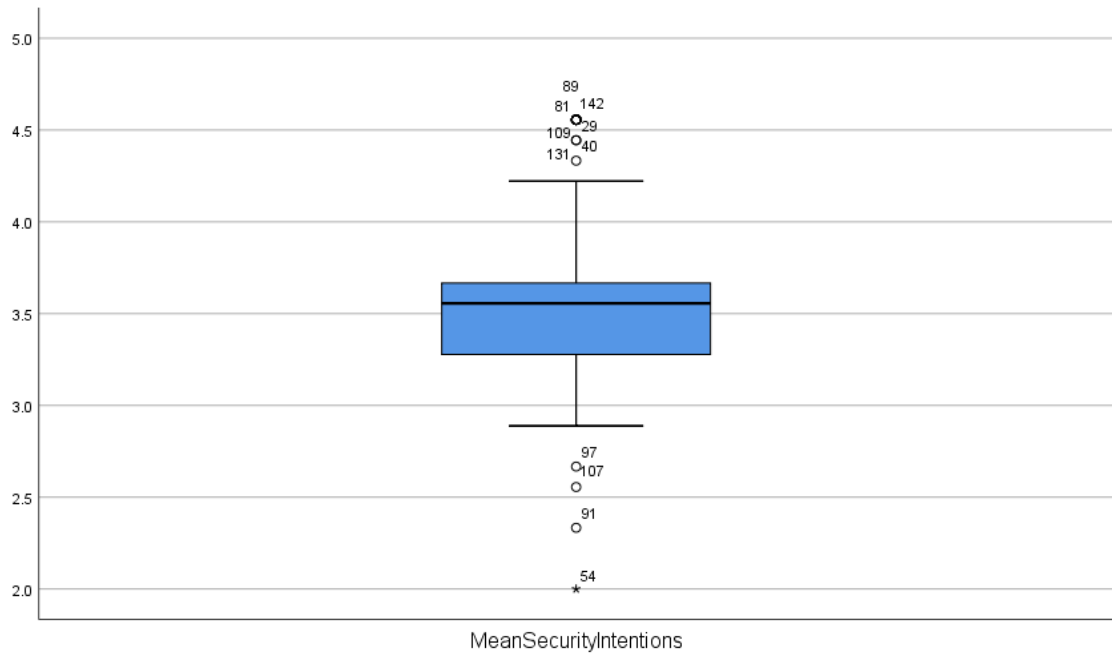
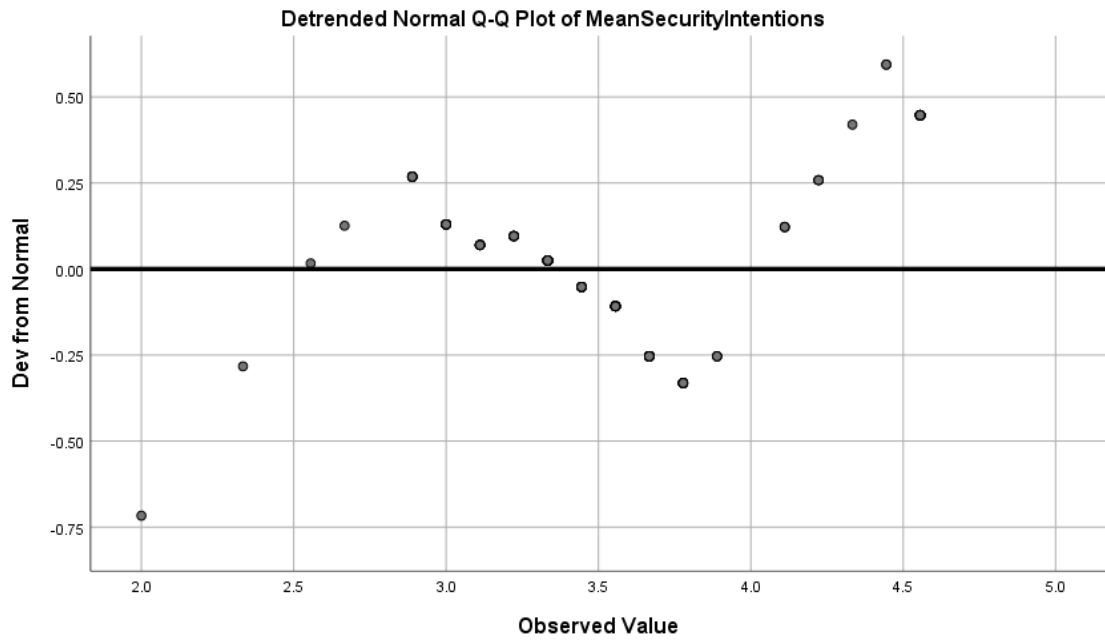
## Descriptives

|                                  |                                  | Statistic   | Std. Error |        |
|----------------------------------|----------------------------------|-------------|------------|--------|
| Security Intentions              | Mean                             | 3.5345      | .03955     |        |
|                                  | 95% Confidence Interval for Mean | Lower Bound | 3.4564     |        |
|                                  |                                  | Upper Bound | 3.6127     |        |
|                                  | 5% Trimmed Mean                  | 3.5287      |            |        |
|                                  | Median                           | 3.5556      |            |        |
|                                  | Variance                         | .232        |            |        |
|                                  | Std. Deviation                   | .48116      |            |        |
|                                  | Minimum                          | 2.00        |            |        |
|                                  | Maximum                          | 4.56        |            |        |
|                                  | Range                            | 2.56        |            |        |
|                                  | Interquartile Range              | .42         |            |        |
|                                  | Skewness                         | .393        | .199       |        |
|                                  | Kurtosis                         | .703        | .396       |        |
|                                  | Threat Severity                  | Mean        | 3.9392     | .03824 |
| 95% Confidence Interval for Mean |                                  | Lower Bound | 3.8636     |        |
|                                  |                                  | Upper Bound | 4.0148     |        |
| 5% Trimmed Mean                  |                                  | 3.9399      |            |        |
| Median                           |                                  | 4.0000      |            |        |
| Variance                         |                                  | .216        |            |        |
| Std. Deviation                   |                                  | .46520      |            |        |
| Minimum                          |                                  | 2.80        |            |        |
| Maximum                          |                                  | 5.00        |            |        |
| Range                            |                                  | 2.20        |            |        |
| Interquartile Range              |                                  | .60         |            |        |
| Skewness                         |                                  | .007        | .199       |        |
| Kurtosis                         |                                  | -.105       | .396       |        |
| Threat Susceptibility            |                                  | Mean        | 2.3324     | .07371 |
|                                  | 95% Confidence Interval for Mean | Lower Bound | 2.1868     |        |
|                                  |                                  | Upper Bound | 2.4781     |        |
|                                  | 5% Trimmed Mean                  | 2.2958      |            |        |
|                                  | Median                           | 2.0000      |            |        |
|                                  | Variance                         | .804        |            |        |
|                                  | Std. Deviation                   | .89672      |            |        |
|                                  | Minimum                          | 1.00        |            |        |
|                                  | Maximum                          | 5.00        |            |        |
|                                  | Range                            | 4.00        |            |        |
|                                  | Interquartile Range              | 1.40        |            |        |
|                                  | Skewness                         | .526        | .199       |        |

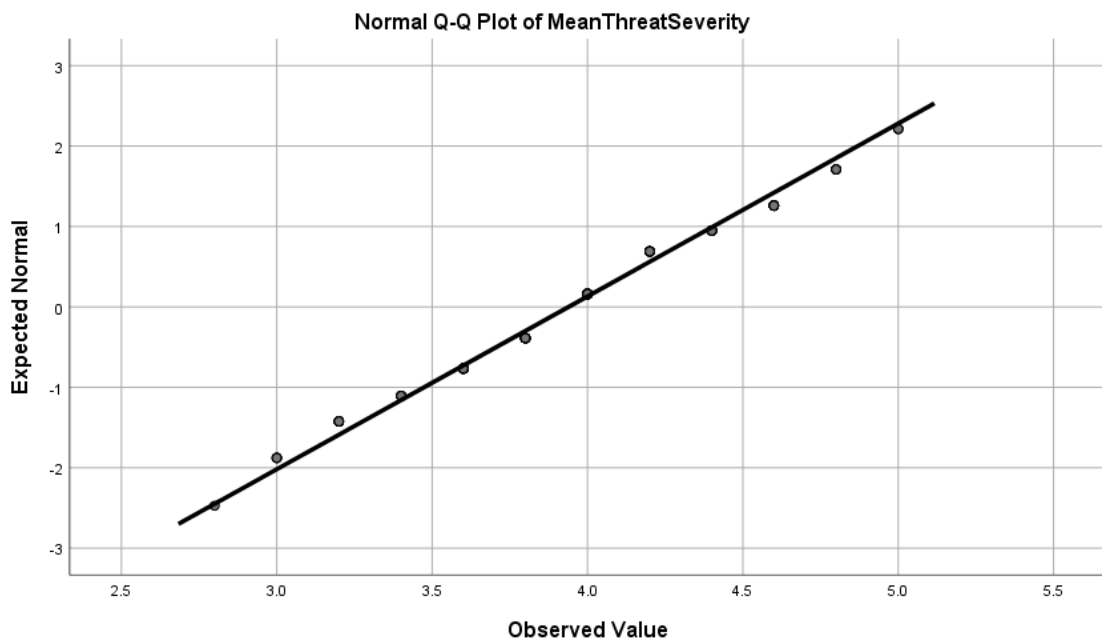
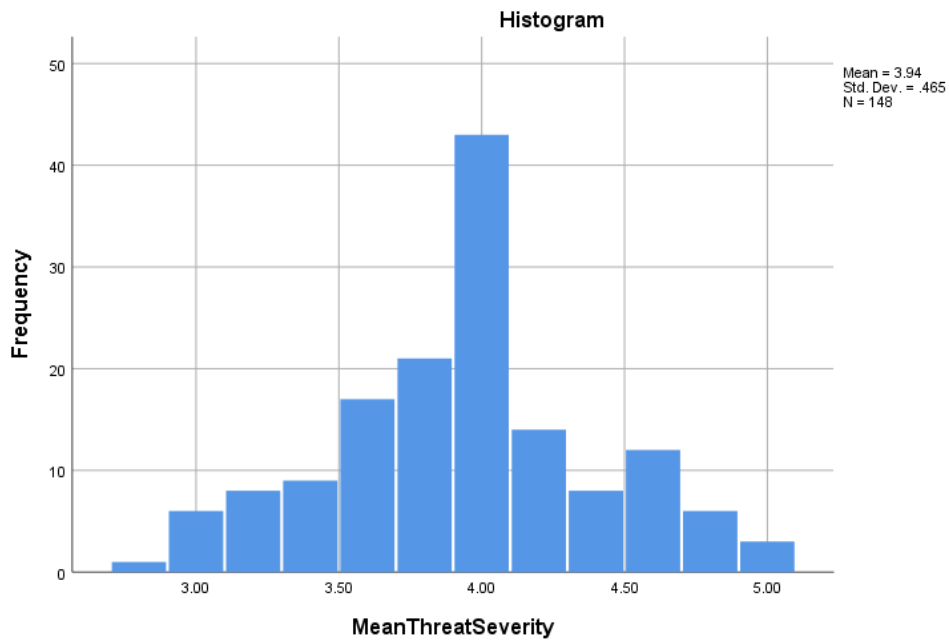
|                                  |                                  |             |        |        |
|----------------------------------|----------------------------------|-------------|--------|--------|
|                                  | Kurtosis                         |             | -.202  | .396   |
| Self-Efficacy                    | Mean                             |             | 3.7676 | .03603 |
|                                  | 95% Confidence Interval for Mean | Lower Bound | 3.6964 |        |
|                                  |                                  | Upper Bound | 3.8388 |        |
|                                  | 5% Trimmed Mean                  |             | 3.7595 |        |
|                                  | Median                           |             | 4.0000 |        |
|                                  | Variance                         |             | .192   |        |
|                                  | Std. Deviation                   |             | .43834 |        |
|                                  | Minimum                          |             | 2.60   |        |
|                                  | Maximum                          |             | 5.00   |        |
|                                  | Range                            |             | 2.40   |        |
|                                  | Interquartile Range              |             | .40    |        |
|                                  | Skewness                         |             | .115   | .199   |
|                                  | Kurtosis                         |             | .798   | .396   |
|                                  | Response Efficacy                | Mean        |        | 3.9811 |
| 95% Confidence Interval for Mean |                                  | Lower Bound | 3.9185 |        |
|                                  |                                  | Upper Bound | 4.0436 |        |
| 5% Trimmed Mean                  |                                  |             | 3.9532 |        |
| Median                           |                                  |             | 4.0000 |        |
| Variance                         |                                  |             | .148   |        |
| Std. Deviation                   |                                  |             | .38498 |        |
| Minimum                          |                                  |             | 3.20   |        |
| Maximum                          |                                  |             | 5.00   |        |
| Range                            |                                  |             | 1.80   |        |
| Interquartile Range              |                                  |             | .40    |        |
| Skewness                         |                                  |             | 1.134  | .199   |
| Kurtosis                         |                                  |             | 1.261  | .396   |

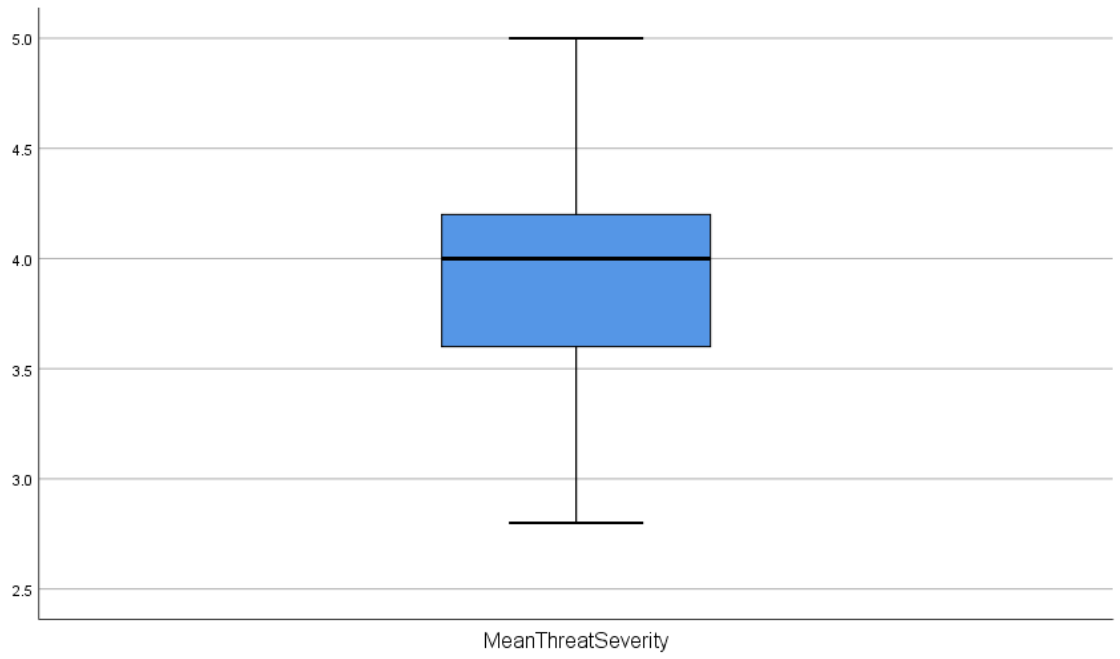
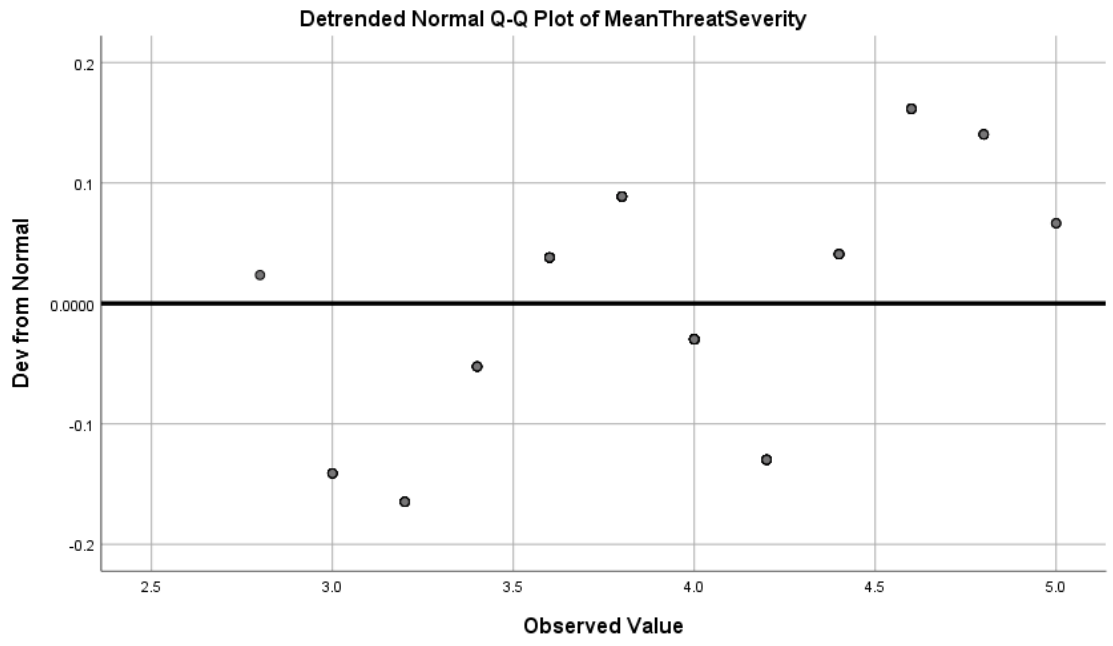
# 1. Security Intentions



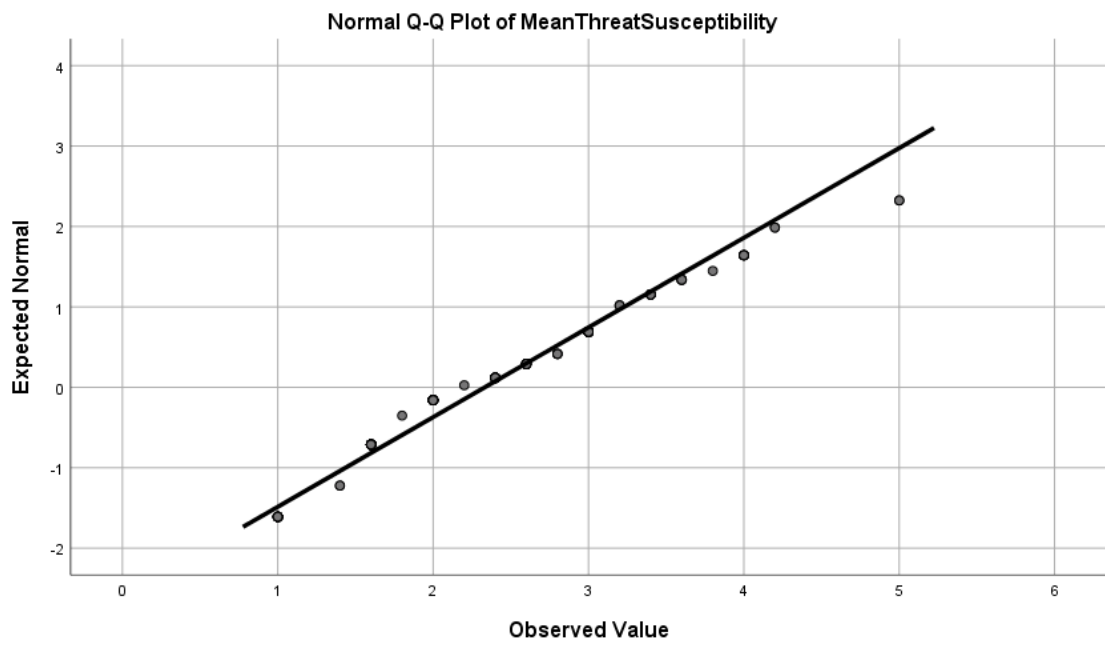
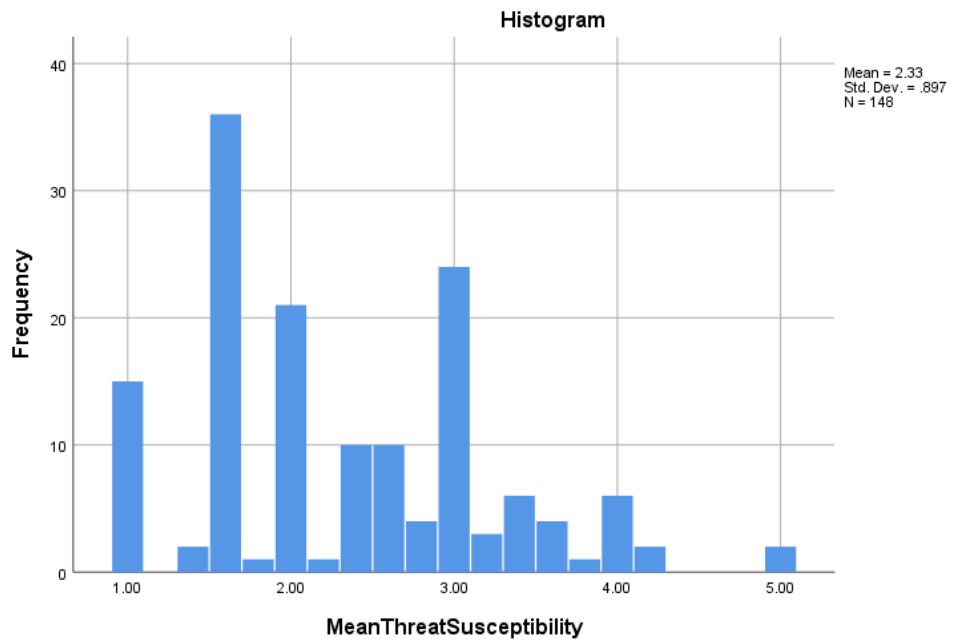


## 2. Threat Severity

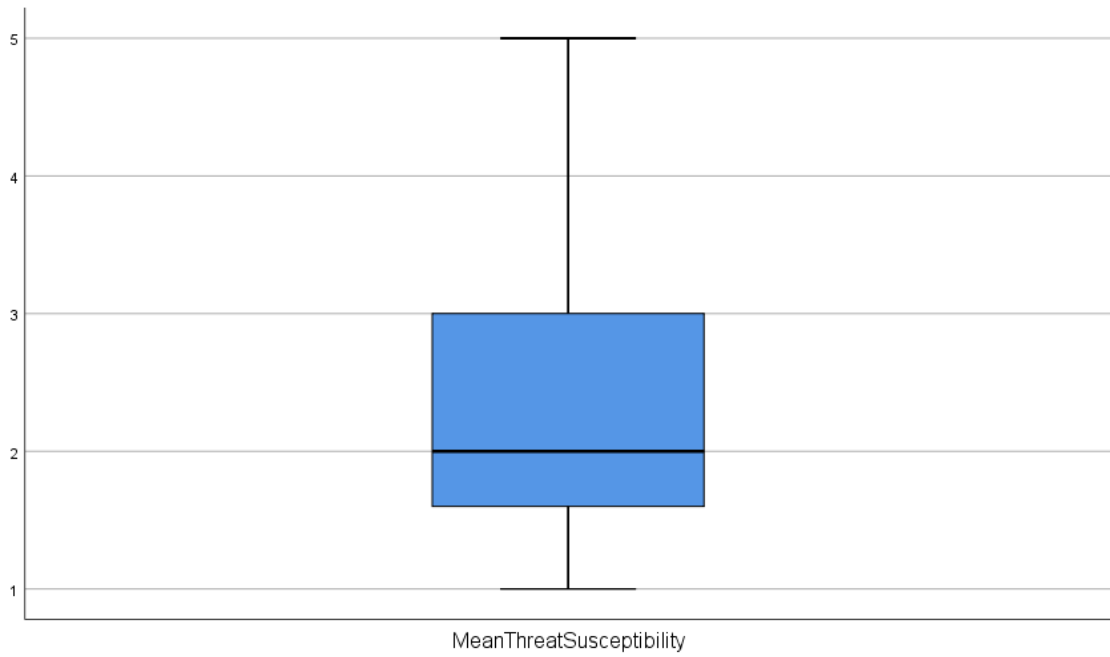
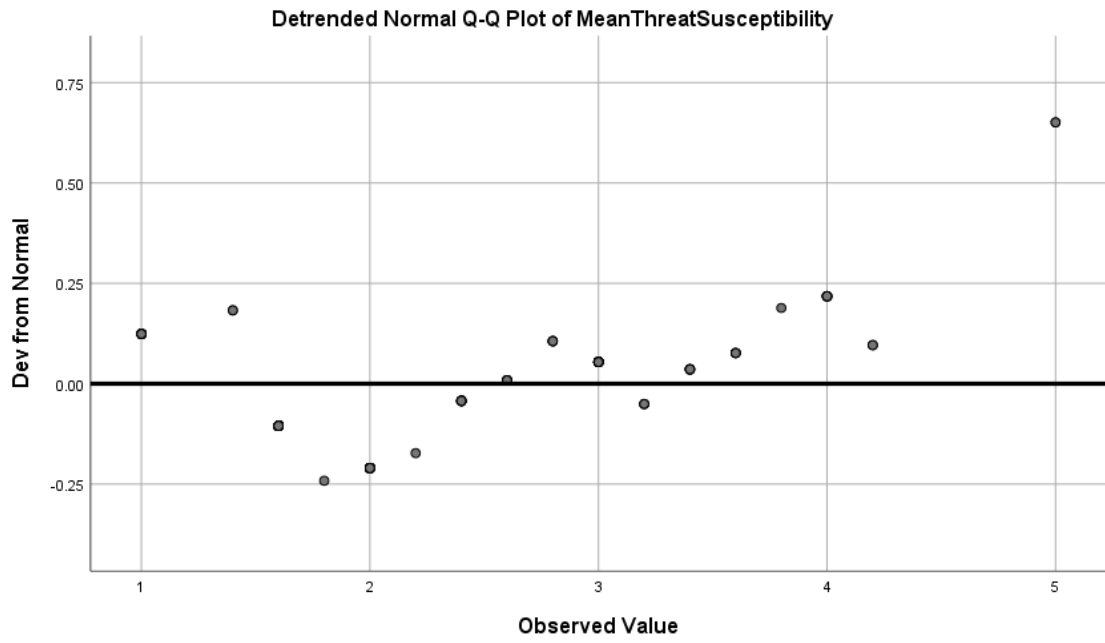




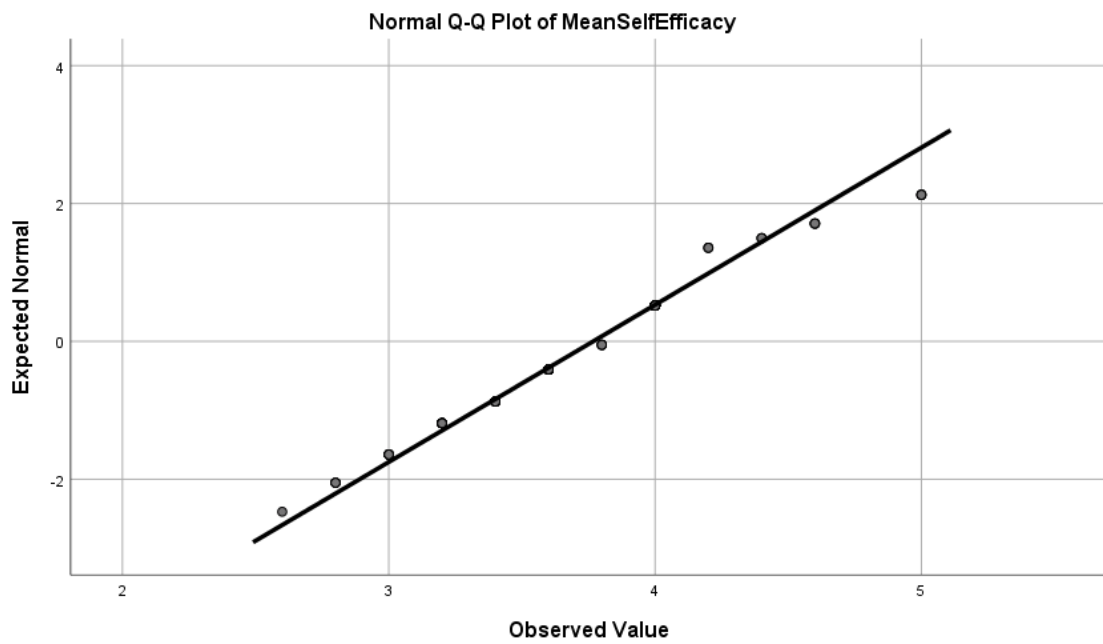
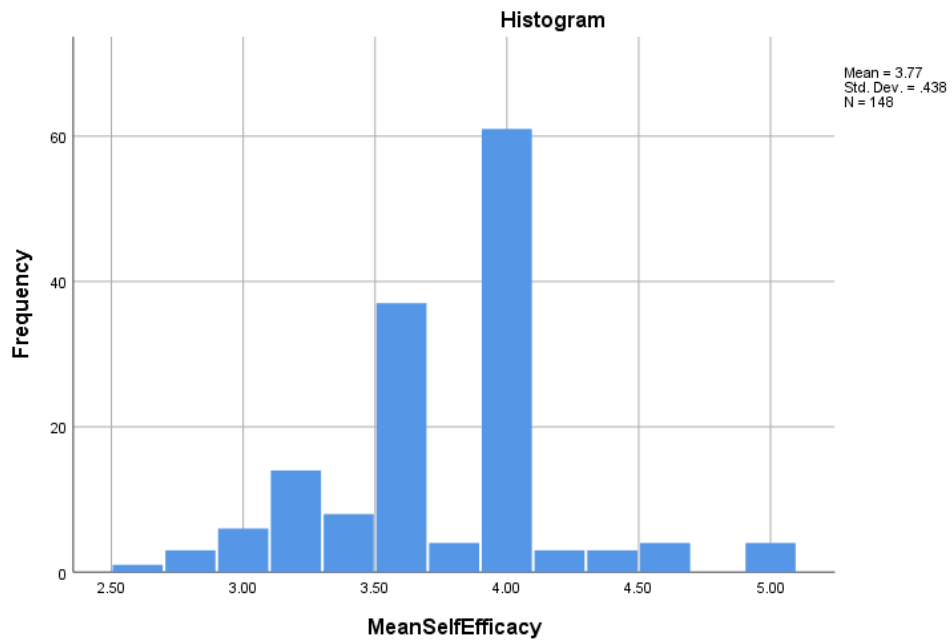
### 3. Threat Susceptibility

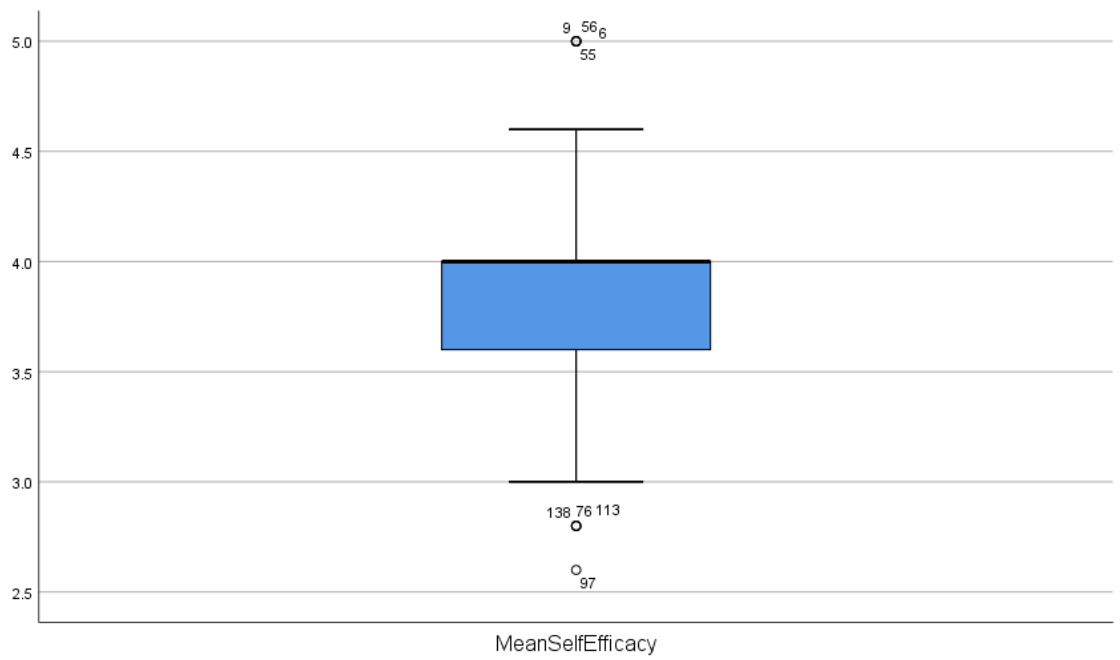
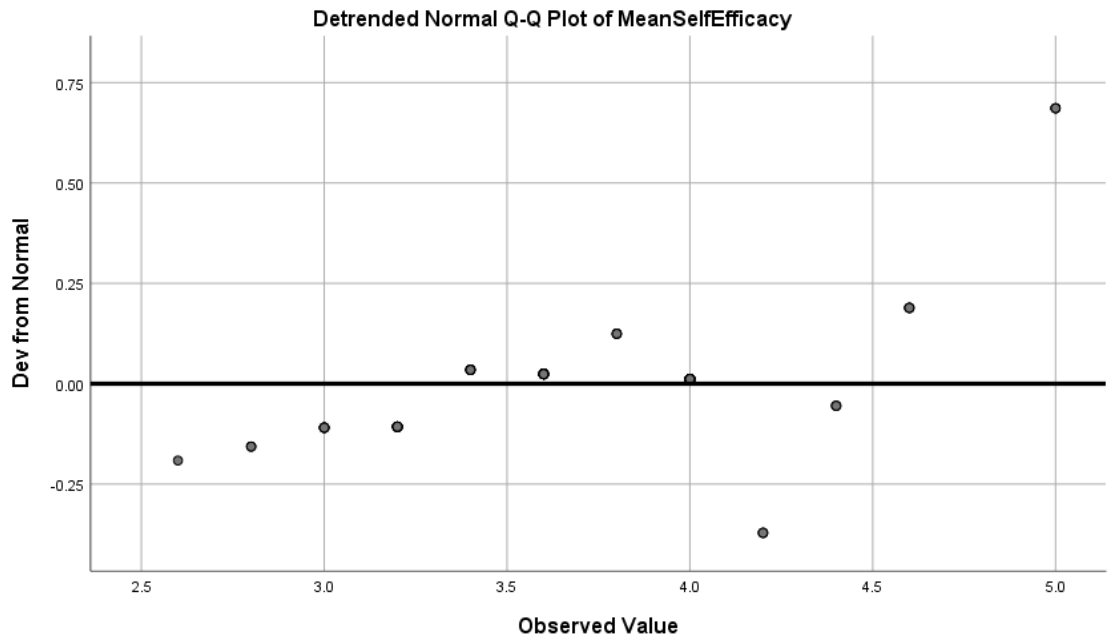






## 4. Self-Efficacy





## 5. Response Efficacy

