DEVELOPMENT OF A PROTECTION MOTIVATION THEORY BASED QUESTIONNAIRE FOR MEASURING PARENTAL DIGITAL SECURITY PRACTICE IN MALAYSIA

MUHD ZULFADLI HAFIZ ISMAIL

THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE
REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PUBLIC HEALTH

FACULTY OF MEDICINE

UNIVERSITY OF MALAYA

KUALA LUMPUR

2020

UNIVERSITY OF MALAYA
ORIGINAL LITERARY WORK DECLARATION

Name of Candidate: **MUHD ZULFADLI HAFIZ BIN ISMAIL**

Name of Degree: **DOCTOR OF PUBLIC HEALTH**

Title of Project Paper/Research Report/Dissertation/Thesis ("this Work"):

DEVELOPMENT OF A PROTECTION MOTIVATION THEORY BASED QUESTIONNAIRE FOR MEASURING PARENTAL DIGITAL SECURITY PRACTICE IN MALAYSIA

Field of Study: **FAMILY HEALTH**

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:

ABSTRACT

Knowledge on parental digital security, which is the parental practice of maintaining the safety of their children online, is crucial to produce good digital citizens. Protection motivation theory (PMT) is a useful theoretical model for explaining protective behaviour and understanding this practice. Many studies and tools for exploring protective behaviour have been produced based on PMT, but there is no assessment tool available for assessing parents' digital security practice in the Malaysian context. Thus, the development of an assessment tool that reflects Malaysian parents' digital security practice based on established frameworks such as the PMT is essential. Therefore, this study attempted to develop a PMT-based instrument for measuring the digital security practice of Malaysian parents and to explain the factors that determine these practices based on the PMT domains. The study was conducted over 2 years from January 2018 to December 2019. It consisted of three major phases: item development, scale development and scale evaluation. Item development consisted of domain identification, item generation, content validity and translation, and involved a systematic review of the literature and engagement with experts and stakeholders. Scale development focused on pretesting, test-retest reliability and pilot testing for exploratory factor analysis. Scale evaluation involved path analysis of the domains and confirmatory factor analysis. The scale development and scale evaluation phases involved Malaysian parents with children below 18-years-old who were selected through purposive sampling, which involved two government clinics in Selangor, three private clinics, one each in Selangor, Perlis and Sabah, and three workplaces in the Klang Valley. The output item development was a bilingual 54-item questionnaire covering seven domains: *perceived susceptibility, perceived severity, perceived self-efficacy, perceived response efficacy, perceived maladaptive reward, perceived response cost* and *parental digital security practice*. Scale development resulted in three items being dropped due to poor reliability and poor loading, and nine domains: *perceived susceptibility, perceived severity, perceived self-efficacy, perceived response efficacy, perceived tangible cost, perceived psychological cost, perceived maladaptive reward, discursive digital security practice* and *control digital security practice*. In the scale evaluation phase, the remaining 51 items showed good discriminant and convergent validity, and both measurement and structural model assessment of the domains were adequate. Further analysis revealed that *perceived self-efficacy* (β= 0.30, $p < 0.001$), *perceived response efficacy* (β= 0.20, p=0.01) and *perceived maladaptive reward* (β=-0.20, $p < 0.001$) to be significant determinants of parental digital security practice. The model was able to explain 34% variation of parental digital security practice. The study contributes to knowledge by producing a validated instrument for measuring parental digital security practice in Malaysia. It also identifies the major determinants of parental digital security practice based on the PMT domains. The validated instrument has the potential to be utilised further to understand cyber parenting practices in general. The study also highlights that efforts need to be made to improve parental efficacy and reduce their perceived maladaptive rewards to keep their children safe online because these factors have a major influence on the effectiveness of parental digital security practice.

Keywords: Cyber parenting, digital, citizenship, security, protection motivation theory.

.

Tajuk: Pembangunan Alat Soal Selidik Berdasarkan Teori Motivasi Perlindungan Dalam Meneroka Keselamatan Digital Keibubapaan Di Malaysia

ABSTRAK

Pengetahuan keibubapaan tentang keselamatan digital merupakan satu tanggungjawab bagi melahirkan anak-anak serta warga digital yang baik. Teori Motivasi Perlindungan (PMT) merupakan satu teori model yang digunakan untuk menerangkan tingkah laku perlindungan dan memahami amalan keibubapaan tentang keselamatan digital. Terdapat banyak penyelidikan dan bahan kajian yang dihasilkan berdasarkan PMT berkenaan tingkah laku perlindungan, namun tiada kajian yang khusus ditemui dalam mengukur tahap kefahaman keibubapaan tentang keselamatan digital di kalangan ibu bapa di Malaysia. Maka, penghasilan alat pengukur yang mencerminkan keselamatan digital keibubapaan berdasarkan teori seperti PMT adalah penting untuk memahami amalan ini dengan lebih baik di Malaysia. Kajian ini dijalankan untuk membangunkan satu alat yang mengukur amalan keibubapaan tentang keselamatan digital di kalangan ibu bapa di Malaysia dan menerangkan faktor yang menentukan amalan ini berdasarkan domain-domain PMT. Kajian ini dijalankan sepanjang 2 tahun dari Januari 2018 hingga Disember 2019. Kajian ini merangkumi tiga fasa utama; pembangunan item, pembangunan skala, dan penilaian skala. Pembangunan item melibatkan pengenalan domain, penjanaan item, kesahan kandungan dan terjemahan. Fasa ini melibatkan semakan sistematik dan penglibatan bersama pemegang taruh dan pakar. Pembangunan skala melibatkan ujian pra, kestabilan kebolehpercayaan, dan ujian rintis untuk analisis faktor penerokaan. Penilaian skala melibatkan analisis laluan domain-domain terlibat dalam analisis faktor pengesahan. Fasa pembangunan dan penilaian skala melibatkan ibu bapa warganegara Malaysia yang mempunyai anak berumur 18 tahun ke bawah secara persampelan. Persampelan ini melibatkan dua klinik kesihatan kerajaan di Selangor, tiga klinik swasta masing-masing di Selangor, Perlis dan Sabah, dan tiga tempat kerja di Lembah Klang. Fasa pembangunan item telah menghasilkan soal selidik yang mengandungi 54 item dwibahasa. Soal selidik ini merangkumi tujuh domain, iaitu tanggapan kerentanan, tanggapan keterukan, tanggapan efikasi kendiri, tanggapan efikasi gerak balas, tanggapan ganjaran maladaptive, tanggapan kos gerak balas, dan amalan keselamatan digital kawalan. Dalam fasa pembangunan skala, tiga item telah dikeluarkan kerana mempunyai kebolehpercayaan yang lemah. Sembilan domain telah dihasilkan dalam fasa ini, iaitu tanggapan kerentanan, tanggapan keterukan, tanggapan efikasi kendiri, tanggapan efikasi gerak balas, tanggapan kos ketara, tanggapan kos psikologi, tanggapan ganjaran maladaptif, amalan keselamatan digital diskursif, dan amalan keselamatan digital kawalan. Dalam fasa penilaian skala, 51 item yang kekal menunjukkan kesahan yang berbeza dan tertumpu. Penilaian domain dalam model yang terhasil, daripada segi struktur dan pengukuran juga adalah mencukupi. Analisis juga menunjukkan tanggapan efikasi kendiri ($\beta = 0.30$, $p < 0.001$), tanggapan efikasi gerak balas ($\beta = 0.20$, $p = 0.01$), dan tanggapan ganjaran maladaptif ($\beta = -0.20$, $p < 0.001$) sebagai penentu-penentu penting terhadap amalan keselamatan digital keibubapaan. Model ini juga mampu menerangkan 34% variasi amalan keselamatan digital keibubapaan. Kajian ini telah berjaya menghasilkan instrumen yang sah dalam mengukur amalan keselamatan digital keibubapaan di Malaysia. Kajian ini juga mengetengahkan item-item penting dalam amalan ini, berdasarkan domain PMT. Instrumen ini mempunyai potensi untuk digunakan dalam memahami keibubapaan siber secara umum, dan usaha perlu diberi untuk meningkatkan efikasi dan mengurangkan tanggapan ganjaran maladaptif ibu bapa dalam memastikan anak mereka selamat di atas talian, di mana dua faktor ini telah didapati mempunyai pengaruh yang besar dalam amalan keibubapaan keselamatan digital.

Kata Kunci: Keibubapaan siber, digital, kewarganegaraan, keselamatan, Teori Motivasi Keselamatan

ACKNOWLEDGEMENTS

First and foremost, I am very grateful to Allah the Almighty for without His graces and blessings, this thesis would not have been possible.

I am highly indebted to Associate Professor Nik Daliana Nik Farid and Associate Professor Rafdzah Ahmad Zaki for their huge support, guidance, constant supervision, and providing sound advice to help me to complete this thesis. It was such an enjoyable and meaningful journey, and both of them played a major part in making it so.

I am very grateful to my main collaborators, namely, Edwan Aidid and Elina Mubin from CyberSecurity Malaysia, whose input and support throughout this journey have been a strong force in encouraging me to complete my thesis.

I would also like to express my gratitude to all my colleagues and friends who helped me throughout this study by providing the necessary guidance. The overall support they gave was a very humbling experience for me indeed.

Special thanks also to my professors, lecturers and all the staff working in the Department of Social and Preventive Medicine for their significance guidance and wisdom as well. This thesis would not have been possible without them.

I reserve my special thanks for my parents, Ismail bin Sulong and Wan Akmal binti Wan Endut, my mother-in-law, Rohani binti Yusof, my wife Shakirah binti Md. Sharif, my daughter Hana Sophia, and all my relatives for their support and understanding. They are my pillars of strength, and for that I am forever grateful.

Lastly, to my batchmates, this journey would not have been possible without the support I received from them. Thank you for being there through difficult moments. This success is yours as much as it is mine.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

AVE	Average Variance Extracted
CB-SEM	Covariance-Based Structural Equation Modelling
CCA	Confirmatory Composite Analysis
CFA	Confirmatory Factor Analysis
CITC	Corrected Item-Total Correlation
CSAT	Cybersecurity Awareness Talk
CSM	Cybersecurity Malaysia
EFA	Exploratory Factor Analysis
HBM	Health Belief Model
HTMT	Heterotrait-Monotrait
MCMC	Malaysian Communication and Multimedia Commission
PLS-SEM	Partial Least Squares Structural Equation Modelling
PMT	Protection Motivation Theory
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
SEM	Structural Equation Modelling
SEU	Subjective Expected Utility
SOP	Standard Operating Procedure
UNICEF	United Nations Children’s Fund
VIF	Variance Inflation Factor

OPERATIONAL DEFINITIONS

Term	Definition
Digital citizenship	Norms of appropriate, responsible behaviour regarding technology use by technology users (Ribble, 2015)
Digital etiquette	The electronic standards of conduct or procedure (Ribble, 2015)
Digital access	The connection a person has to resources, information and online opportunities, which shapes their digital participation in society (Ribble, 2015)
Digital law	Electronic responsibility for actions and needs (Ribble, 2015)
Digital literacy	Process of teaching and learning about technology and the use of technology (Ribble, 2015)
Digital communication	Practices of digital exchange of information (Ribble, 2015)
Digital commerce	Electronic buying and selling of goods (Ribble, 2015)
Digital rights and responsibilities	Requirements and freedoms extended to everyone in a digital world (Ribble, 2015)
Digital health and wellness	Physical and psychological well-being related to digital technology use (Ribble, 2015)
Digital security	Ability to maintain security and safety online (Ribble, 2015)
Self-efficacy	Ability to perform a behaviour (Maddux & Rogers, 1983)
Response efficacy	Belief in the effectiveness of the behaviour (Maddux & Rogers, 1983)
Response cost	The cost, not necessarily in monetary terms, that a person has to bear when adopting a protective behaviour (Boehmer, LaRose, Rifon, Alhabash, & Cotten, 2015a)
Susceptibility	The perceived likelihood of the individual being affected by potential negative consequences (Maddux & Rogers, 1983)
Maladaptive reward	The positive effect of not performing protective behaviour (MacDonell et al., 2013)
Severity	The magnitude of the negative consequences of not performing protective behaviour (MacDonell et al., 2013)
Active mediation	Sharing of information, commenting on contents and providing advice to children on using the internet (Nikken & Jansz, 2014)
Restrictive mediation	Imposing rules and control over time spent online by children and the content children are allowed to use (Nikken & Jansz, 2014)
Co-use mediation	Parents and their children using the internet together at the same time, and sharing the experience together (Nikken & Jansz, 2014)
Supervision mediation	Children are allowed to use the internet on his/her own, but with the presence of their parents nearby (Nikken & Jansz, 2014)
Monitoring mediation	Parents checking their children's online activities after usage (Nikken & Jansz, 2014)

LIST OF APPENDICES

CHAPTER ONE: INTRODUCTION

1.1 Introduction

This chapter starts by explaining the broad concept of digital citizenship which serves as the foundation for this study. Following this, the chapter zooms into the concept of digital security, before focusing further on the concept of parental digital security which is the main concept addressed in this study. The chapter continues by looking into the situational analysis of the issue under study and the health implications related to poor online practices among children and adolescents, which are an indirect result of poor parental digital security practice. Next, the study rationale is presented, followed by clarifying why there is a need for a theory-based questionnaire to investigate this issue in the Malaysian context, which is the main aim of this study. Then, the research questions and study objectives are presented, and lastly, an outline of the thesis is provided, followed by a summary of the chapter.

1.2 Digital Citizenship, Digital Security and Parental Digital Security

1.2.1 Digital Citizenship

The term 'citizen' is "most commonly defined as a native or naturalised person who owes allegiance to a larger state or collective and who shares in the rights and responsibilities afforded by all members of that collective" (Ribble, 2015, p. 7). In the digital world, the term 'digital citizens' can then be extended to denote "individuals who actively participate in an online community at a local, global, and digital level simultaneously" (Curran, 2017, p. 36). Further, the 'digital citizenship' concept can be defined as the "norms of appropriate, responsible behaviour regarding technology use by technology users" (Ribble, 2015, p. 15). Similarly, Lyons (2011) has defined digital citizenship as "a subset of citizenship, [which] supports responsible actions when using technology" (p. 40). Thus, digital citizenship emphasises the responsible and appropriate usage of technology and is the overarching concept of interest to this study.

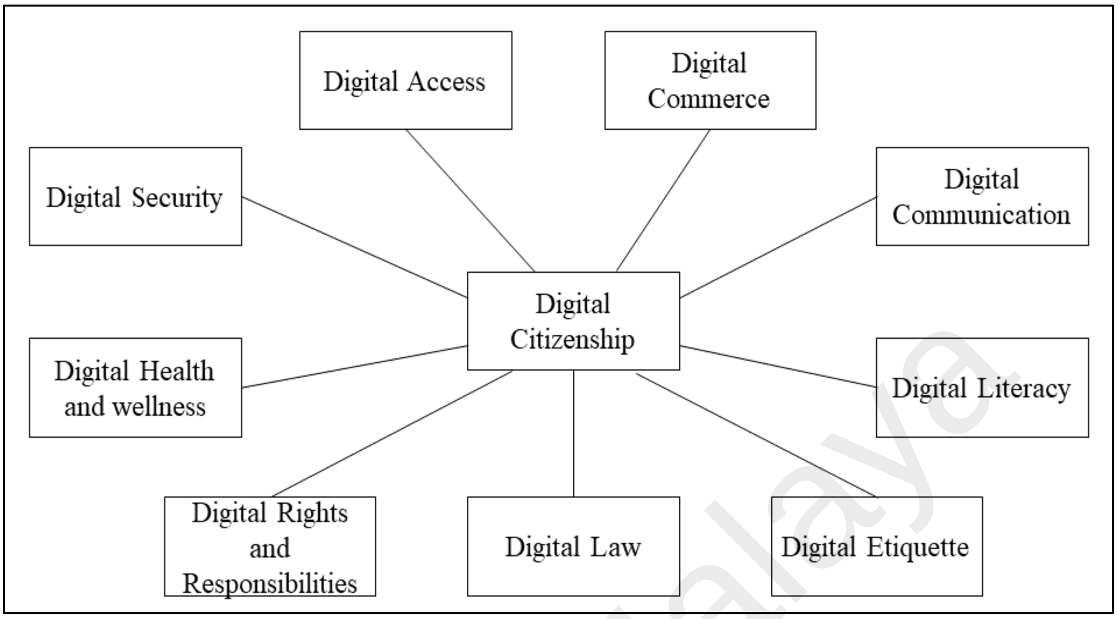

Figure 1.1: Digital citizenship framework

Adapted from: *Ribble, M. (2015).* Digital Citizenship in Schools*: International Society for Technology in Education.*

According to Ribble (2015), there are nine elements of digital citizenship: digital access, digital commerce, digital communication, digital literacy, digital etiquette, digital law, digital rights and responsibilities, digital health and wellness, and digital security (see Figure 1.1). These elements serve as a starting point for becoming good digital citizens (Ribble, 2015). Ribble (2015) emphasises that some of these nine elements may be of "more concern to technology leaders while others may be more of [a] focus for users" (p. 17), depending on the situation. On that note, in this study, not all of the nine elements are focused upon; rather, the focus is guided by public health needs in respect of digital issues.

One of the elements in the digital citizenship framework is digital etiquette. Digital etiquette is defined as "the electronic standards of conduct or procedure" (Ribble, 2015, p. 39). It concerns social norms and appropriate conduct when interacting with one another, which evolve with the development of technology (Ribble, 2016).

Another element is digital access, which refers to the “connection one has to resources, information and online opportunities, which will shape their digital participation in the society [sic]” (Ribble, 2015, p. 25). It emphasises the availability of opportunities for people to use technology, which is influenced by factors such as socioeconomic status, disabilities and physical location (Ribble, 2015).

A further element in the digital citizenship framework is digital law, which is defined as the “electronic responsibility for actions and needs” (Ribble, 2015, p. 42). Currently, it focuses on three main areas, namely, personal information collection and sharing; copyright issues; and criminal behaviour such as sharing inappropriate images and cyberbullying (Ribble, 2016).

On the other hand, the element digital literacy focuses on the “process of teaching and learning about technology and the use of technology” (Ribble, 2015, p. 35). Digital literacy requires the capability to use digital technologies, know-how and an understanding of when to use these technologies (Ribble, 2016). It also concerns the ability to understand information and evaluate it (Glister, 1997).

Digital communication is the element that refers to the practices involved in the digital exchange of information (Ribble, 2015). The various platforms of communication, such as cell phones, social networking and texting, have created a new social structure for interaction (Ribble, 2015). It also concerns the sharing of content in an effective and relevant manner (Ribble, 2016).

Meanwhile, the element digital commerce relates to the “electronic buying and selling of goods” (Ribble, 2015, p. 28). This element concerns the exposure of personal financial information, as well as the digital footprints that are created when purchasing online (Ribble, 2016).

Another element in the digital citizenship framework is digital rights and responsibilities, which is defined as the “requirements and freedoms extended to everyone in a digital world” (Ribble, 2015, p. 46). Digital rights must be understood and respected and digital responsibilities must be recognised by every digital user. These rights and responsibilities are guided by rules, regulations and acceptable-use policies (Ribble, 2015).

On the other hand, the digital health and wellness element focuses on “physical and psychological well-being related to digital technology use” (Ribble, 2015, p. 49). It addresses the balance a person needs to have between living in the real world and living online (Ribble, 2016).

The last element described in the framework is the digital security element. This refers to “electronic precautions to guarantee safety” (Ribble, 2015, p. 52). It involves having the technical ability to protect oneself from digital threats by using tools such as firewalls and antivirus software (Ribble, 2015). It also concerns the ability to make a judgement about revealing personal information online (Ribble, 2016).

1.2.2 Digital Security

Digital security is the element of interest to this study as it is essential in addressing public health needs in respect of digital issues, as demonstrated in subsequent sections. In the literature, the conceptualisation of digital security varies. However, generally, as proposed by Lorenz (2017), digital security is comprised of three interrelated concepts: information security, computer security, and digital safety. Information security and computer security focus on the technical measures taken to protect oneself from threats such as data corruption, confidentiality breaches and property theft (Lorenz, 2017). On the other hand, digital safety focuses on human interaction and behaviour when dealing with people and information online (Lorenz, 2017). Examples of online human interaction related to digital safety are internet crimes such as identity theft, stalking, cyberbullying and privacy breaches (Lorenz, 2017). Terms such as ‘internet safety’ and ‘electronic safety’ have also emerged in the literature, and reflect the idea of ‘self-protection’, which combines both the technical and behavioural aspects of security (Lorenz, 2017). A similar scope is used in this study, in which the term ‘digital security’ is used as the preferred terminology. Here, digital security is defined as the “ability to maintain security and safety online”, to reflect self-protection on both the technical and behavioural level, as implied in Ribble’s (2015) digital citizenship framework.

1.2.3 Parental Digital Security

This study further focuses on the parental aspect of digital security because the aspect of digital security is essential in promoting good child and adolescent health in regards to digital citizenship, which is an issue that will be discussed in subsequent sections. However, the concept of parental digital security is not properly defined in the literature. Moreover, while there are many guidelines on parental digital security that are available from established organisations around the world, the actions that these guidelines recommend that parents take to ensure the security and safety of their children are based only on internet mediation techniques (CommonSense, 2014; Connect Safely, 2015; CyberSecurity Malaysia, 2015; CyberSecurity Malaysia, 2017). Examples of such techniques are setting parental controls, installing filters, and giving advice to children on how to behave online safely (CommonSense, 2014; Connect Safely, 2015; CyberSecurity Malaysia, 2017; MediaSmarts, 2017). These mediation techniques include measures that require technical ability as well as address human interaction and behaviour online. As such, the inclusion of both type of measures by these guidelines is in line with the digital security definition adopted by this study. Therefore, parental digital security is defined here as the practices used by parents in maintaining the safety of their children online. Hence, the examination of parental digital security in this study will be heavily based on the internet mediation techniques used by parents.

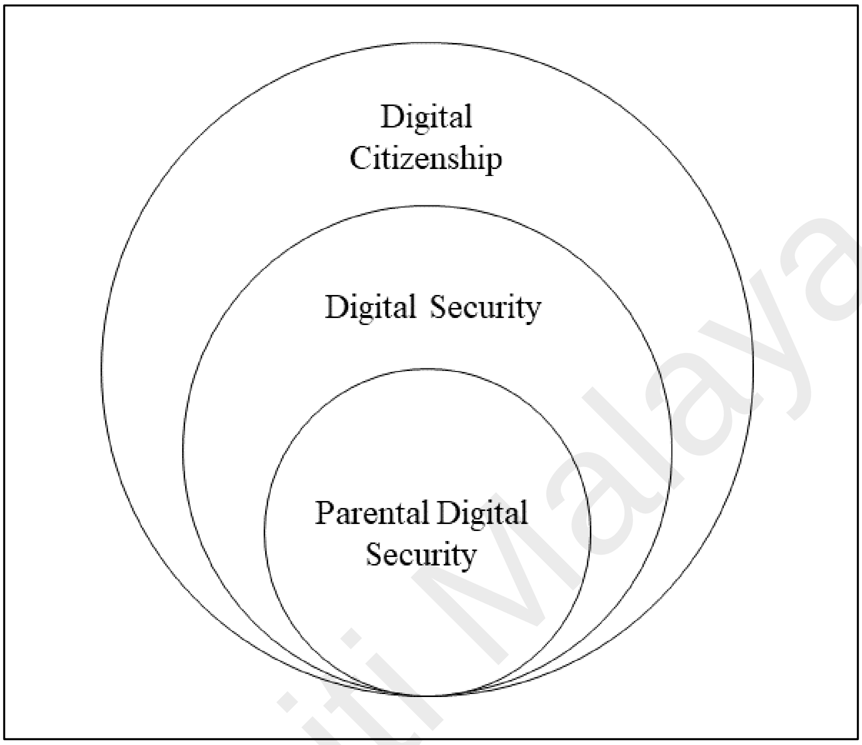

Figure 1.2: Scope of study

Figure 1.2 illustrates the scope of this study in which digital citizenship is the overarching concept and in which the focus is the digital security angle, which includes both the technical and behavioural aspects of self-protection. Specifically, this study examines parental digital security practice, which is based on internet mediation techniques.

1.3 Situational Analysis

The number of technology users globally has increased in recent years due to improved access to computers and the internet (Information Technology Union [ITU], 2018). Worldwide, an estimated 51.2% of the total population were internet users in 2018 (ITU, 2018). A similar trend was seen in the Asia Pacific region where 47% of the total population were internet users in 2018 (ITU, 2018).

In Malaysia, the percentage of internet users is noticeably higher; it was estimated that 87.4% of the total population were internet users in 2018, an increase from 76.9% in 2016 (Malaysian Communications and Multimedia Commission [MCMC], 2018). The survey also showed that most Malaysian internet users accessed the internet at their own house with a total percentage of 88.6% in 2018, an increase from 85.6% in 2016 (MCMC, 2018). Also, smartphones appeared to be the most popular device used to access the internet among Malaysians. A total of 93.1% of internet users in Malaysia used smartphones to go online in 2018, an increase from 89.4% in 2016 (MCMC, 2018). These statistics show that accessibility and internet activity in Malaysia has increased in recent years. This trend has led to increased exposure of young children and adolescents to the digital world as well. A survey conducted in Malaysia involving 18,000 participants aged 10–18 years old revealed that 96.5% of them used the internet, with 39% using it daily (Institute of Public Health [IPH], 2017). A similar trend has been found in other countries such as the United States of America (USA). For example, a nationwide survey in the United States of America by Pew Research Centre in 2018 has shown that up to 95% of teenagers aged 13-17 years old were internet users (Pew Research, 2018). Such findings highlight that internet usage among the younger generation is a common global phenomenon.

Increased exposure to the internet can pose a threat to children and adolescents, especially if they practise poor online behaviours, especially with regard to digital security. In Malaysia, a recent nationwide survey involving children aged 7–19 years old highlighted that 40% of them did not know how to protect themselves on the internet (CyberSecurity Malaysia, 2014). The survey also discovered that 83% of children did not take adequate action to protect themselves on the internet, with 30% of them taking no action or just one action to ensure their digital security (CyberSecurity Malaysia, 2014). Lack of adequate digital security measures, coupled with the growing use of internet, has led to concerns about the younger population being exposed to bullying, harmful content, internet addiction and predators online (United Nations Childrens Fund [UNICEF], 2014). The same survey also revealed that 26% of both primary and secondary school students in Malaysia had been cyberbullied at least once (CyberSecurity Malaysia, 2014). Another study involving 161 secondary school students in Perak, Malaysia showed that 28.6% of them were addicted to the internet (Isa, 2016). Moreover, a study involving 149 secondary school students in Selangor revealed that 50% of them had been exposed to pornography (Maha, 2010). The increased exposure of children and adolescents to the digital world, can thus potentially lead to many online threats to their health and well-being, especially because it seems that poor digital security measures are adopted by this population.

1.4 Health Implications

Online issues such as cyberbullying, sexting and internet addiction among children and adolescents are related to both mental and physical health problems. The World Health Organisation (WHO) has highlighted some of the potential health problems that could arise due to excessive use of the internet, including musculoskeletal problems due to poor posture, hearing problems due to exposure to harmful levels of sound, visual symptoms such as eyestrain, and insufficient physical activity, as well as injuries and accidents when users are distracted when surfing the internet using mobile electronic devices while doing other tasks (WHO, 2014). Moreover, Bannink et al. (2014) have highlighted that cyberbully-based victimisation of female school students is significantly related to mental health problems after controlling for baseline mental health (odds ratio [OR] 2.38; 95% confidence interval [CI] 1.45–3.91). Similarly, Bauman, Toomey, and Walker (2013) have also revealed being a cyberbully victim is a significant predictor of depression among female high school students ($p < 0.001$). The same study also showed that there is a significant association between cyberbullying and suicidal attempts among male high school students, after adjusting for depression ($p < 0.05$) (Bauman et al., 2013).

A meta-analysis by Sohn, Rees, Wildridge, Kalk, and Carter (2019) of 41 studies showed that there is a significant association between addiction to smartphone usage and depression (OR 3.17; 95% CI 2.30–4.37), perceived stress (OR 1.86; 95% CI 1.24–2.77), increased anxiety (OR 3.05; 95% CI 2.64–3.53) and poor sleep quality (OR 2.60; 95% CI 1.39–4.85). Moreover, a prospective study conducted among adolescents in China showed that those who are addicted to the internet have a higher risk of depression compared to those who are not (relative risk [RR] 2.50; 95% CI 1.3–4.3) (Lam & Peng, 2010). Another study in the United States of America (USA) revealed that there is a significant association between addiction to online games and attention deficit hyperactivity disorder in adolescents ($p < 0.05$) (Chan & Rabinowitz, 2006). Furthermore, a study conducted in South Koreaby Kim et al. (2010) showed that internet addiction among Korean adolescents is significantly associated with depression ($p < 0.05$) and suicidal ideation ($p < 0.05$). The study, which involved 853 junior high school children, also revealed that those who are at high risk of internet addiction have a significantly higher amount of irregular bedtimes ($p < 0.05$), higher usage of alcohol ($p < 0.05$) and higher usage of tobacco ($p < 0.05$) compared to those who do not have a risk of internet addiction (Kim et al., 2010). The study further highlighted that users with a high risk of internet addiction have poorer dietary behaviour compared to those with no risk of internet addiction, as demonstrated by loss of appetite ($p < 0.05$), high frequency of skipping meals ($p < 0.05$) and snacking ($p < 0.05$) (Kim et al., 2010).

Furthermore, a review article by Flood (2009) has highlighted that children and adolescents who view pornographic material online are more likely to engage in riskier sexual acts and experience sexual activity at an earlier age. The same study also stated that exposure to pornography online may also encourage adolescents to commit sexual assault because they were more susceptible to endorsing the violent attitudes seen in pornography itself (Flood, 2009). These findings imply that viewing pornography online may have a profound effect on the sexual and reproductive health of children and adolescents.

1.5 The Need for an Understanding of Parental Digital Security Practice

Adults, including parents, play a major role in empowering children to practise responsible online usage (CyberSecurity Malaysia, 2014). Appropriate cyber parenting practice can help to curb poor online behaviours and thereby reduce cyber issues among children and young adolescents (CyberSecurity Malaysia, 2014). As shown by the results of a survey conducted among children aged 7–18 years old, 61% of them would confide in their parents if they had a negative internet experience (CyberSecurity Malaysia, 2014). Moreover, another survey highlighted that children who are cyberbullied have a higher likelihood of seeking help from parents: on a scale of 1 to 5, the children who were surveyed scored 3.99 for the statement "If I am bullied on the internet, my parents will help me" (CyberSecurity Malaysia, 2015). These findings show that parents are a major source of guidance for children, especially when children have negative experiences online.

However, parents themselves might have poor knowledge and practice with respect to parental digital security, which would hinder their ability to guide their children on positive and safe online experiences. Indeed, this is an issue of growing concern because a survey has shown that there was an increase in the prevalence of parents who were not confident in their ability to control their children's use of technology, from 10% in 2014 to 15% in 2015 (Family Online Safety Institute [FOSI], 2015). Moreover, the same survey also highlighted that 18% of parents are not sure about how to use parental control features (FOSI, 2015). Hence, there is a mismatch between the demand for guidance from children and the readiness of parents to engage in parental digital security practice. Specifically, these findings show that there is still a gap that needs to be addressed with regards to capacity-building among parents in respect of parental digital security for their children, and in respect of cyber parenting in general. However, a report by UNICEF highlighted that there are limited sources on the views of parents in Malaysia on and around the issue of cyber parenting (UNICEF, 2014). Therefore, there is an urgent need to produce more knowledge and evidence on cyber parenting, and particularly on parental digital security from parents' point of view.

1.6 The Need for a Theory-based Questionnaire

In light of the above-identified need to understand and produce evidence on parental digital security practice in Malaysia, it is crucial that studies based on established frameworks, models and theories are conducted on this topic. This is because such studies will provide a strong foundation and a blueprint for firstly understanding the aspects of the issue that need to be tackled, in this case parental digital security practice. Following this, suitable interventions can be designed, evaluated and improved (Glanz, Rimer, & Viswanath, 2008). Programmes which are based on established frameworks, models and theories can also facilitate the implementation and expansion of the utilisation of such programmes, hence improving their sustainability (Van Belle, van de Pas, & Marchal, 2017).

In this study, the main theory that is used to understand parental digital security practice is protection motivation theory (PMT), which is a fear appeal cognitive-based theory, developed by Maddux and Rogers (1983). This theory focuses mainly on the threat and coping appraisal components of the cognitive processes. Using a cognitive-based theory as the foundation of this study will help to gain an understanding of the intrapersonal factors that affect parental digital security practice. The relevance of focusing on intrapersonal factors, namely, the cognitive processes of both threat and coping appraisal, as well as the selection of this theory for this study are further discussed in Chapter Two.

Additionally, in order to embed the components of these established frameworks, models and theories in this study, suitable measurement tools that represent these components need to be present. Not only must these measurement tools be comprehensive enough to represent the components, they also need to be valid as well. Validated measurement tools are important because they ensure that the findings are measured in a true and accurate manner. However, a systematic review conducted for this study, the details of which can be found in Chapter Three and Chapter Four, reveals the lack of a PMT-based tool for measuring parental digital security practice. Hence, for this study, it is imperative to firstly design a validated questionnaire that is able to measure parental digital security practice based on PMT, and secondly, to use this questionnaire to measure parental digital security practices, and then explain the results using the components of this theory.

1.7 Study Rationale

The situational analysis, health implications, and the importance of understanding parental digital security practice and the need to develop of a theory-based questionnaire have been demonstrated in the previous sections of this chapter. This background information underpins the rationale for conducting this study. Essentially, good parental digital security practice among parents in Malaysia will help their children to become good digital citizens, and thereby reduce the public health burden due to poor online usage among the population.

However, currently, there is a lack of information from which to gain a full understanding of parental digital security practice from parents' perspectives, and there is also an absence of a validated tool to measure parental digital security practice among Malaysian parents. These gaps are hindering progress on producing parents with good digital security practices because their needs with regard to this issue are not being assessed comprehensively. Hence, this study intends to address these gaps by producing a validated tool by which to understand parental digital security practice among Malaysian parents as well as to gain an understanding of the cognitive factors influencing this practice by using an established theory, namely, PMT. By doing so, parents' needs in relation to digital security practice can be understood better, and measures can then be taken to instil parents with good cyber parenting skills.

1.8 Research Questions

Based on the situational background elaborated in the previous sections, three main research questions were developed:

1. How do we measure parental digital security practice among Malaysian parents?
2. What are the factors that influence parental digital security practice among Malaysian parents?
3. How suitable is PMT for explaining parental digital security practice among Malaysian parents?

1.9 Study Objectives

In order to answer the above research questions, the following study objectives were defined:

1.9.1 General Objective

To develop a PMT-based instrument for measuring parental digital security practice among Malaysian parents and to explain the factors that determine their practice based on the PMT domains.

1.9.2 Specific Objectives

1. To assess the quality of existing PMT-based questionnaires on digital security in terms of item development, reliability and validity;
2. To identify items to be included in the parental digital security questionnaire for Malaysian parents;

3. To establish the validity and reliability of the parental digital security questionnaire for Malaysian parents;
4. To determine the relationship between the domains identified in order to explain parental digital security practice among Malaysian parents.

1.10 Thesis Outline

The thesis consists of six main chapters including this introduction as Chapter One. The subsequent paragraphs describe the outline of the remaining chapters of this thesis.

Chapter Two presents the literature review conducted for this study, which looks into the factors that determine the digital security practice of adults, the factors that influence parents to protect their children online, and the existing questionnaires on parental digital security practice, and which provides the foundations for the theoretical and conceptual framework developed for this study. This chapter also discusses the gaps identified in the literature that this study aims to address.

Chapter Three explains the methods used in this study and describes the process of questionnaire development and validation. This chapter consists of four sections which cover the overall research design and describe the various phases in the research process, the population involved, the instrumentation used and the type of analysis employed for each of the stages in the questionnaire development and validation process.

Chapter Four presents the results of the study. The results are presented in accordance with the stages in the questionnaire development and validation process, namely, item development, scale development and scale evaluation.

Chapter Five discusses the results of the study. It also describes how the findings could be utilised, their research implications, and their public health and policy implications. The chapter also highlights the contributions as well as the strengths and limitations of the study. The chapter ends by discussing the policy and research recommendations from the study.

Chapter Six concludes the thesis by summing up the main findings of the study, as well as the lessons learned from conducting this study. The thesis content is summarised in Table 1.1.

Table 1.1: Thesis content by chapter

Chapter	**Content**
Chapter One: Introduction	Digital citizenship concept, parental digital security concept, situational analysis, health implications, study rationale, research questions, objectives, outline of thesis
Chapter Two: Literature review	Factors influencing adults' and parents' digital security practice, existing tools for digital security practice, theoretical and conceptual framework
Chapter Three: Methodology	Overall research design, population, sample, data collection process, instrumentation, analysis
Chapter Four: Results	Findings for each stage of the research, namely, item development, scale development, and scale evaluation
Chapter Five: Discussion	Interpretation of the research findings, utilisation of the study findings, public health and policy implications, research significance, limitations and strengths, policy and research recommendations.
Chapter Six: Conclusion	Conclusions based on the research findings, and lessons learned from conducting the study

1.11 Summary of Chapter One

This chapter provided an overview of the nine components of digital citizenship, before zooming into digital security, which is one of the components of digital citizenship. Adopting this concept, parental digital security was described as the practice by parents of maintaining the safety of their children online. Then a situational analysis was presented that revealed that increasing numbers of children and adolescents in Malaysia and worldwide are using the internet. The analysis also highlighted the worrying trend of poor online usage among this population. The health implications caused by poor online practices among children and adolescents were then explained, including musculoskeletal, vision, hearing, poor lifestyle, depression and suicide issues. Following this, the need to gain a fuller understanding of parental digital security practice was highlighted by emphasising the importance of the parents' role in tackling the above issues due to poor online practices among children, as well as by drawing attention to the limited number of studies available for understanding parents' perspectives on digital security. Then, PMT was introduced briefly, before explaining the importance of using a theory-based questionnaire to gain a comprehensive understanding of digital security practice among Malaysian parents, which is the main orientation of this study. Following this, the study rationale was described, and the research questions and study objectives were presented, which centred on the development of a parental digital security practice questionnaire for Malaysian parents, and exploring the factors influencing their practice, particularly by using PMT-based components.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

The literature review presented in this chapter firstly focuses on the factors that influence an adult in performing digital security practice. Following that, the review extends to the factors that affect individuals when carrying out their parental role in mediating their children's safety online. Subsequently, the review explores the existing tools that are available for explaining parental digital security practice. The findings and gaps in the literature are then discussed. After that, the theoretical frameworks relevant to this study, which were identified through the literature review, are presented, followed by a justification of the selection of the main theoretical framework for this study. Lastly, the conceptual framework adopted for this study is presented and a brief summary of the chapter is provided.

2.2 Factors that Influence Adults' Digital Security Practice

The review of the literature conducted for this study revealed that two major factors influence an adult in performing digital security practice, namely, confidence in digital security and perceived online threats.

2.2.1 Confidence in Digital Security

Bubaš, Orehovački, and Konecki (2008) highlighted that internet users who are more aware of behaviour related to security and privacy online are more likely to encounter computer infections ($\beta = 0.22$; $p < 0.01$). This finding reflects their increased practice of checking for viruses and infections on their personal computers (PCs) due to their higher level of awareness. Also, Jeske and van Schaik (2017) revealed that familiarity with internet threats is positively associated with computer security behaviours ($\beta = 0.43$; $p < 0.001$). Knowledge on spyware also increases the likelihood of installing anti-spyware programmes ($\beta = 0.29$; $p < 0.001$), as highlighted by Kwak, Kizzier, and

Jung (2011). This finding is supported by Lee, Tan, and Siah (2017) who discovered that internet self-efficacy is significantly associated with online technical protection (β = 0.31; p < 0.001). Moreover, interestingly, Huang, Rau, and Salvendy (2010) showed that knowledge on internet threats appears to be negatively associated with the perceived danger of internet threats (β = -0.08; p < 0.001). This result could be explained by the notion that users with increased knowledge of internet security may be exposed to more internet threats because they perceive the danger of threats to be lower.

However, a few issues need to be highlighted in respect of these studies. Firstly, the study by Bubaš et al. (2008) involved participants who were college students enrolled in an information technology department. Similarly, in the study by Jeske and van Schaik (2017) the majority of the respondents were university students in the United Kingdom (UK) and the USA. Likewise, Kwak et al. (2011) recruited samples from among students in a university in the USA, while Lee et al. (2017) focused on Malaysian undergraduate students, and Huang et al. (2010) recruited participants from among university students in China. Hence, the findings of these studies may only represent a population that consists of literate and experienced internet users. Secondly, the samples for all these studies were obtained by using convenience sampling. This choice of sampling methodology, coupled with the homogeneity of the recruited study populations, thus limits the generalisability of the findings to other population groups. Lastly, apart from the study by Kwak et al. (2011), other studies that were appraised did not explore additional cognitive processes that may lead to digital security practice, such as perceived threats and attitude.

Hence, in general, the findings of these studies imply that users with a better understanding of internet threats are more likely to adopt better online safety behaviours and practices. It is equally important to gauge the individual’s level of confidence in regards to online safety because this factor has been shown to have a major influence on online safety practices. Furthermore, a major gap still needs to be addressed in this respect, namely, the relationship between self-efficacy and security practices among the general population, rather than only focusing on literate and experienced internet users.

2.2.2 Perceived Online Threats

Ng, Kankanhalli, and Xu (2009) showed that perceived susceptibility to online threats is positively associated with the computer security measures taken ($\beta = 0.23$; $p < 0.001$). Also, Thompson, McGill, and Wang (2017) showed that the more people feel that they are vulnerable to internet threats, the more likely they are to have the intention to improve their computer security ($\beta = 0.12$; $p < 0.001$). Also, privacy concerns were found to be negatively associated with the disclosure of data online among adults ($\beta = -0.78$; $p < 0.001$), as shown by Walrave, Vanwesenbeeck, and Heirman (2012). Meanwhile, Zhang and McDowell (2009) discovered that fear of internet threats is a predictor that is positively associated with the intention to use a strong online password among users ($\beta = 0.28$; $p < 0.001$). Furthermore, Huang et al. (2010) found that perceived severity ($\beta = 0.27$; $p < 0.001$), the potential impact of the threats ($\beta = 0.24$; $p < 0.001$), the possibility of experiencing online threats ($\beta = 0.21$; $p < 0.001$), and knowledge of threats ($\beta = -0.08$; $p < 0.001$) are all significant predictors of perceived online threats.

However, most of the above-mentioned studies did not comprehensively cover the components of digital security practice. Ng et al. (2009), in their study, only focused on a specific computer security behaviour, namely, checking email. Zhang and McDowell (2009) also focused on a single type of digital security practice, namely, password usage. Thompson et al. (2017) focused only on the technical aspect of digital security practice, such as running antivirus software and performing backups. However, their study attempted to widen the coverage of digital security practice by taking into account mobile and home computer usage. On the other hand, Walrave et al. (2012) examined the behavioural component of digital security practice by looking into measures taken for online social network usage, including trust and peer influence.

The variation in the scope of digital security practices studied highlight a gap in the literature, namely, the need to examine these practices in a wider context by taking into account both the behavioural and technical aspects of digital security.

Also, in general, these studies emphasise the role that perceived online threats play in influencing online safety behaviours and practices. Again, this highlights the importance of gaining an understanding of the attitude towards online threats among the general adult population because this would give a good indication of their behaviours and practices in relation to online safety.

2.3 Factors that Influence Parental Internet Mediation

As adults move into the demanding role as parents, their lives would be changed and influenced by many complex features, including social, psychological and daily routine adjustments in the family (Nomaguchi, 2003). Due to the interplay of these complex features, the factors influencing their digital security practices might differ, particularly in respect to protecting their children through internet mediation as opposed to protecting their own self as was covered in section 2.2. As such, it is important to explore on the crucial factors that would influence parents in keeping their children safe online through internet mediation techniques to gain more insight on this behaviour from the parents' perspectives in the literature. By doing so, the literature review in this section would be able to reveal if some of the factors would overlap with findings in section 2.2, and if any additional factors related to parental internet mediation would emerge. This makes the overall understanding on factors influencing digital security practices, particularly among parents to be comprehensive.

The literature review revealed that several factors influence parental internet mediation. One of the most important factors is the perceived rewards gained by parents from mediating their children’s internet use. Certain family sociodemographic are also influential as well. Furthermore, parental confidence and perceived threats are two other two important factors, which is consistent with the findings discussed above regarding the factors that influence adults to perform protective online behaviours.

2.3.1 Variation in Perceived Rewards

It has been shown that facilitating their children’s internet use can be rewarding to parents in various ways. A study by Boddum (2013) involving 141 parents with children aged 2–5 years old in the USA showed that 31% of the parents believe that the internet is a good educational tool for their children. In a similar vein, Chiong and Shuler (2010) in their study on 812 parents in the USA revealed that 12% of them believe that mobile device applications have the potential to be useful educational tools for children. Boddum (2013) also highlighted that 25% of the parents in the study believe that internet use is an important source of entertainment for their children. This finding is similar to that reported in the earlier study by Chiong and Shuler (2010), in which it was found that 24% of parents think that internet usage is a source of entertainment for children. Boddum (2013) also showed that about 8% of parents believe that allowing their children to use the internet is part of promoting the autonomy of children.

Parents also believe that internet usage is a useful distraction tool that enables parents to relax and obtain other practical gains. Boddum (2013) also revealed that almost 30% of parents believe that internet use among children helps parents to have time for themselves and is a good distraction tool.

These different reasons were found to influence the usage of the internet allowed to their children.Nikken and Schols (2015), in their study based in Holland, found that children spend significantly more time on mobile devices when parents believe that internet usage by children provides parents with an opportunity to rest ($\beta = 0.21$; $p < 0.001$). Furthermore, a study by Roy and Paradis (2015) involving 55 parents with children aged 1–4 years old showed that the frequency of parents allowing their children to use a smartphone is significantly associated with parents using the smartphone as a distraction, as a reward for good behaviour, and to improve their child's autonomy ($p < 0.01$). Hence, the suggested association between screen time and different rewards could potentially influence the mediation techniques differently.

However, the following issues should be noted in relation to the above-mentioned studies. Firstly, the study by Boddum (2013) only focused on children aged 2–5 years old in a single region in the USA. Similarly, the study by Chiong and Shuler (2010) also focused on parents with young children, in this case, those aged 7 years and below in the USA. Moreover, parents with young children aged 1–4 years old were also the main focus of the study by Roy and Paradis (2015) conducted in the USA, while the sample for the study by Nikken and Schols (2015) only involved parents with children aged below 7 years old in Holland. Hence, studies that investigate parents' perceived rewards for giving access to the internet to older children are much needed in order to understand parental digital security practice better. Parents' perceived rewards might be culturally influenced as well, and this aspect is certainly worth exploring in the local context of Malaysia because most of the previous studies identified in the literature review involved parents in the USA and Europe. Additionally, apart from Nikken and Schols (2015), the studies used a descriptive approach to investigate parents' perceived rewards in relation to their children's use of the internet. Hence, studies that relate perceived rewards to actual parental digital security practice are lacking and this issue needs to be explored as well.

2.3.2 Family Sociodemographic

Families of higher socioeconomic status appear to adopt more internet rules compared to those of lower socioeconomic status ($p < 0.001$), as demonstrated by Livingstone and Helsper (2008) in their study conducted in the UK. Family size also influences the existence of mediation techniques. Notten and Kraaykamp (2009) showed that family size is negatively associated with parents' mediation of their children's media use ($\beta = -0.19$; $p < 0.001$). It has also been found that the education level of parents is negatively associated with adopting restrictive ($\beta = -0.13$; $p < 0.001$) and active strategies ($\beta = -0.10$; $p < 0.001$) (Nikken & Jansz, 2014). However, Notten and Kraaykamp (2009) showed that parents' education level is positively associated with mediation ($\beta = 0.11$; $p < 0.001$). Also, parents who are divorced appear to impose less mediation as compared to parents who are not divorced ($p < 0.01$) (Notten & Kraaykamp, 2009).

The differences in the mediation techniques by certain sociodemographic characteristics might be a reflection of the barriers and efforts a parent has to put into mediating his or her child due to the family structure and conditions. For instance, parents with a large family size may need to exert more effort to impose online safety measures on their children as compared to those with a smaller family size. Similarly, parents who are divorced may have to put in more effort in mediating their children's online safety due to the absence of support from their ex-partner in managing the family. Also, a lower level of education might lead to less mediation because the perceived psychological barrier to performing mediation techniques is greater. However, to the researcher's knowledge, studies that examine the association between perceived efforts and mediation techniques are lacking. Hence, exploring the relationship between perceived effort and mediation techniques is worthwhile to gain a better understanding of the factors that influence parental mediation techniques.

2.3.3 Parental Confidence

Parents who perceive that they have a higher level of internet skills are more likely to mediate their children's internet use (β = 0.11; $p < 0.001$), according to Livingstone and Helsper (2008). Moreover, Nikken and Jansz (2014) showed that parents who have higher internet skills tend to adopt technical safety guidance for their children's use of the internet as well (β = 0.14; $p < 0.001$). Parents who are confident in their own internet use are also more likely to monitor (β = 0.10; $p < 0.01$) and impose restrictive mediation techniques (β = 0.09; $p < 0.05$) on their children, as shown by Sonck, Nikken, and de Haan (2013). Furthermore, Hwang, Choi, Yum, and Jeong (2017) revealed that parents who feel that restrictive mediation is useful in preventing online threats are more likely to implement this technique (β = 0.20; $p < 0.001$).

In essence, based on the findings of the above-cited studies, parents who are confident in their ability to perform protective online actions to protect their children are more likely to do so. Similarly, the studies show that parents who believe such actions are effective in combating online threats are more likely to perform those actions. These two factors are worth exploring further in order to determine parental digital security practices because these factors have been shown to be influential in predicting parents' protective behaviour towards their children online.

However, the reviewed studies have some limitations in terms of the generalisability of the findings. For instance, the study by Hwang et al. (2017) only focused on Korean parents with children aged 10–12 years old, and the samples were selected through convenience sampling. Similarly, Nikken and Jansz (2014) also obtained their samples through convenience sampling and only involved parents with children aged 2–12 years old in Holland. On the other hand, Livingstone and Helsper (2008) engaged with parents with a restricted range of older children aged from 9–17 years old who were sampled through probability sampling in the UK. Likewise, Sonck et al (2013) involved parents with children aged 9–16 years old who were recruited through probability sampling in Holland. Thus, it can be seen that the study population of each study is not representative of parents with children across the complete age spectrum from infancy to adolescence. Furthermore, the studies are geographically limited because most studies were conducted in Europe and East Asia. Hence, replicating such studies in the Malaysian context is essential because the findings of these studies cannot be generalised to the Malaysian setting due to possible cultural differences.

2.3.4 Perceived Threats

Nikken and Schols (2015) demonstrated that parents' attitude towards media influences the mediation techniques they adopt. More specifically, they found that parents who perceive media as having negative effects are more likely to adopt supervision and restrictive mediation techniques ($p < 0.001$). Also, Hwang and Jeong (2015) showed that parents' severity perception of internet threats increases the likelihood of them adopting restrictive mediation ($\beta = 0.28$; $p < 0.001$) and active mediation ($\beta = 0.40$; $p < 0.001$). Nikken and Jansz (2014) demonstrated that parents who perceive negative effects of the internet are more likely to adopt active mediation, co-use, and restrictive mediation techniques ($p < 0.001$), whereas parents who perceive positive effects of the internet tend to adopt co-use and active mediation techniques ($p < 0.001$). Sonck et al. (2013) highlighted that parents who are worried about internet risks are more likely to monitor ($\beta = 0.13$; $p < 0.001$) and restrict their children's internet use ($\beta = 0.09$; $p < 0.01$).

However, as mentioned above, the study by Nikken and Schols (2015) only involved parents with children aged 0–7 years old in Holland, while that of Hwang and Jeong (2015) was conducted among parents with children aged 10–19 years old in Korea. Also, as described earlier, the studies by Nikken and Jansz (2014) and Sonck et al. (2013) also have limitations in terms of their study populations, which are not representative of parents with children of all ages and are only applicable to their respective regions. Thus, although the above-mentioned studies established that parents' views on the effects that the internet has on their children is a significant factor that influences the types of mediation technique that they adopt, it is necessary to replicate this type of study in the Malaysian context and to also involve children across a wider age spectrum in order to address the gaps identified in these studies.

2.4 Existing Tools for Digital Security Used by Adults and Parents

The literature review also revealed that there are several gaps in relation to the existing tools that are used to assess digital security among adults and parents. Firstly, no 'gold standard' assessment tool for digital security was found in the literature. Secondly, the tools were mainly designed and originated in Europe and North America. Although there are existing tools on digital security developed in the Asian context, the majority of the studies on digital security using these tools were confined to East Asian region and of certain countries, namely from China, South Korea, and Japan. The focus of the studies is also varied. For instance, studies on parents' online mediation techniques vary in terms of the children's age group and the type of online behaviour (Hwang & Jeong, 2015; Nikken & Jansz, 2014; Sonck et al., 2013). For instance, Sonck et al (2013) explored online mediation technique of parents with children aged 9–16 years old in Holland, thus excluding preschool children. Hwang et al. (2017) focused only on mediation techniques for smartphone usage among children in Korea. Nikken and Jansz (2014) developed scales for online mediation techniques for children aged 2–12 years old in Holland, thus excluding adolescents. Thirdly, none of the questionnaires in the studies addresses the cognitive processes that influence parental digital security practice for general online activities, the findings from which would be beneficial in guiding parents' behaviour towards cyber parenting in general. Thus, there is a clear need to develop a tool to assess parental digital security practice comprehensively in the Malaysian context that is based on the cognitive processes and that covers the general online activities of children and adolescents of all ages.

2.5 Overall Findings of the Literature Review

The literature review highlighted a few aspects of importance for direction of this study. Firstly, two factors were found to be critical in determining digital security practice, namely, the individual's confidence in carrying out digital security practice and their perception of online threats, both of which heavily influence a person in performing the protective action, whether as an adult individual or as a parent. Secondly, some additional factors were also found to have an influence on parental online mediation techniques. For instance, it is apparent that different motivations and views on the benefits of children being online determine the mediation patterns exhibited by parents. Thirdly, certain sociodemographic factors seem to lead to different perceptions regarding the efforts a parent has to make in mediating the online usage of their children and these then also influence parental digital security practice. Essentially, the findings reported in the literature highlight the influence that intrapersonal components have in determining parents' digital security practices. In terms of the existing tools for the assessment of digital security practices, most of the tools have been developed in North America, Europe and East Asian regions, and there is a lack of a comprehensive tool that covers all the different aspects of digital security practices and the full age range of children from preschool through adolescence.

The literature review also revealed a few gaps that need to be addressed. Firstly, most of the findings in previous studies are not generalisable due to geographical and sampling limitations. Secondly, all the reviewed studies only cover a certain age range and did not comprehensively involve parents with children from a wider age group. Thirdly, most of the studies also focus on particular online behaviours, such as smartphone usage and online gaming, rather than internet usage in general. Lastly, there seems to be no existing study on parental digital security and online mediation that comprehensively covers all the cognitive factors identified in this literature review, such as perceived confidence, perceived threats, perceived rewards and perceived efforts. Thus, conducting a study that covers all these gaps is necessary. This can be done by developing a tool which is suitable for parents with children of all ages. Such a tool will facilitate the assessment of all the factors which were found in this literature review to influence parental digital security with regards to general online usage among children. By doing so, we will be able to identify which factors are truly important and need to be enhanced in order to improve parental digital security practice, particularly in the Malaysian setting.

2.6 Theoretical and Conceptual Frameworks

The factors found in the literature review which were described in the previous sections mirror the general components in the fear appeals approach. Hence, theoretical frameworks on fear appeal were chosen as the main focus for this study in order to explore their potential in explaining parental digital security practice. In public health, threat communication or fear appeals approaches are widely used in health campaigns (Peters, Ruiter, & Kok, 2013). Fear appeals are defined by Kim Witte (1994) as “persuasive messages that arouse fear by depicting a personally relevant and significant threat, followed by a description of feasible recommendations for deterring the threat” (p.114). The fear appeals approach triggers the motivation of an individual to take action by provoking fear about or threats to his or her well-being. Generally, there are three major groups of fear appeals theories, namely, drive theories, parallel response models, and subjective-expected-utility (SEU)-based models (Dillard, 1994).

2.6.1 Drive Theories

Drive theories were used in earlier research to explain fear appeals approaches. The fundamental concept behind drive theories is that a person’s fear-arousal level can be manipulated through making fear appeals, which subsequently drives the individual's motivation to carry out protective actions (Dillard, 1994). The relationship between fear and action is thought to be U-shaped, in which a moderate amount of fear arousal is deemed optimum to change behaviour (Dillard, 1994). This assumption is based on the argument that although fear arousal can motivate a person to take action, fear can also lead to avoidance effects (Witte & Allen, 2000). In other words, too much fear arousal will lead to avoidance without changing the behaviour, and too little fear arousal will not trigger action.

2.6.2 Parallel Response Models

The parallel response model was proposed by Leventhal (1970), who suggested that fear appeals produce two independent and simultaneous processes: fear control and danger control. This model attempts to distinguish between the emotional response reflected by the fear control process and the cognitive response as manifested through the danger control process (Dillard, 1994). The fear control process reflects the emotional response to fear appeals, focusing on efforts to reduce or eliminate the unpleasant experience of fear (Leventhal, 1970). In contrast, the danger control process is a cognitive process that focuses on efforts to reduce or eliminate the threats.

2.6.3 Subjective-Expected-Utility (SEU)-based Models

Subjective-expected-utility-based models address decision-making and cognitive processes. The model proposes that an individual will choose courses of action that will provide rewards and avoid punishments (Dillard, 1994). Thus, SEU-based models are used to explore what makes a fear appeal effective in a logical manner through an individual's cognitive processes (Witte & Allen, 2000). A meta-analysis of fear appeals undertaken by Peters et al. (2013) highlighted the extensive use of SEU-based models in explaining fear appeals. This reflects the suitability and usefulness of SEU-based models in fear appeals research. The meta-analysis also highlighted that protective behaviours are functions of two components of fear appeals, namely, perceived threat and perceived efficacy (Peters et al., 2013). Two of the most commonly employed SEU-based models for fear appeals are the health belief model (HBM) (Rosenstock, 1974) and PMT (Maddux & Rogers, 1983).

The HBM was originally developed in the 1950s in order to predict health-promoting behaviours for the public health services in the USA, such as the uptake of screening programmes (Rosenstock, 1974). As shown in Figure 2.1, there are several domains in this model; perceived susceptibility refers to the risk of being exposed to a disease/condition; perceived severity reflects the beliefs on the condition's seriousness and related consequences; perceived benefits refers to the advantage and positive outcome of taking a particular action; cues to action refers to the signals that encourage a person to take action; and perceived barriers reflects the disadvantage and obstacles preventing the taking of a particular action (Rosenstock, 1974). These domains are also influenced by modifying factors such as demographics and the personality of the individual (Rosenstock, 1974). Overall, these domains determine the likelihood of an action being taken.

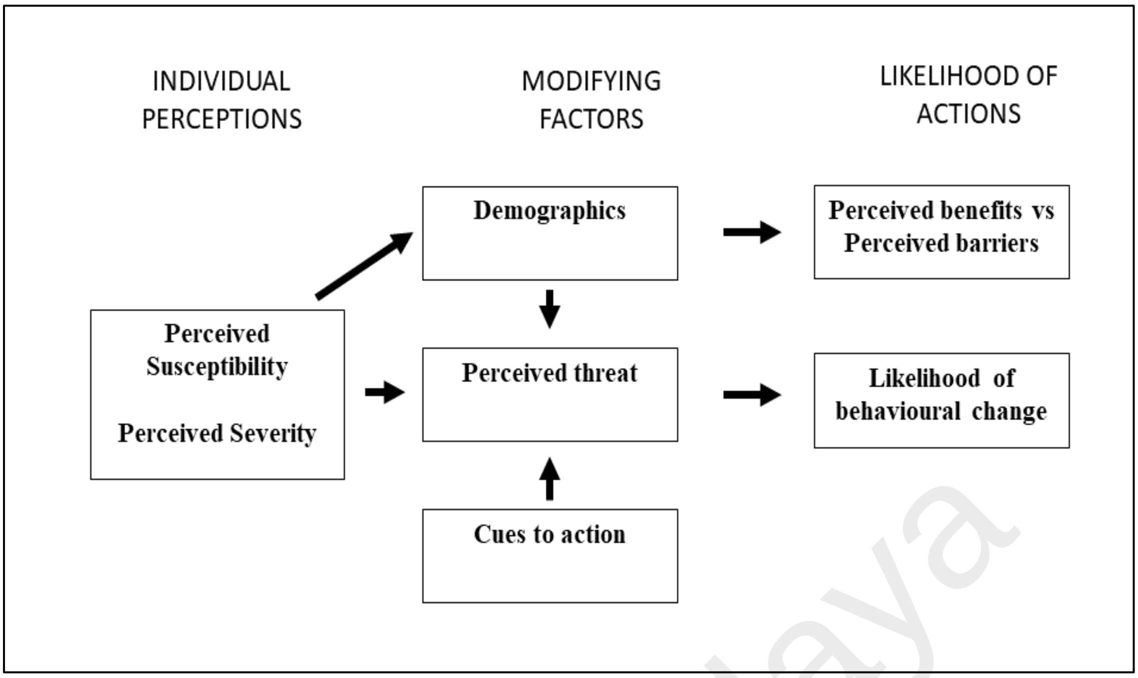

Figure 2.1: Health Belief Model

Adapted from: Rosenstock, I. M. (1974). The health belief model and preventive health behavior. *Health education monographs, 2*(4), 354-386.

Although the HBM is designed for health-related actions, the flexibility of this model makes it popular in other disciplines as well. Hence, this model has also been adopted in cyber-related fields. For instance, Dodel and Mesch (2017) adapted this model to explain cyber victimisation protection behaviour among adults. In addition, Claar and Johnson (2012) used this model to explain home PC security actions among adults.

Protection motivation theory was developed by R.W. Rogers in 1975, and revised in 1983 (Maddux & Rogers, 1983). It is a cognitive-based theory that is used to explain the protective behaviours of individuals (Maddux & Rogers, 1983). Central to this theory are two cognitive processes, namely, coping appraisal and threat appraisal, which influence the intention of a person to adopt a particular protective behaviour (Maddux & Rogers, 1983). A coping appraisal is determined by response efficacy, self-efficacy and response costs related to a particular protective behaviour (Maddux & Rogers, 1983). A threat appraisal is based on susceptibility to risks, perceived vulnerability, and maladaptive rewards related to not performing the protective behaviour (Maddux & Rogers, 1983). The theoretical framework of PMT is depicted in Figure 2.2.

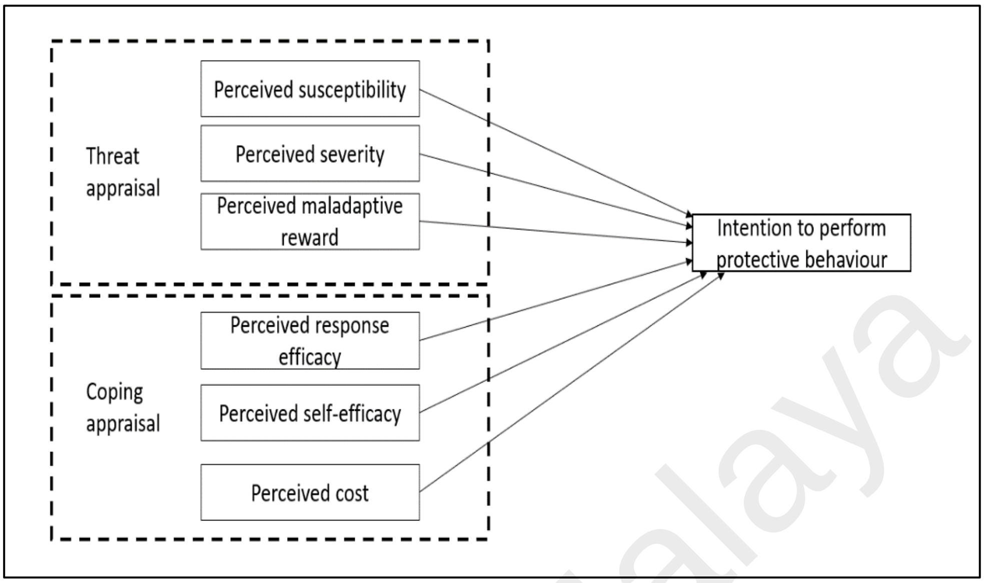

Figure 2.2: Framework of protection motivation theory

Adapted from: Maddux, J. E., & Rogers, R. W. (1983). Protection motivation theory and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*, 469-479.

The coping appraisal of threats appears to be the most significant predictor of the intention and the practice of a protective behaviour (Milne, Sheeran, & Orbell, 2000). In the coping appraisal, the dimension of self-efficacy refers to the ability to perform protective behaviour (Boehmer et al., 2015). Response efficacy, on the other hand, refers to the belief in the effectiveness of the protective behaviour (Boehmer et al., 2015). Efficacy is built based on, among others, a person’s own experiences and by observing other people’s experiences (Bandura, 1994). Thus, a person’s assessment of the efficacy of a protective behaviour can be seen as a reflection of their knowledge on that particular behaviour. Another dimension of coping appraisal is response cost. This term refers to the cost, not necessarily in monetary terms, that a person has to bear when adopting a protective behaviour (Boehmer et al., 2015). The theory posits that high self-efficacy and response efficacy, coupled with a low response cost, will increase the motivation to practise a protective behaviour (Maddux & Rogers, 1983).

In the threat appraisal, the dimension of perceived severity refers to the magnitude of the individual's perception of the negative consequences of not performing the protective behaviour (MacDonell et al., 2013). On the other hand, perceived susceptibility refers to the perceived likelihood of the individual being affected by potential negative consequences (MacDonell et al., 2013). The last dimension in threat appraisal is maladaptive reward, which refers to the positive effect of not performing protective behaviour (MacDonell et al., 2013). The theory posits that high susceptibility and severity coupled with low maladaptive reward will increase the intention of practising protective behaviour (Maddux & Rogers, 1983).

2.7 Identification of the Main Theory for Fear Appeal for this Study

The literature review revealed that fear appeal theories can be categorised into three major types: drive theories, parallel response models and SEU-based models. Drive theories were eventually rejected because in practice they lack empirical evidence to support the main notion that fear and action have a U-shaped relationship (Witte & Allen, 2000). The dependence on emotional responses, without addressing cognitive processes, was another major limitation of these theories (Witte & Allen, 2000) that led to their rejection. On the other hand, parallel response models attempt to explore both the emotional process in the form of fear control and the cognitive process in the form of danger control. However, this model does not explain when and how these two processes would be initiated and interact (Witte & Allen, 2000). Additionally, the model has been criticised because it cannot be tested due to the difficulty of operationalising and specifying these two processes (Witte & Allen, 2000). Thus, the complexity of this model and the difficulty of discriminating these two processes make this type of fear appeal theory unsuitable for this study.

Hence, the theoretical framework for this study is based on the SEU-based model, and focuses on the cognitive process of fear appeal. The extensive use of the SEU-based model in predicting protective behaviours reflects the suitability and practicality of this type of model. Under the SEU model, two main theories are explored, namely, the HBM and PMT.

Although the HBM has the potential to be utilised in explaining protective behaviour, it has some limitations. A meta-analysis of HBM-related studies that was conducted by Carpenter (2010) showed that the correlation between the domains and behaviour was poor, ranging between 0.05 and 0.30. This indicates that the HBM might not be appropriate or comprehensive enough to explain protective behaviours. These findings are reflected in an earlier study by Armitage and Conner (2000), which highlighted some additional drawbacks of the HBM. For instance, the operationalisation of the HBM domains was found to be challenging, particularly the cues to action and modifying factors. Also, the difficulty of operationalisation, combined with the lack of combinational rules for this model, leads to inconsistent application and poor discriminant validity (Armitage & Conner, 2000).

Protection motivation theory is a type of SEU-based model which has proven to be useful in explaining fear appeal (Peters et al., 2013). The components of PMT are deemed adequate and appropriate for explaining protection behaviour from the angle of fear appeal (Peters et al., 2013). This theory has also been successfully used in studies on online safety matters, as well as on parental protection (MacDonell et al., 2013). This implies that the PMT shows promise for explaining parental digital security. Moreover, a meta-analysis by Sommestad, Karlzén, and Hallberg (2015) showed that the components of PMT were able to explain 34% to 50% of the variance in information security behaviour among the studied population. The high explanatory ability of PMT is most likely due to the ease with which the domains can be operationalised and the explicit relationship direction between the domains proposed in PMT. Hence, although there are overlaps between the HBM and PMT in terms of the main domains, PMT has a possible advantage over the HBM based on the above arguments. Therefore, PMT is used as the main theoretical framework in this study.

2.8 Conceptual Framework

Based on the findings derived from the literature review, three main components were identified as being of interest and are thus the focus of this study. The investigation of the connections among these components is guided by PMT (Maddux & Rogers, 1983) and the established digital citizenship framework (International Society for Technology in Education, 2011), as well as previous studies on online mediation techniques and digital security (Nathanson, 2001; Nikken & Jansz, 2014; Sonck et al., 2013).

2.8.1 Component 1: Parents' Digital Security Practice

Parents' digital security practice is the main component that will be examined in this study. This component is based on the digital citizenship framework (Figure 1.1), in which digital security is one of the essential elements needed to produce good digital citizens. In this study, parental digital security practice refers to the practices used by parents to maintain the safety and security of their children online.

As there is no proper definition of parental digital security in the literature to the researcher's knowledge, this component was heavily based on the internet mediation techniques that parents have been found to apply to their children. As mentioned in Section 1.2.3 in Chapter One, this approach to this component was justified based on the examination of various guidelines on parental digital security practice that have been produced by established organisations (CommonSense, 2014; Connect Safely, 2015; CyberSecurity Malaysia, 2017; MediaSmarts, 2017). These guidelines highlight good parental digital security and safety practice by recommending various internet mediation techniques, such as parental control and giving advice.

Based on the literature review, studies have examined parental internet mediation techniques generally based on the framework proposed by Nathanson (2001), who broadly categorised the mediation techniques that parents use to manage their children's television viewing. However, over the years, recommendations have been made to expand the types of mediation technique so that they are applicable to the context of internet use. These proposed techniques include active mediation, restrictive mediation, co-use, supervision, and monitoring (Livingstone & Helsper, 2008; Nikken & Jansz, 2014; Sonck et al., 2013). The active mediation technique involves parents sharing information, commenting on contents and providing advice when their children are using the internet (Nikken & Jansz, 2014). The restrictive mediation technique includes imposing rules and control over the amount of time spent on the internet and the content that the children are allowed to view (Nikken & Jansz, 2014). Co-use refers to parents and their children using the internet together at the same time and sharing the experiences together (Nikken & Jansz, 2014). The supervision mediation technique occurs when children are allowed to use the internet on their own, but with the presence of their parents nearby (Nikken & Jansz, 2014). Lastly, monitoring is defined as parents checking their children's online activities after usage (Livingstone & Helsper, 2008; Sonck et al., 2013). This study uses these mediation techniques as guidance in examining parental digital security practice.

2.8.2 Component 2: Threat Appraisal

There are three dimensions of threat appraisal based on PMT, namely, perceived susceptibility, perceived severity, and perceived maladaptive reward. In this study, perceived susceptibility refers to parents' perception of their children's likelihood of being unsafe online, while perceived severity refers to the degree of harm that parents perceive that their children will experience if the children were exposed to online threats. Lastly, perceived maladaptive reward refers to the alternative benefit that parents would gain from not adopting parental digital security practice. Many of the previous PMT-based studies have excluded the perceived maladaptive reward component (Milne et al., 2000). One of the arguments given for this is that because the conceptual difference between response cost and maladaptive reward is not clear in respect of security behaviours (Abraham, Sheeran, Abrams, & Spears, 1994) and it is therefore difficult to separate these dimensions. However, to ensure the completeness and comprehensiveness of the examination of parental digital security practice using the PMT model, perceived maladaptive reward is included in this study.

2.8.3 Component 3: Coping Appraisal of Internet Threats

There are also three dimensions of coping appraisal based on PMT, which are examined in this study, namely, perceived response efficacy, perceived self-efficacy, and perceived response cost. In this study, perceived self-efficacy refers to parents' perception of their own ability to protect their children online, while perceived response efficacy refers to parents' perception of the effectiveness of their parental digital security practice in actually protecting their children online. Lastly, the response cost refers to the cost that parents have to bear in applying digital security practices for the benefit of their children. A diagrammatic representation of the conceptual framework and its components is depicted in Figure 2.3.

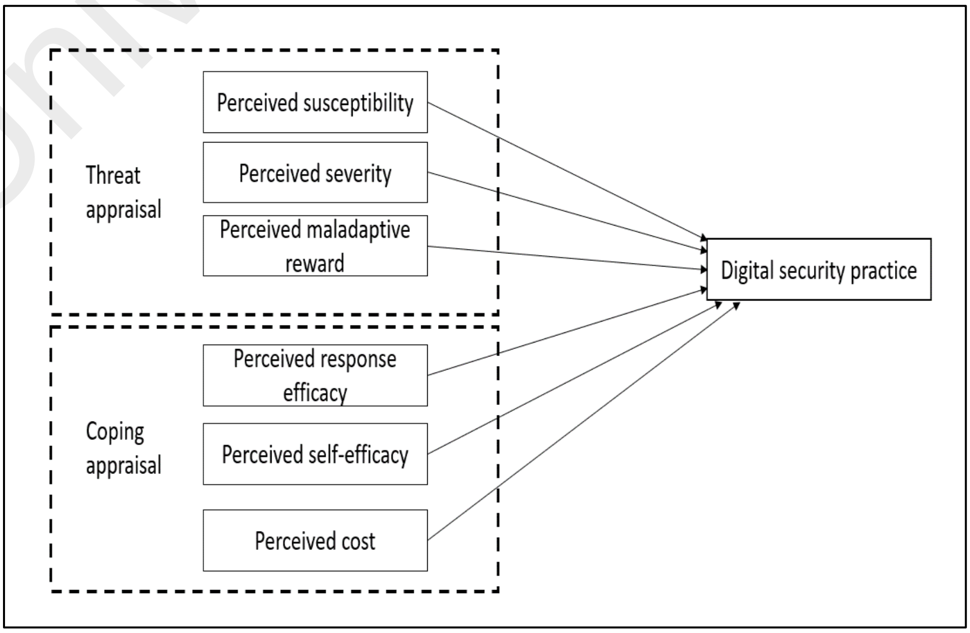

Figure 2.3: Conceptual framework of study

2.9 Summary of and Rationale for the Developed Conceptual Framework

Protection motivation theory is seen as one of the best theories for explaining protective behaviour and practice from the fear appeal angle. This provides further justification for heavily basing the formation of the conceptual framework for this study on PMT. Feedback from stakeholders, particularly from CyberSecurity Malaysia (CSM), also revealed the usefulness of exploring the components in the conceptual framework (see Appendix A). This is because the components of the advocacy activities on parental digital security that are performed by CSM revolve around the components included in the framework. Thus, an examination of these components can provide guidance to stakeholders in various ways. Firstly, it can enhance the understanding of how the individual components influence digital security behaviour. Secondly, because the components in PMT are useful for changing behaviours, the manipulation of these components may be crucial for developing effective interventions (Jansen & van Schaik, 2017). Lastly, understanding the influence that these components have on digital security is expected to help to facilitate an improvement to existing advocacy activities.

2.10 Summary of Chapter Two

In summary, the findings of the literature review presented in this chapter revealed that perceived threats and perceived self-efficacy were the main factors that influence adults to adopt digital security practices. The chapter also showed that these factors also influence parental internet mediation techniques, in addition to perceived rewards and family sociodemographic. Moreover, it elaborated that all these factors reflect the intrapersonal components of parental digital security practice. Hence it was decided that these factors would be the focus of this study. The chapter also explored the existing tools for assessing digital security practice and revealed the lack of appropriate tools to measure the cognitive aspect of parental digital security practice in the Malaysian context. Furthermore, the chapter explained that the factors discovered in the literature mirrored those in the theoretical framework of the fear appeals approach, which was therefore chosen as the main foundation for this study. Specifically, the PMT was chosen due to the potential strength it possesses for explaining protective behaviours such as parental digital security practice based on empirical evidence. The chapter concluded by highlighting how the conceptual framework for this study closely mimics the components in PMT.

CHAPTER THREE: METHODOLOGY

3.1 Introduction

This chapter describes the methodology used for questionnaire development and validation. It consists of four main sections. The first section covers the research design and explains the overall process followed in developing and validating the questionnaire. The second section focuses on the populations, samples and various data collection techniques that were used in each stage of questionnaire development. The third section concentrates on the instruments used throughout the development and validation process. Lastly, the fourth section describes the analysis techniques used in each stage of the questionnaire development process. An overview of the content of these sections is provided in Figure 3.1.

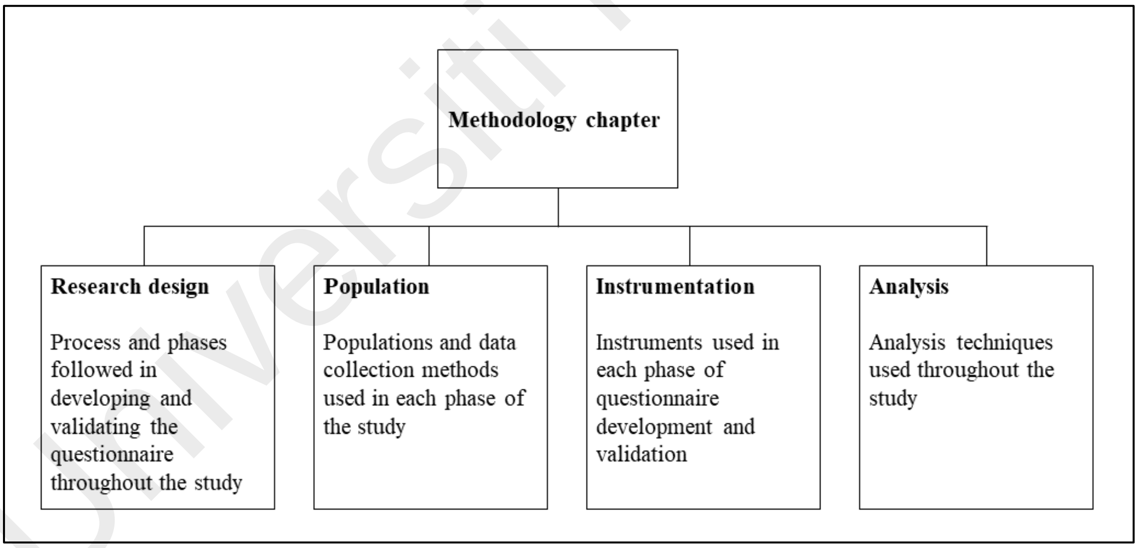
Methodology chapter
Research design
Process and phases followed in developing and validating the questionnaire throughout the study
Population
Populations and data collection methods used in each phase of the study
Instrumentation
Instruments used in each phase of questionnaire development and validation
Analysis
Analysis techniques used throughout the study

Figure 3.1: Description of methodology chapter by section

3.2 Research Design

This study was conducted by using the deductive approach, specifically by exploring an established theory, namely PMT, in order to explain the parental digital security phenomenon. Thus, the questionnaire developed for this study was heavily based on the components of PMT. The parental digital security questionnaire was developed by taking several steps to ensure good validity and reliability, as elaborated in the subsequent sections of this chapter. The steps were based on several guidelines (Boateng, Neilands, Frongillo, Melgar-Quiñonez, & Young, 2018; Di Lorio, 2005; Hinkin, 1998; Schmiedel, Vom Brocke, & Recker, 2014; Slavec & Drnovsek, 2012; Streiner & Norman, 2008; Tafforeau, Cobo, Tolonen, Scheidt-Nave, & Tinto, 2005).

The steps that were followed can be grouped into three major phases: item development, scale development and scale evaluation. The process flow and the activities performed in each phase are summarised in Figure 3.2.

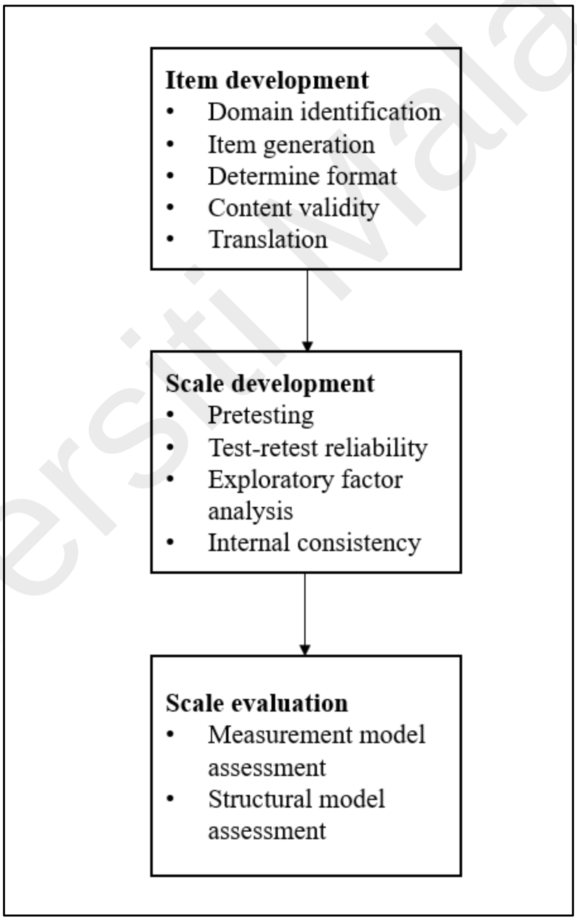

Figure 3.2: Major phases and activities performed in study

The study used the mixed methods design, in which the activities of each phase were conducted by using both qualitative and quantitative research techniques. The major phases, activities and types of data collected are summarised in Table 3.1.

Table 3.1: The phases, activities and types of data collected in this study

Phase	Activity	Type of data
Item development	• Domain identification • Item generation • Determine format • Content validity • Translation	Qualitative Qualitative Qualitative Qualitative and quantitative Qualitative
Scale development	• Pretesting • Test-retest reliability • Exploratory factor analysis • Internal consistency	Qualitative Quantitative Quantitative Quantitative
Scale evaluation	• Measurement model assessment • Structural model assessment	Quantitative Quantitative

3.2.1 Item Development

The item development phase consisted of five major steps or activities: domain identification, item generation, design of questionnaire, content validity, and translation, as shown in Figure 3.3.

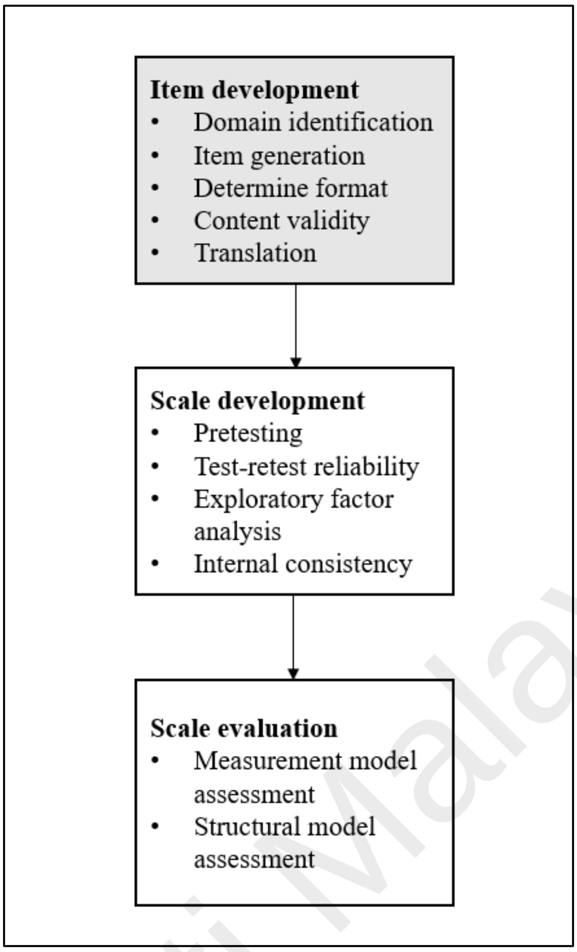

Figure 3.3: Activities performed in item development phase (highlighted in grey box)

Domains are abstract concepts that researchers attempt to measure (McCoach, Gable, & Madura, 2013). The objective of domain identification is to link abstract concepts that are targets of a study to empirical items. Hence, the identification of domains is an essential first step because it leads to the generation of tangible items that are representative of the abstract concepts to be measured. McCoach et al. (2013) suggested some steps to follow in identifying the domains of a study and their approach was adopted in this study. The steps they suggest are as follows: (a) identify and specify the purpose of the domain to be developed, (b) confirm the unavailability of similar instruments that would serve the same purpose, (c) describe and provide a conceptual definition of the domains, and (d) specify the dimensions of the domain if known, or form dimensions based on statistical computation through the development process.

After the domains had been identified, several items were generated. Two types of approach can be used to generate items, namely, a deductive or an inductive approach (Hinkin, 1995). The deductive approach is based on the description of the domains, in which a literature review and an assessment of existing scales is performed in order to identify items that fit the domain descriptions (Hunt, 1991). On the other hand, the inductive approach involves the generation of items based on responses received from selected individuals (Hunt, 1991). These responses are obtained by using qualitative methods such as interviews and expert discussions (Hunt, 1991). Items are then identified inductively from the responses obtained. A combination of the both deductive and inductive approach is considered best practice for item generation (Boateng et al., 2018). In line with this view, both approaches were used in this study. The deductive approach was followed by conducting a systematic review and the inductive approach was followed by engaging with stakeholders through online surveys and discussions with experts.

The systematic review provided a comprehensive overview of PMT-based questionnaires that were available in the literature at the time of this study. As such, the systematic review served two purposes. The first purpose was to obtain available items that could be adapted in this study. This is important because using validated questionnaires for item generation increases the reliability of the items (Straub, 1989). Apart from facilitating the generation of items, the systematic review was also able to reveal the quality of and the areas related to digital security covered by the existing PMT-based questionnaires. The systematic review was performed based on the preferred reporting items for systematic reviews and meta-analyses (PRISMA) guidelines (Moher, Liberati, Tetzlaff, & Altman, 2009).

The search strategy included an online search of six online databases, namely, PubMed, E-journal, ACM Digital Library, Scopus, Psychology and Behaviour, and Science Direct. Keyword searching included Medical Subject Headings (MeSH) terms as well as index terms for each database. The following keywords and combinations based on the Boolean search strategy were used:

(Online OR internet OR cyber OR digital OR web OR data OR information)

AND

(Security OR Safety)

AND

(Questionnaire OR scale OR measure OR tool OR survey)

AND

(“protection motivation theory” OR “protection motivation”)

All the articles that were identified by the above search criteria were stored in EndNote citation management software version 8.1. Duplicates were removed and then an initial screening was conducted by reading the titles and abstracts to determine the eligibility of identified articles. This step was conducted by two independent reviewers. Any disagreement was discussed, and if necessary, another opinion was sought from a third reviewer, and the majority decision was used.

The search encompassed articles published during the past 10 years, starting from the year 2008. Only English-language articles were considered, and only studies that contained the development of a scale using PMT for digital security were eligible for inclusion. Studies published in a language other than English, non-peer-reviewed materials, and studies on topics other than digital security were excluded. Studies which were inaccessible despite various steps being taken to obtain them were also excluded.

The full text of the eligible studies was retrieved and reviewed independently by two reviewers. In addition, cross-referencing was performed, whereby reference lists of eligible articles were manually searched for relevant articles not retrieved from the database search. The eligible studies were then subjected to information extraction (see Appendix C) and quality assessment using an established document analysis protocol which is described in Section 3.4.

As mentioned above, the inductive approach was also used in this study to identify items and this approach was followed by engaging with stakeholders through online surveys and discussions with experts. The engagement process was conducted qualitatively. An online survey with open-ended questions pertaining to parental digital security practice, online threat concerns, and barriers to performing digital security practice was administered using the Google survey platform in order to obtain parents' views.

The use of an online platform for gathering qualitative data has a few advantages, as highlighted in the literature (Lefever, Dal, & Matthiasdottir, 2007; Wright, 2005). Firstly, the participants captured using this technique has a high degree of heterogeneity in respect of age, occupation and geographical background. At this stage of the study, volunteer sampling rather than probability sampling is required. The use of an online platform helped to reach out to more people easily without the need to consider the issue of sampling bias. The ability to reach out to a wider audience and increase heterogeneity helped to provide rich data on parental digital security practice and concerns.

Secondly, the anonymity that the online survey technique provides allows respondents to provide answers that reflect their true views more willingly. Thirdly, the online platform is relatively cheap, easy to manage, and able to capture data quickly. These advantages are not obtainable using other face-to-face qualitative techniques such as focus groups and interviews. Focus groups, for example, require a certain degree of homogeneity in terms of the number of participants per group, can be costly, and have the potential to not produce rich data if the participants are reluctant or not comfortable about expressing their views (Acocella, 2012).

However, using an online platform has its limitations (Lefever et al., 2007; Wright, 2005). One of the main concerns is the inability to verify the respondents' identities and characteristics because the respondents are anonymous. As such, the responses might be fabricated. Secondly, respondents might not interpret the questions posed correctly, hence their responses may jeopardise the quality of the data. Lastly, the answers given might be ambiguous and not interpreted correctly by the researcher. Thus, the quality of the data obtained needs to be verified using other means to ensure its validity.

In light of the above, to ensure the robustness of the data, the themes that emerged from the online survey, together with the inventory of items and domains obtained from the initial systematic review, were discussed by a number of experts, namely, the researcher, stakeholders from CSM, a public health specialist, an expert on cyber parenting, a parents' representative, and an expert on adolescent health. The experts were invited to take part based on the years of experience they had in a relevant field (at least 5 years). The experts' suggestions regarding the modification of items, the addition and deletion of items or domains were taken into account, and the feedback was synthesised by the researcher.

The next step in item development was the design of the questionnaire. In designing the questionnaire, four aspects were considered: (a) the format of the questionnaire, (b) the creation of an item pool, (c) the formulation of the scale formula, and (d) the instructions for the participants (DeVellis, 2017; Tafforeau et al., 2005). The format of the questionnaire needs to be appropriate for participants to respond appropriately and to measure the domains of parental digital security practice accurately (Tafforeau et al., 2005). The quality of the analysis of the questionnaire responses is also dependent on the format and design of the questionnaire (Tafforeau et al., 2005). Hence the item pool needs to be suitable in terms of reflecting the respective domains (Tafforeau et al., 2005). In addition, the instructions for participants need to be clear to reduce response bias.

The next step in item development was content validity. Content validity is considered to be the first source of validity evidence that is gathered (Streiner & Norman, 2008). Content validation is undertaken to ensure that the items generated reflect the domains that are being investigated and adequately represent those domains (Tafforeau et al., 2005). Content validity is deemed a more rigorous form of theoretical validity, as compared to face validity which, as the name implies, just validates the items 'on the face of it' (Trochim, 2006). The content validity process involved selecting content and measurement experts who had sufficient knowledge and experience to validate the individual items.

Following content validation, the items in the questionnaire were translated into the Malay language by using the forwards-backwards technique. The translation procedure was adapted from published guidelines (Beaton, Bombardier, Guillemin, & Ferraz, 2000; Guillemin, Bombardier, & Beaton, 1993). It is argued that a questionnaire in two languages enhances bilingual respondents' understanding of the statements. This is because they are able to read each statement a second time in the alternative language to double-check their understanding (Hendricson et al., 1989). Respondents can also study both versions of the statement and produce a composite understanding of it too (Hendricson et al., 1989). Hence, it is justifiable to use a dual-language questionnaire format to reach out to a greater diversity of respondents while maintaining the accuracy of the included concepts. In this study, the translation was done in the item development stage in preparation for validity and reliability testing, and to obtain a more varied sample of participants at the subsequent scale development stage.

The quality of the translation process depends on two factors: the number of translations and the quality of the translators (Guillemin et al., 1993). According to Guillemin et al. (1993), a minimum of two versions of the translation by qualified translators is recommended. Qualified translators include those who are familiar with the language and who are aware of the objectives of the questionnaire. Therefore, to fulfil these criteria, in this study, two language teachers were recruited who had experience in both the English and the Malay language. They were also aware of the questionnaire's rationale and able to relate the translation to the questionnaire's objective of ascertaining the participants' views on parental digital security practice. Secondly, their familiarity with both languages added credibility to the translations they produced.

Guillemin et al. (1993) also recommends the usage of a committee to review the translation and produce a single version of the translated questionnaire. Thus, for this study, a committee was established, which consisted of the researcher, stakeholders from CSM and an expert in cyber parenting, to review the translated versions. This approach helped to enhance the quality of the translation, in line with proposed guidelines (Beaton et al., 2000; Guillemin et al., 1993).

The initial step in the translation process in this study involved two independent translators proficient in the English and Malay languages, but whose native language is Malay. The two translators translated the questionnaire from English into Malay. Based on the guidelines (Beaton et al., 2000; Guillemin et al., 1993), the two versions were then compared and synthesised by the above-mentioned committee. The outcome of this process was a single translated version of the questionnaire. Following that, a reverse translation process was conducted.

A reverse translation was done because it is deemed insufficient to depend solely on a direct forwards translation to transfer the concepts of a questionnaire cross-culturally (Banville, Desrosiers, & Genet-Volet, 2000). This is because translators might introduce errors when using words that have a subtly different meaning to those in the original questionnaire (Banville et al., 2000). As such, the use of back translation is recommended to enhance the equivalence property of a translated questionnaire (Beaton et al., 2000; Guillemin et al., 1993). Therefore, the back-translation method was incorporated into the translation process for producing the dual-language questionnaire for this study. The Malay version that was produced was translated into English by another two independent translators. Both translators were proficient in both languages. Similar to the forward translation process, the two versions were compared with the original English version by the same committee. When a consensus was achieved, the final version of the questionnaire in both languages was produced. The process of translation was iterative and there was constant communication between the committee and translators in order to obtain an accurate version in both languages.

In essence, the dual-language questionnaire process possesses three key strengths. Firstly, the steps taken in producing a dual-language questionnaire are based on established guidelines. Secondly, the backwards translation process enhances the equivalence property of the two versions of the questionnaire. This is because this step enables the transfer of concepts cross-culturally as compared to the forwards translation method. Lastly, the usage of dual-language questionnaire helps to broaden participation while maintaining the clarity of the concepts that the questionnaire intends to explore, which is particularly relevant for the context of Malaysia which has a culturally diverse population.

3.2.2 Scale Development

In the scale development phase of this study, four major steps or activities were performed: pretesting, test-retest reliability, domain extraction through exploratory factor analysis (EFA), and item reduction through internal consistency testing. These steps are shown in Figure 3.4.

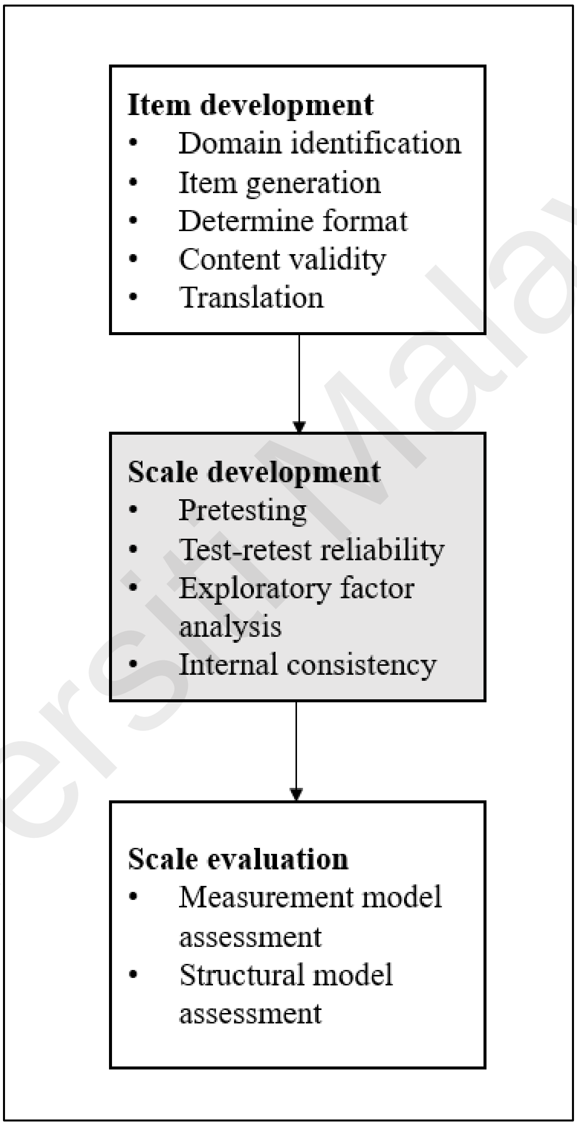

Figure 3.4: Activities performed in scale development phase (highlighted in grey box)

Pretesting is crucial in reducing measurement error due to an inaccurate understanding of the statements by respondents (Collins, 2003). By performing pretesting, one can explore whether respondents are able to understand the statements' concepts (Collins, 2003). Secondly, pretesting reveals whether respondents' understanding of statements is consistent (Collins, 2003). Lastly, through pretesting, researchers can determine whether the respondents' understanding of statements is similar to the researchers' intention (Collins, 2003). There are many techniques that can be used in pretesting. However, cognitive debriefing is one of the recommended techniques (Nanda, Gupta, Kharub, & Singh, 2013). Cognitive debriefing enables researchers to explore the cognitive processes that respondents employ when answering the questionnaire (Nanda et al., 2013). Of relevance to this study, the literature recommends the utilisation of cognitive debriefing to confirm the comprehensibility and readability properties of dual-language questionnaires (Beaton et al., 2000; Goerman & Caspar, 2010; Guillemin et al., 1993). Cognitive debriefing should be performed on the questionnaire in its dual-language format because this yields greater input in terms of identifying the adjustments that need to be made (Goerman & Caspar, 2010) as compared to performing cognitive debriefing on separate versions of the questionnaire. Therefore, pretesting using the cognitive debriefing method was used to assess the dual-language questionnaire developed for this study.

Cognitive debriefing targets the mental processes that respondents use when completing questionnaires, where these processes follow a question–answer model. There are four aspects to consider when assessing these mental processes, namely, comprehension, retrieval, judgement and response (Dillman, Sinclair, & Clark, 1993; McCoach et al., 2013; McColl, Meadows, & Barofsky, 2003; Mullin, Lohr, Bresnahan, & McNulty, 2000). A fifth aspect that can also be assessed during cognitive debriefing is the respondent burden. Relevance, questionnaire length, ease of navigation, visual distractions, and the degree of computation required all affect the respondent burden (Dillman et al., 1993; Mullin et al., 2000). In the cognitive debriefing performed in this study, the verbal probe technique was used (Di Lorio, 2005). Participants were first asked to answer the questionnaire. Following that, a debriefing session was conducted with the researcher in order to assess the mental processes and respondent burden, as explained above.

Following the cognitive debriefing, the next step in scale development was the test-retest reliability assessment. Test-retest reliability is used to assess the consistency of the measures produced by the same person when the administration of an instrument is repeated at a different time (Vitoratou, Ntzoufras, Smyrnis, & Stefanis, 2009). A reliable instrument should be able to reproduce results in a consistent manner over time in a stable population (Lohr, 2002). Thus, instruments which have poor temporal stability can be deemed as unreliable and therefore possess a high degree of measurement error (Leppink & Pérez-Fuster, 2017). The test-retest reliability assessment involves the participants answering the questionnaire, and then the same participants complete the same questionnaire 2 weeks later (Tafforeau et al., 2005).

In this research, a relatively large field study was conducted in order to obtain data for the subsequent steps of scale development, namely, factor extraction and item reduction. The data collected was used to determine the underlying domains and to explore dimensionality through EFA. Following this, a further item reduction based on the internal consistency of the items was performed. The factor extraction and item reduction steps were performed through a statistical analysis process using the Statistical Package for the Social Sciences (SPSS) version 23. Details of the analysis procedures can be found in Section 3.5.

3.2.3 Scale Evaluation

Lastly, scale evaluation was performed. In this stage, the data from the field study was used to confirm the dimensionality and the validity of the scale by undertaking a measurement model assessment and a structural model assessment, as depicted in Figure

3.5. These assessments were conducted using the structural equation modelling (SEM) technique, which is described in depth in the Section 3.5.

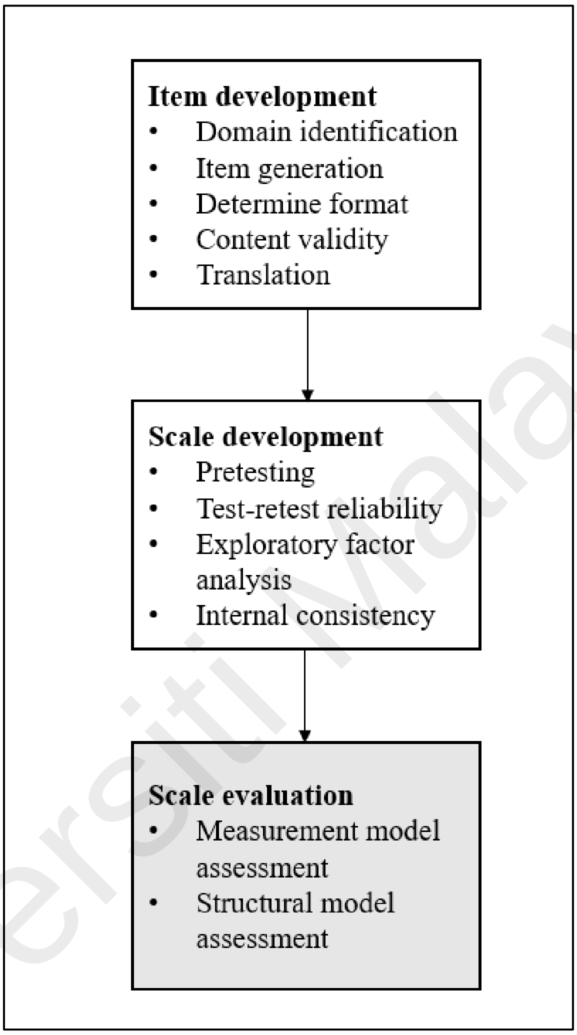

Figure 3.5: Activities performed in scale evaluation phase (highlighted in grey box)

3.3 Populations, Samples and Data Collection Process

The development and validation process required the use of various data collection techniques involving various populations at different phases of the questionnaire development process. A summary of the populations involved and the methods of data collection for the respective phases is presented in Table 3.2.

Table 3.2: The populations and methods of data collection for each phase of questionnaire development

Phase	Population involved	Method of data collection	Minimum sample size needed
Item development	• Malaysian parents through an online survey • Experts including public health specialists, a cyber parenting expert, a cybersecurity expert, medical anthropologist, and a digital citizenship expert	• Review of literature • Systematic review • Open-ended online survey • Content validity • Translation	Not applicable
Scale development	• Malaysian parents from several health clinics and workplaces	• Cognitive debriefing • Cross-sectional field survey	• Less than 20 for cognitive debriefing • 30 for test retest • 300 for exploratory factor analysis
Scale evaluation	• Malaysian parents from several health clinics and workplaces	• Cross-sectional field survey	• 100 for scale evaluation

As the study focuses on theory generalisation as opposed to sampling generalisation, non-probability sampling is considered the most appropriate approach (Rowley, 2014). This is because a degree of homogeneity of participants is needed to ensure the precision of the explanatory relationship in the model representing the theory that is to be tested (Rowley, 2014). In this study, non-probability sampling was performed for all three major phases of questionnaire development. In each study phase, purposive sampling was performed to obtain the participants with certain characteristics, to ensure the homogeneity of participants.

However, the homogeneity of the participants needs to be balanced with a degree of heterogeneity, to ensure that the theory generalisation can be replicable to a wider range of population beyond the study (Rowley, 2014). Then, maximum variation sampling was applied to ensure the presence of a diversity of backgrounds in the population from various locations in order to obtain rich input for each phase of this study. The use of maximum variation sampling ensured that the respondents from different backgrounds based on gender, race, socioeconomic status and location were represented as much as possible.

3.3.1 Population, Sample, and Data Collection for the Item Development Phase

In the item generation phase, the deductive process of generating items through a systematic review involved reviewing relevant articles published during the past 10 years, starting from the year 2008. This timeframe was selected in view of the rapid evolution of the digital world, which necessitated focusing on the most recent articles. On the other hand, the inductive process of generating the items involved two separate data collection components. The first component consisted of views from parents which were obtained through an online survey that targeted parents who were internet users and had children below 18 years old who were also internet users. Snowballing sampling technique was performed to obtain these participants. The online survey was distributed through WhatsApp, and participants were asked to forward the online survey to other parents. Data collection was ceased once saturation point has been achieved, when no new information or themes emerged from the data (Guest, 2006). The second component consisted of opinions that were obtained from experts involved in the generation of items. These experts were selected through purposive sampling, based on years of experience and background. A total of five experts were engaged for the inductive process in this item development phase.

It is essential that the individuals in a panel of experts are professionals who meet certain criteria, including work experience, qualifications and training in a relevant field of study (Grant & Davis, 1997; Rubio, Berg-Weger, Tebb, Lee, & Rauch, 2003). In this study, all the experts approached were well-qualified in their respective fields based on their working experience and their formal qualifications. Secondly, the combination of experts is also crucial. This is because there may be a need to draw on the knowledge of experts from different backgrounds if the research field is complex (Davis, 1992). As this research study focused on parental digital security practice, which encompasses a number of disciplines and is therefore by its very nature is complex, the experts that were selected were from different backgrounds that were relevant to the topic under study. Specifically, the experts were from the fields of digital citizenship, cybersecurity, public health, child and adolescent health, cyber parenting, and anthropology. This range of expertise was sought in order to ensure that the items selected would be representative and suitable for the various angles investigated in this research and that the selected items were based on the perspectives of the experts' respective backgrounds (Davis, 1992).

Furthermore, if a research study is based on a particular theoretical concept, engaging with experts in that area can be useful as well (Davis, 1992). This approach was therefore adopted for this study by recruiting an additional expert well versed in the concept of digital citizenship upon which this study was based. Apart from experts who can provide validity content-wise, experts who are familiar in instrument construction should be included as well (Davis, 1992). Thus, this study employed this approach by engaging with an expert who had vast experience in questionnaire validation and survey instrumentation.

The number of experts needed varies in the literature, ranging from 2 to 20, depending on the desired range of representation required on the panel (Davis, 1992; Grant & Davis, 1997). In this study, six experts were involved in the first round of content validation. Out of the initial six experts engaged from the first round, only four of them were involved in the second round of content validation. These numbers were deemed sufficient because the experts involved were adequately representing the necessary fields in digital security practice.

3.3.2 Population, Sample, Data Collection for the Scale Development Phase

3.3.2.1 Cognitive Debriefing

In the scale development phase, the participants who were recruited were a reflection of the target population of this study. A total of 10 participants were selected for the cognitive debriefing step which was deemed sufficient (Nanda et al., 2013). All the participants were recruited from Institute of Health Systems Research (IHSR) which provided the diverse background of participants needed. A list of staffs from IHSR was obtained, and these participants were recruited using purposive sampling based on age, ethnicity, gender, and education level.

In this study, the cognitive debriefing sessions were conducted in three small group settings using a dedicated discussion room in IHSR. Each group session consisted of three to four respondents. There are some advantages to conducting cognitive debriefings using small group settings. Indeed, group sessions are known to be useful in exploring the cognitive processes of respondents in questionnaire development (Czaja, 1998; Nanda et al., 2013). Firstly, the answers obtained through well-argued discussions can provide rich insights on ways to revise the questions and items (Nanda et al., 2013), which it might not be possible to obtain through individual interviews. Also, group discussions enable different views to be obtained on cognitive processes quickly with fewer resources (Czaja, 1998). Hence, for this study, the use of group discussions for cognitive debriefing is justifiable.

Although arguably, cognitive debriefings through individual interviews might yield a deeper understanding of cognitive processes, this study employed certain strategies to increase the depth of the cognitive findings derived from the group sessions. Firstly, the group sessions were limited to a maximum of four respondents per session. This was done to ensure that each respondent had adequate opportunities to elaborate on their cognitive processes as required in cognitive debriefings without compromising the benefits of group discussions. Secondly, the findings from earlier group sessions were used and built upon when conducting the subsequent sessions, thereby producing rich and comprehensive findings towards the end of the pretesting phase.

The cognitive debriefing process was carefully designed to maximise the feedback from the respondents. The probing technique was used in assessing the respondents' cognitive processes, and involved asking respondents certain questions to elicit their cognitive processes. This technique was performed after the respondents had answered the questionnaire. The probing technique was preferred because it has been shown to be more acceptable to respondents, as opposed to the well-known thinking aloud technique (Collins, 2003). A semi-structured guide (see Appendix D) was used to ensure that the cognitive processes of the respondents were comprehensively explored. This guide included probing questions that were aimed at eliciting the respondents' comprehension, retrieval, judgement, and response (Dillman et al., 1993; McColl et al., 2003; Mullin et al., 2000).

3.3.2.2 Test-retest reliability

In assessing the test-retest reliability of a questionnaire, a minimum of 30 participants is recommended in the literature (Bujang & Baharum, 2017). Hence this number was recruited for this study. Purposive sampling was used to recruit the participants based on the criteria as such:

i. Malaysian nationality

ii. Internet user

iii. Has at least one child aged below 18 years old who is an internet user

iv. Proficient in Malay or/and English language.

Participants were recruited from several workplaces, mainly from the National Institutes of Health under the Ministry of Health, Malaysia. The questionnaire was also passed to spouses via the participants whenever possible. The approach of using workplaces to recruit participants and their spouses ensures that the participants are traceable. This is particularly important when participants are involved in assessing the test-retest reliability of a questionnaire. Also, including spouses in the sample increases variation in the sample and the representation of those outside of the workforce. Where there are similarities in the cognitive processes used to assess the questionnaire items among diverse respondents, this gives an assurance that the items in the questionnaire will be uniformly understood by the study population at large. Furthermore, having access to a diversity of respondents helps in eliminating items that are not suitable for all parents.

3.3.3 Population, Sample, Data Collection for the Scale Evaluation Phase

In the scale evaluation, and in part of the scale development phase, a large field study was performed to obtain the necessary data. Purposive sampling was applied to recruit the participants for the field study based on the following criteria:

Inclusion criteria:

i. Malaysian nationality

ii. Parents who are internet users

iii. Has at least one child aged below 18 years old who is an internet user

iv. Proficient in Malay or/and English language.

Exclusion criteria:

i. Parents who are not physically, or/and mentally capable of providing accurate information for the study

ii. Parents who refused to participate in the study.

The sample size for the data collection conducted in this stage was determined based on the statistical methods used to determine the underlying domains, to explore dimensionality, internal consistency, and to confirm dimensionality and construct validity. In this study, the underlying domains and the exploration of dimensionality were determined through EFA. At least 100 observations are required for EFA (Hair et al., 2006). However, some studies suggest a minimum of 300 or 5:1 ratio per item as adequate for EFA (Comrey & Lee, 2013; Hinkin, 1995; Reise, Waller, & Comrey, 2000; Worthington & Whittaker, 2006).

Following this, the dimensionality and construct validity were determined through confirmatory factor analysis (CFA) and confirmatory composite analysis (CCA), which were both used in the measurement model assessment. Structural equation modelling (SEM) was used to examine the results of the CFA and CCA.SEM technique was preferred because it is able to determine the subsequent structural model assessment as well. In this study, the SEM technique that was applied was variance-based SEM for the reasons explained in Section 3.5.3.3.

For this study, the minimum sample size was calculated through power analysis using G-power software (Faul et al., 2009). By setting the effect size as medium, with an alpha value of 0.05, a power of 0.8 and the number of predictors as six (based on the conceptual framework), the estimated minimum sample size needed for variance-based SEM was found to be 98. Therefore, a total minimum sample of 400 participants was required for this study in order to perform EFA and SEM.

The data collection in the scale evaluation phase involved multicentre study sites. This was deliberate as this approach was expected to improve the variety of characteristics among the respondents involved in the data collection. The majority of the study sites were located in the state of Selangor. The state is located in Peninsular Malaysia in the west coast region (Department of Statistics. Malaysia, 2017). It has nine districts, as shown in Figure 3.6.

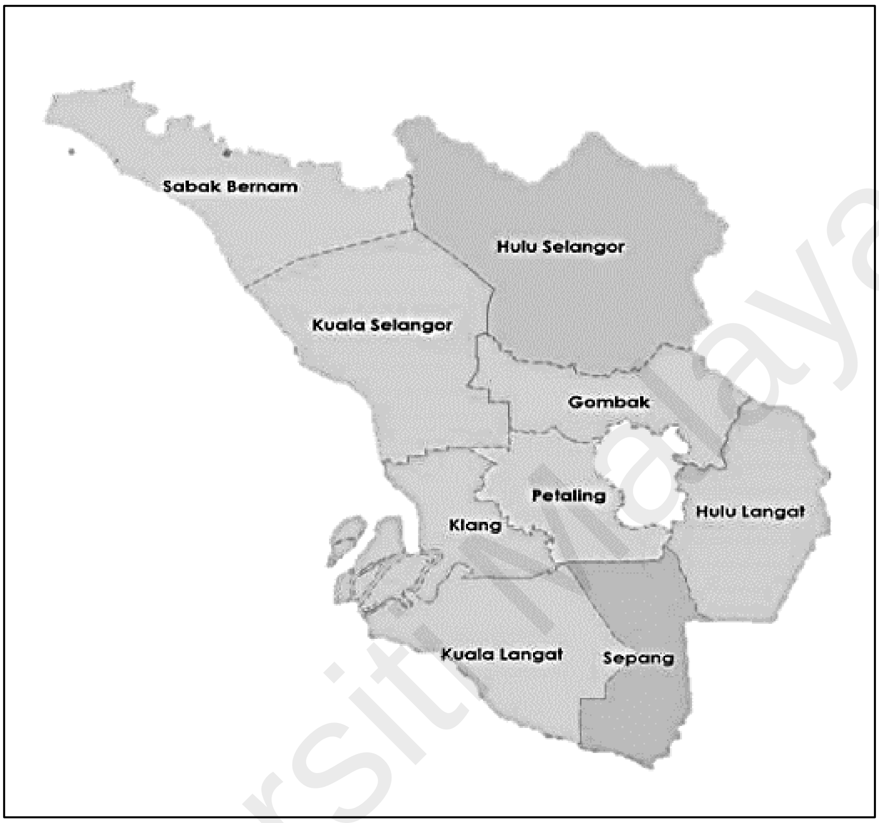

Figure 3.6: Districts in Selangor, Malaysia

Picture source: Selangor Economic Planning Unit. (2006). Selangor district map: Selangor State Department. Retrieved from http://www.selangor.gov.my/imageupload/Peta_Daerah_Negeri_Selangor-23Jul2006-064620.jpg

In 2016, Selangor had a total population of 6.3 million, which means it is one of the most highly populated states in Malaysia (Department of Statistics Malaysia, 2017). Moreover, Selangor accounted for 21% of the internet users in Malaysia, making the state the highest contributor of internet users in the country (MCMC, 2016). Furthermore, up to 97% of school children in Selangor were internet users in 2014 (CyberSecurity Malaysia, 2015). Hence, due to the high number of internet users in both the general population and the child population, an examination of these populations will greatly help in achieving the objectives of this study.

The study sites for this study included government and private health clinics. Data from the National Health Morbidity Survey 2015 revealed that almost 10% of the total population in Malaysia would utilise outpatient services in either a government or private setting (IPH, 2015). It was also noted from the same survey that 60% of those who utilise outpatient services are in the age group of above 18 years old (IPH, 2015). This setting thus provided a good opportunity to recruit participants from the community who belonged to various sociodemographic backgrounds.

The study sites that were involved in the field study are shown in Figure 3.7, from which it can be seen that the majority of the sites were located in Selangor and Klang Valley.

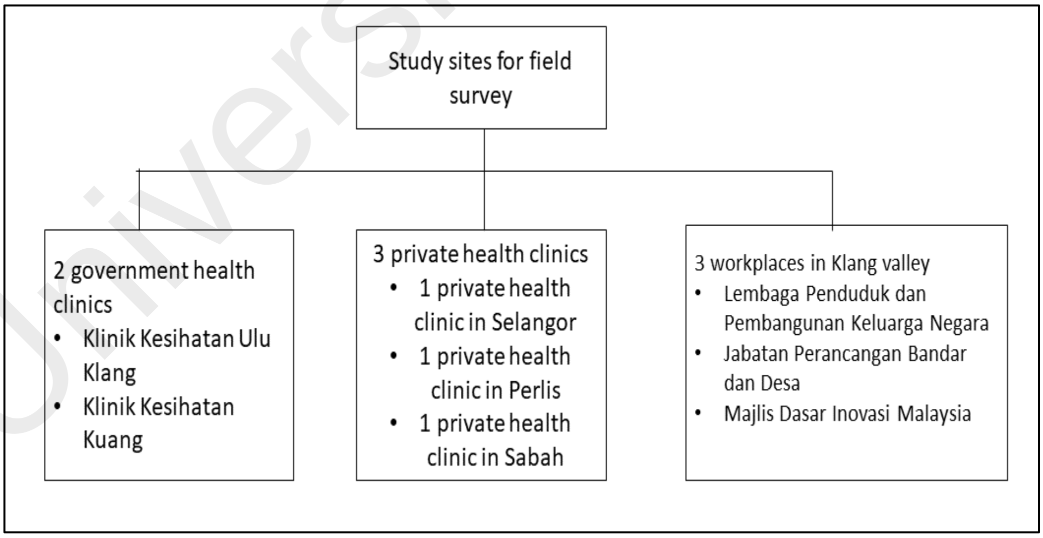
Study sites for field survey
2 government health clinics
• Klinik Kesihatan Ulu Klang
• Klinik Kesihatan Kuang
3 private health clinics
• 1 private health clinic in Selangor
• 1 private health clinic in Perlis
• 1 private health clinic in Sabah
3 workplaces in Klang valley
• Lembaga Penduduk dan Pembangunan Keluarga Negara
• Jabatan Perancangan Bandar dan Desa
• Majlis Dasar Inovasi Malaysia

Figure 3.7: Study sites involved in field study

Two government health clinics in Selangor were selected for data collection: Klinik Kesihatan Ulu Klang to represent the urban area in Selangor and Klinik Kesihatan

Kuang to represent the rural area of Selangor. A few private clinics from other major regions in Malaysia were approached as well. This resulted in the inclusion of one private clinic in the northern peninsular region (Perlis) and one private clinic in East Malaysia (Sabah). It was envisaged that the data obtained from these clinics would increase the variation in the respondents' backgrounds and characteristics due to the distinct characteristics of these different geographical regions. In addition, in collaboration with CSM, participants from various workplaces, particularly in Klang Valley and Selangor, were also approached. This was done by conducting the data collection during CSM's awareness talks at organisations and workplaces, in which the attendees at these talks were approached to request their participation in the study.

Prior to conducting the study, permission was obtained from relevant parties for each study site, such as the Ministry of Health, the State Health Departments and District Health Offices, and the Ministry of Science, Technology and Innovation as well as other authorities (see Appendix E). When permission had been obtained, the top management personnel of each study site were contacted and briefed on the study, ideally one month before the actual data collection. A member of personnel at each study site was identified and appointed as the site investigator in order to facilitate the data collection process. In addition, a dedicated WhatsApp group for each study site was created to facilitate constant communication between the researcher and the staff involved at each study site (see Appendix F).

The next few paragraphs describe the measures taken to ensure that the quality of the collected data was maintained. A briefing was conducted at each study site throughout the two-weeks prior to actual data collection. Ideally this briefing was face to face when possible. The briefing included familiarisation with the questionnaire content, handling the distribution and collection of questionnaires, and mechanisms for reporting to the researcher. Following the face-to-face briefing, information and clarification regarding the data collection process was constantly reinforced through the WhatsApp group. The data collection for the field study was conducted over three months, from October 2018 to December 2018.

The recruitment of the participants at the clinics required the assistance of selected clinic staff and nurses, specifically in screening for eligibility and in the distribution and collection of the questionnaires. The data collection process was also facilitated by the site investigator at each clinic. Adequate copies of consent forms and questionnaires were placed at the registration counter. Individuals who were eligible and met the inclusion criteria for participation in the study were asked by the clinic staff if they would agree to complete the questionnaire after they had registered with the clinic. Before completing the questionnaire, the participants were provided with an explanation about the study and their written consent was obtained. They were also assured that the confidentiality would be maintained (see Appendix H). The participants who agreed to proceed were asked to return the completed questionnaire to the registration counter. The returned questionnaires were kept in a special folder. In addition, for record-keeping purposes, designated clinic staff recorded on a form the number of participants who were eligible and how many of them agreed or disagreed to participate in the study. A flowchart of the participant recruitment process at the clinic sites can be found in Appendix G.

As regards to the recruitment process at workplaces, the liaison officer for the cybersecurity awareness talk at the respective organisation was approached and asked for their permission to conduct the validation of the questionnaire by involving employees attending the awareness talk. In each awareness talk involved, firstly, explanation of the study was given to the employees participating in the awareness talk by the researcher who was in attendance. Following that, the questionnaire together with the consent form were distributed to the audience prior to the talk. A designated time slot was provided for the audience to answer the questionnaire before the awareness talk commenced. Consent was taken by filling out the consent form, and the completed questionnaires were collected by the researcher himself by hand, in which the confidentiality was maintained throughout the process (see Appendix H). All the completed questionnaires were kept in a special folder by the researcher. Once this process was complete, the awareness talk would then commence.

Continuous monitoring of progress and troubleshooting was done through the dedicated WhatsApp group for each study site. The information about the data collection process was updated regularly on a dedicated monitoring board from researcher's operation area including the number of questionnaires distributed and completed for each study site. Appropriate actions were taken for any troubleshooting issues that were identified.

Prior to the administration of the questionnaire, training of the site investigators and clinic staff was conducted to ensure that the data collection ran smoothly. Training included the provision of details on the screening eligibility process, a guide on approaching potential participants, a guide on answering the questions in the questionnaire, details of the mechanism for safeguarding the completed questionnaires, and a guide on communicating updates and feedback between the researcher and staff on site throughout the data collection period. In addition, a standard operating procedure (SOP) document was developed for overall guidance (see Appendix I), and those involved in administering the study were made aware of the SOP and the details of the data collection process in order to ensure that the integrity of the data was maintained throughout the study. A monitoring form was also completed by designated staff during data collection to ensure that there was no discrepancy between the number of participants who agreed to participate and the number of questionnaires collected, and this form was reviewed on a continual basis (see Appendix J).

As mentioned above, the researcher ensured that the confidentiality of the participants was maintained. This was done by separating the consent form, which contained identifying details such as name and identity card number, from the questionnaire. However, each questionnaire was matched with the respective consent form based on a paired matching coding number. This was done to ensure that the participants' answers were traceable, but was only used if clarification was needed from the participant.

Appropriate data management strategies were employed throughout the data collection and analysis period. Data entry was conducted simultaneously with data collection. A weekly audit of data entry was performed by selecting 20 random samples and comparing the contents of the hard copies with the data entered. In addition, data cleaning was performed, and any clarification of the data that was needed was done by contacting the participants if necessary. Several backups of the data were made as well. This was done by storing the data in multiple copies in multiple locations, such as on an external drive and on a designated computer. To maintain the integrity and confidentiality of the data, the actual questionnaires and consent forms were placed in a designated area, which was only accessible to the members of the study team.

3.4 Instrumentation

This section describes the instruments that were used throughout the three major stages of the questionnaire development and validation process. Six instruments were used at different stages of this process: (1) a document analysis forms, including a data extraction form for the online search and a quality assessment form for the systematic review, (2) an online survey questionnaire for obtaining input from parents, (3) a content validity document protocol for experts, (3) a translation report form for the forward-backward translation process, (4) a self-report questionnaire draft for test-retest reliability and cognitive debriefing, (5) a semi-structured interview guide for cognitive debriefing, and (6) a self-report questionnaire for the field study (see Table 3.3).

Table 3.3: Instruments used in each phase of questionnaire development

Phase	Instrument
Item development	• Document analysis protocol • Online survey questionnaire • Content validity document protocol • Translation report form
Scale development	• Semi-structured interview guide • Self-report questionnaire
Scale evaluation	• Self-report questionnaire

3.4.1 Instrumentation for the Item Development Stage

In the item development stage, the document analysis forms that were used for the systematic review ensured that the extraction of information from each article was done in a systematic manner to facilitate evidence synthesis and quality assessment. The data extraction form included information on the characteristics of the study, including author(s), year, country of origin, the aim of the measurement, participants' characteristics, number of items, methods of administration, domains of PMT included, factor analysis used, and internal consistency score. Another form was used to assess the quality of the questionnaire development process mentioned in the article. This form included the reliability and validity components required for questionnaire development established by Cyril et al.(2015).

The online survey form for parents was dual language, namely, Malay and English. It contained a brief explanation of the study, demographic questions and three open-ended questions that addressed the concerns about digital security practice, the respondents' current practice and barriers to practice. The three open-ended questions were worded as follows: "What are your concerns when your children are online?", "What actions have you taken to ensure the safety of your children while they are online?", and "What are the barriers to performing actions to keep your children safe online?".

A document protocol was provided to the experts involved in content validation. In order to maximise their output, the reviewers needed to be well oriented with the conceptual basis of the study (Davis, 1992). To this end, Waltz, Strickland, and Lenz (2010) suggest providing a study description, theoretical definitions, and conceptual definitions of the intended domains and the items to the expert reviewers. Therefore, the protocol in this study contained the following (Streiner & Norman, 2008):

a) Written instructions explaining how to evaluate the scale

b) Overview of the domain and PMT

c) Description of the questionnaire

d) Copy of the actual questionnaire

e) Evaluation form for rating the items.

In the evaluation form, the experts were asked to rate each item in terms of clarity (How clear is this question to you?) and relevance (How relevant is this question to the domain?).

As for the content validation process, in this study this process was based on the literature and requisite steps were taken to ensure the quality of the content validation. However, even when steps have been taken, content validity is still subject to bias due to the qualitative nature of the data. Hence further psychometric properties are needed to be tested in order to validate this tool.

The review of the forwards-backwards translation by the expert panel was facilitated by a document which contained a few columns; the first column consisted of all the items of the original language of the questionnaire, followed by the two versions of translated questionnaires by two independent translators of the other language, and the last column that represented the translated version chosen for each item. The consensus of the panel was reflected in the items chosen in the last column.

3.4.2 Instrumentation for the Scale Development Stage

Two types of instrument were used in the scale development process. Firstly, a draft of the dual-language self- reported questionnaire, containing the items, the participant information sheet, consent form, and demographic questions was distributed to the participants in the cognitive debriefing. During the cognitive debriefing, the verbal probe technique was used (Di Lorio, 2005). Participants were first asked to answer the questionnaire. Following that, a debriefing session was conducted. Another instrument, namely, a semi-structured interview guide, was used to facilitate the debriefing. The semi-structured interview guide contained general questions aimed at assessing the overall mental processes and respondent burden, as well as specific questions for each item, in order to assess the participants' understanding of the keyword or phrases of each item. Feedback received at the debriefing sessions was then used to make revisions and produce another set of questionnaires that was used in the test-retest reliability assessment.

3.4.3 Instrumentation for the Scale Evaluation Stage

Lastly, the instrument that was built and revised in the scale development phase was administered to participants in the scale evaluation stage. Similar to the instrument in the scale development phase, the instrument used in the scale evaluation phase contained the revised items, participant information sheet, consent form, and demographic questions.

3.5 Analysis

Various analysis techniques were applied in each stage of the questionnaire development and validation process. This section describes the analysis techniques that were used in each stage.

3.5.1 Analysis in the Item Development Phase

In the item development phase, the articles retrieved in the systematic review were analysed qualitatively. Two aspects were analysed for each article, namely, the quality of the scale development methodology described and the quality of the measurement properties of the developed scale. The assessment of the quality of the methodology employed for scale development was performed based on three aspects: item development, reliability, and validity, in accordance with Cyril et al. (2015). The item development assessment included the usage of a literature review, an empirical study or a panel of experts in instrument development (Moher et al., 2009). The reliability assessment included whether test-retest reliability and internal consistency were reported (Moher et al., 2009). The validity assessment addressed content validity, structural and construct validity (Moher et al., 2009; Mokkink et al., 2010).

In addition to the above assessment of the methodology used for scale development, a quality assessment of the measurement properties of the scales was done using a rating scale developed by Cyril et al. (2015). Six criteria were used in the assessment, namely, using a theoretical framework, content validity, internal reliability of more than 0.7 (either Cronbach's alpha or CR), structural validity using EFA, internal construct validity (goodness-of-fit indexes) and external construct validity (convergent and discriminate properties of the scales). A score of 1 was given for each criterion that was fulfilled. Thus, a maximum of six points could be given to an article. The interpretation of the scores regarding the quality of the scales used in the studies was as follows: ≤2 = poor quality; 3-4 = medium quality; 5-6 = high quality (Cyril et al. (2015). Additionally, the items derived from the medium- and high-quality questionnaires were analysed and gathered in an inventory, in terms of the structure and keywords representing their respective domains. This inventory was used to design and generate the items for this study.

The inductive process of gathering input from parents through the online survey and from discussions with experts was also analysed qualitatively. Firstly, a thematic analysis was performed on the feedback received from parents. This was done by coding the responses that were extracted from the online survey. In order to strengthen the consistency as well as the identification of themes from the responses, continuous and iterative discussions took place between the members of the research team. The written answers that the respondents had given were analysed line by line to identify the codes. The number of codes was decreased gradually by removing similar and overlapping codes, which were then combined under sub-themes. Finally, the sub-themes were merged under similar themes. At the end of this process, the final set of themes were presented to the experts, and a thematic analysis was performed on any additional input based on the discussions with experts.

In the content validation process, the experts needed to rate the items based on clarity and relevance. Clarity was measured according to a four-point scale (1 = not clear, 2 = somewhat clear, 3 = clear, 4 = very clear). Relevance was also measured using a four-point scale (1 = not relevant, 2 = somewhat relevant, 3 = relevant, 4 = very relevant). The responses from the experts were gathered from their completed evaluation forms, and the level of agreement among the experts on content validity, in terms of clarity and relevance, was analysed. The level of agreement on each item was calculated using the content validity index (CVI), with the aim of obtaining a CVI value of at least 0.8 for an individual item and an overall CVI value of at least 0.9 (Lynn, 1986; Polit & Beck, 2006; Streiner & Norman, 2008). Additional feedback from the experts was also evaluated, and any necessary changes to the items were then made and sent back to the experts for re-evaluation. This iterative process was conducted until a satisfactory agreement level among the experts was reached in terms of the clarity and relevance of the items.

3.5.2 Analysis in the Scale Development Phase

3.5.2.1 Cognitive debriefing

In the scale development stage, the input from the participants in the cognitive debriefing sessions was analysed qualitatively and amendments were made based on the feedback received from the debriefings.

3.5.2.2 Test-retest reliability

Following this, the test-retest reliability assessment was performed the results of which were analysed based on the weighted kappa technique. The kappa coefficient represents the level of agreement reached by the same rater at two different times, known as intra-rater reliability, for each individual item. Weighted kappa with linear weightage was applied because each individual item was rated on an ordinal five-point Likert-type scale, and the difference between one point and another was of equal importance (Gwet, 2014). The values of the kappa coefficient were categorised in accordance with Landis (1977):

< 0: poor
0.01–0.20: slight
0.21–0.40: fair
0.41–0.60: moderate
0.61–0.80: substantial
0.81–1.0: almost perfect.

According to the literature (Landis, 1977; Walter, 1998), an acceptable level for the kappa coefficient is 0.4 and above, as this is deemed to indicate good temporal reliability. Thus, in this study, the value of 0.4 was used as the cut-off value for evaluating the items.

As part of the scale development phase, the subsequent data obtained from the field study was used for EFA and internal consistency analyses. However, prior to these analyses, the data collected from the field study was split randomly using SPSS to produce two separate datasets. The literature strongly suggests using a different dataset when performing EFA and the subsequent SEM for scale evaluation phase (Green, Tonidandel, & Cortina, 2016; Hair, Black, & Babin, 2010; Henson & Roberts, 2006). One set of data was used for the EFA and internal consistency assessment and the other set of data was used for SEM.

3.5.2.3 Exploratory Factor Analysis

Exploratory factor analysis was conducted as part of the construct validity assessment. The aim of EFA is to examine the existence of the dimensions proposed for a questionnaire in order to ensure that the items that are categorised under each dimension are strongly correlated with each other, as well as to identify items that are ‘weak’ (Streiner & Norman, 2008). In addition, this type of analysis can be used to explore dimensionality among the items, which is particularly useful for this study because the scale used in this study is newly developed. Exploratory factor analysis can also be used as a data reduction technique.

A few criteria need to be taken into account when exploring domains. Firstly, for factor analysis to proceed, the sampling adequacy criterion needs to be fulfilled. The Kaiser–Meyer–Olkin (KMO) statistic is a measure of sampling adequacy for factor analysis. A KMO value of more than 0.7 is considered good (Hair et al., 2010). Another statistical test that determines the suitability of data for factor analysis is Bartlett’s test of sphericity. This test is used to verify the null hypothesis that no relationships exist between any of the variables (items) (Nunnally, Bernstein, & Berge, 1967). If the Chi-square value is significant from the Bartlett’s test of sphericity, it means that there are discoverable relationships in the data and there is at least one domain present (Nunnally et al., 1967). In this study, the sampling adequacy was established by performing these two measurements prior to further EFA procedures.

The items must also be correlated adequately; not too low (lack of convergence) and not too high (extreme multicollinearity). Based on Cohen's criterion, a correlation value of more than 0.3 is considered sizeable (Cohen, 2013). Furthermore, Hair et al. (2010) state that a correlation value of more than 0.9 indicates the presence of multicollinearity.

When the suitability of the samples has been established, the domains can then be extracted. Two major types of extraction method have been proposed in the literature, namely, principal component analysis (PCA) and principal axis factoring. However, according to Worthington and Whittaker (2006), principal axis factoring should be the method of choice for a newly developed scale. This is because the main aim of using PCA is to reduce the number of items while retaining as much of the original item variance as possible (Worthington & Whittaker, 2006), reflecting the formative relationship between domains and items. On the other hand, principal axis factoring produces latent domains based on the shared variance among items (Worthington & Whittaker, 2006), reflecting the reflective relationship between domains and items. Thus, in this study, which involved developing a new scale which is in a reflective relationship between domains and items, principal axis factoring was used for extraction.

The number of domains to be extracted is based on certain criteria. According to the Kaiser criterion, domains with eigenvalues of less than 1.0 should not be retained and domains whose eigenvalues are greater than or equal to 1.0 should be retained (DeVellis, 2017). Thus, in this study, this criterion was applied in determining which domains to retain. Additionally, using Cattell's criterion, the scree test was also used to determine the number of domains to retain. The scree test (DeVellis, 2017; Worthington & Whittaker,

2006) is a visual inspection of the data that permits examination of the descending eigenvalues in order to locate a break in the size of the eigenvalues, after which the remaining values tend to level off horizontally (DeVellis, 2017; Worthington & Whittaker, 2006). The vertical portion of the scree plot has substantial domains while the horizontal portion is the scree that should be discarded (DeVellis, 2017). Cattell's criterion was applied in order to retain the domains that lie above the elbow of the plot (DeVellis, 2017).

Lastly, parallel analysis was also used to determine the number of extracted domains (Horn, 1965) using the Factor software version 10. In parallel analysis, multiple randomised datasets are generated from the original datasets and factor analysis is performed on both the original and the randomised generated datasets (Worthington & Whittaker, 2006). The number of domains to be retained is determined by comparing the eigenvalues of these two datasets (Worthington & Whittaker, 2006). A domain is retained if the eigenvalue of the original dataset is higher than that of the randomised dataset (Worthington & Whittaker, 2006). In this study, the adoption of parallel analysis in particular increased the confidence that the number of domains extracted was accurate. This is because, compared to Kaiser criterion and scree plot, the parallel analysis approach is the only technique that assesses the probability of whether a domain was formed due to chance (Wood, Akloubou Gnonhosou, & Bowling, 2015). Hence, its usage can minimise the overestimation of domains, taking into account the sampling error, and it is superior in terms of accuracy as compared to reliance on factor analysis alone (Wood et al., 2015).

Following factor extraction, factor rotation was performed. Factor rotation strengthens the relationship between the variables (items) and a domain (Nunnally et al., 1967), thereby producing a solution with the best structure. Factor rotation increases interpretability by identifying clusters of variables (items with a strong association with only one and the same domain) (DeVellis, 2017). Oblique rotation such as Promax is preferred because it provides a more realistic representation of how domains are interrelated (Worthington & Whittaker, 2006). This is because oblique rotation takes the assumption that the domains are correlated to a certain degree. This technique was used in this study because it mimics the real-world relationship and it was expected that the variables of interest in this study would influence one another and would not influence the dependent variable in isolation.

For each domain, the items were retained based on the factor loading value for the individual item and the absence of cross-loading. The factor loading represents the correlation between the latent domain and an individual item. Hair et al. (2010) suggest that a factor loading value of more than 0.7 is desirable but it must be at least 0.4. Cross-loading occurs when an item loading differences are less than 0.15 between two domains (Worthington & Whittaker, 2006).

By performing the steps outlined above, the assumption that the domains were appropriately extracted was met. Lastly, the conceptual interpretability of each domain was performed.

Conceptual interpretability is a definitive domain-retention criterion. A domain must be retained only if it can be interpreted in a meaningful way, no matter how solid the evidence for its retention based on the empirical criteria described above (Worthington & Whittaker, 2006). Therefore, the recommendation is to consider a relevant theory when determining the appropriate number of domains to retain (Fabrigar, Wegener, MacCallum, & Strahan, 1999). Thus, the domains extracted were interpreted and compared with the underlying PMT domains whenever possible.

3.5.2.4 Internal Consistency Analysis

After the domains and dimensionality had been explored, the internal consistency analysis and item reduction process were performed using the same dataset as for EFA, by examining both the Cronbach's alpha value for each domain and the corrected item-total correlation (CITC) for each item in its respective domain. The rationale for examining both of these parameters is explained in the following paragraphs. A value of more than 0.3 for the CITC (Cristobal, Flavián, & Guinaliu, 2007) and a value of more than 0.7 for Cronbach's alpha (Cortina, 1993) are considered acceptable.

Cronbach's alpha has been used extensively in determining the internal consistency of domains (Cortina, 1993). However, many issues can arise in relying on Cronbach's alpha alone. Firstly, Cronbach's alpha tends to underestimate the reliability value (DeVellis, 2017). This is because the accuracy of Cronbach's alpha relies on the assumption of tau-equivalence (Cortina, 1993). The tau-equivalence assumption implies that all items need to be equally good items of the single domain that they share (DeVellis, 2017). If this assumption is violated, the Cronbach's alpha values tend to be underestimated. In a practical sense, the assumption of tau-equivalence is difficult to achieve because most items possess a different value of covariance to that of their domain. As such, the Cronbach's alpha value produced might be lower than the true reliability score. Secondly, the Cronbach's alpha value might not reflect accurately the individual items' intercorrelation (Cortina, 1993). For instance, if one item has low correlation while the remaining items in a domain are highly correlated, the Cronbach's alpha value tends to be reasonably good. This is because the value is artificially inflated due to the high correlation between items which dampens the effect of the unrelated item in the domain.

However, the Cronbach's alpha value is still deemed a valid measure. Hence it was used to determine the internal consistency at this stage of the study for a few reasons. Firstly, because Cronbach's alpha tends to represent a lower bound of reliability, the value obtained serves as a conservative level of reliability (DeVellis, 2017). Secondly, in item development process it was found that the items conformed to unidimensionality, thus the essential tau-equivalent assumption was met to a certain extent by the set of items. Hence, it was considered that the effect of the tau-equivalent violation was reduced. Thirdly, at the item level, in order to ensure that each of the items were intercorrelated and consistent, the CITC value was examined, in line with the suggestions in the literature (see e.g., Boateng et al., 2018; DeVellis, 2017). The CITC reflects the correlation between the item and the sum score of the remaining items bar itself. Thus, the CITC is a preferred technique in determining whether each item is adequately correlated with the other items in a particular domain (Boateng et al., 2018).

Hence, in this study, the internal consistency was examined based on the overall set of items using Cronbach's alpha, and at the individual item level using the CITC. The use of both techniques provided a high degree of confidence that the internal consistency among the items in their respective domains was good.

3.5.3 Analysis in the Scale Evaluation Phase

In the scale evaluation phase and part of the scale development phase, the analysis that was performed was mainly done to establish the construct validity of the questionnaire. The main process involved in this phase was using the SEM technique.

3.5.3.1 PLS-SEM justification

Following the EFA and the item reduction process which was based on reliability measures, the validation process was further enhanced by examining the measurement model and the structural model of the proposed questionnaire. First, the measurement model assessment explored the construct validity and confirmation of the domains. Then a structural model assessment was undertaken to determine the path analysis of the model. As mentioned earlier, SEM is the preferred technique for performing these analyses.

Generally, there are two types of SEM, namely, variance-based SEM and covariance-based SEM (CB-SEM). In this study, variance-based SEM, also known as partial least squares SEM (PLS-SEM) was used. The decision to use PLS-SEM was based on a number of reasons.

Firstly, PLS-SEM is more suitable for predicting key domains and when the nature of the study leans towards theory exploration rather than theory confirmation (Hair, Hult, Ringle, & Sarstedt, 2016). In developing the parental digital security questionnaire, one of the objectives was to discover whether the domains formed would influence parental digital security practice. Also, the nature of this study was exploratory because, as far as the researcher was aware, the application of PMT to parental digital security practice was a novel aspect of this research.

Secondly, compared to other modelling and analysis methods, PLS offers the flexibility of permitting latent domains to be modelled either as reflective or formative domains (Hair et al., 2016). In this study, the proposed model used for SEM contained formative domains. Hence it was more appropriate to use PLS-SEM.

Thirdly, PLS-SEM is preferred over CB-SEM when the model is complex (Hair et al., 2016). The proposed conceptual model in this study was a higher-order model. Specifically, the model was a reflective-formative design, also known as a type II model (Hair et al., 2016). The exploration of a type II model warrants the use of PLS-SEM over CB-SEM due to the former's advantages in dealing with the structure of this type of model. Therefore, in this study, the use PLS-SEM in conducting the measurement model assessment and structural model assessment was justifiable.

3.5.3.2 Preliminary data assessment prior to PLS-SEM analysis

Prior to the PLS-SEM analysis, missing data and outliers were examined and treated accordingly. Although PLS-SEM can handle missing data and outliers to a certain extent, cleaning the data by checking these two aspects is still appropriate and strongly recommended when performing statistical analysis (Hair et al., 2016).

In addition, when using a multivariate analysis technique such as SEM, a multivariate normality assessment needs to be performed. This assessment was performed in this study because it would provide a picture of the normality of the data that would then guide the researcher on the appropriate steps to take in handling the data during analysis.

Another issue that was addressed was common method bias. This is a type of systematic error that can arise in a measurement tool. The presence of common method bias indicates that the variance found in the model is due to the measurement method as opposed to the actual domains that the measurement tool is supposed to represent (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). This is a particularly important issue to address in a single-source respondent survey technique, such as the one employed in this study, in which the independent and dependent variables are collected from the same source (Podsakoff et al., 2003). As such, it is recommended that a full collinearity test is used to detect the presence of common method bias (Kock & Lynn, 2012). Hence this test was used in this study prior to the SEM analysis.

3.5.3.3 Measurement and structural model assessment using PLS-SEM

The measurement model assessment was performed to determine the relationship between the items and their respective domains. This assessment was performed by using the CFA procedure which was particularly suitable for the reflective items. Specifically, CFA was used to examine the reliability of the domains, the construct validity, and the convergent validity and discriminant validity of the domains (Brown, 2014; Hair et al., 2016). As for the higher-order domains, which are formative in nature, the collinearity and significance weight of the domains were assessed using CCA (Hair et al., 2016).

When assessing the convergent validity, the criteria examined included factor loadings and the average variance extracted (AVE). Loading values equal to and greater than 0.5 are acceptable if the summation of the loadings results in high loading scores, contributing to AVE scores of greater than 0.5 (Byrne, 2016). The AVE should exceed 0.5 to give confidence that there is adequate convergent validity (Bagozzi & Yi, 1988; Fornell & Larcker, 1981).

Traditionally, discriminant validity is assessed based on the Fornell–Larcker criterion. However, there are several shortcomings associated with using this criterion for assessing discriminant validity and it is deemed unreliable (Henseler, Ringle, & Sarstedt, 2015). The heterotrait-monotrait (HTMT) ratio was developed to overcome these shortcomings (Henseler et al., 2015). A HTMT ratio which is closer to 1 indicates a lack of discriminant validity. The cut-off value for the HTMT ratio is 0.85 (Henseler et al., 2015). This is the most stringent criterion that can be used to assess discriminant validity; hence it was applied in this study.

As regards the internal consistency of the measurement model, this was assessed by examining the composite reliability (CR), rather than by Cronbach's alpha. This is because Cronbach's alpha has a few limitations, including its tendency of being influenced by a number of items which tends to lead to an underestimation of the internal consistency reliability (Hair et al., 2016; McNeish, 2017). Composite reliability, which measures the reliability of a set of items, is able to overcome these limitations in assessing internal consistency. The CR value needs to be at least 0.7 to indicate that there is adequate internal consistency (Gefen, Straub, & Boudreau, 2000).

As for the higher-order formative domains, the measurement model assessment was based on collinearity and the contribution of the formative subdomains to a particular domain, as recommended by Hair et al. (2016). The aim of assessing the formative subdomains is to avoid collinearity. This is because high levels of collinearity between formative subdomains will have an impact on the estimation of weights and their statistical significance. In this study, the collinearity level was determined through the variance inflation factor (VIF). A VIF value of below 3.3 is deemed to indicate no issue of multicollinearity (Diamantopoulos & Siguaw, 2006).

The relevance and significance of the formative subdomains are based on outer weight values (Hair et al., 2016). The values of the outer weights can be compared with each other and can, therefore, be used to determine each item's relative contribution to the domain or its relative importance. The statistical significance of the outer weight values further indicates that the formative subdomains truly contribute to the formation of their respective domain (Hair et al., 2016).

After the measurement model assessment had been completed, the structural model assessment was performed. The assessment was based on the inner model structure, i.e., the latent variables of the model. This assessment was conducted by examining collinearity, the path coefficient, the effect size, and the coefficient of determination (R^2), as suggested by Hair et al. (2016).

When two variables are collinear, they are said to be the same or to represent the same underlying meaning. This needs to be avoided in a valid instrument because, ideally, each variable needs to represent a unique aspect of the model. In the structural model assessment, collinearity among the latent variables was assessed through the use of the VIF. The threshold value for the structural model VIF was 3.3, as recommended by Diamantopoulos and Siguaw (2006). This means that if the VIF value of the latent variables is equal to or more than 3.3, the model can be considered to have multicollinearity issues.

The path coefficient was used to assess the relationship among the latent variables. As PLS does not rely on distribution assumptions, inference statistics such as significance testing of the relationship among the latent variables might be an issue. A non-parametric technique such as bootstrapping would be able to overcome this. Hence, in this study, the path coefficients were obtained through the bootstrapping technique. Bootstrapping involves applying a resampling technique with sample replacement to gauge the population parameter. The path model is estimated for each bootstrap sample. The resulting estimates can be viewed as approximations of the sampling distribution. Each bootstrap sample produces a standard error. Ultimately, the bootstrap standard error is used to compute the inference statistics (Hair et al., 2016). The larger the iteration process, i.e., the larger the bootstrap samples, the more normal the standard error distribution becomes. Thus, the inference statistics produced in this way can provide a good approximation of the population parameter (Hair et al., 2016).

The coefficient of determination, R^2, represents the combined effects of the exogenous latent variables on the endogenous latent variable. The value of R^2 ranges from 0 to 1. Falk and Miller (1992) recommend that the R^2 values should be equal to or greater than 0.10 in order for the explanation of the variance of a particular endogenous domain to be deemed adequate. As regards the level of variance explained, Hair et al. (2016) suggest that a cut-off value of R^2 0.75 denotes that a substantial amount of variance is explained, while a value of 0.50 represents a moderate and a value of 0.25 a weak level of variance explained.

Lastly, the F^2 effect size measures the impact that each exogenous domain has on the endogenous domain. It is measured by examining the change in the R^2 value when a specified exogenous domain is omitted from the model. This study followed the guideline proposed by Cohen (2013), in which F^2 effect size values of 0.02, 0.15, and 0.35 represent, respectively, a small, medium, and large effect of the exogenous domain.

3.6 Ethics Approval

This study was registered on the National Medical Research Register (NMRR), under NMRR number NMRR-17-3093-39434 (IIR). Ethical clearance was obtained from the Medical Research and Ethics Committee (MREC) of the Ministry of Health Malaysia and the University Malaya Research Ethics Committee (UMREC) under reference number UM.TNC2/UMREC – 211 (see Appendix B).

3.7 Summary of Chapter Three

In summary, this chapter first provided details of the research design highlighting the three major phases of questionnaire development, namely, item generation, scale development, and scale evaluation. The chapter then described the various data collection processes used, including an online survey aimed at parents, engagement with experts for item generation, and cognitive debriefing sessions to obtain feedback from parents, as well as the conduct of a self-reported survey among parents at various study sites for scale development and scale evaluation. Following this, the chapter explained how various instruments were used in different stages of the questionnaire development process, including the document analysis forms for the systematic review, online survey questionnaire for parents, content validity document protocol for experts, semi-structured interview guide for cognitive debriefing, translation report, and the self-report questionnaire itself. Lastly, the chapter elucidated how the qualitative and quantitative analyses were performed in the questionnaire development process. Specifically, it highlighted that qualitative analysis using thematic analysis was more prominent in the item generation stage, while quantitative analysis was used in determining reliability and validity in the scale development and scale evaluation stages of the questionnaire development process.

CHAPTER FOUR: RESULTS

4.1 Introduction

This chapter presents the findings of this study. The earlier part of the chapter concentrates on the findings in the item development stage, namely, domain identification, generation of the items, and translation of the items. Subsequently, the scale development findings are presented, particularly those obtained from the cognitive debriefing sessions and from the test-retest reliability assessment. The latter part of the chapter focuses on the construct validity of the questionnaire, and explains the factor analysis and internal consistency assessment of the domains produced. Lastly, the chapter presents the findings of the SEM analysis, namely, the measurement model and structural model assessments.

4.2 Domain Identification in the Item Development Phase

As highlighted earlier in the section on the conceptual framework, the domains that were identified were heavily influenced by the components of PMT. The domains were *perceived susceptibility, perceived severity, perceived maladaptive reward, perceived cost, perceived self-efficacy, perceived response efficacy* and *parental digital security practice*. These domains were identified as having the potential to explain parental digital security practice. The subsequent item generation processes were based on these domains.

4.3 Item Generation through the Systematic Review in the Item Development Phase

The initial database search generated 502 articles. When the identified duplicates were removed (n = 52), this left 450 articles for screening. Title and abstract screening yielded 60 articles. The full texts of these articles were obtained, read and screened for eligibility. As a result of the full-text screening, 30 articles were excluded. Then, cross-referencing was performed on the remaining articles (n = 30), which led to the inclusion of an additional three articles, giving a final number of 33 accepted studies (Figure 4.1).

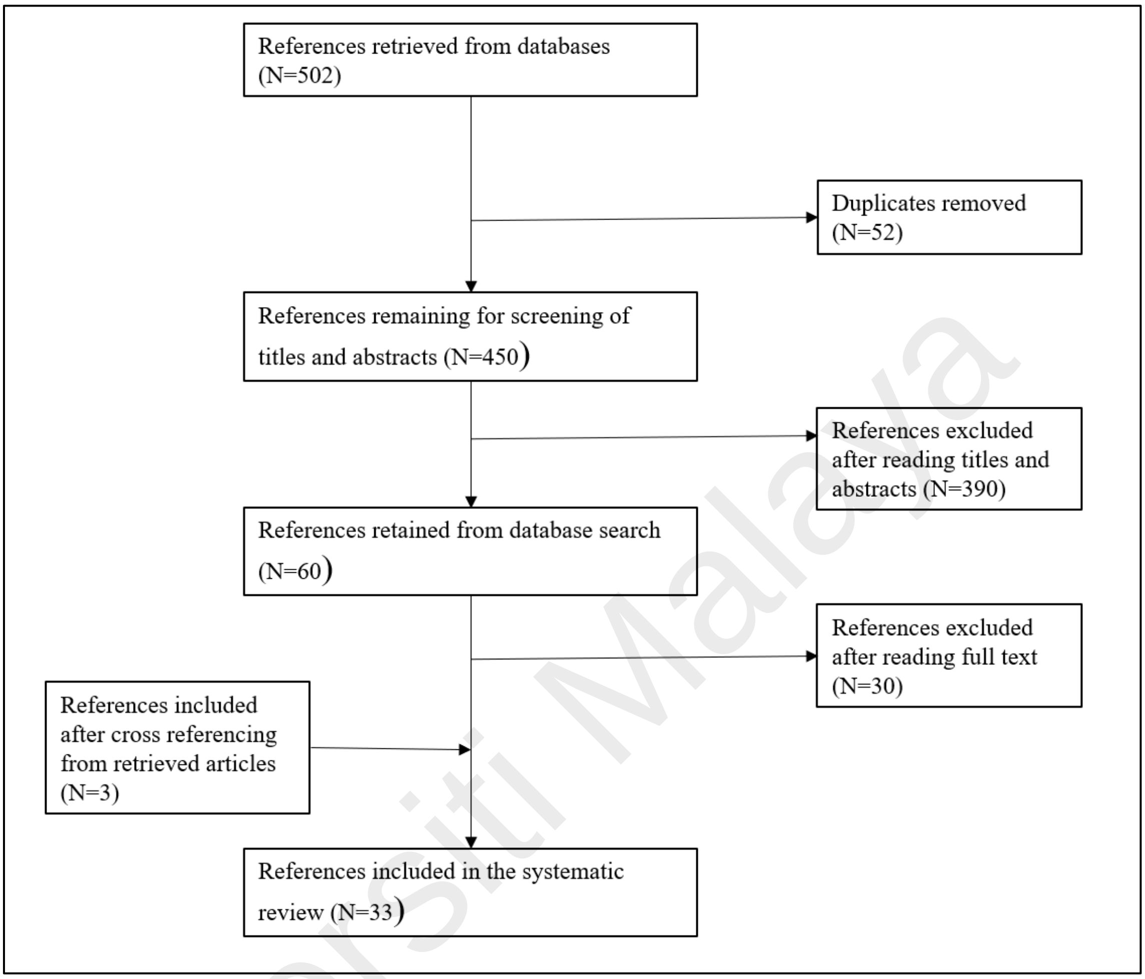
References retrieved from databases (N=502)
Duplicates removed (N=52)
References remaining for screening of titles and abstracts (N=450)
References excluded after reading titles and abstracts (N=390)
References retained from database search (N=60)
References excluded after reading full text (N=30)
References included after cross referencing from retrieved articles (N=3)
References included in the systematic review (N=33)

Figure 4.1: Flow chart of study selection process

4.3.1 Characteristics of the Included Studies

Out of the 33 studies included, 19 originated from North America (USA = 18 articles, Canada = 1) (Anderson & Agarwal, 2010; Aurigemma & Mattson, 2018; Boehmer et al., 2015; Burns et al., 2017; Chai et al., 2009; Crossler et al., 2014; Doane et al., 2016; Gurung et al., 2009; Herath & Rao, 2009; Ifinedo, 2012; Johnston & Warkentin, 2010; Lee & Larsen, 2009; Menard et al., 2014; Meso et al., 2013; Thompson et al., 2017; Tsai et al., 2016; Tu et al., 2015; Visinescu et al., 2016; Warkentin et al., 2016), nine from

Asia (Malaysia = 3, South Korea = 2, China = 1, Indonesia = 1, Taiwan = 1, Singapore = 1) (Chou & Chou, 2016; Hina & Dominic, 2017; Hoon Kim et al., 2014; Hovav & Putri, 2016; Lwin et al., 2012; Mohamed & Ahmad, 2012; Safa et al., 2015; Yoon et al., 2012; Zhang et al., 2017), four from Europe (Finland = 3, Holland = 1) (Jansen & van Schaik, 2017; Johnston et al., 2015; Siponen et al., 2014; Vance et al., 2012), and one from Oceania (Australia = 1) (Dang-Pham & Pittayachawan, 2015).

The sample sizes in the studies ranged from 68 to 1200 participants. The populations studied were diverse. Of the 33 studies, 11 involved employees of organisations (Burns et al., 2017; Herath & Rao, 2009; Hina & Dominic, 2017; Hoon Kim et al., 2014; Hovav & Putri, 2016; Ifinedo, 2012; Johnston et al., 2015; Lee & Larsen, 2009; Safa et al., 2015; Siponen et al., 2014; Vance et al., 2012), 11 involved university students (Aurigemma & Mattson, 2018; Crossler et al., 2014; Dang-Pham & Pittayachawan, 2015; Gurung et al., 2009; Johnston & Warkentin, 2010; Menard et al., 2014; Meso et al., 2013; Mohamed & Ahmad, 2012; Visinescu et al., 2016; Warkentin et al., 2016; Yoon et al., 2012), six involved home users (Anderson & Agarwal, 2010; Burns et al., 2017; Jansen & van Schaik, 2017; Thompson et al., 2017; Tsai et al., 2016; Tu et al., 2015), four involved adolescents and young adults (Boehmer et al., 2015; Chai et al., 2009; Doane et al., 2016; Lwin et al., 2012), and one involved teachers (Chou & Chou, 2016).

The areas of digital security examined in all the studies can be divided into two general contexts: organisational and individual. Among the studies, 11 focused on digital security in the organisational context (Burns et al., 2017; Herath & Rao, 2009; Hina & Dominic, 2017; Hoon Kim et al., 2014; Hovav & Putri, 2016; Ifinedo, 2012; Johnston et al., 2015; Lee & Larsen, 2009; Safa et al., 2015; Siponen et al., 2014; Vance et al., 2012). From these 11 studies, 10 looked into organisational behaviour, including compliance with organisational information security policies. The remaining study (Lee & Larsen,

2009) examined employees' utilisation of anti-malware software. In the individual context, five studies examined digital threats related to human behaviour and interaction, such as privacy (n = 3) (Chai et al., 2009; Mohamed & Ahmad, 2012; Zhang et al., 2017), cyberbullying (n = 1) (Doane et al., 2016) and online harassment (n = 1) (Lwin et al., 2012). The remaining 17 studies examined individual abilities and measures in relation to digital security, such as the use of anti-malware, cloud backup, anti-spyware, and password protection (Anderson & Agarwal, 2010; Aurigemma & Mattson, 2018; Boehmer et al., 2015; Gurung et al., 2009; Johnston & Warkentin, 2010; Yoon et al., 2012; Meso et al., 2013; Chou & Chou, 2016; Crossler et al., 2014; Dang-Pham & Pittayachawan, 2015; Jansen & van Schaik, 2017; Menard et al., 2014; Thompson et al., 2017; Tsai et al., 2016; Tu et al., 2015; Visinescu et al., 2016; Warkentin et al., 2016;). None of the studies addressed the issues of cyber parenting or parental digital security. Table 4.1 provides a summary of the 33 selected studies.

Table 4.1: Characteristics of articles reviewed in the systematic review

Author	Year	Objective(s)	Country	Participants	Context	Theories used	No. of domains	No. of items	Questionnaire administration	Factor analysis (EFA/ CFA)	Internal consistency (reliability)
Gurung	2009	To develop a research framework and empirically analyse the factors that motivate consumers to adopt and use anti-spyware tools when they are faced with security threats	USA	232 students	Use of anti-spyware	PMT	5	17	Self-report	CFA	Cronbach's alpha
Chai	2009	To examine factors that influence internet users' private-information-sharing behaviour	USA	285 teenagers	Information privacy protection behaviour	PMT, social cognitive theory	7	18	Self-report	EFA	Cronbach's alpha
Lee	2009	To examine the determinants affecting the adoption by the executives of small and medium-sized businesses (SMBs) of anti-malware software for their organisations by using PMT	USA	239 executives of SMBs	Anti-malware software adoption	PMT	11	29	Self-report	CFA	Cronbach's alpha

Table 4.1, continued

Author	Year	Objective(s)	Country	Participants	Context	Theories used	No. of domains	No. of items	Questionnaire administration	Factor analysis (EFA/ CFA)	Internal consistency (reliability)
Herath	2009	To evaluate the effect of employees' organisational commitment on security policy compliance intentions	USA	312 employees	Information security compliance at organisation level	PMT Information security adoption Deterrence Theory Organisational Behaviour	14	43	Self-report	EFA CFA	Composite reliability
Anderson	2010	To examine the factors influencing home computer users' security behaviour	USA	594 home computer users	Online safety among home users	PMT	8	NA	Self-report	NA	Cronbach's alpha
Johnston	2010	To investigate the influence of fear appeals on the compliance of end users with recommendations to enact specific individual computer security actions to mitigate threats	USA	275 university students	Security actions of computer-savvy individuals	PMT	6	24	Self-report	CFA	Composite reliability

Table 4.1, continued

Author	Year	Objective(s)	Country	Participants	Context	Theories used	No. of domains	No. of items	Questionnaire administration	Factor analysis (EFA/ CFA)	Internal consistency (reliability)
Vance	2012	To evaluate usage of PMT in predicting compliance with information system security procedures	Finland	210 clerical and administrative staff of an organisation	Information security compliance at the organisation level	PMT	9	33	Self-report	EFA	Cronbach's alpha
Lwin	2012	To examine the predictors motivating the intention of youth to adopt protection behaviour against online harassment	Singapore	537 high school students	Protection against online harassment among adolescents	PMT	5	35	Self-report	-	Cronbach's alpha
Ifinedo	2012	To investigate information system security policy compliance	Canada	124 adults (managers in Canadian organisations and information system professionals)	Information security compliance at the organisation level	PMT, TPB	8	45	Self-report	CFA	Composite reliability
Yoon	2012	To understand students' information security behaviours	South Korea	202 students	Information security behaviour	PMT, Habit theory	9	23	Self-report	CFA	Composite reliability

Table 4.1, continued

Author	Year	Objective(s)	Country	Participants	Context	Theories used	No. of domains	No. of items	Questionnaire administration	Factor analysis (EFA/ CFA)	Internal consistency (reliability)
Mohamed	2012	To gain insights into information privacy concerns, their antecedents and the use of privacy measures in social networking sites	Malaysia	340 undergraduate students	Privacy measure use in social networking sites	PMT, social cognitive	6	21	Self-report	CFA	Composite reliability
Meso	2013	To compare the influence of information security knowledge garnered from lectures-only courses with that garnered from courses emphasising hands-on projects, on students' post-training security behaviour	USA	77 students	Information security compliance at the individual level	PMT	6	19	Self-report	CFA	Cronbach's alpha
Crossler	2014	To test PMT against a unified measure of security-related practices (USP)	USA	81 graduate students	Information security	PMT, USP	12	30	Self-report	CFA	Cronbach's alpha
Siponen	2014	To validate empirically a new multi-theory-based model on security compliance	Finland	669 employees of Finnish corporations from various business sectors	Information security compliance at the organisation level	PMT, TRA, cognitive evaluation	9	29	Self-report	EFA	Cronbach's alpha

Table 4.1, continued

Author	Year	Objective(s)	Country	Participants	Context	Theories used	No. of domains	No. of items	Questionnaire administration	Factor analysis (EFA/ CFA)	Internal consistency (reliability)
Hoon	2014	To find the factors that influence the members of an organisation to comply with the organisational information security policy	South Korea	194 employees	Information security compliance at the organisation level	PMT, TRA, Neutralisation theory	15	46	Self-report	CFA	Cronbach's alpha
Menard	2014	To explore users' intentions to utilise the cloud for their data backup efforts	USA	152 university students	Utilisation of cloud system for data backup	PMT	4	7	Self-report	EFA	Composite reliability
Boehmer	2015	To test the relationship between personal responsibility for online safety and other protection motivation theory (PMT) variables	USA	565 college students	Online safety behaviour	PMT	16	88	Self-report	EFA	Cronbach's alpha
Dang-Pham	2015	To examine malware-avoidance behaviours among personal mobile device users	Australia	252 higher education (university) students	Malware-avoidance behaviour in a bring-your-own-device (BYOD) setting	PMT	7	25	Self-report	EFA	Cronbach's alpha
Johnston	2015	To explore the effectiveness of an enhanced fear appeal rhetorical framework	Finland	559 employees of multiple suborganisations	Testing fear appeal for three different scenarios involving	PMT, Fear appeal	10	Not available	Self-report	EFA	Cronbach's alpha

Table 4.1, continued

Author	Year	Objective(s)	Country	Participants	Context	Theories used	No. of domains	No. of items	Questionnaire administration	Factor analysis (EFA/ CFA)	Internal consistency (reliability)
		through the use of a hypothetical scenario research design involving three unique threat/behaviour pairs that are typical of fear appeal implementations in practice		within the same city government	information security at the organisation level	rhetorical framework					
Tu	2015	To understand the security behaviours of mobile users with respect to mobile loss/theft	USA	339 users	Digital security among mobile users	PMT, Social learning theory	7	23	Self-report	EFA	Cronbach's alpha
Safa	2015	To change users' behaviour to conscious care behaviour in the domain of information security	Malaysia	212 employees	Information security compliance at the organisation level	PMT, TPB	9	43	Self-report	CFA	Cronbach's alpha
Visinescu	2016	To test a model that explains the mechanisms that lead individual users to develop a protection strategy for data storage	USA	203 young adults and university students	Protection strategy for individuals' safe use of software testing as a service	PMT, theory of self preservation	8	27	Self-report	EFA	Cronbach's alpha

Table 4.1, continued

Author	Year	Objective(s)	Country	Participants	Context	Theories used	No. of domains	No. of items	Questionnaire administration	Factor analysis (EFA/ CFA)	Internal consistency (reliability)
Warkentin	2016	To assess the predictive capabilities of the proposed protective security behaviour continuance model in respect of security software utilisation behaviour	USA	253 experienced computer users who were undergraduate students	Utilisation of security software among individuals	PMT	6	22	Self-report	EFA	Composite reliability
Doane	2016	To examine the ability of PMT to explain electronic communication behavioural intentions, actual electronic communication behaviours and cyberbullying victimisation	USA	577 college students	Cyberbullying	PMT	10	> 35	Not mentioned	-	Cronbach's alpha
Tsai	2016	To examine how classical and new PMT factors predict online safety intentions	USA	988 median 24-year-olds	Online safety among home users	PMT	11	52	Self-report	-	Cronbach's alpha
Chou	2016	To explore factors that relate to teachers' information security behaviour	Taiwan	505 teachers	Information security behaviour	PMT	5	34	Self-report	EFA	Cronbach's alpha

Table 4.1, continued

Author	Year	Objective(s)	Country	Participants	Context	Theories used	No. of domains	No. of items	Questionnaire administration	Factor analysis (EFA/ CFA)	Internal consistency (reliability)
Hovav	2016	To examine employees' intention to comply with organisational BYOD security policies	Indonesia	230 employees in an organisation with a BYOD policy	Information security behaviour in a BYOD setting at the organisation level	PMT, Reactance theory	8	44	Self-report	CFA	Cronbach's alpha
Hina	2017	To investigate the integration of PMT and the theory of planned behaviour (TPB) in information security policy compliance among Malaysian university employees	Malaysia	68 faculty and staff of public and private universities	Information security at the organisation level	PMT, TPB	11	44	Self-report	EFA	Cronbach's alpha
Thompson	2017	To improve understanding of personal computing and mobile device security behaviour based on PMT	USA	629 personal computing users: 322 home computer (desktop/laptop) users and 307 mobile device (smartphone/	Security behaviour of personal computing and mobile device users	PMT, TPB	11	52	Self-report	EFA	Cronbach's alpha
Jansen	2017	To evaluate three models in terms of their effectiveness in explaining precautionary online behaviour	Holland	1200 users	Digital security among online banking end users	PMT, Reason action approach	10	31	Self-report	CFA	Composite reliability

Table 4.1, continued

Author	Year	Objective(s)	Country	Participants	Context	Theories used	No. of domains	No. of items	Questionnaire administration	Factor analysis (EFA/ CFA)	Internal consistency (reliability)
Burns	2017	To explore the relationship between insiders' psychological capital and the mechanisms of PMT	USA	377 organisational insiders	Digital security at the organisation level	PMT	8	35	Self-report	CFA	Composite reliability
Zhang	2017	To explore the antecedents and consequences of health information privacy concerns in online health communities	China	337	Personal online health information privacy	PMT, dual calculus	8	25	Self-report	CFA	Cronbach's alpha
Aurigemma	2018	To measure the effect of uncertainty avoidance on motivations to adopt voluntary information security controls (specifically password manager applications)	USA	227 undergraduate business students in a private university	Adoption of password manager application following fear appeal message	PMT	9	25	Self-report	CFA	Composite reliability

4.3.2 Development and Refinement of Scale Items by Included Studies

All the selected studies performed a literature review when developing their respective items (n = 33). An empirical study including pretesting and face validity was performed in 22 studies (Anderson & Agarwal, 2010; Aurigemma & Mattson, 2018; Boehmer et al., 2015; Chai et al., 2009; Crossler et al., 2014; Dang-Pham & Pittayachawan, 2015; Gurung et al., 2009; Herath & Rao, 2009; Hina & Dominic, 2017; Hovav & Putri, 2016; Ifinedo, 2012; Jansen & van Schaik, 2017; Johnston et al., 2015; Lee & Larsen, 2009; Menard et al., 2014; Safa et al., 2015; Siponen et al., 2014; Tu et al., 2015; Vance et al., 2012; Visinescu et al., 2016; Warkentin et al., 2016). However, only 14 studies of the 33 studies involved an expert panel in the item development stage (Crossler et al., 2014; Doane et al., 2016; Herath & Rao, 2009; Hina & Dominic, 2017; Johnston & Warkentin, 2010; Johnston et al., 2015; Lee & Larsen, 2009; Menard et al., 2014; Safa et al., 2015; Tu et al., 2015; Vance et al., 2012; Visinescu et al., 2016; Warkentin et al., 2016; Zhang et al., 2017).

Out of the 33 studies, 11 adopted all three approaches for item development (Crossler et al., 2014; Herath & Rao, 2009; Hina & Dominic, 2017; Johnston et al., 2015; Lee & Larsen, 2009; Menard et al., 2014; Safa et al., 2015; Tu et al., 2015; Vance et al., 2012; Visinescu et al., 2016; Warkentin et al., 2016).

All the studies used priori theoretical frameworks for item development, where 15 explicitly used only PMT (Anderson & Agarwal, 2010; Aurigemma & Mattson, 2018; Boehmer et al., 2015; Burns et al., 2017; Chou & Chou, 2016; Dang-Pham & Pittayachawan, 2015; Doane et al., 2016; Gurung et al., 2009; Johnston & Warkentin, 2010; Johnston et al., 2015; Lwin et al., 2012; Menard et al., 2014; Meso et al., 2013; Tsai et al., 2016; Warkentin et al., 2016), 12 used PMT and one additional framework (Chai et al., 2009; Crossler et al., 2014; Hina & Dominic, 2017; Ifinedo, 2012; Jansen & van Schaik, 2017; Mohamed & Ahmad, 2012; Safa et al., 2015; Thompson et al., 2017;

Tu et al., 2015; Vance et al., 2012; Visinescu et al., 2016; Zhang et al., 2017), and six used PMT and two or more additional frameworks (Herath & Rao, 2009; Hoon Kim et al., 2014; Hovav & Putri, 2016; Lee & Larsen, 2009; Siponen et al., 2014; Yoon et al., 2012).

Scrutinising the extensiveness of PMT usage in the studies included, a few patterns emerged. Only three studies utilised all six domains of PMT in their studies (Burns et al., 2017; Dang-Pham & Pittayachawan, 2015; Vance, 2012). A total of 14 studies used five out of the six domains in PMT (Boehmer et al., 2015; Chou & Chou, 2016; Crossler et al., 2014; Gurung et al., 2009; Herath & Rao, 2009; Ifinedo, 2012; Jansen & van Schaik, 2017; Lee & Larsen, 2009; Meso et al., 2013; Mohamed & Ahmed, 2012; Thompson et al., 2017; Tsai et al., 2016; Visinescu et al., 2016; Yoon et al., 2012). A total of 11 studies used four out of the six domains in PMT (Aurigemma & Mattson, 2018; Chai et al., 2009; Doane et al., 2016; Hina & Dominic, 2017; Johnston & Warkentin, 2010; Johnston et al., 2015; Lwin et al., 2012; Menard et al., 2014; Siponen et al., 2014; Warkentin et al., 2016; Zhang et al., 2017). The remaining five studies used only three out of the six domains in PMT (Anderson & Agarwal, 2010; Hoon Kim et al., 2014; Hovav & Putri, 2016; Safa et al., 2015; Tu et al., 2015).

Out of the six domains of PMT, the domain that is the least included is *perceived maladaptive reward*, in which only four out of the 33 studies included this domain in their studies (Burns et al., 2017; Dang-Pham & Pittayachawan, 2015; Mohamed & Ahmed, 2012; Vance, 2012). *Perceived self-efficacy* and *perceived response efficacy* have the highest frequency of inclusion in the studies. Only one study did not include *perceived self-efficacy*, namely by Hovav & Putri (2016). Similarly, only the study by Safa et al (2015) did not include *perceived response efficacy* in their study.

4.3.3 Reliability and Validity Testing by Included Studies

For reliability testing, the majority of the studies employed either Cronbach's alpha (n = 9) (Anderson & Agarwal, 2010; Boehmer et al., 2015; Chou & Chou, 2016; Doane et al., 2016; Gurung et al., 2009; Hina & Dominic, 2017; Lwin et al., 2012; Siponen et al., 2014; Tsai et al., 2016), composite reliability (n = 10) (Aurigemma & Mattson, 2018; Burns et al., 2017; Herath & Rao, 2009; Johnston & Warkentin, 2010; Ifinedo, 2012; Jansen & van Schaik, 2017; Menard et al., 2014; Mohamed & Ahmad, 2012; Warkentin et al., 2016; Yoon et al., 2012), or both (n = 14) (Chai et al., 2009; Crossler et al., 2014; Dang-Pham & Pittayachawan, 2015; Hoon Kim et al., 2014; Hovav & Putri, 2016; Lee & Larsen, 2009; Meso et al., 2013; Safa et al., 2015; Siponen et al., 2014; Thompson et al., 2017; Tu et al., 2015; Vance et al., 2012; Visinescu et al., 2016; Zhang et al., 2017). From the total number of 33 studies examined, 31 studies have reliability scores, either through Cronbach's alpha or composite reliability of more than 0.7 for the scales used. The remaining two studies did not report the reliability scores (Anderson & Agarwal, 2010; Johnston et al., 2015). None of the studies reported test-retest reliability.

Content validity was reported in 23 studies (Anderson & Agarwal, 2010; Chai et al., 2009; Crossler et al., 2014; Dang-Pham & Pittayachawan, 2015; Gurung et al., 2009; Herath & Rao, 2009; Hina & Dominic, 2017; Hovav & Putri, 2016; Ifinedo, 2012; Jansen & van Schaik, 2017; Johnston & Warkentin, 2010; Johnston et al., 2015; Lee & Larsen, 2009; Lwin et al., 2012; Menard et al., 2014; Siponen et al., 2014; Safa et al., 2015; Thompson et al., 2017; Tu et al., 2015; Vance et al., 2012; Visinescu et al., 2016; Warkentin et al., 2016; Zhang et al., 2017).

Structural validity was examined through EFA in 14 studies (Boehmer et al., 2015; Chai et al., 2009; Chou & Chou, 2016; Dang-Pham & Pittayachawan, 2015; Herath & Rao, 2009; Hina & Dominic, 2017; Johnston et al., 2015; Menard et al., 2014; Siponen et al., 2014; Thompson et al., 2017; Tu et al., 2015; Vance et al., 2012; Visinescu et al., 2016; Warkentin et al., 2016).

In terms of the internal construct validity, of the 33 studies, 11 reported the values of goodness-of-fit indexes, either the comparative fit index (CFI) or the goodness-of-fit index (GFI), or both (Chou & Chou, 2016; Dang-Pham & Pittayachawan, 2015; Gurung et al., 2009; Hoon Kim et al., 2014; Mohamed & Ahmad, 2012; Johnston et al., 2015; Safa et al., 2015; Siponen et al., 2014; Tu et al., 2015; Thompson et al., 2017; Zhang et al., 2017). Both the CFI and GFI values in these studies were > 0.90, except for one, where the GFI was 0.86 (Hoon Kim et al., 2014).

Regarding external construct validity, examination of the scales' convergent and discriminate properties were reported in 27 studies (Aurigemma & Mattson, 2018; Burns et al., 2017; Chai et al., 2009; Chou & Chou, 2016; Crossler et al., 2014; Dang-Pham & Pittayachawan, 2015; Gurung et al., 2009; Herath & Rao, 2009; Hoon Kim et al., 2014; Hovav & Putri, 2016; Ifinedo, 2012; Jansen & van Schaik, 2017; Johnston & Warkentin, 2010; Johnston et al., 2015; Lee & Larsen, 2009; Menard et al., 2014; Meso et al., 2013; Mohamed & Ahmad, 2012; Siponen et al., 2014; Safa et al., 2015; Thompson et al., 2017; Tu et al., 2015; Vance et al., 2012; Visinescu et al., 2016; Warkentin et al., 2016; Yoon et al., 2012; Zhang et al., 2017). All of these studies reported good discriminant validity, where the R^2 values were lower than the respective AVEs between the domains. All except two of these studies also reported convergent validity by examining the AVE and CR, in which it was reported that the AVE ranged between 0.45 and 1.00, the CR was > 0.7 and the CR > AVE. Gurung et al (2009) and Johnston et al (2015) did not report the AVE and CR values explicitly, although both studies stated that convergent validity was satisfactory.

4.3.4 Rating of Instrument Quality by Included Studies

Based on the six criteria outlined in Section 3.5.1 for rating the scales used by the included studies, the majority of these studies (n=17) (Anderson & Agarwal, 2010; Aurigemma & Mattson, 2018; Boehmer et al., 2015; Burns et al., 2017; Chou & Chou, 2016; Crossler et al., 2014; Hina & Dominic, 2017; Hoon Kim et al., 2014; Hovav & Putri, 2016; Ifinedo, 2012; Jansen & van Schaik, 2017; Johnston & Warkentin, 2010; Lee & Larsen, 2009; Lwin et al., 2012; Meso et al., 2013; Mohamed & Ahmad, 2012; Yoon et al., 2012) were rated as medium quality (33% of the total studies scored 4 and 21% of the total studies scored 3). A total of 14 studies (Chai et al., 2009; Gurung et al., 2009; Herath & Rao, 2009; Dang-Pham & Pittayachawan, 2015; Johnston et al., 2015; Menard et al., 2014; Safa et al., 2015; Siponen et al., 2014; Thompson et al., 2017; Tu et al., 2015; Vance et al., 2012; Visinescu et al., 2016; Warkentin et al., 2016; Zhang et al., 2017) were rated as high quality (9% of the total number of studies scored 6 and 30% of the total number of studies scored 5). The remaining two studies from the total included studies were rated as poor quality (6% of the total studies scored 2) (Doane et al., 2016; Tsai et al., 2016). Table 4.2 provides details of the ratings given to the questionnaire developed by each of the included studies.

Table 4.2: Ratings of the questionnaires developed by the reviewed studies (1 if present; 0 if absent)

Study		**Quality Scoring**							
Author	**Year**	**Followed an a priori explicit theoretical framework**	**Reported efforts to achieve content validity**	**Structural Validity through EFA**	**Internal construct validity (goodness-of-fit indexes)**	**External construct validity (discriminant and convergent)**	**Reliability scores above 0.7**	**Total score**	**Interpretation: ≤2 = poor quality, 3-4 = medium quality, 5-6 = high quality**
Gurung	2009	1	1	0	1	1	1	5	High quality
Chai	2009	1	1	1	0	1	1	5	High quality
Lee	2009	1	1	0	0	1	1	4	Medium quality
Herath	2009	1	1	1	0	1	1	5	High quality
Anderson	2010	1	1	0	0	1	N/A	3	Medium quality
Johnston	2010	1	1	0	0	1	1	4	Medium quality
Vance	2012	1	1	1	0	1	1	5	High quality
Lwin	2012	1	1	0	0	0	1	3	Medium quality
Ifinedo	2012	1	1	0	0	1	1	4	Medium quality
Yoon	2012	1	0	0	0	1	1	3	Medium quality
Mohamed	2012	1	0	0	1	1	1	4	Medium quality
Meso	2013	1	0	0	0	1	1	3	Medium quality

Table 4.2, continued

Study		Quality Scoring							
Author	**Year**	**Followed an a priori explicit theoretical framework**	**Reported efforts to achieve content validity**	**Structural Validity through EFA**	**Internal construct validity (goodness-of-fit indexes)**	**External construct validity (discriminant and convergent)**	**Reliability scores above 0.7**	**Total score**	**Interpretation: ≤2 = poor quality, 3-4 = medium quality, 5-6 = high quality**
Crossler	2014	1	1	0	0	1	1	4	Medium quality
Siponen	2014	1	1	1	1	0	1	5	High quality
Hoon	2014	1	0	0	1	1	1	4	Medium quality
Menard	2014	1	1	1	0	1	1	5	High quality
Boehmer	2015	1	0	1	0	0	1	3	Medium quality
Dang-Pham	2015	1	1	1	1	1	1	6	High quality
Johnston	2015	1	1	1	1	1	N/A	5	High quality
Tu	2015	1	1	1	1	1	1	6	High quality
Safa	2015	1	1	0	1	1	1	5	High quality
Visinescu	2016	1	1	1	0	1	1	5	High quality
Warkentin	2016	1	1	1	0	1	1	5	High quality
Doane	2016	1	0	0	0	0	1	2	Poor quality
Tsai	2016	1	0	0	0	0	1	2	Poor quality
Chou	2016	1	0	1	1	0	1	4	Medium quality

Table 4.2, continued

Study		**Quality Scoring**							
Author	**Year**	**Followed an a priori explicit theoretical framework**	**Reported efforts to achieve content validity**	**Structural Validity through EFA**	**Internal construct validity (goodness-of-fit indexes)**	**External construct validity (discriminant and convergent)**	**Reliability scores above 0.7**	**Total score**	**Interpretation: ≤2 = poor quality, 3-4 = medium quality, 5-6 = high quality**
Hovav	2016	1	1	0	0	1	1	4	Medium quality
Hina	2017	1	1	1	0	0	1	4	Medium quality
Thompson	2017	1	1	1	1	1	1	6	High quality
Jansen	2017	1	1	0	0	1	1	4	Medium quality
Burns	2017	1	0	0	0	1	1	3	Medium quality
Zhang	2017	1	1	0	1	1	1	5	High quality
Aurigemma	2018	1	0	0	0	1	1	3	Medium quality

*N/A: Results not available in the article.

4.3.5 Adaptation of Items in Included Articles into Current Study

From the systematic review, only items in the instruments that were rated as being of either medium or high quality were re-examined and included in the item inventory for adaptation in this study. The examination of the available items corresponding to the PMT domains in the high- and medium-quality articles revealed a particular pattern, as shown in Table 4.3.

Table 4.3: Common patterns identified in the inventory of items extracted

Domain	Keywords/ question structure	Author	Year
Perceived susceptibility	How likely…? How likely are you to…? It is likely… The likelihood…	Lee Herath Ifinedo Boehmer Tu	2009 2009 2012 2015 2015
Perceived self-efficacy	I would feel comfortable… I feel confident when… I feel confident… I am confident I can…	Herath Dang-Pham Boehmer Burns	2009 2015 2015 2017
Perceived severity	It would be a serious problem for me to… It is a serious problem for me… (threat) is a serious problem…	Mohamed Ifinedo Boehmer Dang-Pham	2012 2012 2015 2015
Perceived maladaptive reward	Not performing (protective action) will (other benefits)	Vance Mohamed Dang-Pham	2012 2012 2015
Perceived response cost	Performing (protective action) is inconvenient It takes a lot of effort to perform (protective action) (protective action) is cumbersome (Protective action) takes considerable effort	Yoon Meso Dang-Pham Thompson Aurigemma	2012 2013 2015 2017 2018
Response efficacy	Performing (protective action) is useful to prevent/stop/reduce (threat) (Performing action) is effective/adequate to remove (threat)	Meso Tu Thompson Burns	2013 2015 2017 2017
Actual protective behaviour	How often do you...?	Crossler Chou	2014 2017

The items under the domain perceived susceptibility contained keywords such as *likely* and *likelihood* to represent the concept of susceptibility to a particular threat. As for the items under perceived severity, the majority contained key phrases such as *serious problem* to represent the severity of the threats. The items under perceived self-efficacy contained words such as *confident* and *comfortable* to represent the concept of efficacy in the items. The structure of the items in the perceived response efficacy domain usually began with the description of the protective action, followed by words such as *useful/effective/adequate* and ended with a phrase that reflected the *removal/stopping/reduction* of the threats measured. In the domain perceived maladaptive reward, the items usually began with phrases such as *by not performing* a particular protective action, which was then followed by a statement regarding the alternative benefits. In respect of perceived response cost, the items contained keywords/phrases such as *cumbersome/considerable effort* and *inconvenient* to represent the domain. Lastly, in articles that measured actual protective behaviour, the behaviour was measured using a time scale, with a question structure such as *how often do you* followed by the items.

The above-mentioned keywords and question structures were adapted in this study in generating the items for the respective PMT domains. However, as none of the articles in the systematic review measured parental digital security practice, the items for parental digital security practice were derived based on engagement with stakeholders and a further review of the literature, as explained in the subsequent section 4.4.

4.4 Item Generation from Parents' Input in the Item Development Phase

A total of 69 parents responded to the online survey. The sociodemographic characteristics of these respondents are described in Table 4.4.

Table 4.4: Sociodemographic characteristics of the respondents of the online survey of parents (n = 69)

Variable (n = 69)	**Frequency (%)**
Gender	
Male	21 (30%)
Female	48 (70%)
Age	
30–40	43 (62%)
41–50	22 (32%)
50 and above	4 (6%)
Ethnicity	
Malay	51 (74%)
Chinese	15 (22%)
Indian	2 (3%)
Others	1 (1%)
Religion	
Islam	52 (75%)
Christianity	9 (13%)
Buddhism	4 (6%)
Hinduism	1 (1%)
Others	3 (5%)
Region of Malaysia	
Northern (Perlis, Penang, Kedah, Perak)	2 (3%)
Central (Selangor, Kuala Lumpur, Putrajaya)	53 (77%)
Negeri Sembilan)	3 (5%)
Southern (Melaka, Johor)	10 (14%)
Eastern (Pahang, Kelantan, Terengganu)	1 (1%)
Sabah and Sarawak	
Occupation	
Government	32 (46%)
Private	24 (35%)
Self-employed	11 (16%)
Unemployed/Home maker	2 (3%)
Highest education level	
No formal education	1 (1%)
Primary school	3 (5%)
Secondary school	2 (3%)
Diploma	15 (22%)
Bachelor's degree	37 (54%)
Master's degree	11 (16%)

4.4.1 Parental Concern

Thematic analysis was performed based on the answers submitted by the respondents through the online survey. A few key themes emerged regarding their concerns about online threats, as illustrated in Figure 4.2.

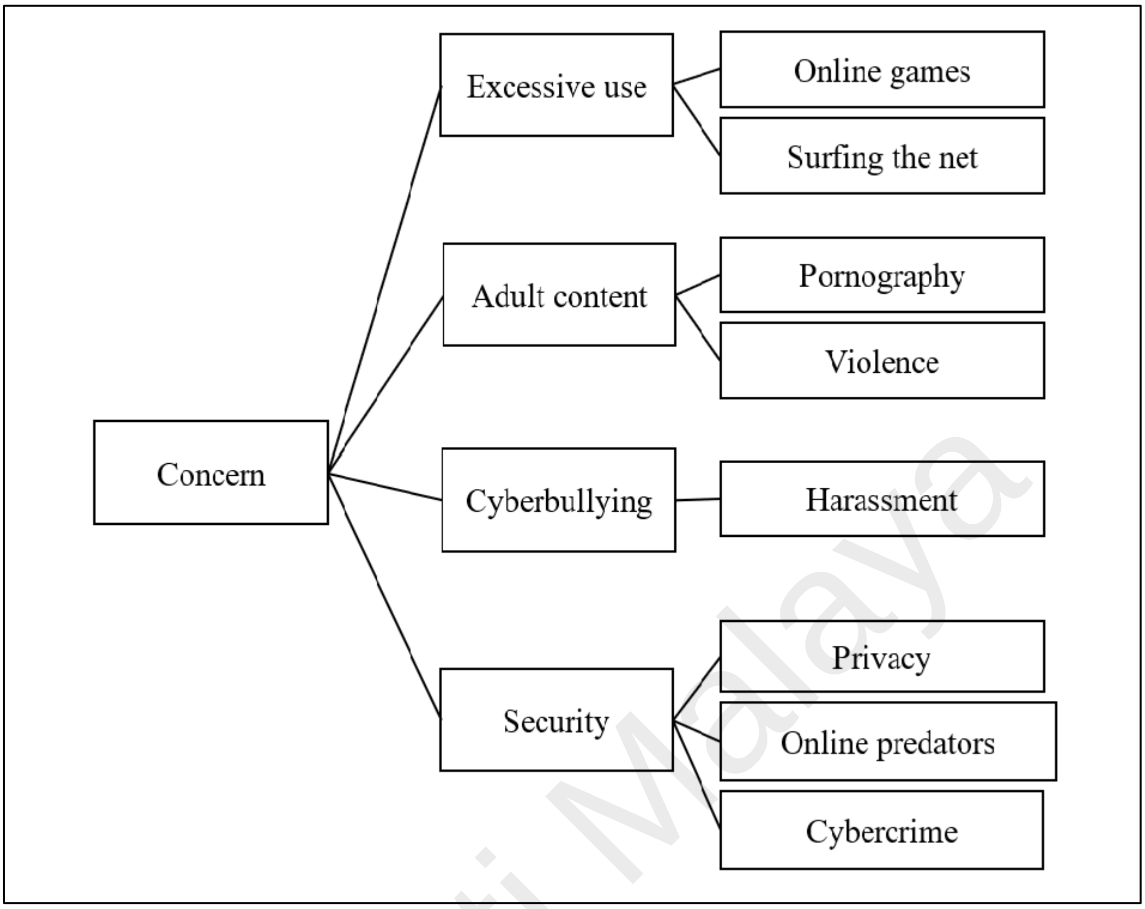

Figure 4.2: Concerns about online threats identified by parents

4.4.1.1 Parental Concern Theme 1: Excessive Usage

Excessive usage of the internet was identified as one of the key themes among the concerns expressed by the parents who completed the online survey. This theme can be further divided into two main domains based on the pattern of usage, namely, excessive usage in surfing the internet and excessive usage in playing online games. The excessive usage of the internet was a concern as it was considered as “time-wasting”, “exposed [children] to online danger” and to interrupt daily routines. For example, one respondent who was a 47-year-old male, stated when answering this question that: “…too much time spent online...until affect[s] study”.

4.4.1.2 Parental Concern Theme 2: Adult Content

Adult content was the most popular theme that emerged from the respondents' answers. Under this theme, two major domains were apparent, namely, pornography and violence. The concerns related to adult content included easy accessibility and exposure to such content, whether intentionally or not. These domains were reflected in several answers given by the respondents, such as:

"Watching porn and vulgarities via online" – *Female, 44 years old*

"Adult advertisements...pop-ups...and violent videos when surfing the internet" – *Male, 35 years old*

4.4.1.3 Parental Concern Theme 3: Cyberbullying

Cyberbullying was another theme that emerged from the respondents' answers. Parents elaborated that cyberbullying as a form of harassment online, included being "shamed" by online contacts. This theme is illustrated by this respondent's statement:

"Bullied...shaming...by friends online" – *Male, 50 years old*

4.4.1.4 Parental Concern Theme 4: Security

Security was a major theme that was discovered from the respondents' answers. Under security, three major domains emerged: privacy, online predators, and cybercrime. Obtaining personal information, exposure to child sexual grooming, scams and frauds were some examples highlighted by the respondents, as illustrated by the excerpts below:

"Hacking...privacy breach" – *Male, 50 years old*

"Preyed on by paedophiles" – *Female, 39 years old*

"Exposed to scams and fraud" – *Male, 37 years old*

4.4.2 Digital Security Practice

The following types of digital security practice emerged from the respondents' answers to the survey: restriction, monitoring, active approach, co-use and supervision (Figure 4.3).

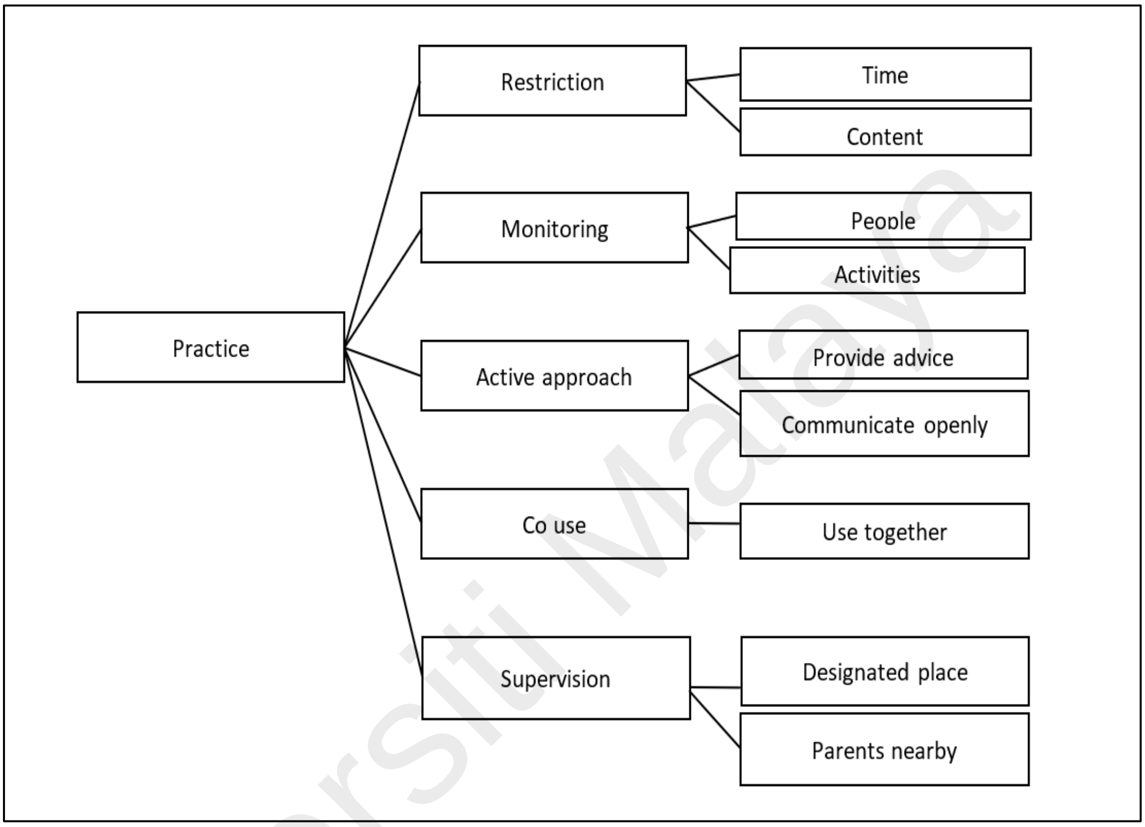

Figure 4.3: Types of digital security practice identified by parents

4.4.2.1 Digital Security Practice Theme 1: Restriction

Based on the answers given, restriction was a popular security practice adopted by parents. Under restriction, two domains emerged; restriction on content and restriction on the duration of internet usage. The usage of the provided filters and setting rules on when to use the internet were some examples of restriction practice that were captured from the responses and elaborated this theme, as shown by the following excerpts:

"Restrict time...Set rules on gadget use" – *Female, 35 years old*

"Use child safe mode" – *Female, 39 years old*

4.4.2.2 Digital Security Practice Theme 2: Monitoring

The theme of monitoring also emerged from the analysis of the respondents' answers regarding the digital security practices they employed. Here, monitoring refers to the parents checking their children's online activities after usage. Under monitoring, two distinctive domains were identified: monitoring contacts online and monitoring internet usage activities. These monitoring practices were achieved by checking the chat history and browsing history of their children. Two examples of the survey responses that illustrate these points are given below:

"Block some users. Check friends they chat with" – *Male, 47 years old*

"Check browsing history" – *Male, 43 years old*

4.4.2.3 Digital Security Practice Theme 3: Active Approach

Taking an active approach in practising digital security was another key theme that emerged from the online survey responses. This approach represents' parents' efforts to provide information to their children through two-way communication. Under this theme, two domains emerged: provide advice and communicate openly. Parents who apply this approach appear to educate their children and make themselves approachable when it comes to discussing online issues. This approach is exemplified by the following excerpts:

"Educate him on the dangers online" – *Male, 32 years old*

"Be open. Always communicate" – *Male, 47 years old*

4.4.2.4 Digital Security Practice Theme 4: Co-use

The theme co-use, which refers to parents using the internet together with their children, also emerged from the respondents' answers. An example of co-use is illustrated by the following response:

“Allow surfing and YouTube only with parents” – *Female, 33 years old*

4.4.2.5 Digital Security Practice Theme 5: Supervision

The theme supervision also emerged from the respondents’ answers. This strategy involves allowing children to use the internet within the parents’ vicinity. Two domains were identified as falling under this theme: supervision through a designated area and supervision through parents being nearby. Two examples of the answers that illustrate supervision being used a digital security practice strategy are given below:

“Online [in] living room only” – *Male, 34 years old*

“Only surf YouTube when I am around” – *Female, 34 years old*

4.4.3 Barriers to Digital Security Practice

The barriers to digital security practice that were identified among the parents were poor knowledge, children's rights, the parent–child relationship, and commitment, as illustrated in Figure 4.4.

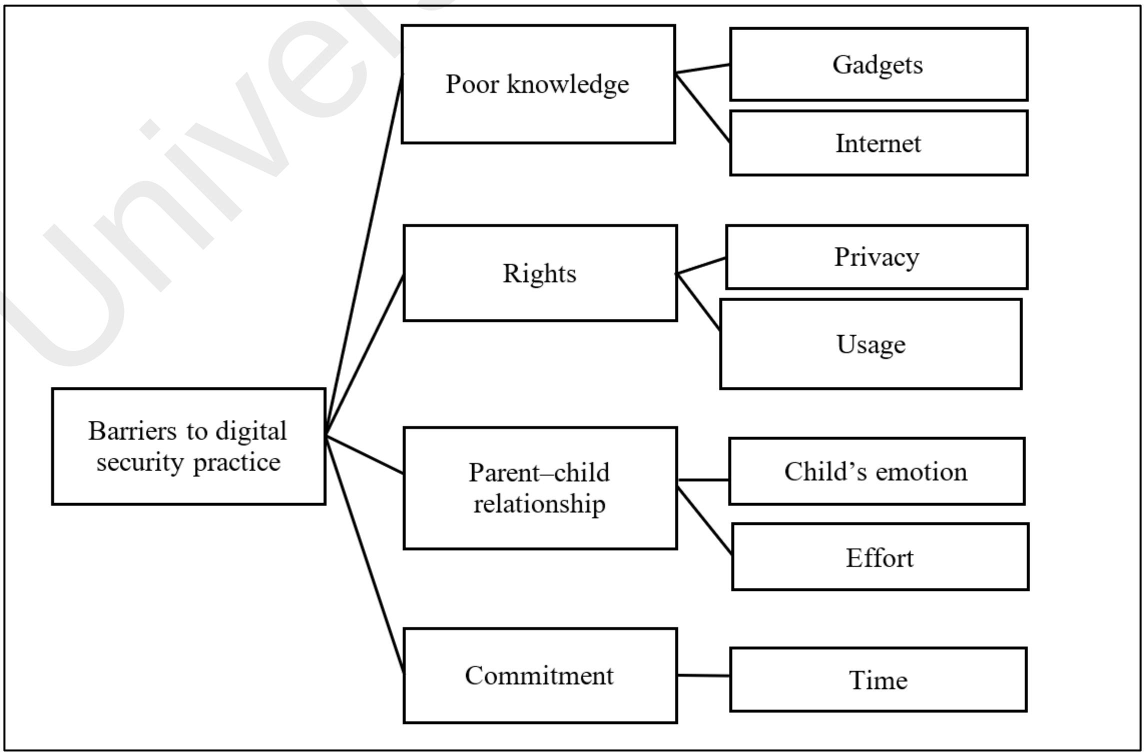

Figure 4.4: Barriers to parental digital security practice identified by parents

4.4.3.1 Barrier Theme 1: Poor Knowledge

Poor knowledge was one of the emergent themes highlighted by the parents when answering the question about what they perceived were the potential barriers to poor digital security practice. Under this theme, two domains were identified: poor knowledge on operating devices/gadgets and poor knowledge on internet threats. The points mentioned by the parents in the following excerpts emphasised the theme of poor knowledge:

"unsure how to control…lack of knowledge" – *Male, 35 years old*

"don't know computer setting[s]." – *Female, 50 years old*

4.4.3.2 Barrier Theme 2: Rights

Another theme that was discovered was that of children's rights. Two domains were identified as falling under this theme, namely, privacy rights and the right of their children to use the internet. Parents might not be applying good parental digital security practices on the pretext of not wanting to violate these rights. These domains are illustrated by the verbatim examples given below:

"Child's privacy – unable to know what is going on when they are online" – *Female, 48 years old*

*"*Don't want to breach their rights to use*"* – *Female, 40 years old*

4.4.3.3 Barrier Theme 3: Parent–Child Relationship

This theme refers to actions that parents take to ensure that they maintain a good parent–child relationship from their point of view. The child's emotion was the major domain under this theme. Parents might allow their children to use the internet without performing proper digital security practices because they believe that by doing so, their children will not be restricted and will be happy. This theme is highlighted by the following verbatim excerpt:

“difficult to balance safe[ty] and not upsetting them” – *Female, 34 years old*

4.4.3.4 Barrier Theme 4: Commitment

Parents’ level of commitment in applying good digital security practice was another potential barrier that was identified from the survey responses. Parents might be occupied with other commitments and not able to allocate time to keep their children safe online. Some parents also stated that the act of keeping their children safe online was troublesome and required a lot of effort, as shown by the following excerpts:

“need a lot of effort to control them” – *Male, 35 years old*

“Sometimes I don’t have time to monitor their usage” – *Female, 51 years old*

4.5 Item Generation from Experts’ Input in the Item Development Phase

The themes that emerged from the online survey were presented to a panel of experts comprised of the following:

a) stakeholders from CSM

b) a public health specialist

c) an expert on cyber parenting

d) a parents’ representative

e) an expert in adolescent health.

All the experts had at least 5 years’ experience in their respective fields. From the discussion with the experts, an additional theme emerged regarding the concerns that parents have about online safety. This theme was harmful content, which was represented by the domain labelled extremism. This theme covered threats such as dark webs, hackers and criminal websites, extremist groups and terrorist movements.

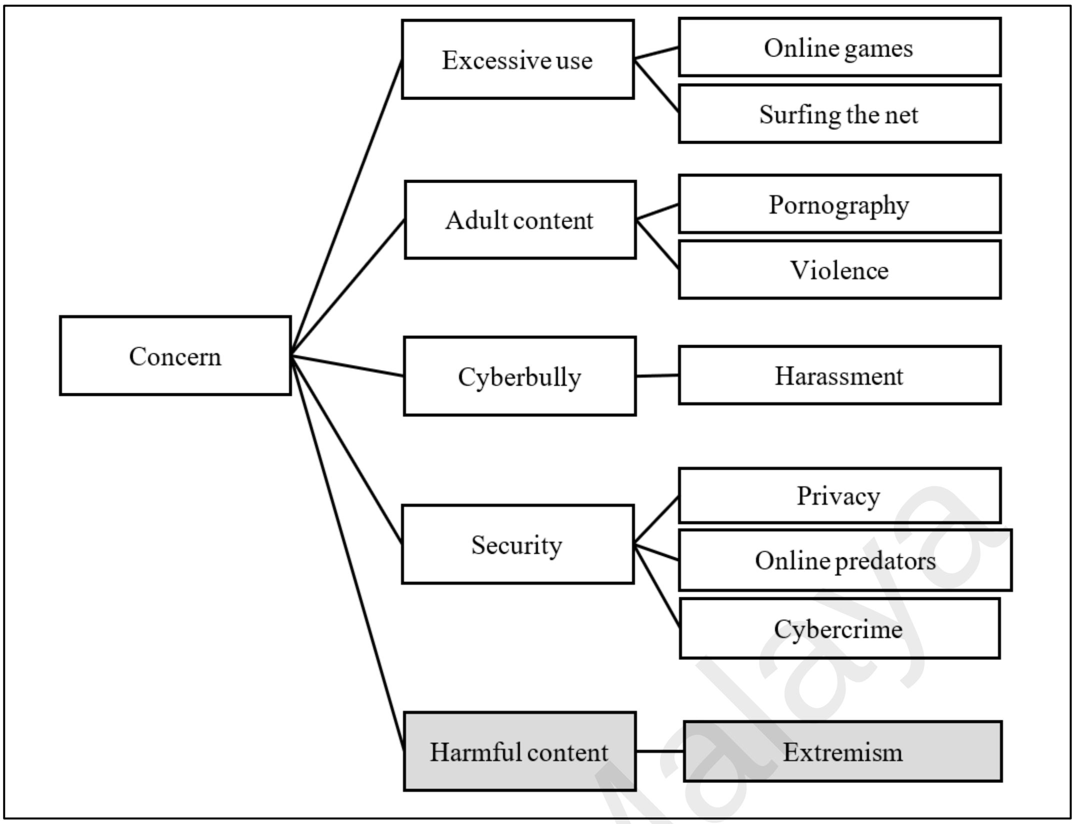

Figure 4.5: Additional theme regarding online concerns (shaded grey) based on discussion with experts

All the experts agreed and were satisfied with the themes that were deduced regarding the types of digital security practice and barriers to digital security practice from the parents' feedback and no additional themes were found.

From the themes that emerged and their respective domains, 52 items were generated. These items were generated and mapped according to the PMT framework. Items for *perceived susceptibility* and *perceived severity* (section B and C, respectively) were derived from themes on concerns about online threats. Items for *perceived self-efficacy* (section D) and *perceived response efficacy* (section E) were derived from themes obtained on digital security practice. Items for *response cost* (section F) and *maladaptive reward* (section G) were derived based on the themes that emerged from barriers to digital security practice. For section H, which covered actual digital security practice, this section contained items derived from the themes on digital security practice, as well as some that were adapted from the literature, particularly the works by Nikken and Jansz (2014) and Sonck et al. (2013).

4.6 Content Validation in the Item Development Phase

Two rounds of content validation were conducted with two different panels of experts. For the first round, six experts were approached and agreed to evaluate the items proposed for the questionnaire. The six experts were from various backgrounds related to cyber parenting and had a minimum of 5 years of experience in their respective fields. The expert panel consisted of a:

a) digital citizenship expert

b) medical anthropology expert

c) early childhood education expert

d) adolescent health expert

e) cybersecurity expert

f) public health expert.

Each of the experts evaluated the relevance and clarity of each item generated.

4.6.1 Content Validation: First Round

4.6.1.1 Relevance

All the items in the respective sections achieved the minimum item level content validity index (I-CVI) of more than 0.8 and overall CVI of more than 0.9. Thus, all of the items for the respective sections were deemed relevant by all the experts in the first round. Table 4.5 provided the I-CVI and overall CVI scores regarding relevance of the items.

Table 4.5: Relevance scores based on I-CVI and overall CVI

Section	No. of items	Minimum I-CVI	Overall CVI
B	7	0.83	0.98
C	7	0.83	0.98
D	7	1	1
E	7	1	1
F	7	0.83	0.98
G	5	0.83	0.93
H	12	1	1

4.6.1.2 Clarity

For section B, seven items were evaluated. Four items (B1, B2, B4 and B7) had an I-CVI of less than 0.8 (i.e. 0.67 respectively). The overall CVI was 0.81. Hence, the experts did not agree on the clarity of the items for section B and therefore the items needed some revision.

For section C, seven items were evaluated. Three items (C2, C4 and C7) had I-CVI of less than 0.8 (i.e. 0.67 respectively). The overall CVI was 0.83. Hence, the experts did not agree on the clarity of the items for section C and therefore the items needed some revision.

For section D, E, F, G and H, all the items in the respective sections achieved the minimum item level content validity index (I-CVI) of more than 0.8 and overall CVI of more than 0.9. Thus, the clarity of all the items for these sections were deemed good by all the experts in the first round. Table 4.6 provides a summary of the I-CVI and CVI values for clarity.

Table 4.6: Clarity scores based on I-CVI and overall CVI

Section	No. of items	Minimum I-CVI	Overall CVI
B	7	0.67	0.81
C	7	0.67	0.83
D	7	0.83	0.95
E	7	0.83	0.98
F	7	0.83	0.98
G	5	0.83	0.93
H	12	0.83	0.97

4.6.1.3 Revisions After the First Round of Content Validation

Based on the feedback received from the expert panel and the CVI values, adjustments were made to several of the items in the questionnaire. The changes are presented in Table 4.7.

Table 4.7: Revisions based on first round of content validation

Item no	Original statement	Revised statement
Section B: Perceived susceptibility		
B1	Be bullied online	Be bullied (harassed, threatened or/and intimidated) online
B2	Be using it excessively	Be spending time online more than he/she should be
B3	Be exposed to adult content (including pornography, violence, gambling)	No revision
B4	Have his/her identity stolen	Have his/her personal information obtained illegally by someone else
B5	Be approached by strangers online	Be approached online by a person he/she does not know
B6	Exchange sexual messages or/and images with his/her friends or/and people online	Exchange sexual messages or/and images with other people online
B7	Exposed to inappropriate content (including self-harm, extremism, terrorism)	*(two items were created representing original B7)* B7. Exposed to online content promoting self- harm (e.g.: websites that encourage suicide, promote eating disorders, drug use) B8. Exposed to online content that promote hate, extreme views and terrorism
Section C: perceived severity		
C1	A child is being bullied online	A child is being bullied (harassed, threatened or/and intimidated) online
C2	A child is using the internet excessively	A child is spending time online more than he/she should be
C3	A child is exposed to adult content (including pornography, violent, gambling)	No revision
C4	A child’s identity is stolen	A child's personal information obtained illegally by someone else

Table 4.7, continued

Item no	Original statement	Revised statement
C5	A child is approached by strangers online	A child is approached online by a person he/she does not know
C6	A child exchanges sexual messages or/and images to their friends or/and people online	A child exchanges sexual messages or/and images with other people online
C7	A child is exposed to inappropriate content (including self- harm, extremism, terrorism)	*(two items were created representing original C7)* C7: A child is exposed to online content promoting self-harm (e.g.: websites that encourage suicide, promote eating disorders, drug use) C8: A child is exposed to online content that promote hate, extreme views and terrorism
Section D: perceived self-efficacy		
D1	I am comfortable in communicating and giving advice to my child on online safety	I am confident in discussing and giving advice to my child on online safety
D2	I am equipped with appropriate knowledge to keep my child safe online	I am confident with my knowledge in keeping my child safe online
D3	I am comfortable with using the internet together with my child	No revision
D4	I am comfortable to impose rules on internet use to my child	I am confident in imposing rules on internet use to my child
D5	I am comfortable with using filtering and monitoring software (parental control applications)	I am confident in using filtering and monitoring software (parental control applications)
D6	I am only comfortable with allowing my child to use the internet when I am around	I am comfortable with restricting my child to use the internet only when I am around
D7	I am comfortable of checking my child's online activities after my child has used it	I am confident in checking my child's online activities after my child has used it
Section E: Perceived response efficacy		
E1	Communicating and giving advice on online safety to my child will keep him/her safe online	Discussing and giving advice on online safety to my child will keep him/her safe online
E2	Having the appropriate knowledge will keep my child safe online	No revision
E3	Using the internet together with my child will keep him/her safe online	No revision
E4	Imposing internet rules to my child will keep him/her safe online	No revision

Table 4.7, continued

Item no	Item no	Item no
E5	Using filtering and monitoring software (parental control applications) will keep him/her safe online	No revision
E6	Allowing my child to use the internet only when I am around will keep him/her safe online	Restricting my child to use the internet only when I am around will keep him/her safe online
E7	Checking my child's online activities after my child has used it will keep him/her safe online	No revision
Section F: perceived response cost		
F1	Communicating and giving advice on online safety to my child is troublesome	Discussing and giving advice on online safety to my child is troublesome for me
F2	It takes a lot of effort to acquire appropriate knowledge on online safety	No revision
F3	It takes a lot of effort to use the internet together with my child	No revision
F4	Ensuring my child follows internet rules is troublesome	Ensuring my child follows internet rules is troublesome for me
F5	Ensuring filtering and monitoring software (parental control applications) are working can be troublesome	Ensuring filtering and monitoring software (parental control applications) are working can be troublesome for me
F6	Allowing my child to use the internet only when I am available requires a lot of effort	Restricting my child to use the internet only when I am available requires a lot of effort
F7	Checking my child's online activities after he/she has use it requires a lot of effort	No revision
Section G: Perceived maladaptive rewards		
G1	By not having constant communication and not giving advice on online safety to my child, this will help in making him/ her more independent	By not having discussions and not giving advice on online safety to my child, this will help in making him/ her more independent
G2	Allowing my child to use the internet on his/her own will allow me to do other things	Allowing my child to use the internet on his/her own will allow me to focus on my own interest
G3	By not imposing internet rules to my child, he/she will be happy	No revision
G4	By not putting up filtering and monitoring software (parental control applications), my child can use the internet better.	By not putting up filtering and monitoring software (parental control applications), my child can use the internet freely.
G5	By not checking my child's online activities after he/she uses it, I am respecting his/her rights	No revision

Table 4.7, continued

Item no	Item no	Item no
Section H: Parental Digital Security Practice		
H1	Communicate and give advice on online safety to your child	Discuss and give advice on online safety to your child
H2	Tell your child how to handle strangers online	Have conversations with your child on how to handle unknown people online
H3	Tell your child to protect personal information online	Discuss with your child on how to protect personal information online
H4	Say what to do if he/she is bullied or harassed online	Have conversations on what to do if he/she is bullied or harassed online
H5	Use the internet together with your child	No revision
H6	Tell your child when/how long to use internet	No revision
H7	Tell your child which websites/social network he/she can visit	No revision
H8	Tell your child what he/she can and cannot do online	No revision
H9	Ensure filtering and monitoring software (parental control applications) are present	No revision
H10	Allow your child to use the internet only when you are present	Restrict your child to use the internet only when you are present
H11	Check the websites that your child visited	No revision
H12	Check which friends or contacts the child adds to a social networking profile	No revision

4.6.2 Content Validation: Second Round

The revised version of the questionnaire, which was amended according to the input from the first round of content validation, was distributed again to the same experts. The experts were only asked to evaluate the clarity of the questionnaire as the relevance of the questionnaire had established in the first round. In this round, four experts responded and gave the feedback needed. As such, all four needed to agree (I-CVI = 1, overall CVI = 1) for the items to be considered to have good clarity. The experts in the second round consisted of a:

a) digital citizenship expert

b) medical anthropology expert

c) cybersecurity expert

d) public health expert.

4.6.2.1 Clarity

For section B, eight items were evaluated. The experts did not reach agreement on the clarity of one item (B4) because one expert disagreed, giving the I-CVI of 0.88. However, the experts agreed that the remaining items had good clarity with I-CVI of 1. Hence, the clarity of the items for section B needed further revision, particularly item B4.

For section C, eight items were evaluated. The experts did not reach agreement about the clarity of one item (C4) because one expert disagreed, giving the I-CVI of 0.88. However, the remaining items were judged by the experts to have achieved good clarity with I-CVI of 1. Hence, the clarity of the items for section C needed further revision, particularly item C4.

For section G, five items were evaluated. The experts did not agree on the clarity of one item (G1) because one expert disagreed, giving an I-CVI of 0.88. However, they agreed that the remaining items had good clarity with I-CVI of 1. Hence, the clarity of the items for section G needed further revision, particularly item G1.

For section D, E, F and H, all the experts agreed that each of the items had good clarity with I-CVI of 1 and overall CVI of 1 to the respective sections. Hence no revisions were needed.

Hence, the clarity of the items in sections B, C and G required some further revision. In particular, the items that needed revision were B4, C4 and G1. The remaining sections had good clarity, with individual and overall CVI of 1 according to the experts in the second round, an improvement from the findings in the first round of content validation.

4.6.2.2 Revisions After the Second Round of Content Validation

Based on input from experts in the second round of content evaluation, three items (B4, C4, G1) were revised. The revisions to these three items are shown in Table 4.8.

Table 4.8: Revisions made after the second round of content validation

Item no	Original statement	Revised statement
B4	Have his/her personal information obtained illegally by someone else	Have his/her personal information obtained without her knowledge or consent
C4	A child's personal information obtained illegally by someone else	A child's personal information is obtained without his/her knowledge or consent
G1	By not having discussions and not giving advice on online safety to my child, this will help in making him/ her more independent	By not having discussions on online safety to my child, this will help in making him/ her more independent

It can be seen from the above table that the revisions were minor. The experts were in agreement that the majority of the items had both clarity and relevance. Thus, it was decided that the second revised version of the questionnaire did not need to undergo another round of content validation by experts. Instead, the revised version of the questionnaire that was produced as a result of the second round of content validation was finalised for use in the subsequent stages of validation.

4.7 Translation of the Items in the Item Development Phase

In creating the dual-language questionnaire, the procedures for forwards-backwards translation that were followed were based on guidelines by Beaton et al. (2000) and Guillemin et al. (1993). In the first step, two different translators who could speak both English and Malay translated the English version into Malay. Both translators were language teachers and each had at least 20 years of teaching experience in both languages. Both translators worked independently. The two versions of the translation were discussed and compared by a panel consisting of the researcher, public health specialists and representatives from CSM (see Appendix K). A single version of the questionnaire that had been translated into Malay was then produced. The second step involved the reverse translation of the Malay questionnaire into English. The reverse translation was carried out by another two translators who were fluent in both English and Malay. These translators were also language teachers and they had at least 10 years of teaching experience in both languages. The result of the reverse translation was discussed by the panel and was compared to the original English questionnaire (see Appendix L). A dual-language version of the questionnaire that contained questions in both English and Malay was then produced.

4.8 Cognitive Debriefing in the Scale Development Phase

Cognitive debriefing targets the mental processes that respondents use when completing questionnaires; processes which are assumed to follow a question–answer model. The model consists of four stages: comprehension, retrieval, judgement and response (Collins, 2003; McColl et al., 2003). A fifth aspect that can be assessed during cognitive debriefing is the respondent burden. Relevance, questionnaire length, ease of navigation, visual distractions and degree of computation required all affect respondent burden (Dillman et al., 1993; Mullin et al., 2000).

A total of 10 respondents from a government agency were recruited for the cognitive debriefing. The respondents were selected through purposive sampling with variation based on gender, ethnicity, religion, and education level. The sociodemographic characteristics of these respondents are shown in Table 4.9.

Table 4.9: Sociodemographic characteristics of the respondents in the cognitive debriefing (n = 10)

Variable	n
Gender	
Male	4
Female	6

Table 4.9, continued

Variable	**n**

Age (years)	Median = 38.5
	Min = 31
	Max = 50

Ethnicity	
Malay	7
Chinese	0
Indian	2
Others	1
Religion	
Islam	7
Christianity	1
Buddhism	0
Hinduism	2
Others	0
Employment	
Government	10
Education	
No formal education	0
Primary school	0
Secondary school	1
Diploma	6
Bachelor's degree	2
Master's degree	1
PhD or equivalent	0

Monthly household income (RM)	Median = RM4500
	Min = RM1500
	Max = RM10000

Marital status	
Married	10

4.8.1 Comprehension

Comprehension explores whether the meaning of the items is consistent across the respondents. In section B, the meaning of the keywords for all the eight items was consistent among all 10 respondents and matched with the researcher's interpretation. A similar observation was made for all the other sections except for section F. In the case of section F, two items, namely, F3 (It takes a lot of effort to use the internet together with my child) and F6 (Restricting my child to using the internet only when I am available requires a lot of effort) produced an inconsistent interpretation of the keyword ‘effort’.

The word ‘effort’ in F3 was interpreted as:

- Effort in equipping oneself with enough knowledge when using the internet with one’s child
- Efforts need to be taken to access the internet with my child
- Actual effort when child and parent are using the internet together

The word ‘effort’ in F6 was interpreted as:

- Effort in ensuring a child is not using the internet more than they need to
- Effort needs to be taken to ensure that the child uses the internet only when the parent is around.

4.8.2 Retrieval

Retrieval refers to whether respondents are able to obtain relevant and correct information from memory. Retrieval was not an issue for most of the sections. However, in the case of section H, the retrieval process for item H12 (Check which friends or contacts the child adds to a social networking profile) was deemed difficult by some of the respondents because the question was not relevant to them, particularly if their children did not have any social network accounts.

4.8.3 Judgement

Judgement refers to the process involved in formulating a response. The respondents did not encounter any problems with this process in respect of most of the items. However, they did face some difficulty in respect of F3, F6 and H12 due to poor comprehension and retrieval.

4.8.4 Response

In the questionnaire, a Likert scale was used to match the response to the category or ‘best fit’. This approach was deemed appropriate by the respondents for all the items in the questionnaire. They were able to reflect and place their answers fittingly across the scale. All the respondents interpreted the middle point in the Likert scale as ‘unsure’ and recognized that the Likert scale was anchored by endpoints of ‘strongly agree/strongly disagree’ or ‘very likely/very unlikely’. In the case of the Likert scale that was anchored with endpoints ‘never/always’, the respondents interpreted the middle point as ‘sometimes’. These interpretations were consistent with the researcher’s intention and interpretation of the Likert scale employed in this study.

4.8.5 Respondent Burden

Overall, the respondents noted that the dual-language format assisted in their comprehension of the questionnaire. They also stated that the flow and structure of the questionnaire were smooth. The minimum time taken to answer the questionnaire was 10 minutes and the maximum time taken was 16 minutes with a median time of 12 minutes. The length and complexity of the questionnaire were deemed appropriate as well. The topic explored in the questionnaire appeared relevant to the respondents, and they were able to relate the contents to their own experience easily.

4.8.6 Revisions Based on the Results of the Cognitive Debriefing

Based on the output of the cognitive debriefing, a few adjustments were made to the questionnaire. Firstly, item H12 was dropped based on the feedback from the cognitive debriefing because the item might not be applicable and not relevant to all the parents in the study population. Secondly, additional definitions for the term ‘effort’ were added to items F3 and F6 in order to clarify the term based on the feedback received about these two items. Thirdly, a definition of ‘internet user’ was also added at the beginning of the questionnaire. This was done to ensure that the respondents would have a common understanding of the term ‘internet user’ when answering the questionnaire. After these adjustments had been made, a total of 53 items remained for the subsequent round of questionnaire development.

4.9 Test-Retest Reliability in the Scale Development Phase

After the questionnaire had been revised based on the output of the cognitive debriefing, a small pilot test was conducted in August 2018 in order to assess test-retest reliability. The interval period between the test and retest ranged from a minimum of 3 days to a maximum of 27 days with a median of 15 days. A total of 35 respondents were recruited from workplaces (Institute for Health Management, Institute for Health Systems Research, Institute for Medical Research) together with their spouses. The sociodemographic characteristics of these respondents are summarised in Table 4.10.

Table 4.10: Sociodemographic characteristics of the respondents in the test-retest (n = 35)

Variable	n (%)
Gender	
Male	7 (20.0)
Female	28 (80.0)

Age (years)	Mean = 37.74
	Min = 28
	Max = 53

Ethnicity	
Malay	27 (77.1)
Chinese	6 (17.1)
Indian	1 (2.9)
Others	1 (2.9)
Religion	
Islam	28 (80.0)
Christianity	0
Buddhism	6 (17.1)
Hinduism	1 (2.9)
Others	0
Employment	
Government	30 (85.7)
Private	2 (5.7)
Self-employed	3 (8.6)
Unemployed	0
Retiree	0
Student	0
Education	
No formal education	0
Primary	0
Secondary	9 (25.7)
Tertiary	26 (74.3)

Table 4.10, continued

Variable	n (%)
Monthly household income (RM)	
< 1000	0
1000–1999	0
2000–2999	3 (8.6)
3000–3999	1 (2.9)
4000–4999	4 (11.4)
5000–5999	12 (34.3)
6000–6999	2 (5.7)
7000–7999	4 (10.4)
8000–8999	2 (5.7)
9000–9999	2 (5.7)
> 10000	5 (14.3)
Marital	
Never married	0
Married	35 (100)
Divorced	0
Widowed	0

The majority of the respondents who participated in the test-retest were female (80.0%) and of Malay background (77.1%). The average age of the respondents was 37.7 years. Most of the respondents followed the religion of Islam (80.0%) and were working in the government sector (85.7%). There was a balanced representation in terms of education level, ranging from secondary school to master's degree, with bachelor's degree having the highest frequency (37.1%). There was a wide range of household income, ranging from RM2000–2999 to > RM10000, with the majority of the respondents falling into the RM5000–5999 income bracket (34.3%). All of the respondents were married.

The weighted kappa value and the agreement level for each item based on the weighted kappa is summarised in Table 4.11.

Table 4.11: Test-Retest Reliability Assessment

Item label	Question	Weighted kappa value	95 % confidence interval		Agreement level
			Lower	Upper	
B1	Be bullied (harassed, threatened or/and intimidated) online. *Dibuli (diganggu, diugut, atau/dan ditakutkan) dalam talian.*	0.64	0.46	0.81	Substantial
B2	Be spending time online more than he/she should. *Menghabiskan masa dalam talian lebih daripada sepatutnya.*	0.71	0.55	0.87	Substantial
B3	Be exposed to adult content (eg: pornography, violence, gambling). *Terdedah kepada kandungan dewasa (contoh; pornografi, keganasan, perjudian).*	0.67	0.51	0.82	Substantial
B4	Have his/her personal information obtained without his/her knowledge or consent. *Maklumat peribadi beliau diperolehi tanpa pengetahuan atau izinnya.*	0.70	0.56	0.85	Substantial
B5	Be approached online by a person he/she does not know. *Didekati oleh orang yang tidak dikenali dalam talian.*	0.76	0.64	0.89	Substantial
B6	Exchange sexual messages or/and images with other people online. *Bertukar mesej/ imej berunsurkan seksual dengan orang lain dalam talian.*	0.73	0.57	0.89	Substantial
B7	Exposed to online content promoting self-harm (eg: websites that encourage suicide, eating disorder, drug use). *Terdedah kepada kandungan dalam talian yang akan menggalakkan perbuatan membahayakan diri sendiri (contoh: laman sesawang yang menggalakkan perbuatan bunuh diri, gangguan pemakanan, penggunaan dadah).*	0.72	0.58	0.86	Substantial

Table 4.11, continued

Item label	Question	Weighted kappa value	95 % confidence interval		Agreement level
			Lower	Upper	
B8	Exposed to online content that promote hate, extreme views and terrorism. *Terdedah kepada kandungan dalam talian yang menggalakkan kebencian, pandangan ekstrem dan terorisme.*	0.72	0.56	0.88	Substantial
C1	A child is being bullied (harassed, threatened or/and intimidated) online. *Kanak-kanak yang dibuli (diganggu, diugut, atau/dan ditakutkan) dalam talian.*	0.49	0.24	0.74	Moderate
C2	A child is spending time online more than he/she should. *Kanak-kanak yang menghabiskan masa dalam talian lebih daripada sepatutnya.*	0.59	0.35	0.83	Moderate
C3	A child is exposed to adult content (including pornography, violent, gambling). *Kanak-kanak yang terdedah kepada kandungan dewasa (contoh; pornografi, keganasan, perjudian).*	0.68	0.43	0.94	Substantial
C4	A child's personal information is obtained without his/her knowledge or consent. *Maklumat peribadi kanak-kanak yang diperolehi tanpa pengetahuan atau izinnya.*	0.49	0.24	0.73	Moderate
C5	A child is approached online by a person he/she does not know. *Kanak-kanak didekati oleh orang yang tidak dikenali dalam talian.*	0.50	0.25	0.74	Moderate

Table 4.11 continued

Item label	Question	Weighted kappa value	95 % confidence interval		Agreement level
			Lower	Upper	
C6	A child exchanges sexual messages or/and images with other people online. *Kanak-kanak yang bertukar mesej/ imej berunsurkan seksual dengan orang lain dalam talian.*	0.51	0.25	0.78	Moderate
C7	A child is exposed to online content that promotes self-harm (eg: websites that encourage suicide, promote eating disorders, drug use). *Kanak-kanak terdedah kepada kandungan dalam talian yang akan menggalakkan perbuatan membahayakan diri sendiri (contoh: laman sesawang yang menggalakkan perbuatan bunuh diri, gangguan pemakanan, penggunaan dadah).*	0.77	0.60	0.95	Substantial
C8	A child is exposed to online content that promotes hate, extreme views and terrorism. *Kanak-kanak terdedah kepada kandungan dalam talian yang akan menggalakkan kebencian, pandangan ekstrem dan terorisme.*	0.77	0.58	0.95	Substantial
D1	I am confident in discussing with my child on online safety. *Saya yakin untuk berbincang dengan anak saya tentang keselamatan dalam talian.*	0.38	0.15	0.61	Fair
D2	I am confident with my knowledge in keeping my child safe online. *Saya yakin dengan pengetahuan saya dalam memastikan anak saya selamat dalam talian.*	0.56	0.33	0.80	Moderate

Table 4.11, continued

Item label	**Question**	**Weighted kappa value**	**95 % confidence interval**		**Agreement level**
			Lower	**Upper**	
D3	I am comfortable with using the internet together with my child. *Saya selesa melayari Internet bersama-sama anak saya.*	0.48	0.25	0.71	Moderate
D4	I am confident in imposing rules on internet use to my child. *Saya yakin untuk melaksanakan peraturan berkenaan penggunaan internet kepada anak saya.*	0.54	0.32	0.77	Moderate
D5	I am confident in using filtering and monitoring software (parental control applications). *Saya yakin dalam menggunakan perisian tapisan dan pemantauan (aplikasi kawalan ibu bapa).*	0.66	0.44	0.87	Substantial
D6	I am comfortable with restricting my child to use the internet only when I am around. *Saya selesa dengan hanya membenarkan anak saya menggunakan internet apabila saya berada bersamanya.*	0.73	0.60	0.92	Substantial
D7	I am confident in checking my child's online activities after my child has used it. *Saya yakin dalam memeriksa aktiviti dalam talian anak saya setelah beliau menggunakannya.*	0.66	0.43	0.89	Substantial
E1	Discussing on online safety with my child will keep him/her safe online. *Berbincang dengan anak saya berkenaan keselamatan dalam talian akan memastikan beliau selamat dalam talian.*	0.54	0.29	0.79	Moderate

Table 4.11, continued

Item label	**Question**	**Weighted kappa value**	**95 % confidence interval**		**Agreement level**
			Lower	**Upper**	
E2	Having the appropriate knowledge will keep my child safe online. *Mempunyai pengetahuan yang bersesuaian akan memastikan anak saya selamat dalam talian.*	0.51	0.25	0.77	Moderate
E3	Using the internet together with my child will keep him/her safe online. *Menggunakan internet bersama-sama dengan anak saya akan memastikan beliau selamat dalam talian.*	0.61	0.42	0.80	Substantial
E4	Imposing internet rules to my child will keep him/her safe online. *Pelaksanaan peraturan berkenaan penggunaan internet kepada anak saya akan memastikan keselamatan beliau dalam talian.*	0.60	0.39	0.82	Substantial
E5	Using filtering and monitoring software (parental control applications) will keep him/her safe online. *Penggunaan perisian tapisan dan pemantauan (aplikasi kawalan ibu bapa) akan memastikan anak saya selamat dalam talian.*	0.51	0.29	0.73	Moderate
E6	Restricting my child to use the internet only when I am around will keep him/her safe online. *Mengehadkan penggunaan Internet oleh anak saya hanya apabila saya berada bersamanya akan memastikan keselamatan beliau dalam talian.*	0.73	0.55	0.90	Substantial

Table 4.11, continued

Item label	Question	Weighted kappa value	95 % confidence interval		Agreement level
			Lower	Upper	
E7	Checking my child's online activities after my child has used it will keep him/her safe online. *Memantau aktiviti dalam talian anak saya setelah beliau menggunakannya akan memastikan keselamatan beliau dalam talian.*	0.61	0.41	0.80	Substantial
F1	Discussing on online safety with my child is troublesome for me. *Berbincang dengan anak saya berkenaan keselamatan dalam talian adalah sesuatu yang menyusahkan bagi saya.*	0.67	0.46	0.88	Substantial
F2	It takes a lot of effort to acquire appropriate knowledge on online safety. *Ia memerlukan usaha yang lebih dalam memperolehi pengetahuan yang bersesuaian berkenaan keselamatan dalam talian.*	0.62	0.45	0.78	Substantial
F3	It takes a lot of effort to use the internet together with my child. *effort refers to attempts taken in ensuring usage of internet together with child, eg; arranging daily routines, or setting up a timetable to cater time for using internet together. *Ia memerlukan usaha yang lebih untuk menggunakan Internet bersama-sama dengan anak saya.* **usaha bermaksud percubaan yang diambil untuk memastikan penggunaan internet bersama-sama dengan anak, seperti mengatur rutin harian, atau menyediakan jadual agar mempunyai masa untuk menggunakan internet bersama-sama dengan anak.*	0.64	0.45	0.83	Substantial

Table 4.11, continued

Item label	Question	Weighted kappa value	95 % confidence interval		Agreement level
			Lower	Upper	
F4	Ensuring my child follows internet rules is troublesome for me. *Memastikan anak saya mematuhi peraturan berkenaan penggunaan internet adalah menyusahkan bagi saya.*	0.74	0.59	0.90	Substantial
F5	Ensuring filtering and monitoring software (parental control applications) are working can be troublesome for me. *Memastikan perisian tapisan dan pemantauan (aplikasi kawalan ibu bapa) agar ia berfungsi adalah sesuatu yang menyusahkan bagi saya.*	0.73	0.56	0.89	Substantial
F6	Restricting my child to use the internet only when I am around requires a lot of effort. *effort refers to attempts taken in ensuring child uses the internet only when parent is around, eg; rules of only allowing usage of gadgets in common areas in the house. *Mengehadkan penggunaan Internet oleh anak saya hanya apabila saya berada bersamanya memerlukan usaha yang lebih* **usaha bermaksud percubaan yang diambil untuk memastikan penggunaan internet oleh anak hanya terhad apabila ibu bapa berada berhampiran, seperti membuat peraturan mengehadkan penggunaan gajet di kawasan umum di rumah.*	0.56	0.37	0.74	Moderate

Table 4.11, continued

Item label	Question	Weighted kappa value	95 % confidence interval		Agreement level
			Lower	Upper	
F7	Checking my child's online activities after he/she has used it requires a lot of effort. *Memeriksa aktiviti dalam talian anak saya setelah beliau menggunakannya memerlukan usaha yang lebih.*	0.70	0.55	0.86	Substantial
G1	By not having discussions on online safety with my child, this will help in making him/ her more independent. *Anak saya akan lebih berdikari jika perbincangan berkaitan keselamatan dalam talian tidak berlaku.*	0.47	0.23	0.72	Moderate
G2	Allowing my child to use the internet on his/her own will allow me to focus on my own interest. *Membenarkan anak saya menggunakan internet secara bebas akan membolehkan saya memberi tumpuan kepada urusan saya sendiri.*	0.58	0.35	0.81	Moderate
G3	By not imposing internet rules to my child, he/she will be happy. *Anak saya akan berasa gembira sekiranya tidak dikenakan peraturan berkenaan penggunaan internet kepada beliau.*	0.57	0.34	0.79	Moderate
G4	By not putting up filtering and monitoring software (parental control applications), my child can use the internet freely. *Anak saya boleh menggunakan Internet secara bebas jika perisian tapisan dan pemantauan (aplikasi kawalan ibu bapa) tidak digunakan.*	0.48	0.20	0.75	Moderate

Table 4.11, continued

Item label	Question	Weighted kappa value	95 % confidence interval		Agreement level
			Lower	Upper	
G5	By not checking my child's online activities after he/she uses it, I am respecting his/her rights. *Saya menghormati hak anak saya dengan tidak memantau aktiviti dalam talian beliau.*	0.56	0.26	0.85	Moderate
H1	Discuss with your child on online safety. *Berbincang dengan anak anda berkenaan keselamatan dalam talian.*	0.71	0.51	0.91	Substantial
H2	Have conversations with your child on how to handle unknown people online. *Mengadakan perbincangan dengan anak anda tentang menangani orang yang tidak dikenali dalam talian.*	0.62	0.43	0.80	Substantial
H3	Discuss with your child on how to protect personal information online. *Berbincang dengan anak anda tentang perlindungan maklumat peribadi dalam talian.*	0.64	0.43	0.85	Substantial
H4	Have conversations on what to do if he/she is bullied or harassed online. *Berbincang dengan anak tentang apa yang perlu dilakukan sekiranya dibuli atau diganggu di atas talian.*	0.58	0.39	0.77	Moderate
H5	Use the internet together with your child. *Melayari Internet bersama-sama dengan anak anda.*	0.77	0.62	0.91	Substantial

Table 4.11, continued

Item label	Question	Weighted kappa value	95 % confidence interval		Agreement level
			Lower	Upper	
H6	Tell your child when/how long to use internet. *Memberitahu anak anda tentang waktu/tempoh masa yang dibenarkan untuk menggunakan Internet.*	0.74	0.52	0.96	Substantial
H7	Tell your child which websites/social network he/she can visit. *Memberitahu anak anda tentang laman sesawang/media sosial yang dibenarkan untuk dilawati.*	0.64	0.40	0.87	Substantial
H8	Tell your child what he/she can and cannot do online. *Memberitahu anak anda tentang perkara yang boleh dan tidak boleh dilakukan dalam talian.*	0.64	0.45	0.84	Substantial
H9	Ensure filtering and monitoring software (parental control applications) are present. *Memastikan perisian tapisan dan pemantauan (aplikasi kawalan ibu bapa) berfungsi.*	0.73	0.55	0.91	Substantial
H10	Restrict your child to use the internet only when you are present. *Mengehadkan penggunaan Internet oleh anak anda hanya apabila anda berada bersamanya.*	0.72	0.53	0.91	Substantial
H11	Check the websites that your child visited. *Memeriksa laman sesawang yang dilawati oleh anak anda.*	0.72	0.56	0.88	Substantial

The weighted kappa values showed that the majority of the items (34) fell into the 'substantial' agreement category. Another 18 items fell into the 'moderate' agreement category with a kappa value ranging between 0.40 and 0.60. However, one item, D1, had a kappa value of 0.38 and was therefore deemed ‘fair’ in terms of test-retest reliability. This item was dropped from the questionnaire because it did not meet the minimum cut-off value of 0.40 (Landis, 1977; Walter, 1998). Thus a total of 52 items were retained for subsequent questionnaire development steps and the field study.

4.10 Survey Administration and Field Study Results for Scale Development and Scale Evaluation

4.10.1 Data Quality Assessment (Univariate)

The data that were obtained from the field study were screened for quality by assessing the missing values and outliers. In total, 708 questionnaires were collected. However, only complete questionnaires were accepted. Hence 680 responses were used in the further analysis and the remaining 28 were deleted through the listwise deletion method. Prior to deletion, the pattern of missing data was analysed and was revealed to be missing completely at random based on Little’s test (Little, 1988). Thus, due to the high number of questionnaires retained for analysis, the listwise deletion method was deemed appropriate for handling missing data.

The outliers of the items of interest were screened in order to detect issues such as incorrect data entry. As such, all the items had a minimum and maximum value that was as expected from the use of a five-point Likert scale.

An examination of skewness and kurtosis revealed that although the majority of the items’ values for both kurtosis and skewness were within +/-1, some items had a larger value of kurtosis and skewness. Hence, this raised the possibility of a non-normal distribution of the data.

Data from a total of 680 individual respondents was used in the factor extraction, dimensionality, internal consistency, and construct validity assessments from October

2018 to December 2018. The sociodemographic characteristics of the 680 respondents are provided in Table 4.12. The sociodemographic characteristics of their children are provided in Table 4.13.

Table 4.12: Sociodemographic characteristics of the respondents in the field study (n = 680)

Variable	n (%)
Gender (n = 680)	
Male	268 (39.4)
Female	412 (60.6)

Age (in years) (n = 670)	Mean = 38.84 (SD = 8.23)
	Min = 21
	Max = 69

Ethnicity (n = 680)	
Malay	542 (79.7)
Chinese	69 (10.1)
Indian	49 (7.2)
Others	20 (2.9)
Religion (n = 680)	
Islam	557 (81.9)
Christianity	24 (3.5)
Buddhism	45 (6.6)
Hinduism	49 (7.2)
Others	5 (0.7)
State of residence (n = 680)	
Selangor	419 (61.6)
WP Kuala Lumpur	151 (22.2)
Perlis	30 (4.4)
Pulau Pinang	15 (2.2)
WP Putrajaya	13 (1.9)
Sabah/WP Labuan	10 (1.5)
Kedah	8 (1.2)
Johor	7 (1.0)
Perak	7 (1.0)
Pahang	6 (0.9)
Kelantan	4 (0.6)
Negeri Sembilan	3 (0.4)
Terengganu	3 (0.4)
Melaka	2 (0.3)
Sarawak	2 (0.3)
Employment (n = 680)	
Government	216 (31.8)
Private	256 (37.6)
Self-employed	106 (15.6)
Unemployed	83 (12.2)
Retiree	17 (2.5)
Student	2 (0.3)
Education (n = 680)	
No formal education	5 (0.7)
Primary	19 (2.8)
Secondary	225 (33.1)

Table 4.12, continued

Variable	n (%)
Tertiary	431 (63.4)
Monthly household income (RM) (n = 667)	
< 1000	32 (4.8)
1000–1999	87 (13.0)
2000–2999	119 (17.8)
3000–3999	109 (16.3)
4000–4999	78 (11.7)
5000–5999	81 (12.1)
6000–6999	37 (5.5)
7000–7999	28 (4.2)
8000–8999	28 (4.2)
9000–9999	21 (3.1)
> 10000	47 (6.9)
Marital (n = 680)	
Never married	9 (1.3)
Married	640 (94.1)
Divorced	25 (3.7)
Widowed	6 (0.9)

Table 4.13: Sociodemographic characteristics of the respondents' child in field study (n = 680)

Variable	n (%)

Child's mean age (n = 638)	Mean = 9.91 (SD 4.56)
	Min = 1
	Max = 17

Child's gender (n = 659)	
Male	363 (53.4)
Female	296 (43.5)

The majority of the respondents in the field study were female (60.6%). The predominant ethnicity was Malay (79.7%). The average age of the respondents was 38.84 years old. Most of the respondents were followers of the religion of Islam (81.9%). Most of the respondents resided in Selangor (61.6%). In terms of employment sector, the highest number of respondents were working in the private sector (37.6%). The most frequent education level among the respondents was secondary school (33.1%). The largest proportion of respondents fell into the RM2000–2999 income bracket (17.8%). The majority of the respondents were married (94.1%). As regards the child's characteristics on which the questionnaire responses were based, the mean age was 9.91

(SD 4.56) with a range from 1 year to 17 years. The majority of the children referred fromin the questionnaire was male (53.4%).

As recommended by Worthington and Whittaker (2006), the data for the EFA and item reduction through internal consistency needs to be different to that used in the CFA, CCA, and structural model assessment. Therefore, two separate datasets were created from the 680 available data. Using SPSS, a dataset that contained 316 data was obtained through random selection. This dataset was used in the EFA and internal consistency assessment. The other dataset, which contained the remaining 364 data was used for the CFA and CCA (measurement model), and structural model assessment.

4.10.2 Construct Validity through Exploratory Factor Analysis

In this section, the results derived from the EFA are discussed.

4.10.2.1 Sampling Adequacy and Suitability

The 52 items were tested simultaneously in the EFA procedure. An examination of the correlation revealed that the highest correlation for each item with at least another item was between 0.3 and 0.9. As shown in Table 4.14, the KMO value obtained was 0.882, which was above the cut-off value of 0.7 set by Hair et al. (2010). The result of the Bartlett's test of sphericity was significant, indicating that there were relationships between the variables. Hence sampling adequacy was fulfilled and the data were suitable for EFA.

Table 4.14: KMO and Bartlett's test

Kaiser–Meyer–Olkin measure of sampling adequacy		.882
Bartlett's test of sphericity	Approx. chi-square	14120.520
	Df	1326
	Sig.	< 0.001

4.10.2.2 Factor Extraction and Rotation

Initial extraction revealed nine domains based on Kaiser's criterion of an eigenvalue of more than 1, and these domains accounted for 72.36% of the shared variance. The scree plot in Figure 4.6 shows that the plot started to show an upwards trend when nine domains were extracted.

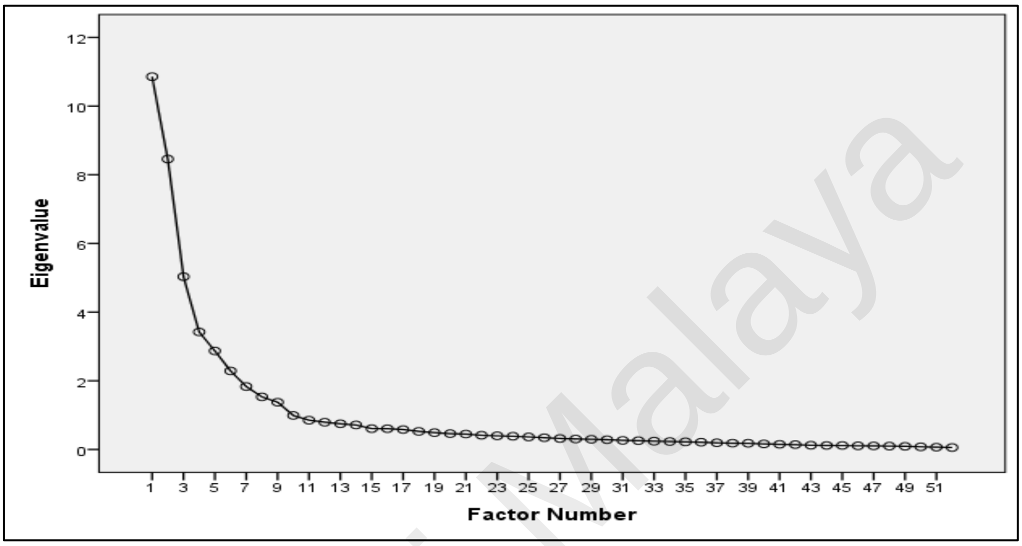

Figure 4.6: Scree plot of domains extracted in initial extraction

As recommended by Timmerman and Lorenzo-Seva (2011), a parallel analysis was conducted with polychoric correlations and 100 iterations to determine the number of domains to be extracted. As shown in Table 4.15, at domain 10, the mean of the random eigenvalue is higher than the real-data eigenvalue. Hence the parallel analysis also indicated that nine domains should be extracted.

Table 4.15: Results of parallel analysis

Variable	Real-data eigenvalue	Mean of random eigenvalue	95th centile of random eigenvalue
1	10.13284*	2.04812	2.15269
2	7.75330*	1.94032	2.02526
3	4.56380*	1.86125	1.92956
4	4.05585*	1.79197	1.84978
5	3.39424*	1.73081	1.78566
6	2.58729*	1.67744	1.72992
7	1.97063*	1.62761	1.67529
8	1.70787*	1.57845	1.62300
9	1.60538*	1.53380	1.57787
10	0.98794	1.49207	1.53088

In light of the above, it was decided to extract nine domains. Then a Promax rotation was performed in order to examine the pattern matrix. All items with factor loadings of less than 0.40 and/or cross-loaded were deleted. Cross-loading was determined to be present if the difference in the factor loadings of a particular item between two domains was less than 0.15 (Worthington & Whittaker, 2006). Using this criterion, item G1 was found to have a poor loading. Therefore, this item was deleted and the analysis was run again.

After the removal of G1, the remaining 51 items revealed nine extracted domains that accounted for 73.38% of the shared variance. The total variance explained for each component shown in Table 4.16 revealed that the component C1-C8 contributed the highest percentage of variance explained at 21.27%, followed by B1-B8 at 16.58% and E1-E7 at 9.69%.

Table 4.16: Individual component total variance explained in percent

Component	**Individual total variance explained (%)**
B1-B8	16.58
C1-C8	21.27
D2-D7	4.40
E1-E7	9.69
F2, F3, F6, F7	3.58
F1, F4, F5	2.60
G2-G5	3.00
H1-H4	5.55
H5-H11	6.70
Total cumulative variance explained	73.38

An examination of the pattern matrix revealed that no items had a poor factor loading or an issue of cross-loading, as shown in Table 4.17.

Table 4.17: Pattern matrix of domains extracted

	Domain								
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
B1	0.79								
B2	0.67								
B3	0.85								
B4	0.85								
B5	0.84								
B6	0.91								
B7	0.87								
B8	0.83								
C1		0.88							
C2		0.72							
C3		0.90							
C4		0.93							
C5		0.92							
C6		0.95							
C7		0.93							
C8		0.93							
D2			0.86						
D3			0.71						
D4			0.90						
D5			0.75						
D6			0.70						
D7			0.57						
E1				0.91					
E2				0.91					
E3				0.78					
E4				0.92					
E5				0.85					
E6				0.72					
E7				0.72					
F1					0.80				
F2						0.82			
F3						0.90			
F4					0.85				
F5					0.86				
F6						0.81			
F7						0.82			
G2							0.72		
G3							0.89		
G4							0.86		
G5							0.58		
H1								0.71	
H2								0.87	
H3								0.89	
H4								0.84	
H5									0.72
H6									0.81
H7									0.73
H8									0.63
H9									0.56
H10									0.87
H11									0.80

At this stage, the domains that had been extracted so far were compared with the underlying PMT domains on which the questionnaire was based in order to give conceptual meaning to these domains. The individual items can be found in Appendix H.

4.10.2.3 Conceptual Interpretability: Domain 1

The eight items that were loaded into this domain were those from section B (B1–B8). These items were intended to reflect the domain *perceived susceptibility*. Hence, this domain was accepted and labelled as such.

4.10.2.4 Conceptual Interpretability: Domain 2

The eight items that were loaded into this domain were those from section C (C1–C8). These items were intended to reflect the domain *perceived severity*. Hence, this domain was accepted and labelled as such.

4.10.2.5 Conceptual Interpretability: Domain 3

The six items that were loaded into this domain were those from section D (D2–D7). These items were intended to reflect the domain *perceived self-efficacy*. Hence, this domain was accepted and labelled as such.

4.10.2.6 Conceptual Interpretability: Domain 4

The seven items that were loaded into this domain were those from section E (E1–E7). These items were intended to reflect the domain *perceived response efficacy*. Hence, this domain was accepted and labelled as such.

4.10.2.7 Conceptual Interpretability: Domain 5 and Domain 6

The items in section F (F1–F7) were intended to reflect the domain *perceived response cost*. However, it was noted that two domains emerged from these items, namely, Domain 5 and Domain 6. Items F1, F4 and F5 were loaded into Domain 5. Items F2, F3, F6, and F7 were loaded into Domain 6. This implied that Domain F was itself a second-order domain formed by Domain 5 and Domain 6 (Awang, 2012). Following an examination of the items of both domains, Domain 5 was labelled as *perceived psychology cost* and Domain 6 was labelled as *perceived tangible cost*. These two domains were linked and treated as subdomains of the main domain, namely, domain F, which was labelled as *response cost*. The formation of the domain *perceived response cost* as a second-order domain maintained the parsimony of the model and also retained the dimensions of PMT as much as possible.

4.10.2.8 Conceptual Interpretability: Domain 7

The four items that were loaded into this domain were those from section G (G2–G5). These items were intended to reflect the domain *perceived maladaptive reward*. Hence, this domain was accepted and labelled as such.

4.10.2.9 Conceptual Interpretability: Domain 8 and Domain 9

The items in section H (H1–H11) were intended to reflect the domain *digital security practice*. However, it was noted that two domains emerged from these items, namely, Domain 8 and Domain 9. Items H1–H4 were loaded into Domain 8. Items H5–H11 were loaded into Domain 9. This implied that domain H was itself a second-order domain formed by Domain 8 and Domain 9 (Awang, 2012). Based on an examination of the items of both domains, Domain 8 was labelled as *discursive digital security* and Domain 9 was labelled as *control digital security*. These two domains were linked and treated as subdomains of the main domain, namely domain H, which was labelled as *digital security practice*. The formation of the domain *digital security practice* as a second-order domain maintained the parsimony of the model and it also retained a relationship with the dimensions of PMT as much as possible.

4.10.3 Summary of EFA Results

Based on the EFA findings, nine domains were extracted, which accounted for 73.4% of the shared variance. One item, namely G1, was dropped due to poor loading.

The nine domains were labelled as *perceived susceptibility, perceived severity, perceived self-efficacy, perceived response efficacy, perceived psychological cost, perceived tangible cost, perceived maladaptive reward, discursive digital security*, and *control digital security*. In order to maintain the parsimony of the model, and to reflect the underlying PMT domains, *perceived psychological cost* and *perceived tangible cost* were treated as subdomains. These two subdomains formed the main domain that was labelled as *perceived response cost*. Similarly, *discursive digital security* and *control digital security* were treated as subdomains forming the main domain *digital security practice*. A schematic diagram of the conceptual model is shown in Figure 4.7.

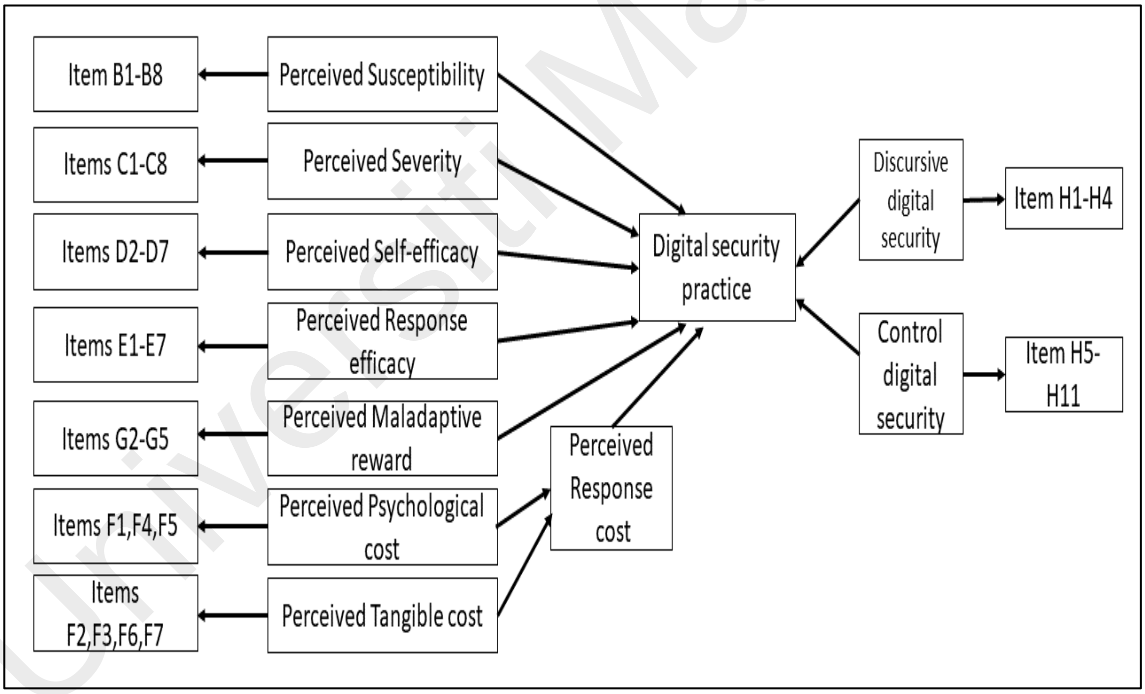

Figure 4.7: Schematic diagram of conceptual model based on EFA

Following the EFA, the item reduction process was performed by assessing the internal consistency based on the domains identified.

4.10.4 Internal Consistency of Domains

The result of the internal consistency assessment of each domain is presented in the following subsections.

4.10.4.1 Internal Consistency Results for the Perceived Susceptibility Domain

For the *perceived susceptibility* domain, all the items fulfilled the properties of good internal consistency, as recommended by Mokkink et al. (2010). The inter-item correlation values ranged between 0.3 and 0.9 (Table 4.18). The CITC values were above 0.3 and the Cronbach's alpha value was above 0.7 (Table 4.19).

Table 4.18: Inter-item correlation matrix of the items for the perceived susceptibility domain

	B1	B2	B3	B4	B5	B6	B7	B8
B1	1.00	0.49	0.59	0.63	0.67	0.60	0.59	0.57
B2	0.49	1.00	0.57	0.50	0.50	0.49	0.54	0.50
B3	0.59	0.57	1.00	0.74	0.71	0.71	0.73	0.70
B4	0.63	0.50	0.74	1.00	0.78	0.75	0.69	0.64
B5	0.67	0.50	0.71	0.78	1.00	0.74	0.70	0.69
B6	0.60	0.49	0.71	0.75	0.74	1.00	0.80	0.77
B7	0.59	0.54	0.73	0.69	0.70	0.80	1.00	0.86
B8	0.57	0.50	0.70	0.64	0.69	0.77	0.86	1.00

Table 4.19: Corrected item-total correlation and Cronbach's alpha for the perceived susceptibility domain

	Corrected item-total correlation	Cronbach's alpha
B1	0.70	0.94
B2	0.60	
B3	0.82	
B4	0.81	
B5	0.82	
B6	0.84	
B7	0.84	
B8	0.81	

4.10.4.2 Internal Consistency Results for the Perceived Severity Domain

For the *perceived severity* domain, all the items fulfilled the properties of good internal consistency, as recommended by Mokkink et al. (2010). The inter-item correlation values were between 0.3 and 0.9 (Table 4.20). The values of the CITC were above 0.3 and the value of Cronbach's alpha was above 0.7 (Table 4.21).

Table 4.20: Inter-item correlation matrix of the items for the perceived severity domain

	C1	C2	C3	C4	C5	C6	C7	C8
C1	1.00	0.60	0.76	0.83	0.78	0.78	0.76	0.77
C2	0.60	1.00	0.72	0.69	0.67	0.67	0.64	0.63
C3	0.76	0.72	1.00	0.87	0.83	0.84	0.82	0.83
C4	0.83	0.69	0.87	1.00	0.87	0.87	0.82	0.85
C5	0.78	0.67	0.83	0.87	1.00	0.86	0.80	0.82
C6	0.78	0.67	0.84	0.87	0.86	1.00	0.89	0.88
C7	0.76	0.64	0.82	0.82	0.80	0.89	1.00	0.89
C8	0.77	0.63	0.83	0.85	0.82	0.88	0.89	1.00

Table 4.21: Corrected item-total correlation and Cronbach's alpha for the perceived severity domain

	Corrected item-total correlation	Cronbach's alpha
C1	0.83	0.97
C2	0.71	
C3	0.90	
C4	0.92	
C5	0.89	
C6	0.92	
C7	0.89	
C8	0.90	

4.10.4.3 Internal Consistency Result for the Perceived Self-Efficacy Domain

For the *perceived self-efficacy* domain, all the items fulfilled the properties of good internal consistency, as recommended by Mokkink et al. (2010). The inter-item correlation values were between 0.3 and 0.9 (Table 4.22), while the CITC values were above 0.3 and the Cronbach's alpha value was above 0.7 (Table 4.23).

Table 4.22: Inter-item correlation matrix of the items for the perceived self-efficacy domain

	D2	D3	D4	D5	D6	D7
D2	1.00	0.50	0.64	0.52	0.55	0.55
D3	0.50	1.00	0.52	0.41	0.45	0.47
D4	0.64	0.52	1.00	0.67	0.67	0.60
D5	0.52	0.41	0.67	1.00	0.57	0.59
D6	0.55	0.45	0.67	0.57	1.00	0.71
D7	0.55	0.47	0.60	0.59	0.71	1.00

Table 4.23: Corrected item-total correlation and Cronbach's alpha for the perceived self-efficacy domain

	Corrected item-total correlation	Cronbach's alpha
D2	0.68	0.88
D3	0.57	
D4	0.78	
D5	0.68	
D6	0.74	
D7	0.73	

4.10.4.4 Internal Consistency Result for the Perceived Response Efficacy Domain

For the *perceived response efficacy* domain, all the items fulfilled the properties of good internal consistency, as recommended by Mokkink et al. (2010). The inter-item correlation values ranged between 0.3 and 0.9 (Table 4.24). The CITC values were above 0.3 and the Cronbach's alpha value was above 0.7 (Table 4.25).

Table 4.24: Inter-item correlation matrix of the items for the perceived response efficacy domain

	E1	E2	E3	E4	E5	E6	E7
E1	1.00	0.81	0.63	0.69	0.62	0.53	0.59
E2	0.81	1.00	0.71	0.74	0.62	0.59	0.59
E3	0.63	0.71	1.00	0.72	0.61	0.73	0.69
E4	0.69	0.74	0.72	1.00	0.74	0.74	0.79
E5	0.62	0.62	0.61	0.74	1.00	0.66	0.70
E6	0.53	0.59	0.73	0.74	0.66	1.00	0.81
E7	0.59	0.59	0.69	0.79	0.70	0.81	1.00

Table 4.25: Corrected item-total correlation and Cronbach's alpha for the perceived response efficacy domain

	Corrected item-total correlation	Cronbach's alpha
E1	0.74	0.94
E2	0.79	
E3	0.80	
E4	0.87	
E5	0.77	
E6	0.79	
E7	0.82	.

4.10.4.5 Internal Consistency Result for the Perceived Psychological Cost Domain

For the *perceived psychological cost* domain, all the items fulfilled the properties of good internal consistency, as recommended by Mokkink et al. (2010). The inter-item correlation values ranged between 0.3 and 0.9 (Table 4.26), while the CITC values were all above 0.3 and the Cronbach's alpha was above 0.7 (Table 4.27).

Table 4.26: Inter-item correlation matrix of the items for the perceived psychological cost domain

	F1	F4	F5
F1	1.00	0.62	0.56
F4	0.62	1.00	0.73
F5	0.56	0.73	1.00

Table 4.27: Corrected item-total correlation and Cronbach's alpha for the perceived psychological cost domain

	Corrected item-total correlation	Cronbach's alpha
F1	0.63	0.84
F4	0.77	
F5	0.72	

4.10.4.6 Internal Consistency Result for the Perceived Tangible Cost Domain

For the *perceived tangible cost* domain, all the items fulfilled the properties of good internal consistency, as recommended by Mokkink et al. (2010). The inter-item correlation values ranged between 0.3 and 0.9 (Table 4.28). The CITC values were above 0.3 and the Cronbach's alpha was above 0.7 (Table 4.29).

Table 4.28: Inter-item correlation matrix of the items for the perceived tangible cost domain

	F2	F3	F6	F7
F2	1.00	0.72	0.56	0.53
F3	0.72	1.00	0.66	0.65
F6	0.56	0.66	1.00	0.76
F7	0.53	0.65	0.76	1.00

Table 4.29: Corrected item-total correlation and Cronbach's alpha for the perceived tangible cost domain

	Corrected item-total correlation	Cronbach's alpha
F2	0.68	0.88
F3	0.78	
F6	0.76	
F7	0.75	

4.10.4.7 Internal Consistency Result for the Perceived Maladaptive Reward Domain

For the *perceived maladaptive reward* domain, all the items fulfilled the properties of good internal consistency, as recommended by Mokkink et al. (2010). The inter-item correlation values were between 0.3 and 0.9 (Table 4.30). The CITC values were all above 0.3 and the Cronbach's alpha value was above 0.7 (Table 4.31).

Table 4.30: Inter-item correlation matrix of the items for the perceived maladaptive reward domain

	G2	G3	G4	G5
G2	1.00	0.50	0.47	0.55
G3	0.50	1.00	0.59	0.38
G4	0.47	0.59	1.00	0.43
G5	0.55	0.38	0.43	1.00

Table 4.31: Corrected item-total correlation and Cronbach's alpha for the perceived maladaptive reward domain

	Corrected item-total correlation	Cronbach's alpha
G2	0.63	0.79
G3	0.61	
G4	0.62	
G5	0.54	

4.10.4.8 Internal Consistency Result for the Discursive Digital Security Domain

For the *discursive digital security* domain, all the items fulfilled the properties of good internal consistency, as recommended by Mokkink et al. (2010). The inter-item correlation values were between 0.3 and 0.9 (Table 4.32). The CITC values were above 0.3 and the Cronbach's alpha was above 0.7 (Table 4.33).

Table 4.32: Inter-item correlation matrix of the items for the discursive digital security domain

	H1	**H2**	**H3**	**H4**
H1	1.00	0.75	0.71	0.70
H2	0.75	1.00	0.86	0.81
H3	0.71	0.86	1.00	0.86
H4	0.70	0.81	0.86	1.00

Table 4.33: Corrected item-total correlation and Cronbach's alpha for the discursive digital security domain

	Corrected item-total correlation	Cronbach's alpha
H1	0.76	0.93
H2	0.88	
H3	0.89	
H4	0.86	

4.10.4.9 Internal Consistency Result for the Control Digital Security Domain

For the *control digital security* domain, all the items fulfilled the properties of good internal consistency, as recommended by Mokkink et al. (2010). The inter-item correlation values ranged between 0.3 and 0.9 (Table 4.34). The CITC values were above 0.3 and the Cronbach's alpha value was above 0.7 (Table 4.35).

Table 4.34: Inter-item correlation matrix of the items for the control digital security domain

	H5	H6	H7	H8	H9	H10	H11
H5	1.00	0.53	0.48	0.46	0.43	0.54	0.49
H6	0.53	1.00	0.62	0.57	0.52	0.58	0.54
H7	0.48	0.62	1.00	0.73	0.56	0.53	0.52
H8	0.46	0.57	0.73	1.00	0.52	0.48	0.51
H9	0.43	0.52	0.56	0.52	1.00	0.54	0.61
H10	0.54	0.58	0.53	0.48	0.54	1.00	0.68
H11	0.49	0.54	0.52	0.51	0.61	0.68	1.00

Table: 4.35: Corrected item-total correlation and Cronbach's alpha for the control digital security domain

	Corrected item-total correlation	Cronbach's alpha
H5	0.61	0.89
H6	0.71	
H7	0.73	
H8	0.69	
H9	0.67	
H10	0.71	
H11	0.72	

4.10.5 Internal Consistency Summary

The internal consistency of all the items was deemed good for their respective domains. Hence, no further items were deleted. Following the completion of the internal consistency evaluation, the CFA, CCA (measurement model), and structural model assessments were performed using SEM.

4.10.6 Structural Equation Modelling Analysis: Initial Data Assessment

A completely new dataset from that used in the EFA and internal consistency assessment was used for the SEM analysis. This dataset contained 364 data. The normality assumption and the common method variance were assessed prior to SEM, the findings of which are described in the next two paragraphs.

The normality assumption was assessed based on Mardia's multivariate normality (Mardia, 1974), in which a significant p-value indicates that the multivariate normality assumption is not met. In this study, the p-value for the data was < 0.001 (Table 4.36), which indicated that the assumption of multivariate normality was not met. Thus, the bootstrapping technique for obtaining estimations was applied in order to address this issue.

Table 4.36: Multivariate normality assumption test

	Beta	**Z**	**p-value**
Skewness	16.16	980.18	< 0.001
Kurtosis	143.53	14.49	< 0.001

The common method variance was explored based on a full collinearity assessment (Kock & Lynn, 2012). This was performed using SPSS to check the collinearity between the latent variable scores. Common method bias is present if multicollinearity is present between the independent variables (lateral collinearity), or between the independent and dependent variables (horizontal collinearity). As shown in Table 4.37, the VIF value between the variables was less than 3.3, which indicated that common method bias was not present.

Table 4.37: Common method variance assessment

Coefficients[a]

	Unstandardised coefficients		Standardised coefficients	t	Sig.	Collinearity statistics	
	B	Std. error	Beta			Tolerance	VIF
(Constant)	0.39	0.03		15.18	0.00		
Control practice	0.02	0.04	0.04	0.58	0.57	0.49	2.06
Discursive practice	0.00	0.03	-0.01	-0.12	0.91	0.64	1.56
Maladaptive reward	0.00	0.03	-0.01	-0.08	0.93	0.77	1.30
Perceived psychological cost	0.02	0.03	0.03	0.53	0.60	0.71	1.40
Perceived response efficacy	0.00	0.04	-0.01	-0.10	0.92	0.40	2.53
Perceived self-efficacy	-0.06	0.04	-0.13	-1.58	0.12	0.41	2.42
Perceived severity	0.02	0.03	0.04	0.70	0.49	0.80	1.25
Perceived susceptibility	-0.01	0.03	-0.01	-0.19	0.85	0.83	1.21
Perceived tangible cost	0.05	0.03	0.11	1.89	0.06	0.80	1.25

4.10.7 CFA and CCA (Measurement Model Assessment)

The measurement model assessment was done on the outer model structure, which was between the items and their respective domains. Based on the proposed model, two types of domain were identified in the outer model structure, namely, reflective and formative domains. The reflective domains were the domains that were identified in the EFA (Figure 4.8).

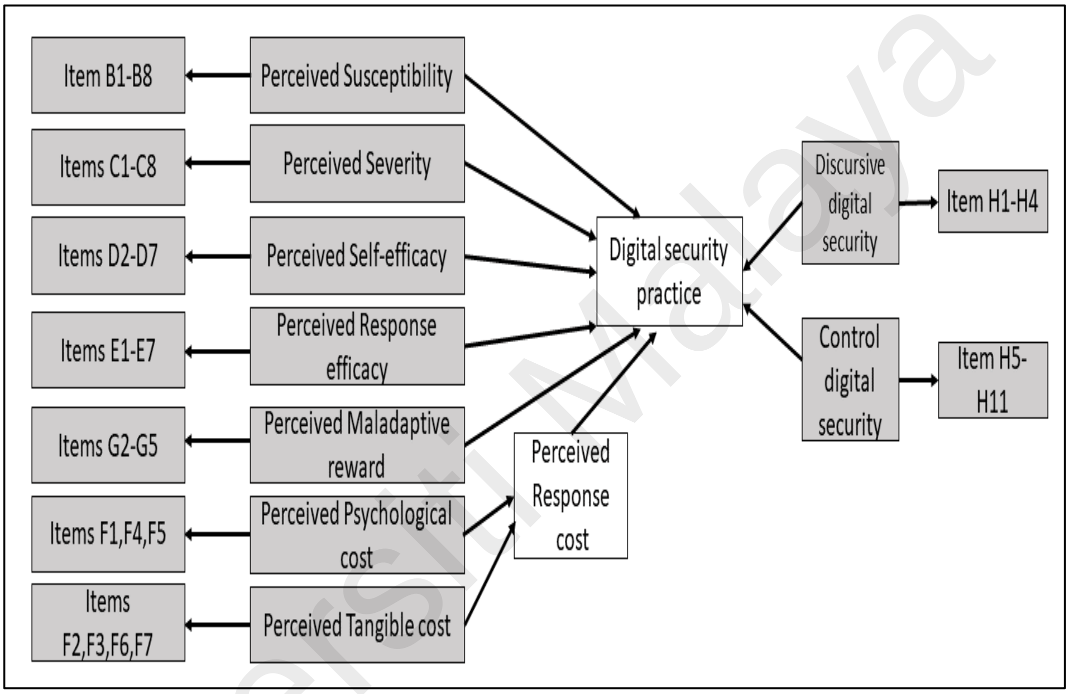

Figure 4.8: Reflective domains and their items (shaded grey) in outer model for measurement model assessment

Additionally, the second-order domains, namely, *digital security practice* and *perceived response cost,* were identified as formative domains (Figure 4.9 and Figure 4.10, respectively).

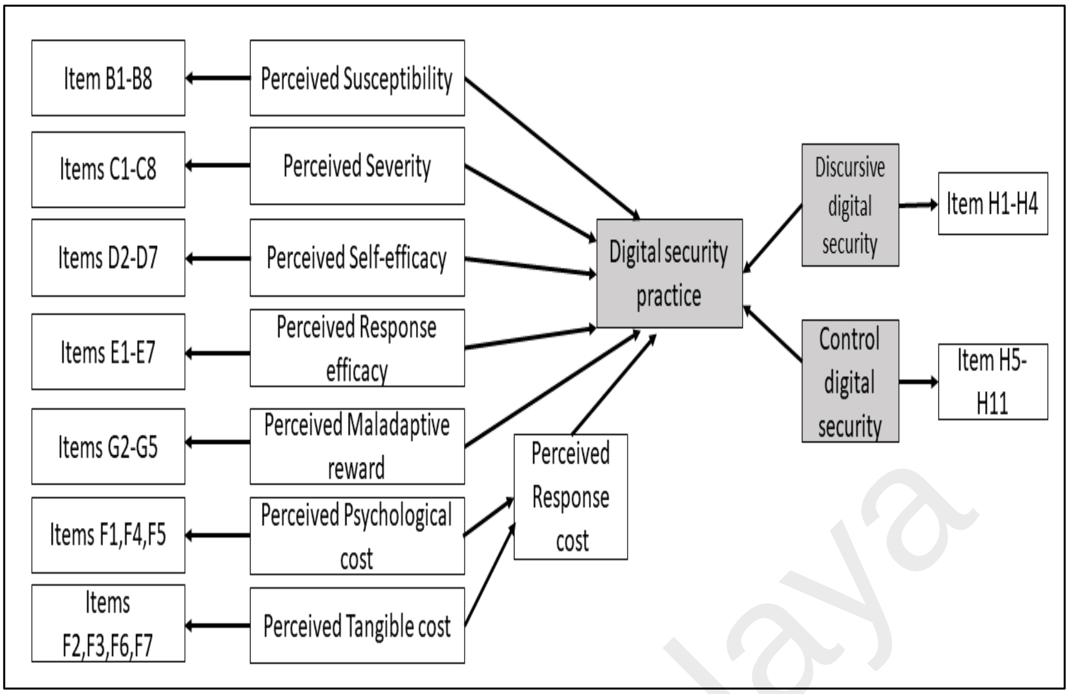

Figure 4.9: Formative domain of digital security practice and its subdomains (shaded grey) in outer model for measurement model assessment

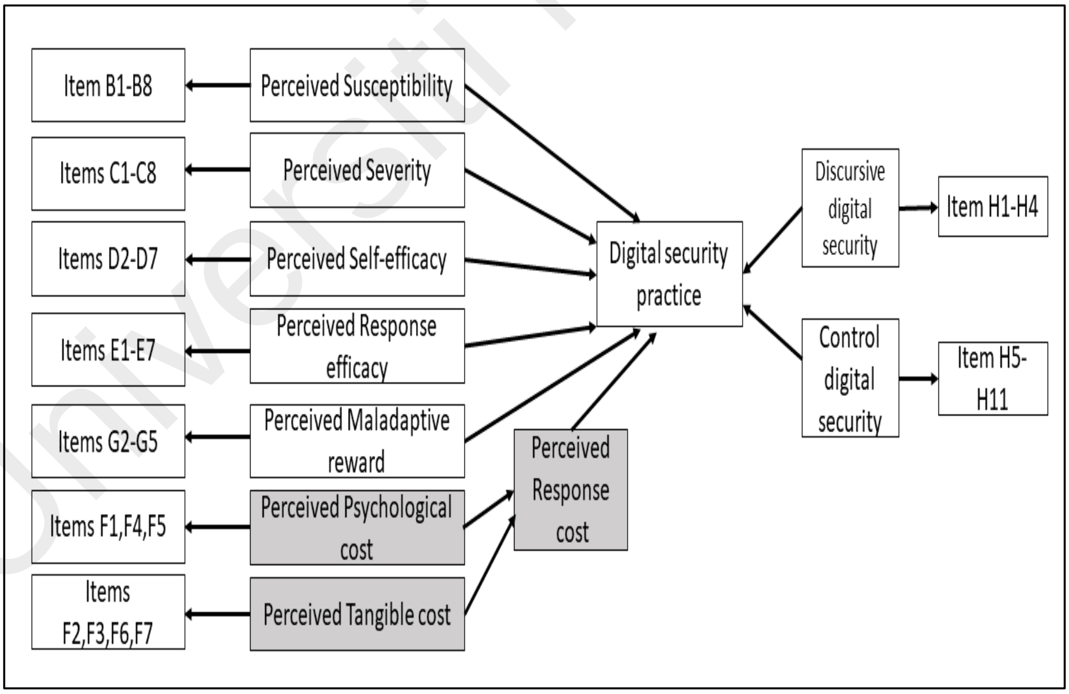

Figure 4.10: Formative domain of perceived response cost and its subdomains (shaded grey) in outer model for measurement model assessment

This distinction is necessary as the measurement model assessment differs between the formative and reflective types of domain. For reflective domains, the measurement model assessment or CFA is based on convergent validity, discriminant validity, and reliability (Hair et al., 2016). On the other hand, CCA involves the inspection of collinearity, outer loadings and the outer weight of the formative domains (Hair et al., 2016).

A measurement model assessment is a crucial step prior to assessing the structural model, which is the inner model structure (Hair et al., 2016). The inner model structure in this study is illustrated in Figure 4.11 below.

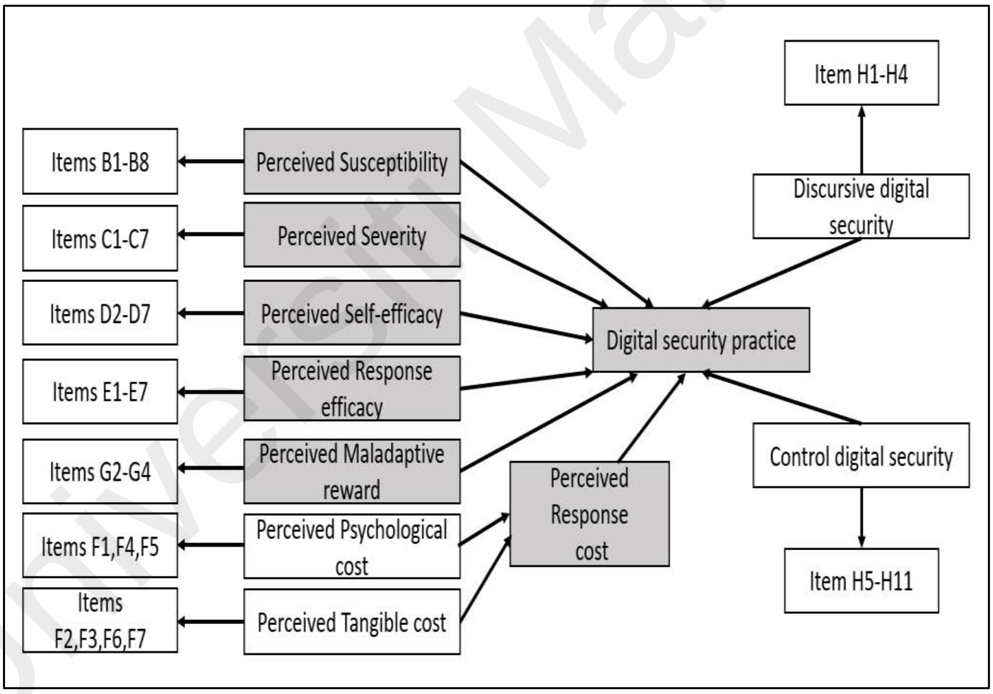

Figure 4.11: Inner model structure (shaded grey) for structural model assessment

4.10.7.1 CFA (Measurement Model Assessment for the Reflective Domains)

For reflective domains, the measurement model assessment or CFA was based on convergent validity, discriminant validity, and reliability. This was performed by using SmartPLS 3.0 software.

Convergent validity was examined based on the factor loadings and AVE of the domains. The factor loadings of the items on their respective domains were all above 0.5 (Table 4.38). Also, the AVE for all the domains was above 50% (Table 4.39).

Table 4.38: The factor loadings of the items on their respective domains

	Perceived susceptibility	**Perceived severity**	**Perceived self-efficacy**	**Perceived response efficacy**	**Perceived psychological cost**	**Perceived tangible cost**	**Perceived maladaptive reward**	**Discursive digital security**	**Control digital security**
B1	0.74								
B2	0.72								
B3	0.85								
B4	0.79								
B5	0.81								
B6	0.88								
B7	0.89								
B8	0.90								
C1		0.78							
C2		0.70							
C3		0.85							
C4		0.94							
C5		0.96							
C6		0.87							
C7		0.84							
C8		0.79							
D2			0.81						
D3			0.72						
D4			0.87						
D5			0.81						
D6			0.79						
D7			0.84						
E1				0.81					
E2				0.82					
E3				0.88					
E4				0.91					
E5				0.90					
E6				0.84					
E7				0.89					
F1					0.83				
F4					0.91				
F5					0.86				

Table 4.38, continued

	Perceived susceptibility	Perceived severity	Perceived self-efficacy	Perceived response efficacy	Perceived psychological cost	Perceived tangible cost	Perceived maladaptive reward	Discursive digital security	Control digital security
F2						0.79			
F3						0.86			
F6						0.85			
F7						0.84			
G2							0.85		
G3							0.78		
G4							0.81		
G5							0.70		
H1								0.88	
H2								0.94	
H3								0.93	
H4								0.90	
H5									0.73
H6									0.83
H7									0.87
H8									0.86
H9									0.77
H10									0.81
H11									0.82

Table 4.39: The average variance extracted for all the reflective domains

	Average variance extracted (AVE)
Control digital practice	0.66
Discursive digital practice	0.83
Perceived maladaptive reward	0.62
Perceived psychological cost	0.75
Perceived response efficacy	0.75
Perceived self-efficacy	0.65
Perceived severity	0.71
Perceived susceptibility	0.68
Perceived tangible cost	0.70

Hence, the reflective domains in this model fulfilled the requirements for convergent validity because all the factor loadings exceeded 0.5 and the items' respective domains had an AVE value of more than 50%.

The discriminant validity of the model was assessed based on the HTMT ratio of the domains in the outer model. The findings showed that all the ratio values were below 0.85, which indicated that there was good discriminant validity among the domains (Table 4.40).

Table 4.40: HTMT ratio of reflective domains

	Control digital practice	**Discursive digital practice**	**Perceived maladaptive reward**	**Perceived psychological cost**	**Perceived response efficacy**	**Perceived self-efficacy**	**Perceived severity**	**Perceived susceptibility**	**Perceived tangible cost**
Control digital practice									
Discursive digital practice	0.63								
Perceived maladaptive reward	0.42	0.23							
Perceived psychological cost	0.21	0.07	0.41						
Perceived response efficacy	0.53	0.28	0.35	0.30					
Perceived self-efficacy	0.57	0.35	0.31	0.34	0.80				
Perceived severity	0.10	0.06	0.09	0.17	0.24	0.17			
Perceived susceptibility	0.13	0.12	0.18	0.16	0.06	0.12	0.33		
Perceived tangible cost	0.16	0.12	0.08	0.36	0.21	0.13	0.12	0.11	

Hence, the reflective domains in the model fulfilled the discriminant validity criteria.

Also, the minimum CR value of the reflective domains was 0.87, which indicated that all the domains possessed good internal consistency. The CR value of each domain is shown in Table 4.41

Table 4.41: Composite reliability value for each reflective domain

	Composite reliability (CR)
Control digital practice	0.93
Discursive digital practice	0.95
Perceived maladaptive reward	0.87
Perceived psychological cost	0.90
Perceived response efficacy	0.95
Perceived self-efficacy	0.92
Perceived severity	0.95
Perceived susceptibility	0.94
Perceived tangible cost	0.90

In summary, from the measurement model assessment of the reflective domains, it was determined that the model fulfilled the convergent validity criteria because all the AVE values of the domains were above 50%, and the factor loadings for all the items were greater than 0.5. The model was also found to have good discriminant validity, as reflected by the HTMT ratio of less than 0.85 for all the outer model domains. Lastly, the assessment also revealed that the model possessed good internal consistency because the CR value was above 0.8 for all the reflective domains. Hence, the reflective domains had good psychometric properties in terms of discriminant validity, convergent validity, and reliability. Therefore, a further assessment was undertaken to examine the formative domains of the measurement model.

4.10.7.2 CCA (Measurement Model Assessment for the Formative Domains)

For formative domains, the measurement model assessment of CCA was based on the collinearity, relevance and significance of the domains. This was performed by using SmartPLS 3.0 software. The process flow followed in assessing the CCA is illustrated in Figure 4.12;

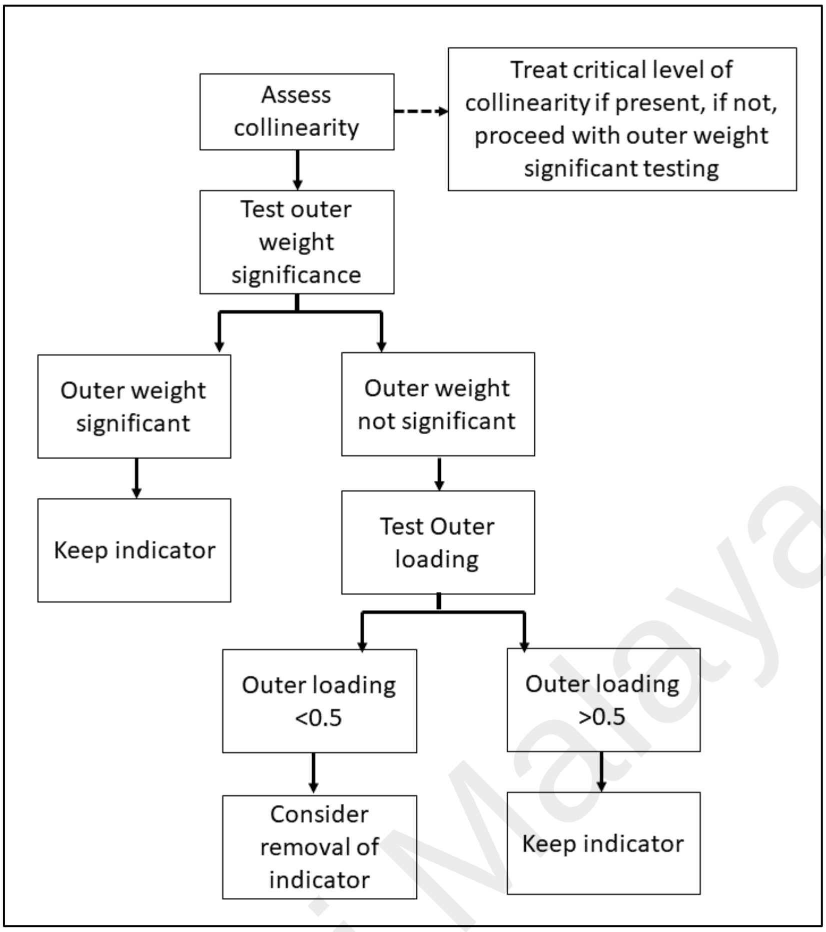
Assess collinearity
Treat critical level of collinearity if present, if not, proceed with outer weight significant testing
Test outer weight significance
Outer weight significant
Outer weight not significant
Keep indicator
Test Outer loading
Outer loading <0.5
Outer loading >0.5
Consider removal of indicator
Keep indicator

Figure 4.12: Process flow for assessing CCA

Adapted from Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*: Sage Publications.

The first aspect that was examined was the collinearity of the subdomains. An examination of the block of subdomains that formed the two second-order formative domains revealed no issue of collinearity between the subdomains and their respective domain. The VIF between the *discursive* and *control practice* subdomains that formed *digital security practice* domain was 1.58, and the VIF between the *psychological cost* and *tangible cost* subdomains that formed *perceived response cost* domain was 1.13. Both values were below the accepted critical cut-off value of 3.3 (Table 4.42).

Table 4.42: VIF values between items for digital security practice and perceived response cost

	VIF
Control digital practice	1.54
Discursive digital practice	1.54
Perceived psychological cost	1.10
Perceived tangible cost	1.10

As the collinearity level was below the critical value, the assessment of the formative proceeded in order to determine the relevance and significance of the formative subdomains in relation to their domains. The relevance and significance were analysed by examining the items' relative and absolute importance for their respective domain. The relative importance of the items to the domain was based on the outer weight assessment, which was the second component of the CCA that was examined, as shown in Figure 4.13.

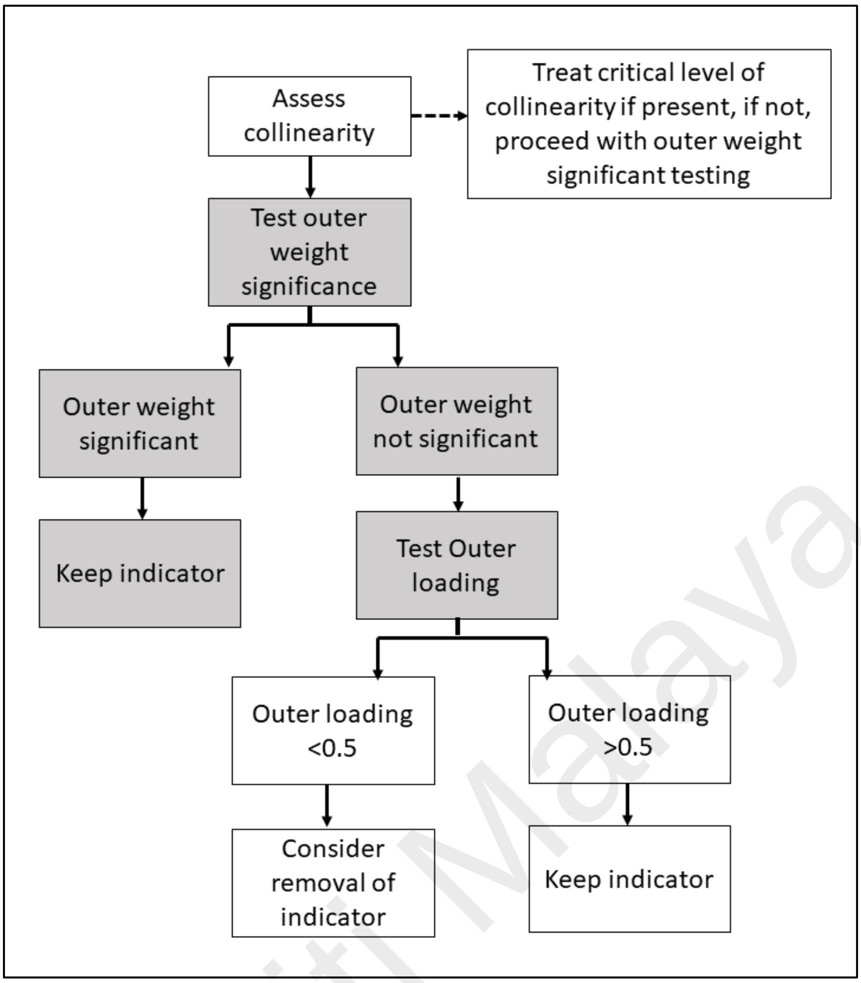
Assess collinearity
Treat critical level of collinearity if present, if not, proceed with outer weight significant testing
Test outer weight significance
Outer weight significant
Outer weight not significant
Keep indicator
Test Outer loading
Outer loading <0.5
Outer loading >0.5
Consider removal of indicator
Keep indicator

Figure 4.13: Process for assessing outer weight significance (shaded grey)

The values of the outer weights can be compared with each other and can, therefore, be used to determine each item's relative contribution to the domain or its relative importance. However, the outer weight's significance level needs to be determined as well. The significance level indicates whether the formative subdomains truly contribute to the formation of the domain.

As shown in Table 4.43, in the case of the formative domain *digital security practice*, the subdomain *control digital practice* had a higher outer weight value as compared to *discursive digital practice*. The assessment also revealed that the *control digital practice* subdomain was statistically significant, but the *discursive digital practice* subdomain was not. As for the formative domain *perceived response cost*, the *perceived psychological cost* subdomain had a higher outer weight than the *perceived tangible cost* subdomain. However, both subdomains were not statistically significant.

Table 4.43: The outer weights of the subdomains for digital security practice and perceived response cost

	Outer weight	**T-statistics**	**P-value**	**95% confidence interval**	
				Lower bound	**Upper bound**
Control digital practice - > digital security practice	1.01	14.96	< 0.001	0.88	1.10
Discursive digital practice - > digital security practice	-0.02	0.14	0.44	-0.21	0.18
Perceived psychological cost - > perceived response cost	0.91	1.02	0.16	-0.94	1.04
Perceived tangible cost - > perceived response cost	-0.77	1.01	0.16	-0.80	0.97

According to Hair et al. (2016), nonsignificant subdomain weights should not automatically be interpreted as indicating poor measurement model quality. The subdomain's absolute contribution to its domain needs to be assessed as well. This is done by looking at the outer loading of the nonsignificant subdomains. If the outer loading is more than 0.5, regardless of its statistical significance, the subdomain can be retained for analysis, as illustrated in Figure 4.14. Hence, the outer loadings of *discursive digital practice*, *perceived psychological cost* and *perceived tangible cost* were assessed further.

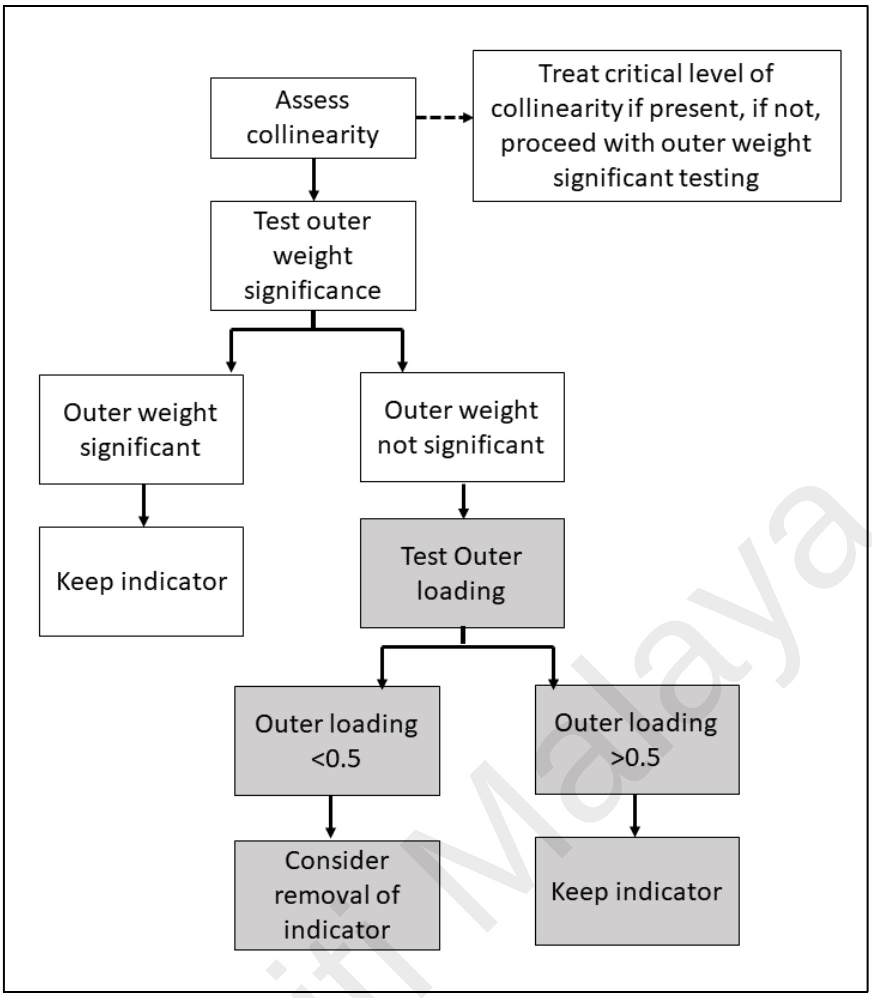
Assess collinearity
Treat critical level of collinearity if present, if not, proceed with outer weight significant testing
Test outer weight significance
Outer weight significant
Outer weight not significant
Keep indicator
Test Outer loading
Outer loading <0.5
Outer loading >0.5
Consider removal of indicator
Keep indicator

Figure 4.14: Process for assessing outer load significance (shaded grey)

From Table 4.44, the outer loading values of all three subdomains were more than 0.5 for their respective domains. Based on Hair et al. (2016), this indicates that the subdomains still contribute to the formative domains and they were therefore retained for further analysis.

Table 4.44: Outer Loading Values for Remaining Subdomains for Formative Domains

	Outer loading	T-statistics	P-value	95% confidence interval	
				Lower bound	Upper bound
Discursive digital practice - > digital security practice	0.58	6.67	< 0.001	0.42	0.72
Perceived psychological cost - > perceived response cost	0.68	1.01	0.16	-0.70	0.88
Perceived tangible cost - > perceived response cost	-0.50	0.98	0.16	-0.54	0.75

Thus, in summary, the CCA results showed that for both of the formative domains, namely, *digital security practice* and *perceived response cost*, there was no issue of multicollinearity. Moreover, the examination of the subdomains that formed both domains revealed that the subdomains were relevant and contributed to the formation of the domains. Thus, the measurement model assessment of the formative domains was considered adequate and acceptable.

As both the reflective and formative domains fulfilled the criteria of the measurement model assessment, the next step that was taken was an assessment of the inner model structure, also known as the structural model assessment.

4.10.8 Structural Model Assessment

The findings of the structural model assessment are presented in the following subsections. This assessment focused on collinearity, path coefficients, the R^2 level, and the effect size. The procedures that were followed were elaborated previously in the 'Methodology' chapter.

4.10.8.1 Assessment of Collinearity

The assessment of collinearity between the latent variables revealed that the highest VIF value was 2.44. This indicated that the issue of multicollinearity was not present because all the VIF values of the latent variables were below the cut-off point of 3.3, as shown in Table 4.45.

Table 4.45: The VIF values between the latent variables in the structural model assessment

	Digital security practice
Maladaptive reward	1.22
Perceived response efficacy	2.44
Perceived self-efficacy	2.26
Perceived severity	1.19
Perceived susceptibility	1.17
Perceived response cost	1.26

4.10.8.2 Assessment of Path Coefficients

An assessment of the path coefficients was conducted by performing bootstrapping with 5000 samples in order to determine the relationship between the independent latent variables and the dependent latent variable in the structural model. The results are shown in Table 4.46.

Table 4.46: The path coefficients between the latent variables and digital security practice in the structural model assessment

	Path coefficient	T Statistics	P Values	95% Confidence Interval	
				Lower bound	Upper bound
Maladaptive reward -> digital security	-0.20	3.57	<0.001	-0.29	-0.11
Perceived response efficacy -> digital security	0.21	2.24	0.01	0.06	0.36
Perceived self-efficacy -> digital security	0.30	3.29	<0.001	0.14	0.44

Table 4.46, continued

	Path coefficient	T Statistics	P Values	95% Confidence Interval	
				Lower bound	Upper bound
Perceived severity -> digital security	0.02	0.26	0.40	-0.14	0.10
Perceived susceptibility -> digital security	-0.06	1.34	0.09	-0.13	0.04
Response cost -> digital security	-0.01	0.21	0.42	-0.11	0.06

From the table, it can be seen that among the independent latent variables, only *perceived maladaptive reward*, *perceived self-efficacy*, and *perceived response efficacy* were significantly associated with *parental digital security practice*. *Perceived maladaptive reward* had a negative relationship with *parental digital security practice* (β = -0.20, p < 0.001). This implies that the higher the level of *perceived maladaptive reward*, the less *parental digital security practice* would be applied. *Perceived self-efficacy* (β = 0.30, p < 0.001) had a positive relationship with *parental digital security practice.* Hence the higher the level of *perceived self-efficacy*, the more *parental digital security practice* would be applied. *Perceived response efficacy* also had a positive relationship with *parental digital security practice* (β = 0.21, p = 0.01). Therefore, the higher the level of *perceived response efficacy*, the more *parental digital security practice* would be applied.

4.10.8.3 Assessment of Coefficient of Determination (R^2) Level

The R^2 level in this model was 0.34, as shown in Figure 4.15. This indicated that 34% of the variation in *parental digital security practice* was explained by the model. Based on the interpretation of R^2 by Hair et al. (2010), this model provides a weak to moderate explanation of the level of variation in *parental digital security practice*.

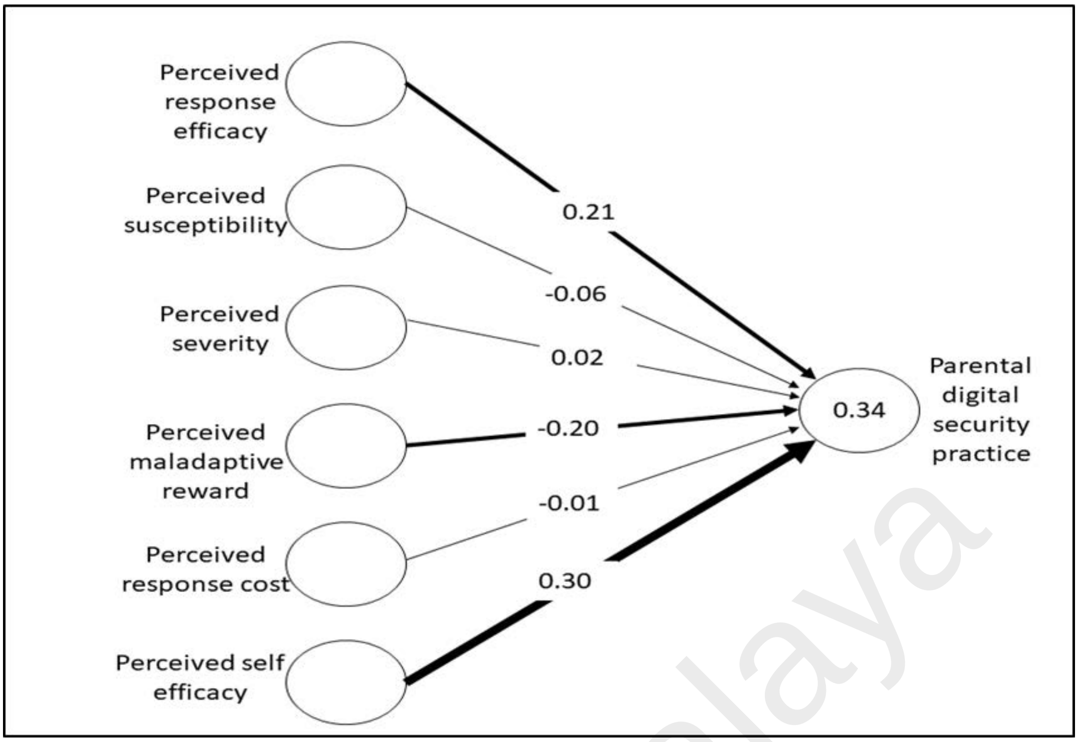

Figure 4.15: Coefficient of determination (R^2) and the respective path coefficient of each domain in the structural model

4.10.8.4 Assessment of Effect Size

The results of the assessment of the size of the effect that each independent latent variable had on the dependent variable *parental digital security practice* is presented in Table 4.47.

Table 4.47: The effect size between the latent variables and parental digital security practice in the structural model assessment

	Parental digital security practice
Perceived maladaptive reward	0.03
Perceived response efficacy	0.05
Perceived self-efficacy	0.08
Perceived severity	0.00
Perceived susceptibility	0.00
Perceived response cost	0.00

By taking 0.02 as the cut-off for the minimum effect size that was deemed to be significant, only *perceived maladaptive reward*, *perceived self-efficacy* and *perceived response efficacy* were found to have any significant effect on *digital security practice. Perceived self-efficacy* showed the highest effect size at 0.08. Even so, the effect size of these three variables was low to moderate based on the effect size criteria in Cohen (2013).

In summary, the structural model assessment revealed that only p*erceived self-efficacy, perceived response cost* and *perceived maladaptive reward* had a statistically significant linear relationship with *parental digital security practice*. *Perceived self-efficacy* and *perceived response cost* had a positive relationship with *parental digital security*, whereas *perceived maladaptive reward* had a negative relationship with *parental digital security practice*. Among these three domains, *perceived self-efficacy* had the highest influence. *Perceived response cost, perceived susceptibility* and *perceived severity* did not have a significant linear relationship with *parental digital security practice*. Overall, the model was able to explain 34% of the variation in *parental digital security practice*. The remaining 66% of the variation was not able to be explained by this model and was therefore considered to be explained by other domains not addressed in this study.

4.10 Summary of Chapter Four

This chapter described how the initial phase of item development produced a bilingual 54-item questionnaire covering six domains, namely, *perceived susceptibility, perceived severity, perceived self-efficacy, perceived response efficacy, perceived maladaptive reward, perceived response cost* and *parental digital security practice*. The chapter then explained how the questionnaire was further refined in the scale development phase, in which two items, namely, D1 and H12 were dropped due to poor relevance to parents and poor test-retest reliability. This was followed by a factor analysis, that further reduced the items due to the dropping of G1 because of poor loading. The scale development resulted in producing a 51-item questionnaire covering nine domains, namely, *perceived susceptibility, perceived severity, perceived self-efficacy, perceived response efficacy, perceived tangible cost, perceived psychological cost, perceived maladaptive reward, discursive digital security practice* and *control digital security practice* (see Appendix M).

The chapter then presented evidence showing that all the items had good internal consistency, with a minimum Cronbach's alpha for the domains of 0.79 and a minimum CITC of 0.54 for the items in their respective domains. Scale evaluation, using SEM was then performed, showing the measurement model assessment to be fulfilled and the final version of the instrument was validated (see Appendix M). It also described the further assessment on the relationship between the domains of PMT on *parental digital security practice*, which revealed that *perceived self-efficacy* was the biggest predictor of *parental digital security practice*, followed by *perceived maladaptive reward* and *perceived response efficacy*. It also stated that *perceived susceptibility, perceived severity* and *perceived response cost* did not have a significant relationship with *parental digital security practice*. The chapter concluded by stating that the model was able to explain 34% of variation in *parental digital security practice*.

CHAPTER FIVE: DISCUSSION

5.1 Introduction

This chapter starts by discussing the results of the study and provides a justification for the processes followed in developing the questionnaire. Firstly, the identification of the domains is discussed, followed by the findings from the systematic review in respect of the quality of existing PMT-based questionnaires. Next, findings from the item and scale development processes are discussed by looking into the items that were removed, the items that were retained and the format of the overall questionnaire. These three aspects are highlighted in this chapter because they represent the end product of the item and scale development processes in this study. Then, the findings from the field survey that was conducted for the scale evaluation are discussed by dissecting the relationship between the domains that were identified by this study as pertaining to parental digital security practice in the Malaysian context. Following this, the potential utilisation of the study findings, the public health implications, the research implications, and the strengths and limitations of the study are explained. Lastly, some recommendations on the policy and future research stemmed from this study were highlighted.

5.2 Domain Identification

Domain identification is a crucial step in the scale development process because it clarifies the direction of the research, the boundaries of the domains, and the method(s) that should be adopted to analyse the data obtained from the scale produced (DeVellis, 2017). Furthermore, DeVellis (2017) recommends that a theory should be chosen to aid in the identification of the domains. This study adopted that approach by using PMT as the basis in identifying the domains. By doing so, the boundaries of the domains became clear, which helped in developing the scale. Additionally, it was envisaged that the use of a grounded theory would assist in explaining the phenomenon of parental digital security because the domains identified had a clear basis in terms of the relationship between them. This study took a further step to enhance the domain identification process, choosing not to rely solely on a theory and the literature in identifying the domains. This additional step involved inviting experts in the field to review and discuss the proposed domains. These experts included CSM personnel, public health practitioners and a digital citizenship expert. This step reinforced the validity of the domains identified in terms of their potential to explain parental digital security practice.

In order to dissect the domain identification process further, Lazarsfeld (1958) suggests using imagery and domain operationalisation. Imagery involves the initial identification of the domains, and domain operationalisation involves the actual definition of the domains identified (Lazarsfeld, 1958). In this study, domain operationalisation was done to clarify the boundary of each domain and the concept that each domain was intended to capture. In this study, domain operationalisation was based on the theoretical definition of the domains according to PMT and this definition was refined to reflect the scope of parental digital security. As such, the boundary and concept of each of the domains became clearer, which helped in generating the items in the subsequent scale development phase.

Besides giving clarity to the boundaries and concepts of the domains, domain operationalisation is also important in determining the relationship between the domains and their respective items (Baxter, 2009; Coltman, Devinney, Midgley, & Venaik, 2008). Specifically, domain operationalisation determines whether the relationship between the domain and items is reflective or formative in nature (Baxter, 2009). A domain with reflective items is classically identified as one in which the nature of the items is 'caused by' the domain (Baxter, 2009). On the other hand, formative subdomains are identified as those in which the items are independent 'causes' of the domain they represent. These reflective and formative relationships are illustrated in Figure 5.1.

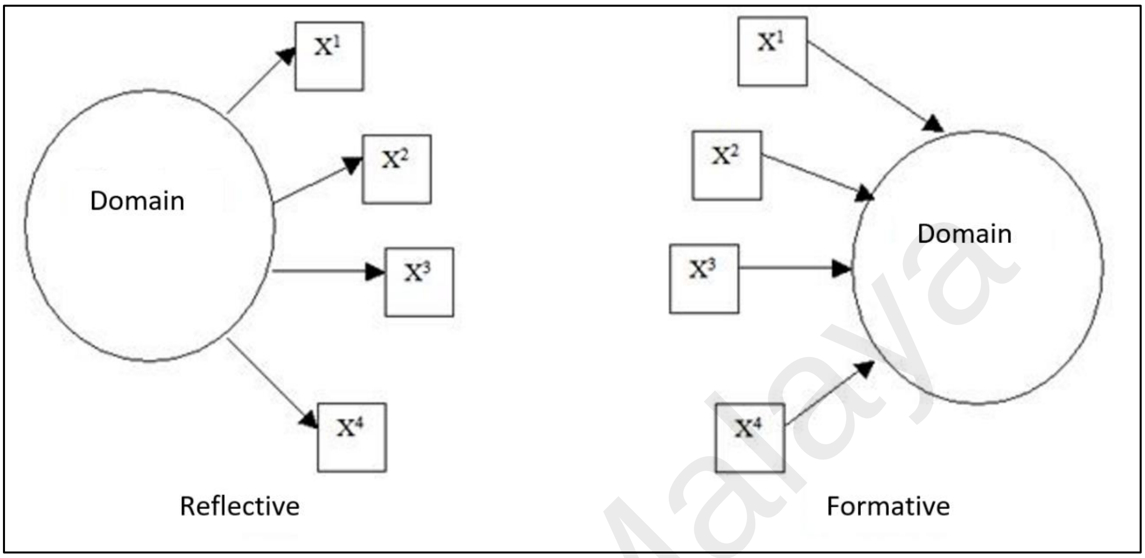

Figure 5.1: Schematic diagram of reflective and formative domains

From a theoretical point of view, reflective items possess a few more characteristics than formative items. The reflective items generally share a common theme and are interchangeable, and thus dropping an item does not change the meaning of the domain (Baxter, 2009; Coltman et al., 2008). A domain with reflective items exists independently of the measures used (Baxter, 2009; Coltman et al., 2008). In contrast, formative items do not necessarily share a common theme and are not interchangeable, and therefore dropping such items may influence the nature of the domain (Baxter, 2009; Coltman et al., 2008). In short, a domain with formative items exists through a combination of the items into a number of subdomains (Baxter, 2009; Coltman et al., 2008).

The operationalisation and definition of a domain thus plays a role in determining whether its relationship with its respective items is either reflective or formative. In this study, the domains *perceived susceptibility, perceived severity, perceived cost, perceived* *response efficacy, perceived self-efficacy* and *perceived maladaptive reward* were found to be reflective in nature. This is because the definition and nature of these domains were not based on the combination of the items. Instead, each of these domains possessed a global conceptual definition, the nature of which was reflected in its respective items. The relationship between these domains and respective items were shown in Figure 5.2.

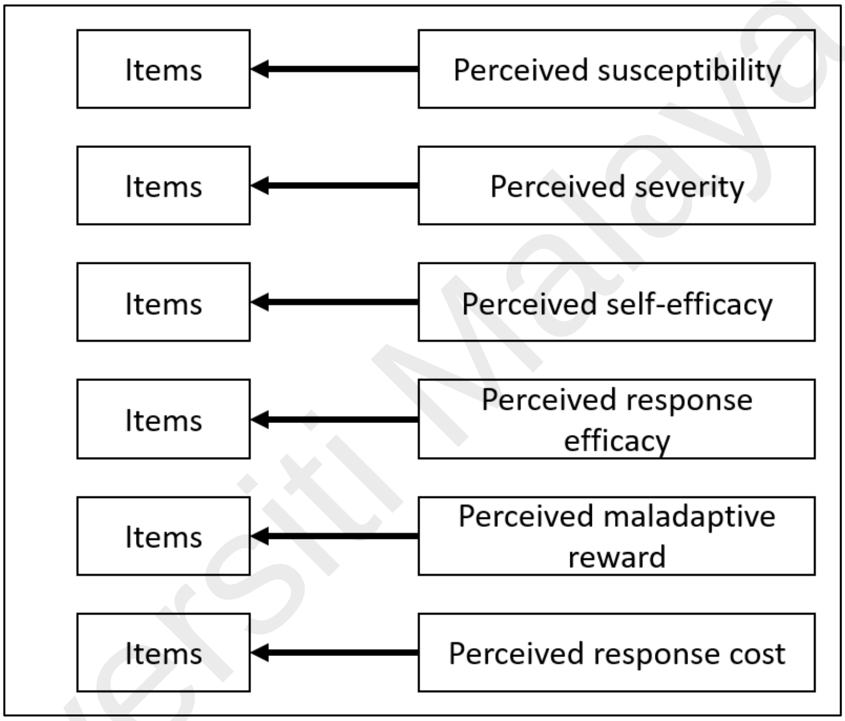

Figure 5.2: Reflective nature of relationship between domains and items in the study

However, the domain *parental digital security practice* was found to be formative in nature because the definition clearly identified the subdomains that made up *parental digital security practice*, namely, active-, monitoring-, restrictive-, co-use- and supervision-based digital security practice. However, these subdomains were found to have a reflective relationship with their items. This was again based on the definition of the subdomains. The conceptual definition of each subdomain was global in nature and reflected their respective items. The reflective/formative nature of the relationship between the domain, its subdomains and items are depicted in Figure 5.3. The distinction between the reflective and formative relationship influences the type of analysis used in validating the domains (Hair et al., 2016), as shown in this study.

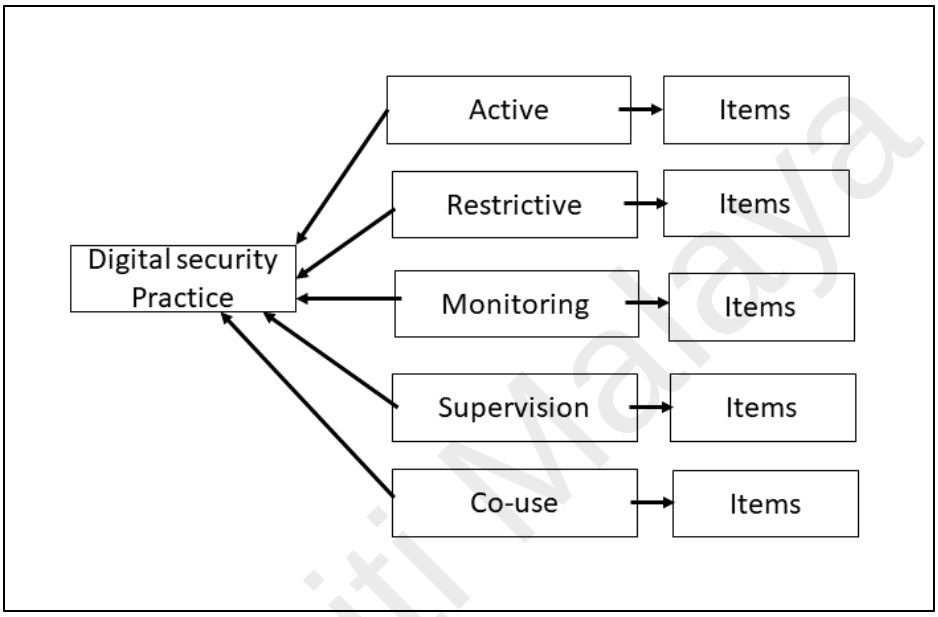

Figure 5.3: Formative nature of relationship between digital security practice domain and its subdomains

Although domain identification and operationalisation are crucial in the scale development stage, often at this stage, domain identification and domain definition are preliminary in nature and are exposed to further refinement as the scale develops (Boateng et al., 2018). Additional subdomains or adjustments to proposed domains might be needed, especially when the items used in the scale development are new and have not been tested, such as identified in this study. However, the structure of the scale developed needs to reflect, as much as possible, the proposed conceptual framework, and any modifications need to be supported by the literature, the domain structure and expert opinion (Akter, D'Ambra, & Ray, 2013; DeVellis, 2017). These additional supports were therefore adopted in this study as part of the scale development process. Initially, the domains, subdomains, and their relationships were initially defined based on the conceptual framework. However, further exploration of the domain structure led to refinement of the domains and subdomains, particularly *perceived response cost* and *parental digital security practice*.

5.3 Quality of Existing PMT-Based Questionnaires

The systematic review served two major purposes: to determine the quality of current existing PMT-based questionnaires on digital security, and to contribute to the deductive process of generating items for the proposed parental digital security questionnaire.

Overall, the systematic review demonstrated that the majority of the questionnaires were of good quality. However, the varying quality of the questionnaires discovered in the systematic review highlighted the challenges researchers face in developing this type of measurement tool. One of the reasons for the existence of poor-quality questionnaires is due to the misconception that the production of a questionnaire is an easy process, and this then leads to methodological errors during the process of questionnaire development (Boynton & Greenhalgh, 2004). Hence, the systematic review highlighted that there was a need to rely on robust and proper guidelines in developing the parental digital security questionnaire for this study.

The systematic review also revealed that the validated PMT-based questionnaires that were found were developed to address a wide variety of digital-related security issues, ranging from individual behaviour to organisational-based digital security practice. This reflected the suitability of using PMT to measure digital security behaviour. It also highlighted the complexity of the phenomenon of digital security itself which has triggered the development of various measurement tools to address different types of digital security behaviour in different populations.

The systematic review also highlighted that some gaps in knowledge on digital security practices were present and needed to be addressed. Firstly, none of the studies addressed parental digital security practice, which clearly showed that there was a huge gap that needed to be tackled. This finding was supported by the fact that PMT was originally designed to explain an individual's own protective behaviour towards themselves, as opposed to performing an action to protect other individuals, as in the case of parental digital security practice. However, since PMT was first proposed, various studies have emerged that have used PMT to explain the protective behaviour of protecting other individuals. For example, Beirens et al. (2008) used PMT to understand parents' motivation to install stair gates for their toddlers and, later, Gainforth, Cao, and Latimer-Cheung (2012) used PMT to understand parents' motivation to have their children immunised against the human papilloma virus.

The second gap that was identified in the systematic review was related to the geographical representation of the existing questionnaires. Geographically, the majority of the studies originated from the North America region and East Asia region. This raised the issue of the need to have questionnaires on digital security that are suitable and culturally appropriate for other parts of the world including Southeast Asia. As highlighted by Guillemin (1995), having culturally suitable measurement tools is important because one population might express and understand a particular issue differently due to cultural influence.

Although none of the studies found in the systematic review addressed parental digital security practice, the items that were extracted from those studies were still useful as part of the deductive process in the item development phase of this study. In particular, the items were used as a reference in terms of the keywords used to reflect the domains of PMT. For example, digital security practices were measured by using anchors that reflected frequency. For instance, items that reflected perceived susceptibility used the keyword ‘likely’, and this term was adopted in this study. Similarly, the keyword ‘seriousness’ was used to reflect the domain perceived severity, and this term was therefore adopted as well. The term ‘confident’ and ‘comfortable’ were also used in the domain perceived self-efficacy, based on the literature extracted in this systematic review as these two terms were used interchangeably and conceptually similar. This was a suitable approach to take because the adoption of terminology from established questionnaires increases the reliability of the items in representing the intended domains (Hunt, 1991; Straub, 1989), and proven so based on the reliability tests performed throughout this study. However, due to the lack of existing literature on parental digital security practice based on PMT, the generation of items in this study relied heavily on using the inductive process.

5.4 Item Retention

All the items that were retained for the final version of the questionnaire were based on the results of the item and scale development processes and were proven to be valid based on content validation and domain validation using factor analysis and measurement model assessment through CFA and CCA in the SEM analysis. The reliability of the items retained was also established, based on test-retest reliability and internal consistency. In the following, the retained items are discussed based on the respective domains they represent according to PMT.

5.4.1 Perceived Susceptibility and Perceived Severity

The domains *perceived susceptibility* to online threats and *perceived severity* to online threats shared the same items, but different question stems were used in order to reflect the difference between the two domains. In the case of *perceived susceptibility*, the stem question focused on asking the parents to judge the likelihood that the threat would occur to their children, as reflected by the phrase "how likely is your child to...?" in the stem question. The scale anchor wording also reflected the degree of likelihood, from very unlikely to very likely. On the other hand, the *perceived severity* stem question focused on the degree of the consequences that the parents perceived would occur if a child were to experience a particular threat. This was reflected in the phrase "how serious are these issues to you?" in the stem question. The domain *perceived severity* is unique to other domains as the items required the respondents to make judgment based on a hypothetical situation that occurs to a child in general, as opposed to their own child as found in other domains. This is based on feedback from experts, particularly from the cyber parenting expert and parents' representative in the item development phase. The discussion highlighted the possible reluctance from parents to answer if the items in *perceived severity* were to reflect their own children. This is because by implying the children were actually facing these online problems, some parents might be defensive and deemed culturally inappropriate. As such, the items were worded to represent a third party, reflected in the phrase "A child is…" in every item to create a more natural stance on the issues highlighted. The scale anchor wording also reflected the degree of severity, from not very serious to very serious. These stem questions were derived from literature that used PMT in exploring a particular protective behaviour. Hence these stem questions were already proven to be able to distinguish between *perceived susceptibility* and *perceived severity*, based on the clear discriminant validity between these two domains.

The *perceived susceptibility* and *perceived severity* domains in the parental digital security questionnaire were each represented by eight items. The items were related to interactions with people, privacy risk, content risk and online addiction risk. The items thus comprehensively reflected the different and common types of online threats, as identified based on the content analysis of the feedback received from Malaysian parents in the online survey conducted for this study, experts' views and as supported by the literature.

Items B1/C1 ("…to be bullied (harassed, threatened or/and intimidated) online), B5/C5 ("…to be approached online by a person he/she does not know) and B6/C7 ("…to exchange sexual messages or/and images with other people online) reflected the online threats based on interactions with people online. This type of online threat is widely reflected in the guidelines and literature related to cyber threats, as highlighted by CyberSecurity Malaysia (2018), Willard (2007), and Livingstone and Haddon (2008). Hence, the inclusion of these items enhanced the questionnaire in terms of having representative questions that reflected this particular important online threat.

Item B4/C4 ("…to have his/her personal information obtained without his/her knowledge or consent) was also retained because it represented another important online threat, namely, privacy risk. A study by CSM involving 20,000 children aged 7 to 17-years-old in 2014 showed that 22% of children were concerned about their privacy online (CyberSecurity Malaysia, 2014). This indicates that this risk is relevant in the Malaysian context. It was therefore right to represent it in the questionnaire developed in this study. Also, a study by the Family Online Safety Institute among 589 American parents of children and adolescents aged 6 to 17-years-old in 2015 revealed that 67% of the parents were worried about their children's online privacy (FOSI, 2015). Furthermore, Livingstone and Haddon (2008) highlighted that the online threat to privacy has been widely studied in the European setting as well, which implies that the relevance of this online threat is universal.

Items B3/C3 ("…to be exposed to adult content (e.g., pornography, violence, gambling)"), B7/C7 ("…to be exposed to online content promoting self-harm (e.g., websites that encourage suicide, eating disorders, drug use") and B8/C8 ("…to be exposed to online content that promotes hate, extreme views and terrorism") represented another type of online threat, namely, that related to content. This type of online threat has been highlighted in many guidelines both locally and internationally (FOSI, 2015; CyberSecurity Malaysia, 2018; Willard, 2007), which indicates the importance of this threat being represented in this study. This type of online threat was also one of the most researched in the European setting according to Livingstone and Haddon (2008), which further signals the huge magnitude that this threat carries among children online.

Lastly, item B2/C2 ("…to be spending more time online than he/she should") represented another online threat, namely, that related to online addiction or excessive usage of the internet. As highlighted by Willard (2007), prolonged usage of the internet increases the probability of children being exposed to other online threats such as content risk, contact risk and privacy issues. Also, the study by CSM involving 20,000 students aged 7 to 17-years-old showed that 20% of the respondents were worried about their excessive online pattern usage (CyberSecurity Malaysia, 2014). Furthermore, the nationwide Malaysian survey, the National Health and Morbidity Survey of 2017 also showed that almost 30% of adolescents aged 13 to 17-years-old are internet addicts (IPH, 2017). In the United States, a study that was conducted by the Family Online Safety Institute among parents showed that around 48% of parents are worried about the amount of online usage among their children (FOSI, 2015). All the above evidence supported the need to retain this item to represent the issue of excessive online usage as a form of online threat.

5.4.2 Perceived Self-Efficacy and Perceived Response Efficacy

The majority of the items for the *perceived self-efficacy* and *perceived response efficacy* domains addressed a similar context, but the general statement structure was different in order to differentiate the two domains. The *perceived self-efficacy* domain focused on the parents' own confidence in carrying out a particular parental digital security practice. This was reflected in the statement structure of the items for this domain, which began with “I am confident…” or “I am comfortable…”. On the other hand, the *perceived response efficacy* domain measured the perception that parents had about the efficacy of the actions taken to actually keep their children safe online. This was reflected in the statement structure used for this domain, in which each statement ended with “…will keep him/her safe online.” The success of these statement structures in differentiating between these two domains was evident due to the clear discriminant validity that was found between the domains. The items were derived based on the responses that were gathered from Malaysian parents through the online survey to the question regarding the common parental digital security practices they performed and supported by the literature as well. Based on the parents’ responses and the literature, the items represented various digital security practices, namely, active mediation, restrictive mediation, supervision, monitoring and co-use.

The items that represented active mediation included items D2/E2 (“...in my knowledge on how to keep my child safe online...”) and item E1 (“Discussing online safety with my child...”). Active mediation, which is the action of sharing, commenting and providing advice can be reflected in the term “discuss” and requires “knowledge” for it to occur, as reflected in these two items. This type of practice was retained in the questionnaire because active mediation is highlighted as one of the most important practices to keep children safe online, particularly older children (CyberSecurity Malaysia, 2018; Nikken & Jansz, 2014; Willard, 2007). Hence, having items to reflect such practice was crucial to ensure that the final developed questionnaire was comprehensive enough to explore parental digital security practice.

Item D3/E3 (“...using the internet together...) reflected the co-use mediation technique. This technique is particularly important for parents with young children, as highlighted by the literature (CyberSecurity Malaysia, 2018; Livingstone & Haddon, 2008; Nikken & Schols, 2015; Willard, 2007). The guideline produced by CSM, for instance, recommends co-using for children under the age of 7 years old (CyberSecurity Malaysia, 2018). As co-use is an important digital security practice, the inclusion of this item in the questionnaire was justifiable.

Item D4/E4 ("…imposing internet rules...") and item D5/E5 ("…using filtering and monitoring software (parental control applications") were representative of the restrictive type of mediation. This type of mediation can be further defined as either imposing internet rules, which reflect behavioural restrictions, such as limiting usage time and the type of content allowed, or parental control applications, which reflect a technical restriction (Nikken & Jansz, 2014). Apart from being highlighted in guidelines (CyberSecurity Malaysia, 2018; Willard, 2007), this type of mediation is commonly used by parents, as shown in studies by Shin and Li (2017) involving parents in Singapore, by Nikken and Schols (2015) among parents in Holland, and by the Family Online Safety Institute among American parents (FOSI, 2015). These studies provide evidence that this type of practice is relevant among parents universally. Therefore, this practice needed to be included in the developed questionnaire.

Item D6/E6 ("…restricting my child to using the internet only when I am around") reflected the supervision mediation technique, which represents the action of parents only letting their children use the internet within the parents' vicinity. According to Shin and Li (2017), around 30% from a total of 586 Singaporean parents adopted this technique. Similarly, according to the Family Online Safety Institute study involving 586 American parents, 34% of them only allowed their children to use the internet in open space at home in their presence (FOSI, 2015). Guidelines on cyber parenting also emphasise the importance of supervision (CyberSecurity Malaysia, 2018; Willard, 2007) as a good parental digital security practice. Hence, having these items in the questionnaire ensured the comprehensiveness of the questionnaire, particularly in exploring the efficacy of this important mediation technique.

Item D7/E7 (…checking my child's online activities after my child has used the internet) reflected the monitoring mediation technique applied by parents. According to cyber parenting guidelines (CyberSecurity Malaysia, 2018; Willard, 2007), this type of mediation is important to curb online threats among children and adolescents. Hence it was important to include this item in the questionnaire in order to represent this mediation technique. According to the feedback from the online survey, this mediation technique is also relevant among parents, which supported the findings in the literature. For instance, the study by Shin and Li (2017), which was conducted in Singapore, showed 30% of parents applied this technique. Also, the study performed by the Family Online Safety Institute among American parents in 2015 highlighted that the monitoring technique was performed by 32% of respondents (FOSI, 2015). Hence, it was justifiable to include these items in the questionnaire because they not only reflected an important mediation technique, they were also relevant and popular among parents.

5.4.3 Perceived Response Cost

A total of seven items were retained to represent the domain *perceived response cost*. Similar to the *perceived response efficacy* and *perceived self-efficacy* domains, the items in this domain were designed to gauge parents' perceived cost of performing various parental digital security practices, namely, active mediation, restrictive mediation, supervision, monitoring and co-use.

Item F1 ("Discussing on online safety with my child is troublesome for me") and item F2 ("It takes a lot of effort to acquire appropriate knowledge on online safety") represented the cost of parents performing active mediation. Item F3 ("It takes a lot of effort to use the internet together with my child") reflected the perceived cost of co-use.

Item F4 (“Ensuring my child follows internet rules is troublesome for me”) represented the cost that parents perceived in performing behavioural restrictive mediation. Item F5 (“Ensuring filtering and monitoring software (parental control applications) are working can be troublesome for me”) was intended gauge the parents’ perception of the cost of performing technical restrictive mediation. The last two items, Item F6 (“Restricting my child to using the internet only when I am around requires a lot of effort”) and item F7 (“Checking my child’s online activities after he/she has used the internet requires a lot of effort”) represented the perceived cost of supervision and monitoring, respectively. As discussed previously, due to the importance that these different mediation techniques have in keeping children safe online, and the relevance of these practices to parents, it was necessary to retain all seven items in order to enhance the comprehensiveness of the questionnaire in terms of exploring the perceived cost level among parents regarding these important practices.

However, it was noted that two subdomains emerged based on the factor analysis of these items, namely, *perceived psychological cost* and *perceived tangible cost*. *Perceived psychological cost* was labelled as such because the items that loaded into this domain, namely, F1, F4, and F5, had a common keyword ‘troublesome’, which reflected the psychological state experienced in performing the actions described in the items. *Perceived tangible cost* was labelled as such because items F2, F3, F6, and F7 that loaded into this domain had a common keyword ‘effort’, which reflected the measurable costs such as time and physical actions. Both *perceived tangible cost* and *perceived psychological cost* were treated as formative components of *perceived response cost*. This was done based on theoretical argument and content validation. From the theoretical perspective, PMT shares certain similarities with another cognitive-based model, the HBM (Prentice-Dunn & Rogers, 1986). In explicating the HBM, Prentice-Dunn and Rogers (1986) explicitly mention that the component of response cost is equivalent to the

HBM's perceived barriers. Perceived barriers in the HBM have been defined as "Belief about the tangible and psychological costs of the advised action" (Glanz et al., 2008, p. 48). Hence, this definition supports the formation of *perceived response cost* by these two new domains. Additionally, the experts during the content validation phase were also in agreement that the items that made up the two domains represented *perceived response cost*. Hence, it was justifiable to label these two domains as stated above and to treat them as formative components of *perceived response cost*.

5.4.5 Perceived Maladaptive Reward

A total of four items were retained to represent the domain *perceived maladaptive reward*. Hence this domain was represented by the fewest items. Nevertheless, as argued by Ofcom (2013) and Marsh, Hau, Balla, and Grayson (1998), a minimum number of three items is needed in a multi-item scale to produce reliable findings in CFA. Hence, the use of four items to represent the domain was deemed sufficient. Two aspects of perceived maladaptive reward were explored based on the items, namely, utilising the internet and less mediation to aid parenting, and parents allowing their children to use the internet in order to facilitate the development of their children.

Item G2 ("Allowing my child to use the internet on his/her own will allow me to focus on my own interests") and item G3 ("By not imposing internet rules on my child, he/she will be happy") reflected the perceived advantage of the internet easing the parenting role. This aspect was derived from the online survey conducted among parents for this study. Similar findings have been reported in the literature as well. A study by Wartella, Rideout, Lauricella, and Connell (2013) involving 2000 American parents with children aged 8 years and below highlighted that 14% of parents would likely give a mobile device to their children to keep them occupied. The same study also revealed that about 17% of parents used a mobile device to calm a child, and as high a proportion as 44% would give it as a reward to their child. In the UK, a qualitative study commissioned by the Office of Communications (Ofcom) involving 85 parents through 10 family interviews and five focus group discussions revealed that allowing internet usage was done to avoid arguments or because the parents were busy (Britain, 2013). Hence, including these items to reflect this aspect of maladaptive reward was both relevant and justifiable.

Item G4 (“By not installing filtering and monitoring software (parental control applications), my child can use the internet freely”) and G5 (“By not checking my child’s online activities after he/she uses the internet, I am respecting his/her rights”) were related to utilising the internet for their child’s development. The study commissioned by Ofcom showed that some parents act less in terms of exercising parental control to ensure that their children ‘keep up’ with the latest trends, as well as to enhance their creativity (Britain, 2013). Also, a qualitative study by Shin (2015) involving parents with children aged 7–12 years old in Singapore revealed that some parents believe that placing less restriction on internet usage by their children allows their children to explore the internet and to become more resourceful in obtaining information. The same study also highlighted that the parents intend to exert less control as their child grew up in order, to respect their child’s autonomy (Shin, 2015). Moreover, the study for Ofcom revealed that among parents with children aged 12–15 years old, about 67% do not monitor their child’s usage as a sign of trust and to allow their children to learn to be responsible (Britain, 2013). Furthermore, a study based in the USA by the Family Online Safety Institute highlighted that 41% of parents do not monitor their children to show that they respect their children by demonstrating this act of trust in them (FOSI, 2015). From the above, it was clear that this aspect of maladaptive reward was universal and relevant to parents. Therefore, the items were retained in the questionnaire developed for this study.

5.4.6 Parental Digital Security Practice

In total, 11 items were included in the questionnaire to reflect actual parental digital security practices. The anchor question ("How often do you…?") and the anchor scale reflecting frequency (not at all to very often) were used and proven to be suitable to gauge the degree to which the parents performed these practices. Consistent with other domains such as domain D (*perceived self-efficacy*), E (*perceived response efficacy*), and F (*perceived response cost*), the items for *parental digital security practice* reflected the main online mediation techniques. The mediation techniques referred to in these items were active mediation, co-use, behavioural restriction, technical restriction, supervision and monitoring.

Items H1 ("Discuss on online safety with your child"), H2 ("Have conversations with your child on how to handle unknown people online"), H3 ("Discuss how to protect personal information online with your child") and H4 ("Have conversations on what to do if he/she is bullied or harassed online") represented active mediation technique. Item H5 ("Use the internet together with your child") reflected co-use. Item H6 ("Tell your child when/how long to use internet"), H7 ("Tell your child which websites/social networks he/she can visit") and H8 ("Tell your child what he/she can and cannot do online") reflected the behavioural restrictive mediation technique. Item H9 ("Ensure filtering and monitoring software (parental control applications) are present") represented the technical restriction technique applied by parents. Item H10 ("Restrict your child to using the internet only when you are present") focused on the supervision technique, and lastly, item H11 ("Check the websites that your child has visited") referred to monitoring of the child's online activities by parents. The inclusion of these items reflected comprehensive coverage of the types of mediation technique encompassed by this domain, which have been previously discussed in terms of their importance and relevance to the parents.

However, it was noted that two subdomains emerged based on the factor analysis of these items, namely, *discursive digital security practice* and *control digital security practice*. *Discursive digital security practice* was labelled as such because the items, namely, H1–H4, that loaded into this domain reflected active and discussion-based actions. *Control digital security practice* was labelled as such because the items loaded into this domain, namely, H5–H11, reflected a common theme of exertion of power and authority by parents in performing the actions. These two domains were treated as subdomains that formed the umbrella domain *parental digital security practice*. In the content validity assessment, the experts agreed that the items forming these two domains reflected digital security practice in general. The decision to group the items under these two subdomains of digital security practice is justifiable based on the literature. Wisniewski, Jia, Xu, Rosson, and Carroll (2015) described two types of parental mediation practice in respect of the social media usage of children, namely, direct mediation and active mediation. According to Wisniewski et al. (2015), direct mediation includes actions taken by parents to directly intervene in their children's social media usage through setting restrictions and applying rules. On the other hand, active mediation applies when parents take actions such as talking to their children and not attempting to directly control their children's social media usage (Wisniewski et al., 2015). These two types of digital security practice described by Wisniewski et al. (2015) are similar to the *discursive digital security* and *control digital security* practices in this study. In addition, a qualitative study by Meehan (2016) highlighted two types of parental mediation strategy for managing children's usage of internet-connected devices, namely, parental control mediation and parental experience. Parental control mediation includes 'covert and overt strategies and tactics', whereas parental experience is associated with the level of trust that parents place in their children and parental understanding of and information on internet-based devices (Meehan, 2016). Parental control mediation is similar to *control* *digital security practice* in this study, and 'parental experience' is reflected in *discursive digital security practice*. Hence, the formation of these two domains was justifiable based on the literature and the content validity assessment that was made by the expert panel.

5.5 Item Removal

A total of three items were deleted during the entire questionnaire development process. Each item that was deleted is discussed below in terms of the justification for its deletion.

Item H12 ("Check which friends or contacts your child adds to a social networking profile") was the first item to be deleted. This deletion occurred at the cognitive debriefing stage. According to Mullin et al. (2000), one of the aspects that determines the suitability of items and which is explored during cognitive debriefing is the retrieval process. This refers to the ability of respondents to relate a particular statement to their own experience (Mullin et al., 2000). As such, the inclusion of item H12 posed a problem with regards to the retrieval process among some of the respondents. This was because some of them did not have experience of having a child with a social networking profile. Hence, they were unable to answer this particular item. Furthermore, because the intended study population consisted of parents with children aged 18 years and below, this situation would have been replicated among a significant proportion of the respondents if this item were not deleted. This is because most social networking sites only allow individuals who are at least 13 years old to open an account (Facebook, 2019; Instagram, 2019). Hence, this item would not be applicable to some parents, particularly those with young children. Therefore, the deletion of this item was justifiable.

The second item that was deleted was item D1 ("I am confident in discussing on online safety with my child"). This deletion occurred at the test-retest stage. This item was deleted due to its low kappa value (0.38), which indicated poor temporal stability.

One of the critiques of the test-retest reliability assessment is its inability to distinguish whether the results are a reflection of the phenomena, the administration procedure or the measurement itself (DeVellis, 2017). A few strategies can be used (DeVellis, 2017) in order to ensure that the results of the test-retest are due to the measurement and not to administration methods or changes in the phenomena, In this study, firstly, the time gap interval between the first and repeated test was considered long enough to ensure that respondents would not be able to recall their answers exactly when answering the questionnaire the second time around, also known as the carryover effect. The time gap was also not too long, which ensured that there would not be time for any contextual changes to occur, such as the launching of mass media campaigns on online safety, that might influence the respondents' second set of answers. In this study, although the median time gap was around 2 weeks, as suggested by Streiner and Norman (2008), the wide range of time gap, which went up to almost 1 month in some cases, might have led to a lower kappa value for some items. A long time gap might have affected the stability of the results because the respondents might have reflected changes in the phenomena or domains of interest over time. Thus, a lower cut-off kappa value of 0.4 (Landis, 1977; Walter, 1998) was adopted to take into account the possibility of phenomena changes for some respondents, rather than the cut-off kappa value of 0.6 suggested by McHugh (2012). However, most of the respondents answered the questionnaire the second time within the suggested time gap. Therefore, it is safe to assume that the phenomena of interest were generally stable for most of the respondents.

In terms of the administration process, the administration of the repeated test was replicated in a manner that was as similar as possible to that of the first test. This included providing clear instructions about answering the questions and not allowing respondents to refer to their previous answers when answering the questionnaire for the second time.

Thus, any low value of kappa that fell below the threshold was most likely due to the item itself rather than changes in phenomena.

Based on the above argument, item D1 was removed because it had a comparatively low kappa value as compared to the other items in the instrument. This isolated low kappa value for D1 in comparison to that for the other items might have reflected a measurement error in the item rather than changes in the phenomena. This could have been due to the content of the item which might have seemed ambiguous to the respondents, and which, in turn, may have led to the respondents giving inconsistent answers over time because they interpreted the item differently upon repetition.

This item represented the confidence that parents have in discussing online issues with their children. The keyword for this item was identified as 'discussion'. In the cognitive debriefing stage, the word 'discussion' was interpreted as two-way communication by some parents, but it was also interpreted as one-way communication such as giving instructions or explaining a particular online safety measure. Hence, the findings from the cognitive debriefing had already highlighted the potential ambiguity in item D1 that could lead to inconsistency in responses. For instance, a parent might interpret the act of 'discussion' as referring to one-way communication when answering the first time. If they were comfortable with performing this type of communication, they would rate the item highly because they were highly confident during the first session. However, in the retest, the same parent might interpret the keyword 'discussion' as two-way communication which they were not confident in performing, hence they would rate the item lower than previously. This discrepancy would then be reflected as poor temporal stability in this item. This poor temporal stability would then affect the overall scoring for the domain. Hence the deletion of this item was justifiable. Moreover, because item D1 was one of seven reflective items that constituted the proposed domain *perceived self-efficacy*, it was considered that the removal of the item at this stage would not be detrimental because the domain would still be reflected adequately by the remaining six items.

The third and final item that was deleted was item G1 (“By not having discussions on online safety with my child, this will help in making him/ her more independent”). This deletion occurred during the EFA. The item was deleted due to a poor loading of less than 0.4, which indicated that the item did not fit in the *perceived maladaptive reward* domain. There are two plausible explanations for the low domain loading for this item. Firstly, this item might have been too ambiguous. In other words, the meaning of ‘independent’ in this item could have been too broadly interpreted because it could mean using the internet freely or referring to the child as independently figuring out how to keep him/herself safe online. As such, this ambiguity would have led to a poor loading for this item.

Secondly, the item itself may not have properly reflected the conceptualisation of maladaptive reward. The main concept in maladaptive reward is the preference of parents to not perform a protective action because the consequences are more appealing as compared those associated with making efforts to perform the action. It is plausible that the link between lack of discussion and the consequence of a child being independent was not well established. Hence, the item failed to reflect the domain maladaptive reward clearly as compared to the other items intended for this domain. Also, because there would be an adequate number of remaining items to represent this domain after the deletion of item G1, this further justified the deletion of the item.

5.6 Questionnaire Format

When writing the items, two aspects were taken into consideration, namely, the number of items and the complexity of the items. In this study, the highest number of items in a domain was 11 (for *parental digital security practice*) and the lowest was four (for *perceived maladaptive reward*). The high number of items generated for the domains at this stage was in line with the recommendations in the literature (Boateng et al., 2018; Holmbeck & Devine, 2009; DeVellis, 2017). This was done because a higher number of items facilitates the determination of the reliability of the items for their respective domains. In addition, the level of reading difficulty of all the items was aimed at the 10– to 12 years old reading level, as recommended by DeVellis (2017). This was achieved by limiting the number of words per item to a maximum of 20 words, as outlined by Fry (1977) and DeVellis (2017). Finally, any confusing sentence structures, such as double-barrelled items, were also avoided. For example, in the item C6 during item development phase, the word "friends" was dropped from the original statement "A child exchanges sexual messages or/and images to their friends or/ and other people online" to become "A child exchanges sexual messages or/and images with other people online". Based on the discussion with experts, the term "other people" should encompass friends and does not required to be separated. In addition, this is to avoid lengthy structure of the item, and prevent double barrelled interpretation on the category of people they interacted with if the term "friends" and "other people" were retained together.

For the measurement of the items, this study employed a five-point Likert scale, using numerical labelling, also known as end-point labelling. This measurement format is discussed in the following paragraphs based on two aspects, namely, the number of response categories and the labelling of the response options.

In regard to the Likert scale, there are debates in the literature on the number of response categories that should be included. This study used a five-point Likert scale for the following reasons. Firstly, the study intended to analyse the data using SEM, which fundamentally estimates the linear relations using correlations. As such, the literature suggests that a rating scale should have at least five response options for the data to be approximated well using linear models and to be treated as continuous data (Bollen &

Barb, 1981; Rhemtulla, Brosseau-Liard, & Savalei, 2012; Srinivasan & Basu, 1989; Weijters, Cabooter, & Schillewaert, 2010). Secondly, the target population was considered when deciding on the number of response categories. An ideal number of responses should be appropriate enough for the respondents to differentiate between the response categories, but not long enough to be taxing cognitively because this could lead to measurement error (Viswanathan, Sudman, & Johnson, 2004). As such, Weijters et al. (2010) suggest that a five-point Likert scale is suitable for the general population, based on cognitive ability and experience with answering questionnaires. Therefore, based on these two aspects, a five-point Likert scale was chosen for this study.

Generally, there are two types of labelling in a Likert-scale response format, namely, fully labelled points (verbal labelling) and end-point labelling (numerical labelling). It has been argued that fully labelled points are preferable because each of the points is explicitly determined, which leads to a similar interpretation among the respondents (Dillman, Smyth, & Christian, 2014), which, in turn, reduces measurement error. It has also been stated that fully labelled points appear to reduce response bias, and particularly extreme response styles (Weijters et al., 2010).

However, Darbyshire and McDonald (2004) state that end-point labelling is appropriate if the scale addresses common categories and is understandable by the respondents based on the end-point labels. In addition, Krosnick and Fabrigar (1997) argue in favour of end-point labelling because it is cognitively less demanding, easier to interpret, and thus leads to less measurement error.

On the other hand, a few studies have highlighted that there is no difference in variance, mean or reliability (Chang, 1997; Huck & Jacko, 1974; Lau, 2008) between fully labelled and end-point labelled scales. This indicates that these two labelling styles exhibit little difference in terms of producing response bias and measurement error.

Moreover, Moors, Kieruj, and Vermunt (2014) highlight that extreme response styles can be present in both labelling formats, which indicates that the occurrence of this response bias is unavoidable regardless of labelling style. Furthermore, Weijters et al. (2010) state that end-point labelling is the best choice for SEM because when respondents use this format it conforms to linear models.

Hence, based on the above findings, this study adopted the end-point labelling style, on the following three premises: (1), end-point labels are cognitively less demanding, (2) the categories used as anchors are commonly understood so that the middle unlabelled points can be interpreted correctly, and (3) the responses produced are suitable for SEM analysis.

In summary, the final version of the developed questionnaire contained items that were relevant and important in reflecting their respective domains. The questionnaire format in terms of the number of items, complexity, type of scale and labelling was also based on best practices and established evidence. This ensured that the questionnaire was valid and reliable, and that the findings obtained in the field survey in terms of the relationship among the domains, which is discussed in the next section, would be valid as well.

5.7 Model Discussion

The model developed in this study showed that out of the six components of PMT, only three components were significant predictors of parental digital security practice. Two of these three significant components, namely, *perceived self-efficacy* and *perceived response efficacy*, are components in coping appraisal. The other significant component was *perceived maladaptive reward*, which is a component in threat appraisal. *Perceived self-efficacy* appeared to have the highest effect size, followed by *perceived response efficacy* and *perceived maladaptive reward*. The remaining two components of threat appraisal, namely, *perceived susceptibility* and *perceived severity* were not significant predictors of *parental digital security practice*, and nor was *perceived response cost*, which was the remaining component in coping appraisal.

Overall, these findings are not consistent with the proposed PMT model because *perceived susceptibility, perceived severity* and *perceived response cost* were not significant in influencing parental digital security practice. However, the findings are consistent with those reported in several studies. Milne et al. (2000), in a meta-analysis of 21 studies using PMT, highlighted that coping appraisal components, particularly *perceived self-efficacy*, most often have the most significant association with intention to practice, with *perceived susceptibility* having the least. Floyd, Prentice-Dunn, and Rogers (2000) performed a meta-analysis on 65 PMT-based studies and concluded that coping appraisal components have more influence than threat appraisal components, with *self-efficacy* having the highest impact. More recently, Ruiter, Kessels, Peters, and Kok (2014) conducted a review of reviews on fear appeal models and also concluded that strengthening *self-efficacy* and *response efficacy* is important for individuals to adopt protective behaviours.

The subsequent subsections dissect each of the components of PMT in the context of this study, and attempt to explain the phenomena of interest to this study in greater detail.

5.7.1 Perceived Susceptibility

This study showed that the *perceived susceptibility* component was not significant in predicting parental digital security practice. The literature has produced mixed findings in relation to *perceived susceptibility* and parental protective behaviour. Boniel-Nissim, Efrati, and Dolev-Cohen (2019) revealed that *perceived susceptibility* is not a significant predictor of parental mediation of children’s exposure to online pornography. Hwang et al. (2017) highlighted that *perceived susceptibility* is not a significant predictor of parental restrictive mediation of smartphone usage among children. In addition, the same study showed that *perceived susceptibility* has a significant negative relationship with active mediation of smartphone usage among children (Hwang et al., 2017). One plausible explanation for the mixed results is that the studies focused on a specific threat, population of interest and behaviour.

There are a few reasons for the insignificant relationship between *perceived susceptibility* and *parental digital security practice* that was found in this study. One possible explanation is that compared to the other domains, *perceived susceptibility* may not be as crucial a factor in influencing the adoption of parental digital security practice. Parents may feel that their children are susceptible to online threats, but they need to acquire the necessary skills and knowledge in order to carry out protective actions to safeguard their children online.

In this study, the significant relationship between *perceived self-efficacy* and *parental digital security practice* and between *perceived response efficacy* and *parental digital security practice* seem to support this notion. Parents' confidence in the benefits of digital security practice and their capability of applying it appear to be more important regardless of the parents' level of perception of online threats. With a high level of efficacy in place, a low level of susceptibility will trigger action because the threats are perceived to be easy to counter. Similarly, a high level of susceptibility will activate actions to control the danger provided that a high level of efficacy is in place.

Secondly, the insignificant relationship between *perceived susceptibility* and *parental digital security practice* may also the result of parents having adopted digital security practice and therefore no longer feeling that their children are susceptible to threats online. This is reflected in the study's findings, in which *perceived susceptibility* has a relatively low mean score (mean 2.6) as compared to *discursive digital practice* (mean 3.4) and *control digital practice* (mean 3.8). However, it was not possible to determine whether *perceived susceptibility* led to protective behaviour or vice versa because of the cross-sectional nature of this study. This highlights one of the shortcomings of this study, namely, that it was not able to determine any causal relationships.

Several moderators that are not explored in this study might explain the insignificant relationship between *perceived susceptibility* and *parental digital security practice*. Firstly, *perceived susceptibility* may appear insignificant due to the assumption that parents have a similar level of awareness of the threats, to begin with. Weinstein (1998) argued that this type of static conceptualisation can be misguided. It is more likely that parents' awareness of the threats differs, hence their perception of susceptibility might be different as well. As such, this might lead to mixed reflections in terms of the degree of perceived susceptibility in the answers given. This has the potential to lead to an underestimation of the relationship between *perceived susceptibility* and *parental digital security practice*. Hence, parents' level of awareness of online threats could be a potential moderator that could be included in further studies.

Secondly, parenting style might moderate the relationship between *perceived susceptibility* and *parental digital security practice*. Hwang et al. (2017), for instance, highlighted that authoritative, authoritarian and permissive parenting have different influences on perceived susceptibility and the types of parenting mediation employed for smartphone use among children. This implies that parenting style may also play a moderating role between *perceived susceptibility* and *digital security practice*. Different parenting styles would influence the relationship between the two variables in different ways, which might lead to a potential underestimation of the significance of the relationship between *perceived susceptibility* and *parental digital security practice.*

As this study aimed to maintain the parsimony of the model explored and focused only on the PMT components, a potential third variable, such as awareness of threats and parenting style, was not included. Hence, these domains will need to be considered in future studies because doing so might help in explaining the relationship between *perceived susceptibility* and *parental digital security practice* further.

5.7.2 Perceived Severity

Perceived severity was found to be an insignificant factor in practising parental digital security. This finding contradicts the PMT concepts and several studies in the literature. For instance, Hwang et al. (2017) and Hwang and Jeong (2015) found that perceived severity influences parents' mediation of mobile use among their children. Moreover, Boniel-Nissim et al. (2019) showed that perceived severity influences parental mediation of online pornography exposure among their children. However, the findings of this study are consistent with two review studies. A meta-analysis of PMT-based studies by Milne et al. (2000) revealed that perceived severity has the weakest association with intention to perform protective behaviours as compared to other PMT components. Similarly, Ruiter et al. (2014) in a review of reviews of PMT-based studies highlighted that perceived severity has the least influence in motivating individuals to adopt protective behaviour.

There seem to be a few possible reasons that may have contributed to the study's finding regarding the insignificant relationship between *perceived severity* and *parental digital security practice*. One possible explanation is that the seriousness of online threats to their children is already widely accepted by parents. As such, ceiling effects may already have been reached and may have reduced the influence of perceived severity on adopting parental digital security practices. Extending this argument further, it could be argued that the perceived severity of online threats did not generate enough motivation among parents to perform actual digital security practice. This may be due to the nature of the threats which are not physically visible and which therefore do not impel them to take action. It could also be argued that regardless of the level of perceived severity, actions can only be taken if parents are capable of taking them, which is in line with the significant relationship between both *perceived self-efficacy* and *perceived response efficacy* and *parental digital security practice* that was found in this study.

Furthermore, the scope and level of severity of the threat as interpreted by parents may explain the nature of the relationship between *perceived severity* and *parental digital security practice* in this study. The concept of severity can be multidimensional, which may include consequences such as emotional, physical, relationship, career and financial. As such, each parent may have interpreted the concept of severity differently when answering the questionnaire, and to a different degree as well. This broad concept of severity may therefore have attenuated the relationship between perceived severity and protective action in this study. The broad context of severity has been identified as an issue in the literature as highlighted by Milne et al. (2000), and it therefore needs to be explored further in future studies.

Lastly, perceptions of severity can also be influenced by whether parents have already engaged in actions that are likely to reduce the severity of online threats to their children. Parents who are well versed in digital security practice may perceive the severity of online threats to their children as low and vice versa. The different degree of severity as perceived according to the protective actions taken may therefore lead to an underestimation of the relationship between *perceived severity* and *parental digital security practice*. As this study captured information on *perceived severity* and *parental digital security practice* at the same time, this issue may have contributed to the nature of the relationship between these two variables. Future longitudinal or experimental studies may be able to address this issue, and a clearer causal effect relationship can then be established.

5.7.3 Perceived Response Cost

Perceived response cost appeared to be insignificant in predicting *parental digital security practice*. This study finding seems to be contradiction with the findings reported in the literature. The two meta-analyses on PMT-based studies (Floyd et al., 2000; Milne et al., 2000) highlighted that response cost has a significant negative relationship with both the performance and the intention to perform protective behaviours. One possible reason for this contradictory finding is the context that this study examined, particularly with regard to whom the behaviour is intended to benefit. Most of the studies that support the negative relationship involve self-referencing of the individuals in taking up protective behaviour. In contrast, in this study, protective behaviour was referenced to the child's online safety. As such, the nature of weighing the cost/benefit of adopting protective behaviour might differ when applying this process to oneself versus someone under one's care.

However, only a limited number of studies were available that investigated the *perceived response cost* of protective behaviours among parents. For instance, Hwang et al. (2017), Beirens et al. (2007), Boniel-Nissim et al. (2019), and Nathanson (2001) did not include *perceived response cost* in their PMT-based studies involving parents. One possible reason behind the limited inclusion of *perceived response cost* in parent-based studies is the assumption that parents always perform protective behaviours towards their children, irrespective of the costs these behaviours might incur. Hence the inclusion of *perceived response cost* might be counterintuitive in nature. However, the lack of empirical evidence to support this possible notion warranted that this study examines the relationship between *perceived response cost* and parental protective behaviour, particularly in the context of digital security practice. The insignificant relationship found in this study seems to support the notion that parents' protective behaviour towards their children is not influenced by the cost it might incur because the obligation and duty of parents to protect their children outweighed the cost.

Other possible reasons that might explain the insignificant relationship include parenting style, which might potentially moderate the relationship. Parents who practise different styles of parenting might interpret the cost/benefit to their child differently. Authoritative parents, for instance, may not be too influenced by the cost of protecting their children because they are more responsive to their children's needs. Neglectful parents, on the other hand, may be highly influenced by the cost because they have low responsive to their children's safety. Hence, the different degrees of interpretation of the cost/benefit by parents might lead to an underestimation of the relationship between *perceived response cost* and *parental digital security practice* when this moderator is not taken into account.

Another reason for the insignificant relationship between *perceived response cost* and *parental digital security practice* is the high level of efficacy parents had in this study. *Perceived tangible cost* and *perceived psychological cost* had relatively low scores as compared to the score for *perceived self-efficacy*. As the parents in this study were confident and able to protect their children online, they may not have found digital security practice to be troublesome and may not have found that it required a lot of effort. Hence, the *perceived response cost* score was low and did not influence *parental digital security practice* much. Similarly, the motivation to protect their children, as reflected by *perceived response efficacy* may have led to the effect of the *perceived response cost* being insignificant. The findings in this study seem to support this argument. Again, *perceived tangible cost* and *perceived psychological cost* had a relatively low score as compared to the score for *perceived response efficacy*. In addition, in contrast to *perceived response cost*, *perceived response efficacy* was significant in influencing *parental digital security practice*.

5.7.4 Perceived Self-Efficacy

Perceived self-efficacy was found to have a significant positive relationship with *parental digital security practice*, and had the highest effect size among the other components of PMT considered in this study. This finding is consistent with the literature (Floyd et al., 2000; Milne et al., 2000; Ruiter et al., 2014). The more confident parents are in their capabilities of performing parental digital security practice, the more likely they will adopt such practices. This result indicates that parents' judgement about their ability has a strong influence on their performance of the protective action to keep their children safe online. *Perceived self-efficacy* has also been shown to be an important predictor in other fear appeals models, such as the HBM (Rosenstock, 1974) and the extended parallel process model (Witte, 1993). In explaining this relationship further, Maddux and Rogers (1983) highlighted that sources of information are important precursors for the PMT model. Thus, prior knowledge of protective measures among parents could amplify the *perceived self-efficacy*, thereby resulting in its significance in predicting *parental digital security practice*. The significance of this relationship further emphasises the need to provide accessible information to parents on how to perform parental digital security practice to protect their children.

5.7.5 Perceived Response Efficacy

Perceived response efficacy was found to be a positive and significant predictor of *parental digital security practice*. This finding is consistent with the majority of the literature, as highlighted in a few meta-analyses and reviews of PMT-based studies (Floyd et al., 2000; Milne et al., 2000; Ruiter et al., 2014) which showed that parents who perceive protective measures to be effective in keeping their children safe online will more likely perform these measures. The relatively significant relationship between both *perceived response efficacy* and *perceived self-efficacy* and *parental digital security practice* in this study also indicates that coping appraisal has a strong influence on *parental digital security practice*. Again, this is consistent with the literature (Ruiter et al., 2014) and supports other fear appeal theories such as the HBM (Rosenstock, 1974) and the extended parallel process model (Witte, 1994). Parents who have high confidence in their ability to perform protective measures and high belief that the measures are effective in keeping their children safe online will likely perform these measures. Similar to the argument explaining the influence of *perceived self-efficacy*, having prior knowledge of the benefits of protective measures may influence parents' *perceived response efficacy* and thereby lead to its significant relationship with *parental digital security practice*.

5.7.6 Perceived Maladaptive Reward

Perceived maladaptive reward was a significant factor in influencing *parental digital security practice*. The negative relationship between *perceived maladaptive reward* and *parental digital security practice* identified by this study is consistent with the proposed PMT model and the literature. Floyd et al. (2000) in their meta-analysis of PMT-based studies discovered that maladaptive reward has a significant negative relationship with protective behaviour. In this study, the higher the reward for not practising digital security practice, the less digital security practice performed by parents to protect their children.

However, only a very limited number of PMT-based studies considered including the maladaptive reward component. Milne et al. (2000) in their meta-analysis of 21 PMT-based studies revealed that only one study included the maladaptive reward variable. The same pattern can be seen in the systematic review conducted for this study, in which only four studies included this domain. One of the reasons that have been suggested for not considering this component is the difficulty in distinguishing between the reward value of risk behaviour and the cost of protective behaviour (Conner & Norman, 2005). However, this study was able to clearly distinguish between *perceived response cost* and *perceived maladaptive reward*, based on the distinctive difference between them in terms of the significance and direction of the relationship towards *parental digital security practice*.

In clarifying the distinction between these two components, *perceived response cost* addresses the convenience level of adopting protective behaviour. For example, parents who might think that installing parental monitoring software is troublesome or takes a lot of effort, hypothetically will not adopt the behaviour. *Perceived maladaptive reward*, on the other hand, addresses the alternative reward that one might obtain for not adopting a particular protective behaviour. For example, parents who feel that not installing parental monitoring software will lead to their child being able to use the internet freely (alternative maladaptive reward), will tend not to install it at the expense of keeping their child safe (intended adaptive reward). Hence, the maladaptive reward is a reflection of a prioritisation process, in which parents make decision to prioritise maladaptive reward over adaptive reward or vice versa. This study thus reflects the importance of addressing the issue of maladaptive reward by creating awareness and helping to make children's online safety a top priority among parents.

5.7.7 Overall Model

The model developed in this study was shown to have the ability to explain 34% of *parental digital security practice*, with *perceived maladaptive reward, perceived self-efficacy* and *perceived response efficacy* being significant predictors of this protective behaviour. The final model is shown in Figure 5.4.

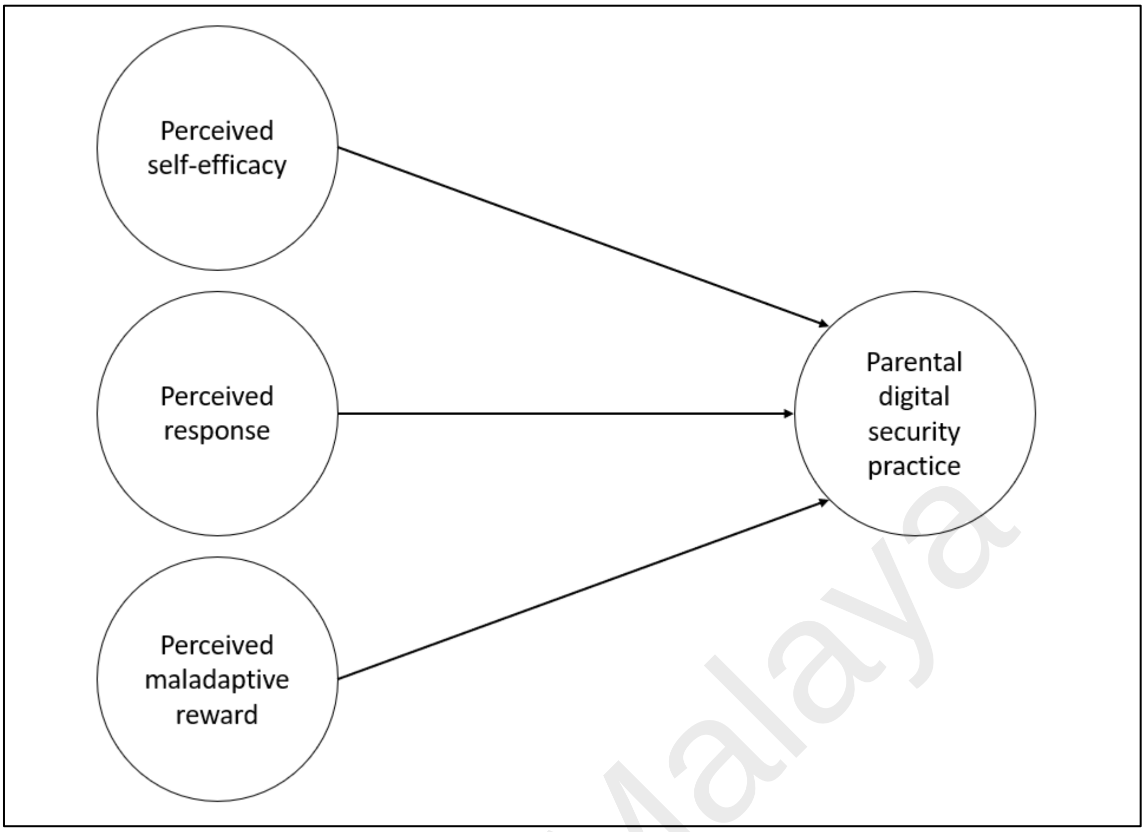
Perceived self-efficacy
Perceived response
Perceived maladaptive reward
Parental digital security practice

Figure 5.4: Final model of the study

A few points should be noted in relation to this model. Firstly, the limited explanatory power of this model in terms of predicting *parental digital security practice* highlights the complexity of this behaviour. As this model only focused on the intrapersonal cognitive processes using the fear appeals angle, other factors might influence digital security practice and explain the remaining 66% of the variation. For example, a meta-analysis by Sommestad (2015) has highlighted the potential importance of the domain *perceived norm* adapted from Theory of Planned Behaviour (Ajzen, 1985) in explaining protective behaviours. Expanding beyond the intrapersonal factors, if the socioecological model (Bronfenbrenner, 1979) is applied to explain such behaviour (see Figure 5.5), it becomes clear that other factors also influence a person's protective behaviour, including interpersonal, institutional, community and policy factors. This include the role of family support, the norm in the community, and policies such as restriction on surfing adult materials including pornography in a particular region. Potentially, introducing these factors into the model would enhance the explanatory power of the model.

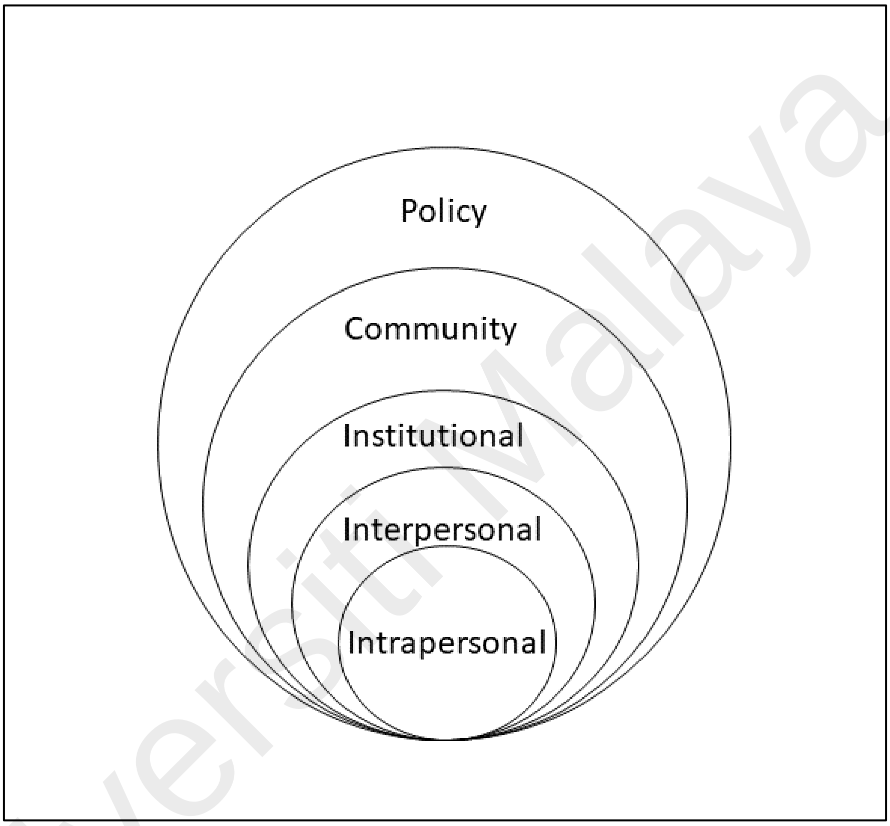

Figure 5.5: Components of socioecological, model

Adapted from: Bronfenbrenner (1979). Ecological models of human development. *Readings on the development of children, 2*(1), 37-43.

If we now zoom in on the components of this study's model, the coping appraisal components, particularly *perceived self-efficacy* and *perceived response efficacy*, appear to have a higher influence on *parental digital security practice* as compared to the threat appraisal components, namely, *perceived susceptibility* and *perceived severity*. Thus, emphasis should be placed on providing knowledge to parents on how to perform digital security practice. Having such knowledge will improve their self-efficacy and response efficacy, and thereby lead to the practice of parental digital security. However, the insignificant relationship between the threat appraisal components and *parental digital security practice* does not mean that these components should be dismissed. Rather, further evaluation is needed in order to understand this phenomenon, and such work should include possible third variables that may influence the magnitude of the relationships in the model. Since relationships are only considered significant if the components show a linear relationship between them, the presence of insignificant relationships may imply that these relationships are not linear and need to be investigated further.

The exploration of *perceived maladaptive reward* in this study highlighted that this factor was not widely examined in the literature. The significance of the relationship between *perceived maladaptive reward* and *parental digital security practice* showed the importance of this factor in predicting *parental digital security practice*. The significant negative relationship of *perceived maladaptive reward* and *parental digital security practice* indicates that parents' degree of priority in performing online protective behaviour is a crucial factor. It is therefore apparent that influencing parents to believe that parental digital security practice should be their top priority is paramount and that this issue needs to be addressed.

5.8 Public Health Implications

This study is an important public health research because the findings are correlated with improving the health of children and adolescents. The developed tool will help to empower parents in various ways. Firstly, the tool can be used to understand parental digital security practice needs. Secondly, the tool will help to direct strategies in improving parental digital security practice. Importantly, these findings will help to tailor such strategies to fit the local context. As such, cyber parenting strategies can be expanded further by not just focusing on how parents need to raise their children in a digital world. Rather, the findings potentially highlight the need to educate the parents themselves as well on good digital practices such as digital security because this will influence the effectiveness of cyber parenting. All these will bring parents closer to becoming good digital citizens and empowered. As parents become more empowered and become good digital citizens, the poor online behaviour of children and adolescents can be curbed. Eventually, the improvement in online behaviour among children and adolescents will help to produce good digital citizens in this population. This will help to reduce the occurrence of online issues such as cyberbullying, sexting, and internet addiction. As such, the health implications arising from these issues can be improved as well, leading to an overall improvement in child and adolescent health.

In a wider context, this study will contribute to the nation of Malaysia in achieving some of the targets set in the sustainable development goals (SDGs). Specifically, SDG 4, which focuses on "ensuring inclusive and equitable quality education and promoting lifelong learning opportunities for all" (United Nations, 2015, p. 19). One of the targets in SDG 4 is to provide "safe, non-violent, inclusive and effective learning environments for all", by stating internet and computer usage for pedagogical purposes as one of the strategies in achieving the target (United Nations, 2015, p. 20). Malaysia has responded by making a statement in its National Education Blueprint 2015–2025 on the provision of internet broadband in schools (MoE Malaysia, 2013). As the nation gears up to provide access to the internet and computers for learning purposes in the education system, more children and adolescents will be exposed to the internet and its inherent threats. It is thus important to ensure that children, adolescents, and parents are good digital citizens so that this SDG target can be upheld without negative consequences. This study will help to achieve this by providing the trigger for producing good digital citizens, empowered parents and children.

In addition, target 2 of SDG 16 focuses on "Ending abuse, exploitation, trafficking, and all forms of violence against and torture or children" (United Nations, 2015, p. 28). This study will help to mitigate the risks of the internet among children and adolescents through empowering their parents. As such, cyber threats such as cyberbullying and sexual grooming can be addressed, hence helping the nation in achieving this target.

Consequently, recognising the significance of this study in the public health domain, a few strategies were adopted to ensure that the study products and findings will be utilised. These strategies are described in the subsequent sections.

5.9 Utilisation of Study Findings through Knowledge Translation

The utilisation of this study was enhanced by adopting the integrated knowledge translation approach (Graham et al., 2006). This section dissects the processes involved in the knowledge translation approach that was used in facilitating the utilisation of the study findings.

5.9.1 Knowledge Translation Overview

Knowledge translation is a broad concept that focuses on turning knowledge into action (Graham et al., 2006). One of the common approaches in knowledge translation is known as the integrated knowledge translation approach (Kothari & Wathen, 2013). This approach has been defined as an "ongoing relationship between researchers and knowledge users for the purpose of engaging in a mutually beneficial research project or programme of research to support knowledge users' activities" (Gagliardi, Berta, Kothari, Boyko, & Urquhart, 2015, p. 1). Regardless of the approaches used, Graham et al. (2006) have proposed a framework, known as the knowledge to action (KTA) cycle for guiding the process of knowledge translation to come to fruition. As shown in Figure 5.6, the KTA cycle consists of two major components, namely, knowledge creation and action cycle (Graham et al., 2006). All the stages in the KTA cycle are iterative and dynamic, in the sense that they can occur sequentially or simultaneously (Graham et al., 2006).

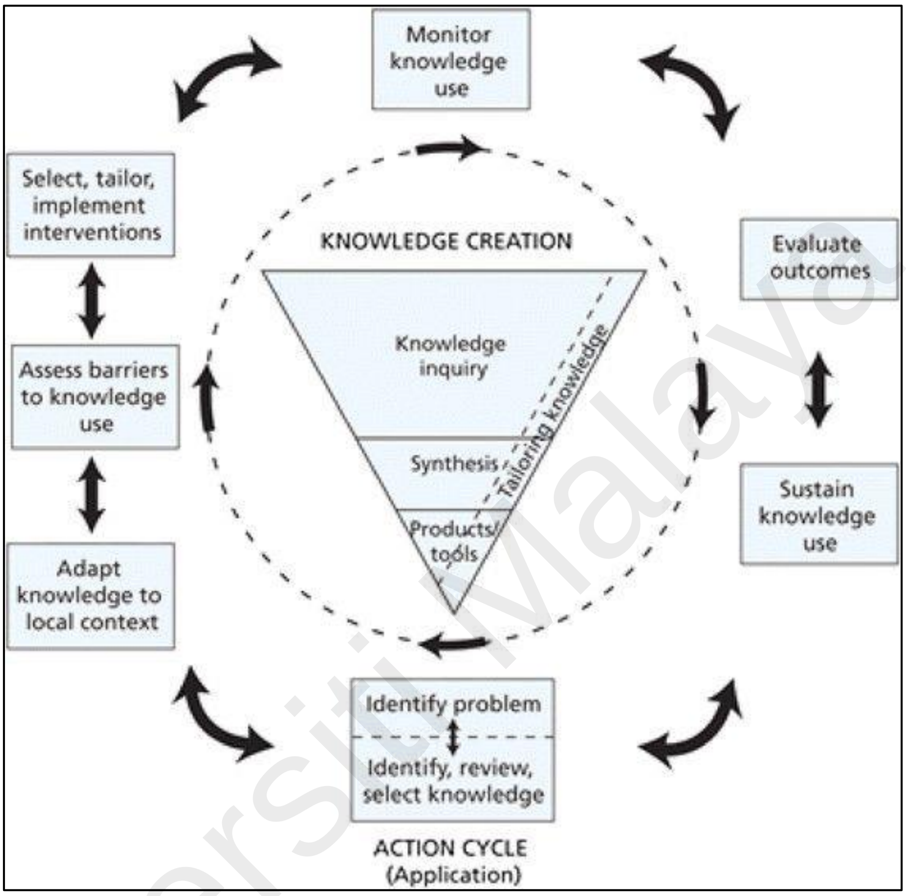
Monitor knowledge use
Select, tailor, implement interventions
Evaluate outcomes
KNOWLEDGE CREATION
Knowledge inquiry
Tailoring knowledge
Synthesis
Products/tools
Assess barriers to knowledge use
Sustain knowledge use
Adapt knowledge to local context
Identify problem
Identify, review, select knowledge
ACTION CYCLE (Application)

Figure 5.6: Knowledge to Action Cycle

Adopted from Graham, I. D., Logan, J., Harrison, M. B., Straus, S. E., Tetroe, J., Caswell, W., & Robinson, N. (2006). Lost in knowledge translation: time for a map? *Journal of continuing education in the health professions, 26*(1), 13-24.

The knowledge creation component involves tailoring and presenting the knowledge to knowledge users through either primary studies (knowledge inquiry), secondary studies (synthesis) or tools such as established guidelines (products/tools), or a combination of all three (Graham et al., 2006). Hence knowledge creation acts as an impetus for further action to be performed in the action cycle.

In the action cycle, the process of identifying the problem generally utilises the knowledge created and involves discussions with knowledge users (Graham et al., 2006). At this stage, gaps are identified and relevant research to address the gaps might be commissioned (Graham et al., 2006). After the problem and research have been identified, steps are taken to ensure that the knowledge in the form of research findings can be adapted in the local context (Graham et al., 2006). The barriers to utilising the research findings are also assessed (Graham et al., 2006). Then, after refinements have been made, measures to utilise the findings are taken (Graham et al., 2006). Following this, monitoring and evaluation of the knowledge is conducted, and strategies to sustain the knowledge produced are examined (Graham et al., 2006).

In this study, by adopting the integrated knowledge translation approach, all the steps in the KTA cycle involved the knowledge users, namely, CSM as the main stakeholders (see Appendix N). The description of this study's integrated knowledge translation process is described in the following subsections, as guided by the framework for the KTA cycle.

5.9.2 Knowledge Creation and Identifying Problem

The process of knowledge creation and problem identification occurred simultaneously in this study. As it was intended that this study would be conducted in an integrated knowledge translation manner, the identification of knowledge users as collaborators was crucial. Therefore, the researcher approached CSM as a potential research partner and collaborator. This engagement was done 6 months prior to actually conducting the study. Throughout the 6 months, multiple engagements through meetings and discussions were conducted to identify the main problem that was useful for both parties and the level of involvement by CSM as a research partner in this study.

As elaborated in Chapter One, the issue that was of interest and relevant to both CSM and the public health community was parental behaviour in performing digital security practices to protect their children and the need to gain a deeper understanding of this complex issue. The conceptual framework that the researcher proposed to use to address this issue was endorsed by CSM, as well as other experts. Upon refining the identified issue further, it was also agreed that having a measurement tool to assess the issue in the Malaysian context was very much needed and that this should inform the direction of the study. At this stage, a systematic review was conducted as a form of knowledge creation. The systematic review further clarified the direction of the study and the findings from the review were used in the development of the measurement scale.

Also, in line with the integrated knowledge translation approach (Graham et al., 2006), the level of involvement by CSM was discussed at this stage as well. It was made clear and agreed upon that CSM would be involved throughout all the stages of the KTA cycle in the study. It was agreed that they would provide expert input for refining the measurement tool and the research findings. It was also agreed that they would provide support in terms of resources and channels for data collection, as well as measures to utilise the questionnaire and findings after the study had been completed.

5.9.3 Adaptation of Knowledge to Local Context and Assessment of Barriers

When ensuring that the measurement tool would be suitable to the local context, inputs from CSM as the main knowledge users as well as those of other local experts were taken into account. The assessment of the suitability of the tool to the local context was primarily conducted in the item generation stage. The items that were generated were based on inputs from Malaysian parents, CSM and other local experts in order to maintain the questionnaire's relevance in the Malaysian setting.

Ensuring the comprehensibility of the questionnaire for a diverse audience and the feasibility of administering the questionnaire are examples of the barriers that were identified by CSM. Hence the development of a dual-language questionnaire was seen as important in reaching out to the general population in Malaysia where it is to be utilised. CyberSecurity Malaysia also provided input in the translation process through a representative on the committee involved in assessing the forwards-backwards translation of the questionnaire content. It was also highlighted by CSM that having a concise questionnaire was also important for it to have the potential to be embedded in CSM's programmes on cyber parenting. An appropriate length of questionnaire was seen to be crucial in getting parents' participation in answering the questionnaire when it is utilised by CSM. Thus, constant feedback was given to CSM in the questionnaire development process on the number of items produced and the relevance of the items retained in the questionnaire.

5.9.4 Implementation of Knowledge

Broadly speaking, this study produced two research products, namely, the parental digital security questionnaire and the factors that influence parental digital security practice. The parental digital security questionnaire was utilised by CSM in several forms. Firstly, the questionnaire was embedded in their cyber parenting talks and seminars under their existing programme known as Cyber Security Awareness Talks (CSAT). During CSAT sessions, CSM members would ask participants to answer the questionnaire. By doing so, they were able to gauge the participants' needs in respect of cyber parenting, and thus guide CSM members in tailoring the delivery of their cyber parenting talks. Secondly, the questionnaire was also embedded in CSM's cyber parenting national guideline (CSM, 2019), which is distributed nationwide. The questionnaire serves as a self-assessment that can be done by parents to help them to understand their digital security practice pattern and to improve on their digital security practice based on the guidelines provided in the booklet.

Based on the model developed in this study, the findings that showed that *perceived self-efficacy*, *perceived response efficacy* and *perceived maladaptive reward* influence *parental digital security practice* were highlighted to CSM members. The findings that *perceived susceptibility*, *perceived severity* and *perceived response cost* are not influential in digital security practice were highlighted as well. Based on these findings, the strategy employed by CSM when delivering cyber parenting awareness sessions has been modified. Specifically, emphasis has been put on providing parents with information and knowledge on how to protect their children and keep them safe online, in addition to highlighting the consequences of not keeping their children safe online.

5.9.5 Monitoring and Evaluation of Knowledge Use

The process of monitoring and evaluating knowledge use utilises the existing mechanisms of CSM. For instance, the monitoring of the usage of the questionnaire by CSM members is performed through an existing dashboard that monitors CSAT activities, including frequency of cyber parenting talks, the number of participants, organisations involved and geographical regions covered. The number of downloads of the cyber parenting booklet can also be used as a monitoring mechanism in reaching out to parents.

In terms of the evaluation of knowledge use, feedback from participants and the demand pattern for cyber parenting sessions under CSAT can be used to gauge the output from the questionnaire's utilisation. In addition, the demand pattern for the cyber parenting booklet can be used indirectly to evaluate the output of the questionnaire because this reflects the level of awareness among parents.

However, the outcome and impact of the study findings may be more difficult to evaluate. One potential measure would be to assess the number of cybercrime cases reported. Although not exclusively due to the study's utilisation, the cybercrimes trend would indicate the effectiveness of the cyber parenting awareness measures to a certain extent and thus, indirectly, the contribution made by the utilisation of the study.

5.9.6 Sustainability of Knowledge Use

The embedment of the questionnaire in CSM's established programmes and tools such as CSAT and cyber parenting booklets strengthens the sustainability of the knowledge use by parents and by CSM as knowledge users. Moreover, the collaborative effort with CSM also provides a direct platform for the researcher to promote the study's findings and questionnaire. For instance, CSM invited the researcher to be a panellist at a cyber wellness seminar organised by CSM in February 2019, which was attended by academicians and parents. The dissemination of findings through such platforms has generated interest among parents and academicians, and demand for the questionnaire was created among the audience who attended the seminar. The embeddingof the questionnaire in the *National Cyber Parenting Guideline* booklet produced by CSM has also enabled the research product to be utilised directly by parents on a wide scale in the Malaysian setting (CSM, 2019). The questionnaire in the booklet, which serves as a self-reflection assessment tool for parents to consider their digital security practice, helps to ensure that the research product remains relevant and consistently utilised by end users.

In summary, the utilisation of the study findings is evident in various forms, including the embedment of the questionnaire in cyber parenting talks and cyber parenting booklets, and the modifications that have been made to the delivery of cyber parenting awareness programmes by CSM. The utilisation and sustainability of the study's products have thus been enhanced through the integrated knowledge translation approach adopted by this study. Moreover, the utilisation and sustainability strategies that have been followed further enhance the study’s contribution to the public health domain as far as addressing cyber-related issues among children and adolescents is concerned.

5.10 Research Significance

First, this study demonstrated that PMT can be used in explaining parental digital security practice. This is a significant contribution because previous studies on PMT focused on the protective behaviours that individuals perform to protect themselves. This study has extended the applicability of PMT by focusing on the protective behaviour performed to protect someone else, in this case, parental protection of their own children. This is a significant contribution because, to our knowledge, no study has used PMT to examine the protective behaviours adopted by individuals to protect those for whom they are responsible in the area of digital security.

Secondly, the study demonstrated that coping appraisal has a greater influence in determining parental digital security practice. This is an important contribution in terms of shaping strategies on empowering parents in cyber parenting. However, the study also highlighted that the factors examined in determining parental digital security can be expanded further. This leads to an appreciation of the fact that parental digital security is a complex issue and needs to be further studied.

5.11 Strengths and Limitations

This study has a number of strengths. Firstly, in the systematic review, multiple electronic databases were searched, as well as the grey literature through cross-referencing, which enhanced the comprehensiveness of the article search. Also, focusing on articles that were published in the last 10 years ensured that the studies included were relevant to the current technology climate.

Secondly, the development of the questionnaire was based on best practices and employed comprehensive measures in the item generation, scale development and scale evaluation phases. Although self-reported questionnaires are exposed to information bias as mentioned earlier, the absence of common method bias in this study highlights that the questionnaire produced in this study is of high quality, and that the findings derived from its usage are valid and not influenced by information bias.

Thirdly, the questionnaire developed in this study is the first validated questionnaire on parental digital security practices based on an established cognitive framework, namely PMT, in the Malaysian context. Moreover, this questionnaire was produced as a dual-language instrument designed to be culturally adaptable to the Malaysian population and it therefore has the potential to be utilised on a wide scale, particularly in Malaysia.

Fourthly, the model produced in this study was also proven to be able to explain *parental digital security practice* comprehensively. Although the model only explained 34% of the variation in *parental digital security practice*, this is considered high in the social sciences field because many factors influence an individual's behaviour, such as interpersonal influences, social norms, environment, media, and existing policies (Ferguson, 2016).

It should also be noted that a few limitations are present in this study. Firstly, the systematic review focused only on PMT-based questionnaires on digital security and did not include other theories that might have been used in the development of questionnaires of a similar nature. This limited the scope of the available questionnaires that were identified. However, the systematic review also demonstrated that the included studies had a good level of model fit and high suitability for examining the issue of digital security. Thus, the systematic review managed to highlight the relevance of using PMT as a good theoretical framework for developing protection-related actions, including digital security practices, which is consistent with the findings of Sommestad, Karlzén, and Hallberg (2015). It should also be mentioned that the inclusion criteria of only English-language articles and peer-reviewed journal articles may have introduced publication bias. However, the wide variation in geographical areas covered and the populations of interest captured by this review indicate the comprehensiveness of the identification and inclusion of the articles. Focusing on peer-reviewed journal articles also maintains the quality of the included articles, which makes the results more robust.

Secondly, the self-report nature of the questionnaire could have potentially given rise to information bias. Social desirability bias might have occurred because parents might have answered questions based on what they perceived to be socially acceptable rather than providing answers that were an accurate reflection of their perceptions and actual practice. This might have led to the overreporting or underreporting of the agreement or frequency of certain items. However, the participants in this study were assured that their anonymity would be maintained and this would have helped to reduce any such bias. Additionally, a detailed explanation of the study and the importance of gathering accurate information was highlighted in the respondent information sheet in order to help to reduce bias further.

Thirdly, it is possible that there may have been instances of respondent error, such as giving inconsistent answers or making recording errors by putting responses in the wrong place. This might have occurred due to the nature of the study sites, which were healthcare facilities, which can be busy and chaotic at times. However, the questionnaire was designed so that it contained easy-to-follow directions, clear formatting, and items that were short sentences composed of easy-to-understand words. This design would have helped to reduce the respondent burden and reduce respondent error. However, future studies might want to consider using different study sites such as respondents' houses or workplaces. Such settings might provide a more comfortable environment in which to answer the questionnaire.

Fourthly, end aversion bias may also have occurred due to the use of a Likert-scale-based questionnaire format. Respondents can sometimes exhibit a tendency to avoid the selection of extreme values on a rating scale. As such, the values might not reflect the respondents' true perception or practice. However, in this study, this bias was reduced by mentioning that there were no right or wrong answers, ensuring anonymity and informing the respondents that the data would be carefully secured. As such, this would have given the respondents the confidence to respond as they truly feel.

Another limitation of this study is due to the cross-sectional survey design used in this study, which means that the results can only represent a snapshot of a distinct period of time. The lack of temporal association offered by this kind of study design thus rendered it impossible to establish any causal relationships between *parental digital security practice* and the PMT domains. Thus, longitudinal studies might help to establish cause and effect better. In addition, the exploration of the relationships between the domains could be enhanced further by conducting qualitative studies as well.

The final limitation of this study lies in its inability to explain the remaining 66% of variation in *parental digital security practice* based on the developed model. This reflects the fact that this study did not include other potentially important variables. Examples of these variables might include parental style and social norms. Inclusion of these variables might help to explain *parental digital security practice* better. However, the variables that were selected for analysis in this study led to the parsimonious nature of the questionnaire. As such, this helped to reduce information bias in the data collected from the respondents and contributed to establishing the validity of the questionnaire.

5.12 Policy and Research Recommendations

A number of recommendations can be made in respect of utilising the research findings to inform policy and direct future research.

5.12.1 Policy

The findings of this study can contribute to each stage of the policy cycle, and can help to fill the policy gaps on cyber parenting, as elucidated below.

5.12.1.1 Recognising the Problem

The tool developed in this study can be used to highlight the current level of parental digital security in Malaysia. Access to this information will help to identify parents' needs and the support required for cyber parenting, in particular digital security. Currently, as highlighted in a report by UNICEF (2014), studies on cyber parenting practice among parents in Malaysia have generally focused on children and adolescents' perspective, and not that of the parents. Thus, by examining the views expressed by parents, this study can go some way to filling this gap in knowledge regarding the needs of parents in relation to effective cyber parenting.

5.12.1.2 Policy Formulation and Implementation

As mentioned above, at the moment, the current guidelines and practice recommendations on cyber parenting in Malaysia are based on studies that concentrate on the views of children and adolescents. By filling this gap, this study can contribute to the formulation of policies on cyber parenting that are tailored to parents' needs, particularly in regards to digital security from the parents' perspective. Additionally, the policies pertaining to cyber parenting can be formulated based on the child's age group to take account of the different needs at different stages of adolescent development.

5.12.1.3 Policy Evaluation

The developed tool can be used to evaluate and monitor cyber parenting policies and programmes, particularly those pertaining to digital security and mediation strategies. This will help in tailoring policies based on parents' needs at any given time. It can also be used to help to assess the effectiveness of any cyber parenting programmes that are conducted.

5.12.2 Future Research

This study has taken the first step in understanding parental digital security practice in the Malaysian landscape. It is thus important to build upon the findings in this study by conducting further research on certain aspects as highlighted below:

- **Questionnaire design and validation**: The questionnaire produced by this study can be further validated by involving more representatives from other regions and backgrounds in Malaysia, such as East Malaysia and southern region of the peninsular Malaysia, which were under-represented in this study. Similarly, the validity of the questionnaire for use among the other major races in Malaysia, such as the Chinese and Indian communities, can be further enhanced by administering it to a study population that has greater representation from these populations in the future. The utilisation of the questionnaire could also be further expanded by translating the items into other languages such as Mandarin and Tamil. In addition, the wording, order of questions and formatting of the questionnaire can be re-examined in these validation studies.
- **Model of *parental digital security practice***: Other factors could be explored and added to the developed model in order to attempt to further explain *parental digital security practice*. As this study only focused on fear appeals factors, the use of other cognitive-based models that address other angles, such as normative beliefs and social influence, may be useful in gaining a deeper understanding of *parental digital security practice*. In addition, the model could be further expanded by using other components that might include interpersonal, social and policy factors such as those reflected by the socioecological model, and which

might be able to add value in terms of understanding *parental digital security practice* better.

- **Longitudinal study design**: This study used a cross-sectional design which could not determine causality. Hence, it might be useful to use a longitudinal study design in order to attempt to determine whether the factors explored in this study have any causal relationships with *parental digital security practice*. It is crucial to understand causality because this will give a clear indication as to which factors truly influence *parental digital security practice*. This will in turn guide us in improving the cyber parenting landscape in general.
- **Intervention study design**: Cyber parenting programmes should utilise the study findings to improve parents' confidence in digital security practices. In this regard, intervention studies may also be useful for improving these programmes. For instance, a study that employs an intervention to provide information and guide parents on parental digital security practices would be useful in terms of improving parents' confidence. In addition, an intervention study that looks at how online issues such as cyberbullying and internet addiction can be reduced through parental digital security practices would be useful as well.
- **Review of cyber parenting programmes**: Evaluation studies should be conducted on existing cyber parenting and parental digital security programmes based on the findings in this study. For instance, an evaluation study that looks into the outcome of parental confidence in performing parental digital security practices when attending such programmes would be useful in terms of reflecting the effectiveness of these programmes. In addition, a process evaluation that looks into the components of existing programmes that could potentially improve parents' self-efficacy and response efficacy while reducing their perceived maladaptive rewards would be beneficial as well.

5.13 Summary of Chapter Five

This chapter discussed the outcome of questionnaire development and validation, and demonstrated that the 51 items that were produced for the questionnaire were justified based on the validity properties and the relevance of the items to Malaysian parents. It also explained, conversely, that the removal of three items was justified due to poor properties of the items either in terms of reliability or validity. The chapter then discussed the developed model which showed that *perceived self-efficacy*, *perceived response efficacy* and *perceived maladaptive reward* were significant determinants of *parental digital security practice*, and how these findings related to the literature. It then discussed the insignificant results found for the remaining domains, namely, *perceived response cost*, *perceived severity* and *perceived susceptibility*, explaining that these results could be due to several reasons, including the influence of possible third variables that were not measured in this study. The chapter also highlighted that the validated questionnaire and the exploratory model had public health and research significance. The chapter concluded by showing how integrated knowledge translation strategies were adopted to enhance the utilisation of the study findings, research significance, strengths, limitations of the study as well as recommendations from policy and future research point of view.

CHAPTER SIX: CONCLUSION

In conclusion, this study has managed to answer the research questions and study objectives.

Firstly, the study revealed through the systematic review that the existing PMT-based questionnaires on digital security were of varying quality. A total of 33 PMT-based questionnaires were discovered, 14 of which were of high quality and 17 were of medium quality while the remaining two were of poor quality. None of questionnaires covered parental digital security practice.

Secondly, the study managed to produce and validate a 51-item PMT-based questionnaire on parental digital security practice that was tailored for Malaysian parents. These 51 items were presented in two languages (English and Malay) and covered nine domains, namely, *perceived susceptibility, perceived severity, perceived self-efficacy, perceived response efficacy, perceived tangible cost, perceived psychological cost, perceived maladaptive reward, discursive digital security practice* and *control digital security practice*.

Lastly, the study highlighted that three factors had a significant influence on *parental digital security practice* based on the PMT model, namely, *perceived self-efficacy, perceived response efficacy* and *perceived maladaptive reward.* Furthermore, the PMT model was able to explain 34% of the variation in *parental digital security practice*.

On a personal level, this study has provided a few valuable lessons. Firstly, this study demonstrated the importance of collective efforts in tackling public health issues in the population. The collaboration with CSM, which is an agency that is outside the public health community, has provided benefits to both parties not just from the research point of view. On the one hand, CSM has benefited from gaining insights from health professionals and others who provided input about issues related to digital security from various health perspectives. Similarly, engagement with CSM has helped the public health community to discover those parts of the digital security landscape that need attention from the public health perspective. Such engagements and the cross-fertilisation of knowledge between these two parties will only benefit the population in general.

Secondly, this study has helped to provide a platform for engaging with parents to gain an understanding of parental digital security and cyber parenting in general. Here too, the collaboration with CSM was fruitful in the sense that they provided opportunities for the researcher to engage with parents through their cyber parenting talks and seminars. The knowledge on cyber parenting obtained through this study has also helped the researcher to spread awareness among parents through various channels including social media. The general lesson and feeling that was obtained from these engagements is that Malaysian parents are aware of the issues and the threats posed their children but are uncertain about how to protect their children online. Needless to say, more studies and programmes need to be produced to empower parents on this matter.

Lastly, this study has provided great satisfaction to the researcher because the findings have been fully utilised by the main stakeholder, namely, CSM. The questionnaire that was produced has been embedded in their cyber parenting talks to gauge the audience's perceptions and practices on digital security. The CSM team has acknowledged that the questionnaire has helped them understand the audience better, and enabled them to tailor their presentations accordingly. Based on the findings, the cyber parenting talks and programmes offered by CSM were adjusted to include content that enhances parents' confidence in carrying out parental digital security practices. This is in contrast to the previous practice, in which CSM put more weight on highlighting the online threats without giving much emphasis to the measures that could be employed to tackle these threats. Additionally, the input given from the study has helped in producing the National Cyber parenting guideline (CSM, 2019) which embeds the questionnaire as well as information to enhance parents' coping appraisal components, as recommended by this study.

Overall, the study has contributed significantly to understanding cyber parenting, particularly in the Malaysian context. Ultimately, the findings from and further expansion of this study in the future will be able to empower parents in providing support to children and adolescents to enable them to become good digital citizens.

REFERENCES

Abraham, C. S., Sheeran, P., Abrams, D., & Spears, R. (1994). Exploring teenagers' adaptive and maladaptive thinking in relation to the threat of HIV infection. *Psychology & Health, 9*(4), 253–272.

Acocella, I. (2012). The focus groups in social research: advantages and disadvantages. *Quality & Quantity, 46*(4), 1125-1136.

Ajzen, I. (1985). From intentions to actions: A theory of planned behavior. *Action-Control: From Cognition to Behavior* (pp. 11–39). Heidelberg, Germany: Springer.

Akter, S., D'Ambra, J., & Ray, P. (2013). Development and validation of an instrument to measure user perceived service quality of mHealth. *Information & Management, 50*(4), 181-195.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS Q., 34*(3), 613-643.

Armitage, C. J., & Conner, M. (2000). Social cognition models and health behaviour: A structured review. *Psychology and Health, 15*(2), 173-189.

Aurigemma, S., & Mattson, T. (2018). Exploring the effect of uncertainty avoidance on taking voluntary protective security actions. *Computers & Security, 73*(1), 219-234.

Awang, Z. (2012). *A handbook on structural equation modeling using AMOS*. Kuala Lumpur, Malaysia: Universiti Technologi MARA Press.

Bagozzi, R. P., & Yi, Y. (1988). On the evaluation of structural equation models. *Journal of the Academy of Marketing Science, 16*(1), 74-94.

Bandura, A. (1994). Self-efficacy. In V. S. Ramachaudran (Ed.), *Encyclopedia of Human Behavior* (Vol. 4, pp. 71-81). New York, NY: Academic Press.

Bannink R., Broeren L., Jansen P., & Waart F. (2014). Cyber and traditional bullying victimization as a risk factor for mental health problems and suicidal ideation in adolescents. *PLoS ONE, 9*(4).

Banville, D., Desrosiers, P., & Genet-Volet, Y. (2000). Translating questionnaires and inventories using a cross-cultural translation technique. *Journal of Teaching in Physical Education, 19*(3), 374-387.

Bauman, S., Toomey, R. B., & Walker, J. L. (2013). Associations among bullying, cyberbullying, and suicide in high school students. *Journal of Adolescence, 36*(2), 341-350.

Baxter, R. (2009). Reflective and formative metrics of relationship value: A commentary essay. *Journal of Business Research, 62*(12), 1370-1377.

Beaton, D. E., Bombardier, C., Guillemin, F., & Ferraz, M. B. (2000). Guidelines for the process of cross-cultural adaptation of self-report measures. *Spine, 25*(24), 3186-3191.

Beirens, T. M. J., Brug, J., van Beeck, E. F., Dekker, R., den Hertog, P., & Raat, H. (2008). Assessing psychosocial correlates of parental safety behaviour using Protection Motivation Theory: stair gate presence and use among parents of toddlers. *Health Educ Res, 23*(4), 723-723.

Boateng, G. O., Neilands, T. B., Frongillo, E. A., Melgar-Quiñonez, H. R., & Young, S. L. (2018). Best practices for developing and validating scales for health, social, and behavioral research: a primer. *Frontiers in Public Health, 6*, 149.

Boddum, M. R. (2013). *Plugged in: A focused look at parents' use of smartphones among children 2-5 years of age* (Doctoral dissertation, Mills College). Retrieved from https://search.proquest.com/docview/1373370794

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: towards an intervention strategy for college students. *Behaviour & Information Technology, 34*(10), 1022-1035.

Bollen, K. A., & Barb, K. H. (1981). Pearson's r and coarsely categorized measures. *American Sociological Review*, *46.* 232-239.

Boniel-Nissim, M., Efrati, Y., & Dolev-Cohen, M. (2019). Parental mediation regarding children’s pornography exposure: the role of parenting style, protection motivation and gender. *The Journal of Sex Research*, *57*(1), 42-51.

Boynton, P. M., & Greenhalgh, T. (2004). Selecting, designing, and developing your questionnaire. *BMJ, 328*(7451), 1312-1315.

Bronfenbrenner, U. (1979). Ecological models of human development. *Readings on the Development of Children, 2*(1), 37-43.

Brown, T. A. (2014). *Confirmatory factor analysis for applied research*. New York, NY: Guilford Publications.

Bubaš, G., Orehovački, T., & Konecki, M. (2008). Factors and predictors of online security and privacy behavior. *Journal of Information and Organizational Sciences, 32*(2), 79-98.

Bujang, M. A., & Baharum, N. (2017). A simplified guide to determination of sample size requirements for estimating the value of intraclass correlation coefficient: a review. *Archives of Orofacial Science, 12*(1), 1-11.

Burns, A. J., Posey, C., Roberts, T. L., & Benjamin Lowry, P. (2017). Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals. *Computers in Human Behavior, 68*, 190-209.

Byrne, B. M. (2016). *Structural equation modeling with AMOS: Basic concepts, applications, and programming*. New York, NY: Psychology Press.

Carpenter, C. J. (2010). A meta-analysis of the effectiveness of health belief model variables in predicting behavior. *Health Commun, 25*(8), 661-669.

Chai, S., Bagchi-Sen, S., Morrell, C., Rao, H. R., & Upadhyaya, S. J. (2009). Internet and online information privacy: An exploratory study of preteens and early teens. *IEEE Transactions on Professional Communication, 52*(2), 167-182.

Chan, P. A., & Rabinowitz, T. (2006). A cross-sectional analysis of video games and attention deficit hyperactivity disorder symptoms in adolescents. *Annals of General Psychiatry, 5*, 16-16.

Chang, L. (1997). Dependability of anchoring labels of Likert-type scales. *Educational and Psychological Measurement, 57*(5), 800-807.

Chiong, C., & Shuler, C. (2010). *Learning: Is there an app for that.* Paper presented at the Investigations of young children's usage and learning with mobile devices and apps, New York, United States of America.

Chou, H.-L., & Chou, C. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior, 65*, 334-345.

Claar, C. L., & Johnson, J. (2012). Analyzing home PC security adoption behavior. *Journal of Computer Information Systems, 52*(4), 20-29.

Cohen, J. (2013). *Statistical power analysis for the behavioral sciences*. New York, NY: Academic Press.

Collins, D. (2003). Pretesting survey instruments: an overview of cognitive methods. *Quality of Life Research, 12*(3), 229-238.

Coltman, T., Devinney, T. M., Midgley, D. F., & Venaik, S. (2008). Formative versus reflective measurement models: Two applications of formative measurement. *Journal of Business Research, 61*(12), 1250-1262.

CommonSense. (2014). *Everything you need to know about parental controls*. Retrieved from https://www.commonsensemedia.org/blog/everything-you-need-to-know-about-parental-controls

Comrey, A. L., & Lee, H. B. (2013). *A first course in factor analysis*. New York, NY: Psychology Press.

Conner, M., & Norman, P. (2005). *Predicting health behaviour*. London, UK: McGraw-Hill Education.

Connect Safely. (2015). *A parents' guide to cybersecurity*. Retrieved from https://www.connectsafely.org/wp-content/uploads/securityguide.pdf

Cortina, J. M. (1993). What is coefficient alpha? An examination of theory and applications. *Journal of Applied Psychology, 78*(1), 98.

Cristobal, E., Flavián, C., & Guinaliu, M. (2007). Perceived e-service quality (PeSQ) measurement validation and effects on consumer satisfaction and web site loyalty. *Managing Service Quality: An International Journal, 17*(3), 317-340.

Crossler, R., B, F., & Langer. (2014). An extended perspective on individual security behaviors: protection motivation theory and a unified security practices (usp) instrument. *SIGMIS Database, 45*(4), 51-71.

Curran, M. B., & Ribble, M. (2017). P–20 model of digital citizenship. *New Directions for Student Leadership*, *2017*(153), 35-46.

CyberSecurity Malaysia. (2014). *Cybersafe in schools*. Retrieved from https://www.cybersecurity.my/en/index.html

CyberSecurity Malaysia. (2015). *Growing digital resilience among malaysian schoolchildren on staying safe online*. Retrieved from https://www.cybersecurity.my/en/index.html

CyberSecurity Malaysia. (2017). *Teach your kids online safety*. Retrieved from http://www.cybersafe.my/cyberparent-tips.html

CyberSecurity Malaysia. (2018). *Panduan keibubapaan digital*. Retrieved from www.cybersafe.my.

CyberSecurity Malaysia. (2019). *Cybersafe parenting: Ke arah kesejahteraan siber*. Retrieved from https://www.cybersafe.my/en/download/CyberSAFE%20Parenting_Booklet-BM-online.pdf .

Cyril, S., Oldroyd, J. C., & Renzaho, A. (2013). Urbanisation, urbanicity, and health: a systematic review of the reliability and validity of urbanicity scales. *BMC Public Health, 13*(1), 513.

Cyril, S., Smith, B. J., & Renzaho, A. M. (2015). Systematic review of empowerment measures in health promotion . *Health Promotion International*, *31*(4), 809-826.

Czaja, R. (1998). Questionnaire pretesting comes of age. *Marketing Bulletin-Department of Marketing Massey University, 9*, 52-66.

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university. *Comput. Secur., 48*(C), 281-297.

Darbyshire, P., & McDonald, H. (2004). Choosing response scale labels and length: Guidance for researchers and clients. *Australasian Journal of Market Research, 12*(2), 17-26.

Davis, L. L. (1992). Instrument review: Getting the most from a panel of experts. *Applied Nursing Research, 5*(4), 194-197.

Department of Statistics Malaysia. (2017). *Selangor*. Retrieved from https://www.dosm.gov.my/v1/index.php?r = column/cone&menu_id = eGUyTm9RcEVZSllmYW45dmpnZHh4dz09

DeVellis, R. (2017). *Scale development; Theory and applications (fourth edition).* Thousand Oaks, United States: Sage Publications.

Di Lorio, C. K. (2005). *Measurement in health behaviour.* San Francisco, United States: John Wiley & Sons.

Diamantopoulos, A., & Siguaw, J. A. (2006). Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. *British Journal of Management, 17*(4), 263-282.

Dillard, J. P. (1994). Rethinkin the study of fear appeals: An emotional perspective. *Communication Theory, 4*(4), 295-323.

Dillman, D. A., Sinclair, M. D., & Clark, J. R. (1993). Effects of questionnaire length, respondent-friendly design, and a difficult question on response rates for occupant-addressed census mail surveys. *Public Opinion Quarterly, 57*(3), 289-304.

Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). *Internet, phone, mail, and mixed-mode surveys: the tailored design method*. New Jersey, United States: John Wiley & Sons.

Doane, A. N., Boothe, L. G., Pearson, M. R., & Kelley, M. L. (2016). Risky electronic communication behaviors and cyberbullying victimization: An application of Protection Motivation Theory. *Computers in Human Behavior, 60*, 508-513.

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

Fabrigar, L. R., Wegener, D. T., MacCallum, R. C., & Strahan, E. J. (1999). Evaluating the use of exploratory factor analysis in psychological research. *Psychological methods, 4*(3), 272.

Facebook (2019). *How do I report a child under the age of 13?* Retrieved from https://www.facebook.com/help/157793540954833

Falk, R. F., & Miller, N. B. (1992). *A primer for soft modeling*. Ohio, United States: University of Akron Press.

Family Online Safety Institute. (2015). *Parents, privacy & technology use*. Retrieved from https://www.fosi.org/good-digital-parenting/parents-privacy-technology-research-findings/

Faul, F., Erdfelder, E., Buchner, A., & Lang, A. G. (2009). Statistical power analyses using G* Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*(4), 1149-1160.

Ferguson, C. J. (2016). An effect size primer: A guide for clinicians and researchers. In A. E. Kazdin (Ed.), *Methodological issues and strategies in clinical research* (p. 301–310). New York, United States: American Psychological Association.

Flood, M. (2009). The harms of pornography exposure among children and young people. *Child Abuse Review, 18*(6), 384-400.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology, 30*(2), 407-429.

Fornell, C., & Larcker, D. F. (1981). *Structural equation models with unobservable variables and measurement error: Algebra and statistics*. Los Angeles, United States: SAGE Publications.

Fry, E. (1977). Fry's readability graph: Clarifications, validity, and extension to level 17. *Journal of Reading, 21*(3), 242-252.

Gagliardi, A. R., Berta, W., Kothari, A., Boyko, J., & Urquhart, R. (2015). Integrated knowledge translation (IKT) in health care: a scoping review. *Implementation Science, 11*(1), 38.

Gainforth, H. L., Cao, W., & Latimer-Cheung, A. E. (2012). Determinants of human papillomavirus (HPV) vaccination intent among three Canadian target groups. *J Cancer Educ, 27*(4), 717-724.

Gefen, D., Straub, D., & Boudreau, M. C. (2000). Structural equation modeling and regression: Guidelines for research practice. *Communications of the Association for Information Systems, 4*(1), 7.

Glanz, K., Rimer, B. K., & Viswanath, K. (2008). *Health behavior and health education: theory, research, and practice*. New Jersey, United States: John Wiley & Sons.

Glister, P. (1997). *Digital literacy*. New Jersey, United States: Wiley.

Goerman, P. L., & Caspar, R. A. (2010). A preferred approach for the cognitive testing of translated materials: Testing the source version as a basis for comparison. *International Journal of Social Research Methodology, 13*(4), 303-316.

Graham, I. D., Logan, J., Harrison, M. B., Straus, S. E., Tetroe, J., Caswell, W., & Robinson, N. (2006). Lost in knowledge translation: time for a map? *Journal of Continuing Education in the Health Professions, 26*(1), 13-24.

Grant, J. S., & Davis, L. L. (1997). Selection and use of content experts for instrument development. *Res Nurs Health, 20*(3), 269-274.

Green, J. P., Tonidandel, S., & Cortina, J. M. (2016). Getting through the gate: Statistical and methodological issues raised in the reviewing process. *Organizational Research Methods, 19*(3), 402-432.

Guest, G., Bunce, A. and Johnson, L. (2006) How Many Interviews Are Enough? An Experiment with Data Saturation and Variability. *Field Methods*, 18, 59-82.

Guillemin, F. (1995). Cross-cultural adaptation and validation of heatth status measures. *Scandinavian Journal of Rheumatology, 24*(2), 61-63.

Guillemin, F., Bombardier, C., & Beaton, D. (1993). Cross-cultural adaptation of health-related quality of life measures: literature review and proposed guidelines. *Journal of Clinical Epidemiology, 46*(12), 1417-1432.

Gurung, A., Luo, X., & Liao, Q. (2009). Consumer motivations in taking action against spyware: An empirical investigation. *Information Management and Computer Security, 17*(3), 276-289.

Gwet, K. L. (2014). *Intrarater reliability*. Retrieved from https://onlinelibrary.wiley.com/doi/full/10.1002/9781118445112.stat06882

Hair, J., Black, W., & Babin, B. (2010). Multivariate Data Analysis. New Jersey,United States: Pearson Prentice Hall.

Hair, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). *A primer on partial least squares structural equation modeling (PLS-SEM)*. California, United States: Sage Publications.

Hendricson, W. D., Russell, I. J., Prihoda, T. J., Jacobson, J. M., Rogan, A., & Bishop, G. D. (1989). An approach to developing a valid Spanish language translation of a health-status questionnaire. *Medical Care*, 959-966.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science, 43*(1), 115-135.

Henson, R. K., & Roberts, J. K. (2006). Use of exploratory factor analysis in published research: Common errors and some comment on improved practice. *Educational and Psychological Measurement, 66*(3), 393-416.

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.

Hina, S., & Dominic, D. D. (2017). *Need for information security policies compliance: A perspective in Higher Education Institutions.* Paper presented at the International Conference on Research and Innovation in Information Systems, ICRIIS.

Hinkin, T. R. (1995). A review of scale development practices in the study of organizations. *Journal of Management, 21*(5), 967-988.

Hinkin, T. R. (1998). A brief tutorial on the development of measures for use in survey questionnaires. . *Organizational Research Methods, 1* (1), 104-121.

Holmbeck, G. N., & Devine, K. A. (2009). *An author's checklist for measure development and validation manuscripts*. Oxford, England: Oxford University Press.

Hoon Kim, S., Hoon Yang, K., & Park, S. (2014). An integrative behavioral model of information security policy compliance. *The Scientific World Journal, 2014*(1).

Horn, J. L. (1965). A rationale and test for the number of factors in factor analysis. *Psychometrika, 30*(2), 179-185.

Hovav, A., & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing, 32*, 35-49.

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

Huck, S. W., & Jacko, E. J. (1974). Effect of varying the response format of the Alpert-Haber Achievement Anxiety Test. *Journal of Counseling Psychology, 21*(2), 159.

Hunt, S. D. (1991). *Modern marketing theory: Critical issues in the philosophy of marketing science*. Tennesee, United Staes: South-Western Pub.

Hwang, Y., Choi, I., Yum, J.-Y., & Jeong, S.-H. (2017). Parental mediation regarding children's smartphone use: Role of protection motivation and parenting style. *Cyberpsychology, Behavior, and Social Networking, 20*(6), 362-368.

Hwang, Y., & Jeong, S.-H. (2015). Predictors of parental mediation regarding children's smartphone use. *Cyberpsychology, Behavior, and Social Networking, 18*(12), 737-743.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Comput. Secur., 31*(1), 83-95.

Information Technology Union [ITU]. (2018) *Measuring the Information Society Report 2018*. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2018/MISR-2018-Vol-1-E.pdf

Instagram (2019). *How do I report a child under the age of 13 on Instagram?* Retrieved from https://help.instagram.com/517920941588885

Institute of Public Health (2015). *National Health and Morbidity Survey 2015: Healthcare Demand Volume III*. Kuala Lumpur, Malaysia: Ministry of Health Malaysia.

Institute of Public Health (2017), *National Health and Morbidity Survey 2017: Adolescent Health and Nutrition Survey*. Kuala Lumpur, Malaysia: Ministry of Health Malaysia.

International Society for Technology in Education. (2011). *Digital citizenship in schools*. Retrieved from http://www.iste.org/docs/excerpts/DIGCI2-excerpt

Isa, M. (2016). Internet addiction among adolescents in Malaysia: the prevalence and its association with attention deficit hyperactivity disorder (ADHD) symptoms. *Malaysian Journal of Psychiatry, 25*(1), 3-18.

Jansen, J., & van Schaik, P. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information and Computer Security, 25*(2), 165-180.

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

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS quarterly*, 549-566.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric. *MIS Q., 39*(1), 113-134.

Kim, Y., Park, J. Y., Kim, S. B., Jung, I.-K., Lim, Y. S., & Kim, J.-H. (2010). The effects of Internet addiction on the lifestyle and dietary behavior of Korean adolescents. *Nutrition Research and Practice, 4*(1), 51-57.

Kock, N., & Lynn, G. (2012). Lateral collinearity and misleading results in variance-based SEM: An illustration and recommendations. *Journal of the Association for Information Systems, 13*(7).

Kothari, A., & Wathen, C. N. (2013). A critical second look at integrated knowledge translation. *Health Policy, 109*(2), 187-191.

Krosnick, J. A., & Fabrigar, L. R. (1997). Designing rating scales for effective measurement in surveys. *Survey Measurement and Process Quality*, 141-164.

Kwak, D.-H., Kizzier, D. M., & Jung, E. (2011). *Spyware knowledge in anti-spyware program adoption: effects on risk, trust, and intention to use.* Paper presented at the System Sciences (HICSS), 2011 44th Hawaii International Conference.

Lam, L. T., & Peng, Z. (2010). Effect of pathological use of the internet on adolescent mental health: A prospective study. *Archives of Pediatrics & Adolescent Medicine, 164*(10), 901-906.

Lau, M. Y.-K. (2008). *Extreme response style: An empirical investigation of the effects of scale response format and fatigue*. Indiana, United States: University of Notre Dame.

Lazarsfeld, P. F. (1958). Evidence and inference in social research. *Daedalus, 87*(4), 99-130.

Lee, W. Y., Tan, C.-S., & Siah, P. C. (2017). The role of online privacy concern as a mediator between internet self-efficacy and online technical protection privacy behavior. *Sains Humanika, 9*(3-2).

Lee, Y., & Larsen, K. R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177-187.

Lefever, S., Dal, M., & Matthiasdottir, A. (2007). Online data collection in academic research: advantages and limitations. *British Journal of Educational Technology, 38*(4), 574-582.

Leppink, J., & Pérez-Fuster, P. (2017). We need more replication research–A case for test-retest reliability. *Perspectives on medical education, 6*(3), 158-164.

Leventhal, H. (1970). Findings and theory in the study of fear communications. In *Advances in experimental social psychology* (Vol. 5, pp. 119-186). California, United States: Elsevier.

Little, R. J. (1988). A test of missing completely at random for multivariate data with missing values. *Journal of the American Statistical Association, 83*(404), 1198-1202.

Livingstone, S., & Haddon, L. (2008). Risky experiences for children online: Charting European research on children and the internet. *Children & Society, 22*(4), 314-323.

Livingstone, S., & Helsper, E. J. (2008). Parental mediation of children's internet use. *Journal of Broadcasting & Electronic Media, 52*(4), 581-599.

Lohr, K. N. (2002). Assessing health status and quality-of-life instruments: attributes and review criteria. *Quality of Life Research, 11*(3), 193-205.

Lorenz, B. (2017). *A digital safety model for understanding teenage internet user's concerns* (Doctoral dissertation, Tallinn University). Retrieved from https://www.digar.ee/arhiiv/en/books/83045

Lwin, M. O., Li, B., & Ang, R. P. (2012). Stop bugging me: An examination of adolescents' protection behavior against online harassment. *Journal of Adolescence, 35*(1), 31-41.

Lynn, M. R. (1986). Determination and quantification of content validity. *Nurs Res*, *35*(6), 382–385.

Lyons, R. (2011). *Investigating student gender and grade level differences in digital citizenship behavior* (Doctoral dissertation, Walden University). Retrieved from https://scholarworks.waldenu.edu/

MacDonell, K., Chen, X., Yan, Y., Li, F., , G., J., , Sun, H., & Stanton, B. (2013). A protection motivation theory-based scale for tobacco research among Chinese youth. *Journal of Addiction Research & Therapy, 4*(154).

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation theory and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*, 469-479.

Maha, A. (2010). Attitude Towards Sex: Study of Secondary Schoolchildren in Selangor State. *Malaysian Journal of Medicine and Health Sciences, 6*(1).

Malaysian Communications and Multimedia Commision [MCMC], (2018). *Internet users survey 2018*. Retrieved from https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/Internet-Users-Survey-2018.pdf

Mardia, K.V. (1974) Applications of some measures of multivariate skewness and kurtosis in testing normality and robustness studies. *Sankhyā: The Indian Journal of Statistics, Series B*, 115-128.

Marsh, H. W., Hau, K. T., Balla, J. R., & Grayson, D. (1998). Is more ever too much? the number of indicators per factor in confirmatory factor analysis. *Multivariate Behav Res, 33*(2), 181-220.

McCoach, D. B., Gable, R. K., & Madura, J. P. (2013). *Instrument development in the affective domain*. New York, United States: Springer.

McColl, E., Meadows, K., & Barofsky, I. (2003). Cognitive aspects of survey methodology and quality of life assessment. *Qual Life Res, 12*(3), 217-218.

McHugh, M. L. (2012). Interrater reliability: the kappa statistic. *Biochemia medica, 22*(3), 276-282.

McNeish, D. (2017). Thanks coefficient alpha, we'll take it from here. *Psychological Methods*, *23*(3), 412.

MediaSmarts, P. S. C. a. (2017). *Digital citizenship: guide for parents*. Retrieved from https://www.getcybersafe.gc.ca/cnt/rsrcs/cmpgns/cmpgn-06/gd-prnts-en.aspx

Meehan S, H. J. (2016). A model of parental mediation of their children's use of internet connected devices. *Psychol Clin Psychiatry, 5*(5), 1-5.

Menard, P., Gatlin, R., & Warkentin, M. (2014). Threat protection and convenience: Antecedents of cloud-based data backup. *Journal of Computer Information Systems, 55*(1), 83-91.

Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. *Journal of Information Privacy & Security, 9*(1), 47-67.

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology, 30*(1), 106-143.

Ministry of Education Malaysia. (2013). *Malaysia education blueprint 2013-2025*. Kuala Lumpur, Malaysia: Ministy of Education Malaysia.

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.

Moher, D., Liberati, A., Tetzlaff, J., & Altman, D. G. (2009). Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement. *BMJ, 339*(2535).

Mokkink, L. B., Terwee, C. B., Patrick, D. L., Alonso, J., Stratford, P. W., Knol, D. L., . . . De Vet, H. C. (2010). The COSMIN checklist for assessing the methodological quality of studies on measurement properties of health status measurement instruments: an international Delphi study. *Quality of Life Research, 19*(4), 539-549.

Moors, G., Kieruj, N. D., & Vermunt, J. K. (2014). The effect of labeling and numbering of response scales on the likelihood of response bias. *Sociological Methodology, 44*(1), 369-399.

Mullin, P. A., Lohr, K. N., Bresnahan, B. W., & McNulty, P. (2000). Applying cognitive design principles to formatting HRQOL instruments. *Quality of Life Research, 9*(1), 13-27.

Nanda, T., Gupta, H., Kharub, M., & Singh, N. (2013). Diagnostics for pretesting questionnaires: a comparative analysis. *International Journal of Technology, Policy and Management, 13*(1), 67-79.

Nathanson, A. I. (2001). Parent and child perspectives on the presence and meaning of parental television mediation. *Journal of Broadcasting & Electronic Media, 45*, 201–220.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems, 46*(4), 815-825.

Nikken, P., & Jansz, J. (2014). Developing scales to measure parental mediation of young children's internet use. *Learning Media and Technology, 39*(2), 250-266.

Nikken, P., & Schols, M. (2015). How and why parents guide the media use of young children. *Journal of Child and Family Studies, 24*(11), 3423-3435.

Nomaguchi, K. M., & Milkie, M. A. (2003). Costs and rewards of children: The effects of becoming a parent on adults' lives. *Journal of Marriage and Family*, *65*(2), 356-374.

Notten, N., & Kraaykamp, G. (2009). Parents and the media: A study of social differentiation in parental media socialization. *Poetics, 37*(3), 185-200.

Nunnally, J. C., Bernstein, I. H., & Berge, J. M. (1967). *Psychometric theory.* New York, United States: McGraw-Hill.

Ofcom. (2013). *Children and parents: Media use and attitudes report*: Retrieved from https://www.ofcom.org.uk/research-and-data/media-literacy

Peters, G.-J. Y., Ruiter, R. A., & Kok, G. (2013). Threatening communication: a critical re-analysis and a revised meta-analytic test of fear appeal theory. *Health Psychology Review, 7*(sup1), S8-S31.

Pew Research (2018). *Teens, social media & technology 2018*. Retrieved from https://www.pewresearch.org/internet/2018/05/31/teens-social-media-technology-2018/

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology, 88*(5), 879.

Polit, D. F., & Beck, C. T. (2006). The content validity index: Are you sure you know what's being reported? Critique and recommendations. *Res Nurs Health, 29*(5), 489-497.

Prentice-Dunn, S., & Rogers, R. W. (1986). Protection motivation theory and preventive health: Beyond the health belief model. *Health Educ Res, 1*(3), 153-161.

Reise, S. P., Waller, N. G., & Comrey, A. L. (2000). Factor analysis and scale revision. *Psychological Assessment, 12*(3), 287.

Rhemtulla, M., Brosseau-Liard, P. E., & Savalei, V. (2012). When can categorical variables be treated as continuous? A comparison of robust continuous and categorical SEM estimation methods under suboptimal conditions. *Psychological Methods, 17*(3), 354.

Ribble, M. (2015). *Digital Citizenship in Schools*. Virginia, United States: International Society for Technology in Education.

Ribble, M. (2016). *White paper: Digital citizenship: a holistic primer.* Retrieved from https://www.imperosoftware.com/us

Rosenstock, I. M. (1974). The health belief model and preventive health behavior. *Health Education Monographs, 2*(4), 354-386.

Rowley, J. (2014). Designing and using research questionnaires. *Management Research Review, 37*(3), 308-330.

Roy, R., & Paradis, G. (2015). *Smartphone use in the daily interactions between parents and young children*. Retrieved from https://www.csustan.edu/sites

Rubio, D. M., Berg-Weger, M., Tebb, S. S., Lee, E. S., & Rauch, S. (2003). Objectifying content validity: Conducting a content validity study in social work research. *Social Work Research, 27*(2), 94-104.

Ruiter, R. A., Kessels, L. T., Peters, G. J. Y., & Kok, G. (2014). Sixty years of fear appeal research: Current state of the evidence. *International Journal of Psychology, 49*(2), 63-70.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65-78.

Schmiedel, T., Vom Brocke, J., & Recker, J. (2014). Development and validation of an instrument to measure organizational cultures' support of business process management. *Information & Management, 51*(1), 43-56.

Shin, W. (2015). Parental socialization of children's Internet use: A qualitative approach. *New Media & Society, 17*(5), 649-665.

Shin, W., & Li, B. (2017). Parental mediation of children's digital technology use in Singapore. *Journal of Children and Media, 11*(1), 1-19.

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.

Slavec, A., & Drnovsek, M. (2012). A perspective on scale development in entrepreneurship research. *Economic and Business Review for Central and South-Eastern Europe, 14*(1), 39.

Sohn, S., Rees, P., Wildridge, B., Kalk, N. J., & Carter, B. (2019). Prevalence of problematic smartphone usage and associated mental health outcomes amongst children and young people: A systematic review, meta-analysis and GRADE of the evidence. *BMC Psychiatry, 19*(1), 1-10

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A meta-analysis of studies on protection motivation theory and information security behaviour. *International Journal of Information Security and Privacy (IJISP), 9*(1), 26-46.

Sonck, N., Nikken, P., & de Haan, J. (2013). Determinants of internet mediation: A comparison of the reports by Dutch parents and children. *Journal of Children and Media, 7*(1), 96-113.

Srinivasan, V., & Basu, A. K. (1989). The metric quality of ordered categorical data. *Marketing Science, 8*(3), 205-230.

Straub, D. W. (1989). Validating instruments in MIS research. *MIS Quarterly*, *13*(2), 147-169.

Streiner, D., & Norman, G. (2008). *Health measurement scales: A practical guide to their development and use*. Oxford, United Kingdom: Oxford University Press.

Tafforeau, J., Cobo, M. L., Tolonen, H., Scheidt-Nave, C., & Tinto, A. (2005). *Guidelines for the development and criteria for the adoption of health survey instruments*. Luxembourg, Luxemborg: European Commission.

Thompson, N., McGill, T. J., & Wang, X. (2017). Security begins at home: Determinants of home computer and mobile device security behavior. *Computers & Security, 70*, 376-391.

Timmerman, M. E., & Lorenzo-Seva, U. (2011). Dimensionality assessment of ordered polytomous items with parallel analysis. *Psychol Methods, 16*(2), 209-220.

Trochim. (2006). *Research methods knowledge base*. Boston, United States; Thomson Learning.

Tsai, H.-y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors. *Comput. Secur., 59*(C), 138-150.

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft. *Inf. Manage., 52*(4), 506-517.

UNICEF (2014). *Exploring the digital landscape in malaysia access and use of digital technologies by children and adolescents*. Retrieved from https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf

United Nations. (2015). *Transforming our world: the 2030 agenda for sustainable development*. Retrieved from https://sustainabledevelopment.un.org/sdg4.

Van Belle, S., van de Pas, R., & Marchal, B. (2017). Towards an agenda for implementation science in global health: there is nothing more practical than good (social science) theories. *BMJ global health, 2*(2).

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.

Visinescu, L. L., Azogu, O., Ryan, S. D., Wu, Y. A., & Kim, D. J. (2016). Better safe than sorry: A study of investigating individuals' protection of privacy in the use of storage as a cloud computing service. *International Journal of Human-Computer Interaction, 32*(11), 885-900.

Viswanathan, M., Sudman, S., & Johnson, M. (2004). Maximum versus meaningful discrimination in scale response: Implications for validity of measurement of consumer perceptions about products. *Journal of Business Research, 57*(2), 108-124.

Vitoratou S, Ntzoufras I, Smyrnis N, & Stefanis, N. (2009). Factorial composition of the aggression questionnaire: a multi-sample study in Greek adults. *Psychiatry Research, 168*(32-39).

Walrave, M., Vanwesenbeeck, I., & Heirman, W. (2012). Connecting and protecting? Comparing predictors of self-disclosure and privacy settings use between adolescents and adults. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace, 6*(1).

Waltz, C. F., Strickland, O. L., & Lenz, E. R. (2010). *Measurement in nursing and health research*. New York, United States: Springer.

Warkentin, M., Johnston, A. C., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems, 92*, 25-35.

Wartella, E., Rideout, V., Lauricella, A. R., & Connell, S. (2013). *Parenting in the age of digital technology*. Illinois, United States: Author.

Weijters, B., Cabooter, E., & Schillewaert, N. (2010). The effect of rating scale format on response styles: The number of response categories and response category labels. *International Journal of Research in Marketing, 27*(3), 236-247.

Weinstein, N. D. (1988). The precaution adoption process. *Health Psychology, 7*(4), 355.

Willard, N. (2007). *Educator's guide to cyberbullying and cyberthreats*. Retrieved from https://socialna-akademija.si/

Wisniewski, P., Jia, H., Xu, H., Rosson, M. B., & Carroll, J. M. (2015). *Preventative vs. reactive: How parental mediation influences teens' social media privacy behaviors.* Paper presented at the Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing.

Witte, K. (1993). A theory of cognition and negative affect: Extending Gudykunst and Hammer's theory of uncertainty and anxiety reduction. *International Journal of Intercultural Relations, 17*(2), 197-215.

Witte, K. (1994). Fear control and danger control: A test of the extended parallel process model (EPPM). *Communications Monographs, 61*(2), 113-134.

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior, 27*(5), 591-615.

Wood, N. D., Akloubou Gnonhosou, D. C., & Bowling, J. (2015). Combining parallel and exploratory factor analysis in identifying relationship scales in secondary data. *Marriage & Family Review, 51*(5), 385-395.

World Health Organization (2014). *Public health implications of excessive use of the internet, computers, smartphones and similar electronic devices meeting report.* Retrieved from https://apps.who.int/iris/handle/10665/184264

Worthington, R. L., & Whittaker, T. A. (2006). Scale development research: A content analysis and recommendations for best practices. *The Counseling Psychologist, 34*(6), 806-838.

Wright, K. B. (2005). Researching Internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services. *Journal of Computer-Mediated Communication, 10*(3).

Yoon, C., Hwang, J. W., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education, 23*(4), 407-416.

Zhang, L., & McDowell, W. C. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce, 8*(3-4), 180-197.

Zhang, X., Liu, S., Chen, X., Wang, L., Gao, B., & Zhu, Q. (2017). Health information privacy concerns, antecedents, and information disclosure intention in online health communities. *Information & Management*, *55*(4), 482-493.

List of Publications

1) Developing and Testing the Psychometric Properties of the Parental Digital Security (P-Dis) Questionnaire for Malaysian Parents (This manuscript has been accepted and has been published by Academy of Science (ASM) Journal, Volume 13, Special Issue 5, page 83-95, 2020)
2) Tackling Cyber Threats in Public Health- Examining Scope and Quality of Protection Motivation Theory-Based Questionnaires on Digital Security: A Systematic Review (This manuscript has been submitted and under review by the Malaysian Journal of Public Health Medicine, with reference number 919/8)
3) Adoption of parental digital security questionnaire as Cyber Parenting Quiz for National Cyber Parenting Guideline produced by CyberSecurity Malaysia (The guideline can be accessed at https://www.cybersafe.my/en/download/CyberSAFE%20Parenting_Booklet-BM-online.pdf)

List of Conference and Scientific Meetings' Presentations

1) *Knowledge Translation: Connecting Knowledge Creators to the World* (Study protocol presentation for both oral and poster, at the 2017 Kyoto Global Conference for Rising Public Health Researchers (KGC) on 7th December 2017 in Kyoto, Japan)

2) *Towards good cyber parenting- Exploring stakeholders' views in understanding parental digital security practice and online threat concerns in Malaysia.* (Poster presentation at the 2018 7th International Public Health Conference, Malaysia, from 28th August 2018-30th August 2018 in Kuala Lumpur, Malaysia)

3) *Enhancing parental digital security awareness programmes among Malaysian parents* (Implementation study protocol oral presentation, at the 2019 GACD-HSRI Implementation Science School on 5th November 2019 in Bangkok, Thailand)