# CYBERSECURITY BEHAVIOURAL MODEL FOR STUDENTS IN THE TERTIARY INSTITUTIONS

FATOKUN FAITH BOLUWATIFE

FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY
UNIVERSITY OF MALAYA
KUALA LUMPUR

2020

# CYBERSECURITY BEHAVIOURAL MODEL FOR STUDENTS IN THE TERTIARY INSTITUTIONS

**FATOKUN FAITH BOLUWATIFE**

**DISSERTATION SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF COMPUTER SCIENCE (APPLIED COMPUTING)**

**FACULTY OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY**
**UNIVERSITY OF MALAYA**
**KUALA LUMPUR**

**2020**

**UNIVERSITY OF MALAYA**

**ORIGINAL LITERARY WORK DECLARATION**

Name of Candidate: **Fatokun Faith Boluwatife**

Matric No: **WOA170009**

Name of Degree: **Masters in Computer Science (Applied Computing)** Title of Project Paper/Research Report/Dissertation/Thesis ("this Work"):

**Cybersecurity Behavioural Model for Students in the Tertiary Institutions**

Field of Study: **Information Systems**

I do solemnly and sincerely declare that:

(1) I am the sole author/writer of this Work;
(2) This Work is original;
(3) Any use of any work in which copyright exists was done by way of fair dealing and for permitted purposes and any excerpt or extract from, or reference to or reproduction of any copyright work has been disclosed expressly and sufficiently and the title of the Work and its authorship have been acknowledged in this Work;
(4) I do not have any actual knowledge nor do I ought reasonably to know that the making of this work constitutes an infringement of any copyright work;
(5) I hereby assign all and every rights in the copyright to this Work to the University of Malaya ("UM"), who henceforth shall be owner of the copyright in this Work and that any reproduction or use in any form or by any means whatsoever is prohibited without the written consent of UM having been first had and obtained;
(6) I am fully aware that if in the course of making this Work I have infringed any copyright whether intentionally or otherwise, I may be subject to legal action or any other action as may be determined by UM.

Candidate's Signature: Date:

Subscribed and solemnly declared before,

Witness's Signature : Date:

Name:

Designation:

**CYBERSECURITY BEHAVIORAL MODEL FOR STUDENTS IN THE TERTIARY INSTITUTIONS**

## ABSTRACT

Humans are majorly identified as the weakest link in cybersecurity. Tertiary institution student's face lot of cybersecurity issues due to their increased Internet exposure, however cybersecurity behavioural studies focusing on tertiary students is limited. This study focused on investigating tertiary institutions students' cybersecurity behaviour, via validated cybersecurity factors, Perceived Vulnerability (PV); Perceived Barriers (PBr); Perceived Severity (PS); Security Self-Efficacy (SSE); Response Efficacy (RE); Cues to Action (CA); Peer Behaviour (PBhv); Computer Skills (CS); Internet Skills (IS); Prior Experience with Computer Security Practices (PE); Perceived Benefits (PBnf); and a newly added factor, Familiarity with Cyber-Threats (FCT), to explore the factors relationship with the students' Cybersecurity Behaviours (CSB). The research also explored if age, gender and educational level had any moderating effect on the cybersecurity behaviour factors. The new construct of Familiarity with Cyber-Threat performed excellently well. The research investigations resulted into a model tagged: Cybersecurity Behavioural Model for Tertiary Institutions Students (CBM-TIS). A cross-sectional online survey was used to gather data from 450 undergraduate and postgraduate students from tertiary institutions within Klang Valley, Malaysia. Series of Structural Equation Modelling techniques was employed for the model's evaluation, and SPSS version 25 was used as the tool for data analysis. Results from regression analysis indicated that the influencing factors of the student's cybersecurity behaviours were their SSE ($t = 4.325$, $P<0.001$), RE ($t = 2.167$, $P = 0.031$), PE ($t = 5.281$, $P<0.001$) and PBnf ($t = 1.978$, $P = 0.04$). Also, from the point biserial correlation analysis, Age had effect only on PBr ($r = 0.101$, $p = 0.036$), while gender had effects on PS ($r = -0.132$, $p = 0.006$), SSE ($r = 0.362$, $p<0.001$), CS ($r = 0.233$, $p<0.001$), IS ($r = 0.115$, $p = 0.016$), PE ($r = 0.123$, p

= 0.010), and CSB (r = 0.150, p = 0.002); however Educational level had effects on CS (r = 0.155, p = 0.001), IS (r = 0.120, p = 0.012), FCT (r = 0.106, p = 0.026), and CSB (r = 0.110, p = 0.022). From the Pearson Correlation analysis conducted, PV ($R^2$ = 0.377, p = 0.003), PBr ($R^2$ = 0.332, p = 0.002), SSE ($R^2$ = 0.670, p < 0.001), RE ($R^2$ = 0.495, p < 0.001), CA ($R^2$ = 0.471, p < 0.001), PBhv ($R^2$ = 0.436, p < 0.001), CS ($R^2$ = 0.594, p < 0.001), IS ($R^2$ = 0.428, p < 0.001), PE ($R^2$ = 0.667, p < 0.001), PBnf ($R^2$ = 0.511, p < 0.001), and FCT ($R^2$ = 0.540, p < 0.001) were all significantly related to the student's cybersecurity behaviours, except PS. Practically, the study instigates the need for more cybersecurity training and practices in the tertiary institutions. The factor of Prior Experiences with Computer Security Practices had the highest influence on the student's cybersecurity behaviour, hence if appropriate security practices are being upheld by tertiary institutions, it would help in maintaining good cybersecurity assurance in the entire institution.

**Keywords:** Cybersecurity, Cybersecurity Behaviours, Tertiary Institution Students, Cybersecurity Beliefs, Cybersecurity Behavioural Model

**MODEL TINGKAH LAKU KESELAMATAN SIBER UNTUK MAHASISWA DI INSTITUSI PENGAJIAN TINGGI**

## ABSTRAK

Manusia adalah insan yang paling lemah dalam kontext keselamatan siber disebabkan kekurangan pendedahan tentang tingkahlaku berhemah ketika berada di alam maya. Akan tetapi, kajian-kajian lepas berkaitan dengan keselamatan siber melibatkan tingkah laku mahasiswa di peringkat IPT adalah terhad. Dalam kajian ini, peyelidik menyiasat tingkah laku keselamatan siber dalam kalangan mahasiswa dengan menggunakan komponen – komponen keselamatan siber yang ditentukan kesahan iaitu *Perceived Vulnerability (PV); Perceived Barriers (PBr); Perceived Severity (PS); Security Self-Efficacy (SSE); Response Efficacy (RE); Cues to Action (CA); Peer Behaviour (PBhv); Computer Skills (CS); Internet Skills (IS); Prior Experience with Computer Security Practices (PE); Perceived Benefits (PBnf);* dan komponen baru, *Familiarity with Cyber-Threats (FCT)* untuk menyiasat bagaimana ia berkait rapat dengan tingkah laku keselamatan dalam kalangan mahasiswa . Dalam kajian ini juga, penyelidik mendapati faktor-faktor sosiologi seperti umur, jantina dan tahap pendidikan mempunyai kesan terhadap tingkah laku keselamatan siber. Konstruk baru *Familiarity with Cyber-Threats (FCT)* terbukti memberi kesan yang positif dalam kajian ini. Oleh itu, sebuah model tingkah laku keselamatan siber untuk mahasiswa telah direka bentuk. Penyelidik telah menggunkan kajian rentas menggunakan soal selidik dalam talian kepada 450 pelajar sarjana muda dan sarjana dari IPT di sekitar Lembah Klang, Malaysia. Pengantar *Structural Equation Modeling (SEM)* telah digunakan untuk membangunkan dan menguji model statistic. Pakej Statistik untuk Sains Sosial versi 25 telah digunakan untuk ujian deskriptif dan inferensi. Analisis regresi menunjukkan bahawa faktor-faktor yang mempunyai pengaruh terhadap tingkah laku keselamatan siber dalam kalangan mahasiswa adalah *SSE* ($t = 4.325$, $P<0.001$), *RE* ($t = 2.167$, $P = 0.031$), *PE* ($t = 5.281$, $P<0.001$) dan *PBnf* ($t = 1.978$,

P = 0.04). Berdasarkan analisis Point-Biserial Ujian Kolerasi, umur mempunyai efek moderasi terhadap *PBr* (r = 0.101, p = 0.036) manakala jantina mempunyai efek moderasi terhadap *PS* (r = -0.132, p = 0.006), *SSE* (r = 0.362, p<0.001), *CS* (r = 0.233, p<0.001), *IS* (r = 0.115, p = 0.016), *PE* (r = 0.123, p = 0.010), dan *CSB* (r = 0.150, p = 0.002). Akan tetapi, tahap pendidikan hanya mempengaruhi *CS* (r = 0.155, p = 0.001), *IS* (r = 0.120, p = 0.012), *FCT* (r = 0.106, p = 0.026), dan *CSB* (r = 0.110, p = 0.022). Analisis korelasi pearson, *PV* ($R^2$ = 0.377, p = 0.003), *PBr* ($R^2$ = 0.332, p = 0.002), *SSE* ($R^2$ = 0.670, p < 0.001), *RE* ($R^2$ = 0.495, p < 0.001), *CA* ($R^2$ = 0.471, p < 0.001), *PBh*v ($R^2$ = 0.436, p < 0.001), *CS* ($R^2$ = 0.594, p < 0.001), *IS* ($R^2$ = 0.428, p < 0.001), *PE* ($R^2$ = 0.667, p < 0.001), *PBnf* ($R^2$ = 0.511, p < 0.001), dan *FCT* ($R^2$ = 0.540, p < 0.001) mempunyai perhubungan yang signifikan terhadap model tingkah laku keselamatan siber kecuali komponen *PS*. Dari segi praktis, kajian ini menyiasat keperluan latihan dan pengamalan keselamatan siber di IPT. Faktor seperti *PE* mempunyai pengaruh yang tinggi terhadap keselamatan siber dalam kalangan mahasiswa. Oleh itu, jika praktis keselamatan yang sesuai dilaksanakan oleh semua IPT, ia akan membantu untuk menjamin keselamatan siber di seluruh institusi.

**Kata Kunci**: keselamatan siber. tingkah laku keselamatan siber, mahasiswa institusi pengajian tinggi, kepercayaan terhadap keselamatan siber, model tingkah laku keselamatan siber

## ACKNOWLEDGEMENTS

I would first love to give my profound gratitude to God Almighty, for giving me life, wisdom and sound health throughout my research period. His name alone be highly exalted and glorified.

My special undiluted appreciation goes to my distinguished and kind-hearted supervisors, **Dr Suraya Hamid** and **Dr Azah Norman**. Indeed, I have been highly privileged to be under their supervision. They have proven to not just be supervisors to me, but my parents here in Malaysia; I would say that without your encouragements and continuous grooming, I am pretty sure I would not be able to get to the end-tail of my research. Indeed, I am grateful, and may God reward you greatly.

I would be an ingrate if I don't acknowledge my lovely parents, **Prof J.O Fatokun** and **Prof KVF Fatokun**, for their unending support, both financially, spiritually, and emotionally towards the progress of my studies. It's only God that can reward you for your labour of love. Furthermore, I would love to appreciate my siblings, **Deborah Fatokun**, **Dorcas Fatokun**, **Delight Fatokun**, **Isaac Fatokun**, and **Israel Fatokun**, for their support in always having me in their minds and praying for my success. Also, my sincere gratitude goes to all my relatives, family members, and loved ones who have in one way or the other reached out to me throughout my research period.

Finally, I would love to appreciate all my colleagues and friends who have contributed in impacting into my life throughout my masters' study period. You are all indeed special and I say thank you.

As I close my appreciation, I just want to pray that all those who have deposited something positive in my life throughout my research period, will experience unlimited favour of God in all your endeavours. Thank you again!

## TABLE OF CONTENTS

## LIST OF FIGURES

## LIST OF TABLES

## LIST OF APPENDICES

# CHAPTER 1: INTRODUCTION

## 1.1 Preamble

This chapter presents an overall viewpoint of the dissertation. It starts by giving a background information on the subject of cybersecurity as well as establishes how it is linked to human behaviour. More so, the problem statement, research scope, objectives and questions; alongside the significance of the research, coupled with the limitations that were encountered during the research, are all presented in this chapter.

## 1.2 Cybersecurity Behaviours: An Overview

As more of the responsibilities and activities that sums up our daily lives dives into the digital space, in the same way also sophisticated computer grids and information systems drive the globe. These enable simpler and enhanced access to resources ranging from critical frameworks and nationwide security to virtual education and shopping.

Due to the fact that the access to Internet is swiftly escalating across the globe, vis-à-vis the expansion of larger connectedness across individuals, finance, and business, building necessary safeguards against privacy and security will only be of more importance. This actuality therefore makes cybersecurity, as well as other outstanding practices that safeguard personal computers, all digital data and programs from attack to be the major critical problems of our generation.

In as much as security academics, companies and security professionals seek answers, efforts have been comprehensively skewed with regards to the discovery of technological solutions. Nevertheless, there is an estimation by experts that between 70-80% of the cost ascribed to cyber-attacks comes mainly as a result of human error. Simple actions such as opening the wrong email attachment, using a virus-affected Universal Serial Bus (USB) drive or even clicking on a bad link can be of vulnerability to network security. In view of this, it can

be stated that the most-robust security network universally is as good as the human with the right access and virtually secured behaviour.

According to Gratian et al. (2018), it is clearly noted that humans are majorly identified as the most weak link in cybersecurity, due to the fact that many technical security solutions are still liable to failures which occur as a result of mistakes made by humans. It is important to state here that no information is actually secured, in the true sense of it, in today's cyber world and therefore, cyber users should not be angry with the technology but with themselves. Reason is because in the real sense, most of the cyber-attacks humans face today are due to lack of precautionary behaviour and could as well be avoided if adequate precaution is adhered to.

Being informed by the arguments of Egelman et al. (2015), there are still limitations in the domain of cybersecurity human behaviours even though a number of researchers have recognized differences in human behaviours that associate with poor practices of security and augmented susceptibility to be a victim of cyber-crimes such as social engineering or phishing. It is very important to note that a researcher's method of research is influenced by a number of variables such as the age of those being researched, their gender, ethnicity and social class. These variables can be referred to as factors. All these have to be put into consideration when deciding on a method of research.

Furthermore, quantitative dissertations/researches of high quality are able to obviously bring together theory, variables and constructs. In vein of this, constructs can be defined as the foundations of theories, which aids to explain broadly the methods and the reasons for certain phenomena behaviours.

Students' regular exposure to the Internet could result to them being more vulnerable to cyber-threats which some studies (Jeske & van Schaik, 2017; Mohebzada et al., 2012)

have investigated and found them more prone to threats. Hence, the improvement of humans' online behaviour could lead to a better cybersecurity assurance.

It is however important to investigate on the cybersecurity behaviour of tertiary institution students because they are regular users of Internet and have been found to be more vulnerable to Cyber-threats (Mohebzada et al., 2012). Also, they share similar age groups, gender ratio & educational level (Yan et al., 2018) which could help in ensuring normality of the analysis data. Factors of age, gender and educational level, among others have effects on cybersecurity behaviours of individuals. Furthermore, previous studies have found that tertiary institution students with lower age group are more prone to attacks (Ogutcu et al., 2016). It was also discovered that gender has a moderating effect on employees' cybersecurity behaviours (Anwar et al., 2017). More so, it has been discovered that educational level has some moderating effects on the impact of online user's security behaviours (Zhang et al., 2009).

### 1.3 Familiarity with Cyber-threats

Due to the continuous changes in the threat landscape of computer security, lot of new and recent threats are coming to emergence on a regular basis. As a result of this, it is possible for users of the Internet/computer users in general, to get more familiarised with some particular online threats than others. In a means of anticipating to see how the users would respond to security challenges in the future, it is hence of much essentiality to have an understanding of the formation of risk perceptions (Bonneau et al., 2012; Garg & Camp, 2012; Huang et al., 2010). Diverse kinds of threats exists to the information of users, this includes the dispersal of public information via social media platforms, identity theft, viruses, user-surveillance, trojans, key loggers, spyware, and phishing (Flores et al., 2014).

Also, with regards to the case of familiarity with threats among students, some studies have found out that undergraduate students tend to be less familiar with cyber threats (Jeske & van Schaik, 2017). It is also known that familiarity with threat differs based on individual differences (Furnell et al., 2008). Furthermore, it is important to note that familiarity with threats, whether through experience or being exposed directly, has the possibilities of emerging due to the interplay that exists between the technical experience (such as, use of the Internet) of the users, their individual characteristics (for example, attitudes towards the Internet), as well as their everyday behaviours. This happens especially if it is being reinforced via technical or social forms- one of which could be the adopting of precautionary behaviours; which might be attained via social norms or nudges).

Users most times are by default and not intentionally assigned as data security training recipients, however they are not essentially seen as active participants of such training. Such arrangements might make sure that the aim of the training is to raise awareness of threats, and not to really foster specific familiarity with threats by directly getting the users involved.

The current study has carried out investigations on the cybersecurity behaviours of tertiary institutions students based on their perceptions, and found out if age, gender and educational level has any moderating effects on the relationships between the student's familiarity with cyber threats, cybersecurity beliefs and behaviours; hence proposing a cybersecurity behavioural model for students in tertiary institutions. This research also builds its theoretical foundations from a baseline cybersecurity behaviour model proposed by (Anwar et al., 2017). Other theoretical foundations for the study are based on the Health Belief Model by (Becker et al., 1978) and Protection Motivation Theory by (Maddux & Rogers, 1983).

## 1.4 Problem Statement

Cybersecurity threats are rampant everywhere on the Internet (Anwar et al., 2017; Halevi et al., 2016). According to Gratian et al. (2018), despite several technological efforts to combat cyber-attacks, cyber-threats still increases due to end users careless cybersecurity behaviours online, which makes humans the weakest link in cybersecurity.

Tertiary institution students are a very important group of Internet users who use cyber-technologies more frequently than other users due to their explorative nature, however from a general perspective, they don't receive formal cybersecurity training (Bennett & Maton, 2010). Although the current study might not address this directly, however, its result could instigate rooms for more formal means of organizing cybersecurity training for the tertiary institution students. The exposure of students to the Internet could result to them being more vulnerable to cyber-threats which some studies (Jeske & van Schaik, 2017; Mohebzada et al., 2012) have investigated and found them to be highly vulnerable to cyber-threats/attacks and careless with regards to their cybersecurity behaviours. Furthermore, these students share a relative proportion of similar age groups, ratio in gender as well as their levels of education, nevertheless they might differ greatly in their social economic statuses, ethnic diversities as well as their academic/course majors (Yan et al., 2018). Hence the investigation on the cybersecurity behaviours of tertiary institution students so as to understand the various factors that are responsible for their poor cybersecurity behaviours, thereby in a way helping to educate the students to be aware of their behaviours online, as being conducted by this study is of much importance and relevance.

In an investigation by a previous study on the familiarity of students with some common cyber-threats, it was informed that students were not familiar with some of the cyber-threats (Jeske & van Schaik, 2017). However, studies on the relationship between

threat familiarity and cybersecurity behaviours with regards to tertiary institution students is lacking in literature.

Most studies focused on examining the moderating effects of gender, age, and educational level on the relationship between cybersecurity perceptions and behaviours of business employees and other user groups and discovered differences to exist (Anwar et al., 2017; Ogutcu et al., 2016; Zhang et al., 2009). However, not much is known about how this affects students of tertiary institutions. Even the few studies that conducted related research on tertiary institution students only focused on the undergraduate students, hence this made it very vital to also test other groups of students like the postgraduate students.

In view of the aforementioned, the act of this current study's investigation on the moderating effects of gender and other factors like age and educational level on the relationships between cybersecurity beliefs and behaviours of both undergraduate and postgraduate level students in tertiary institutions, is quite interesting.

Additionally, more concentration in literature with regards to cybersecurity behavioural models has been on business organizations workers cybersecurity attitudes with a few on general users (Addae et al., 2017; Al-Mahrouqi et al., 2015; Anwar et al., 2017), with none focusing on tertiary institution students. Thus, there is a lack of suitable cybersecurity model that focuses on the cybersecurity behaviours of tertiary institution students, which is the major outcome of this research. Hence, the current research has given room for more explorations on cybersecurity behaviour among tertiary institutions students.

In response to the above stated gaps, the current study was able to investigate on the cybersecurity behaviours of both undergraduate and postgraduate tertiary institutions students based on their perceptions, and explored as to if age, gender and educational

level has any moderating effects on the relationship between the factors of the cybersecurity behaviours; as well as examined the relationships that exists between the cybersecurity beliefs, familiarity with cyber-threats and the cybersecurity behaviours of the students, which have led to the proposal of a cybersecurity behavioural model for students in tertiary institutions.

Very importantly, the new construct of familiarity with cyber threats (FCT) has been tested and added to enhance the existing model. It is however interesting to note that this construct performed very well. The proposed model could serve as a tool for tertiary institutions researchers who are interested in cybersecurity behavioural studies, and the results of investigation has the possibility of strengthening the existing body of knowledge.

### 1.5 Scope of Research

The research covers a critical review on cybersecurity behavioural studies with regards to human factors. The research's focused population are tertiary institution students. More specifically, the students for this study comprised both undergraduate and postgraduate students. Also, the study was carried out among students from tertiary institutions within Klang Valley in Malaysia.

### 1.6 Research Objectives

The major objective of this research is to empirically investigate the cybersecurity behaviours of tertiary institutions students based on their perceptions, and find out if age, gender and educational level has any moderating effects on the relationships between tertiary institution students' familiarity with cyber threats, cybersecurity beliefs and behaviours, hence proposing a cybersecurity behavioural model for students in tertiary institutions. The following are specific research objectives:

1. To identify factors affecting tertiary institution students' cybersecurity behaviours.
2. To assess the predicting factors of the cybersecurity behaviours of tertiary institution students.
3. To propose a cybersecurity behavioural model for tertiary institution students.

## 1.7 Mapping between Research Objectives and Research Questions

In order to have a clearer representation of the link between the research objectives and questions, Table 1.1 below shows the mapping between research objectives and the respective questions answering each objective.

**Table 1.1:** Research Objective and Research Questions Mapping

| **Research Objectives (RO)** | **Research Questions (RQ)** |
|---|---|
| 1. To identify factors affecting tertiary institution students' cybersecurity behaviours. | 1. What are the factors affecting tertiary institution students' cybersecurity behaviours? |
| 2. To assess the predicting factors of the cybersecurity behaviours of tertiary institution students. | 2. What moderating effects do sociological factors such as age, gender and educational level, have on the factors of the cybersecurity behaviour of tertiary institution students?<br>3. What are the significant predictors of the cybersecurity behaviours of tertiary institution students? |
| 3. To propose a cybersecurity behavioural model for tertiary institution students. | 4. What are the factors of the cybersecurity behavioural model for tertiary institution students? |

## 1.8 Research Significance

This research is significant in the following aspects:

- Contribution to Knowledge: This study contributes by giving a clear exploration as to what extent age, gender and educational level, plays a role in mediating the factors that affect cybersecurity beliefs and behaviours. The added construct of Familiarity with Cyber Threat also gives insight on how Threat Familiarity could relate with Cybersecurity Behaviours of Tertiary Institution Students.
- Contribution to Practitioners: The research model can serve as guide/framework to Tertiary Institution Researcher's that are interested in conducting cybersecurity behavioural studies among the tertiary institutions students.
- Contribution to Participants: The participants of the study (students) were educated about certain security issues via the survey.
- Contribution to Training: The results from the research could instigate the need for group-focused cybersecurity training for Tertiary Institution Students.

## 1.9 Organization of Thesis

The remaining part of this dissertation is organized accordingly thus:

**Chapter Two:** This provides critical and comprehensive review of previously related literature. The major purpose of this chapter is the provision of a solid foundation for the research.

**Chapter Three:** In this chapter, the methods and approaches that have been used in conducting the research, as well as all constructs being used for the model's development are clearly explained step by step.

**Chapter Four:** This chapter presents the analysis and the results of the conducted analysis. All relevant statistical test being conducted are presented here as well. It also gives a clarified interpretation of the analysis results.

**Chapter Five:** This chapter is the final chapter of this dissertation, and it provides a summary of the results, as well as critically discuss some insight into the results. Also, it gives recommendations from the study and propose future works.

# CHAPTER 2: LITERATURE REVIEW

## 2.1 Preamble

A reasonable number of previous studies have carried out research on security behaviours intentions and how it correlates with human traits. Both quantitative and qualitative research have also been carried out on the domain of cybersecurity behaviour intention. Most of the previous research focused on employees in an organization, only few focused on students. This section shall therefore give a summary of related literature with regard to the domain.

## 2.2 The Concept of Cybersecurity with regards to Human Behaviour

What then is cybersecurity actually? And can we say cybersecurity should only be for the technological aspect and not the humans? Who are the users of the 'cyber' space? They are still humans and therefore this makes the involvement of the human very essential in cybersecurity. According to the arguments of (Hadlington, 2018; Von Solms & Van Niekerk, 2013), though a substantial overlap exists between information security and cybersecurity, yet both concepts can't be said to be totally analogous. Cybersecurity therefore shouldn't be necessarily seen alone as the protection of the cyberspace itself, but also the protection of individuals that function in the cyberspace as well as their assets which could be reached via the cyberspace. In view of this, cybersecurity can be defined as the protection of the cyberspace itself, electronic information, the Information Communication and Technologies (ICTs) that gives support to the cyberspace, the cyberspace users in either their national, societal or personal capacity, putting into consideration their interests (whether tangible or intangible), that could be of vulnerability to cyberspace originating attacks.

It is important to note that even though quite a reasonable number of security researchers, companies as well as professionals seek to find answers to cybersecurity issues, unfortunately, their efforts have been comprehensively twisted with regards to technological solutions discoveries (Addae et al., 2017; Gratian et al., 2018). Notwithstanding, experts have estimated that over 70-80% of ascribed expenses of cyber-attacks is usually caused as a result of human error (Kelley, 2018). It is of much interest as well of much surprise to know that simple actions like opening wrong email attachments, use of a virus-attacked pen drive (also known as USB drive) or even deliberately clicking on a known untrusted tempting link can be causes of vulnerability to the security of the network. Having stated this, it could be agreed on that as much as we need very strong robust security networks globally, we also need humans with right attitudes and virtually secured behaviours.

## 2.3 Existing Cybersecurity Behaviour Scales and Models

### 2.3.1 Security Behaviour Scales

Egelman et al. (2015), developed the Security Behaviour Intention Scale (SeBIS) for the purpose of measuring user's security behaviour intentions. Their exploration began with a group of 30 prospective end-user behaviours, which resulted from providers of Internet service, "the United States Computer Readiness and Security Team (US-CERT), industry consortia, and computer security expert feedback". Their final scale gave rise to a sequence of questions which lead to the measurement of 4 security behaviours: password generation, device securement, updating and proactive awareness. The four behaviours identified had their basis on four discrete themes that arose from their questionnaire items as well as gave significant prediction on the variance in the response of users.

Another similar scale to that of the SeBIS scale is the Domain-Specific Risk-Taking (DoSpeRT) scale, that measures a person's self-reported tendency to engross in perilous behaviours across four measurements: health/safety, social, recreational, ethical, and financial (Blais & Weber, 2006).

### 2.3.2 Security Behaviour Models

Apart from security behaviour scales, it is also important to state that previous researchers have developed cybersecurity behaviour models based on some theories. Some even went ahead to study some constructs adapted from both previous theories and models to build their own refined models.

One is the case of Safa et al. (2016) who informed that their study tried to diversify and amplify explorations on information security on one hand, and on the other hand, the sharing of knowledge as an efficient and effectual method to mitigate the threat of information security breaches. They went further to state that Theory of Planned Behaviour (Ifinedo, 2012; Montano & Kasprzyk, 2015), Triandi's model and the Motivation Theory, aided them to conceptualize the model of "Information Security Knowledge Sharing (ISKS)" in organizations.

Another case is that of the major benchmark paper of this proposed research. This research proposes to adopt the constructs derived from the Cybersecurity Behaviour model of (Anwar et al., 2017), which to the best of researcher's knowledge is one of the latest model on Cybersecurity Behaviour.

Anwar et al. (2017) stated that "they adapted their research constructs from the Health Belief Model (Becker et al., 1978) and Protection Motivation Theory (Maddux & Rogers, 1983), Their adopted research constructs were: security self-efficacy (SSE), perceived severity (PS), perceived vulnerability (PV), perceived benefits (PB), computer skills (CS), Internet skills (IS), prior experience with computer security (PE), perceived barriers

(PBR), response efficacy (RE), cues to action (CA), peer behaviour (PBEH), and self-reported cybersecurity behaviour (SRCB)". These constructs were prone to statistical analytics via gender factors and overall score was good enough to deem the model fit. The model was then called Cybersecurity Behaviour Model.

### 2.4 Cybersecurity & Human Behaviours

Some researchers have carried out studies on the correlation between human traits and cybersecurity, some carried out exploratory studies on factors in end user security, cultural & psychological factors, gender difference and employee cybersecurity, risk perceptions of cybersecurity and precautionary behaviours, analysis of personal information security and gender difference and employee cybersecurity behaviour among many others. Some of these related works are summarized in this section of literature review.

#### 2.4.1 Cybersecurity Behaviours among General Internet Users

Some researchers focused on correlating human characteristics with the intentions of cybersecurity behaviour, thereby presenting a wide-ranging study that examines how some factors such as: decision-making styles, personality traits, demographics and risk-taking preferences impact the security behaviour intentions of password generation, updating, proactive awareness, and device securement (Egelman et al., 2015; Gratian et al. (2018)).

Rajivan et al. (2017), identified four factors that constitute security expertise in end users to be: basic computer skills, advanced computer skills, security knowledge and advanced security skills. Furthermore, Halevi et al. (2016), explored the relationship between cyber-security and cultural, personality and demographic variables. They found out that culture was a predictor of privacy attitude, but only had low effect on behaviour.

Recent studies like that of (Coffey, 2017; Noureddine et al., 2017) tried to address and present interactions between humans and technology, thereby stating that the humans could be the major causes of cybersecurity threats that befalls them and also that they could as well be the right solutions to those problems if the human error is identified and corrected.

Furthermore, Coffey's study addressed the roles of individual errors that makes them open to vulnerabilities on the Internet and also tried to give the importance of training as well as technology which could in one way or the other protect both the systems and the system users in extension. Studies related to cybersecurity behaviours have been on research for some years now, Far back in 2005, an investigation was conducted to analyse security behaviours of end users through a survey of 1167 US end users in respect of their behaviours towards password management (Stanton et al., 2005). Their results showed that only few of the categories of the survey kept good password management, but a bulk of them had poor password security management. Well even though this is more related to Information security, it is as well correlated to cybersecurity.

Closely related to this study was a recent study by (Öğütçü et al., 2016), whose focus was to investigate on Information System Users dangerous behaviours based on the scales of Conservative Behaviour, Risky Behaviour, Risk Perception, and Exposure to Offence in order to discover which of these behaviours actually poses a threat to information security and cybersecurity in extension. Their results showed that all of these scales had significant differences. Other studies carried out to assess the perceptions of personal and organizational Internet users with regards to their security revealed that many of the users investigated upon had quite a high level of confidence of being aware of cyber threats and have tried to use many relevant ways to safeguard/protect themselves, yet there are still many areas lacking which could be related to their behaviours of novice users on the

Internet and role of social engineering scams (Furnell et al., 2007; Kearney & Kruger, 2016).

Coming from another school of thought, a study by (Dodel & Mesch, 2017) investigated the determinants of cyber-safety behaviours, placing more focus on the factors linked with the use of antivirus software by the general cyber users population. Findings from their study showed that some of the basic determinants of antivirus preventive behaviours are: Internet frequent use, seniority online, age, education and gender. Though this research findings could be a form of signalling the necessity for future research using the Health Belief Model (HBM) as the foundation for understanding cyber-safety, however, there was no clarity on the role of previous victimization incidents.

Common limitations from the above studies with regards to cybersecurity behaviours among the general Internet users are: the lack of specific target group, no specific design interventions and more focus on victimization episodes. The current research however has tried to solve some of this issues like examining the cybersecurity behaviours of university students in particular with specific design interventions. Also, the current study did not only focus on the victimization parts of not being cyber-secured but general cybersecurity behaviour perspectives.

### 2.4.2 Cybersecurity Behaviours among Business Organizational Workers

A recent investigation was carried out specifically on the difference between gender and cybersecurity behaviours of employees in a business organization (Anwar et al., 2017); this study found that gender had some effect in some of the psychosocial constructs used (prior experience, computer skills, security self-efficacy) and little effect in others like cues to action and self-reported cybersecurity behaviours. Other studies that were carried out to assess the perceptions of personal and organizational Internet users with regards to their security, revealed that many of the users investigated upon had quite a

high level of confidence of being aware of cyber threats and have tried to use many relevant ways to safeguard/protect themselves; yet there are still many areas lacking which could be related to their behaviours of novice users on the Internet and role of social engineering scams (Furnell et al., 2007; Kearney & Kruger, 2016).

A study was conducted with regards to this consideration by exploring the association that existed between impulsivity, addiction to the Internet, attitudes towards cybersecurity in a business environment, as well as cybersecurity behaviours that are risky (Lee Hadlington, 2017). From the results achieved from the study, it was discovered that the attitude of employees towards cybersecurity had negative correlation to the frequency of their engagements in risky cybersecurity behaviours. However, it is important to note that despite the employing of the state-of-the-art technical controls, breaches in security are still experienced by organizations, which calls for the importance of awareness in cybersecurity issues. In view of this, a recent research was conducted by (McCormac et al., 2017) to examine the link between the information security awareness of individuals and their difference variables, such as gender, age, propensity to take risk and personality. The outcomes of this investigation found out that variance in individuals' information security awareness were significantly explained via factors such as: conscientiousness, emotional stability, propensity to take risk and agreeableness. Implementing ways of preventing as well as mitigating cybersecurity risks is of much importance, however the behavioural science plays a most important role in the stages of both developing and designing as well as the maintenance of web systems (Padayachee, 2012).

As much as it is important to study about the cybersecurity behaviours and attitudes of organizational staff, which most researchers in the cybersecurity behavioural domain focus on more, it is also of much importance to carry out similar studies on other facets of Internet users in the society such as university students. However, some common limitations/critiques from the previous studies include: the recommendation of larger

datasets, and more factors should be tested on, which in the current research, have introduced a new construct of the Familiarity with Cyber-Threats.

### 2.4.3 Cybersecurity Behaviours among Tertiary Institutions Community

Coming to a most recent study whereby human traits were correlated with cybersecurity behaviour intents, in a way of validating and expanding Egelman and Peers work (Egelman et al., 2015), the authors presented a comprehensive study that investigated on how demographics, decision making styles, personality traits and risk taking preferences could influence security behaviours of password generation, updating, device securement and proactive awareness (Gratian et al., 2018). However, this study focused on higher education, more specifically the participants were chosen from a large public university in the USA. The authors however mentioned that one major reason why they decided to use the university community was due to reasons being that universities have been victims of diverse phishing attacks of high profiles. Hence, they further stated that the study was conducted to unveil a better understanding of university population's security behaviours and to help in improving overall university security. From the study it was revealed that gender, financial risk-taking, extraversion and rational decision making had positive significant correlations with good security behaviours. However, this study didn't focus on a particular group in the university but rather was conducted on total university population.

Furthermore, another study was conducted in the UAE to investigate on how the university community can engage in a phishing experiment (Mohebzada et al., 2012). Phishing is a way of mimicking a fake copy of a known website but with the aim of breaching the intended victim's privacy and confidentiality. In this study, findings indicated that students were more vulnerable to be attacked with regards to the phishing attacks when compared to the faculty or staff. This could however in one way show that

experience might be a victimization factor for a person in course of a cyber-attack. Also, from their study, no strong association existed between the demographic information of individuals with respect to phishing's susceptibility, hence giving room for more analysis on more focused group like the students to see if results might differ.

A more recent work still carried out on university community on the prediction of threat detection from human behaviours still used the approach of a phishing experiment to test the level of cybersecurity behaviour and knowledge of the participants, but this time around made use of an after-experiment survey (Kelley et al., 2018). From this study, it was observed that knowledge of security had a systematic relationship with correct recognition of the websites, however it didn't relate with other variables used by the researchers. It was also known that the fake websites were very difficult to correctly recognize with only 49% of the university participants being able to identify the fake websites. This shows that there is still lack of cybersecurity assurance among the university community, however studying on their security behaviours and attitudes could give much insights.

From the studies above, common limitations that existed were: lack of much factors being investigated on specific groups of people, the lack of demographic factors being used to predict cybersecurity behaviours, better measures of reliability and validity for the studies, since most of them conducted just phishing experiments rather than focusing on other cybersecurity behaviour constructs.

### 2.4.4 Cybersecurity Behaviours among Tertiary Institution Students

A recent study conducted on how undergraduate students make cybersecurity judgment with specific aim of identifying the weakest links of the weakest link found out that about 65% of the college students gave a correct cybersecurity judgement which shows a high level of cybersecurity knowledge (Yan et al., 2018), however there were

also indications that no significant differences were found between the rational and intuitive conditions with respect to controlled years of study of the students, their majors of study and gender. This gives a suggestion that the rational judgment competency of students might be one of the weakest links in the protection of cybersecurity. However, a previous study, such as that of Yan et al. (2018) only focused on undergraduate students and did not test on other levels of students like postgraduate, pre-degree and others, which this proposed research included in its investigation. More so, a number of researchers have recommended the expansion of cybersecurity behavioural studies to the wider scope of higher education students, not just focusing on a particular group (Gratian et al., 2018; Mohebzada et al., 2012). In Egelman et al. (2015) work, a comprehensive study that investigated on how demographics, decision making styles, personality traits and risk taking preferences could influence security behaviours of password generation, updating, device securement and proactive awareness, was conducted. This asserts the importance of testing out demographics of the students, of which level of education is one, hence grouping the students into different levels of education such as undergraduates and postgraduates would result to more distinct inferences and expositions about the cybersecurity behaviours of tertiary institution students, rather than just focusing on the undergraduate students (Wang, 2013).

Furthermore, an investigation was conducted with the aim of finding how familiar university students were with Internet threats through a quantitative approach (Jeske & van Schaik, 2017). From this study it was discovered that the university students were not very familiar with the four specific threats used in the experiment which are: zero-day attacks, botnets, key loggers, and rogue ware. This shows that a clear need for cybersecurity training as well as campaigns of awareness for university is of much importance. However, it was also discovered that the experts, like cybersecurity staff were likely used to security features than other university participants in the study. Also gender

and status of employment proved to be significantly correlated to the level of threat familiarity. This gives a suggestion that testing the gender differences of university students with regards to cybersecurity behaviours could give interesting explorations.

Additionally, yet another study was conducted to find out if Media Multitasking (means using different online media technology) frequency has any linking with higher levels of risky cybersecurity behaviours of university students (Lee Hadlington & Murphy, 2018). The study employed a quantitative approach through the use of online surveys, also with a focus group of undergraduate students as previous studies. Results from the study indicated that students who engaged in frequent media multitasking reported to have had cognitive failures and had a higher frequency of being more vulnerable to cybersecurity attacks and behaved more risky on the Internet.

From the above studies, common limitations/critiques are: More behavioural tests can be conducted, different dataset is needed and improved design, only undergraduate (bachelor) students were investigated in most of the reviewed studies. Hence, the current research has been able to fill this gap by investigating on the general student group comprising of all levels of education.

From the review of literature so far, it can be said that research in this domain have a large scope but is still limited. Most of the previous works have focused more on organizations and employees, some others focused just on the general users, however not much have tried to investigate on tertiary institution student's cybersecurity behaviours. This is why the current proposed research seeks to perform an empirical study to investigate the impact of self-reported cybersecurity behaviours on tertiary institution students in particular based on multiple factors and constructs, hence proposing a model. This research builds on the work of (Anwar et al., 2017) with a larger scope, with different target group and in a different environment. Also, this proposed research expands and

validate the existing cybersecurity model, as it makes use of its constructs, coupled with an additional construct of familiarity with cyber-threats, for critical investigations.

### 2.5 Familiarity with Cyber-Threats

Some scholars have examined attitudinal roles in regards to the Internet, coupled with hiding of information versus the sharing of information (Acquisti & Grossklags, 2004). Correspondingly, user's precautionary behaviour, like the usage of the security features of a computer, also needs a specific awareness as well as familiarity of threats that is being faced by the user (Dinev et al., 2009; Kruger et al., 2010). In this research, familiarity is differentiated from awareness, this is because to be aware of an issue does not really gives an indication more than just attaining a certain level of knowledge that a particular type of threat exists.

Awareness on its own might be subjected to a continuous exposure, and hence might be subjected to an habitual condition, which could eventually lead to reduced attention that is being given to warning (Anderson et al., 2016). This nevertheless doesn't ascertain the knowledgeability or familiarity of the user with the entailment of such threat, leaving them to just recognize the threat. However, on the other hand, familiarity can be linked to knowledge in more complex ways, such that knowledge is viewed as the ability to know something via one's experience or by associating, hence implying a comprehension of a certain threat. Due to this, it would be in place to state that the precursor of familiarity might be awareness.

To best of the knowledge of the researcher, no study have investigated on the relationship between familiarity with threats and cybersecurity behaviours, however there's a similar study which investigated on the familiarity with Internet threats and how this goes beyond just awareness of the threats (Jeske & van Schaik, 2017). In this study, the researcher conducted a cross-sectional survey, which led to the collection of data from

323 participants, who were students. The survey was focused on finding out how familiar the students were with sixteen (16) various threats on the Internet. Furthermore, the researchers presented the participants with detailed definition of the threats, and then requested them to state their level of familiarity with each of the threats. The responses gathered from the students were hence made use of in identifying the degree of which familiarity of threat varied amongst the sample.

The researchers were able to identify three diverse clusters. The first group were labelled as experts- because they had relative knowledge of all the threats; the second group showed themselves to be more familiar only with threats that were well known; while the third group were familiar the more with new threats. Insights from their results showed that the experts' group participants had more likelihood of engaging in computer security behaviours than their counterparts in other clusters. They were also able to provide evidences as to the fact that familiarity is a mediator between the use of Internet and security behaviours, although this could call for a future reflection.

In the current research, familiarity with cyber-threat was first used to determine the level of familiarity the students had with cyber-threats, and to find the relationship between familiarity with cyber-threats and cybersecurity behaviours, coupled with the cybersecurity beliefs constructs. This is still a very prime research area which could be investigated more on in the future.

**2.6 Theoretical Framework**

This section shall discuss the theoretical framework on which this research model is based on. The theoretical foundations are based on two founding and major theories used in the behavioural studies which is widely used by security studies as well. The theories are Health Belief Model by (Becker et al., 1978) and Protection Motivation Theory by (Maddux & Rogers, 1983). The motivation for the intended model was gotten based on a

similar cybersecurity model by Anwar et al. (2017), however his model was developed based on employees cybersecurity behaviours. Hence, the current research adapted the constructs obtained from this baseline theories, and they are discussed specifically in section 2.7.

### 2.6.1 Brief Definitions of Foundational Theories and Model

#### 2.6.1.1 Protection Motivation Theory

This theory has been used majorly for explaining the intentions of users to employ security technologies, as well as the means and time a user can adopt either adaptive or maladaptive behaviours when being informed of a threatening security incident. The founding author of the theory was Maddux and Rogers (1983) and the constructs derived from the theory are: Perceived Susceptibility, Perceived Severity, Security Self-Efficacy, Response Efficacy, Computer Skills, Internet Skills, Prior Experience to Security, Perceived vulnerability, and Information-seeking skills.

#### 2.6.1.2 Health Belief Model

The health belief model was developed by Becker et al. (1978). This is a conceptual model that was developed to explain the reason behind the non-participation of people in health behaviours. This is actually the base of the protection motivation theory. It is important to note that the Protection Motivation Theory was reworked from this model. Constructs derived from this model are: Perceived Susceptibility, Perceived Severity, Perceived Benefits, Perceived Barriers, Cues to Action, and Self Efficacy.

### 2.6.2 Existing Cybersecurity Behaviour Model

The most recent and quite related cybersecurity model with regards to the concept of this research is that of Anwar et al. (2017). This model was developed as a result of a

study which used gender as a moderating factor to test existing relationships on cybersecurity behaviours of employees. This model made use of the above discussed two theories and adapted their constructs. After the final model of the researcher, the modified constructs were: Perceived Vulnerability, Perceived Severity, Security Self-efficacy, Perceived Barriers, Perceived Benefits, Response Efficacy, Cues to Action, Peer Behaviour, Computer Skills, Internet Skills, Self-reported cybersecurity behaviour and Prior Experience with computer security practices. However, this model was developed based on the gender differences in the cybersecurity behaviours of employees, which gives more room for more exploration to be made in other areas and with different group of respondents. The current study made use of this recent model as a benchmark. Reason is because the constructs modified by the author are closely related to the nature of the proposed study. Also, the constructs have been further redefined to suit the cybersecurity context by previous author. However, the existent model has also been enhanced through the inclusion of an additional construct, Familiarity with Cyber-threats, which was used to address the level of tertiary institution student's familiarity with some cyber-threats. This construct was selected because in some other studies that have investigated on the familiarity of users with online threats (Garg & Camp, 2012; Jeske & van Schaik, 2017; Suleman et al., 2017), it was found out that the level of familiarity with threat was an important factor for cybersecurity behaviours.

## 2.7 Summary

This chapter has presented a critical review of cybersecurity behavioural studies. It has also been discovered from literature that though, a number of researchers have carried out investigations of cybersecurity behaviour on different group of users, such as general Internet users (Egelman & Peer, 2015; Gratian et al., 2018), business organization workers (Anwar et al., 2017; Lee Hadlington, 2017), tertiary institution community

(Kelley, 2018; Mohebzada et al., 2012), however, there is a lack of research with regards to the cybersecurity behaviours among tertiary institution students, studies that even conducted related investigations on them (Jeske & van Schaik, 2017; Yan et al., 2018), only focused on undergraduate students and investigated on their cybersecurity intentions and not perceptions as this current study did. Also, to the best of the researcher's knowledge, no previous study has been able to incorporate the relationship between familiarity with cyber-threat and the cybersecurity behaviours of tertiary institution students into the cybersecurity behavioural model.

# CHAPTER 3: RESEARCH METHODOLOGY

## 3.1 Preamble

This segment shall discuss the procedures/methods that have been employed in this research. It will also explain how the researcher went about the research. Specifically, the research approach, subjects (participants), measurements, data-collection and analysis methods shall be discussed also.

## 3.2 Research Approach

This research employed a quantitative approach in carrying out investigations, gathering of data as well as analyzing the collected data. This is basically due to the fact that the research focused on investigating the cybersecurity behaviours of students in the tertiary institutions across quite an extensive area in the metropolis of Malaysia, which is Klang Valley. Hence, the best way suitable for easier and effective way of gathering data was via a quantitative method, by administering surveys to the diverse institutions.

## 3.3 Subjects/Participants for study

Knowing well that this is an empirical research which included the conduct of investigations, there was therefore an obvious need for participants to investigate on. The current research investigated on the students of tertiary institutions (such as universities, colleges, and other higher educational institutions), within Klang Valley, Malaysia. The category of students involved in this research are undergraduate and postgraduate students who were actively studying in those institutions. They are the target focus and a survey-based investigation has been carried out on them, to find out about their behaviours/attitudes towards cybersecurity. Regarding the number of participants who contributed to the study, generally according to literature and the generally accepted rule

for surveys, 5% of margin error, 95% of confidence level and 20% of response rate of the intended population is accepted (McCall, 1982).

### 3.4 Measurements

The most appropriate/suitable instrument that can be used in an empirical survey investigation is the use of questionnaires to help in evaluating user's response based on appropriate constructs. The proposed research therefore adopted the survey instrument used by related previous studies (Anwar et al., 2017; Jeske & van Schaik, 2017) for data collection. This instrument has been validated already by the previous studies from which they were adapted, therefore it was deemed fit as a valid tool for the current research. In order to apply directly and more specifically to the current research setting, some of the questionnaire items were duly modified. The constructs that were used were also adapted from previous literature based on the health Belief Model (Becker et al., 1978) and the Protection Motivation Theory (Maddux & Rogers, 1983), as explained earlier in chapter two. The moderating variables that were used in this research consist of student's details such as: age, gender, and education level. Specifically, the constructs used in this research are: Cybersecurity Behaviour (CSB) which also serves as the Dependent Variable (DV), while the construct for the Independent Variables (IVs) are: Perceived Vulnerability (PV), Perceived Severity (PS), Security Self-Efficacy (SSE), Perceived Barriers (PB), Response Efficacy (RE), Cues to Action (CA), Peer Behaviour (PBhv), Computer Skills (CS), Internet Skills (IS), Prior Experience with Computer Security Practices (PE), Perceived Benefits (PB), and a newly added construct of Familiarity with Cyber-Threats (FCT). Each of the measures are being explained clearly in the following sections.

#### 3.4.1 Perceived Vulnerability

The Perceived Vulnerability scale was used in measuring the students' belief on their risk to cyber-threats. This scale contained 8 items and they were measured on a 5-likert

reversed- response scale, ranging from Strongly Disagree-1, Disagree-2, Neutral-3, Agree-4, and Strongly Agree-5. In order to ensure that the items attained a quite reasonable level of reliability, a reliability analysis was conducted, and the Cronbach alpha coefficient obtained was: 0.744, which shows a very good level of reliability.

### 3.4.2 Perceived Severity

The Perceived Severity scale was used in measuring the student's perceptions on the consequences of how they take risky cybersecurity behaviours seriously. This scale contained 4 items and they were measured on a 5-likert reversed-response scale, ranging from Strongly Disagree-1, Disagree-2, Neutral-3, Agree-4, and Strongly Agree-5. In order to ensure that the items attained a quite reasonable level of reliability, a reliability analysis was conducted, and the Cronbach alpha coefficient obtained was: 0.756, which shows a very good level of reliability.

### 3.4.3 Security Self-Efficacy

The Security Self-Efficacy scale was used in measuring the student's confidence level of handling cyber-threats issues. This scale contained 6 items and they were measured on a 5-likert reversed-response scale, ranging from Not at all-1, No I don't-2, Not Sure-3, Yes, I do-4, and Very Sure-5. In order to ensure that the items attained a quite reasonable level of reliability, a reliability analysis was conducted, and the Cronbach alpha coefficient obtained was: 0.882, which shows a high level of reliability.

### 3.4.4 Perceived Barriers

The Perceived Barriers scale was used in measuring the student's inconveniency levels in checking for cybersecurity issues. This scale contained 4 items and they were measured on a 5-likert reversed-response scale, ranging from Strongly Disagree-1, Disagree-2, Neutral-3, Agree-4, and Strongly Agree-5. In order to ensure that the items attained a

quite reasonable level of reliability, a reliability analysis was conducted, and the Cronbach alpha coefficient obtained was: 0.566, which shows an acceptable level of reliability.

### 3.4.5 Response Efficacy

The Response Efficacy scale was used in measuring the response level of the students in regard to the cybersecurity policies adherence. This scale contained 4 items and they were measured on a 5-likert reversed-response scale, ranging from Strongly Disagree-1, Disagree-2, Neutral-3, Agree-4, and Strongly Agree-5. In order to ensure that the items attained a quite reasonable level of reliability, a reliability analysis was conducted, and the Cronbach alpha coefficient obtained was: 0.834, which shows a high level of reliability.

### 3.4.6 Cues to Action

The Cues to Action scale was used in measuring the level of promoting good cybersecurity behaviour in an organization. This scale contained 4 items and they were measured on a 5-likert reversed-response scale, ranging from Never-1, Rarely-2, Sometimes-3, Often-4, and Always-5. In order to ensure that the items attained a quite reasonable level of reliability, a reliability analysis was conducted, and the Cronbach alpha coefficient obtained was: 0.857, which shows a high level of reliability.

### 3.4.7 Peer Behaviour

The Peer behaviour scale was used in measuring the level of the students' belief about their friend's security behaviour. This scale contained 4 items and they were measured on a 5-likert reversed-response scale, ranging from Strongly Disagree-1, Disagree-2, Neutral-3, Agree-4, and Strongly Agree-5. In order to ensure that the items attained a

quite reasonable level of reliability, a reliability analysis was conducted, and the Cronbach alpha coefficient obtained was: 0.763, which shows a good level of reliability.

### 3.4.8 Computer Skills

The Computer Skills scale was used in measuring the basic computer competency level of the students. This scale contained 4 items and they were measured on a 5-likert reversed-response scale, ranging from Very Uncomfortable-1, Uncomfortable-2, Neutral-3, Comfortable-4, and Very Comfortable-5. In order to ensure that the items attained a quite reasonable level of reliability, a reliability analysis was conducted, and the Cronbach alpha coefficient obtained was: 0.852, which shows a high level of reliability.

### 3.4.9 Internet Skills

The Internet Skills scale was used in measuring the competency level of the students with the Internet. This scale contained 7 items and they were measured on a 5-likert reversed-response scale, ranging from Very Uncomfortable-1, Uncomfortable-2, Neutral-3, Comfortable-4, and Very Comfortable-5. In order to ensure that the items attained a quite reasonable level of reliability, a reliability analysis was conducted, and the Cronbach alpha coefficient obtained was: 0.876, which shows a high level of reliability.

### 3.4.10 Prior Experience with Computer Security Practices

The Prior Experience with Computer Security Practices scale was used in measuring the experience level of the students with regards to good cybersecurity practices. This scale contained 6 items and they were measured on a 5-likert reversed-response scale, ranging from Strongly Disagree-1, Disagree-2, Neutral-3, Agree-4, and Strongly Agree-5. In order to ensure that the items attained a quite reasonable level of reliability, a reliability analysis was conducted, and the Cronbach alpha coefficient obtained was: 0.760, which shows a good level of reliability.

### 3.4.11 Perceived Benefits

The Perceived Benefits scale was used in measuring the perception of the students with regards to the benefits of good cybersecurity practices. This scale contained 6 items and they were measured on a 5-likert reversed-response scale, ranging from Strongly Disagree-1, Disagree-2, Neutral-3, Agree-4, and Strongly Agree-5. In order to ensure that the items attained a quite reasonable level of reliability, a reliability analysis was conducted, and the Cronbach alpha coefficient obtained was: 0.822, which shows a high level of reliability.

### 3.4.12 Familiarity with Cyber-Threat

The Familiarity with Cyber-Threat scale was used in measuring the students' level of familiarity of some defined cyber-threats. This scale contained 13 items and they were measured on a 5-likert reversed-response scale, ranging from Fully Unfamiliar-1, Unfamiliar-2, Neutral-3, Familiar-4, and Fully Familiar-5. In order to ensure that the items attained a quite reasonable level of reliability, a reliability analysis was conducted, and the Cronbach alpha coefficient obtained was: 0.940, which shows a very high level of reliability.

### 3.4.13 Cybersecurity Behaviour

The Cybersecurity Behaviour scale was used in measuring the actual cybersecurity behaviour of the students. This scale contained 13 items and they were measured on a 5-likert reversed-response scale, ranging from Never-1, Rarely-2, Sometimes-3, Often-4, and Always-5. In order to ensure that the items attained a quite reasonable level of reliability, a reliability analysis was conducted, and the Cronbach alpha coefficient obtained was: 0.709, which shows a good level of reliability.

### 3.5 Sampling

Obviously, it is impractically impossible to carry out an investigation on an entire population, especially in the case of the current research which employed a quantitative approach via use of questionnaire surveys. Thus, there is a need to sample the population. Sampling can be referred to as an approach which gives researchers a chance in inferring information regarding a population on the basis of the results from the population's subset, thus not needing to conduct investigation on each individual in that population. There are basically two categories of sampling, which are probability and non-probability sampling, with diverse specific types. This research employed a simple-random sampling method, which is one of the types of the probability sampling. Simple random sampling is a kind of sampling that gives an equal chance, or probability to every member of the intended population to be selected for participation in the study (Patten & Newhart, 2017).

Regarding the sample size calculation, generally according to literature and the generally accepted rule for surveys, 5% of margin error, 95% of confidence level and 20% of response rate of the intended population is accepted (McCall, 1982). In view of this, since the students were from different random institutions, and their exact population size couldn't be achieved, the researcher made use of an online sample size calculator (Qualtrics, 2019) to determine the required number of respondents by inputting about 1million as the population size. From the calculation, it was discovered that at least 385 respondents were needed as participants for the study. However, the researcher was able to attain up to 450 respondents from the data collection exercise.

### 3.6 Validation of Instruments

Validation involves collecting and analysing data to access the accuracy of an instrument. In this research data was collected appropriately and were analysed by

performing well conducted statistical tests as mentioned earlier. The research hypothesis has been tested and validated to provide inferences.

Thus, the validity of the quantitative instrument initially passed through pilot testing by some experts just to find out about the simplicity and understanding of the items in order to ensure reliability and validity of the instrument before final collections. However, since the tool is not totally a new one, and has been validated by previous scholars, there was no need for a proper pilot study analysis.

With regards to the validation of the instrument by experts, at the initial stages of the survey development, the researcher ensured that the supervisory committee set up by the faculty carried out critical investigations on the survey questionnaire items, hence checking if they were suitable for the intended population. Also, grammar checks as well as inconsistency checking were carried out by some Ph.D. experts in the field of computer science, before finally publishing the survey online.

### 3.7 Data Collection Method

The period of data collection spanned for about three months, within January to March 2019. This was so because the survey was administered via an online means, hence the researcher had no direct contact with the respondents.

This research employed the use of online survey to collect data. The online survey was sent to tertiary institution students within Klang valley via means such as institution mailing systems, institution's Facebook pages, students WhatsApp and Facebook discussion forums, among others. The online survey was designed using google forms, coded in a way that a respondent can attempt one survey, only after inputting their email address in order to avoid the problem of inconsistencies and double responses by one participant, and these were shared via secured URL links. Nevertheless, despite such

restrictions, few issues of double responses were noticed and removed during the data cleaning process.

The gathered data was monitored by the researcher directly in order to avoid compromise of data. Since the researcher made use of google forms to distribute the data and this platform is a secured one provided by google. Thus, the data were monitored, and responses were able to be tracked and gathered from the spreadsheet provided by google forms.

At the end of the data gathering period, a total of 450 responses were harvested and subjected to a data cleaning process. However, despite all the initially placed constraints in order to avoid inconsistencies, 15 of the collected data were either incomplete or doubly responded. Thus, the researcher removed those data out of the final data used for analysis, hence leaving only 435 responses that were eventually used for final data analysis.

### 3.8 Data Analysis and Interpretation

A quantitative approach was utilized for the analysing of the collected data in this research. Hence the gathered data were analysed using statistical procedures, which involved a combination of both descriptive and inferential statistics, in order to have clearer understanding of the data and to make conclusions.

The tool used in analysis of the data is Statistical Package for Social Sciences (SPSS) version 25.

The SPSS package was used for analysing both descriptive statistics and inferential statistics. Analysed data and results gotten via the SPSS tests were interpreted by the researcher. Descriptive statistics was conducted to understand the nature of the overall data. Tests such as frequency, percentages, mean, standard deviation and uses of chart were utilized for clearer data description on the participants demographics. While all

major objectives and questions of the research were answered via the conduct of inferential statistics.

The first research question was analysed via Spearman's Rho Correlation test. Furthermore, the second question was answered through a Biserial Point Correlations Analysis, using the Spearman's Rho and One-Way ANOVA. The Biserial Point Correlation (BPC) Analysis was first conducted to find the differences/relationships between the moderating factors and the IVs and DVs. Then, in other to investigate more deeply into the factors that have a moderating effect from results of the BPC analysis, a One-Way ANOVA was also conducted. The third research question was answered via the conduct of a Multiple Regression Analysis; through the Multiple Regression Analysis, independent variables of the research were tested on the Dependent variable to find out how each IV predicts the DV and to identify the most influencing IVs according to hierarchy, which produced the final factors for the proposed model in the final research question. In order to find the significant predictors of the Cybersecurity Behaviours of Tertiary Institution Students, a Multiple Regression Analysis was conducted via SPSS. Multiple regression in general, is used in explaining what relationship exists between numerous predictor variables, also known as independent variables, and one criterion or dependent variable; it is a statistical technique that is widely used in the behavioural science (Cohen et al., 2014). It examines the influence of one or more independent variable on the dependent variable. It is important to state that the evaluation of the proposed model was achieved via the following metrics: Normality Test, Reliability Test and Hypothesis Testing. The proposed model passed through a Normality Test to see if all the data were normalized, reliability test also ensured that all the constructs of the model had a good Cronbach alpha, and the hypothesis were the last to be tested so as to make final modifications to the model by either accepting (+) or rejecting (-) the postulated hypothesis and coming up with the final inferences.

### 3.8.1 Age Distribution

With regards to the age distribution, the students were requested to choose their ages from four categories given as thus: “17-20”; “21-30”; “31-40”; and “Above 40”. When the data was coded into SPSS, those in age range of “17-20” were assigned a value of 1, while those in range of “21-30” were coded with a value of 2, followed by the range of “31-40” coded as 3, and finally the group of “Above 40” were coded as 4.

### 3.8.2 Gender Distribution

With regards to the gender distribution, the students were requested to choose their gender from two categories given as thus: Female or Male. When the data was computed in SPSS, females were coded with a value of 0, while male entries were coded as 1.

### 3.8.3 Educational Level Distribution

With regards to the educational level distribution, the students were requested to choose their level of education from three categories given as thus: Bachelor, Masters, and PHD. When the data was computed in SPSS, Bachelor Students were coded with a value of 1, followed by master’s Students coded as 2, while the PHD students were coded as 3.

### 3.8.4 Rate of Internet Usage per Day Distribution

As part of gathering demographic data, the students were asked to rate their Internet usage per day: that is how often they make use of the Internet on a daily basis. This was measured in terms of time duration. Three categories were provided for the students to choose from, which included and was coded in the SPSS program thus: “1- Less than 1 hour”; 2- “2-5 hours”; 3- “More than 6 hours”.

### 3.8.5 Distribution on the Level of Internet Expertise

In a means of trying to establish the level of Internet expertise of the students, a part of the demographic details required the students to give rate their level with regards to their expertise of the Internet. The variable was based on three categories, given thus: Beginner, Intermediate, and Expert. These variables were coded in SPSS as thus: 1- Beginner, 2- Intermediate, 3- Expert.

### 3.8.6 Distribution on their Social Media Usage

Finally, with regards to the descriptive analysis, demographic data was gathered from the students regarding the rate of their social media usage. The students were prompted to choose from a category of three social media platforms, the one they frequently use on a daily basis. The categories are thus: None-coded as 1 in SPSS, Only WhatsApp- coded as 2 in SPSS, Facebook and WhatsApp- coded as 3 in SPSS.

## 3.9 Definitions of Cybersecurity Behavioural Constructs

The constructs that have been adapted for this research which also have been used by previous researchers are being defined briefly in this section. They have been put together in table 3.1 below:

**Table 3.1:** Cybersecurity Behavioural Constructs Definitions

| CONSTRUCT | DEFINITION IN TERMS OF CYBERSECURITY | REFERENCES |
|---|---|---|
| Perceived Vulnerability | Used to measure user's belief on their risk to cyber threat. | (Ifinedo, 2012; Mohamed & Ahmad, 2012; Ng et al., 2009) |
| Perceived Severity | Used to measure user's perceptions on consequences of risky cybersecurity behaviours serious. | (Ifinedo, 2012; Mohamed & Ahmad, 2012; Ng et al., 2009; Ng & Xu, 2007) |
| Security Self-efficacy | Used to measure the confidence level of handling cyber-threats issues. | (Ifinedo, 2014; Ng et al., 2009; Rhee et al., 2009) |
| Perceived Barriers | Used to measure inconvenience levels in | (Ng et al., 2009) |

| | | |
|---|---|---|
| | checking for cybersecurity issues. | |
| Response Efficacy | Used to measure response level with regards to cybersecurity policies adherence. | (Vance et al., 2012) |
| Cues to Action | Used to measure the level of promoting good cybersecurity behaviour in an organization. | (Ng et al., 2009) |
| Peer Behaviour | Used to measure level of user's belief about their friend's security behaviour. | (Anderson & Agarwal, 2006; Chan et al., 2005; Herath & Rao, 2009) |
| Computer Skills | Used to measure the basic computer competency level of a user. | (Schulenberg et al., 2006) |
| Internet Skills | Used to measure competency level of a user with the Internet. | (Schulenberg et al., 2006; Smith, 2006) |
| Prior Experience with computer security practices | Used to measure experience level of a user with regards to good cybersecurity practices. | (Aytes & Connolly, 2005; Ng et al., 2009) |
| Perceived Benefits | Used to measure the perception of a user with regards to benefits of good cybersecurity practices. | (Ng et al., 2009) |
| Cybersecurity behaviour | Use to measure actual cybersecurity behaviours of users. | (Davinson & Sillence, 2010; Ng et al., 2009; Shih et al., 2008; Vance et al., 2012) |
| Familiarity with Cyber-Threats (**New)** | Used to measure the users' level of familiarity of some defined common cyber-threats. | (Garg & Camp, 2012; Jeske & van Schaik, 2017; Suleman et al., 2017) |

### 3.10 Research Hypothesis

Since this research was statistically conducted, it was hinged on some hypothesis which have been postulated as follows based on previous works from literature:

**$H_1$**: Perceived Vulnerability is a significant predictor of Tertiary Institution Students' Cybersecurity Behaviours.

It has been informed by previous studies that relationships exists between perceived vulnerability of individuals and their cybersecurity behaviours (McCormac et al., 2017;

Sheng et al., 2010). Other studies also found out that younger employees and less educated employees were more prone to risk of cyber threats (Pattinson et al., 2015).

**$H_2$:** Perceived Barriers is a significant predictor of Tertiary Institution Students' Cybersecurity Behaviours.

Furthermore, with regards to how individual differences could affect relationships between perceived severity and cybersecurity behaviours, a study on online shopping intentions with regards to data breaches was conducted on younger and older adults (Chakraborty et al., 2016). From this study, it was discovered that younger adults had a marginal significance with regards to a hacking incidence perceptions of severity, also they found out that gender had some significant differences with regards to perceived severity of online shopping security intentions, hence indicating associations between perceived severity and cybersecurity intentions (Chakraborty et al., 2016).

**$H_3$:** Perceived Severity is a significant predictor of Tertiary Institution Students' Cybersecurity Behaviours.

Also, it has been discovered from literature that, security self-efficacy had a high relationship with cybersecurity behaviours. A likely study of such which focused on a moderating effect of gender, discovered relationships existed amongst the self-efficacy of the respondents and their cybersecurity behaviours (Anwar et al., 2017). Also, another study informed that there were inequalities with regards to age, gender and other factors with regards to digital skills and online secured behaviours adoptions (Dodel & Mesch, 2018). Rhee et al. (2009), in their study also believed such assertions that individual differences would exist with regards to their self-efficacy in relation to cybersecurity behaviours.

**$H_4$:** Security Self-Efficacy is a significant predictor of Tertiary Institution Students' Cybersecurity Behaviours.

Furthermore, past studies have found individuals perceived barriers to differ with regards to their age, gender, and educational level in relationship with cybersecurity behaviours and beliefs, it was also found that gender in particular had a strong moderating effect on cybersecurity behaviours and perceptions (Anwar et al., 2017; Blythe et al., 2015).

**$H_5$:** Response Efficacy is a significant predictor of Tertiary Institution Students' Cybersecurity Behaviours.

With regards to the issue of response efficacy of individuals and its relationship with cybersecurity behaviours, Sheng et al. (2010) has investigated and found out that differences exists in the perceptions of individuals based on demographic factors with regards to their response efficacy to cybersecurity policies and its relationship with security behaviours online.

**$H_6$:** Cues to Action is a significant predictor of Tertiary Institution Students' Cybersecurity Behaviours.

Furthermore, assertions have been made by previous studies in alliance with the fact that cues to actions of a person can vary based on their individual characteristics/differences, with regards to cybersecurity behaviours. For instance, a study that analysed personal information security behaviour and awareness found students with lower age group to be more vulnerable in their cues to actions with regards to their cybersecurity behaviours online, that is they don't act on security warnings they get (Ogutcu et al., 2016). Also another study which focused on investigating individual differences in cybersecurity behaviours based on password sharing, found out that younger people were had more cues to actions in sharing passwords that the older ones, instigating that relationships existed between cues to action and cybersecurity behaviours (Whitty et al., 2015).

**$H_7$:** Peer Behaviour is a significant predictor of Tertiary Institution Students' Cybersecurity Behaviours.

With regards to the fact of whether individuals differ in their peer behaviours with relation to cybersecurity behaviours, some studies have informed that this could be a possibility. For example, a study that was conducted on human traits and cybersecurity behaviour intentions found out that demographic factors was a good predictor of cybersecurity behaviours (Gratian et al., 2018). Being informed yet by another study, it was found that gender had a moderating effect on the peer behaviours of employees in association to their cybersecurity behaviours (Anwar et al., 2017).

**$H_8$:** Computer Skills is a significant predictor of Tertiary Institution Students Cybersecurity Behaviours.

Additionally, it has been found out from previous literature that variations could occur with regards to individuals on their computer skills and its relationship with online security behaviours (Schulenberg et al., 2006). Similarly in the study of Anwar et al. (2017), on gender differences and employee cybersecurity behaviours, it was discovered that males had better computer skills than males, thus, it was found out that computer skills had some relationship with cybersecurity behaviours and attitudes of cyber users. Although, the current study is focusing on tertiary institution students, it is still probable that computer skills might have some relationship with the students' cybersecurity behaviour as they usually make use of computers for their academic pursuit.

**$H_9$:** Internet Skills is a significant predictor of Tertiary Institution Students' Cybersecurity Behaviours.

In concordance with the above, it was also discovered that user's Internet skills could differ with regards to their age, gender, level of education and other personal factors.

Hence, some studies have found this to be true and have carried out investigations with regards to such assertions (Schulenberg et al., 2006; Smith, 2006).

**$H_{10}$:** Prior Experience with Computer Security Practices is a significant predictor of Tertiary Institution Students' Cybersecurity Behaviours.

Furthermore, studies have also been conducted to discover if individual differences could affect their prior experience with computer security practices and its relationship with cybersecurity behaviours. It has however been discovered that gender, age and educational level of individuals has some effects with regards to their previous experiences with computer security practices (Ifinedo, 2014; Ng et al., 2009).

**$H_{11}$:** Perceived Benefits is a significant predictor of Tertiary Institution Students' Cybersecurity Behaviours.

Literature has also informed that differences in persons could affect their perceived benefits and how this relates with their cybersecurity behaviours (Ng et al., 2009; Sun et al., 2015). Furthermore, the research of Sun et al., (2015), informed that there is a gender difference in the perceived benefits of individuals.

**$H_{12}$:** Familiarity with Cyber-Threats is a significant predictor of Tertiary Institution Students' Cybersecurity Behaviours.

Concerning the issue of familiarity with cyber threats and its relationship with cybersecurity behaviours, not much study has been done on that, however, some studies have found out that individual actually differ in their level of familiarity with cyber-threats. A study found out that younger group of students were less familiar with threats unlike the older ones, showing that age actually has a difference in threat familiarity (Jeske & van Schaik, 2017).

### 3.11 Conceptual Framework

The proposed research hence after rigorous and critical review of literature as well as studying the theories explained above and trying to understand how the constructs have been used by the benchmark related cybersecurity model developed by Anwar et al. (2017), have come out with the conceptual framework for this research. The framework is presented below in Figure 3.1.

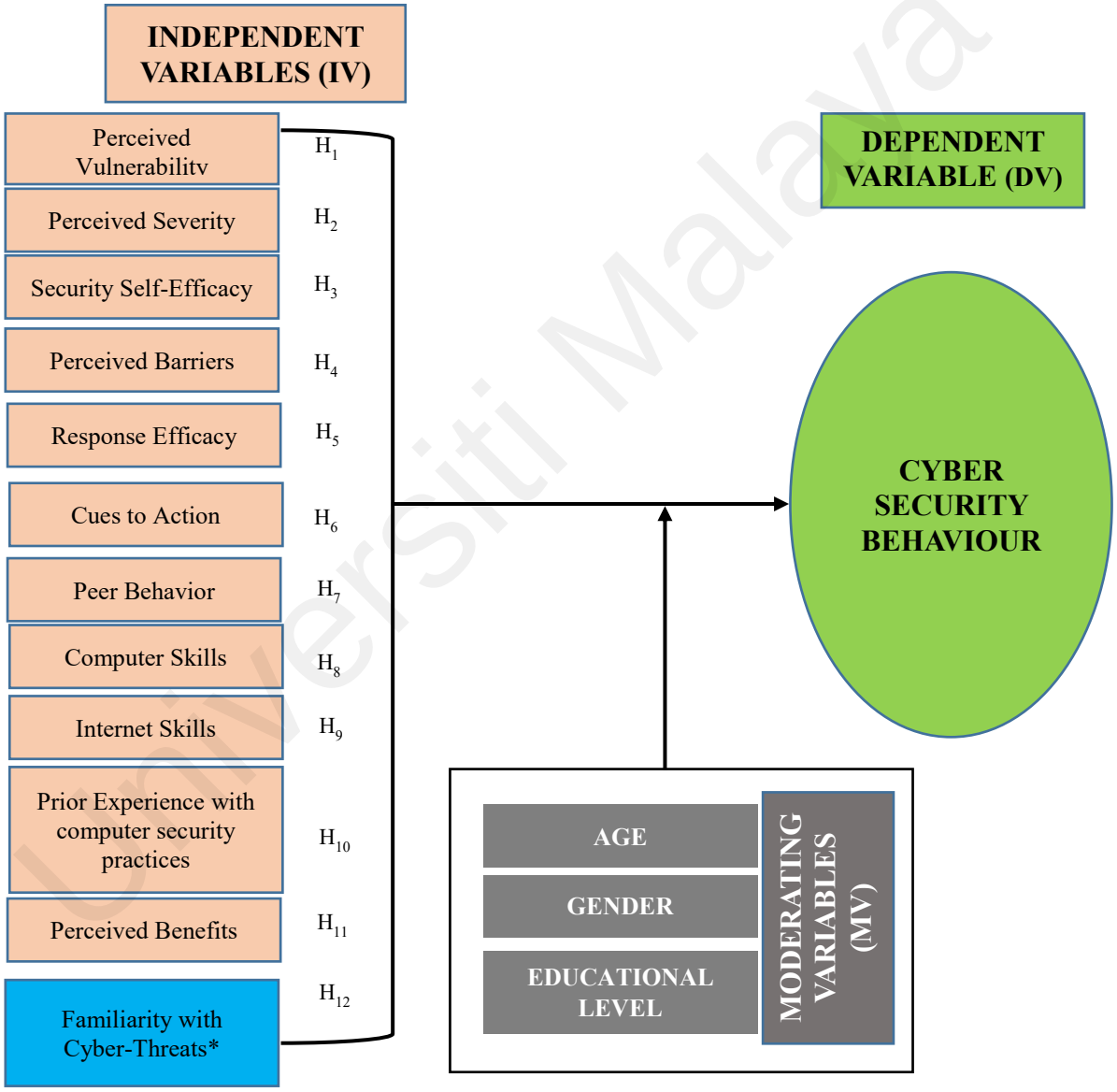


**Figure 3.1:** Research Conceptual Framework

### 3.12 Summary

This chapter has provided the detailed methods and approach that has been employed in the development of the cybersecurity behavioural model for students in the tertiary institution. More specifically, it comprehensively discussed the participants of the study, measurements, data collection method, data analysis and interpretation, as well as the validation process. Thus, the next chapter shall provide the results gotten from data analysis, backed up with discussions from the obtained results.

# CHAPTER 4: RESULTS & DISCUSSION

## 4.1 Preamble

This chapter firstly presents the analysis of data and then presents the results obtained based on the analysed data. The data analysis result is divided into two segments; the first gives a descriptive analysis of the data and presents its results in clear terms, hence giving a clear understanding of the gathered data; while the second phase of the result presents the results from the inferential analysis conducted. In this case, the inferential analysis is used to answer all the research questions amicably. The chapter shall end with a summary of the results.

## 4.2 Descriptive Analysis Results

This section shall deal with the results of the descriptive analysis of the gathered data, which focuses more on the demographics of the respondents. This is so to understand the data and how the responses are distributed among the respondents. The major focuses of the descriptive analysis for this research includes: age distribution, gender distribution, educational level distribution, rate of Internet usage per day distribution, level of Internet expertise distribution, and social media usage distribution, among the students. The following sub-sections shall present the results of the descriptive analysis for each of the demographics.

### 4.2.1 Age

The highest distribution of students based on age were those within the age range of twenty-one years old to thirty years old. This was followed by those in the range of thirty-one to forty years of age. Table 4.1 presents the students frequency distribution with regards to their age group.

**Table 4.1:** Age Frequency

| | Frequency | Percent |
|---|---|---|
| 17-20 | 36 | 8.3 |
| 21-30 | 251 | 57.7 |
| 31-40 | 113 | 26.0 |
| Above 40 | 35 | 8.0 |
| Total | 435 | 100.0 |

| Statistics | |
|---|---|
| Age Group | |
| Mean | 2.34 |
| Std. Deviation | .743 |

### 4.2.2 Gender

The highest distribution of students based on their gender were the female students, who were about 17.2% more than the males. Table 4.2 presents the students frequency distribution with regards to their respective gender.

**Table 4.2:** Gender Frequency Distribution

| | Frequency | Percent |
|---|---|---|
| Female | 255 | 58.6 |
| Male | 180 | 41.4 |
| Total | 435 | 100.0 |

| Statistics | |
|---|---|
| Gender | |
| Mean | .41 |
| Std. Deviation | .493 |

### 4.2.3 Educational Level

There were more bachelor and master students who responded to the survey than the PHD students. Table 4.3 presents the students frequency distribution with regards to their level of education.

**Table 4.3:** Educational Level Distribution

| | Frequency | Percent |
|---|---|---|
| Bachelors | 176 | 40.5 |
| Masters | 178 | 40.9 |
| Phd/Doctorate | 81 | 18.6 |
| Total | 435 | 100.0 |

| **Statistics** | |
|---|---|
| Educational Level | |
| Mean | 1.78 |
| Std. Deviation | .738 |

### 4.2.4 Rate of Internet Usage per Day

Majority of the participants reported that they used the Internet daily for more than six hours, followed by the average users, who made use of the Internet for 2-5 hours daily; however just a very insignificant number of persons claimed to make use of the Internet less than 1 hour per day. The comprehensive frequency distribution result based on rate of Internet usage daily, as obtained from the analysis is presented in Table 4.4 below.

**Table 4.4:** Daily Internet Usage Rate

| | Frequency | Percent |
|---|---|---|
| Less than 1 hour | 4 | .9 |
| 2-5 hours | 155 | 35.6 |
| More than 6 hours | 276 | 63.4 |
| Total | 435 | 100.0 |

| Statistics | |
|---|---|
| Rate of Internet Usage Per Day | |
| Mean | 2.63 |
| Std. Deviation | .503 |

### 4.2.5 Level of Internet Expertise

From the gathered analysed data, a little percentage of the students reported to have been beginners with regards to their Internet expertise; however, a majority of the students, totalling a 68.7% of the entire number of participants, reported that they were neither experts nor beginners, but were in their intermediate or average level of Internet expertise. Table 4.5 gives the complete frequency distribution regarding the level of Internet expertise.

**Table 4.5:** Level of Internet Expertise

| | Frequency | Percent |
|---|---|---|
| Beginner | 27 | 6.2 |
| Intermediate | 299 | 68.7 |
| Expert | 109 | 25.1 |
| Total | 435 | 100.0 |

| Statistics | |
|---|---|
| Level of Internet Expertise | |
| Mean | 2.19 |
| Std. Deviation | .527 |

### 4.2.6 Social Media Usage

From the analysis, it was discovered that a very insignificant percentage of the respondents, around 1.6% reported to not make use of any social media platform. However, this could be seeming biasing as perhaps they might not be using the particular social media platforms provided in the survey. As expected, a large proportion of the

respondents reported that they make use of more than one social media on a daily basis, in this case Facebook and WhatsApp; hence making it possible for them to be more exposed to cybersecurity issues. Table 4.6 below gives the frequency distribution among the participants with regards to their social media usage.

**Table 4.6:** Social Media Usage

| | Frequency | Percent |
|---|---|---|
| None | 7 | 1.6 |
| Only WhatsApp | 141 | 32.4 |
| Facebook and WhatsApp | 287 | 66.0 |
| Total | 435 | 100.0 |

| **Statistics** | |
|---|---|
| Social Media Usage | |
| Mean | 3.63 |
| Std. Deviation | .575 |

## 4.3 Inferential Analysis Results: Answering Research Questions

In this section, results from the inferential analysis are being presented. Inferential analysis is a statistical analysis conducted in order to show significances, hence making it possible for the researcher to either make assertions or inferences, which could lead to conclusions. Hence, it was deemed fit for the answering of the research questions.

### 4.3.1 ANSWERING RQ1: What are the factors affecting tertiary institution students' cybersecurity behaviours?

This aspect of the analysis was conducted in order to initially understand the factors that have a relationship between the factors of the cybersecurity behaviour scale of tertiary institution students. Hence to achieve this, a Pearson correlation analysis was carried out to see if the constructs of the cybersecurity behaviour are related to each other. The significant relationship is mainly determined by a correlation significance level of

P<0.01, while the Pearson coefficient helps in explaining the measure of the association strength between the correlative variables (Dependent and Independent Variables).

In this research, the Dependent Variable is the Cybersecurity Behaviour of Tertiary Institution Students, which is denoted by CSB, while the independent variables are thus: Perceived Vulnerability (PV), Perceived Barriers (PBr), Perceived Severity (PS), Security Self-Efficacy (SSE), Response Efficacy (RE), Cues to Action (CA), Peer Behaviours (PBhv), Computer Skills (CS), Internet Skills (IS), Prior Experience with Computer Security Practices (PE), Perceived Benefits (PBnf), and the newly added one, Familiarity with Cyber-Threats. Hence, the outcome of the correlation analysis is being presented accordingly via the following tables. Consequently, the obtained results would be assessed again via a regression analysis in research question 3, which would be used as major building blocks for the final Cybersecurity Behavioural model for Tertiary Institution Students.

The correlation analysis results are presented for the relationships existing between each independent variable and the cybersecurity behaviour of the tertiary institution students in the following tables.

#### 4.3.1.1 Relationship between Perceived Vulnerability and Cybersecurity Behaviours of Tertiary Institution Students

This section presents the results from the correlation analysis between Perceived Vulnerability and Cybersecurity Behaviours of students in the Tertiary Institutions. Furthermore, it comprises of both the correlation coefficient table, which shows the significant relationships that exists between the variables.

**Table 4.7:** Relationship between Perceived Vulnerability (PV) and Cybersecurity Behaviours (CSB) of Tertiary Institution Students

| Correlations between CSB & PV | | | |
|---|---|---|---|
| | | CSB | PV |
| CSB | Pearson Correlation | 1 | .142* |
| | Sig.(2- tailed) | | .003 |
| | N | 435 | 435 |

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

From Table 4.7 above, there is no significant correlation between Perceived Vulnerability and the Cybersecurity Behaviours of students in the tertiary institutions. The correlation is not significant as the P-value is greater than 0.01, thus P = 0.003.

#### 4.3.1.2 Relationship between Perceived Barriers and Cybersecurity Behaviours of Tertiary Institution Students

This section presents the results from the correlation analysis between Perceived Barriers and Cybersecurity Behaviours of students in the Tertiary Institutions. Furthermore, it comprises of both the correlation coefficient table, which shows the significant associations that exists between the variables.

**Table 4.8:** Relationship between Perceived Barriers (PBr) and the Cybersecurity Behaviours (CSB) of Tertiary Institution Students

| Correlations between PBr and CSB | | | |
|---|---|---|---|
| | | CSB | PBr |
| CSB | Pearson Correlation | 1 | -.110* |
| | Sig.(1-tailed) | | .011 |
| | N | 435 | 435 |

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

From Table 4.8 above, there is no significant correlation between Perceived Barriers and Cybersecurity Behaviours of students in the tertiary institutions. This is achieved as a result of the significance level, P-value which is less than 0.01, thus P = 0.011.

### 4.3.1.3: Relationship between Perceived Severity and Cybersecurity Behaviours of Tertiary Institution Students

This section presents the results from the correlation analysis between Perceived Severity and Cybersecurity Behaviours of students in the Tertiary Institutions. Furthermore, it comprises of both the correlation coefficient table, which shows the significant associations that exists between the variables.

**Table 4.9:** Relationship between Perceived Severity (PS) and the Cybersecurity Behaviours (CSB) of Tertiary Institution Students

| Correlations between PS and CSB | | | |
|---|---|---|---|
| | | CSB | PS |
| CSB | Pearson Correlation | 1 | .072 |
| | Sig.(1-tailed) | | .067 |
| | N | 435 | 435 |

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

From Table 4.9 above, there is no significant correlation between Perceived Severity and the Cybersecurity Behaviours of students in the tertiary institutions. This is achieved as a result of the significance level, P-value which is greater than 0.01, thus P = 0.072.

#### 4.3.1.4 Relationship between Security Self-Efficacy and Cybersecurity Behaviours of Tertiary Institution Students

This section presents the results from the correlation analysis between Security Self-Efficacy and Cybersecurity Behaviours of students in the Tertiary Institutions. Furthermore, it comprises of both the correlation coefficient table, which shows the significant correlations that exists between the variables.

**Table 4.10:** Relationship between Security Self-Efficacy (SSE) and the Cybersecurity Behaviours (CSB) of Tertiary Institution Students

| Correlations between SSE and CSB | | | |
|---|---|---|---|
| | | CSB | SSE |
| CSB | Pearson Correlation | 1 | .449** |
| | Sig.(1-tailed) | | .000 |
| | N | 435 | 435 |

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

From Table 4.10 above, there is a very high positive significant correlation between Perceived Vulnerability and the Cybersecurity Behaviours of students in the tertiary institutions. This is achieved as a result of the significance level, P-value which is less than 0.01, in fact in this case, it is less than 0.01, showing a very high correlation, thus $P<0.01$; More interestingly, the Pearson correlation rho, $r = 0.449$, which is moderately high, shows the strength of the existing relationship, and hence indicates that the association is a positive and strong one, as the value of rho is moderately close to 1.

#### 4.3.1.5 Relationship between Response Efficacy and Cybersecurity Behaviours of Tertiary Institution Students

This section presents the results from the correlation analysis between Response Efficacy and Cybersecurity Behaviours of students in the Tertiary Institutions. Furthermore, it comprises of both the correlation coefficient table, which shows the significant associations that exists between the variables.

**Table 4.11:** Relationship between Response Efficacy (RE) and the Cybersecurity Behaviours (CSB) of Tertiary Institution Students

**Correlations between RE and CSB**

| | | CSB | RE |
|---|---|---|---|
| CSB | Pearson Correlation | 1 | .245** |
| | Sig.(1-tailed) | | .000 |
| | N | 435 | 435 |

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

From Table 4.11 above, there is a quite high positive significant correlation between Response Efficacy and the Cybersecurity Behaviours of students in the tertiary institutions. This is achieved as a result of the significance level, P-value which is less than 0.01, in fact in this case, it is less than 0.01, showing a very high correlation, thus $P<0.01$; More interestingly, the Pearson correlation rho, $r = 0.245$, which is moderately okay, shows the strength of the existing relationship, and hence indicates that the association is a positive and an averagely strong one, as the value of rho is not too far and not too close to 1.

#### 4.3.1.6 Relationship between Cues to Action and Cybersecurity Behaviours of Tertiary Institution Students

This section presents the results from the correlation analysis between Cues to Action and Cybersecurity Behaviours of students in the tertiary institutions. Furthermore, it comprises of both the correlation coefficient table, which shows the significant associations that exists between the variables.

**Table 4.12:** Relationship between Cues to Action (CA) and the Cybersecurity Behaviours (CSB) of Tertiary Institution Students

| Correlations between CA and CSB | | | |
|---|---|---|---|
| | | CSB | CA |
| CSB | Pearson Correlation | 1 | .222** |
| | Sig.(1-tailed) | | .000 |
| | N | 435 | 435 |

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

From Table 4.12 above, there is a quite high positive significant correlation between Cues to Action and the Cybersecurity Behaviours of students in the tertiary institutions. This is achieved as a result of the significance level, P-value which is less than 0.01, in fact in this case, it is less than 0.01, showing a very high correlation, thus $P<0.01$; More interestingly, the Pearson correlation rho, $r = 0.222$, which is moderately okay, shows the strength of the existing association, and hence indicates that the relationship is a positive and an averagely strong one, as the value of rho is not too far and not too close to 1.

#### 4.3.1.7 Relationship between Peer Behaviours and Cybersecurity Behaviours of Tertiary Institution Students

This section presents the results from the correlation analysis between Peer Behaviours and Cybersecurity Behaviours of students in the Tertiary Institutions. Furthermore, it comprises of both the correlation coefficient table, which shows the significant

associations that exists between the variables. Table 4.13 gives the results of the relationship between Peer Behaviours and Cybersecurity Behaviours.

**Table 4.13:** Relationships between Peer Behaviours (PBhv) and the Cybersecurity Behaviours (CSB) of Tertiary Institution Students

| Correlations between PBhv and CSB | | | |
|---|---|---|---|
| | | CSB | PBhv |
| CSB | Pearson Correlation | 1 | .190** |
| | Sig.(1-tailed) | | .000 |
| | N | 435 | 435 |

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

From Table 4.13 above, there is a quite high positive significant correlation between Peer Behaviour and the Cybersecurity Behaviours of students in the tertiary institutions. This is achieved as a result of the significance level, P-value which is less than 0.01, in fact in this case, it is less than 0.01, showing a very high correlation, thus $P<0.01$; However, the Pearson correlation rho, $r = 0.190$, is a bit low, hence might need further analysis, shows the strength of the existing association, and thus indicates that although the relationship is positive, yet it possesses a somehow low strength, as the value of rho seems not to be close to 1.

#### 4.3.1.7 Relationship between Computer Skills and Cybersecurity Behaviours of Tertiary Institution Students

Results from the correlation analysis between Computer Skills and Cybersecurity Behaviours of students in the Tertiary Institutions is presented in this section. Furthermore, it comprises of both the correlation coefficient table, which shows the significant associations that exists between the variables. Table 4.14 gives the results of the relationship between Computer Skills and Cybersecurity Behaviours.

**Table 4.14:** Relationship between Computer Skills (CS) and the Cybersecurity Behaviours (CSB) of Tertiary Institution Students

| Correlations between CS and CSB | | | |
|---|---|---|---|
| | | CSB | CS |
| CSB | Pearson Correlation | 1 | .353** |
| | Sig.(1-tailed) | | .000 |
| | N | 435 | 435 |

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

From Table 4.14 above, there is a very high positive significant correlation between Computer Skills and the Cybersecurity Behaviours of students in the tertiary institutions. This is achieved as a result of the significance level, P-value which is less than 0.01, in fact in this case, it is less than 0.01, showing a very high correlation, thus $P<0.01$; More interestingly, the Pearson correlation rho, $r = 0.353$, which is moderately high, shows the strength of the existing association, and hence indicates that the relationship is a positive and strong one, as the value of rho is moderately close to 1.

#### 4.3.1.9 Relationship between Internet Skills and Cybersecurity Behaviours of Tertiary Institution Students

This section presents the results from the correlation analysis between Internet Skills and Cybersecurity Behaviours of students in the Tertiary Institutions. Furthermore, it comprises of both the correlation coefficient table, which shows the significant relationships that exist between the variables. Table 4.15 gives the results of the relationship between Internet Skills and Cybersecurity Behaviours.

**Table 4.15:** Relationship between Internet Skills (IS) and the Cybersecurity Behaviours (CSB) of Tertiary Institution Students

| Correlations between IS and CSB | | | |
|---|---|---|---|
| | | CSB | IS |
| CSB | Pearson Correlation | 1 | .183** |
| | Sig.(1-tailed) | | .000 |
| | N | 435 | 435 |

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

From Table 4.15 above, a positive significant correlation exists between Peer Behaviour and the Cybersecurity Behaviours of students in the tertiary institutions. This is achieved as a result of the significance level, P-value which is less than 0.01, in fact in this case, it is less than 0.01, showing a very high correlation, thus $P<0.01$; Furthermore, the Pearson correlation rho, $r = 0.183$, which is low, shows that the strength of the existing association seems to be weak, and hence indicates that the relationship is a positive and possesses a low strength, as the value of rho seems not to be too close to 1.

#### 4.3.1.10 Relationship between Prior Experience with Computer Security Practices and Cybersecurity Behaviours of Tertiary Institution Students

This section presents the results from the correlation analysis between Prior Experience with Computer Security Practices and Cybersecurity Behaviours of students in the Tertiary Institutions. Furthermore, it comprises of both the correlation coefficient table, which shows the significant associations that exists between the variables. Table 4.16 gives the results of the relationship between Prior Experience with Computer Security Practices and Cybersecurity Behaviours.

**Table 4.16:** Relationship between Prior Experience with Computer Security Practices (PE) and the Cybersecurity Behaviours (CSB) of Tertiary Institution Students

| Correlations between PE and CSB | | | |
|---|---|---|---|
| | | CSB | PE |
| CSB | Pearson Correlation | 1 | .445** |
| | Sig.(1-tailed) | | .000 |
| | N | 435 | 435 |

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

From Table 4.16 above, there is a very high positive significant correlation between Prior Experience with Computer Security Practices and the Cybersecurity Behaviours of students in the tertiary institutions. This is achieved as a result of the significance level, P-value which is less than 0.01, in fact in this case, it is less than 0.01, showing a very high correlation, thus $P<0.01$; More interestingly, the Pearson correlation rho, $r = 0.445$, which is moderately high, shows the strength of the existing association, hence indicates that the relationship is a positive and strong one, as the value of rho is moderately close to 1.

### 4.3.1.11 Relationship between Perceived Benefits and Cybersecurity Behaviours of Tertiary Institution Students

This section presents the results from the correlation analysis between Perceived Benefits and Cybersecurity Behaviours of students in the Tertiary Institutions. Furthermore, it comprises of both the correlation coefficient table, which shows the significant associations that exists between the variables. Table 4.17 gives the results of the relationship between Perceived Benefits and Cybersecurity Behaviours.

**Table 4.17:** Relationship between Perceived Benefits (PBnf) and the Cybersecurity Behaviours (CSB) of Tertiary Institution Students

| Correlations between PBnf and CSB | | | |
|---|---|---|---|
| | | CSB | PBnf |
| CSB | Pearson Correlation | 1 | .261** |
| | Sig.(1-tailed) | | .000 |
| | N | 435 | 435 |

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

From table 4.17 above, there is a quite high positive significant correlation between Perceived Benefits and the Cybersecurity Behaviours of students in the tertiary institutions. This is achieved as a result of the significance level, P-value which is less than 0.01, in fact in this case, it is less than 0.01, showing a very high correlation, thus $P<0.01$; More interestingly, the Pearson correlation rho, $r = 0.261$, which is averagely okay, shows the strength of the existing association, and hence indicates that the relationship is a positive and an averagely one, as the value of rho is not too far and not too close to 1.

#### 4.3.1.12 Relationship between Familiarity with Cyber-Threats and Cybersecurity Behaviours of Tertiary Institution Students

This section presents the results from the correlation analysis between Familiarity with Cyber-Threats and Cybersecurity Behaviours of students in the Tertiary Institutions. Furthermore, it comprises of both the correlation coefficient table, which shows the significant associations that exists between the variables. Table 4.18 gives the results of the relationship between Familiarity with Cyber-Threats and Cybersecurity Behaviours.

**Table 4.18:** Relationship between Familiarity with Cyber-Threats (FCT) and the Cybersecurity Behaviours (CSB) of Tertiary Institution Students

| Correlations between FCT and CSB | | | |
|---|---|---|---|
| | | CSB | FCT |
| CSB | Pearson Correlation | 1 | .292** |
| | Sig.(1-tailed) | | .000 |
| | N | 435 | 435 |

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

From Table 4.18 above, there is a quite high positive significant correlation between Familiarity with Cyber-Threats and the Cybersecurity Behaviours of students in the tertiary institutions. This is achieved as a result of the significance level, P-value which is less than 0.01, in fact in this case, it is less than 0.01, showing a very high correlation, thus P<0.01; More interestingly, the Pearson correlation rho, r = 0.292, which is moderately okay, shows the strength of the existing association, and hence indicates that the relationship is a positive and an averagely one, as the value of rho is not too far and not too close to 1.

#### 4.3.1.13 Summary of the Results from Research Question 1

In order to give a clear summary of the results from the Pearson correlation analysis conducted in finding the associations existing amongst the cybersecurity behaviour scale constructs, table 4.19 below presents the results with both R values, and R-squared values.

**Table 4.19:** Summary of the Results from Research Question 1

| DV: CSB | | | |
|---|---|---|---|
| **IVs** | **r** | **$R^2$** | **P** |
| PV | 0.142 | 0.377 | 0.003 |
| PBr | -0.110 | 0.332 | 0.022 |
| PS | 0.072 | 0.268 | 0.133 |
| SSE | 0.449 | 0.670 | <0.001 |
| RE | 0.245 | 0.495 | <0.001 |
| CA | 0.222 | 0.471 | <0.001 |
| PBhv | 0.190 | 0.436 | <0.001 |

| | | | |
|---|---|---|---|
| CS | 0.353 | 0.594 | <0.001 |
| IS | 0.183 | 0.428 | <0.001 |
| PE | 0.445 | 0.667 | <0.001 |
| PBnf | 0.261 | 0.511 | <0.001 |
| FCT | 0.292 | 0.540 | <0.001 |

### 4.3.2 ANSWERING RQ2: What moderating effects do sociological factors such as age, gender and educational level, have on the Cybersecurity Behaviour of Tertiary Institution Students?

The intention of this research question was to find out if the relationship between the students' Familiarity with Cyber-Threats, Cybersecurity beliefs and cybersecurity behaviour is being effected moderately by sociological factors such as age, gender and educational level. In order to achieve this, a series of regression analyses were conducted to examine the association between each of the predictor variable and the sociological factors on their relationship with cybersecurity behaviour, which is the dependent variable. More specifically, the Univariate General Linear Model statistical technique in SPSS, was used for this analysis. For all the analyses conducted in this regard, the terms were constructed via the calculation of the centred scores product with the binary variable of age, gender, and educational level, based on the centred mean score of the predictor variables, which are: Familiarity with Cyber-Threats; Perceived Vulnerability (PV); Perceived Barriers (PBr); Perceived Severity (PS); Security Self-Efficacy (SSE); Response Efficacy (RE); Cues to Action (CA); Peer Behaviours (PBhv); Computer Skills (CS); Internet Skills (IS); Prior Experience with Computer Security Practices (PE); and Perceived Benefits (PBnf). Analysis results for the moderating effects of age, gender, and educational level are presented respectively and explained accordingly in the following sub-sections.

#### 4.3.2.1 Age Effects

The association of age with the Cybersecurity measurement scales was being examined via a series of biserial point correlations, where the ages were split into two groups, with students below age of 30 coded as 0-Younger Students, and those above the age 30 coded as 1- Older Students. The well accepted significance alpha level of <0.05 was maintained, so as to avoid over-interpretation of the effect sizes of the relationships. From the analysis conducted, as shown in Table 4.10, age only had an effect on the Perceived Barriers of the students (r= 0.101; P=0.036). Furthermore, it was discovered that the older students (those above 30 years) reported slightly lower levels of perceived barriers (M= 3.01; SD= 0.71) than their counterparts, with a higher mean value of 3.15 (SD = 0.69). Hence, these results shows that age does affect the cybersecurity beliefs and behaviours of tertiary institution students and could affect the way they perceive certain barriers, that is their inconvenience levels in checking for cybersecurity issues. The younger students perhaps due to the fact that they are still active and might be always up-to-date with latest technologies, and may not have barriers in dealing with cybersecurity issues (Sawyer & Hancock, 2018). Table 4.20 gives a presentation of the results obtained for age effects.

**Table 4.20:** Results of the experiments means (M), standard deviations (SD), point-biserial correlation, with reported age differences for the different cybersecurity scales

| | **Younger Students (Below 30) (N = 287)** | | **Older Students (Above 30) (N = 148)** | | **r** | **P** |
|---|---|---|---|---|---|---|
| | M | SD | M | SD | | |
| **PV** | 3.77 | 0.51 | 3.80 | 0.54 | 0.026 | 0.582 |
| **PBr** | 3.01 | 0.71 | 3.15 | 0.69 | 0.101* | 0.036 |
| **PS** | 4.26 | 0.61 | 4.19 | 0.76 | -0.053 | 0.270 |
| **SSE** | 2.82 | 0.85 | 2.84 | 0.86 | 0.014 | 0.771 |
| **RE** | 3.94 | 0.57 | 4.01 | 0.65 | 0.047 | 0.329 |

| | | | | | | |
|---|---|---|---|---|---|---|
| **CA** | 2.67 | 0.86 | 2.70 | 0.87 | 0.015 | 0.759 |
| **PBhv** | 2.90 | 0.67 | 3.01 | 0.65 | 0.072 | 0.132 |
| **CS** | 3.77 | 0.71 | 3.76 | 0.69 | -0.001 | 0.975 |
| **IS** | 3.77 | 0.71 | 3.76 | 0.66 | -0.004 | 0.939 |
| **PE** | 3.01 | 0.69 | 2.99 | 0.68 | -0.015 | 0.748 |
| **PBnf** | 3.96 | 0.57 | 3.97 | 0.55 | 0.006 | 0.906 |
| **FCT** | 3.63 | 0.95 | 3.65 | 0.95 | 0.012 | 0.808 |
| **CSB** | 3.22 | 0.52 | 3.31 | 0.56 | 0.070 | 0.148 |

#### 4.3.2.2 Gender Effects

The students' gender were split into two groups, with female students coded as 0, and male students coded as 1. The well accepted significance alpha level of <0.05 was maintained, so as to avoid over-interpretation of the effect sizes of the relationships. From the analysis conducted, as shown in Table 4.21, gender had effects on six factors of the cybersecurity behaviour model which are as follows: Perceived Severity (r= -0.132, P=0.006); Security Self Efficacy (r= 0.362, P<0.001); Computer Skills (r= 0.233, P<0.001); Internet Skills (r= 0.115, P= 0.016), Prior Experience with Computer Security Practices (r= 0.123, P= 0.010), and Cybersecurity Behaviour (r = 0.150, P= 0.002). Importantly, gender had the most effective moderation with regards to the relationship between the factors of cybersecurity behaviour. The highest effect of gender on the student's cybersecurity scale was found in their Security Self Efficacy, while the lowest effect was found in their Internet Skills.

With regards to the moderation of gender among the specific groups, the means of both male and females were compared and is being interpreted thus. For the effect of gender on the Perceived Severity of the students, the female students reported a higher level of severity (M= 4.31, SD= 0.63) than the male students. Hence, the female students were more concerned about the consequences of risky cybersecurity behaviours. However, male students reported higher level of self-efficacy (M= 3.21; SD= 0.83), with regards to

their cybersecurity than the female students. Hence, it can be asserted that male students tend to have higher levels of confidence in handling cyber-threat issues. This is in concordance with a recent related investigation that was carried out on employees in an organization (Anwar et al., 2017), where the male employees had a higher level of security self-efficacy than their female counterparts. Furthermore, the second highest gender effect was found on computer skills, where males again reported to have had higher levels of computer skills (M= 3.96, SD= 0.69) than the females. With regards to Internet Skills gender effects, the female students reported a lower degree of Internet skills (SD= 0.70) than the male correspondents. However, these differences between them was not so much, hence the assertions are based on the statistical results provided. More so, regarding to the Prior Experiences with Computer Security Practices, the male students also reported to have had more experiences than the females, with a mean value of 3.10. Finally, regarding the effect of gender on the factor of cybersecurity behaviours of tertiary institution students, it was discovered that the male students reported higher levels of cybersecurity behaviour (M= 3.34, SD= 0.53) than the female students.

In summary, it is obvious that gender has effects in the relationship between the factors of cybersecurity behavioural scale. Hence, male and female students differ in the way they react to cybersecurity issues, which in return affects their security behaviours as well. Table 4.21 gives a presentation of the results obtained for gender effects.

**Table 4.21:** Results of the experiments means (M), standard deviations (SD), point-biserial correlation, with reported gender differences for the different cybersecurity scales

| | Female Students (N = 255) | | Male Students (N = 180) | | r | P |
|---|---|---|---|---|---|---|
| | M | SD | M | SD | | |
| **PV** | 3.79 | 0.51 | 3.77 | 0.55 | -0.025 | 0.598 |
| **PBr** | 3.02 | 0.73 | 3.08 | 0.66 | 0.034 | 0.480 |
| **PS** | 4.31 | 0.63 | 4.13 | 0.71 | -0.132* | 0.006 |
| **SSE** | 2.57 | 0.77 | 3.21 | 0.83 | 0.362* | <0.001 |
| **RE** | 3.94 | 0.62 | 3.98 | 0.58 | 0.034 | 0.481 |
| **CA** | 2.69 | 0.83 | 2.67 | 0.91 | -0.016 | 0.735 |
| **PBhv** | 2.95 | 0.64 | 2.93 | 0.69 | -0.012 | 0.805 |
| **CS** | 3.63 | 0.69 | 3.96 | 0.69 | 0.233* | <0.001 |
| **IS** | 3.69 | 0.70 | 3.86 | 0.67 | 0.115* | 0.016 |
| **PE** | 2.93 | 0.64 | 3.10 | 0.73 | -0.123* | 0.010 |
| **PBnf** | 3.97 | 0.54 | 3.96 | 0.61 | -0.013 | 0.795 |
| **FCT** | 3.57 | 0.99 | 3.73 | 0.89 | 0.081 | 0.090 |
| **CSB** | 3.18 | 0.53 | 3.34 | 0.53 | 0.150* | 0.002 |

#### 4.3.2.3 Educational level Effects

The relationship between educational level and the Cybersecurity measurement scales was being examined via a series of biserial point correlations, where the students' educational level was split into two groups, with undergraduate students coded as 0, and postgraduate students coded as 1. The well accepted significance alpha level of <0.05 was maintained, so as to avoid over-interpretation of the effect sizes of the relationships. From the analysis conducted, as shown in Table 4.22, it is revealed that educational level had effects on four factors of the cybersecurity behaviour scale which are as follows: Computer Skills (r= 0.155, P=0.001); Internet Skills (r= 0.120, P= 0.012), Familiarity with Cyber-Threats (r= 0.106; P= 0.026) and Cybersecurity Behaviour (r = 0.110, P=

0.022). The highest effect of educational level on the student's cybersecurity scale was found in Computer Skills, while the lowest effect was found in Familiarity with Cyber-Threats.

With regards to the relationship between educational level and the factors of the cybersecurity scale, the following observations were discovered based on the group means comparison. For Computer Skills, it was revealed that the postgraduate students reported a higher computer skills score (M=3.86; SD=0.65) than the undergraduates; this is expected as it can prove that the higher the educational level, the more additional skills and exposure the students would have. Also, most undergraduate students undertake lectures, whereas postgraduates mostly use the computers for their research work, hence probably having more chances of cybersecurity issues (Jeske & van Schaik, 2017).

Furthermore, it was discovered that educational level has an impact on the Internet Skills of tertiary institution students, with the postgraduates again attaining a higher mean score of 3.83 than their undergraduate counterparts. Moreover, some effects were found from the relationship between the level of education and familiarity with cyber-threats of the students (Jeske & van Schaik, 2016), whereby postgraduate students yet again reported a slightly higher score of being familiar with cyber-threats (M= 3.72) than the undergraduate students, this could be so due to experience accumulation and constant use of the Internet. Finally, from the interactions of educational level on the cybersecurity behaviours of the students, results reveal that the undergraduate students had a slightly lower standard deviation of 3.18 than the postgraduate students, hence making the postgraduate students to still have a higher educational effect count.

From these results obtained, it was indicated that for all the effects of educational level, the postgraduate students scored higher, hence establishing the fact that the more educated one is, the more informed and well-behaved such a fellow could be; also, education can

help in maintaining good cybersecurity behaviours. Table 4.22 below shows the results obtained for the effects of educational level on the cybersecurity scales.

**Table 4.22:** Results of the experiments means (M), standard deviations (SD), point-biserial correlation, with reported educational level differences for the different cybersecurity scales

| | **Undergraduates (N = 176)** | | **Postgraduates (N = 259)** | | **r** | **P** |
|---|---|---|---|---|---|---|
| | M | SD | M | SD | | |
| **PV** | 3.84 | 0.50 | 3.09 | 0.53 | -0.094 | 0.049 |
| **PBr** | 2.98 | 0.69 | 3.09 | 0.71 | 0.076 | 0.113 |
| **PS** | 4.27 | 0.69 | 4.22 | 0.66 | -0.036 | 0.459 |
| **SSE** | 2.76 | 0.84 | 2.88 | 0.86 | 0.066 | 0.169 |
| **RE** | 3.93 | 0.57 | 3.98 | 0.62 | 0.036 | 0.457 |
| **CA** | 2.74 | 0.88 | 2.64 | 0.85 | -0.058 | 0.224 |
| **PBhv** | 2.93 | 0.68 | 2.94 | 0.65 | 0.008 | 0.862 |
| **CS** | 3.63 | 0.76 | 3.86 | 0.65 | 0.155* | 0.001 |
| **IS** | 3.66 | 0.74 | 3.83 | 0.65 | 0.120* | 0.012 |
| **PE** | 2.97 | 0.72 | 3.03 | 0.66 | 0.045 | 0.347 |
| **PBnf** | 3.99 | 0.56 | 3.95 | 0.57 | -0.032 | 0.509 |
| **FCT** | 3.52 | 0.96 | 3.72 | 0.93 | 0.106* | 0.026 |
| **CSB** | 3.18 | 0.57 | 3.31 | 0.51 | 0.110* | 0.022 |

### 4.3.3 ANSWERING RQ3: What are the significant predictors of the Cybersecurity Behaviours of Tertiary Institution Students?

Multiple Regression Analysis was employed in assessing the significant predictors among the factors of the cybersecurity behavioural model. This analysis was carried out to be able to find the predictors of the Cybersecurity Behaviour (CSB), which is the dependent variable, on the Independent Variables, of which in this research are: Perceived Vulnerability (PV); Perceived Barriers (PBr); Perceived Severity (PS); Security Self-Efficacy (SSE); Response Efficacy (RE); Cues to Action (CA); Peer Behaviours (PBhv);

Computer Skills (CS); Internet Skills (IS); Prior Experience with Computer Security Practices (PE); Perceived Benefits (PBnf); and Familiarity with Cyber-Threats (FCT). Hence, the result from analysis are being presented in the following tables accordingly and shall be explained.

**Table 4.23:** Cybersecurity Behaviour Regression Model Summary

| Model Summary[b] | | | | | |
|---|---|---|---|---|---|
| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate | Durbin-Watson |
| 1 | .568[a] | .323 | .304 | .44834 | 1.946 |

a. Predictors: (Constant), FCT, PBhv, PBr, PS, CA, IS, PV, PBnf, SSE, RE, PE, CS
b. Dependent Variable: CSB

From the Table 4.23 above, the values of Rho and R square are being provided. The Rho value gives a representation of the simple correlation amongst the predictor and dependent variable, in this case, R = 0.568, which indicates a high degree of correlation, as it's not very far from 1. However the R square value, of which in this case is 0.323, gives an indication of how much total variation of the dependent variable, Cybersecurity Behaviour (CSB) is being explained by the independent variables, of which are Perceived Vulnerability (PV); Perceived Barriers (PBr); Perceived Severity (PS); Security Self-Efficacy (SSE); Response Efficacy (RE); Cues to Action (CA); Peer Behaviours (PBhv); Computer Skils (CS); Internet Skills (IS); Prior Experience with Computer Security Practices (PE); Perceived Benefits (PBnf); and Familiarity with Cyber-Threats (FCT). Hence, 32.3% of the total variance of the dependent variable is being explained by the independent variables, which is averagely fair enough and is acceptable as human behaviour cannot fully be predictable (Kelley et al., 2018; Neter et al., 1985, 1989), because they can change at any time. The ANOVA results from regression analysis is being presented in Table 4.8.

**Table 4.24:** ANOVA Results describing how well the Regression equation fits the data

| ANOVA[a] | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Sum of Squares | df | Mean Square | F | P |
| 1 | Regression | 40.461 | 12 | 3.372 | 16.774 | .000[b] |
| | Residual | 84.825 | 422 | .201 | | |
| | Total | 125.286 | 434 | | | |

a. Dependent Variable: CSB

b. Predictors: (Constant), FCT, PBhv, PBr, PS, CA, IS, PV, PBnf, SSE, RE, PE, CS

Table 4.24 gives a report on the level at which the data is being fitted by the regression equation; that is how the dependent variable is being predicted. Furthermore, it gives an indication that the dependent variable, which is Cybersecurity Behaviours is being predicted by the regression model significantly well. This is done via checking the significance column, also known as p-value, which gives an indication of the statistical significance of the run regression model. From the results, $p < 0.001$, which is less than 0.05; hence it shows that the regression model attainted a significantly statistical prediction of the outcome variable; which also proves that the data is in a good fit. Table 4.25 gives the results of the regression analysis coefficients for the predictors of Tertiary institution students' cybersecurity behaviours.

**Table 4.25:** Results of the Regression Analysis Coefficients of the predictors of Tertiary Institution Students Cybersecurity Behaviours

| Coefficients[a] | | | | | | |
|---|---|---|---|---|---|---|
| Model | | Unstandardized Coefficients | | Standardized Coefficients | T | P |
| | | B | Std. Error | Beta | | |
| 1 | (Constant) | 1.100 | .266 | | 4.130 | .000 |
| | PV | .036 | .046 | .035 | .788 | .431 |
| | PBr | .002 | .032 | .003 | .063 | .950 |
| | PS | -.005 | .036 | -.006 | -.126 | .900 |
| | SSE | .149 | .035 | .238 | 4.325 | .000 |
| | RE | .096 | .044 | .107 | 2.167 | .031 |
| | CA | -.014 | .029 | -.022 | -.473 | .637 |

| | | | | | |
|---|---|---|---|---|---|
| PBhv | .017 | .036 | .021 | .478 | .633 |
| CS | .056 | .048 | .073 | 1.153 | .250 |
| IS | -.047 | .041 | -.060 | -1.130 | .259 |
| PE | .217 | .041 | .277 | 5.281 | .000 |
| PBnf | .090 | .046 | .095 | 1.978 | .049 |
| FCT | .046 | .026 | .081 | 1.743 | .082 |

a. Dependent Variable: CSB

To be able to directly and finally answer RQ3, in finding the significant predictors of Cybersecurity Behaviours, Table 4.25, depicts it all. Thus, Table 4.25 presents relevant information that can be used in predicting Cybersecurity Behaviours based on the independent the constructs of Cybersecurity psychosocial factors and familiarity with cyber-threats. It also helps in determining as to whether the psychosocial factors and familiarity with cyber-threats are able to statistically and significantly influence the model (this is achieved by checking the significance column, also known as the P-value, to see if it's less than 0.05). Thus, from the regression analysis conducted, the factors that predict the tertiary institution students' Cybersecurity Behaviours, are: Security Self-Efficacy (SSE): $t = 4.325$, $P < .001$; Response Efficacy (RE): $t = 2.167$, $P = .031$; Prior Experience with Computer Security Practices (PE): $t = 5.281$, $P < .001$; and a little influence by Perceived Benefit (PBnf): $t = 1.978$, $P = .049$. Therefore, the factor that influences the cybersecurity behaviours of the tertiary institution students most from the analysis is Prior Experience with Computer Security Practices (PE), meaning that the previous experiences of the students with computer security practices can influence them in the way they would behave with regards to being secure online, and this is a positive influence. Also, this is followed by their security self-efficacy, which means that the confidence level of handling cyber-threats by the students has a high way of influencing their cybersecurity behaviour, this is also a positive influence. Security Self Efficacy has proven in a number of studies to be a good predictor of security behaviours (Arachchilage & Love, 2014; Ng et al., 2009; Rhee et al., 2009). Consequently, in a study that focused

on trust and distrust on the web, it was found out that the experiences of users actually reflected in the manner by which they handled trust issues while using the Internet (Seckler et al., 2015), thus also reflecting their behavioural attitude to security issues. More so, another study informed that security self-efficacy was moderately effected by gender in relation to the cybersecurity behaviours of employees in an organization (Anwar et al., 2017).

### 4.3.4 ANSWERING RQ4: What are the factors of the Cybersecurity Behavioural Model for tertiary institution students?

The answer to this research question is simply the outcome of the proposed model which is being generated from the results of the regression analysis in research question 3. Thence, the significant predictors that have emerged for the final cybersecurity behavioural model for tertiary institution students are: Security Self-Efficacy (SSE): $t = 4.325$, $P < .001$; Response Efficacy (RE): $t = 2.167$, $P = .031$; Prior Experience with Computer Security Practices (PE): $t = 5.281$, $P < .001$; and a little influence by Perceived Benefit (PBnf): $t = 1.978$, $P = .049$. The final proposed Model is presented in Figure 4.1.

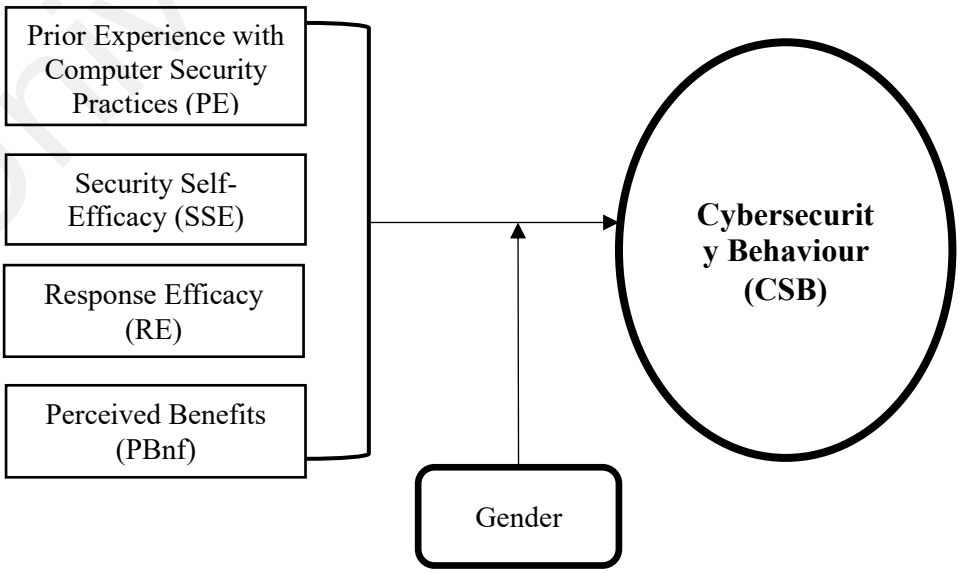


**Figure 4.1:** Cybersecurity Behavioural Model for Tertiary Institution Students (CBM-TIS)

## 4.4 Summary

This chapter has given a comprehensive and clarifying presentation of the results obtained from the statistical analysis conducted, hence answering the questions of the research. First and foremost, the chapter presented the result of the descriptive analysis of the gathered data, hence helping to provide a background and clear understanding of the data distribution among the participants.

With regards to finding the significant predictors of Cybersecurity Behaviours of students in the tertiary institutions, it was found that the predicting factors were: Security Self Efficacy, Response Efficacy, Prior Experience with Computer Security Practices, and a little influence by Perceived Benefits. However, the most influencing of the factors happened to be the students' Prior Experiences with Computer Security Practices. This hence means that the more experienced the students are, the more cybersecurity conscious and assured they would be, however, it is in absolute concordance with previous studies (Caulkins et al., 2019; Seckler et al., 2015) which informed that experiences of security practices is a very important and influencing factor as regarding the security behaviours of Internet/cyber users.

Furthermore, it has been obtained that age, gender, and educational level have some moderating effect on the relationships between the factors of the cybersecurity behaviours of tertiary institution students. However, the sociological factor with much effects is gender, which had effects on 6 of the cybersecurity behavioural factors (Perceived Severity, Security Self-Efficacy, Computer Skills, Internet Skills, Prior Experience with Computer Security Practices, and Cybersecurity Behaviour), which was followed by educational level, which had effects on 4 factors (Computer Skills, Internet Skills, Familiarity with Cyber-Threats, and Cybersecurity Behaviour); although age did not

seem to have much effects as the other two factors, however it had little effect on the Perceived Behaviour of the students.

Final assertions and conclusions based on the results and objectives would be made in the next chapter.

# CHAPTER 5: CONCLUSION

## 5.1 Preamble

This chapter is the final chapter of this thesis. It shall give an overall summary of the research that has been carried out, and based on the results obtained from data analysis, make assertions and inferences. Consequently, the chapter shall make final decisions to the postulated hypothesis of this research. Furthermore, recommendations and future work would be suggested as well, so as to aid the furtherance and expansion of the research field.

## 5.2 Concluding on the Objectives

This study aimed at answering three objectives which are:

1. To identify the factors affecting tertiary institution students' cybersecurity behaviours.
2. To assess the predicting factors of the cybersecurity behaviours of tertiary institution students.
3. To propose a cybersecurity behavioural model for tertiary institution students.

Results from analysis conducted in chapter 4 suggests that the objectives have been duly answered. Objective 1 which aimed at identifying the relating factors of tertiary institution student's cybersecurity behaviours was achieved via a correlation analysis, thus producing the following factors to be relatives of the tertiary institution students' cybersecurity behaviours. The relating factors obtained are: Security Self Efficacy, Response Efficacy, Cues to Action, Peer behaviour, Computer Skills, Internet Skills, Prior Experiences with Computer Security Practices, Perceived Benefits and Familiarity with Cyber threats.

Regarding the second objective, which is the main objective of the research, aimed at finding the associating factors of cybersecurity behaviours of tertiary institution students' was achieved via a regression analysis. Emerging factors are: Prior Experience with Computer Security Practices, Security Self Efficacy, Response Efficacy, and Perceived Benefits. The aforementioned factors predicted the cybersecurity behaviours of the tertiary institution students. Interestingly, the performance of the top predictors from this study findings, which are Prior Experiences and Security Self Efficacy, are in concordance with findings from past security studies (Anwar et al., 2017; Arachchilage & Love, 2014; Blythe & Coventry, 2018; Caulkins et al., 2019; Chan et al., 2005; Ifinedo, 2012; Jeske & van Schaik, 2017; Ng et al., 2009), which have proven that the two factors are strong influencers of security behaviours.

The final objective have also been achieved, thus a cybersecurity behavioural model for tertiary institution students (CBM-TIS) has been proposed in Figure 4.1 in the previous chapter.

### 5.3 Insights

In this final section of this dissertation, some insights are being made based on linkage between the final research questions results and the reported data gathered from the participants.

Recalling from the results of the second research question, which in return is the building block of the final research model, there are some insights to make, in conjunction with the responses from the students. Specifically, in order not to over interpret effects from results obtained, only the highest two significantly related factors of the cybersecurity model would be deliberated on.

The second to the top highest predictive effect was found on Security Self Efficacy of the Students, as this had the strongest relationship with the Cybersecurity Behaviour of the students. This is in agreement with some studies which have reported significant relationships between Security Self Efficacy and Cybersecurity Behaviours or attitude as the case may be (Anwar et al., 2017; Dodel & Mesch, 2018; Rhee et al., 2009).

Thus, some insight has been found from the responses of the students with regards to their Security Self-Efficacy, which shows how this actually affects their cybersecurity behaviour in reality. From the first item that was used to find out if the students had the knowledge of applying security patches to operating systems (M=2.82; SD=1.085), as expected by the researcher, majority about 42.3% reported that they had no idea about such, only 29.4% of them stated that they had such idea, although another 28.3% reported not being sure. Hence from this, it can be seen that the students don't have basic security solution ideas and they are not sure of handling security issues like this. Another item which was used in finding out their confidence level in resetting web-browsers to diverse levels of security (M=3.21; SD=1.013), as simple as this might seem, yet a majority of around 55.8% were either not confident or not sure of their confidence levels. Regarding an item that was used to examine the confidence levels of the students in handling files that have being infected with virus (M=2.74; SD= 1.123), it was quite shocking to know that majority again of the students, around 71.7% didn't have confidence or were not sure of their level of confidence in dealing with such issues. Another insight was found in their responses to the item which tried to measure if they had the feeling of confidence in dealing with spyware or malwares from their computer (M=2.84; SD=1.143). The majority as usual were in the categories of No and Maybe, summing them up to 66.4%. Furthermore, a very high rate of unsureness or inability, around 75.2% was found in their responses regarding if their possession of skills for implanting security measures to stop intruders from gaining unauthorised access to their confidential information. Finally,

when being asked if they possessed skills to implement security measures that can help in stopping people from causing damage to their computer (M=2.67; SD=1.060), a huge 70.5% of them reported to have no skill at all or were absolutely unsure if they had such skills.

Hence, from these insights, it is obvious that students in tertiary institution still has a long way to go regarding their confidence level in handling security issues and this definitely can affect their cybersecurity behaviours, in extension their cybersecurity assurance.

Furthermore, the next insight is taken with regards to how the students' Prior Experiences to Computer Security Practices (PE) was the highest predictor to their cybersecurity behaviours, this is in line with the results from the study of D. Kelley (2018), where it was observed that knowledge of security had a systematic relationship with correct recognition of the websites, however it didn't relate with other variables used by the researchers. Moreover, in the current study, this was also reflective in their responses to the items of the scale, which shall be deliberated thus.

The first item that was used in measuring the PE scale was a statement that tried to assess if the students have had formal training on basic/common practices of computer security (M=2.44; SD=1.017). From their responses, it was so obvious that most of the participants have not had such training. In fact, 58.9% of the total responses indicated that they had not had any training of such sort, and 23% of them were not sure about it, leaving just 18.1% who reported to have gone through computer security training in the past. These findings ring an alarm as there is need for tertiary institutions to either boost up their already existing security practices or should set up active ones. The second item measured if there was an established cybersecurity policy in the institutions where they were currently studying (M=3.29; SD=0.907). From the responses gathered, a fair

proportion of them, around 42.3% reported that their institutions have such in place, however still bulk of 57.8 were either not sure or were sure that nothing of such was in their institution. Hence, this calls for the institutions to make awareness of their security policies to the entire institution community. Furthermore, when being asked if their institution provided cybersecurity training for students (M= 2.72; SD=0.987), the responses was absolutely discouraging as bulk of them, around 79.1% stated that no training of such is being provided by their institutions. Finally, when being asked if their institutions made provision of security-based articles or newsletters for the student's consumption, it was actually found out that yet a majority, around 72.4% either disagreed or remained neutral in such statement.

Thus, as a way of concluding the insights, it is clear that the responses of the students in regard to the selected two factors of the cybersecurity model, does not seem to be favourable, and hence needs urgent action by respective tertiary institutions around the country, as this study has been conducted within Malaysia. More recommendations would be made in the final section.

### 5.4 Contributions

The following major contributions have been made by this study.

- This study contributes by giving a clear exploration as to what extent age, gender and educational level plays a role in moderating the factors that affect cybersecurity beliefs and behaviours.
- It have been discovered that Prior Experiences with Security practices have proven to be very relevant and achieved a significant relationship with the Cybersecurity Behaviours of Tertiary Institution Students, hence the need for tertiary institutions to implement and ensure adequate cybersecurity policies.

- ❖ The research model can serve as guide/framework to Tertiary Institution Researcher's that are interested in conducting cybersecurity behavioural studies among the tertiary institutions students, by improving on the current model, or replicating it in other institutions, or environment.
- ❖ The Study provides lot of recommendations for Tertiary Institutions to implement active Cybersecurity training centres and enforce cybersecurity policies that boost a good cybersecurity assurance.
- ❖ The results from the research instigates the need for formal cybersecurity training for students in the Tertiary Institutions.

### 5.5 Study Limitations

Every study would definitely have some drawbacks or limitations due to certain constraints, hence this study is not an exception as it encountered some limitations in the course of its conduct. The first limitation of this research is regarding the time duration. There was not enough time to conduct the research, hence this served as a restraint to limit the weight of the research, as there was no opportunity to investigate other cybersecurity factors, apart from those used. Yet another limitation that was encountered is the inability to actually interact directly as this was a quantitative research, hence making it not quite possible to actually measure their exact cybersecurity behaviours. Perhaps, an experimental approach would have given clearer insights to how the users really behave with regards to their cybersecurity.

### 5.6 Recommendations and Future Work

This research is finally coming to a close, however there are recommendations and future work that can be done on this research area. The first recommendation would be the need and urgency to implement working and effective cybersecurity policies in higher institutions around Malaysia, and in extension to other tertiary institutions all over the

world. This is so because as the students keep getting familiar with the right thing to do when being faced with cyber-threats or cybersecurity issues, it would actually help in increasing their cybersecurity assurance and behaviour as well. Also, institutions can make use of their centralised emailing systems to always send regular security newsletters, articles or updates to the students' emails as this might also be a form of awareness. It is obvious that students make little mistakes which could affect their cybersecurity, if they are always reminded of the dangers, they could be forewarned as well as forearmed. Technical solutions are not enough to ensure good cybersecurity, but rather the building up of good cybersecurity behaviours is of more importance.

Future work in this area can think of conducting this research on a larger population, with the proposed model in this research. Also, future work can modify the model and add other constructs such as Perceived Risks, Trust, Fear, amongst others, to see if they affect cybersecurity behaviours of students. Other factors such as social media usage, duration of daily Internet usage, as well as, level of Internet expertise could be used as moderating factors in checking if they effect the relationships of the Cybersecurity model of tertiary institution students. Finally, regarding future work, other factors such as cultural background, academic performance, and health related factors could be tested on the cybersecurity behaviours of students in the tertiary institutions.

In conclusion, it has been discovered that the influencing factors of cybersecurity behaviours of tertiary institutions students are: Prior Experience with Computer Security Practices (the highest influence), Security Self-Efficacy, Response Efficacy, and Perceived Benefits. Also, it was found that gender and educational level have some effect on some of the factors of the cybersecurity behaviours, hence seeing the need perhaps to organize group-based training for the groups who might be lacking more. Finally, it was also discovered that all the factors of the cybersecurity behavioural scale were related to

cybersecurity behaviour of the tertiary institution students, except that of Perceived Severity, which has been dropped from the research model. However, it is not clear as to why it wasn't related in this research, hence giving room for future research to test it out on other population. Hence, if the appropriate and right security practices are being upheld and put in place by various tertiary institutions, it would help in securing both the servers of such institutions, the students, and the entire institution.

## REFERENCES


Acquisti, A., & Grossklags, J. (2004). Privacy attitudes and privacy behavior *Economics of information security* (pp. 165-178): Springer.

Addae, J. H., Brown, M., Sun, X., Towey, D., & Radenkovic, M. (2017). Measuring attitude towards personal data for adaptive cybersecurity. *Information and Computer Security, 25*(5), 560-579. doi: 10.1108/ics-11-2016-0085

Al-Mahrouqi, A., Abdalla, S., & Kechadi, T. (2015). Cyberspace Forensics Readiness and Security Awareness Model. *Int. J. Adv. Comput. Sci. Appl, 6*, 123-127.

Anderson, C. L., & Agarwal, R. (2006). *Practicing safe computing: Message framing, self-view, and home computer user security behavior intentions.* Paper presented at the ICIS 2006 Proceedings - Twenty Seventh International Conference on Information Systems.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437-443. doi: 10.1016/j.chb.2016.12.040

Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior, 38*, 304-312. doi: https://doi.org/10.1016/j.chb.2014.05.046

Aytes, K., & Connolly, T. (2005). Computer security and risky computing practices: A rational choice perspective *Advanced Topics in End User Computing* (Vol. 4, pp. 257-279).

Becker, M. H., Radius, S. M., Rosenstock, I. M., Drachman, R. H., Schuberth, K. C., & Teets, K. C. (1978). Compliance with a medical regimen for asthma: a test of the health belief model. *Public Health Reports, 93*(3), 268-277.

Bennett, S., & Maton, K. (2010). Beyond the 'digital natives' debate: Towards a more nuanced understanding of students' technology experiences. *Journal of computer assisted learning, 26*(5), 321-331.

Blais, A. R., & Weber, E. U. (2006). A Domain-Specific Risk-Taking (DOSPERT) scale for adult populations. *Judgment and Decision Making Journal, 1*(1), 33-47.

Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior, 87*, 87-97. doi: 10.1016/j.chb.2018.05.023

Blythe, J. M., Coventry, L. M., & Little, L. (2015). *Unpacking Security Policy Compliance: The Motivators and Barriers of Employees' Security Behaviors.* Paper presented at the SOUPS.

Bonneau, J., Herley, C., Oorschot, P. C. v., & Stajano, F. (2012, 20-23 May 2012). *The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes.* Paper presented at the 2012 IEEE Symposium on Security and Privacy.

Brinton Anderson, B., Vance, A., Kirwan, C. B., Eargle, D., & Jenkins, J. L. (2016). How users perceive and respond to security messages: a NeuroIS research agenda and empirical study. *European Journal of Information Systems, 25*(4), 364-390.

Caulkins, B., Marlowe, T., & Reardon, A. (2019) Cybersecurity Skills to Address Today's Threats. *Vol. 782. Advances in Intelligent Systems and Computing* (pp. 187-192).

Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S., & Raghav Rao, H. (2016). Online shopping intention in the context of data breach in online retail stores: An examination of older and younger adults. *Decision Support Systems, 83*, 47-56. doi: https://doi.org/10.1016/j.dss.2015.12.007

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy and Security, 1*(3), 18-41. doi: 10.1080/15536548.2005.10855772

Coffey, J. W. (2017). *Ameliorating Sources of Human Error in CyberSecurity: Technological and Human-Centered Approaches.* Paper presented at the The 8th International Multi-Conference on Complexity, Informatics and Cybernetics, Pensacola.

Cohen, P., West, S. G., & Aiken, L. S. (2014). *Applied multiple regression/correlation analysis for the behavioral sciences*: Psychology Press.

Davinson, N., & Sillence, E. (2010). It won't happen to me: Promoting secure behaviour among Internet users. *Computers in Human Behavior, 26*(6), 1739-1747. doi: https://doi.org/10.1016/j.chb.2010.06.023

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal, 19*(4), 391-412.

Dodel, M., & Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human Behavior, 68*, 359-367.

Dodel, M., & Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors. *Information, Communication & Society, 21*(5), 712-728.

Egelman, S., & Peer, E. (2015). Predicting privacy and security attitudes. *ACM SIGCAS Computers and Society, 45*(1), 22-28.

Egelman, S., Peer, E., & Assoc Comp, M. (2015). *Scaling the Security Wall Developing a Security Behavior Intentions Scale (SeBIS)*.

Furnell, S., Bryant, P., & Phippen, A. D. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security, 26*(5), 410-417.

Furnell, S., Tsaganidi, V., & Phippen, A. (2008). Security beliefs and barriers for novice Internet users. *Computers & Security, 27*(7-8), 235-240.

Garg, V., & Camp, J. (2012). *End user perception of online risk under uncertainty.* Paper presented at the System Science (HICSS), 2012 45th Hawaii International Conference on.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers and Security, 73*, 345-358. doi: 10.1016/j.cose.2017.11.015

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, 345-358.

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

Hadlington, L. (2018). The "human factor" in cybersecurity: Exploring the accidental insider *Psychological and Behavioral Examinations in Cyber Security* (pp. 46-63).

Hadlington, L., & Murphy, K. (2018). Is Media Multitasking Good for Cybersecurity? Exploring the Relationship Between Media Multitasking and Everyday Cognitive Failures on Self-Reported Risky Cybersecurity Behaviors. *Cyberpsychology, Behavior, and Social Networking, 21*(3), 168-172.

Halevi, T., Memon, N., Lewis, J., Kumaraguru, P., Arora, S., Dagar, N., . . . Chen, J. (2016). *Cultural and psychological factors in cyber-security*. Paper presented at the Proceedings of the 18th International Conference on Information Integration and Web-based Applications and Services, Singapore, Singapore.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Huang, D. L., Rau, P. L. P., & Salvendy, G. (2010). Perception of information security. *Behaviour and Information Technology, 29*(3), 221-232. doi: 10.1080/01449290701679361

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95. doi: https://doi.org/10.1016/j.cose.2011.10.007

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management, 51*(1), 69-79. doi: https://doi.org/10.1016/j.im.2013.10.001

Jeske, D., & van Schaik, P. (2016). Familiarity with threats, Internet experience and user behaviors.

Jeske, D., & van Schaik, P. (2017). Familiarity with Internet threats: Beyond awareness. *Computers & Security, 66*, 129-141.

Kearney, W. D., & Kruger, H. A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? *Computers & Security, 61*, 46-58.

Kelley, D. (2018). Investigation of Attitudes Towards Security Behaviors. *McNair Research Journal SJSU, 14*(1), 10.

Kelley, T., Amon, M. J., & Bertenthal, B. I. (2018). Statistical models for predicting threat detection from human behavior. *Frontiers in Psychology, 9*(APR). doi: 10.3389/fpsyg.2018.00466

Kruger, H., Drevin, L., & Steyn, T. (2010). A vocabulary test to assess information security awareness. *Information Management & Computer Security, 18*(5), 316-327.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469-479. doi: 10.1016/0022-1031(83)90023-9

McCall, C. H. (1982). *Sampling and statistics handbook for research*: Iowa State University Press Ames.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69*, 151-156.

Mohamed, N., & Ahmad, I. H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia.

*Computers in Human Behavior, 28*(6), 2366-2375. doi: https://doi.org/10.1016/j.chb.2012.07.008

Mohebzada, J., El Zarka, A., BHojani, A. H., & Darwish, A. (2012). *Phishing in a university community: Two large scale phishing experiments.* Paper presented at the Innovations in Information Technology (IIT), 2012 International Conference on.

Montano, D. E., & Kasprzyk, D. (2015). Theory of reasoned action, theory of planned behavior, and the integrated behavioral model. *Health behavior: Theory, research and practice*, 95-124.

Neter, J., Wasserman, W., & Kutner, M. H. (1985). Applied linear statistical models: Regression, analysis of variance, and experimental designs, Homewood, IL: Richard D. Irwin. *Inc.[701]*.

Neter, J., Wasserman, W., & Kutner, M. H. (1989). Applied linear regression models.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825. doi: https://doi.org/10.1016/j.dss.2008.11.010

Ng, B.-Y., & Xu, Y. C. (2007). Studying Users' Computer Security Behavior Using the Health Belief Model.

Noureddine, M. A., Marturano, A., Keefe, K., Bashir, M., & Sanders, W. H. (2017). *Accounting for the Human User in Predictive Security Models.* Paper presented at the Dependable Computing (PRDC), 2017 IEEE 22nd Pacific Rim International Symposium on.

Ogutcu, G., Tastik, O. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83-93. doi: 10.1016/j.cose.2015.10.002

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security, 56*, 83-93.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers & Security, 31*(5), 673-680.

Patten, M. L., & Newhart, M. (2017). *Understanding research methods: An overview of the essentials*: Routledge.

Pattinson, M., Butavicius, M., Parsons, K., McCormac, A., & Calic, D. (2015). *Factors that Influence Information Security Behavior: An Australian Web-Based Study.* Paper presented at the International Conference on Human Aspects of Information Security, Privacy, and Trust.

Qualtrics. (2019). Calculating Sample Population Size from https://www.qualtrics.com/blog/calculating-sample-size/

Rajivan, P., Moriano, P., Kelley, T., & Camp, L. J. (2017). Factors in an end user security expertise instrument. *Information and Computer Security, 25*(2), 190-205. doi: 10.1108/ics-04-2017-0020

Rhee, H.-S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*(8), 816-826. doi: https://doi.org/10.1016/j.cose.2009.05.008

Rocha Flores, W., Holm, H., Svensson, G., & Ericsson, G. (2014). Using phishing experiments and scenario-based surveys to understand security behaviours in practice. *Information Management & Computer Security, 22*(4), 393-406.

Safa, N. S., Solms, R. V., & Futcher, L. (2016). Human aspects of information security in organisations. *Computer Fraud and Security, 2016*(2), 15-18. doi: 10.1016/S1361-3723(16)30017-3

Sawyer, B. D., & Hancock, P. A. (2018). Hacking the Human: The Prevalence Paradox in Cybersecurity. *Human Factors, 60*(5), 597-609. doi: 10.1177/0018720818780472

Schulenberg, S. E., Yutrzenka, B. A., & Gohm, C. L. (2006). The computer aversion, attitudes, and familiarity index (CAAFI): A measure for the study of computer-related constructs. *Journal of Educational Computing Research, 34*(2), 129-146.

Seckler, M., Heinz, S., Forde, S., Tuch, A. N., & Opwis, K. (2015). Trust and distrust on the web: User experiences and website characteristics. *Computers in Human Behavior, 45*, 39-50. doi: 10.1016/j.chb.2014.11.064

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. (2010). *Who falls for phish?: a demographic analysis of phishing susceptibility and effectiveness of interventions.* Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

Shih, D. H., Lin, B., Chiang, H. S., & Shih, M. H. (2008). Security aspects of mobile phone virus: a critical survey. *Industrial Management & Data Systems, 108*(4), 478-494. doi: doi:10.1108/02635570810868344

Smith, A. D. (2006). Exploring security and comfort issues associated with online banking. *International Journal of Electronic Finance, 1*(1), 18-48.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124-133.

Suleman, T., Burhan-Ul-Haq, H., & Zafar, S. (2017). User Trust on Online Social Network on the basis of Security and privacy. *International Journal for Electronic Crime Investigation*, 35.

Sun, Y., Wang, N., Shen, X.-L., & Zhang, J. X. (2015). Location information disclosure in location-based social network services: Privacy calculus, benefit structure, and gender differences. *Computers in Human Behavior, 52*, 278-292.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management, 49*(3-4), 190-198.

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

Wang, P. A. (2013). *Assessment of cybersecurity knowledge and behavior: an anti-phishing scenario.* Paper presented at the International Conference on Internet Monitoring and Protection (ICIMP).

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking, 18*(1), 3-7.

Yan, Z., Robertson, T., Yan, R., Park, S. Y., Bordoff, S., Chen, Q., & Sprissler, E. (2018). Finding the weakest links in the weakest link: How well do undergraduate students make cybersecurity judgment? *Computers in Human Behavior, 84*, 375-382.

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security, 17*(4), 330-340.