FLORIDA INTERNATIONAL UNIVERSITY

Miami, Florida

DRIVERS OF INTENTION TO TAKE PROTECTIVE CYBERSECURITY ACTIONS IN HOME USERS: A PROTECTION MOTIVATION THEORY APPROACH

A dissertation submitted in partial fulfillment of

the requirements for the degree of

DOCTOR OF BUSINESS ADMINISTRATION

by

Humberto Rayti Noguera

2023

To: Dean William G. Hardin
College of Business

This dissertation, written by Humberto Rayti Noguera, and entitled Drivers of Intention to Take Protective Cybersecurity Actions in Home Users: A Protection Motivation Theory Approach, having been approved in respect to style and intellectual content, is referred to you for judgment.

We have read this dissertation and recommend that it be approved.

_____

Attila J Hertelendy, Member

_____

Jayati Sinha, Member

_____

Chaitali Paresh Kapadia, Member

_____

Miguel Aguirre-Urreta, Major Professor

Date of Defense: June 26, 2023

The dissertation of Humberto Rayti Noguera is approved.

_____

Dean William G. Hardin
College of Business

_____

Andrés G. Gil
Vice President for Research and Economic Development
and Dean of the University Graduate School

Florida International University, 2023

DEDICATION

I dedicate this dissertation to my children. As a tangible example for you that with discipline, effort, and dedication all goals in life can be fulfilled. Never give up.

ACKNOWLEDGMENTS

I wish to thank the members of my committee for their dedication, professionalism, and support. Their recommendations and guidelines have been much appreciated. All members, including Dr. Tali Kapadia, Dr. Attila Hertelendy, and Dr. Jayati Sinha, provided useful and important feedback and guidance regarding the core structure of this dissertation. I will always be thankful for their dedication and their contribution to this dissertation. I would like to thank Dr. George Marakas for providing me with the necessary guidance and inspiration from the very beginning. Finally, I would like to thank my major professor, Dr. Miguel Aguirre-Urreta. From the beginning, he approached me with respect, professionalism, and patience. Dr. Miguel Aguirre-Urreta is the finest and most complete academic professional I have ever met; he has always guided me to complete this degree with the highest possible level of quality and excellence.

I have found the doctoral curriculum beneficial. I have learned important information, techniques, and methods in my coursework through the curriculum and instructions program. I am confident that the knowledge acquired in this program will fit in my future professional endeavors and it will help me to provide feasible and scientific solutions in real world case scenarios.

ABSTRACT OF THE DISSERTATION

DRIVERS OF INTENTION TO TAKE PROTECTIVE CYBERSECURITY ACTIONS IN HOME USERS: A PROTECTION MOTIVATION THEORY APPROACH

by

Humberto Rayti Noguera

Florida International University, 2023

Miami, Florida

Professor Miguel Aguirre-Urreta, Major Professor

Home users have become targets of interest for cybercriminals due to their lower cybersecurity sophistication, compared to corporate and government operations. In order to identify factors which contribute to cybercrime perception and preparation in home users, the current study uses an extended version of the Protection Motivation Theory (PMT) as the theoretical lens for the study. Specifically, the current study includes the role of internet trust, trust in the ISP, and usage of social media as potential drivers of PMT drivers of intention to protect oneself from cybercrime, to study the extent to which device security and digital literacy affect the abovementioned PMT drivers, and to study the extent to which having been exposed to cybersecurity training and awareness efforts has an impact on the PMT drivers. Data collection for this research was conducted via an online survey from 582 respondents.

The results from the antecedents to the core constructs of the PMT concluded: in the case of internet trust that home users who believe that the internet is a safe space perceive cybercrime as less of a threat and minimise effort spent in protecting themselves from it. In the case of device security the findings indicate that the more device security measures or features are implemented the more aware the home user becomes of the severity of cyberthreats and which indicates that more device security measures or features are implemented the more home users to belief on their own personal skills and abilities to be able to perform certain tasks; indirectly, therefore, device security plays a role in the formation of intention to take protective actions. In the case of digital literacy, the findings concluded that further investigation is required. In the case of social media usage this finding indicates that the more home users are investing time on social media platforms, the greater extent, or the frequency of social media usage the more they believe the internet is a safe space to transact and engage with others. In the case of ISP compliance, the findings indicates that the more home users become aware and perceived ISPs as providing an extra layer of security for their protection, the more likely they are to trust the internet as a safe space to engage and transact. Finally, in the case of training and awareness the findings concluded that the more trained home users are about cybersecurity, the more they will be aware about device security reaffirming that an untrained and unaware home user is more at high risk to become vulnerable to cybercrime. Also, home user device security behavior is influenced by knowledge about security threats and the intentions to be security compliant. This study was also able to validate the importance of each core construct of the PMT on their impact to take protective measure against cybercrime.

TABLE OF CONTENTS

CHAPTER PAGE

CHAPTER I. INTRODUCTION 1
Problem Statement 1
Significance of the Problem 4
Research Questions 6
Research Contributions 6

CHAPTER II. BACKGROUND LITERATURE REVIEW AND THEORY 10
Protection Motivation Theory (PMT) 12
Digital Literacy 16
Device Security 18
Social Media 19
Training & Awareness 22
Internet Service Provider 24
Internet Trust 25

CHAPTER III. RESEARCH MODEL AND HYPOTHESES 27
Conceptual Research Model 28
Theoretical Development and Hypotheses 29
Threat appraisal 29
Coping appraisal 31

Internet trust 33
Device Security 34
Social Media Usage 37
Internet Service Provider 39
Digital Literacy 41
Training & Awareness 43

IV. RESEARCH METHODOLOGY 46
Research Design 46
Measurements 47
Participants and Procedure 56
Pilot Study 57

V. DATA ANALYSIS AND RESULTS 65
Sample and Demographics 65
Path coefficients and hypothesis testing 73
Main Hypotheses Study Summary: 80

VI. DISCUSSION AND CONCLUSION 82
Discussion 82
Limitations and Future Research 89
Conclusion 92

Theoretical Implications 93

Practical Implications 94

LIST OF REFERENCE 96

APPENDICES 106

VITA 109

LIST OF TABLES

CHAPTER PAGE

Table 1 Construct Summary…….....47

Table 2 Pilot Statistics Demographics……...…….....58

Table 3 Pilot Construct Reliability and Validity……....61

Table 4 Pilot Discriminant Validity……62

Table 5 Pilot Low Loadings Removed…….…….…….63

Table 6 Pilot Revised Construct Reliability and Validity.…….....64

Table 7 Pilot Revised Discriminant Validity…...……...65

Table 8 Statistics Demographics……67

Table 9 Measurement Model Construct Reliability and Validity…….....68

Table 10 Low Loadings Removed List…….……69

Table 11 Loadings List……...70

Table 12 Discriminant Validity……..72

Table 13 Path Coefficients…….....74

Table 14 Collinearity Statistics Inner List…….....79

Table 15 VIF List…….…….....80

Table 16 Hypotheses Summary…….81

LIST OF FIGURES

CHAPTER PAGE

Figure 1 The Conceptual Research Model..... 28

Figure 2 Measurement Model……....60

Figure 3 Revised Measurement Model……..63

Figure 4 Structure Measurement Model……73

CHAPTER I. INTRODUCTION

Problem Statement

It is undeniable that major advances in information technology over the past few decades have radically transformed the operations of businesses, running of governments, and habits and practices of home users. One such example is the significant growth of e-Commerce around the world, which provides a number of advantages over traditional brick-and-mortar retail, such as a lower cost structure, greater flexibility, a broader scale and scope of products and services, great transparency and accountability, and much faster transaction processing (Kabango & Asa, 2015). Technological advances also allow for connecting a variety of institutions, corporations, government at various levels, and individual consumers or home users. Although it was already in the adoption process prior to the Covid-19 pandemic, telehealth exploded during the latter event and allowed for faster and more efficient communication between healthcare professionals and patients at home. Through extensive use of videoconferencing technologies, telehealth provides important benefits to both providers and users, as well as making it possible to extend the reach of healthcare practitioners by delivering first-time access to sophisticated healthcare services to new populations of patients, particularly those in rural and remote areas (Rising, Ward, Goldwater, Bhagianadh & Hollander, 2018).

Another major development made possible by advances in Information Technology, for both producers and consumers of content, is the emergence of social media. Social media helps companies, schools, governments, and other organizations to reach out to an increasing audience of consumers with not only advertisement but also important information (as a distribution channel which can be used to share

announcement and deliver content economically to large numbers of people). In addition, social media allows individuals to reach out and connect with others, whether transactionally (as content producers do) but also on a personal level; all these processes are supported by social media platforms and applications that catalyze online social media interactions (Boyd & Ellison, 2010; Kaplan & Haenlein, 2010; Obar & Wildman, 2015; Mathur, 2019). In all these scenarios, the Internet has become an indispensable channel for the delivery of information, products, and services (Kabango & Asa, 2015). Home users access the Internet exclusively through Internet Service Providers (ISPs), which connect our individual homes, apartments, etc. to the Internet and then to these different marketplaces, platforms, or social media. As such, access to the Internet through a dedicated connection, be it wired or wireless, is fundamental for a globalized economy in which the home users have the power to decide and buy based on a free market economy. In economies at all stages of development, it is crucial to have widely available access to electronic networks and communication (Information Highway Advisory Council (IHAC), 1995a and 1995b; Keenan & Trotter, 1999).

As impressive and transformational these advances in Information Technology have been, they are not without their perils. A central issue, for both organizations and individual consumers or end users, is cybercrime. Cybercrime is a worldwide complex phenomenon which has created a number of financial and operational issues for both organizations and end consumers alike. In the United States alone, loses due to cybercrime are in excess of $100 billion (Lewis, 2013) to as much as $400 billion, while globally they may have reached up to $2.1 trillion in 2019 (Morgan, 2016). Of particular interest for this research, cybercriminals have been known to specifically target home

users, not only for direct gains, but also as intermediate steps through which they can execute more complete cyberattacks at a larger scale (Symantec Security Response, 2016; Thompson, McGill & Wang, 2017). A well-known example is the compromising of a large number of user devices ("bots") in order to create a large network of those (a "botnet") which can then be used to launch a concentrated attack at scale, typically on government or corporate critical infrastructure, through sending large amounts of spam, phishing, malware, or the conduct of a distributed denial-of-service attack, in order to overwhelm and cripple the targeted infrastructure (Markoff, 2007).

Although there is no consensus or standardization on what exactly constitutes cybercrime, and the US Federal Government does not provide a formal definition of cybercrime that distinguishes it from other criminal offenses or cyber threats (including cyber warfare and cyber terrorism) (Phillips, Davidson, Farr, Burkhardt, Caneppele & Aiken, 2022), we employ the wording offered by the United Nations as an encompassing definition of cybercrime: 1. "Any illegal behavior directed by means of electronic operations that target the security of computer systems and the data processed by them" and 2. "Any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network" (Council of Europe. Convention on Cybercrime; European Treaty Series No. 185; Council of Europe: Budapest, Hungary, 2001; pp. 1–25).

Significance of the Problem

Home users have thus become targets of interest for cybercriminals due to their lower cybersecurity sophistication, compared to corporate and government operations. Home users are particularly vulnerable to cybercrime activities such as privacy exploitation, identity theft, crimes against the machine (such as unauthorized access to bank accounts), crimes in the machine (such as storage of critical data exploitation images, SSN, and financial information), and crimes via the machine (such as email or web mediated fraud, dark web, and spam emails) (Mendoza, 2017). Cybercrime activities, such as privacy exploitation and identity theft, can have longer-term consequences and will affect many aspects of U.S. home users including the ability to apply for personal or business loans, social status, and the ability to develop a secure and successful local or international business transaction. An additional concern is that cyber-attacks are getting more sophisticated, and accurate with the targeted audience they want to negatively affect.

The constant progress of Information Technology, cyber security infrastructure, connectivity, and the endless improvements in cybersecurity software and appliances are making computer systems very complex. There is a known correlation between a computer system complexity and its security; as a computer system gets more complex, it becomes less secure (Schneier, 2000). This additional complexity in devices and computer systems as well as computer network infrastructure, including the Internet, have resulted in an increase in the frequency of targeting individual end users, and with increasingly more complex attacks (Tounsi & Rais, 2018). As a result, it is of great

importance to identify the factors that are contributing to home users becoming more vulnerable to cybercrime activities in order to be able to provide more accurate and functional solutions to this problem at the home user level and the intention to take protective measures against cybercrime.

This research seeks to identify factors which contribute to cybercrime perception and preparation in home users by using Protection Motivation Theory (PMT) as the theoretical lens for the study. The goals of this research are (1) to study the role of internet trust, trust in the ISP, and usage of social media as potential drivers of PMT drivers of intention to protect oneself from cybercrime, (2) to study the extent to which device security and digital literacy affect the abovementioned PMT drivers, and (3) to study the extent to which having been exposed to cybersecurity training and awareness efforts has an impact on the PMT drivers. The context of interest here are Internet users operating from home and outside of the boundaries of corporate environments, where teams of specialists are in charge of cybersecurity. This research, on the other hand, examines the importance of these drivers for home users who, to various extents, are responsible for providing their own cybersecurity in order to protect themselves from malicious attacks, as those described above.

This research contributes to the growing body of literature that examines the behavior of home users towards cybersecurity in the following ways: (1) it examines the relationship between PMT drivers and intentions to take protective actions against cybersecurity in the home user context, whereas much research has examined similar models in an organizational or workplace environment, where end users are not themselves directly responsible with the majority of cybersecurity efforts, (2) proposes

and examines an extension to the PMT model which considers antecedents to the core PMT constructs, in order to better understand how those core perceptions are developed in the case of home users, and (3) through the examination of both, and their relative indirect impact on intention to take protective action, helps identify which antecedents should be targeted to prompt home users to become more aware and sophisticated in their cybersecurity defenses, and take an active role in the provision and monitoring of the same. As a result, this research seeks to answer the following two research questions:

Research Questions

(1) What is the relative importance of each core construct of the PMT on their impact on intention to take protective action, in the context of home Internet usage?

(2) What are the antecedents to the core constructs of the PMT and what is their relative importance, in the same context of home Internet usage?

Research Contributions

A key contribution of this research is the identification and testing of various antecedents of the core constructs of the PMT, in the context of home Internet usage. These are of primary importance since they provide entry points through which future action could be targeted in order to prompt users to improve their cybersecurity efforts at home. These antecedents include *Social Media Usage*, *ISP Compliance*, *Internet Trust*, *Digital Literacy*, *Training and Awareness*, and *Device Security*. Of particular theoretical interest here is the role of the ISP in the home cybersecurity context. As ISPs are the sole

provider of connectivity to the online world while at home, they are in a unique position to introduce and/or enforce security services and protocols on all online traffic going in and out of a home environment through their capability to monitor traffic flowing inbound and outbound of a home, and most commonly through an networking appliances (modes and routers) which are provided by the ISPs themselves (through leasing, lease-to-own arrangements, or bundled into the provision of online access). ISPs are therefore in a position to monitor the traffic, bandwidth, and overall network utilization to and from homes (and the users which reside in them). Through the use of alerts, patterns, and thresholds, ISPs could identify and put an end to excessive malicious traffic (such as that caused by worms or spam bots) as well as filter out any suspicious traffic. As well, in response to filed complaints from owners of copyrighted content, which is distributed without permission, temporarily or permanently suspend Internet access from a particular location.

Moreover, ISPs can force their users to adopt more security on their host computers (Rowe, Reeves & Gallaher, 2009). In fact, some ISPs have started to offer security solutions in order to assist home users in better protecting themselves from cybercrime. While the specifics of these vary from ISP to ISP, they typically include Fully External Solutions (which provide users with security advice, e.g., how to set up a firewall or free products, such as antivirus software); Fully Internal Solutions (which implement increased filtering at the ISP level so that suspicious activity is addressed and potentially punished by the temporary loss of sending privileges); and Partially Internal/Partially External Solutions (where ISPs impose policies on users that cause them to play a role in preventing unwanted traffic, such as requiring customers to

approve e-mail received from unknown senders before the e-mail is delivered) (Rowe, Reeves & Gallaher, 2009). As a result of these advances in security provided by ISPs, it is possible that home users will abdicate their responsibilities on the logic, whether founded or not, that home cybersecurity of the purview of ISPs and, therefore, the users themselves should not be concerned about it. This is certainly not the case, as strong home cybersecurity requires all involved parties to take charge of these measures, but our research seeks to understand how home users view ISPs in this role. This is not an area which has received attention in extant research, and an important contribution to this work.

It is evident that cybercrime is a problem felt at all levels, including governments, corporations, and individual home users. While in their role of employees in a corporate environment users benefit from the existence of security departments and specialist which are dedicated to providing a (cyber) secure workplace, the majority of home users do not have the same level of protection and access to knowledge and skills to create the same secure environment at home. As such, it is imperative to understand what drivers home users to take actions to protect themselves from these threats, and the extent to which those drivers have more or less an impact on those intentions. This research adopts the theoretical lens of Protection Motivation Theory in order to identify the most proximate drivers of intentions to take protective action from cybercrime while in an in-home environment. Then, the research extends those drivers backwards, by theorizing factors which have an impact on the core constructs of PMT. Doing so would allow for the identification of more distal predictors of intentions to take protective action, which could in turn be used to identify targets for interventions or training programs, with the

ultimate goal of motivating home users to take stronger and more proactive measures to protect themselves, or at least minimize the effects of cybercrime.

The remainder of this work proceeds as follows. Chapter 2 provides a literature review and theoretical background on the core theory and constructs employed in this research. Then, Chapter 3 develops a research model, and associated hypotheses, for the main relationships of interest in this research. Finally, Chapter 4 discusses the operationalization of the constructs in the research model as well as data sources and analytical issues.

CHAPTER II. BACKGROUND LITERATURE REVIEW AND THEORY

While certainly a luxury when it first started to be rolled out a few decades ago, the Internet has become a necessity for most home users (Kritzinger & Von Solms, 2013). Once permanent access to the Internet became both commonplace as well as affordable, there was a marked increase in the number of home users with access (potentially reaching saturation levels), as well as the number and variety of devices (computers, laptops, smartphones, gaming consoles, and tablets) employed by home users to access online content, services, platforms, etc. With this increased use of the Internet, and all the advantages it affords to home users, it has also become an important avenue through which home users can be the target of criminal activity, particularly due to the ubiquitousness of the Internet as well the relatively low cost of committing cybercrime. As a result, home users have an increasingly greater responsibility to keep their devices and online usage protected from criminals. This is even more so the case when Internet access is "always on", home users spend more and more time online, and increasingly more of their activities (including shopping, working, etc.) are conducted over the Internet.

Given that many home users are not technologically-savvy and may not fully understand or be aware of their vulnerability to cybercrime, other parties, such as their Internet Service Providers (ISPs), may be in a better position to deploy necessary technical preventive measures and countermeasures to protect home users (or at least minimize the likelihood of) from becoming victims of cybercrime. These providers can

deploy hardware and software solutions, such as intrusion detection and prevention systems, filtering, monitoring, and software security, to protect home users from unauthorized intrusion into their systems, with potential short- and long-term consequences; an example of a short-term consequence could be gaining access to a bank account to steal savings, while a long-term consequence may involve identity theft, which can take years to clear.

Whether through direct education of home users, the deployment of technical measures by ISPs, or likely some combination of both, in order to reduce the likelihood that they will be victims of cybercrime, home users need to first understand these cyber threats or how to protect themselves against cyberattacks while using the Internet. It is therefore imperative to provide home users with the necessary support to make sure that they are cybersecure, or as much as it is reasonably possible to be.

There are several ideas and proposals regarding how an external third party, for example, an ISP, can be engaged to take over the majority of cyber security obligations for the home users (Kritzinger & Von Solms, 2013). However, there is a limit to what an ISP can do and, even if these ideas were to come to fruition (ISP liability is an open question in terms of the degree of responsibility that ISPs would need to absorb, which would likely be passed on to home users as an increase in the cost of providing access to the Internet from home), the need for home users to be responsible and in charge of their own personal security is not likely to go away anytime soon. As a result, this research seeks to examine a model of the antecedents considered by home users and how those affect their intentions to take protective action.

The rest of this chapter discusses the theoretical lens employed for this research (Protection Motivation Theory) as well as reviews research on the key constructs included in the research model developed in detail in Chapter 3.

2.1. Protection Motivation Theory (PMT)

Protection Motivation Theory (PMT) has been used to explain in what way individuals are motivated to react to warnings about probable threats or dangerous behaviors (Rogers, 1975, 1983) and it is one of the most applicable theories in explaining individual intention to actively become involved in cybersecurity protective actions (Ifinedo, 2012). PMT has proven its value as a reliable framework to study the cognitive processes that take is been executing when individuals are faced with a serious and trustable threat in a cybercrime situation (e.g.Herath and Rao 2009; Lee and Larsen 2009; (Crossler and Bélanger 2014; Dang-Pham and Pittayachawan 2015; Tsai et al. 2016). According to Norman, Boer, and Seydel, PMT states that two cognitive processes influence people's protection motivation (i.e., the intention to perform a recommended action or behavior): threat appraisal and coping appraisal (Norman, Boer, and Seydel 2005).

Threat appraisal is a cognitive process that assesses the seriousness of a particular risk. In other words, it evaluates severity of a risk as it is perceived by the individual as well as the perceived vulnerability or exposure of the individual to that specific risk. Moreover, vulnerability is another important executor against home users cognitive process in order to take protective measure against cybercrime. In this study, the goal is

to identify the threat appraisal cognitive process stated in the PMT which is the perceived vulnerability to cybercrime; the definition and concept of "vulnerability" change depending on the context according to (Adger, 2006). To compound this issue further, cyber-attackers increasingly pick the easy targets in order to minimize their effort (Thompson, McGill, & Wang, 2017). Cyber-attacks such as the record 1.2 Tbsp Denial of Service attacks reported in late 2016 by Symantec® Security Response, 2016, demonstrate that malicious actors have their sights set on the home computer sector, not just as the eventual targets, but even as instruments in larger attacks (Thompson, McGill, & Wang, 2017). Kaspersky's® another software security company, reported in their "threat evolution report" provides a more detailed insights into the level of the issues encountered in the mobile arena too (Thompson, McGill, & Wang, 2017) In Q1 2016 over 2 million malicious installation packages were detected by their mobile telemetry. This was an increase of 11 percent over the previous quarter, and 23 percent over Q3 2015(Kaspersky Labs, 2016). The trend is continuing, with no signs of slowing. The same report highlights the growth in attacks on mobile banking apps. For example, a single strain of the Marcher Trojan was attacking nearly 40 mobile banking apps in Europe (Thompson, McGill, & Wang, 2017). This suggests that home users are increasingly at risk when they transact on the Internet. (Thompson, McGill, & Wang, 2017). Moreover, the concept of vulnerability has been a powerful analytical tool for describing states of susceptibility to harm, powerlessness, and marginality of both physical and social systems, and for guiding the normative analysis of actions to enhance well-being through reduction of risk (Adger, 2006). In general, home users can describe, or they will be able to provide some states of susceptibility and become more aware that

they somehow are vulnerable to cybercrimes. For the purpose of this study, the concept of vulnerability will be exclusively applied to cyber-attacks and to the consequences of these attacks, in other words, cybercrimes. In cybersecurity, the concept of vulnerability is basically a weakness or a security breach including a user's lack of digital literacy and cybersecurity training and awareness (like password complexity), minimum, or null device security that can be exploited by cybercriminals to gain unauthorized access to a computer system or operating systems. After exploiting a vulnerability, a cybercriminal can run different cyber-attacks such as malicious code, install malware, and even steal sensitive data or impersonate users' email, accounts, and other sensitive critical data (Abi Tyas Tunggal., 2022)

The coping appraisal, on the other hand, focuses on an individual's capability to cope with or avoid the risk in question (Rippetoe and Rogers 1987), through the following process: First, it incorporates an evaluation of the efficacy of proposed countermeasure(s) in stopping the threat, also known as response-efficacy (or the efficacy of a potential response to the identified thread); second, self-efficacy is assessed, which comprises the notion that an individual is competent of executing the necessary actions to diminish the threat (Norman, Boer, and Seydel 2005). According to Rogers (1983), both appraisals can be initiated by several sources of information or antecedents, such as observational learning, personality variables, or prior experience with the threat under consideration. The outcome of the appraisal processes is the intention to initiate, maintain, or refrain from coping behaviors (Floyd, Prentice-Dunn, and Rogers 2000). In order to be able to accurately understand cybersecurity behaviors, this study applied the PMT framework to the study of its core perceptions, and their antecedents, in the context

of home users. Moreover, PMT was developed on the principle that an individual secures the information as a relevant aspect of an effort to decrease cybersecurity threats and risks. Furthermore, this theory has been applied in other studies focused on cybersecurity.

There are some studies that have used the PMT framework in the past, they have made important and positive contributions to the research focused on cybercrime specifically in cyber security measures against malware, scams, and cybercrime in general (Martens, De Wolf, & De Marez, 2019), cybersecurity policy awareness (Li, He, Xu, Ash, Anwar, Yuan, 2019), cybersecurity risks behavior (Debb, & McClellan, 2021).

Some studies just focused on malware protection due to the fact that is one of the most concerning attacks when using devices such as laptops, tablets, and smartphones at home (Dang-Pham, & Pittayachawan, 2015) Other studies have a different approach focusing more on the effects of antecedents and mediating factors on cybersecurity protection behavior (Li, Xu, & He, 2022). The studies provided evidence of the effectiveness of using the Protection Motivation Theory framework; it also helps explain why knowledge is a key factor influencing the decision-making cognitive process (Debb, & McClellan, 2021).

The PMT model with extended hypotheses further explains the cognitive process and how these factors change their effects from one context to another (Dang-Pham, & Pittayachawan, 2015). Academics and practitioners are strongly recommended to increase awareness in developing the intention to take protective measures against malware and cybercrime. In all those studies, the extended PMT conceptual model has provided a clear path to enhance IT security training and awareness, specifically in

helping home users effectiveness to avoid malware and cyberattacks in general by exploiting the PMT cognitive effects (Dang-Pham, & Pittayachawan, 2015). That is the huge contribution of the PMT framework in the use of cybersecurity behavior, cybersecurity risk, and cybercrime in general.

2.2. Digital Literacy

Digital literacy is a set of skills required by 21st Century individuals to use digital tools to support the achievement of goals in their life situations (Reddy, P., Sharma, B., & Chaudhary, K., 2020); together with knowledge about cybersecurity, it represents a fundamental key factor for an inexperienced home user (Fu, 2013). Additionally, Information and communication technologies (ICTs) have become an important tool for home users in the implementation and distribution of digital literacy. ICT can now be defined as the use of digital technologies to generate, distribute, collect, and administer information and communicate in real-time (instant messaging, voice over IP (VOIP) and video conferencing) among others (tech terms, 2018; Sarkar, 2012) and, as such, digital literacy skills are of central importance to the effective use and operation of ICTs. Moreover, ICTs have become an essential part of life for the home users of our digital era, primarily because these modern technologies are playing an important role in improving the quality of living (Reddy, Sharma, & Chaudhary, 2020).

In this new digital era, it is imperative that home users know how to use the technology to prepare them for the next challenges and, of central importance for this

research, how to defend themselves from these new cyber-attacks. Home users can potentially become overwhelmed by multiple new concepts and innovations, as we become an "e-permeated society" (digital society), as well as and digital tools and technologies like mobile devices, computer-aided manufacturing tools, communication tools, smart learning cities, and new social media platforms, etc. have appeared (Reddy, Sharma, & Chaudhary, 2020). Moreover, the implementation of updated online platforms to develop the necessary knowledge for home users. Furthermore, the implementation of AI and VR, and other methodologies to help distribute and successfully deliver the necessary knowledge, as a result, the home user will be able to have a bigger probability to prevent cybercrimes against themself. (Shute, & Ke, 2012).

Some researchers have shown that digital literacy was an important topic of study during COVID-19 pandemic since technology and the internet specifically played an important role in keeping home users' families safe by reducing the physical interaction with others for example at the hospitals; health care professionals increased the use of Telehealth (Nurhayati, Musa, Boriboon, Nuraeni, & Putri, 2021) The COVID-19 pandemic basically forced individuals to learn new technologies and computer basic skills like the use of internet web-based solutions (Nurhayati, Musa, Boriboon, Nuraeni, & Putri, 2021). However, the lack of basic skills on technology can compromise individuals' privacy and increase the gaps for individuals that cannot possess the opportunity to access reliable internet connection, devices, or their technological literacy limitations (Hart, Turnbull, Oppenheim, & Courtright, 2020).

2.3. Device Security

Device Security has become one of the most important factors for home users when it comes to cybersecurity, due to the fact that "security begins at home" (Thompson, McGill, & Wang, 2017). Personal computing home users are vulnerable to information security threats, as they must independently make decisions about how to protect themselves, often with little understanding of technology or its implications (Thompson, McGill, & Wang, 2017). Moreover, it is well-known that the home internet has been under attack for many years, since the internet emerged and became accessible for all home users, the home internet user or home user has been dealing with a hostile cyber-space environment full of potential cyber-attacks and vulnerabilities on their computers and other devices. These attacks have been increasing at an alarming rate and have inflicted severe damage, both psychological and financial, on home users. Cybercriminals exploit the vulnerabilities of home user's personal computer, as a result, these cyberattacks have the potential to neutralize and destroy the critical infrastructures of entire countries (Claar, & Johnson, 2012). Therefore, device security is extremely important in order to protect home users and decrease vulnerability to cybercrimes.

Previous researches related to security studies that adapted and extended the PMT framework to the home computer security domain, have found that the intentions to perform security behaviors were shown to successfully and it significantly influence the security behavior for all home users devices (Thompson, McGill, & Wang, 2017) Nowadays, home users are moving from desktop computer to different types of mobile

devices, and that is basically the reason that PC security evolve and extended to device security with new features in order to be able to cover all devices that are currently in use for home users (Thompson, McGill, & Wang, 2017).

There are many device security suite solutions in the market available for home users. There are a variety of anti-virus (AV) software from different vendors which provide a variety of features and levels of protection depending on the home user's needs. For example, Norton AV offers reputation-based security, which classifies an unknown program based on its reputation among Symantec's community of users (Sukwong, Kim, & Hoe, 2011). Other AV solutions, such as Kaspersky AV, offer in-the-cloud security, which offloads the data needed to detect malware to the provider's servers (Sukwong, Kim, & Hoe, 2011). Moreover, this feature helps free up space needed in users' computers due to the growth in virus definitions. It also improves the response times since users can immediately access information about malware as soon as it is identified (Sukwong, Kim, & Hoe, 2011). In addition, there are some ISPs that have started to offer internet security suite solutions for their customers; these security suit solutions from the ISP will help to monitor the internet network traffic and therefore identify some suspicious activities in the home user's personal computers and potential risks in social media usage.

2.4. Social Media

Social media platforms have been changing home users' lifestyles for both personal and business matters for the last few years. There is no doubt that social media is

important to keep home users and businesses connected and informed. Social media are online interactive platforms that emphasize information-sharing and relationship building oriented among firms and home users (Labrecque, 2014; Ryden, Ringberg, & Wilke,2015). Firms that leverage social media are better able to improve customer-firm relationships and firm sales (Giamanco & Gregoire, 2012; Kumar, Bezawada, Rishika, Janakiraman, & Kannan, 2016, Mathur, 2019). As a result, social media usage has exploded beyond its origins in personal sharing and connections and has become a platform of central importance for both business and consumers. However, there are important security features that home users might take into consideration before using social media platforms, for example, the increasing popularity due to its ability to make people share personal content with friends and the world, it is important to be aware of the content that home users shares such as photos, feelings, videos, which bears a high-security concern (Almansoori, Alshamsi, Abdallah, & Salloum, 2021). Additionally, in criminology research, there is a new approach that can help to identify another vulnerability to cybercrime through social media use; Problematic Social Media Use (PSMU) (Marttila, Koivula, & Räsänen, 2021) is a habitual pattern of excessive use of social media platforms. Several past research has suggested that PSMU predicts risky online behavior and negative life outcomes, but the relationship between PSMU and cybercrime victimization is not properly understood (Marttila, Koivula, & Räsänen, 2021). As an example, there are some social media (for example, TikTok) that have been dramatically increasing the risk of cyber-attacks for home users by collecting specific and highly sensitive data, with a potential high risk of violation of privacy. Furthermore, it is estimated that there is a cyber-attack every 39 seconds. (Haung & Madnick., 2020). It is

simply amazing the number of users around the world using the app called TikTok, the issue with this app is that it collects specific sensitive data like many other smartphone apps so that there is a high risk of violation of privacy (Haung & Madnick., 2020). Furthermore, there are other studies focusing on both physical and social systems normative analysis of actions to enhance well-being through reduction of risk (Adger, 2006), there is a new discipline in psychology called "cyberpsychology" which is the study of human behavior on the continued and excessive use of the internet and technology specifically in online behavior, personality changes; the change in human behavior when using social media platforms. (Ancis, 2020). Additionally, researchers have found that humans are changing their behavior when they are online or interacting with other humans through cyberspace than face-to-face. The studies remark five factors (neuroticism, emotional stability, extraversion among others), but there are other social psychological factors affecting people's live i.e., cyberbullying (very common in Youngs individuals) among other online criminal activities (Joinson, 2007). Other empirical studies have also found that there is a drastic increase in the use of smartphones in the general population in the United States. As a consequence, this increase in access to the internet and social media platforms through smartphones has created a situation in which home users are now generally more exposed to cyber-attacks and as a result more vulnerable to cybercrimes. (Park, Yi, & Jeong, 2014).

In this research, one of the goals is to clearly identify if excessive social media usage actually increases the trust in the internet when using the platform and also if this frequency of social media usage increase the vulnerability to cybercrimes in home users, as many researchers have proposed that the outcomes of social media use depend on the

way platforms are used and that the negative outcomes are concentrated among those who experience excessive social media use (Kross et al., 2020; Wheatley & Buglass, 2019) (Almansoori, Alshamsi, Abdallah, & Salloum, 2021, June). As a result, understanding the relationship between extent and frequency of social media usage and vulnerability to cybercrime for home users, given the penetration that social media platforms have reached at all levels of society, is of central importance. In this research we make the connection between social media usage, trust on the internet, and core perceptions in PMT.

2.5. Training & Awareness

There are many different training & awareness programs that cover many well-known vulnerabilities to cybercrime and enforced the application of the knowledge learned about cybersecurity; this has become a scheduled task for many Information Technology departments and organizations' security compliance. For example, the Cybersecurity Awareness Training Model (CATRAM) provides a substantial foundation for the implementation of any personal and organizational cybersecurity awareness program and was created to deliver cybersecurity awareness training to specific groups within any organization (Sabillon, 2022). CATRAM was designed to deliver awareness training for the members of the Board of Directors, Top Executives, Managers, IT staff, and is also applicable to end-users or home users (Sabillon, 2022). There are also other training and awareness programs which were designed to help home users, as these

personal internet users are becoming more vulnerable to security threats and cyber-attacks due to the use of information communication technologies in combination with an overall low level of technological sophistication (Furnell et al., 2007, Sophos, 2009, Symantec, 2007).

The vulnerability to information security threats and cyber-attacks are the result of many personal internet users that do not possess the information, knowledge, and experiences about cybersecurity, in other words, the necessary training and awareness to understand and protect their PC and therefore their personal information (Kritzinger, & von Solms, 2010). In this study, one of the goals is to identify the proper training & awareness program for home users that will help decrease the risk levels of vulnerability to cybercrime. An example of a program is the E-Awareness Model (E-AM), in which home users can acquaint themselves with the risks involved in venturing into cyberspace. The E-AM consists of two components: the awareness component housed in the E-Awareness Portal, and the enforcement component (Kritzinger, & von Solms, 2010). In addition, there are Virtual Reality (VR), Artificial Intelligence, computerized software, and mobile device applications that all together can be used in the implementation of training, awareness, and educational programs for individual home users. Artificial Intelligence can also be implemented at the cybersecurity stage to help with education, training, and awareness. (Feldon, & Kafai, 2008). Governments have begun exploring using the E-Awareness program to deploy, monitor, and enforce, the policies through the Internet Service Provider (ISP). (Kritzinger, & von Solms, 2010).

2.6. Internet Service Provider

Internet Service Providers (ISPs) play an important role in cybersecurity. ISPs have increasingly begun offering new services oriented towards cybersecurity. For example, as the sole channel through which home users gain access to the internet, ISPs are able to monitor and observe home users' computer network traffic. This allows ISPs to create their own rules, alerts, and internet use compliance which they can either recommend or, possibly in the future, impose on home users. Additionally, ISPs oversee assigned public IPs to their appliances and, by doing this IP assignment or leasing, the home user becomes less vulnerable to cybercrime. Moreover, several ISPs are offering security services as well as training and awareness courses for home users in addition to only providing internet access.

ISP security solutions can be categorized into three main categories of implementation and deployment in order to enhance their home user's security: (1) Fully External, which provides users with security advice (e.g., how to set up a firewall) or free products (e.g., antivirus software) (Rowe, B., Reeves, D., & Gallaher, M., 2009); (2) Fully Internal, which implements increased filtering at the ISP level so that suspicious activity is addressed (e.g., a user or group of users is investigated and possibly loses sending privileges temporarily) (Rowe, B., Reeves, D., & Gallaher, M., 2009), and (3) Partially Internal/Partially External, which imposes policies on users that cause them to play a role in preventing unwanted traffic (e.g., an ISP forces customers to approve e-

mail received from unknown senders before the e-mail is accepted) (Rowe, B., Reeves, D., & Gallaher, M., 2009).

In this study, one of the goals is to identify if the implementation of ISP's security services, and the beliefs by home users that ISPs are playing an active role in their protection from cyberattacks, will help to decrease vulnerability to cybercrime. There are already several countries which are developing, implementing, and creating alliances with their local ISPs in order to improve cyber security. For example, in 2010, Australia created a voluntary code of practice for ISPs, asking that they maintain a system for notifying infected computers, keep up-to-date threat information, provide resources for end users, and use a reporting mechanism to inform the government about severe threats (Internet Industry Association 2010) (Rowe, B., Reeves, D., & Gallaher, M., 2009). Japan has already seen positive impacts from its "Cyber Clean Center," a collection of over 70 ISPs dedicated to improving cyber security (OECD 2010) (Rowe, B., Reeves, D., & Gallaher, M., 2009).

2.7. Internet Trust

Trust in the safety of the internet has become an important topic when using the different internet platforms available for businesses in general and more importantly for home users (Mathur, M. (2019). According to (De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K., 2022) We perceived the concept of trust as "the belief that the other party will behave in a socially responsible manner" (Pavlou 2003, 106). In other words, the belief that the whole internet experiences are safe, and that the individual involve in the online interaction will act in a responsible manner like their peers (Wang, & Emurian,

2005). E-commerce and social media platforms usage are the most affected when cybersecurity breaches are reported, the trust on the internet including social media platforms and some other firms are damaged (Mathur, M., 2019). In fact, some studies have shown that the lack of trust on the internet (online) has become one of the most notable barriers to home users for engaging in e-commerce transactions (Wang, & Emurian, 2005), the fact that in order to complete any transaction on the internet a standardized step by step process must be follow, this process includes the input of a variety of personal data like demographics and bank or credit card information on web-based forms, after that, all of this information is shared with the merchants.

Internet (online) trust has been subject of multiple studies. According to (Wang, & Emurian, 2005) based on the literature from other research Kim, Song, Braynov, and Rao (2001) they have divided the factors of internet(online) trust into six which are: information content, product, transaction, technology, institutional, and consumer-behavioral dimensions. Furthermore, there are three main characteristics for internet trust that can be taking in consideration: 1.- Trustor and trustee, 2.- vulnerability, 3.-Subjective matter, and 4.- Produced actions (Wang, & Emurian, 2005)

CHAPTER III. RESEARCH MODEL AND HYPOTHESES

Cybersecurity is a complex and extended discipline emerging from the complex interaction of both human factors and technology. Most security vulnerabilities are the result of biases, ignorance, poor judgment, lack of digital literacy, and mistakes by end users (Sulaiman, Fauzi, Hussain, & Wider., 2022). In this research, I will apply the foundations of Protection Motivation Theory (PMT) to the study of cybercrime, as well as expand the model upstream by examining antecedents to the core constructs of PMT. For the purpose of this study, cybercrime is defined as "any crime that is facilitated or committed using a computer, network or hardware device" (Gordon and Ford 2006, 14). The complete research model studied in this work is presented in Figure 1. The core relationships in the PMT will be elaborated first, e.g., threat appraisal (perceived severity to cybercrime and perceived vulnerability to cybercrime) and coping appraisal (perceived self-efficacy to cybercrime and perceived response-efficacy), followed by the hypothesized relationships and effects between these constructs and other antecedents to those included in the research model. The complete research model has a total of fifteen hypotheses which are explained in detail below; structurally, it is comprised of one ultimate dependent variable (Intention to Take Protective Measures), the core PMT constructs, six antecedent variables (device security, training and awareness, digital literacy, internet trust, ISP compliance, and social media), and control variables (age, gender, education, and past victim to cybercrime). This research seeks to answer the following research questions (RQ):

RQ1: What is the relative importance of each core construct of the PMT on their impact on intention to take protective action, in the context of home Internet usage?

RQ2: What are the antecedents to the core constructs of the PMT and what is their relative importance, in the same context of home Internet usage?

Conceptual Research Model

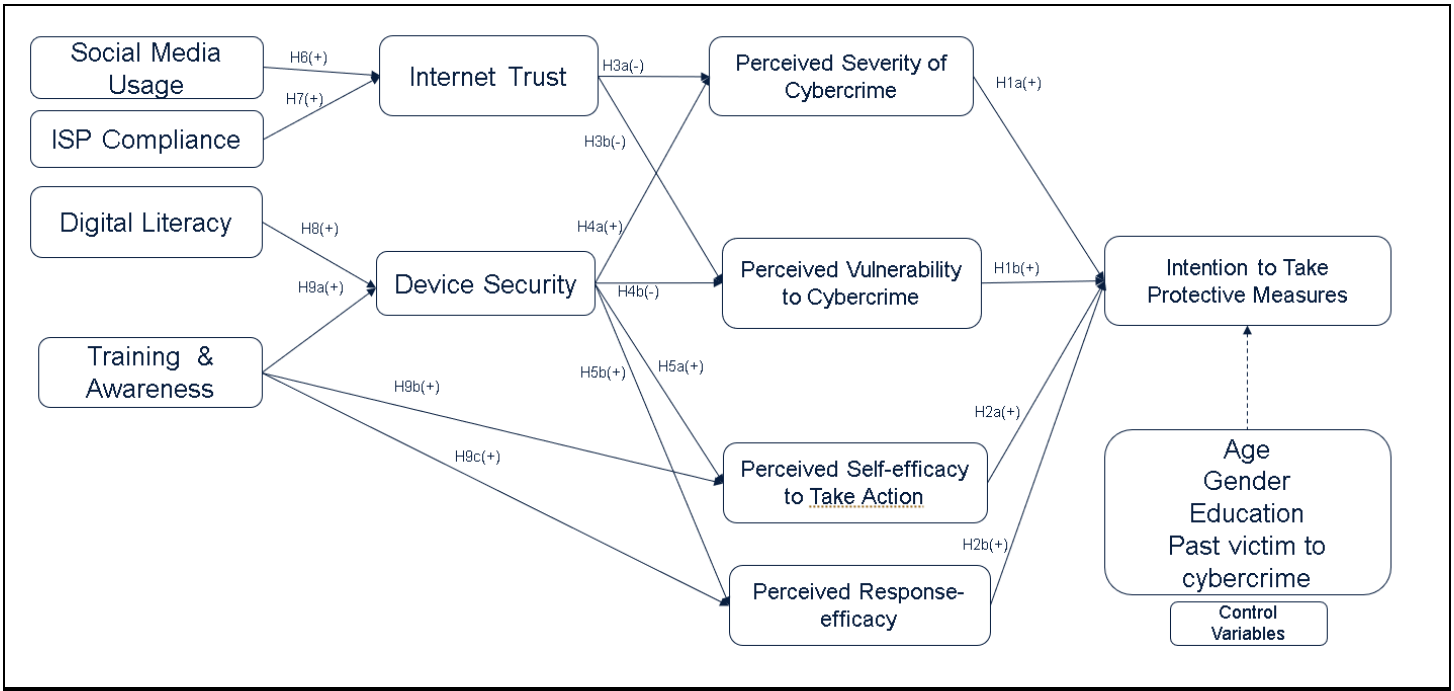

Figure 1 The Conceptual Research Model

Theoretical Development and Hypotheses

3.1. Threat appraisal

PMT states that threat appraisal is determined by perceived severity and perceived vulnerability of a particular threat with which the individual is faced (Norman, Boer, and Seydel 2005). Threat appraisal is a cognitive process that impacts intention to take protective actions. *Perceived severity* implies the level of understanding or awareness about how dangerous the consequences of some events are perceived by an individual (De Kimpe, Walrave, Verdegem, & Ponnet, 2022). While cybercrime incidents can be catastrophic and extremely severe for some home users, others may measure the threat or the consequences of a given instance of cybercrime completely different in terms of severity (Ng, Kankanhalli, and Xu 2009). Other research shows that perceived severity to cyber-attacks, for example, related to malware threats, increases home user motivation to perform or take protective measure to malware avoidance behavior (Dang-Pham and Pittayachawan 2015). There are other findings from research on cybersecurity that also provide evidence of the consistency of these findings; for example, Anderson and Agarwal (2010) showed that being concerned about security threats resulted in a more positive attitude towards taking protective measures or action. Another study by Crossler and Bélanger (2014) showed that perceived severity has a positive influence on implementing security practices.

Based on the tenets of PMT and these results, a positive relationship between perceived severity and intention to take protective actions is expected, such that individuals that perceive the severity of a cybersecurity threat to be high will also be more likely to want to take actions to protect themselves from cyberattacks. The following hypothesis is thus proposed:

H1a: Perceived severity of cybercrime will be positively related to the intention to take protective measures against cybercrime.

The second cognitive process involved in threat appraisal under PMT involves *perceived vulnerability,* or the assessment of the probability of being involved with threating events, such as becoming a victim of cybercrime (Infinedo 2012). This assessment considers the extent to which home users sense the threat and feel a lack of preventive measures and actions against cybercrime (Vance et al., 2012). Past research shows that individuals that are able to perceive an event as a threat will likely change their behavior towards that threat or negative event, with the extent of this change or adaptation dependent on the level of risk perceived by an individual (Ifinedo 2012) In other words, the more intense the perceived threat the greater the increase in motivation to avoid the threat (Liang and Xue 2010). For example, in the specific case of perceived vulnerability to email safety, this perception of vulnerability to infected email attachments attack (such as phishing), has been shown to be positively related to computer security behavior (Ng, Kankanhalli, and Xu 2009). Generally, there is a positive relationship between perceived vulnerability to cybercrime and protection motivation (De Kimpe, Walrave, Verdegem, & Ponnet, 2022). Therefore, as a result,

home users will act based on their perception of vulnerability and take measures against cybercrime; individuals who perceived themselves to be more vulnerable to cybercrime are expected to show higher levels of intention to take protective actions as a result. Hence, I hypothesize:

H1b: Perceived vulnerability will be positively related to intention to take protective measures against cybercrime.

3.2. Coping appraisal

According to PMT, the cognitive process of coping appraisal serves to evaluate the preventive measures that home users can take against a particular threat; here, against the threat of cybercrime. These preventive measures depend on individual ability and resources available to undertake those courses of action. For the purpose of this study, *self-efficacy* refers to an individual perception of the skills and abilities necessary to be able to apply or implement cybersecurity and information security protective measures. Examples of these preventive and protective measures include the installation of intrusion detection and intrusion prevention systems, or other device security software (e.g., antivirus, firewall, antimalware, web protection, track removers, etc.). Previous studies have showed that perceived self-efficacy is a valuable predictor of individual cybersecurity or information security behaviors (Ng, Kankanhalli, and Xu 2009; Crossler and Bélanger 2014; De Kimpe, Walrave, Verdegem, & Ponnet, 2022) and of their intention to take protective measures against cybercrime (Ifinedo 2012; Dang-Pham and Pittayachawan 2015; Hooper and Blunt 2020). In other words, perceived capability to implement a specific behavior against cybercrime will make it more likely that such

actions will be implemented, and that those individuals will intend to do so. As a result, higher levels of self-efficacy are expected to be related to higher intentions to take protective action. Hence, the following hypothesis is offered:

H2a: Perceived self-efficacy will be positively related to intention to take protective measures against cybercrime.

The second mechanism of the coping appraisal process involves the construct of *response-efficacy*. Preventive and protective measures against cybercrime should be perceived as effective and feasible solutions to protect home users before those are interested in implementing them, and this perception is expected to affect subsequent behavior (Rippetoe and Rogers 1987). The relationship between perceived response-efficacy and intention to take protective actions has received extensive empirical support in the context of cybersecurity measures (Lee and Larsen 2009; Ifinedo 2012; Dang-Pham and Pittayachawan 2015; Tsai et al. 2016; De Kimpe, Walrave, Verdegem, & Ponnet, 2022). Individuals who perceive potential actions and measures against cybercrime to be efficacious in addressing that threat will exhibit higher levels of intention to take those actions. As a result, the following hypothesis is offered:

H2b: Perceived response-efficacy will be positively related to intention to take protective measures against cybercrime.

3.3. Internet trust

This research seeks to extend the basic framework of the PMT by examining antecedents to the core constructs in the theory. One such antecedent is the construct of *internet trust*, which has been extensively studied in the Information Systems literature, as well as in relation to PMT (De Kimpe, Walrave, Verdegem, & Ponnet, 2022). For the purpose of this study, internet trust is defined as 'the belief that the other party will behave in a socially responsible manner' (Pavlou 2003, 106). In other words, it involves whether home users expect and believe that the internet is safe for their daily activities and that all the users involved in the same transactions or interactions in the same platforms and/or operations on the internet will act in a responsible, respectful, and ethical manner toward their peers (Wang and Emurian 2005). Trust is considered to be the counterpart of perceived risk (Riek, Böhme, and Moore 2014; De Kimpe, Walrave, Verdegem, & Ponnet, 2022) and in fact reduces the amount of risk that is perceived (Pavlou 2003). In performing risky online acts, such as online banking, social media, ecommerce activities, and the use of other platforms that home users used the most for daily activities, trust serves to alleviate existing uncertainty about the outcomes of those activities (Montazemi and Saremi 2013). The extent to which home users trust the internet is expected to negatively relate to their perceptions of vulnerability and severity, since the more users trust the internet, the less they are likely to perceive it as a dangerous space (De Kimpe, Walrave, Verdegem, & Ponnet, 2022). As a result, the following relationships are hypothesized:

H3a: Internet trust will be negatively related to perceived severity of cybercrime.H3b: Internet trust will be negatively related to perceived vulnerability to cybercrime.

3.4. Device Security

A second antecedent of interest in the research model is the construct of *device security*; specifically, the construct is defined as "computer security solutions available in the form of anti-virus, anti-spyware, and firewall software, etc." (Claar, C. L., & Johnson, J., 2012). In this research, device security includes all security hardware and software which can be installed and deployed in any device used to access the internet and perform any activities online. While hardware devices and security solutions are possible (e.g., dedicated firewalls), in the context of home users most security actions and solutions are likely to be implemented through software, whether as part of the operating system of a device or through external, third-party apps.

The internet has provided a great opportunity for home users to enhance productivity, communication, and entertainment. On the other hand, the internet has also provided the opportunity for cyber-criminals to attack vulnerable home users (Claar, C. L., & Johnson, J., 2012). Therefore, the implementation of comprehensive device security (software and/or hardware) will decrease the risk of becoming vulnerable to cybercrimes. While home users are taking advantage of the internet without malicious intentions, the same technological advances have also provided an opportunity-rich environment for

criminals and others with malicious intent. Moreover, cybercriminals increasingly target and seek to exploit computer users who do not adequately protect themselves from the ever-increasing number of cyber threats (Claar, & Johnson, 2012). Using device security solutions available in the form of anti-virus, anti-spyware, and firewall software in addition to ensuring that operating systems are properly updated provides home users with effective protection from these online threats, or at least reduces their likelihood to a manageable state (Claar, & Johnson, 2012).

Since device security takes into account the extent to which home users have implemented security measures in their devices, it is expected that it will impact the PMT constructs involved in the threat assessment process. Specifically, those individuals who have gone to greater lengths in order to add or enable protective measures in their devices are more likely to perceive that the severity of cybercrime is higher, or they would not have otherwise spend the additional time, effort, and money, in implementing more security measures; therefore, a positive relationship between both constructs (device security and perceived severity) is expected. On the other hand, those individuals who have implemented those measures (e.g., those exhibiting high levels of device security) are more likely to perceive that they are better protected as a result, and thus feel less vulnerable to cybercrime; conversely, those who have taken fewer measures are more likely to feel more vulnerable. Based on these, the two following hypotheses are offered:

H4a: Device security will be positively related to perceived severity of cybercrime.

H4b: Device security will be negatively related to perceived vulnerability to cybercrime.

Device security is also expected to have an impact on the two constructs related to the coping process in PMT, self-efficacy and response-efficacy. Device security will have a positive impact on both self- and response-efficacy perceptions. Regarding the former, home users with higher levels of device security will naturally exhibit higher levels of self-efficacy when it comes to taking action to protect themselves from cyberthreats; that is, a greater belief that they can "search, install, configure, and maintain the device security software on their computer devices (Claar, & Johnson, 2012). Since experience in the performance of a task is the primary determinant of self-efficacy beliefs, home users who have implemented more device security measures will have a greater experience in working with and operating those than home users who have implemented fewer measures, and as a result exhibit higher levels of self-efficacy. Regarding response-efficacy, since the construct centers around the posited efficacy of possible responses to deal with perceived threats, as one of the core processes in PMT, then those home users who have implemented more device security measures are more likely to believe they are better equipped to handle potential cyberthreats, and thus exhibit higher levels of (perceived) response-efficacy. Taken together, the following two hypotheses are offered about the role of device security in the coping aspect of PMT:

H5a: Device security will be positively related to perceived self-efficacy.

H5b: Device security will be positively related to perceived response-efficacy.

3.6. Social Media Usage

There is a significant increase in home users' social media usage (Perrin, 2015). For the purpose of this study, it will determine that 'social media is a group of internet-based applications that build on the ideological and technological foundations of Web 2.0, and that allow the creation and exchange of user-generated content' (Rosen, Whaling, Carrier, Cheever, and Rokkum, 2013). In addition, the purpose is also to study the extent of social media usage or the frequency of home users investing their time on social media platforms. The study is also investigating the perceived trust in the safety of the internet and specifically in social media platforms.

Research has shown that the increase in social media usage is noticeable and has affected United States home users in different layers such as demographics, gender, age, socio-economic background, racial and ethnic, and community differences and others (Perrin, 2015). Nearly two-thirds of American adults (65%) use social networking sites, up from 7% when Pew Research Center began systematically tracking social media usage in 2005(Perrin, 2015). Moreover, according to (Perrin, 2015) the growth of social media has affected or changed the regular way home users interact with such things as work, politics, and political deliberation, as well as communications patterns around the world. Additionally, it has also affected or changed the way people receive, process, and share information about persona and critical information such as health, civic life, news consumption, neighborhoods, adolescent life, parenting, dating, and even family's level of stress (Perrin, 2015). In other words, more home users accessing and using social media

for different purposes have also increased the amount of “internet users” who had adopted those social media platforms.

Social media is undoubtedly one of the most innovative ideas of the use of technology advances, generating a massive impact in our society and of course to home users by facilitating person-to-person communication for example sharing content, pictures, and sounds (Akram, & Kumar, (2017). Some studies have found a positive effect of social media on society that also benefits home users such as connectivity which is recognized as the first and most important benefit, another positive effect of social media is towards education, social networking provides multiple benefits of connectivity for students and professors, another positive effect of social media is on healthcare which contributes in connecting health care professionals with their patients through the internet online web-based systems basically anywhere and anytime the service was needed.

During COVID-19 pandemic, one of the most used forms of communication technology today appears to be social media platforms (Pennington, 2021). According to (Auxier & Anderson, 2021) the social media use in 2021 report mentioned that 7 out of 10 say that they started to use social media in the last 12 months.

These findings strongly suggest that the massive increase in social media usage can be perceived as a positive effect on home users' trust in internet safety when using social media platforms. Therefore, with this finding in mind, I hypothesize:

H6: Social media usage has a positive effect with the Internet Trust

3.7. Internet Service Provider

Access to the internet has gone from being a luxury to becoming an essential service for home users, with the vast majority of them (in the United States) enjoying broadband-level speeds and “always on” conn. Access to the internet private corporations known as Internet Service Providers (ISPs, such as Comcast, AT&T, or Verizon, to name a few). As there is no alternative way for home users to gain access to the internet except to contract the service from an ISP, these organizations in effect are the sole point of entry from the home to the Internet.

As a result, ISPs play a major role in the quality of access to, and usage of the Internet enjoyed by home users. Moreover, they are in a key position to provide an additional layer of protection to that implemented by home users themselves. While the majority of home usage of the Internet has traditionally been for browsing, shopping, social media usage, and entertainment, following the advent of the Covid-19 pandemic, most home users (and their families) found themselves also working and/or attending classes from home as well, which greatly expanded the extent and scope of internet usage, but also opened up additional opportunities for cyberthreats to arise (as a result of this significance increase in usage). Along with increases in cyber activity come increases in cyber threats, attacks, and incidents (Kritzinger, & Von Solms, 2013). Many home users are not technology savvy and, therefore, do not understand these cyber threats or how to protect themselves (and their information) while using the internet. Hence, it is vital that home users be assisted to ensure that they are “cyber secure”. (Kritzinger, & Von Solms, 2013). Over the past few years, Many ISPs have been changing their role

from passive to active against cyber-attacks and cybercrimes. Some ISPs have started to offer additional security services or solutions for end-users or home users (Mellor, 2006), with some ISPs in the United States and abroad offering "fully internal" services to business users. For example, BT began to offer a service that involved robust e-mail scanning (Mellor, 2006). ISPs such as Comcast have also tried imposing penalties on their customers who allow zombies and other cybersecurity risks to operate on their network (Rowe, Reeves, & Gallaher, 2009). Additionally, there is an initiative in the Unites States government to work in partnership with ISPs in the enforcing and implementation of better security solutions in parallel with home user's device security, training & awareness programs, social media usage monitoring, and time limits among other useful services offered via ISPs security suites (Nagest, 2009). As part of this initiative, the U.S. government solicited secure Internet connections from ISPs through the Trusted Internet Connections Initiative (Nagest, 2009); this would provide fully internal security services to U.S. government agencies. AT&T was the first provider of such services (Rowe, Reeves, & Gallaher, 2009).

Home users may have the opportunity to add a second security layer by allowing or adding the security services that some ISPs started to offer (and which may become mandatory, or at least strongly encouraged, in the future). Home users can then tap into the expertise of ISPs to provide sophisticated solutions to many cybersecurity issues, while ISPs also reduce their exposure to risks arising from unmonitored activities by home users. Given these developments, and the fact that ISPs control the single point of access to the Internet for home users, it is likely that home users have developed a belief that cybersecurity (or at least some aspects of it) is something that is actively managed by

their ISPs (or, possibly, something for which the ISPs are or should be responsible) and therefore not a major concern for home users any longer. To the extent home users hold this belief to some degree, this perception will then be expected to have an impact on their trust on the internet. Specifically, I hypothesize that those users who more strongly believe ISPs are actively monitoring and engaging with cybersecurity issues will perceive the internet to be a safe place to browse, search, connect, and otherwise engage in a variety of activities:

H7: Perceptions about Internet Service Providers (ISPs) will have a positive effect on Internet Trust.

3.8. Digital Literacy

The digital literacy of home users is a major factor that can impact their exposure or vulnerability to cybercrime. Many years ago, before personal computers and other computing devices became an essential tool for personal and professional daily tasks, it was not as important for home users to understand or use technology, but this has since changed dramatically (Spante, Hashemi, Lundin, & Algers, 2018). Technology has become so pervasive in the home environment that some degree of digital literacy is essential in order to understand the working of different technologies as well as being able to gain the many benefits offered by their usage, both personally and professionally.

Digital literacy involves the confident and critical use of technology for work, leisure, and communication (Spante, Hashemi, Lundin, & Algers, 2018). It is underpinned by basic skills in the usage of technology, e.g., “The use of computers to retrieve, assess, store, produce, present and exchange information, and to communicate

and participate in collaborative networks via the Internet" (Spante, Hashemi, Lundin, & Algers, 2018). This research examines whether digital literacy is a high-risk factor for home users to become vulnerable to cybercrime. While the emergence and pervasiveness of technology that has occurred over the past few years would seem to indicate that the development of digital literacy skills would have accompanied this process, it is also important to note the existence of differences in accessibility to digital literacy courses or education. In many cases, this access can be affected directly or indirectly by socio-economic factors. Empirical research focusing on the social-economic factors of cybercrime found three social-economic characteristics (unemployment, GDP per capita, and education) to be most relevant (Ilievski, & Bernik, 2016); as a result, it can be expected there will be variations in the extent and quality of digital literacy skills across different segments of the population.

There are many definitions for digital literacy; for the purpose of this study, digital literacy refers to the ability to understand and apply knowledge about computerized systems and devices. As a result, digital literacy refers to the ability to handle technological devices (hardware and software), which sees digital literacy as a basic skill (Spante, Hashemi, Lundin, & Algers, 2018) which can be expected to be exhibited by home users at various levels. Home users with more developed digital literacy skills should be more able to implement cybersecurity measures in their devices, as a result of both an increased understanding of the need for these as well as having the technical knowledge and ability to put those measures into effect. Therefore, the following positive relationship between digital literacy and device security is hypothesized: H8: Digital literacy will be positively related to device security.

3.9. Training & Awareness

Despite noticeable advances in cybersecurity tools and state-of-the-art artificial intelligence cybersecurity systems, which are increasingly available to home users as well as those in corporate environments, cyber-criminals continue to successfully attack home users on an ongoing basis. Cybersecurity training & awareness is a key component of this state of affairs due to the "human factor" involved in effective cybersecurity. Since individual users are often the weakest link in the cybersecurity process (Teh et al., 2015; De Maggio et al., 2019), education of individual users in both cyberthreats and best practices to protect themselves from those could have a major impact on improving vulnerability to cyberattacks in the future. Moreover, individual home users would also benefit from creating and maintaining a culture of security awareness (Norris et al., 2019). Training & awareness courses have a negative effect on risks arising from social engineering attempts, which are one of the most common cyberattacks; social engineering is an approach which seeks to exploit the weakness in human nature and take advantage of the naivety of an average person (Aldawood & Skinner 2019). The content of these programs includes training materials, policy and regulatory frameworks, and training and safety measures to be taken before and after a cyberattack (Aldawood, & Skinner, 2019).

On the other hand, researchers have found that, even when users have gone through training and awareness programs, these are not always sufficient to make an impact on cybersecurity behavior and practices by home users (Aljedaani, Ahmad, Zahedi, & Ali Babar, 2020); despite having the required knowledge, home users to do not

always exhibit the expected behavior, which could be due to an unwillingness or lack of understanding to implement security practices that compromise critical data even when faced with social, legal, and financial consequences (Aljedaani, Ahmad, Zahedi, & Ali Babar, 2020).

Cybercriminals have become increasingly creative when it comes to deploying cyberattacks over the internet but, at the same time, many of these cyberattacks can be managed or outright prevented by well-educated home users who take the necessary precautions to protect themselves. As a result, it is imperative for home users to implement updated security technologies and protocols, but it is also the case that home users are unlikely to be able to do so without the provision of ongoing training (Norris et al., 2019). A recent IBM (2019) report reiterated that human errors continue to facilitate security breaches, as more employees fall for phishing scams and misconfigured servers (Zhang, & Abdous, 2021); it can be expected that the situation can be as dire, if not much worse, when home users at large are considered. Research also shows that security-related behaviors (such as mobile device security) are influenced by knowledge about security threats and the intentions to be security compliant (Moletsane, & Tsibolane, 2020). Therefore, it can be expected that home users who have undertaken training and are therefore more aware of both the existence of cyberthreats and how to protect themselves for those will, everything else being equal, be more likely to have taken the necessary steps to implement protective practices in their computing devices. Therefore, the following positive relationship between training and awareness and device security is offered:H9a: Training & awareness will have a positive effect on device security.

In addition, training & awareness education seeks to ensure that individuals have both the knowledge and skills necessary to understand and manage cybersecurity threats and attacks (Haeussinger, & Kranz, 2013). In other words, training & awareness education leads to cybersecurity knowledge acquired during this process, which involves both objective knowledge as well as self-confidence (De Kimpe, Walrave, Verdegem, & Ponnet, 2022; Raju, Lonial, and Mangold 2015). Knowledge and self-efficacy are closely intertwined (Arachchilage and Love 2014), and knowledge on phishing risks has been shown to be positively related to perceived self-efficacy for handling those risks (Arachchilage and Love 2014). Knowledge is assumed to be important when studying perceived response-efficacy, an important part of the cognitive appraisal process involved in PMT (Moletsane, & Tsibolane, 2020) Furthermore, in the home user context, both self-efficacy and response efficacy positively influenced intention to protect computer devices, and knowledge and self-confidence are an important antecedent to those perceptions (Tu et al, 2015). As a result, it can be expected that undergoing training and awareness education will lead to home users perceiving themselves better equipped to handle cybersecurity threats, as well as believing that their responses to those are likely to have the desired effect of protecting them from those threats. The following positive relations between training and awareness and perceived self-efficacy and perceived response-efficacy are therefore hypothesized:

H9b: Training and awareness will have a positive effect on perceived self-efficacy.

H9c: Training and awareness will have a positive effect on perceived response-efficacy.

IV. RESEARCH METHODOLOGY

Research Design

Data collection for this research was conducted via an online survey. The survey itself was designed in Qualtrics, while data collection was conducted using Connect by Cloud Research, an online research and data collection firm (for the main study) or Amazon MTurk (for the pilot study). The unit of analysis was the individual response.

The survey was designed to measure the core constructs of PMT, the six antecedent variables (device security, training and awareness, digital literacy, internet trust, ISP compliance, and social media) included in the research model, as well as the control variables (age, gender, education, and past victim to cybercrime). In addition, the survey collected data on the demographic characteristics of the participants in the sample. In addition to the role of some of these (e.g., gender, age) as control variables, demographic variables were used to categorize and describe the collected data. Table 1. includes construct definitions, scale sources, measurement scales, and the complete list of items used in this research. These are described next in more detail.

Measurements

Table 1. Construct Summary

Construct	Definition	Source	Questions
Social Media Usage	Extent and frequency to which users spend time interacting with social media	Rosen, Whaling, Carrier, Cheever & Rokkum (2013) Media and Technology Usage and Attitudes Scale (General Social Media Usage subscale)	[Scale: Never, Once a month, Several times a month, Once a week, Several times a week, Once a day, Several times a day, Once an hour, Several times an hour, All the time] How often do you do each of the following activities on social networking sites such as (Facebook, Instagram, and Twitter)? 1.-Check your social media page or other social networks 2.-Check your social media page from your smartphone 3.-Check social media at work or school. 4.-Post status updates 5.-Post photos on social media 6.-Browse profiles and photos 7.-Read postings 8.-Comment on postings, status updates, photos, etc.
ISP Compliance	Belief in the extent to which ISPs take measures to actively prevent or mitigate cybercrime	Developed for this study	[Likert 5-point] 1.-My ISP is actively engaged in preventing cybercrime 2.-My ISP is responsible for ensuring I am not a victim of cybercrime 3.-I do not have to worry about taking security measures because my ISP takes care of that

			4.-My ISP makes sure I do not have to worry about safety on the Internet 5.-My ISP is responsible for the security of my connection to the Internet 6.-Cybersecurity is the responsibility of my ISP 7.-My ISP makes sure the Internet is safe
Digital Literacy	Digital literacy is a set of skills required by 21st century individuals to use digital tools to support the achievement of goals in their life situations.	Digital Competence scale from Monteiro & Leite (2012)	[Likert scale in which 1 = I do not master and 4 = I completely master] 1.-Find data information and content through a simple online 2.-Apply filters to obtain data, information, and content 3.-Select digital technologies to interact and identify appropriate simple communication means for a given context 4.-Use a variety of digital technologies in order to interact with other people 5.-Identify simple ways to protect personal devices and digital content 6.-Create and edit simple content in simple formats 7.-Choose the best way of expression through the creation of simple digital means 8.-Know at least one Programming language 9.-Design digital applications to solve specific problems
Training and Awareness		Haeussinger & Kranz (2013)	[Likert 5-point]

			1.-I am aware of potential security threats and their negative consequences 2.-I have sufficient knowledge about the cost of potential security problems 3.-I understand the concerns regarding information security and the risks they pose 4.-I have received training to help me improve my awareness of computer and information security issues 5.-I understand my responsibilities when it comes to device and Internet security 6.-I am aware of what needs to be done in order to protect myself from cybercrime 7.-I have received training from an external party (ISP, bank, employer, etc.) on the importance of cybersecurity and how to protect myself 8.-I am well aware of cybersecurity needs and mechanisms, and how to protect myself
Internet Trust	Belief that the internet is safe, and its users will act in a responsible manner	De Kimpe, Walrave, Verdegem & Ponnet (2022)	[Likert 5-point] 1.-I am optimistic about the safety of the internet 2.-I have every confidence that the internet is safe 3.-I am satisfied with the safety of the internet
Device Security	Actual usage of computer security software. It is assessed using questions to determine if the individual has anti-virus,	Claar & Johnson (2012)	[Scale: I am not sure what that is, I know what it is, but I do not have/use it, I know what it is and have it installed/use it] Consider the device you most often use to go online and the

	firewall, and anti-spyware software installed and the level of usage.		home network through which you connect to the Internet. In that device (or network, as applicable) do you have: 1.-The latest version of the operating system 2.- An up-to-date antivirus 3.- System updates are set up to download and install automatically 4.- Important data are backed up in a separate storage or location 5.- Passwords changed periodically (every 90 days at least) 6.- Anti-spam, anti-malware, and anti-phishing rules fully implemented in your email accounts 7.- A firewall in your local device or network 8.- Scheduled periodic scanning of all your devices to detect malware and remove unwanted cookies and trackers 9.- Smart Home Manager (ISP App) to monitor your network hardware and devices connected to your home network 10.-Multi-factor authentication implemented 11.- Malware detection software is installed and up to date
Perceived Severity of Cybercrime	Perceived severity entails how serious the consequences of a certain event are perceived by an individual.	De Kimpe, Walrave, Verdegem & Ponnet (2022)	[Likert 5-point] 1.-I believe that cybercrime is significant 2.-I believe that cybercrime is serious 3.-I believe that cybercrime is severe

			4.-Cybercrime is not really a big deal 5.-The consequences of cybercrime have been exaggerated
Perceived Vulnerability to Cybercrime	Perceived vulnerability relates to a person's assessment of the probability of being confronted with threatening events, such as becoming a victim of cybercrime	De Kimpe, Walrave, Verdegem & Ponnet (2022)	[Likert 5-point] 1.-It is possible that I will be a victim of cybercrime 2.-It is likely that I will be a victim of cybercrime 3.-There is a great risk that I'll be a victim of cybercrime 4.-I feel vulnerable to cybercrime 5.-I am unlikely to be the victim of cybercrime
Perceived Self-Efficacy to Cybercrime	Perceived skills or ability to perform online protective measures, such as installing antivirus software or changing passwords regularly.	De Kimpe, Walrave, Verdegem & Ponnet (2022)	[Likert 5-point] 1.-Taking the necessary security measures is entirely under my control 2.-Taking the necessary security measures is easy 3.-I feel comfortable taking security measures 4.- I have the knowledge and skills needed to take necessary cybersecurity measures to protect myself 5.-Nothing nor nobody can stop me from taking necessary security measures
Perceived Response Efficacy	Perception of whether suggested measures are indeed perceived as effective in protecting internet users against online threats	De Kimpe, Walrave, Verdegem & Ponnet (2022)	[Likert 5-point] 1.-Security measures are effective in preventing cybercrime 2.-By taking security measures, I can prevent cybercrime 3.-If I take security measures, I am less likely to be a victim of cybercrime

			4.-Cybercrime can be controlled by taking appropriate security measures
Intention to Take Protective Measures	Any precautionary action, procedure or installation conceived or undertaken to guard or defend from harm persons, property, or the environment	De Kimpe, Walrave, Verdegem & Ponnet (2022)	[Likert 5-point] 1.-I am likely to take (more) security measures 2.-I am certain that I will take (more) security measures 3.-It is possible that I will take (more) security measures 4.-I will take action to protect myself from cybercrime by adopting more security measures

Social Media Usage, the extent and frequency to which users spend time interacting with social media, was measured with eight items from the Media and Technology Usage and Attitudes Scale from Rosen et al (2013). The measurement scale for this construct asked about the frequency with which certain activities are undertaken in social media sites, ranging from “Never” to “All the time”. The response items included activities such as “Check your social media page and other social networks”, “Post status updates”, or “Browse profiles and photos”.

Digital Literacy, the set of skills required by 21st century individuals to use digital tools to support the achievement of goals in their life situations, was measured with nine items from the Digital Competence scale from Monteiro and Leite (2012). The measurement scale for this construct was a 4-point Likert, anchored at “I do not master” and “I completely master”, and asked respondents to evaluate the extent to which they believe they mastered the different digital skills presented in the prompts.

Examples of these include “Find data, information, and content through a simple online search”, “Create and edit simple content in simple formats”, or “Know at least one programming language”.

Training and Awareness was measured with eight items from the scale developed by Haeussinger and Kranz (2013). The response format was a 5-point Likert, anchored at “Strongly disagree” and “Strongly agree”. The questions asked respondents to express their extent of agreement with statements about their awareness of cybersecurity risks. Examples of these include “I am aware of potential security threats and their negative consequences”, “I have received training to help me improve my awareness of computer and information security issues”, or “I am aware of what needs to be done in order to protect myself from cybercrime”.

Device Security, which captures actual usage of security measures in personal computing devices, was measured with eleven items from Claar and Johnson (2012). The response format presented participants with a series of cybersecurity practices and asked them to answer about their awareness and current usage of those with regards to the device they most often use to access the Internet. The response options were presented in a 3-point scale, with the labels “I am not sure what that is”, “I know what it is, but I do not have/use it”, and “I know what it is and have it installed/use it”. Examples of these security measures include “System updates are set up to download and install automatically”, “multi-factor authentication implemented”, or “Malware detection software is installed and up to date”.

For the measurement of ISP Compliance, the belief in the extent to which ISPs take measures to actively prevent or mitigate cybercrime, a combination of items from past research as well as additional novel items, was employed. Questions from the research instrument by Bulgurcu et al (2010) were employed, to which new questions were added for increased coverage of the theoretical definition of the construct as well as for increasing the number of questions used in the measurement. A total of seven questions were ultimately included in the survey. The response format was a 5-point Likert, anchored at "Strongly disagree" and "Strongly agree". The questions asked respondents to express their extent of agreement with statements about the extent to which their ISP was actively engaged in protecting them from cybersecurity threats and risks. Examples of these include "My ISP is actively engaged in preventing cybercrime", "I do not have to worry about taking security measures because my ISP takes care of that," or "Cybersecurity is the responsibility of my ISP".

Internet Trust, the belief that the internet is safe, and its users will act in a responsible manner, was measured with three items previously validated by De Kimpe et al (2022). The response format was a 5-point Likert, anchored at "Strongly disagree" and "Strongly agree". The questions asked respondents to express their extent of agreement with statements about the extent to which they believed the internet is a safe space in which to conduct transactions, engage with others, etc. The three statements for this measure were "I am optimistic about the safety of the internet", "I have every confidence that the internet is safe", and "I am satisfied with the safety of the internet".

The core constructs of PMT were measured by scales previously employed and validated by De Kimpe et al (2022). In all cases, the response format was a 5-point Likert scale, anchored at “Strongly disagree” and “Strongly agree”. Respondents were asked to express their agreement to a serious of statements related to the various core constructs of the PMT. Perceived Severity of Cybercrime, which how serious the consequences of a certain event are perceived by an individual, was measured by five items, examples of which are “I believe that cybercrime is serious” or “The consequences of cybercrime have been exaggerated” (which is reverse-coded). Perceived Vulnerability to Cybercrime, a person’s assessment of the probability of being confronted with threatening events, such as becoming a victim of cybercrime, was measured by five items, examples of which are “It is likely that I will be a victim of cybercrime” or “I am unlikely to be the victim of cybercrime” (which is reverse-coded). Perceived Self-Efficacy to Cybercrime, the perceived skills or ability to perform online protective measures, such as installing antivirus software or changing passwords regularly, was measured with five items, examples of which are “I feel comfortable taking security measures” or “Nothing nor nobody can stop me from taking necessary security measures”.

Perceived Response Efficacy, the perception of whether suggested measures are indeed perceived as effective in protecting internet users against online threats, was measured by five items, examples of which include “Security measures are effective in preventing cybercrime” or “Cybercrime can be controlled by taking appropriate security measures”. Finally, Intention to Take Protective Measures, which are defined as any precautionary action, procedure or installation conceived or undertaken to guard or defend from harm persons, property, or the environment, was measured by four items.

Examples of these include “I am likely to take (more) security measures” or “I will take action to protect myself from cybercrime by adopting more security measures”.

Participants and Procedure

The data collection for both pilot and main study proceeded as follows. First, participants were presented with a consent form describing the research, discussing what would be required from them in terms of time and effort, if they chose to participate, and what compensation they would be receiving in return. Second, participants were then presented with questions to gather their demographic characteristics. Third, participants were then presented with questions measuring each of the constructs involved in the research model, as just discussed. In addition to these, attention check questions were included at about one third and two thirds of the survey progression in order to verify that respondents were carefully reading and answering the questions as presented. Responses to these were then used to filter out respondents from the final analyses (for both pilot and main study).

4.2 Pilot Study

A pilot study was conducted in order to test out the survey and questionnaire and gather preliminary data on the validity of the scales employed, as well as their reliability. Another goal of the pilot study was to identify which questions, if any, turned out to be problematic and would need to be either rewritten for the main study, or removed from the data collection instrument altogether. The data collection process was the same as outlined above and employed also for the main study. Data from the pilot study were gathered by posting the survey as a task on the Amazon MTurk platform.

The original sample collected included 355 responses to the survey. The next step involved removing those data from those respondents who failed one or both of the attention check questions, as well as those who took less than 3 minutes to complete the entire survey, which was deemed the minimum reasonable time to carefully read the questions and answer them appropriately. This resulted in a large number of responses dropping out from the subsequent analyses. The final usable dataset included only 171 participants (this problematic data quality was also a motivation in switching data collection platforms for the main study).

Table 2. Pilot Statistics-Demographics

Age					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	5	2.9	2.9	2.9
	2	50	29.2	29.2	32.2
	3	65	38	38	70.2
	4	23	13.5	13.5	83.6
	5	22	12.9	12.9	96.5
	6	6	3.5	3.5	100
	Total	171	100	100	
Gender					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	93	54.4	54.4	54.4
	2	78	45.6	45.6	100
	Total	171	100	100	
Education					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	2	3	1.8	1.8	1.8
	3	3	1.8	1.8	3.5
	4	2	1.2	1.2	4.7
	5	131	76.6	76.6	81.3
	6	32	18.7	18.7	100
	Total	171	100	100	
Income					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	4	2.3	2.3	2.3
	2	15	8.8	8.8	11.1
	3	12	7	7	18.1
	4	20	11.7	11.7	29.8
	5	29	17	17	46.8
	6	36	21.1	21.1	67.8
	7	16	9.4	9.4	77.2
	8	19	11.1	11.1	88.3
	9	5	2.9	2.9	91.2
	10	7	4.1	4.1	95.3
	11	8	4.7	4.7	100
	Total	171	100	100	

Of the 171 participants, 93 (or 54.4%) were men and 78 (or 45.6%) were women, with the most often selected age category being 30 to 39 years old. One hundred and thirty-one (or 76.6 %) had a bachelor's degree, 32 (or 18.7 %) had a graduate degree, 3 (or 1.8%) had only finished high school, 3 (or 1.8%) answered some college but no degree, and 2 (or 1.2 %) answered associate degree. For Income, 36 (or 21.1%) of the respondents were in the range between $50,000-$59,999, 29 (or 17.0%) in the range between $40,000-$49,999, 15 (or 8.8 %) in the range between $10,000-$19,999, and only 8 (or 4.7 %) answered $100,000 or more.

The main goal of the pilot study was to assess the measurement model and quality of the measures to be employed in the main study of this research. The same modeling approach as will be used in the main study was employed here, namely structural equation modeling (SEM), specifically the PLS approach, as implemented by the SmartPLS software. Each of the constructs in the research model was modeled as a composite of the indicators used to measure it in the survey, in all cases assuming a reflective specification (which is consistent with the way in which the scales employed in this research were originally developed and validated). Figure 2 shows the initial measurement model, where numbers in the relationships between construct and items indicate the loadings of the latter on the former and includes the control variable as well.

Measurement-Model: SEM Algorithm

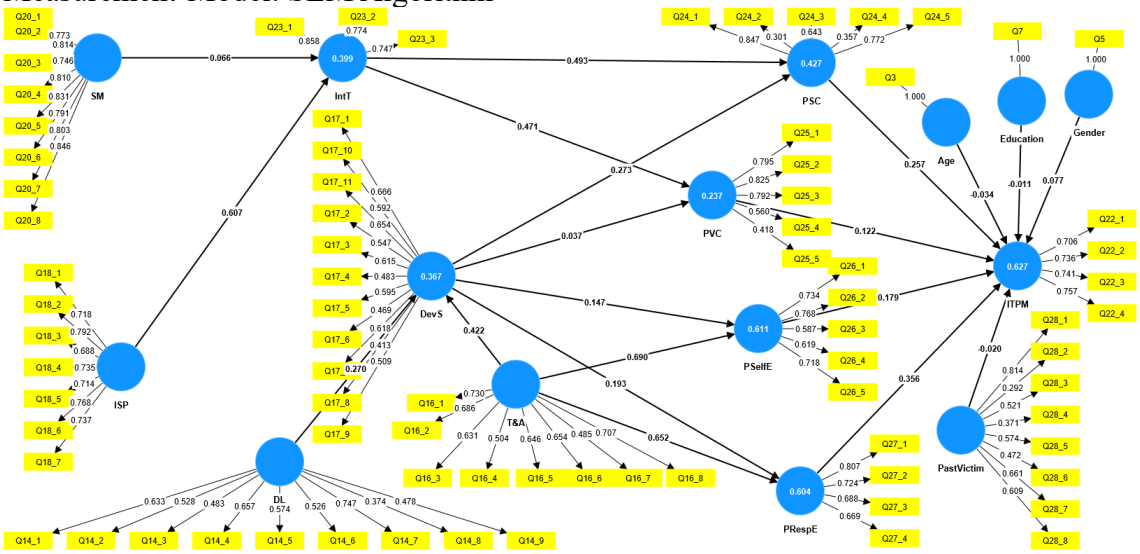

Figure 2. Measurement-Model

Table 3 shows the reliabilities, both Cronbach's alpha as well as two forms of composite reliability measures, and the average variance extracted (AVE) for each of the constructs in the model. For the former, an ideal reliability is at least 0.70 for each construct, indicating that the shared variance between a composite of the items and the construct they are intended to measure is at least 70%. For the AVE, the guideline is at least 0.50 or 50%, indicating that, on average, a construct explains at least 50% of the variance in its set of indicators.

As the results show, reliability was acceptable for the majority of the constructs; depending on which composite reliability measure was employed, this was the case for all constructs (when measured with the ρ_c statistic) or for most of them (when measured with either a or the ρ_a statistic).

Table 3. Pilot Construct Reliability and Validity

	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
DL	0.760	0.762	0.821	0.339
DevS	0.783	0.789	0.835	0.319
ISP	0.826	0.830	0.870	0.489
ITPM	0.716	0.715	0.824	0.540
IntT	0.665	0.665	0.817	0.598
PRespE	0.683	0.690	0.808	0.513
PSC	0.647	0.678	0.777	0.419
PSelfE	0.710	0.718	0.812	0.465
PVC	0.717	0.736	0.814	0.469
SM	0.922	0.926	0.936	0.646
T&A	0.810	0.819	0.857	0.431

Note: DL= Digital Literacy, DevS= Device Security, ISP= Internet Service Provider, ITPM= Intention to Take Protective Measures, IntT= Internet Trust, PRespE= Perceived Response Efficacy, PSC= Perceived Severity of Cybercrime, PSelfE= Perceived Self-Efficacy to Cybercrime, PVC= Perceived Vulnerability to Cybercrime, SM= Social Media Usage, T&A= Training and Awareness.

For the convergent validity of the measures, the results were less promising. As Table 3 shows, there were several constructs (Digital Literacy, Device Security, Perceived Severity, Perceived Self-Efficacy, and Training and Awareness) which did not reach the minimum threshold of 0.50 for the AVE of construct, per recommended construct validation guidelines (e.g., Fornell and Larcker, 1981).

Table 4 shows the results of discriminant validity tests employing the HTMT approach, as implemented in Smart PLS. The criteria to meet here is that pairs of constructs show a value of less than 0.90 in order to show adequate discriminant validity. As the initial testing results show, this was not the case for several pairs of constructs in the initial measurement model; for example, the HTMT was above the 0.90 threshold for the pair Response Efficacy – Intention, as well as for others in the model.

Table 4. Pilot Discriminant Validity

	DL	DevS	ISP	ITPM	IntT	PRespE	PSC	PSelfE	PVC	SM	T&A
DL											
DevS	0.614										
ISP	0.662	0.484									
ITPM	0.694	0.701	0.740								
IntT	0.635	0.611	0.873	0.953							
PRespE	0.675	0.698	0.713	1.075	0.865						
PSC	0.763	0.652	0.833	1.014	1.020	1.056					
PSelfE	0.677	0.748	0.748	1.069	0.900	1.177	1.029				
PVC	0.669	0.372	0.801	0.750	0.775	0.759	1.037	0.738			
SM	0.654	0.308	0.491	0.319	0.411	0.302	0.539	0.303	0.579		
T&A	0.802	0.712	0.837	0.978	0.842	1.023	0.971	1.027	0.809	0.411	

The initial measurement model showed a number of items with very low loadings, indicating a weak relationship between those and the construct of which they were measures. As a result, selected items from each of the constructs were removed, and the model was re-estimated with the remaining items, until all those left had sufficiently high loadings on their construct. Table 5 shows the removed questions from each construct as well as the loadings which flagged those for removal.

Table 5. Pilot Low Loadings Pilot Removed.

Construct	Question #	Loadings
DevS	Q17_4	0.483
	Q17_6	0.469
	Q17_4	0.583
PVC	Q25_5	0.48
DL	Q14_8	0.396
	Q14_9	0.320
PastVictim	Q28_2	0.292
	Q28_4	0.371

Note: DL= Digital Literacy, PVC= Perceived Vulnerability to Cybercrime, DevS= Device Security

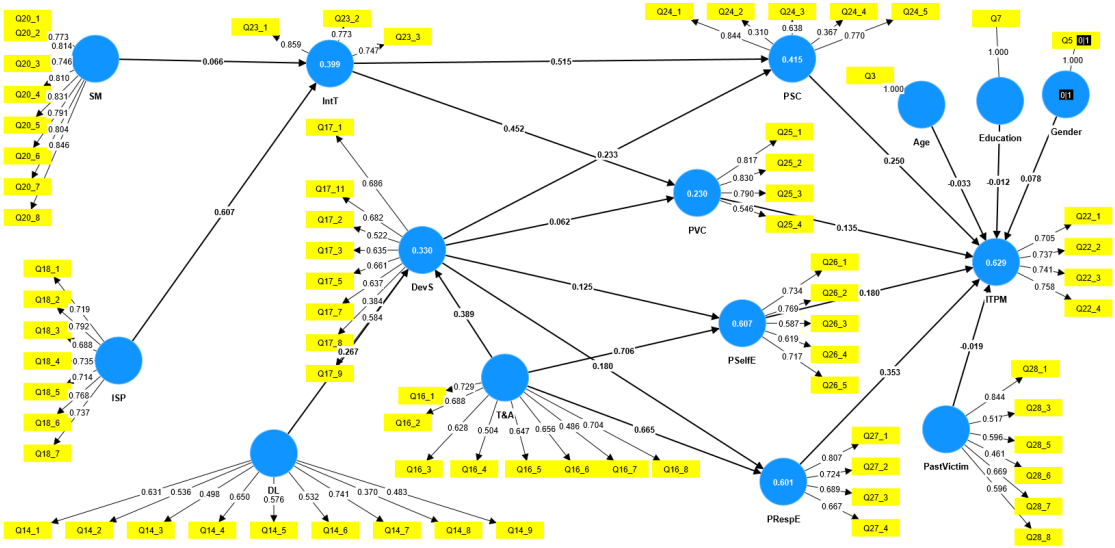

Figure 3. Revised measurement-model.

Table 6 shows the revised reliabilities, both Cronbach's alpha as well as two forms of composite reliability measures, and the average variance extracted (AVE) for each of the constructs in the model. For the former, an ideal reliability is at least 0.70 for each construct, indicating that the shared variance between a composite of the items and the construct they are intended to measure is at least 70%. For the AVE, the guideline is at least 0.50 or 50%, indicating that, on average, a construct explains at least 50% of the variance in its set of indicators.

Table 6. Pilot Revised Construct Reliability and Validity

	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
DL	0.746	0.762	0.805	0.321
DevS	0.752	0.764	0.820	0.368
ISP	0.861	0.868	0.893	0.543
ITPM	0.717	0.719	0.825	0.541
IntT	0.707	0.723	0.836	0.631
PRespE	0.695	0.703	0.814	0.524
PSC	0.563	0.659	0.737	0.389
PSelfE	0.720	0.731	0.817	0.474
PVC	0.750	0.803	0.838	0.570
SM	0.921	0.933	0.935	0.644
T&A	0.789	0.803	0.842	0.404

Table 7 shows the results of discriminant validity tests employing the HTMT approach, as implemented in Smart PLS. The criteria to meet here is that pairs of constructs show a value of less than 0.90 in order to show adequate discriminant validity.

Table 7. Pilot Revised Discriminant Validity

	DL	DevS	ISP	ITPM	IntT	PRespE	PSC	PSelfE	PVC	SM	T&A
DL											
DevS	0.560										
ISP	0.545	0.426									
ITPM	0.573	0.613	0.662								
IntT	0.490	0.518	0.779	0.835							
PRespE	0.566	0.708	0.536	1.035	0.685						
PSC	0.693	0.636	0.740	0.993	0.993	0.983					
PSelfE	0.513	0.652	0.574	0.938	0.658	1.141	0.941				
PVC	0.512	0.316	0.699	0.639	0.609	0.571	0.913	0.509			
SM	0.572	0.246	0.366	0.231	0.314	0.162	0.450	0.163	0.498		
T&A	0.701	0.650	0.750	0.927	0.698	0.989	0.923	1.002	0.719	0.288	

V. DATA ANALYSIS AND RESULTS

5.1 Sample and Demographics

Connect by Cloud Research was employed for the data collection in the main study of this research (while data collection for the pilot was conducted through Amazon mTurk, but the quality of the resulting data motivated the search for an alternative online research mechanism).

A total of 600 responses were collected for the main study. After removing those respondents who failed one or both of the attention check questions, and those who took less than 2.5 minutes to answer the complete questionnaire (which was deemed a minimum reasonable time for answering all questions while paying sufficient attention to those), a final sample of 582 participants was retained.

Of these 582 retained participants, 341 (or 58.6%) were male, 234 (or 40.2%) were female, 6 on-binary / third gender (or 1.0%), and 1 (or .2%) Prefer not to say. The most common age grouping was 30 to 39 years old. With regards to education, 288 respondents (or 46.0 %) had a bachelor's degree, 103 respondents (or 17.7 %) had a graduate degree, 101 respondents (or 17.4%) had some college but no degree, 57 respondents (or 9.8%) had finished high school but had no formal education beyond that, and 52 respondents (or 8.9 %) had an associate degree. Out of the 582 respondents, 75 respondents (or 12.9%) declared an annual income in the $100,000 or more range, 68 respondents (or 11.7%) declared between $50,000-$59,999, 65 respondents (or 11.2 %) declared between ($10,000-$19,999), and 19 respondents (or 3.3 %) declared between ($80.000-89,999).

Table 8. Statistics Demographics

Age					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	10	1.7	1.7	1.7
	2	120	20.6	20.6	22.3
	3	206	35.4	35.4	57.7
	4	116	19.9	19.9	77.7
	5	71	12.2	12.2	89.9
	6	59	10.1	10.1	100
	Total	582	100	100	
Gender					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	341	58.6	58.6	58.6
	2	234	40.2	40.2	98.8
	3	6	1	1	99.8
	4	1	0.2	0.2	100
	Total	582	100	100	
Education		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	1	0.2	0.2	0.2
	2	57	9.8	9.8	10
	3	101	17.4	17.4	27.3
	4	52	8.9	8.9	36.3
	5	268	46	46	82.3
	6	103	17.7	17.7	100
	Total	582	100	100	
Income					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	62	10.7	10.7	10.7
	2	65	11.2	11.2	21.8
	3	57	9.8	9.8	31.6
	4	64	11	11	42.6
	5	51	8.8	8.8	51.4
	6	68	11.7	11.7	63.1
	7	50	8.6	8.6	71.6
	8	44	7.6	7.6	79.2
	9	27	4.6	4.6	83.8
	10	19	3.3	3.3	87.1
	11	75	12.9	12.9	100
	Total	582	100	100	

Table 9. Measurement Model: Construct Reliability and Validity

	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
DL	0.902	0.908	0.922	0.630
DevS	0.792	0.803	0.857	0.546
ISP	0.933	0.942	0.946	0.716
ITPM	0.925	0.926	0.947	0.817
IntT	0.916	0.919	0.947	0.856
PRespE	0.846	0.847	0.897	0.686
PSC	0.815	0.825	0.871	0.577
PSelfE	0.865	0.886	0.903	0.651
PVC	0.895	0.899	0.927	0.761
SM	0.899	0.950	0.912	0.567
T&A	0.898	0.916	0.919	0.589

Note: DL= Digital Literacy, DevS= Device Security, ISP= Internet Service Provider, ITPM= Intention to Take Protective Measures, IntT= Internet Trust, PRespE= Perceived Response Efficacy, PSC= Perceived Severity of Cybercrime, PSelfE= Perceived Self-Efficacy to Cybercrime, PVC= Perceived Vulnerability to Cybercrime, SM= Social Media Usage, T&A= Training and Awareness.

Table 9 reports on the reliabilities (Cronbach's alpha and two composite reliability measures) as well as on the convergent validity (as evidenced by the Average Variance Extracted) for each construct in the research model. These were obtained from a PLS-SEM analyis using the SmartPLS software package.

During the analysis, low loadings (below 0.6) were removed from the main study as well as 2 low loadings from one control variable as shown in Table 10. The measurement model was estimated with the items measuring each construct in the research model as reflective indicators. Table 11 shows the loadings of each of the items on its construct.

Table 10. Low Loadings Removed List

Construct	Question #	Loadings
DevS	Q17_1	0.485
	Q17_5	0.464
	Q17_9	0.459
	Q17_10	0.51
	Q17_3	0.515
	Q17_4	0.583
PVC	Q25_5	-0.592
DL	Q14_8	0.396
	Q14_9	0.32
PastVictim	Q28_2	0.511
	Q28_4	0.275

Table 11. Loadings List

Q#	Original sample (O)	Q#	Original sample (O)
Q14_1 <- DL	0.706	Q22_1 <- ITPM	0.944
Q14_2 <- DL	0.787	Q22_2 <- ITPM	0.901
Q14_3 <- DL	0.845	Q22_3 <- ITPM	0.854
Q14_4 <- DL	0.825	Q22_4 <- ITPM	0.915
Q14_5 <- DL	0.831	Q23_1 <- IntT	0.92
Q14_6 <- DL	0.794	Q23_2 <- IntT	0.939
Q14_7 <- DL	0.759	Q23_3 <- IntT	0.917
Q16_1 <- T&A	0.739	Q24_1 <- PSC	0.761
Q16_2 <- T&A	0.767	Q24_2 <- PSC	0.64
Q16_3 <- T&A	0.786	Q24_3 <- PSC	0.84
Q16_4 <- T&A	0.651	Q24_4 <- PSC	0.74
Q16_5 <- T&A	0.86	Q24_5 <- PSC	0.803
Q16_6 <- T&A	0.843	Q25_1 <- PVC	0.817
Q16_7 <- T&A	0.569	Q25_2 <- PVC	0.891
Q16_8 <- T&A	0.876	Q25_3 <- PVC	0.907
Q17_11 <- DevS	0.801	Q25_4 <- PVC	0.871
Q17_2 <- DevS	0.694	Q26_1 <- PSelfE	0.753
Q17_6 <- DevS	0.712	Q26_2 <- PSelfE	0.767
Q17_7 <- DevS	0.715	Q26_3 <- PSelfE	0.882
Q17_8 <- DevS	0.766	Q26_4 <- PSelfE	0.747
Q18_1 <- ISP	0.669	Q26_5 <- PSelfE	0.873
Q18_2 <- ISP	0.85	Q27_1 <- PRespE	0.851
Q18_3 <- ISP	0.859	Q27_2 <- PRespE	0.822
Q18_4 <- ISP	0.899	Q27_3 <- PRespE	0.767
Q18_5 <- ISP	0.87	Q27_4 <- PRespE	0.868
Q18_6 <- ISP	0.867	Q28_1 <- PastVictim	0.608
Q18_7 <- ISP	0.887	Q28_3 <- PastVictim	0.8
Q20_1 <- SM	0.674	Q28_5 <- PastVictim	0.713
Q20_2 <- SM	0.716	Q28_6 <- PastVictim	0.713
Q20_3 <- SM	0.657	Q28_7 <- PastVictim	0.74
Q20_4 <- SM	0.866	Q28_8 <- PastVictim	0.737
Q20_5 <- SM	0.842	Q3 <- Age	1
Q20_6 <- SM	0.715	Q5 <- Gender	1
Q20_7 <- SM	0.694	Q7 <- Education	1
Q20_8 <- SM	0.829		

As these results show, all constructs exhibited adequate construct reliability, well in excess of the 0.70 acceptable threshold, and this was the case regardless of which reliability statistic was employed. Moreover, all construcs also show evidence of convergent validity, such that the AVE was in all cases above the 0.50 acceptable threshold. Finally, Table 12 reports on the results of a discriminant validity analysis. In a PLS-SEM analysis, discriminant validity is established when the HTMT criterion, for any pair of constructs, shows a value of 0.90 or less (ideally, 0.85 or less). This is taken as evidence that there is sufficient discriminant validity such that the measurement of any pairs of constructs can be argued to be sufficiently different that the constructs involved should indeed be considered to be different from one another (in other words, there is not enough overlap between a pair of constructs that it could be questioned whether two different constructs are indeed being measured).

For any pair of constructs in the research model, the HTMT criterion was below the 0.85 threshold, providing evidence of discriminant validity. Taken together, all constructs in the research model exhibited sufficient reliability (Table 9), convergent validity (in the form of AVE, Table 9), and discriminant validity (based on the HTMT criterion, Table 12), as well as loadings which were sufficiently high for each item on their intended construct (Table 11). As a result, the measurement portion of the research model is deemed satisfactory and it is possible to use this measurement model as the basis for the analysis of the structural relationships of interest.

Table 12. Discriminant Validity

	DL	DevS	ISP	ITPM	IntT	PRespE	PSC	PSelfE	PVC	SM	T&A
DL											
DevS	0.317										
ISP	0.108	0.153									
ITPM	0.306	0.311	0.182								
IntT	0.077	0.075	0.520	0.085							
PRespE	0.346	0.252	0.173	0.426	0.243						
PSC	0.164	0.145	0.213	0.436	0.287	0.364					
PSelfE	0.550	0.430	0.149	0.369	0.299	0.656	0.188				
PVC	0.057	0.042	0.098	0.137	0.335	0.173	0.225	0.198			
SM	0.166	0.098	0.282	0.106	0.227	0.094	0.129	0.069	0.094		
T&A	0.632	0.465	0.103	0.374	0.147	0.480	0.280	0.705	0.092	0.096	

Note: DL= Digital Literacy, DevS= Device Security, ISP= Internet Service Provider, ITPM= Intention to Take Protective Measures, IntT= Internet Trust, PRespE= Perceived Response Efficacy, PSC= Perceived Severity of Cybercrime, PSelfE= Perceived Self-Efficacy to Cybercrime, PVC= Perceived Vulnerability to Cybercrime, SM= Social Media Usage, T&A= Training and Awareness.

5.2 Path coefficients and hypothesis testing

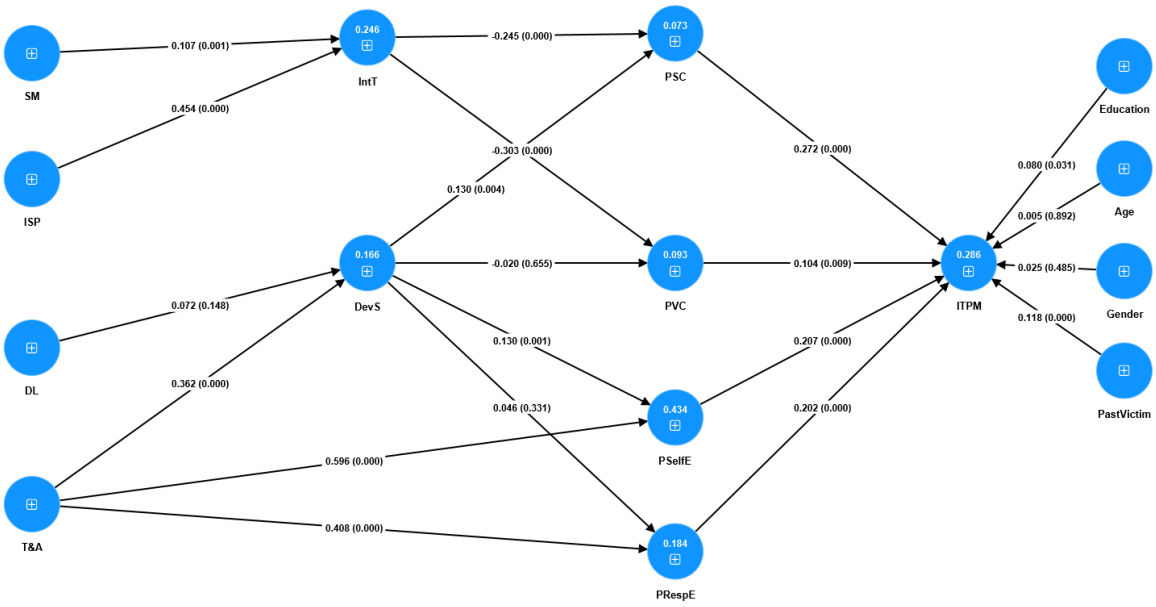

Figure 4. Structure-Measurement Model

Figure 4 shows the results of the structural portion of the research model. The reported values are the standardized paths between the different constructs (and control variables) in the research model, with the values within parentheses the p-values for those relationships, obtained from a bootstrapping run with 5,000 replications. Table 13 reports the original estimate for each relationship as well as the mean of the bootstrap replicates, the standard deviation of the bootstrapped estimates, the ratio of the original estimates to the calculated standard deviation, and the associated p-values for each relationship. These form the basis of the hypotheses testing discussed next for each hypothesis in the research model.

Table 13. Path Coefficients

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/STDEV|)	P values
Age -> ITPM	0.005	0.006	0.037	0.135	0.892
DL -> DevS	0.072	0.076	0.049	1.445	0.148
DevS -> PRespE	0.046	0.047	0.047	0.972	0.331
DevS -> PSC	0.130	0.133	0.045	2.888	0.004
DevS -> PSelfE	0.130	0.132	0.040	3.280	0.001
DevS -> PVC	-0.020	-0.020	0.044	0.447	0.655
Education -> ITPM	0.080	0.079	0.037	2.162	0.031
Gender -> ITPM	0.025	0.025	0.035	0.699	0.485
ISP -> IntT	0.454	0.453	0.038	11.906	0.000
IntT -> PSC	-0.245	-0.246	0.044	5.603	0.000
IntT -> PVC	-0.303	-0.304	0.041	7.483	0.000
PRespE -> ITPM	0.202	0.202	0.056	3.606	0.000
PSC -> ITPM	0.272	0.275	0.048	5.702	0.000
PSelfE -> ITPM	0.207	0.206	0.054	3.820	0.000
PVC -> ITPM	0.104	0.099	0.039	2.629	0.009
PastVictim -> ITPM	0.118	0.130	0.031	3.777	0.000
SM -> IntT	0.107	0.113	0.033	3.213	0.001
T&A -> DevS	0.362	0.363	0.048	7.468	0.000
T&A -> PRespE	0.408	0.408	0.048	8.593	0.000
T&A -> PSelfE	0.596	0.596	0.031	18.966	0.000

Hypothesis 1 examined the relationship between the two PMT constructs involved in the threat assessment process and the dependent construct of intentions to take action. Specifically, H1a predicted a positive relationship between Perceived Severity of Cybercrime and Intention to Take Protective Measures, such that respondents who perceived cybercrime to be more severe of a threat would also exhibit a higher intention to take actions to prevent it. The results show a positive and significant relationship between Perceived Severity of Cybercrime and Intention to Take Protective Measures ($b = 0.272, p < .001$), which provides support for the relationship predicted by H1a. H1b

predicted a positive relationship between Perceived Vulnerability to Cybercrime and Intention to Take Protective Measures, such that respondents who perceived themselves to be more vulnerable to cybercrime would also exhibit a higher intention to take actions to prevent it. The results show a positive and significant relationship between Perceived Vulnerability to Cybercrime and Intention to Take Protective Measures ($b = 0.104$, $p = .009$), which provides support for the relationship predicted by H1b as well.

Hypothesis 2 examined the relationship between the two PMT constructs involved in the coping assessment process and the dependent construct of intentions to take action. Specifically, H2a predicted a positive relationship between Perceived Self-Efficacy and Intention to Take Protective Measures, such that respondents who perceived themselves more capable of protecting themselves from cybercrime would also exhibit a higher intention to take actions to prevent it. The results show a positive and significant relationship between Perceived Self-Efficacy and Intention to Take Protective Measures ($b = 0.207$, $p < .001$), which provides support for the relationship predicted by H2a. H2b predicted a positive relationship between Perceived Response-Efficacy and Intention to Take Protective Measures, such that respondents who perceived protective actions to have an impact on cyberthreats would also exhibit a higher intention to take actions to prevent it. The results show a positive and significant relationship between Perceived Response-Efficacy and Intention to Take Protective Measures ($b = 0.202$, $p < .001$), which provides support for the relationship predicted by H2b as well.

Hypothesis 3 examined the relationship between Internet Trust and the two PMT constructs involved in the threat assessment process. Specifically, H3a predicted a negative relationship between Internet Trust and Perceived Severity of Cybercrime, such

that those respondents who trusted the internet more and perceived it to be a safe space would believe cybercrime was less severe of a threat. Results show a negative and significant relationship between Internet Trust and Perceived Severity of Cybercrime ($b = -0.245, p < .001$), which provides support for H3a. H3b also predicted a negative relationship between Internet Trust and Perceived Vulnerability to Cybercrime, such that those respondents who trusted the internet more and perceived it to be a safe space would believe they were less vulnerable to cybercrime. Results show a negative and significant relationship between Internet Trust and Perceived Vulnerability to Cybercrime ($b = -0.303, p < .001$), which provides support for H3b as well.

Hypothesis 4 examined the relationship between Device Security and the two PMT constructs involved in the threat assessment process. Specifically, H4a predicted a positive relationship between Device Security and Perceived Severity of Cybercrime, such that those respondents with more security features enabled in their devices would believe that cybercrime was more severe of a threat. Results show a positive and significant relationship between Device Security and Perceived Severity of Cybercrime ($b = 0.130, p = 0.004$), which provides support for H4a. H4b predicted a negative relationship between Device Security and Perceived Vulnerability to Cybercrime, such that respondents with more security features enabled in their devices would believe they were less vulnerable or likely to be victims of cybercrime. Results show a negative and non-significant relationship between Device Security and Perceived Vulnerability to Cybercrime ($b = -0.020, p = 0.655$), which does not provide support for H4b.

Hypothesis 5 examined the relationship between Device Security and the two PMT constructs involved in the coping assessment process. Specifically, H5a predicted a

positive relationship between Device Security and Perceived Self-Efficacy, such that respondents with more security features enabled in their devices would believe they would be able to take actions to protect themselves. Results show a positive and significant relationship between Device Security and Perceived Self-Efficacy (*b = 0.130, p = .001*), which provides support for H5a. H5b also predicted a positive relationship between Device Security and Perceived Response-Efficacy, such that respondents with more security features enabled in their devices would believe their actions would be more likely to have an effect to protect them from cybercrime. Results show a positive but not significant relationship between Device Security and Perceived Response-Efficacy (*b = 0.046, p = 0.331*), which does not provide support for H5b.

Hypothesis 6 examined the relationship between Social Media Usage and Internet Trust, and predicted a positive relationship between the two constructs, such that those respondents who engaged more with social media would perceive the internet to be a safe space. Results show a positive and significant relationship between Social Media Usage and Internet Trust (*b = 0.107, p = .001*), which provides support for H6.

Hypothesis 7 examined the relationship between ISP Compliance and Internet Trust, and predicted a positive relationship between the two constructs, such that those respondents who thought their ISP took a more active role in protecting them from cybersecurity threats would perceive the internet to be a safe space. Results show a positive and significant relationship between ISP Compliance and Internet Trust (*b = 0.454, p < .0001*), which provides support for H7.

Hypothesis 8 examined the relationship between Digital Literacy and Device Security, such that those respondents with higher levels of digital literacy would be

expected to have more security features enabled in their devices. Results show a positive but not significant relationship between Digital Literacy and Device Security (*b = 0.072, p = 0.148*), which does not provide support for H8.

Finally, Hypothesis 9 examined the role of Training and Awareness as a predictor of both Device Security and the PMT constructs involved in the coping assessment process. Specifically, H9a predicted a positive relationship between Training and Awareness and Device Security, such that those respondents who had been more exposed to training and educational programs would be expected to have more security features enabled on their devices. Results show a positive and significant relationship between Training and Awareness and Device Security (*b = 0.362, p < .0001*), which provides support for H9a. H9b predicted a positive relationship between Training and Awareness and Perceived Self-Efficacy, such that those respondents who had been more exposed to training and educational programs would believe they would be able to take actions to protect themselves. Results show a positive and significant relationship between Training and Awareness and Perceived Self-Efficacy (*b = 0.596, p < .0001*), which provides support for H9b. H9c predicted a positive relationship between Training and Awareness and Perceived Response-Efficacy, such that those respondents who had been more exposed to training and educational programs would believe their actions would be more likely to have an effect to protect them from cybercrime. Results show a positive and significant relationship between Training and Awareness and Perceived Response-Efficacy (*b = 0.408, p < .0001*), which provides support for H9c.

In addition to the hypotheses of interest, the research model also includes a number of control variables as predictors of the ultimate dependent variable of interest,

Intention to Take Protective Measures. These are Age (*b = 0.005, p = 0.892*), Gender (*b = 0.025, p = 0.485*), Education (*b = 0.080, p = .031*) and whether respondents had been a Past Victim of Cybercrime (*b = 0.118, p < .0000*). Of the control variables, only two had a significant effect on Intention to Take Protective Measures: Education, such that those with higher levels of education were more likely to take protective actions, and Past Victim of Cybercrime, such that those respondents who had been victims of cybercrime in the past would be more likely to take protective actions in the future.

Given the large number of relationships modeled and examined in this research, the presence of strong collinearity between the predictors is always a concern. Tables 14 and 15 present inner and outer collinearity statistics and VIF results, all of which are below the recommended threshold value of 5. As a result, collinearity is not an issue of concern with regards to these findings.

Table 14. Collinearity Statistics Inner List

	Age	DL	DevS	Edu	Gen	ISP	ITPM	IntT	PRespE	PSC	PSelfE	PVC	PastV	SM	T&A
Age							1.043								
DL			1.496												
DevS									1.194	1.003	1.194	1.003			
Education							1.033								
Gender							1.052								
ISP								1.093							
ITPM															
IntT										1.003		1.003			
PRespE							1.624								
PSC							1.207								
PSelfE							1.485								
PVC							1.154								
PastVictim							1.059								
SM								1.093							
T&A			1.496						1.194		1.194				

The results in Table 14. showed collinearity statistics results and all the factors VIF are uniformly below the threshold value of 5. I conclude, therefore, that collinearity does not reach any critical levels.

Table 15. VIF List

	VIF
Age -> ITPM	1.043
DL -> DevS	1.496
DevS -> PRespE	1.194
DevS -> PSC	1.003
DevS -> PSelfE	1.194
DevS -> PVC	1.003
Education -> ITPM	1.033
Gender -> ITPM	1.052
ISP -> IntT	1.093
IntT -> PSC	1.003
IntT -> PVC	1.003
PRespE -> ITPM	1.624
PSC -> ITPM	1.207
PSelfE -> ITPM	1.485
PVC -> ITPM	1.154
PastVictim -> ITPM	1.059
SM -> IntT	1.093
T&A -> DevS	1.496
T&A -> PRespE	1.194
T&A -> PSelfE	1.194

5.3 Main Hypotheses Study Summary:

In this study, I examined the relationship between the PMT constructs involved in the threat assessment process and the dependent construct of intentions to take action, also the relationship between the antecedents to PMT. The results were collected as shown in Table 16.

Table 16. Hypotheses Summary

Hypotheses	Description	P
H1a	Perceived severity of cybercrime is positively related to the intention to take protective measures against cybercrime	Supported
H1b	Perceived vulnerability is positively associated with the intention to take protective measures against cybercrime	Supported
H2a	Perceived self-efficacy is positively related to the intention to take protective measures against cybercrime	Supported
H2b	Perceived response-efficacy is positively related to the intention to take protective measures against cybercrime	Supported
H3a	Internet trust is negatively related to perceived severity of cybercrime	Supported
H3b	Internet trust is negatively related to perceived vulnerability to cybercrime	Supported
H4a	Device security is positively related to perceived severity of cybercrime	Supported
H4b	Device security is negatively related to perceived vulnerability to cybercrime	Not supported
H5a	Device security is positively related to Perceived self-efficacy	Supported
H5b	Device security is positively related to Perceived response-efficacy	Not Supported
H6	Social Media Usage has appositive effect with the Internet Trust	Supported
H7	Internet Service Provider (ISP) has a positive effect with the Internet Trust	Supported
H8	Digital literacy has a positive effect with Device Security	Not Supported
H9a	Training & Awareness has a positive effect with Device Security	Supported
H9b	Training & Awareness has a positive effect with perceived self-efficacy	Supported
H9c	Training & Awareness has a positive effect with perceived response-efficacy	Supported

VI. DISCUSSION AND CONCLUSION

6.1. Discussion

In today's globalized world, the constant progress of Information Technology cyber security infrastructure, connectivity, and the endless improvements in cybersecurity software and appliances are making computer systems very complex. There is a correlation between a computer system's complexity and cyber security; as a computer system gets more complex, it gets less secure (Schneier, 2000). Therefore, the complication in digital computerized systems and computer network infrastructure including the internet; the complex changes in security systems have been leading to a change in the cyber-attack forms, functions, and sophistication from just a few years ago targeting individual end users, businesses, and government agencies (Tounsi, & Rais, 2018). Therefore, it is of great importance to identify the drivers of intention to take protective cybersecurity actions in home users by studying the factors that can contribute positively to feasible solutions for home users and their intention to take protective measures against cybercrime.

This study seeks to identify factors which contribute to cybercrime perception and preparation in home users by using Protection Motivation Theory (PMT) as the theoretical lens. As a result, this research seeks to answer the following two research questions:

(1) What is the relative importance of each core construct of the PMT on their impact on intention to take protective action, in the context of home Internet usage?

(2) What are the antecedents to the core constructs of the PMT and what is their relative importance, in the same context of home Internet usage?

In this research I have emphasized the use of the protection motivation theory in the implementation and execution of cybersecurity studies. Therefore, in order to be able to expand on the results for this study; it is important to keep in mind that the PMT states that two cognitive processes influence people's protection motivation (i.e., the intention to perform a recommended action or behavior): threat appraisal and coping appraisal (Norman, Boer, and Seydel 2005). Threat appraisal is a cognitive process that assesses the seriousness of a particular risk. In other words, it evaluates severity of a risk as it is perceived by the individual as well as the perceived vulnerability or exposure of the individual to that specific risk. The coping appraisal, on the other hand, focuses on an individual's capability to cope with or avoid the risk in question (Rippetoe and Rogers 1987), through the following process: First, it incorporates an evaluation of the efficacy of proposed countermeasure(s) in stopping the threat, also known as response-efficacy (or the efficacy of a potential response to the identified thread); second, self-efficacy is assessed, which comprises the notion that an individual is competent of executing the necessary actions to diminish the threat (Norman, Boer, and Seydel 2005).

As expected in the PMT (Rogers, 1975, 1983), perceived severity of cybercrime, perceived vulnerability to cybercrime, perceived self-efficacy, and perceived response-efficacy are significantly and positively related to the intention to take protective measures. The results confirm and validate the use of the PMT framework in the use of cybersecurity, information security, and personal computing security studies in home users' domain. This study also represents an effort to acquire more insight into the PMT

cognitive processes in the home user personal computer domain as they relate to taking protective measures against cybercrime.

This research had two main goals. First, to examine the applicability of PMT to the cybersecurity space in general and, in particular, to the domain of home usage, which lies outside of the protective boundaries of corporate environments, where the responsibility for cybersecurity is delegated to a specialized group. Second, to examine antecedents to the core constructs of PMT such that it would be possible to identify the drivers of those factors, with an eye towards future development of training programs or interventions which can be implemented to foster home users improving their cybersecurity practices. Specifically, internet trust, device security, digital literacy, social media usage, ISP compliance, and training and awareness were examined as to their role as antecedents to the core constructs of the PMT framework.

The PMT results indicate that when home users perceive that cybercrime to be a real and severe risk (high levels of perceived severity) and that they are themselves vulnerable to cybercrimes (high levels of perceived vulnerability), they are more likely to take protective measures against cyberthreats. Additionally, the results indicate that when home users believe they possess the ability, skills, and capability to implement protective measures against cyberthreats (high levels of perceived self-efficacy) and that when they perceive those actions to have the desired effects to protect them from those threats (high levels of perceived response-efficacy), they are more likely to take actions to protect themselves from those threats. These relationships have been established several times in the context of cyberthreats and cybersecurity measures (De Kimpe et al 2022; Lee and Larsen 2009; Ifinedo 2012; Dang- Pham and Pittayachawan 2015; Tsai et al. 2016) and

the current research contributes to these findings by doing the same in the context of personal, home usage of the internet.

Internet trust is not modeled as a direct antecedent of intentions to take protective measures, but rather operates through its effects on perceived severity and perceived vulnerability. internet trust does have a negative relstionship between perceived severity to cybercrime and perceived vulnerability to cybercrime. In both cases, and as hypothesized, the relationships were negative in nature. That is, home users who believe that the internet is a safe space perceive cybercrime as less of a threat and minimise effort spent in protecting themselves from it (De Kimpe et al, 2022). As a consequence, this may lead to home users feeling less of a need to take protective measures due to the fact that trust is considered to be the counterpart of perceived risk (Riek, Böhme, and Moore 2014) and in fact reduces the amount of risk that is perceived (Pavlou 2003) in performing risky online acts, such as online banking, social media, ecommerce activities like stores online, and the use of other platforms that home users used the most for daily activities; that is, trust alleviates existing uncertainty (Montazemi and Saremi 2013). Given the importance of internet trust as an antecednt to the core constructs of PMT, and thus indirectly to intention to take protective actions, interventions can seek to better calibrate home user perceptions about the dangers and risks involved in internet usage, which would in turn impact their perceptions and, ultimately, actions.

Mixed results were found with respect to the antecedent device security in its relationship with the threat assessment appraisal process of PMT. On the one hand, device security was positively related to perceived severity to cybercrime, which implies that the more device security measures or features are implemented the more aware the

home user becomes of the severity of cyberthreats. On the other hand, the negative relationship of device security to perceived vulnerability to cybercrime was not supported. Results were also mixed with device security and its relationship with the coping appraisal process of PMT. There was a significant relationship between device security and perceived self-efficacy, which indicates that more device security measures or features are implemented the more home users to belief on their own personal skills and abilities to be able to perform certain tasks; indirectly, therefore, device security plays a role in the formation of intention to take protective actions. However, device security was not a significant predictor of perceived response-efficacyIn parallel, it is important to remark that the suggested measures are actually perceived as effective by the home user, which means that response-efficacy can be implemented. In other words, if the home users are able to believe that they are capable to perform certain task, the home user will include or implement the effectiveness of the recommended countermeasures with the main purpose of tackling the threat and that is what PMT call response-efficacy (De Kimpe et al, 2022).

As expected, social media usage has a positive effect on internet trust. This result indicates that the more home users are investing time on social media platforms, the more they increase their perception in internet trust, in other words, the greater extent or the frequency of social media usage or the frequency that home users are investing time on social media platforms the more they believe the internet is a safe space to transact and engage with others. Together with the trend towards increasing usage of social media platforms (Auxier and Anderson, 2021), particularly during the Covid-19 pandemic and continuing afterwards (Pennington, 2021), this points to an important avenue through

which assessments of cybersecurity risks and vulnerabilities are impacted, and then indirectly future intentions to take action about those. The increased usage of social media, together with direct effects on internet trust and then onto the threat appraisal constructs of PMT, contrasts with the increasing cybersecurity risks faced by users and organizations in general, and home users in particular, such that both trends reinforce each other and lead to a likely increase in cybersecurity risk in the future. This reinforces the importance of conducting research which examines the dynamics of these relationships within a home user context.

Internet Service Provider (ISP) compliance had a positive effect on internet trust, such that the more home users become aware and perceived ISPs as providing an extra layer of security for their protection, the more likely they are to trust the internet as a safe space to engage and transact. As ISPs have increasingly taken more of an active role in cybersecurity, users may perceive that they may have the opportunity to add a second security layer by allowing or adding the security services that some ISPs started to offer to their end. Some ISP started to offer additional security services or solutions for end-users or home users (Mellor, 2006). As a result, home users believe that the internet is safer place, therefore, since their ISP will protect them from cyberattacks. Similarly, to the case of social media usage, when these perceptions are not an accurate reflection of actual actions taken by ISPs, they may play a counterproductive role in that they would lead users to lower their guard out of a belief that there is a third-party handling cybersecurity and, therefore, they should not be overly concerned about it.

A positive relationship between digital literacy and device security was hypothesized. This was based on the logic that users with higher levels of digital literacy

would be more likely, everything else being equal, to implement more security features and measures in their devices, given greater awareness of the possibility of threats. However, this relationship was not supported by the data. This is an unexpected finding, which certainly requires further investigation. It may be possible that alternative measures of digital literacy, or of devise security, or both, may lead to different results.

Finally, training and awareness shows positive effects on device security, on perceived self-efficacy, and on perceived response-efficacy, as hypothesized. The first result indicates that the more trained home users are about cybersecurity, the more they will be aware about device security reaffirming that an untrained and unaware home user is more at high risk to become vulnerable to cybercrime. Moreover, end user device security behavior is influenced by knowledge about security threats and the intentions to be security compliant (Moletsane and Tsibolane, 2020). Training and awareness are perceived as knowledge acquired during this process (De Kimpe et al, 2022), and perceived knowledge has been characterized as a combination of knowledge and self-confidence (Raju, Lonial, and Mangold 2015). Consequently, perceived knowledge and self-efficacy are closely intertwined (Arachchilage and Love 2014), and knowledge on phishing risks, for example, has been shown to be positively related to perceived self-efficacy (Arachchilage and Love 2014), which further underscores these relationships.

In addition to the main theoretical relationships of interest shown in the research model and hypothesized above, this research also examined a number of control variables as potential influences on intention to take protective action, but which were not the main focus of this research. There was no significant relationship between age or gender and intentions to take protective measures. However, both education and past victim status

did show significant relationships with intention to take protective measures. While not of theoretical interest in the current study, these are interesting areas for future study.

6.2. Limitations and Future Research

The limitations of this study should be considered. The mixed findings in antecedents to PMT such as device security and digital literacy generate new research questions and improvements in the research model as well. In the questionnaire there are some questions that the clarity of may be reviewed even though most of the wording of the items was based on an existing already validated scale. This study took multiple safety measures to guarantee the data was valid and reliable i.e., attention checks were used to ensure the best possible quality and reliable data. The research collected data via survey as direct observation at a single point in time (it is a correlational study). Therefore, as a quantitative study the variables were taken through a series of computations to determine in a scientific methodology if there is relationship between them (Asamoah, M. K. 2014). Hence, when I say that antecedent to PMT impacts PMT core variables, it is based on theory and logic, and those relationships could be observed over time. Even though the survey was designed and implemented to provide enough time to participants to complete it, limitations were identified regarding the selections of the respondents and the minimum amount of time they took to respond to the survey. Moreover, another limitation is that there is no control over the selections of the respondent, therefore, the study cannot be claimed as a random sample. Furthermore, this study extended the antecedent to PMT with more than 2 antecedents, it was not possible to establish and validate the relationship between those antecedents, the results for the

device security and digital literacy were not significant, future research could increase the antecedents, integrate them as complementary variables or change them with different factors. It would be very interesting to study the control variable past victim to cybercrime as antecedents due to a very important significant value found to intention to take protective measures.

The results found in this study were mixed, some relationships between the constructs were very interesting in particular the ISP findings, such that those respondents who thought their ISP took a more active role in protecting them from cybersecurity threats would perceive the internet to be a safe space, more research is needed in this area of study, one interesting finding was the answers from the participants which the following questions i.e., "My ISP is actively engaged in preventing Cybercrime", the participants responded under the section "Neither agree or disagree" result was 223 participants 37.17% , the next question, "My ISP is responsible for ensuring I am not a victim of cybercrime", the participants responded under the section "Neither agree or disagree" result was 190 participants 31.67%. This result can indicate that more research can be done in this domain, even though the relationship is supported, there is a significant number of participants that answered, "Neither agree or disagree" This can generate new research questions about home users believe that their ISP took a more active role in protecting them from cybersecurity threats would perceive the internet to be a safe space.

As I mentioned in the discussion, more research is needed with the antecedent to PMT digital literacy, it is understood that digital literacy is also the ability to understand and apply knowledge about computerized systems and devices. As a result, digital

literacy refers to the ability to handle technological devices (hardware and software) (Spante, Hashemi, Lundin, M., & Algers, 2018). in this study, such that those respondents with higher levels of digital literacy would be expected to have more security features enabled in their devices. The results show a positive but not significant relationship between Digital Literacy and Device Security. More research is needed on digital literacy and its relationship towards intention to take protective measures against cybercrime. Another interesting relationship for future studies would be digital literacy to internet trust. Some researchers have shown that digital literacy was an important topic of study during COVID-19 pandemic since technology and the internet specifically played an important role in keeping home users' families safe by reducing the physical interaction with others for example at the hospitals; health care professionals increased the use of Telehealth. (Nurhayati, Musa, Boriboon, Nuraeni, & Putri, 2021).

Additionally, mixed results were found for device security, interesting that there was not significant value found towards response-efficacy, such that respondents with more security features enabled in their devices would believe their actions would be more likely to have an effect to protect them from cybercrime, since the construct centers around the posited efficacy of possible responses to deal with perceived threats, as one of the core processes in PMT, then those home users who have implemented more device security measures are more likely to believe they are better equipped to handle potential cyberthreats, and thus exhibit higher levels of (perceived) response-efficacy in contrast, significant value was found to self-efficacy. Future research should investigate further the relationship between perceived response-efficacy and device security. Future research

should investigate a combination of different factors towards response-efficacy, this can generate new research questions.

6.3 Conclusion

Home users are more vulnerable to cybercrimes than the organizational domain or users working for well-structured state of the art security information and event management and information technology infrastructure. Therefore, it is imperative that home users make the right decision about how to protect themselves taking into consideration the limited knowledge, digital literacy, training & awareness, and the tools that may be available for their own protection like ISP internet security suite.

This research was able to identify the factors that contribute to cybercrime perception and preparation in home users by implementing the Protection Motivation theory (PMT) framework. The results of this study show that the PMT can be used in cybersecurity context focusing on home user's domain. There is indeed a need for more cybersecurity research extending the antecedent to PMT (Rogers, 1975, 1983) and probably introducing new complementary variables. Moreover, mixed results were found identifying the antecedents to the core construct of the PMT and their relative importance in the context of home user internet usage.

6.4. Theoretical Implications

These findings provide both theoretical implications and implications for future research. In the case of the theoretical implications, the study examined the relationship between the two PMT theoretical framework constructs involved in the threat assessment cognitive process and the dependent construct of intentions to take action against cybercrime in home users' domain.

One important defenses andmplication is that this research contributes to the growing body of literature that examines the behavior of home users towards cybersecurity in the following ways: (1) it examined the relationship between PMT drivers and intentions to take protective actions against cybersecurity in the home user context, whereas much research has examined similar models in an organizational or workplace environment, where end users are not themselves directly responsible with the majority of cybersecurity efforts, (2) proposed and examined an extension to the PMT model which considers antecedents to the core PMT constructs, in order to better understand how those core perceptions are developed in the case of home users, and (3) through the examination of both, and their relative indirect impact on intention to take protective action, the theoretical implications help to identify which antecedents should be targeted to prompt home users to become more aware and sophisticated in their cybersecurity defenses, and take an active role in the provision and monitoring of the same.

6.5 Practical Implications

In the case of the implications for future research, findings provided regarding drivers of intention to take protective cybersecurity actions in home users were significant. For example, Future research should investigate the role of ISP in home users specifically in the development of a better way to keep home users informed and updated to new security products for them to be able to make the right decision in the case they need the ISP extra security layer.

One way to implement this solution is to develop training, interventions programs, and an aggressive marketing campaign informing home users about their options to better protect themselves against cybercrimes. In this study, I suggest customizing and segmenting training programs based on demographics. For segment 1, Age (between 21-49), Gender (Male and Female), Education (between High school to bachelor's degree), and Income (between $9,999 to 59,999). For segment 2, Age (between 50-60 or older), Gender (Male and Female), Education (between bachelor's degree to Graduate degree), and Income (between $70,000 to 100,000). Another important segment of study will be participants the variety of electronic devices home users have at home connected to the internet. For example, in the case of smartphones, participants responded that 97.31% or (579 participants?) do have smartphones, do not have smartphones 2.69% or (16 participants), interesting finding in the case of Laptops, participants responded to the question if they have or use laptop, they responded that 93.96% or (560 participants) do have laptops, do not have laptops 6.04% or (36 participants) Please refer to the Appendix section for more details.

A follow up could be a field study, significant segments have been identified, in order to show that the training works; for example, a before-after study showing the changes due to training in understanding of cybersecurity will be implemented as a validation of knowledge gathered during the trainings. Moreover, in the case of digital literacy future research should investigate the real value of digital literacy for home users by integrating complementary variables into the research model. This study was also able to provide significant findings from the antecedents to PMT. Additionally, the study was able to answer the research questions; the results were significant, supported, and able to validate the importance of each core construct of the PMT on their impact to take protective measure against cybercrime.

LIST OF REFERENCE

Adger, W. N. (2006). Vulnerability. Global environmental change, 16(3), 268-281.

Akram, W., & Kumar, R. (2017). A study on positive and negative effects of social media on society. International Journal of Computer Sciences and Engineering, 5(10), 351-354.

Aldawood, H., & Skinner, G. (2019, May). Challenges of implementing training and awareness programs targeting cyber security social engineering. In 2019 cybersecurity and cyberforensics conference (ccc) (pp. 111-117). IEEE.

Aldawood, H., & Skinner, G. (2019, May). Challenges of implementing training and awareness programs targeting cyber security social engineering. In 2019 Cybersecurity and Cyberforensics Conference (CCC) (pp. 111-117). IEEE.

Aljazzaf, Z. M., Perry, M., & Capretz, M. A. (2010, September). Online trust: Definition and principles. In 2010 Fifth International Multi-conference on Computing in the Global Information Technology (pp. 163-168). IEEE.

Aljedaani, B., Ahmad, A., Zahedi, M., & Ali Babar, M. (2020, December). Security awareness of end-users of mobile health applications: an empirical study. In MobiQuitous 2020-17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (pp. 125-136).

Almadhoor, L. (2021). Social media and cybercrimes. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), 2972-2981.

Almansoori, A., Alshamsi, M., Abdallah, S., & Salloum, S. A. (2021, June). Analysis of Cybercrime on Social Media Platforms and Its Challenges. In The International

Conference on Artificial Intelligence and Computer Vision (pp. 615-625). Springer, Cham.

Alshaikh, M., Naseer, H., Ahmad, A., & Maynard, S. B. (2019). Toward sustainable behaviour change: an approach for cyber security education training and awareness.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. MIS quarterly, 613-643.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. MIS quarterly, 613-643.

Asamoah, M. K. (2014). Re-examination of the limitations associated with correlational research. Journal of Educational Research and Reviews, *2*(4), 45-52.

Auxier, B., & Anderson, M. (2021). Social media use in 2021. Pew Research Center, 1, 1-4.

Budzanowski, A. (2017). Why Coolness Should Matter to Marketing and When Home users Desire a Cool Brand: An Examination of the Impact and Limit to the

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, 523-548.

Chevers, D. A. (2019). The impact of cybercrime on e-banking: A proposed model. In CONF-IRM (p. 11). <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1001&context=confirm2019>.

Choi, N. G., & DiNitto, D. M. (2013). The digital divide among low-income homebound older adults: Internet use patterns, eHealth literacy, and attitudes toward computer/Internet use. Journal of medical Internet research, 15(5), e2645.

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

Collen, A., Nijdam, N. A., Augusto-Gonzalez, J., Katsikas, S. K., Giannoutakis, K. M., Spathoulas, G., ... & Dimas, M. (2018). Ghost-safe-guarding home IoT environments with personalised real-time risk control.

Council of Europe. Convention on Cybercrime; European Treaty Series No. 185; Council of Europe: Budapest, Hungary, 2001; pp. 1–25. Available online: https://rm.coe.int/1680081561 (accessed on 6 April 2022).

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security*, *48*, 281-297.

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour & Information Technology, 41(8), 1796-1808.

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour & Information Technology, 41(8), 1796-1808.

De Kimpe, L., Walrave, M., Verdegem, P., & Ponnet, K. (2022). What we think we know about cybersecurity: an investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. Behaviour & Information Technology, 41(8), 1796-1808.

Debb, S. M., & McClellan, M. K. (2021). Perceived Vulnerability As a Determinant of Increased Risk for Cybersecurity Risk Behavior. *Cyberpsychology, Behavior, and Social Networking*, *24*(9), 605-611.

Folsom, S. R., & Officer, C. C. (2016). I. COURSE OVERVIEW.for DDoS attacks; 2016.

Fornell, C., & Larcker, D. F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics.

from: https://securelist.com/files/2016/05/Q1_2016_MW_report_FINAL_eng.pdf. [Accessed 7 October2016].

Haeussinger, F., & Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior.

Hair, Joe, Jr.; Hult, G. Tomas M.; Ringle, Christian M.; Sarstedt, Marko (2021-07-06). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). SAGE Publications. Kindle Edition.

Hajli, M. N. (2014). A study of the impact of social media on consumers. International journal of market research, 56(3), 387-404.

Hart, J. L., Turnbull, A. E., Oppenheim, I. M., & Courtright, K. R. (2020). Family-centered care during the COVID-19 era. *Journal of pain and symptom management*, *60*(2), e93-e97.

Haung & Madnick(2020). The TikTok ban should worry every company. Harvard Business. Published on HBR.org

Herath, T. B., Khanna, P., & Ahmed, M. (2022). Cybersecurity practices for social media users: a systematic literature review. Journal of Cybersecurity and Privacy, 2(1), 1-18.
Herath, T. B., Khanna, P., & Ahmed, M. (2022). Cybersecurity practices for social media users: a systematic literature review. Journal of Cybersecurity and Privacy, 2(1), 1-18.
Hoffman, D. L., Moreau, C. P., Stremersch, S., & Wedel, M. (2022). The Rise of New Technologies in Marketing: A Framework and Outlook. Journal of Marketing, 86(1), 1-6.

Ilievski, A., & Bernik, I. (2016). Social-economic aspects of cybercrime. Peer-reviewed academic journal Innovative Issues and Approaches in Social Sciences.

Kabango, C. M., & Asa, A. R. (2015). Factors influencing e-commerce development: Implications for the developing countries. International Journal of Innovation and Economic Development, 1(1), 64-72.

Kaspersky Labs. IT Threat Evolution in Q1 2016; 2016. Available

Keenan, T. P., & Trotter, D. M. (1999). The changing role of community networks in providing citizen access to the Internet. Internet Research.

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. Computers & Security, 29(8), 840-847.

Kritzinger, E., & Von Solms, S. H. (2013, October). Home user security-from thick security-oriented home users to thin security-oriented home users. In 2013 Science and Information Conference (pp. 340-345). IEEE.

Lahoud, H. A., & Tang, X. (2006, October). Information security labs in IDS/IPS for distance education. In Proceedings of the 7th conference on Information technology education (pp. 47-52).

Lebek, B., Uffen, J., Neumann, M., Hohler, B., & Breitner, M. H. (2014). Information security awareness and behavior: a theory-based literature review. Management Research Review.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, 45, 13-24.

Li, L., Xu, L., & He, W. (2022). The effects of antecedents and mediating factors on cybersecurity protection behavior. *Computers in Human Behavior Reports*, *5*, 100165.

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, *92*, 139-150.

Marttila, E., Koivula, A., & Räsänen, P. (2021). Cybercrime victimization and problematic social media use: findings from a nationally representative panel study. American journal of criminal justice, 46(6), 862-881.

Mathur, M. (2019). Where is the security blanket? Developing social media marketing capability as a shield from perceived cybersecurity risk. Journal of Promotion Management, 25(2), 200-224.

McCarthy, C., Harnett, K., & Carter, A. (2014). A summary of cybersecurity best practices (No. DOT HS 812 075). United States. National Highway Traffic Safety Administration.

Mendoza, D. K. O. (2017). The vulnerability of cyberspace-the cyber crime. Journal of Forensic Sciences & Criminal Investigation, 2(1), 1-8.

Mezzour, G., Carley, L., & Carley, K. M. (2014). Global mapping of cyber-attacks. Available at SSRN 2729302.

Moletsane, T., & Tsibolane, P. (2020, March). Mobile information security awareness among students in higher education: An exploratory study. In 2020 conference on information communications technology and society (ICTAS) (pp. 1-6). IEEE.

Moletsane, T., & Tsibolane, P. (2020, March). Mobile information security awareness among students in higher education: An exploratory study. In 2020 conference on information communications technology and society (ICTAS) (pp. 1-6). IEEE.

Monteiro, A., & Leite, C. (2021). Digital literacies in higher education: Skills, uses, opportunities and obstacles to digital transformation. *Revista de Educación a Distancia (RED)*, *21*(65).

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815-825.

Norton, W. B. (2001, May). Internet service providers and peering. In Proceedings of NANOG (Vol. 19, pp. 1-17).

Nurhayati, S., Musa, S., Boriboon, G., Nuraeni, R., & Putri, S. (2021). Community Learning Center efforts to improve information literacy in the community for cyber-crime prevention during a pandemic. *Journal of Nonformal Education*, *7*(1), 32-38.

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

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

Patel, A., Qassim, Q., & Wills, C. (2010). A survey of intrusion detection and prevention systems. Information Management & Computer Security.

Pennington, N. (2021). Communication outside of the home through social media during COVID-19. *Computers in human behavior reports*, *4*, 100118. Perception of Brand Coolness (Doctoral dissertation, Universität St. Gallen).Perrin, A. (2015). Social media usage. Pew research center, 125, 52-68.

Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. Forensic Sciences, 2(2), 379-398.2001; pp. 1–17.

Protective Measure Definition <https://www.eionet.europa.eu/gemet/en/concept/11662#:~:text=Definition,persons%2C%20property%20or%20the%20environment.>

Reddy, P., Sharma, B., & Chaudhary, K. (2020). Digital literacy: A review of literature. International Journal of Technoethics (IJT), 11(2), 65-94.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & security, 28(8), 816-826.

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. Computers & security, 28(8), 816-826.

Rising, K. L., Ward, M. M., Goldwater, J. C., Bhagianadh, D., & Hollander, J. E. (2018). Framework to advance oncology-related telehealth. JCO clinical cancer informatics, 2, 1-11.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change1. The journal of psychology, 91(1), 93-114.

Rogers, R. W. (1985). Attitude change and information integration in fear appeals. *Psychological reports*, *56*(1), 179-182.

Rosen, L., Whaling, K., Carrier, L., Cheever, N. and Rokkum, C. (2013). "The Media and Technology Usage and Attitudes Scale: An empirical investigation," Computers in Human Behavior, 29, pp. 2501-2511.

Rowe, B., Reeves, D., & Gallaher, M. (2009). The role of internet service providers in cyber security. Institute for Homeland Security Solutions.

Rowe, B., Reeves, D., & Gallaher, M. (2009). The role of internet service providers in cyber security. Institute for Homeland Security Solutions.

Sabillon, R. (2022). The cybersecurity awareness training model (CATRAM). In Research Anthology on Advancements in Cybersecurity Education (pp. 501-520). IGI Global.

Sponcil, M., & Gitimu, P. (2013). Use of social media by college students: Relationship to communication and self-concept. Journal of Technology Research, 4(1), 37-49.

Sukwong, O., Kim, H., & Hoe, J. (2011). Commercial antivirus software effectiveness: an empirical study. Computer, 44(03), 63-70.

Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. Information, 13(9), 413.

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.

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.

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber-attacks. Computers & security, 72, 212-233.

Wall, D.S. Introduction: Cybercrime and the Internet. In Crime and the Internet;Wall, D.S., Ed.; Routledge: New York, NY, USA,

Wang, Y. D., & Emurian, H. H. (2005). An overview of online trust: Concepts, elements, and implications. *Computers in human behavior*, *21*(1), 105-125.

Wanjala, M. Y., & Jacob, N. M. (2018). Review of Viruses and Antivirus patterns. Global Journal of Computer Science and Technology.

Wu, F., Yuan, Y., Deng, Z., Yin, D., Shen, Q., Zeng, J., ... & Sun, C. (2022). Acceptance of COVID-19 booster vaccination based on the protection motivation theory: A cross-sectional study in China. Journal of medical virology, 94(9), 4115-4124.

Yang, K., & Forney, J. C. (2013). The moderating role of home user technology anxiety in mobile shopping adoption: differential effects of facilitating conditions and social influences. Journal of Electronic Commerce Research, 14(4), 334.

Yiakoumis, Y., Katti, S., Huang, T. Y., McKeown, N., Yap, K. K., & Johari, R. (2012, September). Putting home users in charge of their network. In Proceedings of the 2012 ACM Conference on Ubiquitous Computing (pp. 1114-1119).

Zeng, B., & Gerritsen, R. (2014). What do we know about social media in tourism? A review. Tourism management perspectives, 10, 27-36.

Zhang, Z. J., He, W., Li, W., & Abdous, M. H. (2021). Cybersecurity awareness training programs: a cost–benefit analysis framework. Industrial Management & Data Systems.

APPENDICES

Appendix A

Questionnaire Items-ISP

This appendix shows all the statistics from the ISP questionnaire presented to the participants.

Question: Please indicate the extent to which you agree or disagree with the following statements, using the scale provided.

Table A1. Questionnaire Results

#	Question	Strongly disagree	#	Somewhat disagree	#	Neither agree nor disagree	#	Somewhat agree	#	Strongly agree	#	Total
1	My ISP is actively engaged in preventing cybercrime	7.17%	43	11.67%	70	37.17%	223	32.00%	192	12.00%	72	600
2	My ISP is responsible for ensuring I am not a victim of cybercrime	15.83%	95	18.50%	111	31.67%	190	25.50%	153	8.50%	51	600
3	I do not have to worry about taking security measures because my ISP takes care of that	31.50%	189	26.00%	156	22.83%	137	14.33%	86	5.33%	32	600
4	My ISP makes sure I do not have to worry about safety on the Internet	26.67%	160	22.83%	137	26.33%	158	18.00%	108	6.17%	37	600
5	My ISP is responsible for the security of my connection to the Internet	19.50%	117	20.17%	121	25.67%	154	23.67%	142	11.00%	66	600
6	Cybersecurity is the responsibility of my ISP	23.67%	142	21.17%	127	27.00%	162	18.83%	113	9.33%	56	600
7	My ISP makes sure the Internet is safe	22.50%	135	17.17%	103	29.83%	179	21.00%	126	9.50%	57	600

Table A2. Statistics Results

#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	My ISP is actively engaged in preventing cybercrime	1	5	3.3	1.06	1.11	600
2	My ISP is responsible for ensuring I am not a victim of cybercrime	1	5	2.92	1.19	1.41	600
3	I do not have to worry about taking security measures because my ISP takes care of that	1	5	2.36	1.21	1.47	600
4	My ISP makes sure I do not have to worry about safety on the Internet	1	5	2.54	1.23	1.51	600
5	My ISP is responsible for the security of my connection to the Internet	1	5	2.87	1.28	1.64	600
6	Cybersecurity is the responsibility of my ISP	1	5	2.69	1.27	1.62	600
7	My ISP makes sure the Internet is safe	1	5	2.78	1.27	1.61	600

Appendix B

Questionnaire Items-Devices

This appendix shows all the statistics from the electronic device's questionnaire presented to the participants.

Question: Which of the following electronic devices do you have in your home? Please select all that apply.

Table B1- Questionnaire Results

#	Question	Yes	#	No	#	Total
1	Smartphones	97.31%	579	2.69%	16	595
2	Tablets	80.24%	471	19.76%	116	587
3	Game consoles (Xbox, Nintendo etc.)	72.66%	420	27.34%	158	578
4	Laptops	93.96%	560	6.04%	36	596

Table B2. Statistics Results

#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Smartphones	1	2	1.03	0.16	0.03	595
2	Tablets	1	2	1.2	0.4	0.16	587
3	Game consoles (Xbox, Nintendo etc.)	1	2	1.27	0.45	0.2	578
4	Laptops	1	2	1.06	0.24	0.06	596

VITA

HUMBERTO RAYTI NOGUERA

2013-2016	B.Sc. Business Administration Management Information Systems Florida International University Miami, FL
2016-2017	Senior Network and System Administrator -Web Developer Loxia Technologies Inc. Miami, Florida
2016-2017	M.S. Information Systems Florida International University Miami, FL
2017-2019	Systems Engineer-Programmer TEVA Pharmaceuticals Davie, Florida
2019-2020	IT Manager- Systems Administrator Greenlane Holdings, Inc Boca Raton, Florida
2021-2023	US|Consultant, IOPS Facilities & IT-Senior Server Automation Engineer Regeneron Pharmaceuticals New York, USA
2019-Present	President and Founder Manage Development Systems Corp. Miami, FL
2019-2023	Doctoral Candidate Florida International University Miami, FL

PUBLICATIONS