Exploring Factors that Affect Adoption of Computer Security Practices among College Students

by

Amani Alqarni

Dissertation

Submitted to the College of Technology

Eastern Michigan University

in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

in

Technology

Concentration in Information Assurance

Dissertation Committee:

Dorothy McAllen, PhD, Chair

Joseph Bauer, PhD

Bilquis Ferdousi, PhD

Huei Lee, PhD

October 25th, 2017

Ypsilanti, Michigan

Dedication

I dedicate this dissertation to the loving memory of my father, to my dear mother, to my lovely husband, to my greatest brothers and sisters, and to my precious children.

Acknowledgments

I would like to sincerely thank almighty Allah for all his grants that he bestowed on me. Thank you for my deceased father, Dhafer, who died when I was in a high school, for instilling the value of education in me. Thank you to my dear mother, Azah, for her never-ending support and prayers, and for her endless sacrifices. Thanks is not nearly enough for you. Thank you to my beloved husband Mr.Abdullah, he did more than humanly possible to support me through this journey and help me to achieve my dreams. Thank you to my lovely kids, Mannaa and Aljudy, whose love and innocence has always inspired me throughout this difficult period. Thank you to my greatest brothers and sisters, for encouraging me and never allowing me to give up, thank you for your support and prayers.

This study would never have been completed without my dissertation chair Dr. McAllen; thank you for being supportive and helpful. I am so thankful for her time, effort, and dedication. I cannot imagine having a better advisor for my dissertation. Sincere thanks go to committee members Dr. Joseph Bauer, Dr. Bilquis Ferdousi, and Dr. Huei Lee for their time, guidance, encouragement, and feedback.

Abstract

Cyber-attacks threaten the security of computer users' information, networks, machines, and privacy. Studies of computer security education, awareness, and training among ordinary computer users, college students, non-IT-oriented user groups, and non-technically trained citizens are limited. Most research has focused on computer security standards and guidelines in organizational contexts. Few studies have analyzed the predictors of college students' adoption of computer security practices. Based on a comprehensive literature review, researchers have relied heavily on well-established behavioral theories, such as the technology acceptance model (TAM), theory of planned behavior (TPB), and protection motivation theory (PMT) to explain the variation in adoption of computer security practices among college students. This dissertation builds on this growing body of scholarship by blending those three into a single conceptual framework with the objective of finding the factors influencing the adoption of computer security practices among college students.

This research tested the empirical fit of a model based on the technology acceptance model, theory of planned behavior, and protection motivation theory in explaining the variation in college students' responses to a set of questions on their likelihood of adopting computer security practices. The model included the following independent variables: perceived vulnerability, perceived severity, response efficacy, computer self-efficacy, attitudes, subjective norms, perceived behavioral control, perceived ease of use, perceived usefulness, and awareness. The demographic variables (age, gender, education level, major, college, and IT experience) were used as control variables moderating the relationship between the cited independent variables and dependent variable. The dependent variable was computer security practices based

on a composed scale of four items asking students to what extent they check, verify, or exercise caution in opening emails and attachments.

Based on a 301 convenience sample collected at a Midwestern University, the analysis resulted in the significance of perceived vulnerability, perceived ease of use, and perceived usefulness. This finding suggests that the TAM enjoys empirical support in the study of computer security practices unlike the TPB or PMT. Results of this study should encourage university administrators to create workshops on teaching students the usefulness and ease of adopting computer security practices. Experimental research is highly encouraged because survey research suffers from several weaknesses such as social desirability.

Table of Contents

List of Tables

Lists of Figures

Chapter 1: Introduction

Cybercrime in all its forms, including, but not limited to, identity theft, privacy invasions, hacking, and computer intrusions, has become an imminent threat to computer users (Anderson & Agarwal, 2010). Electronics retailers and computer manufacturers have developed detailed guides for users with the sole goal of securing their computers and information (Furnell, Bryant, & Phippen, 2007). Motivated by the goal of protecting and securing users' information and computers, researchers have embarked on the quest to find the predictors of security practices, seeking to assist in the fight against cybercrime and to secure citizens' private information (Furnell et al., 2007; Anderson & Agarwal, 2010). A study by Anderson and Agarwal (2010) concluded that "results from a survey of 594 home computer users from a wide range of demographic and socio-economic backgrounds suggest that computer users' intention to perform security-related behavior is influenced by a combination of cognitive, social, and psychological components." The study noted the need for conducting more scientific studies to pinpoint the specific factors explaining the information security behavior of computer users (Anderson & Agarwal, 2010).

Noting the challenging nature of identifying the correlates of information security practices among computer users, Li and Siponen (2011) argue that "individuals' information security behaviors under different contexts may be complex and changeable" (p. 54). The information assurance literature is filled with studies on predicting information security practice within organizations (Anderson & Agarwal, 2010; Hu, Hart, & Cooke, 2006; Ion, Reeder, & Consolvo, 2015; Kim, 2014; Ng, Kankanhalli, & Xu, 2009). Many authors have tried to identify the correlates of information security policy compliance among employees in firms, governments, and organizations (Bulgurcu, Cavusoglu, & Benbasat, 2010; Herath & Rao, 2009:

Peltier, 2013; Safa et al., 2015; Siponen, Mahmood, & Pahnila, 2014). Sanctions, threat appraisals, fear appeals, organizational control, and subjective norms have all been found to explain differences in complying with information security guidelines (Ahmad, Maynard, & Park, 2014; Crossler et al., 2013; Siponen, Mahmood, & Pahnila, 2014). The investigation on predictors of the information security practices of computer users seems more difficult because of the less restrictive environment home users operate in, the lack of information security monitoring from an authority, and the greater latitude home users enjoy in utilizing their machines (Arachchilage & Love, 2014; Ball, Ramim, & Levy, 2015; Mensch & Wilkie, 2011). This has led to the limited empirical evaluation of the factors influencing home users' information security practices.

Statement of the Problem

Empirical study of computer users' adoption of computer security practices and habits outside of organizational settings is limited (Fagan & Khan, 2016; White, Ekin, & Visinescu, 2016). Further, the analysis of factors of computer security practices among college students is inadequate (Hajli & Lin, 2016; Meso, Ding, & Xu, 2013). This study aims to address the above problems in the literature by studying the factors influencing college students' willingness to adopt computer security practices.

Nature and Significance of the Problem

Cyberattacks are becoming more frequent, larger in scope, threatening, and more innovative. Such threats not only jeopardize citizens' information and privacy concerns, but also businesses' information assurance and governments' national information infrastructures. Cyberattacks occur due to fragile computer networks and both poor awareness and compliance with security standards. Unfortunately, many individuals today dedicate their time, efforts, and

skills to become professional cyberattackers. Government agencies, business, organizations, and universities/colleges have established special units tasked with information security and minimizing the threats of cyberattacks. Fundamental goals of such offices are the protection of personal information, names, social security numbers, addresses, and sensitive information such as work histories, medical records, financial data, and credit information (Kim, 2014; White, Ekin, & Visinescu, 2016).

Over the past two decades, universities and colleges across the globe have significantly improved their technical security infrastructures. Simultaneously, higher education institutions have invested in security, awareness, education, and training programs, coaching their staff as well as students on the importance of information assurance and best practices for securing personal and institutional information. The limited number of studies on college students' information security behavior highlights the lack of training and compliance of students in areas of information assurance and privacy. Students often exchange passwords with each other, ID numbers, credit card information, banking records, and do not abide by the best practices in protecting their networks (Hajli & Lin, 2016; Hu, Hart, & Cooke, 2006).

While interest in cyber security has exponentially increased in the past few years, knowledge on students' awareness and training in information security is still limited. Government agencies, businesses, and not-for-profit organizations have commissioned studies and surveys to learn about their staff and workforces' knowledge of and compliance with information security standards. This type of information is crucial in preparing computer users to prevent, avoid, address, and manage cyber-attacks. Recent surveys across the public, private, and non-profit sectors overwhelmingly indicates that individuals do not have sufficient education and

training to equip them with the necessary skills to bypass cyber-attacks (Anderson & Agarwal, 2010; Ding, & Xu, 2013).

In their survey investigating college students' information security awareness and practices at the California State University-Los Angeles, Slusky and Partow-Navid (2012) found that college students typically possess adequate knowledge of the risks and vulnerabilities to their information. However, when using computers in real-life settings, students fail to comply with security guidelines. Similarly, Kim (2014) concluded that college students constitute a great target group for cybercriminals due to their limited adoption of information security standards. Students have been found to lack information security training and awareness and to be more vulnerable to cyber-attacks than other groups in the general population (Ramalingam, Khan, & Mohammed, 2016).

College students possess a more frequent and intense presence online and utilize computers more frequently compared to other groups. They are likely to create social networking site accounts, shop online, take online courses, and communicate with potential employers and other professional entities over the World Wide Web more often than other groups in the general population. College students, therefore, are more likely to become victims of cyber-attacks.

College students face an imminent problem in protecting their privacy. Admission committees, potential employers, and other organizations of interest to the student, attempt to obtain as much as information as possible on them in order to help make crucial decisions on admitting, hiring, or developing a professional relationship with the student. Faculty members communicate sensitive information to students (names, grades, places of scheduled meetings, intellectual property works, etc.) over electronic platforms, emails, and other sites. With the proliferation of online communication tools today, faculty members send students messages over

social networking sites, personal accounts, on other webpages, or personal links. Students may not be aware of the duration faculty members or other academic services providers can retain their information.

Working on school or work projects, students may not be aware of the fact that they need to keep privileged information, names, records, accounts numbers, and other sensitive information out of their online communications with their friends or faculty members. Students are also faced with an imminent threat of data loss. Their computers, flash drives, and phones may be lost or stolen jeopardizing their privacy, confidentiality, and anonymity. Further, student accounts are exposed to hacking or unauthorized intrusions that lead to data loss. Students who lack the necessary awareness and technical knowledge on protecting their computers fall victim to hackers or their own friends who possess the requisite knowledge to retrieve information from others' accounts (Fagan & Khan, 2016; White, Ekin, & Visinescu, 2016).

Proposed Model

Previous research has utilized several theories to explore the factors influencing the adoption of computer security practices among college students. This study incorporated the technology acceptance models (TAM), theory of planned behavior (TPB), and protection motivation theory (PMT), and to construct a comprehensive conceptual framework presented in figure 1 below. While the model seems more complex compared to any other theoretical framework, it is more comprehensive, robust, and accurate; this is because three explanatory theoretical frameworks are used (TAM, TPB, and PMT) rather than a single theoretical framework, which strengthens the predictive power of the model. Notice that all of the included variables and theories in the framework have been widely cited by previous researchers possessing a significant relationship with computer security practices adoption. Previous studies

have only considered the influence of a single or modified version of the discussed theoretical frameworks above. Biased findings result when researchers fail to model the effects of other important variables in theoretical models. This model assists in the identification of the influence of each theoretical perspective while holding others constant, which revealed the magnitude of each framework in explaining the variance in the adoption of computer security practices among computer users.

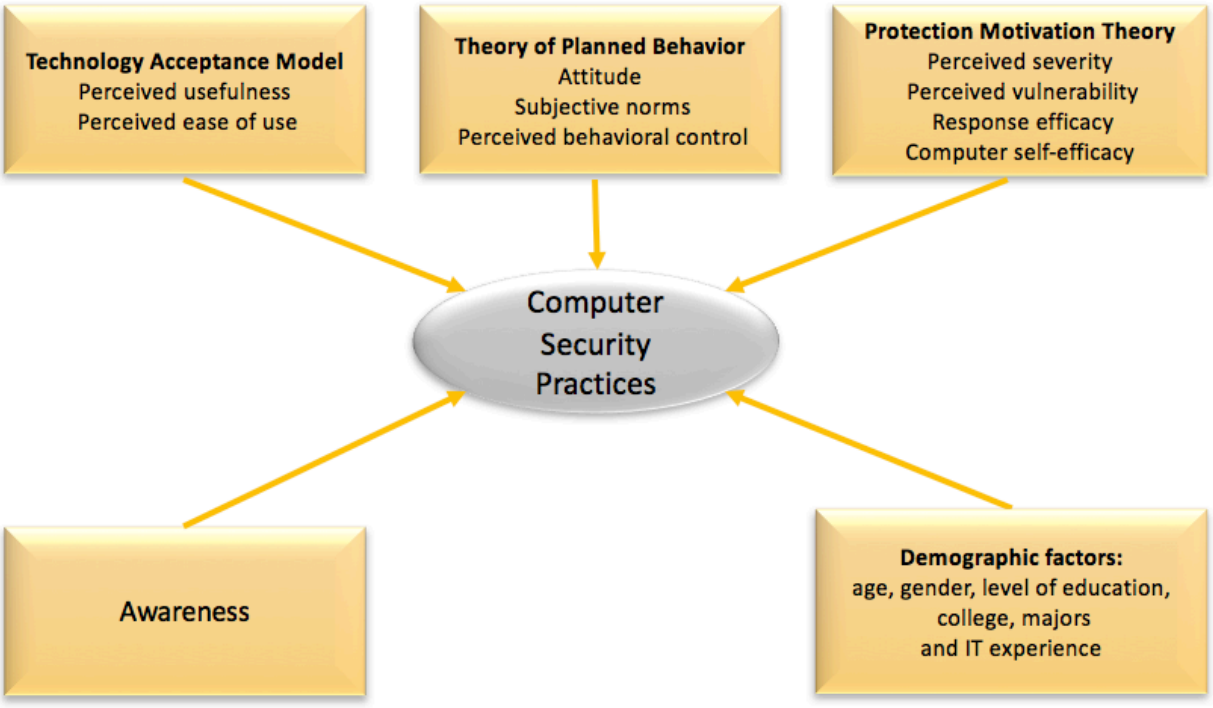

Figure 1. The conceptual framework of different factors and their effects on computer security practices adoption among college students.

Objective of the Research

This study aimed to identify the factors influencing college students' adoption of computer security practices. It constructed a conceptual frameworks based on the protection motivation theory, technology acceptance model, and theory of planned behavior and collected survey data to test the empirical fit of the model. Recommendations were developed for

stakeholders on strengthening computer security practices among college students based on the results from this analysis.

Research Questions

1. To what extent do perceived usefulness, perceived severity, and perceived vulnerability toward computer security practices affect college student adoption of computer security practices?

2. To what extent do perceived ease of use, perceived computer self-efficacy, and perceived response efficacy toward computer security practices affect college student adoption of computer security practices?

3. To what extent do attitudes, subjective norms, and perceived behavioral control toward computer security practices affect college student adoption of computer security practices?

4. To what extent does awareness toward computer security practices affect college student adoption of computer security practices?

5. To what extent do demographic factors (age, gender, education level, major, college, and IT experience) toward computer security practices affect college student adoption of computer security practices?

Hypotheses

- Hypothesis 1. Increased levels of perceived usefulness, perceived severity, and perceived vulnerability will increase college students' likelihood of adopting computer security practices.
    - Null. There is no association between (perceived usefulness, perceived severity, and perceived vulnerability) and the adoption of computer security practices among college students.
- Hypothesis 2. Increased levels of perceived ease of use, perceived computer self-efficacy, and perceived response efficacy will increase college students' likelihood of adopting computer security practices.
    - Null. There is no association between (perceived ease of use, perceived computer self-efficacy, and perceived response efficacy) and the adoption of computer security practices among college students.
- Hypothesis 3. Increased levels of attitudes, subjective norms, and perceived behavioral control will increase college students' likelihood of adopting computer security practices.
    - Null. There is no association between (attitudes, subjective norms, and perceived behavioral control) and the adoption of computer security practices among college students.
- Hypothesis 4. Increased levels of perceived awareness will increase college students' likelihood of adopting computer security practices.
    - Null. There is no association between perceived awareness and the adoption of computer security practices among college students.

- Hypothesis 5. Demographic variables (age, gender, education level, major, college, and IT experience) influence college students' adoption of computer security practices.
    - Null. Demographic variables (age, gender, education level, major, college, and IT experience) do not influence college students' adoption of computer security practices.

Limitations and Delimitations

There are no studies without limitations or delimitations. This research utilizes a convenience sampling design, a non-probability technique that yields lower levels of external validity. The data collection period took place during the summer semester when many students were not enrolled in courses on campus, limiting the available pool of students for the research. Researcher bias also, in being present when students filled out the survey, may have altered students' opinions or the way they filled out the questionnaires. More importantly, correlational designs are suited only to study associations between variables and do not provide the capability to conclude causal links between the independent variables and the outcome variable in this research.

Definition of Terms

Table 1 shows the definition of terms used in the present study.

Table 1.

Definitions of Terms

Term	Definition	Source
Computer Security Practices	A wide range of specific behaviors users may adopt and implement to protect the integrity, reliability, availability, accessibility, and other related aspects to their information and machines.	Ng, Kankanhalli, and Xu (2009)
Severity of Threats	"The degree to which respondents' are concerned with the severity of computer security threats posed during their home use."	Boer and Seydel (1996).
Vulnerability of Threats	"The degree to which respondents believe they are vulnerable to computer security threats posed during their home use"	Boer and Seydel (1996)
Response Efficacy	"The degree to which respondents believe that the recommended action deal with and avoid the computer security threats."	Boer and Seydel (1996)
Computer Self-efficacy	"A judgment of one's capability to use a computer."	Compeau and Higgins(1995)
Attitudes	"Attitude is a psychological tendency which is shown in the evaluation on certain entities with some degree of favor or disfavor."	Eagly and Chaiken (1993)
Subjective Norms	"Subjective norms are one's perceptions or assumptions about others' expectations of certain behaviors that one will or will not perform"	Huda, Rini, Mardoni and Putra, (2012)

Table 1 *continued*

Perceived Behavioral Control	"One's perceived ease or difficulty in performing one particular behavior."	Ajzen (2005)
Perceived Usefulness	"The degree to which a person believes that using a particular system would enhance his or her job performance."	Davis, Bagozzi, and Warshaw (1989)
Perceived Ease of Use	"The degree to which a person believes that using a system would be free of effort."	Davis, Bagozzi, and Warshaw (1989)

Assumptions

This research assumed that ordinary computer users differ from each other with respect to their information security practices, and this difference may be objectively studied. It also assumed that this difference can be predicted using correlates, an assumption of the general scientific method approach. Further, the study assumed that survey responses would yield truthful responses from individuals who chose to participate in the study, allowing for exploring real patterns in information security practices behavior. The researcher assumed that the obtained sample from Midwestern University students would approximately reflect the population of college students in the United States.

Contribution

The findings of this study can help university administrators design an appropriate security, education, training, and awareness (SETA) program to mitigate the risks of information security threats. SETA programs assist universities in creating human firewalls. Human firewall refers to the idea that if people within an organization are properly educated, coached, and mentored on how to prevent and deal with information security risks, and they are aware of the

great threats posed to systems, then they will form another layer of protection to the information infrastructure at the organization.

The findings of this dissertation will also benefit the business and productivity of universities and colleges. Having an educated workforce as well as a vigilant student body with respect to information security threats, the university minimizes the risks of losing essential or important records, information, or data that is significant to its business and service objectives. Knowing the factors influencing students' adoption of security practices helps administrators draft better policies, programs, and protocols to protect students' crucial information and make them more efficient in preventing and dealing with information risks.

The results of the dissertation will also shed light on the contemporary debate concerning the predictors of computer security practices. The findings will allow researchers to compare the predictive power of three different, well-established behavioral models in information security: technology acceptance model, theory of planned behavior, and protection motivation theory. This allows future researchers to refine their models and construct more context-specific formulations for studying various populations with respect to the same underlying subject, the adoption of computer security practices.

Chapter 2: Literature Review

This chapter provides a foundational conceptual and empirical note on the definitions of computer users, their attitudes and behavior with respect to the best practices of computer security, and the proposed theoretical frameworks explaining user adoption of security practices. Computer users are viewed as those who do not possess advanced information technology knowledge and utilize their machines merely for ordinary use, studying, shopping, banking, and surfing the web. Existing surveys concluded that computer users suffer from low levels of education, training, and awareness with respect to the best practices of securing computers. While few studies found that awareness is high among certain segments of the population of young users and college students, such groups are also found guilty of not practicing what they know, jeopardizing their machines and information. Finally, the chapter includes a brief discussion on the theories used by authors to explain why some users adopt security practices while others do not. This discussion includes a brief introduction of the health belief model, technology acceptance model, and protection motivation theory. This section also outlines the empirical support for each proposed model and how it is situated with the overall picture of security practices adoption and implementation.

Computer Users

Despite the growing number of studies on computer users' security practices, there has been no consensus on what constitutes a typical computer user (Arachchilage & Love, 2014; Bartsch & Dienlin, 2016). Computer users can be college students who simply use their machines for educational purposes. They can be working adults who shop, bank, and network online. They can be anyone who uses a computer from the home environment to conduct any activity. This population is huge and difficult to estimate. Recent estimates suggested that more

than 40% of the world population is connected to the World Wide Web (Davidson, 2015). This study excluded users with formal IT training and those who developed solutions for IT associated risks. The clear majority of computer users lack any type of formal IT training and have little to no experience with information security (Wash, 2010). This study focused on a sub-group of computer users, college students.

Computer Users Security Practices

Reznik, et al. (2011) conducted a survey on 3,000 students at Rochester Institute of Technology in the winter semester of 2010, asking respondents to report their awareness, training, and education levels concerning computer security practices. The study found that about 33% of respondents practice strong password setting standards, that is, the use of numbers, alternating cases, and symbols. Older individuals, 35 and higher, were found to practice less safe password setting habits by only using numbers to increase the complexity of their passwords. The age group spanning from 26 to 35 was found to be the most cautious group in setting strong passwords. Password setting practices did not differ greatly from critical passwords (those used for financial institutions or government sites) to non-critical passwords (those used for less important webpages in the perception of the user). Results of the study also indicated that Linux or Unix users have better security practices and compliance compared to Windows or Mac OS users. The study also found that users under the age of 21 and those between the ages of 35 and 50 do not differ in practicing security standards or using a firewall, anti-virus software, and anti-spyware. Finally, the study found that Linux/Unix users practice systems and network security standards at a more frequent and intense rate compared to Windows or Mac OS users.

One of the most frequently mentioned security practices for computer users is backing up their data regularly. BackBlaze, a computer security webpage, has conducted an annual survey

since 2008 asking respondents about the frequency of backing up their information. Figure 2 indicates that users are slowly adopting healthy habits of backing up their data daily. Most users back up their data yearly, and the percentage of such individuals is on the rise as can be seen in the figure below. The simple survey concluded, in 2017, that 91% of Americans do not back up their information on a daily basis.

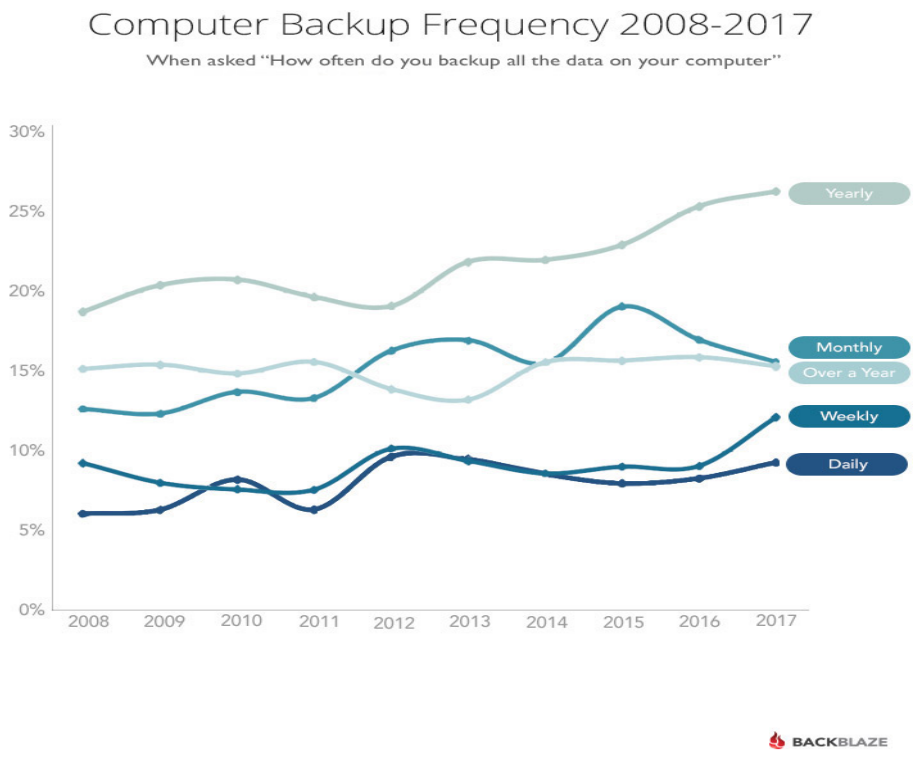

Figure 2. Computer backup frequency 2008-2017 (Klien, 2017).

An earlier survey of undergraduate students at Indiana University of Pennsylvania in 2004 found that almost 40% of the 213 respondents surveyed never updated their anti-virus software (Tekerek & Tekerek, 2013). This figure increased to 50% once students were asked regarding their updating of antispyware software. The survey also found that about 45% of users did not use or know about the use of firewalls. About 50% of respondents did not use unique or

complex passwords. The survey also found that only 8% of users secured their wireless networks.

A recent survey conducted by Pew Research in the Spring of 2016 indicated that 64% of respondents experienced major data breaches. The study also found that 50% of Americans do not trust the Federal government or social media sites in protecting their private information. About 40% of Americans encountered fraudulent charges on their cards, and 35% received a form of notice informing them that some of their sensitive information had been compromised. The study reported that only 12% of Americans use password management software and 3% rely on this technique to generate their passwords. Sixty-five percent of internet users simply rely on memorization to remember their passwords while 40% of Americans reported that they shared their passwords with someone (a friend or family member), and 40% also indicated that they use the same or very similar passwords to access different platforms online. About 30% of Americans do not use best practices for securing their smartphones, such as the use of screen locks or similar features.

The Internet Crime Compliance Center (IC3), a joint venture between the Federal Bureau of Investigation and the National White Collar Crime Center, has found that college students are special targets for cybercrime. Many warnings have been released urging college students to avoid internet scams, such as that of January 2015 when fake companies emailed lists of students, asking them to provide their banking account information to set up direct deposits. During the last two years, college students have been subjected to national scam campaigns including receiving phone calls from thieves claiming affiliation with the Internal Revenue Services or Homeland Security. Therefore, to assist in the effort of fighting cybercrime, this study focuses on college students adopting computer security practices during their use.

Recent surveys have demonstrated that students do not regularly update their security software that protects them from malware infections. Those surveys have also indicated that students rarely update their personal passwords and fail to remove their usernames and credentials from public machines. Many also overwhelmingly choose to open pop-ups where their information could be jeopardized. Students also are more likely to post their personal information online for variety of uses at a rate higher than other groups (Garrison & Posey, 2006).

Explaining Computer Users' Adoption of Computer Security Practices

Empirical scholarship on the factors influencing computer users' adoption of security practices is limited (Arachchilage & Love, 2013; Liang & Xue, 2010; Howe, et al., 2012; Ng, Kankanhalli, & Xu, 2009). Many theoretical models have been utilized to explain users' computer security behaviors (Crossler, et al., 2013). IT researchers have thought of the adoption of computer security measures as protective behaviors, like those individuals undertake to avoid or mitigate the occurrence of negative health conditions (DiGiusto, 2008). This has led researchers to utilize the health benefit model, as well as protection motivation theory, in studies of human protective measures in computer usage (Ng, et al., 2009). Another group of scholars thought of security measure adoption as a similar behavior to the adoption of a new technology or a related aspect to it (Jones, McCarthy, & Halawi, 2010). Therefore, the utilization of technology acceptance models in various forms has been prevalent in the computer security practice literature. In addition to the use of health and technology models, researchers have heavily investigated the role of security practices awareness in increasing the frequency and intensity of computer security practices among users (Teer, Kruck & Kruck, 2007). The following section will outline the most utilized theoretical frameworks and their statistical

support in explaining the adoption of computer security practices outside of the organizational context.

Health Belief Model

The health belief model (HBM) was developed by behavioral researchers in the 1950s to investigate the influence of an individuals' attitude toward illness, specifically, on their likelihood of undertaking protective measures, avoiding whatever initiates or exacerbates such a condition. Its earlier applications concerned the avoidance of patients to tuberculosis diagnostic checks after the Second World War (Janz & Becker, 1984). Underlying logic of the model entails that individuals will value specific goals and perform actions to advance such outcomes in order to score health benefits. People do not want to worsen their illness; the goal, thus is motivating them to engage in actions and behaviors serving that goal. Over time, the HBM shown in figure 3, has been applied to a wide range of health-related, behavioral, and social behaviors.

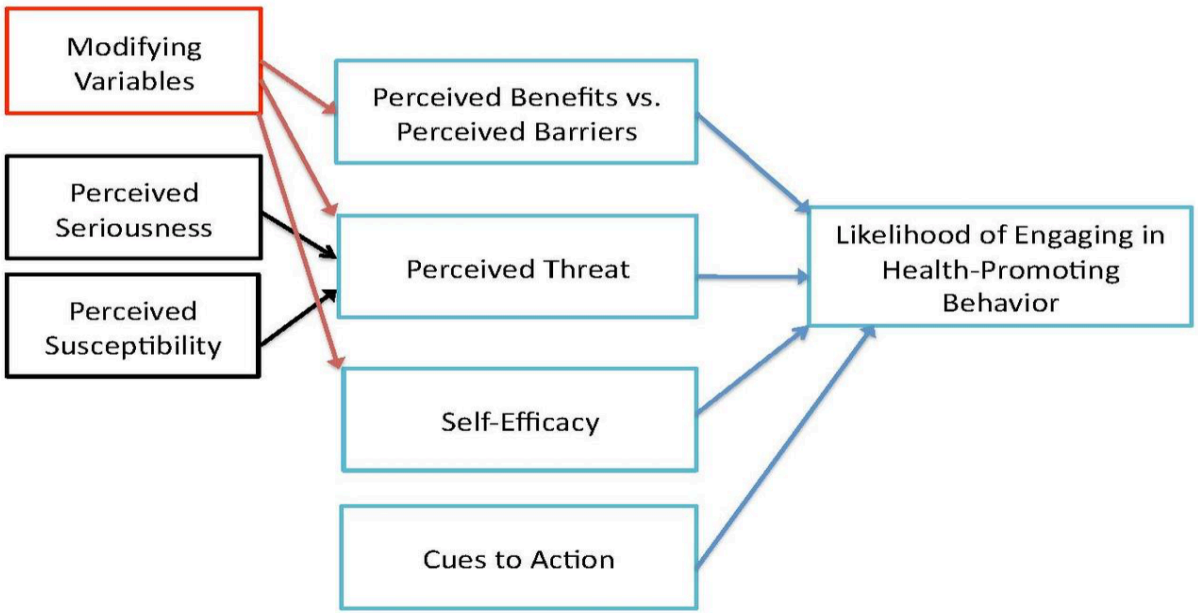

Figure 3. The Health-Belief Model (Janz & Becker, 1984).

First, perceived susceptibility refers to the chance of getting the condition or engaging in the behavior in question. Second, perceived severity refers to the level of harm associated with the behavior. Third, perceived benefits denote any utility obtained from the engagement of the behavior. Fourth, perceived barriers refer to the challenges preventing the individual from engaging in the action in question. Fifth, cues to action are any helpful information provided by the environment of the individual that guides him or her to engage in the behavior. Finally, self-efficacy refers to the potency of the individual to cope and manage the behavior or condition studied.

The HBM framework suggests that demographic characteristics of individuals, such as age, gender, education, etc., influence peoples' perceptions of their susceptibility of getting a condition. Their levels of computer self-efficacy cope with threats, the severity of such risks, and the benefits and barriers to getting and dealing with negative conditions. Individual's perceived

certainty of getting a condition influences their perceived levels of threat. The HBM also asserts that perceived benefits assist in reducing the likelihood of obtaining the condition, but perceived barriers impede the individuals' ability to avoid it, and the expectations of individuals regarding the condition thus influences their action. Individuals' computer self-efficacy is expected to influence perceptions of susceptibility, threats, and expectations, and the higher it gets the more an individual is poised to undertake behaviors avoiding the condition. Finally, the HBM does not neglect the influence of the external environment, where cues can assist the individual to engage in positive or negative behaviors that influence actions taken.

The empirical evaluation of the HBM framework in the health sciences has been plentiful. Studies of vaccination behavior found perceived susceptibility, threat, benefits, and barriers to be robust predictors of individuals' vaccination behavior. Similarly, researchers have applied the HBM to investigate whether breast cancer screenings could be predicted using the model. The findings of this research agenda can be summarized with the suggestion that higher perceived benefits of screenings, higher exposure to helpful information, higher perceived threats, and lower barriers are associated with higher probability of women seeking screening tests.

Few authors have critiqued the HBM theoretical framework when explaining health related behaviors (Taylor, 2007). One view suggested that the HBM is a psychological model based on individual perceptions, neglecting other factors such as habits in explaining outcomes. Therefore, HBM models suffer from biased specifications when designed to explain an outcome in correlational studies. Second, the HBM specifies relationships between unobserved constructs, raising the chances of committing measurement error and resulting in more varied findings.

Statistical evidence.

The HBM theoretical framework has been one of the most widely used models in the investigation of computer security practice. Ng, et al. (2009) applied the model to analyzing the predictors of email security behavior among computer users. The study modified the model by including additional attitudinal constructs such as the general security perceptions. Similarly, Clear (2011) used the HBM, with slight modifications, to analyze the factors influencing the adoption of computer security behavior. Authors have used different labels to refer to HBM in their models, as in the case of Liang and Xue (2010) who studied the predictors of security risk avoidance. They changed the names of certain constructs, such as perceived barriers and benefits, and referred to them as safeguarding measures. Their modified model was referred to as the threat technology avoidance model. Similar to health-related behaviors, the empirical evidence on the predictive ability of HBM to computer security practice is robust. Higher perceptions of threats, computer self-efficacy, susceptibility, and benefits are all positively related to adopting and practicing computer security practices.

Ng et al. (2009) investigated individuals' computer security practices in an organizational setting. Using a survey instrument, they collected data on HBM constructs from a sample of employees at an organization. They found that computer self-efficacy, perceived susceptibility, and perceived benefits to be robust predictors of computer security measures. They suggested that cues to action, perceived barriers, general orientation to security, and perceived severity are insignificant in influencing individuals' computer security practices. Despite their significance to affect the practice of computer security among organizations' staffs, those factors would have a bigger effect when interacting with each other. For instance, perceived severity alone may not make IT professionals adopt or engage in more security practices, however, when coupled with

awareness programs and training workshops, it becomes more powerful in determining employee behavior.

Clear (2011) investigated whether the HBM framework was a robust explanatory framework for the adoption of computer security practices among college students. The research utilized the HBM to analyze whether perceived vulnerability, severity, benefits, barriers, computer self-efficacy, and cues to action determine students' computer security behavior. The findings suggested that computer self-efficacy and perceived vulnerability constituted the best predictors to student behavior. On the other hand, perceived severity, cues to action, perceived benefits, and barriers were not found to be significant in determining students' actions. These results may be due to the assumption that experienced users, those who suffered malware incidents, believe that they will be threatened by such dangers regardless of whether they perform protective measures.

Technology Acceptance Models

Technology acceptance models are a set of theoretical frameworks based on earlier behavioral theories. Theory of reasoned action and planned behavior theory explain users' acceptance and use of a particular technology or aspects relevant to it. In the mid-1970s, social psychologists Fishbien and Ajzen (1977) suggested that an individuals' attitudes and subjective norms regarding a specific action influence their actual engagement in such a behavior. Attitudes refer to the positive or negative feeling of the individual toward the particular behavior. Subjective norms refer to the individual's perceptions of whether those important to him view the behavior as positive or negative. Building on the theory of reasoned action (TRA) model, Ajzen (1985) developed what has become known as the theory of planned behavior (TPB). This theory simply added a third construct to the two specified by the TRA model, namely perceived

behavioral control. This refers to the ability of the individual to control his or her engagement with the behavior. The TRA and TPB have been widely tested and found to be significantly useful in predicting the adoption and engagement in of a variety of psychological and social behaviors.

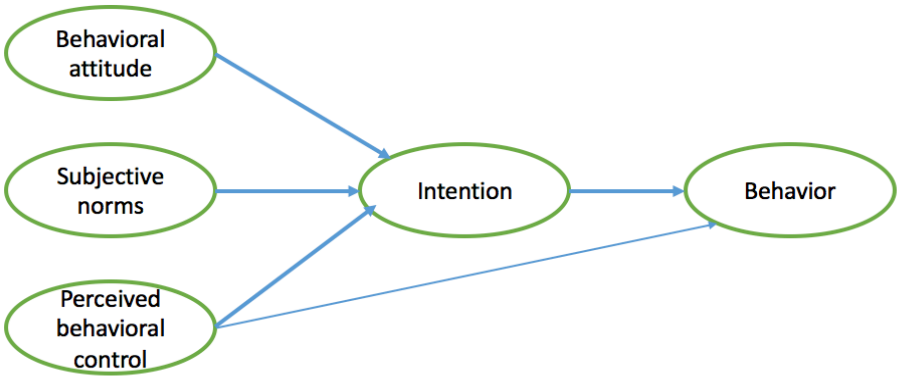

Figure 4. Theory of planned behavior (Ajzen, 2011).

The original technology acceptance model developed by Davis (1986, 1989) is depicted in figure 5 below. The technology acceptance model (TAM) has been found to be one of the most robust models that explain and predict users' adoption of new technologies and their related practices. TAM is grounded in earlier behavioral theories, theory of reasoned action and theory of planned behavior, and is easily implemented across a wide range of applications in information technology. According to the original representation, two main factors influence users' attitudes about adopting and implementing technologies and their practices: perceived ease of use and perceived usefulness. As shown in the model, users' actual utilization of technologies is influenced by their perceived usefulness, ease of use and external variables, their attitudes towards the technology, subjective norms, and their behavioral control.

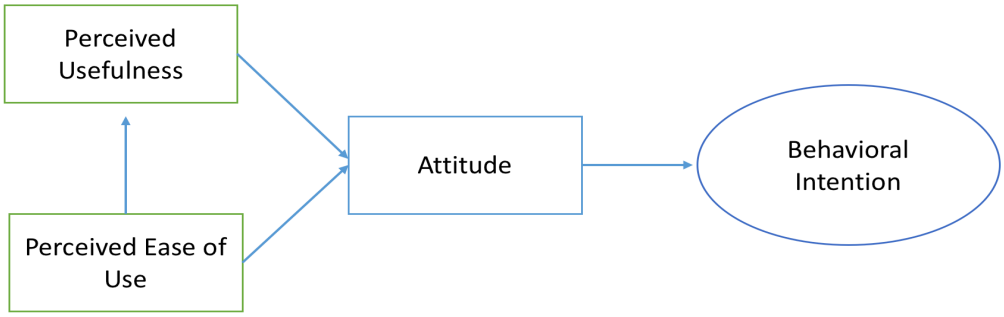

Figure 5. Technology acceptance model (Davis, 1989).

Studies have shown that the TAM accounts for 40% to 50% of users' acceptance and use of new technologies and practices. Over the past three decades, TAM has evolved and new variables have been introduced to the original model as will be discussed later in this section in the unified theory of acceptance and use of technology. Trying to understand the predictors of adoption and use of information technology in organizations, Davis (1989) built on the above models to construct the TAM. The TAM, shown in figure 6, simply suggests that perceived ease and perceived usefulness of a technology or aspect relevant to it will influence an individuals' decision to adopt and use it. The model has been widely tested on a variety of contexts and found to be robust. Perceived usefulness refers to the extent to which the individual finds the technology useful in performing work. Perceived ease refers to the extent to which individuals can learn the technology without investing much effort (Davis & Venkatesh, 1996; Davis, 1993).

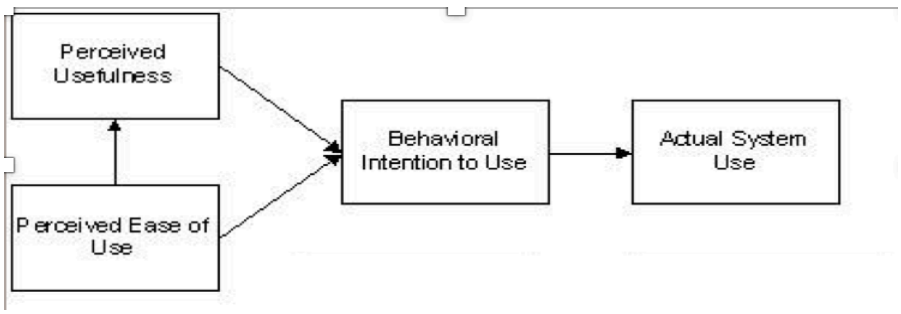

*Figure 6***.** Technology acceptance model (Venkatesh, Morris, Davis, & Davis, 2003).

Like the HBM framework, TAM has seen much modification by many authors since its inception. Trying to unify most of these, Venkatash et al. (2003) blended several technology acceptance models and constructed what they called the unified theory of acceptance and use of technology (UTAUT), shown in figure 7. This theory suggested that performance expectancy, effort expectancy, social influence, and facilitating conditions all influence individuals' adoption and use of technology. Demographic variables are included in the model as mediating factors to the main constructs presented by the model. Using a number of statistical analyses, cross-sectional as well as longitudinal, the authors have established the validation of the model as a robust explanatory framework to the adoption and use of technology.

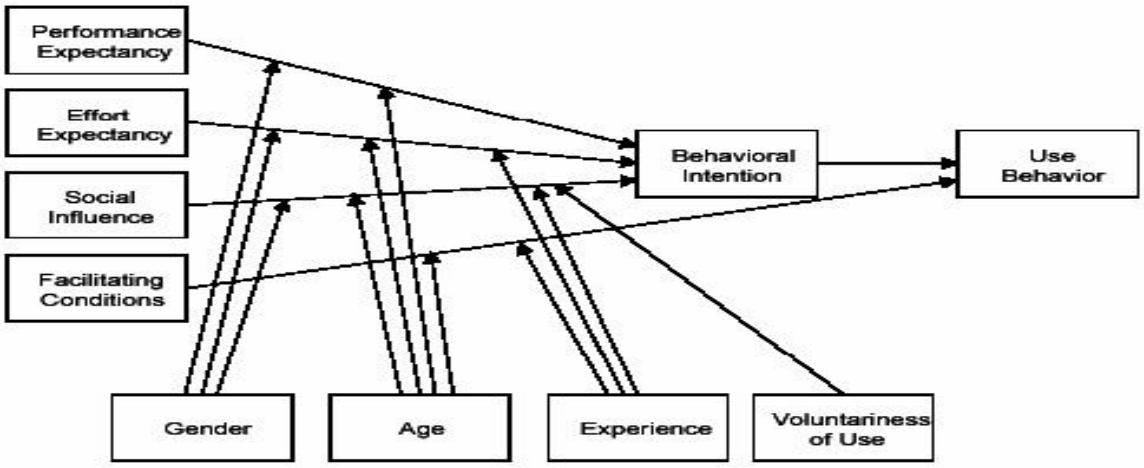

Figure 7. Unified theory of technology use and acceptance (Venkatesh et al., 2003).

More recently Venkatash et al. (2003) have refined the unified theory of acceptance and use of technology to be more applicable to ordinary household users. This marks a departure from earlier models since they have heavily focused on organizational or large enterprise audiences. Within the new model, referred to as the model of adoption of technology in households, three main domains are theorized to influence individuals' decision to adopt a new

technology in the household. These are attitudinal, normative, and control constructs. The first domain included individuals' perceptions about utility in personal, family, and work-related usage. In the second domain, constructs related to perceptions of how family, friends, and coworkers perceive the technology are specified. Finally, control constructs, such as necessary effort, perceived usefulness, cost, and adaptability to changes in technology, are included.

Statistical evidence.

Conklin (2006) used the diffusion of innovation (DOI) theory to investigate computer users' security practices. This has shifted the interest from the organizational to the domestic setting, a new research agenda. Conklin's' model included five factors: characteristics of the individual and innovation, communication channels, social consequences, and the decision to adopt. The intended behavior of the research, the outcome variable, was whether an individual will purchase security software. Using 356 completed online surveys from a non-probability sample, Conklin fitted the model using structural equation modeling. Findings of the model indicated that the software characteristics and social consequences were significant factors in deciding the behavior of users.

Liang (2010) analyzed the factors of using antispyware software among personal computer users. Using survey research, he collected information of perceived susceptibility, severity, threat, and safeguard effectiveness. This study was among the first attempts to validate a modified model of technology use and acceptance. The paper found that users engage in computer security practices if they perceive real and avoidable threats. More importantly, the study suggested that perceived susceptibility and severity motivate users to avoid malicious threats. Their effects are mediated by threat perception, a finding that clarifies the literatures' empirical inconsistencies regarding those factors' effects on computer security measures.

Contrary to conventional wisdom, the study found that safeguard effectiveness and threat perception has a negative effect on the threat avoidance outcome when they interact. As one increases it leads to a weaker effect by the other on antispyware solution adoption among personal computer users. The authors suspect that such a counterintuitive effect is a result of a methodological misspecification.

McGregor, et al. (2015) investigated the predictors of journalists' adoption of computer security tools and practices. They collected data from 15 journalists in the United States and France through lengthy semi-structured interviews. They found that usability and specific aspects to the journalistic process prevented journalists from adopting or practicing computer security tools. Governmental oversight, physical security concerns, and a desire to protect the professional standards of confidentiality have all influenced journalists' decisions to adopt or refrain from computer security practice. The authors suggested that researchers within information security need to incorporate specific variables relevant to the population under study when conducting computer security practice research.

Jones, et al. (2010), analyzed the factors leading employees to adopt security practices in various organizations across the United States and Canada. Using 174 valid responses, they found that the technology acceptance model constituted a useful explanatory framework for the adoption and practice of computer security measures among employees. The partial least squares analysis indicated that the path coefficients of perceived usefulness and perceived ease of use were positive and significant. Analysis also found that subjective norms had a significantly positive effect, mediated by top management support, on the employees' adoption of computer security measures.

Protection Motivation Theory.

Protection motivation theory (PMT) originated within fear appeals research on health outcomes in the late 1960s. In essence, individuals appraise the risks associated with certain behaviors, as well as their coping skills in dealing with such actions. The product of this process is an intention to do something, which likely leads to the action. This outcome may improve or deteriorate the conditions of individuals. Rogers (1983) refined fear appeal and behavioral research models to propose the PMT framework.

The theory, shown in figure 8, suggests that threat appraisals, as well as coping appraisals, influence individuals' actions. Threat appraisals are products of perceived vulnerability and severity of a particular behavior. Perceived vulnerability refers to the extent to which the individual thinks she or he will fall victim to the condition. Perceived severity refers to the extent to which the condition is believed to have a negative impact. Coping appraisal is the product of response and computer self-efficacy. Response efficacy refers to the degree to which the individual believes that the recommendation or information provided on the condition is helpful. Computer self-efficacy refers to the perceived ability of individuals to cope with the condition if attained (Celik & Yesilyurt, 2013).

The PMT framework has been widely applied to studying health and non-health related behaviors. Initially the model was used to investigate whether patients engaged in protective actions to avoid deteriorating conditions of cancer, asthma, and addiction. The findings have indicated that threat appraisals and coping appraisal are significant predictors of human behavior. Similarly, the theory has been applied to studying a variety of social and economic behaviors such as compliance with organizations' policies.

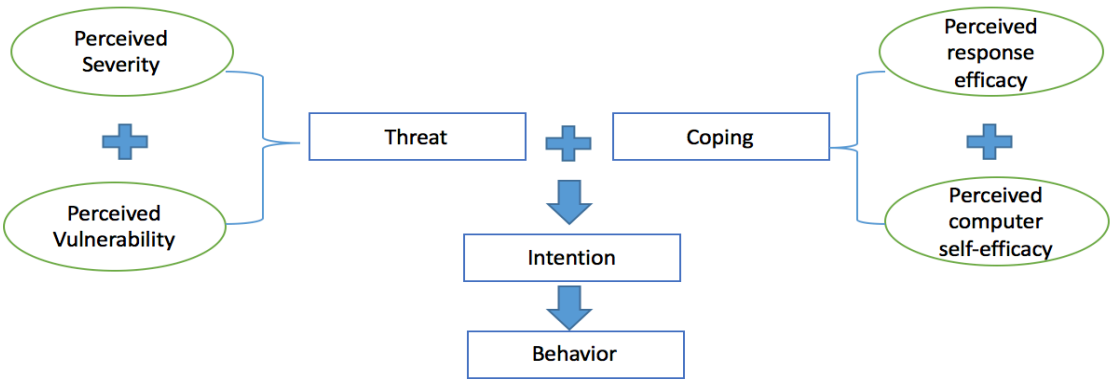

Figure 8. Protection motivation theory (Woon, Tan, & Low, 2005).

Statistical evidence.

Woon, Tan, and Low (2005) investigated the empirical fit of the protective motivation model on network security behavior. Their dependent variable was a binary measure of whether individuals enabled network security features or not. They used the PMT model with five independent variables: perceived vulnerability, perceived severity, self-efficacy, response efficacy, and cost efficacy. They found that PMT constituted a satisfactory explanation for security practices concerning computer networks. Interestingly, the authors found no support for their hypothesis, claiming a positive relationship between perceived vulnerability and security behavior. This finding suggested that increasing awareness on the possible risks associated with the lack of secure computer networks at homes may not influence the action of users. However, if users felt that the threats posed to their privacy and personal data were severe, they will be more likely to enable network security measures. The authors also alluded to the positive relationship between computer self-efficacy and the adoption and implementation of computer security behavior (Woon et al. 2005).

DiGiusto (2008) replicated Woon, et al.'s study using a sample of computer users in New Zealand. He used the protection motivation theoretical model to predict whether perceived

vulnerability, severity, computer self-efficacy (response and cost), and rewards influenced users' intentions to enable wireless network security features. The data was collected through an online survey with 33 items from two groups of users. Analysis found that perceived severity and vulnerability were not significant in predicting users' intentions to enable network security measures. On the other hand, computer self-efficacy was found to be a robust factor increasing individuals' computer security awareness, as well as practice (DiGiusto, 2008). The unexpected findings are ascribed to the belief that people require further assistance to set up secure networks when they feel vulnerable or threatened severely.

Awareness and Computer Security Practice

Teer et al. (2007) surveyed 86 students at James Madison University in Virginia, questioning them regarding their computer security perceptions and practices. The majority, more than 70%, of students reported that they installed antivirus software that they regularly update. They also indicated that they verify email senders prior to opening them, as well as install patches for their operating systems. The authors acknowledge that the study possessed few limitations with regard to the sample, questionnaire, and social desirability.

David and Shannon (2007) investigated whether awareness of security practices influenced college students' computer safety practices. Analyzing 867 responses provided by students attending universities in Nigeria, they found that students practice safety measures in six of their ten practices. These were simple passwords, sophisticated passwords, email scans, antivirus, firewall, and systems scams. The authors have only described the data obtained and did not delve into analyzing the correlates of security practices among students. The survey used was widely criticized by many researchers as the authors indicated before its implementation.

Mensch and Wilkie (2011) conducted a descriptive study investigating the attitudes and behaviors of undergraduate and graduate students' security practices. They found that age was related to certain aspects of computer use practice. Older individuals seemed to be more apt to implement security practices compared to younger students. The authors provided a detailed recommendation for universities to enhance security awareness among students and increase the safety of their computers.

Huang et al. (2011) used an experimental research design to investigate whether the increase of knowledge regarding security practices influenced individuals' computer security practice. Using two experiments, 64 participants each, the study concluded that raising awareness on the potential benefits and risks associated with e-banking in experiment one, and password setting in experiment two, affected the intentions and actions of participants. Higher levels of information security awareness were associated with better computer security practices. The authors encouraged future experimental research on other potential constructs that may improve security practices among computer users.

Summary

This chapter outlined the existing scholarship on computer users' definitions and attitudes toward computer security awareness, training, and security, and the available surveys on their compliance with computer security best practices. It also discussed the various theoretical models proposed by authors to explain the variation in adopting and implementing computer security practices among users. This discussion included the theoretical and empirical scholarship on the links between the TAM, TPB, PMT, and awareness, and computer security awareness. Finally, a brief discussion on the empirical support of each model has been presented.

All in all, the study of the adoption of computer security practices among college students is limited and warrants expansion, which is the endeavor of this dissertation.

Chapter 3: Methodology

This chapter outlines the methodology, research design, data collection, and data analysis techniques utilized by this study. Correlational descriptive design is the most appropriate design, given the goal of the dissertation of analyzing relationships among a set of quantitative variables. The data was collected by administering a questionnaire to a sample of 301 college students at a university in the Midwestern region of the United States. Once the data was obtained, the researcher utilized one-way analysis of variance (ANOVA) and multiple linear regression analysis to estimate the proposed model.

Research Design

This research investigated the association between several predictors and a given outcome. The appropriate research design for this type of analysis is correlational. Correlational research designs aim to explore the associations among several variables. This study analyzed the relationship between the technology acceptance model (TAM), theory of planned behavior (TPB), protection motivation theory (PMT), awareness, and demographic constructs as well as computer security practices among college students.

The design of the study was cross-sectional as well. Research analyzed the relationship among the variables at one point in time and with a single sample, contrary to longitudinal designs where the research measures the same variables using the same sample over time. Cross-sectional designs only measure variables on one sample at once. This makes it one of the weakest designs when it comes to establishing robust generalizable inferences. Nevertheless, most survey research is characterized as cross-sectional given the cost-effectiveness of such designs.

Population and Sample

The target population for the study is all students attending a Midwestern university. This includes full-time, as well as part-time, students in all majors across the five colleges at the university. The researcher obtained the sample from that university located in Southeast Michigan.

The university was established in 1849 and was known as a normal school, then a college, and finally a university. The university offers about 200 majors, minors, graduate degrees, and special certifications, and has five colleges: arts and sciences, technology, education, health and human services, and business. The university has about 700 international students from 40 countries around the world. As of the fall of 2016, the university had a total enrollment of 21,105 students, of which 17,541 were undergraduates. The number of female students attending the university in fall 2016 was 10,417, and the number of male students was 7,124. Ethnically, 11,303 students were Caucasian, 3,416 were African-American, 846 were Hispanic, and almost 2,000 identified as another ethnicity.

To obtain the sample for the study, the researcher utilized convenience sampling design. Convenience sampling refers to the process of selecting research subjects based on accessibility, availability, and the readiness of subjects to participate in each study. It is the easiest to administer sampling technique. Convenience sampling is cost-effective and, more importantly, yields a higher response rate. While probability sampling designs, such as simple random sampling, could be used with the help of the Office of Institutional Research and Information Management at the university, participants were not contacted face-to-face, thus generating a lower response rate as well as a longer time-frame for completing the research. To overcome

such problems, the researcher was in the field, the university's campus, and administered the survey instrument physically to students in their classrooms.

The researcher reached out to faculty teaching courses in the fall semester at the university to obtain permission to distribute the survey in their classrooms. The researcher contacted teaching faculty during September of 2017, seeking their permission to administer the questionnaire in their classrooms. The researcher asked instructors to appear to their classrooms and hand out the survey in the first or final 15 minutes of the class. Before beginning the completion of surveys, the researcher explained the purpose of the project, went over the consent form, and ensured mentioning that participation in strictly voluntary. The researcher obtained the consent of each student before they filled out the survey by administering informed consent forms to the classroom prior to the filling out of the survey (see Appendix A). Students used traditional paper and pencil methods to complete the questionnaires in class before leaving the classroom. This method is likely to increase response rate, ensure data availability in a quick time, and allow the researcher to complete the project according the scheduled timeline.

It is difficult to estimate the sample size for this research given the lack of information on students' computer security practices or attitudes. Therefore, the researcher estimated that 300 responses would be sufficient to represent the target population and fulfill the goals of this research. The researcher administered the survey to as many classrooms as necessary to obtain the 300 complete surveys.

Human Subject's Approval

Prior to the collection of relevant information to fulfill the objectives of the study, permission was requested from the institutional review board (IRB) administrators of the university to conduct research on human subjects. A formal application with the board was filed

and the process was completed prior to collect any data (see Appendix B). The students' supervisor at the college of technology ensured that the IRB process is followed meticulously, ensuring the privacy and confidentiality of research subjects and their information.

Data Collection

Survey development and validation.

This study used a pre-prepared paper questionnaire to collect information on college students' computer security practices, perceived vulnerability, perceived severity, response efficacy, computer self-efficacy, perceived usefulness, perceived ease of use, awareness, attitudes, subjective norms, perceived behavioral control concerning computer security practices, and demographic information. Each subject in the study was informed that his or her participation in this research is strictly voluntary and they could choose not to participate at any moment. The questionnaire was developed based on an extensive literature review on computer security practices among computer users. Prior to the development of the questionnaire, the researcher set clear objectives for the study, testing the empirical fit of the proposed model above. To do so, the researcher identified measures for the dependent, as well as independent, variables. Table 2 includes the constructs, items measuring them, and sources that validated such items. In cases where the researcher failed to identify a previously validated measure, new items was created and validated.

While many of the survey items have been previously validated by researchers in the literature, few constructs, especially those related to the theory of planned behavior, have not been fully operationalized with respect to the study of college students' adoption of computer security practices. Thus, scales have been developed to measure individuals' attitudes, subjective norms, and perceived behavioral control with respect to computer security practices. The items

constructed are simple, easy to understand, and clear, possessing both facial and content validity. Note that items borrowed from the literature appeared in the survey instrument as they appear in original research published by their authors. This is done to retain the reliability and validity of the items. To test the reliability and validity of the self-developed constructs, a pilot study was conducted. Ten graduate students from a Midwestern university were contacted to fill out the survey and corrections were made based on results obtained.

Measures

The main dependent variable in the study is computer security practice. One of the most straightforward and clear computer security practices prevalent among users, especially college students, is phishing preventative measures. One of the clearest activities involved in this outcome is checking the authenticity and validity of emails received by users. Rogers (2002) and Ng et al (2009) have developed and validated several items measuring this activity. Checking an email's authenticity, subject, filenames attached, virus infection, and content are a few examples of simple computer security practices college students undertake daily. This study used four items listed in Table 2 to construct a scale measuring college students' computer security practices as the dependent variable in the multiple linear regression analysis that followed data collection.

Computer security practices is a multidimensional construct where it could be measured in several ways. The choice of measurement by this dissertation was to use a simple, accessible, straightforward, and common practice in the daily lives of college students, email verification. While this is a narrow measurement strategy, emails' verification was found to correlate highly with other computer security practices such as password settings, back-up practices, and setting strong checks on personal files. Therefore, it provides a great indicator for the operationalization

of computer security practices. Today's concerns with email security have not changed much from those prevalent in the beginning of the century in the early 2000s. Students are still concerned with infected emails and files attached to them as they were 20 years ago. As a matter of fact, students should be more concerned today than 20 years, given the exponential increase in cybersecurity with the availability of the internet to more criminals. While social media and in house platforms are starting to replace emails in colleges where students no longer send the same amount of emails compared to a decade earlier, students still send many emails for whatever reasons on a daily basis (Garrison & Posey, 2006; Reznik et al., 2011).

This research hypothesized that protection motivation theory, technology acceptance model, and theory of planned behavior directly influence an individual's adoption of computer security practices. Therefore, the independent variables of this research are the constructs specified by each of the three models: perceived vulnerability, perceived severity, computer self-efficacy and response efficacy from protection motivation theory; perceived ease of use, and perceived usefulness from technology acceptance model; and attitudes, subjective norms, and perceived behavioral control from planned behavior theory. In addition to those constructs, awareness has been proposed as an influential factor in determining the variation in the adoption of computer security practices, and therefore, it was included in the survey. This research included demographic variables (age, gender, education level, major, college, and IT experience) as control variables to verify the robustness of the effect of the main independent variables. Note that demographic variables used in this research have been previously cited as control variables, moderating the relationship between the cited independent variables and computer security practices. The measurement strategy for each demographic variable, such as age grouping, has

been designed with the extensive guidance and suggestion of Dr. Dorothy McAllen; this choice was meant to make survey items more readable to respondents generating high response rates.

All items presented in table 2 were validated by the original authors except those that are self-developed by the author of the present study. All items are measured on 1-5 Likert scales where 1 = strongly disagree and 5 = strongly agree.

Validity

The study assessed the construct validity of the survey by considering various approaches. Construct validity refers to the whether the items used to measure the construct in the survey reflects it. Simply put, construct validity aspires to make a statement concerning how well the instrument is measuring what is intended to be measured, the constructs in the study. Validating the survey started by assessing its face validity. The researcher presented the survey to information security experts at a Midwestern university, who evaluated the instrument on its face, whether it constitutes a good operational measure of the intended measured constructs or not. Second, the researcher conducted a content validity analysis for the instrument. This was done by checking the relevant literature and comparing its various ways of operationalization to computer security practices with the instrument developed by this research. Throughout this approach, the researcher was able to identify whether the items used to measure the constructs are representative or existent in the extant literature on information security.

In addition to construct validity, the researcher evaluated the instruments' criterion-validity through evaluating convergent and discriminant validity. Convergent validity refers to how similar the operationalization is to those we expect them to be theoretically similar to. One way to assess this is through examining the correlation structure among a set of items measuring the same construct. If the correlation was high, r = 0.70 or higher, among all items, then

convergent validity is achieved. By the same token, discriminant validity refers to the extent to which the operationalization differs from that operationalization from which it is theoretically expected to diverge. To achieve this, a correlation analysis can be carried out on two constructs that are expected to correlate weakly, and if the result confirmed this expectation, then it is said that discriminant validity is achieved.

Reliability

Reliability refers to the consistency of a given measure or instrument. While there are many estimating techniques for reliability, this study used internal-consistency measures. Internal-consistency refers to how good items measuring the same construct yield similar results. One of the popular measures used for evaluating internal-consistency is Cronbach's alpha. If the value of the measure exceeds 0.70, then we can conclude that the measure is reliable. For each construct, the study estimated its Cronbach's alpha and evaluated where the used items are reliable or not. Prior to data collection, the researcher obtained authors' permission to use their measures.

Table 1**.**

Constructs

Construct	Items	Sources
1-Computer Security Practices	CSP1: Before reading an email, I will first check if the subject and the sender make sense. CSP2: Before opening an email attachment, I will first check if the filename of the attachment makes sense. CSP3: I exercise caution when I receive an email attachment as it may contain a virus. CSP4: I do not open email attachments if the content of the email looks suspicious.	Rogers (2002) and Ng, et al. (2009)
2-Perceived Vulnerability	PV1: The chances of receiving an email attachment with virus are high. PV2: There is a good possibility that I will receive an email attachment with virus. PV3: I am likely to receive an email attachment with virus.	Champion (1984)
3-Perceived Severity	PS1: Having my computer infected by a virus as a result of opening a suspicious email attachment is a serious problem for me. PS2: Losing data as a result of opening a suspicious email attachment is a serious problem for me. PS3: If my computer is infected by a virus as a result of opening a suspicious email attachment, my daily work could be negatively affected.	Woon, Tan, and Low (2005) and Ng, et al. (2009)

Table 2 *continued*

4-Response Efficacy	RE1: In case of receiving a suspicious email, I can react effectively in a timely manner. RE2: I have the necessary skills to deal with an email attachment containing a virus. RE3: Once I detect a suspicious email or attachment, I know how to respond to it.	Self-developed
5- Computer Self-Efficacy	SE1: I am confident of recognizing a suspicious email. SE2: I am confident of recognizing suspicious email headers. SE3: I am confident of recognizing suspicious email attachment filename SE4: I can recognize a suspicious email attachment even if there was no one around to help me.	Ng, et al (2009)
6-Perceived Usefulness	PU1: Checking if the sender and subject make sense is an effective in preventing viruses from infecting my computer. PU2: Checking if the filename of the email attachment makes sense is an effective in preventing viruses from infecting my computer. PU3: Exercising care before opening email attachments is an effective in preventing viruses from infecting my computer.	Ng, et al (2009)

Table 2 *continued*

7-Perceived Ease of Use	PEU1: Exercising care when reading emails with attachments is convenient. PEU2: Exercising care when reading emails with attachments is not time-consuming. PEU3: Exercising care when reading emails with attachments would not require considerable investment of effort other than time. PEU4: Exercising care when reading emails with attachments would not require starting a new habit, which is difficult.	Woon, Tan, and Low (2005) and Champion (1984)
8-Awareness	A1: I read information security bulletins or newsletters. A2: I am concerned about security incidents and try to take action to prevent them. A3: I am interested in information about computer security A4: I am constantly mindful about computer security.	Jayanti and Burns (1998)
9-Attitude Toward Computer Security Practices	ATT1: Computer security is really important. ATT2: Learning how to prevent security incidents is important. ATT3: Investing in learning and developing skills for computer security is an essential quality everyone should have.	Self-developed

Table 2 *continued*

10-Subjective Norms	SN1: My family and friends believe that computer security is important. SN2: My co-workers/classmates believe that computer security is quite essential. SN3: My professors/supervisors at work believe that computer security is very important.	Self-developed
11-Perceived Behavioral Control	PBC1: It is difficult to exercise computer security for me. PBC2: It is difficult to check emails or files for viruses or suspicious material for me. PBC3: It is difficult to cope with a corrupted email or file sent to me.	Self-developed
12- Demographics	Age , Gender, Level of Education, College Major, and IT knowledge/experience in years	Self-developed

Data Analysis

Following the collection of data from the college students, the researcher created a spreadsheet in statistical software SPSS to input the raw data in preparation for analysis. After entering the data into the software, the researcher excluded incomplete responses and miscoding, and then replaced missing data with the mean value of the corresponding item. Prior to the implementation of inferential statistical techniques, the researcher displayed descriptive statistics on all variables, means, standard deviations, bar charts, and frequency distributions to provide an overview of responses. The researcher also evaluated the assumptions of the multiple linear regression analysis and commented on the violations, if detected, and how such misgivings were remedied in subsequent analyses.

After the analysis of survey measures using descriptive techniques, the researcher utilized the analysis of variance (ANOVA) to detect any significant differences on the dependent variable based on demographic attributes. Significant differences were reported and presented in tabular, as well as graphical forms. Prior to the presentation of ordinary least squares tables of coefficients, the researcher reported the bivariate correlations among the variables utilized in the study to inspect the associations and better assess the data readiness for a multiple linear regression analysis, the main technique used by this research to evaluate the relationship between computer security practices and the technology acceptance model, theory of planned behavior, and protection motivation theory.

This study collected quantitative measures on computer security practices and a set of predictors based on protection motivation theory, technology acceptance model, and theory of planned behavior as presented in figure 1 above. To assess the direction and magnitude of relationships between the proposed constructs and the criterion outcome, computer security practices, multiple linear regression analysis was used. Multiple regression provides researchers with information about the predictive weight of two or more independent variables on a single dependent outcome, which is the goal of this research.

In the present research context, the study estimated the effects of perceived vulnerability, perceived severity, response efficacy, computer self-efficacy, practice usefulness, ease of use, awareness, attitudes, subjective norms, and perceived behavioral control concerning computer security practices on college students' adoption of security practices, such as phishing prevention measures as discussed above. Multiple regression produced the best linear combination of scores on the independent variables that best predicted scores on the dependent variable. It generates a statistic referred to as multiple correlation (R), the correlation between predicted scores on the

dependent variable and actual scores. If this correlation was strong and positive, above 0.70, then the result shows that the overall model possesses good fit and explains a significant amount in the variation within the dependent variable.

Multiple regression also provides researchers with regression coefficients indicating the direction and magnitude of the relationship between a given predictor and the criterion, independent of all other predictor variables. This coefficient represents the part of variation explained by that given predictor in the scores of the dependent variable. Using multiple pieces of information, residuals (difference between predicted scores and actual scores) and descriptive statistics of variables, multiple regression calculates a regression coefficient for each variable included in the model. Regression coefficients are the slopes representing the relationship between predictors and the outcome variable. Each coefficient represents the change in the dependent variable, given a one-unit increase in the given predictor holding other predictors constant.

Multiple regression is an appropriate method for data analysis in this research because it provides comparable output statistics allowing the researcher the ability to compare the direction and magnitude of the different predictors used. For instance, the effect of a one-unit increase on subjective norms (SN)1 on CSP1 can be compared to the effect of a one-unit increase on perceived value (PV)1 on the same variable. Multiple regression also supplies researchers with measures of goodness of fit, or how well the model fits the data collected. A high goodness of fit is indicative of the strength of the model, whereas a poor goodness of fit indicates the weakness of the model in explaining the outcome. Multiple regression provides researchers with R-squared as a measure of goodness of fit where larger scores correspond to stronger models. R-squared represents the amount of variation in the dependent variable explained by the model.

Summary

This research aims to explore the factors of computer security practices among college students. College students are one of the most targeted groups for cybercrime, and they are the least likely to practice the recommended actions taken to minimize computer threats during home use. Therefore, this study has set out to explore the factors that make college students adopt and implement computer security practices in their home use of computers.

Chapter 4: Results

This chapter presents the results of the various statistical analyses applied to the survey responses collected throughout this study. First, a descriptive analysis of the sample, dependent variable, and independent variables are carried out. Second, a detailed measurement analysis of the reliability and validity of the instrument is outlined in order to assess the extent to which the survey possesses robust psychometric properties. Finally, the chapter displays the results from the regression analysis, using SPSS to evaluate the empirical support of the research hypotheses proposed in the first chapter.

The data for this research was collected throughout the fall of 2017 semesters at a Midwestern university. Fourteen faculty members were directly contacted about allowing the researcher to distribute the survey in their classrooms. Nine agreed to let the researcher come into their classroom, distribute the survey, and collect them after completion by the students. These classes were in the fields of computer information systems, management, computer science, human resources, engineering management, and the social and natural sciences. The total number of surveys distributed to students was 400, and 301 completed surveys were recovered, which was a response rate of 75%. Classes included freshmen, sophomore, junior, and senior level undergraduate as well as graduate level courses. Class sizes ranged between 15 students to more than 50 students. Five main colleges were represented: college of technology, college of business, college of arts and sciences, college of education, and college of health and human services.

Descriptive Analysis

The survey collected information on the students' age, gender, college affiliation, major, degree type, and information technology experience (measured in years). These include nominal, ordinal, and interval level variables, thus informing the choice of tabular and graphical display for the results. Table 3 represents the samples' distribution by age. Notice that the total number of respondents was 301, 90% of which are between the ages of 18 and 28 and representative of the traditional college age group. Only thirty responds were 29 or older.

Table 2**.**

Sample Distribution by Age

Age Group	Frequency	Valid Percent
18-28	271	90.0
29-38	23	7.6
+39	7	2.3
Total	301	100.0

Table 4 presents the distribution of the sample by college. Forty-eight percent (48%) of the respondents were from the college of business. Other colleges are represented relatively evenly, about fifteen percent each for the colleges of arts and sciences, technology, and health and human services. The least represented college was the college of education, the sample making up only 6% of the total number of respondents. Table 5 displays the samples' distribution based on the college major of the respondent. Notice that the measurement of this indicator is binary, either IT or non-IT. Given the complexity of coding the questions, they were left open ended. It seems that 82% of the total number of respondents is majoring in disciplines

other than computer science, computer information systems, information technology, information management systems, or information assurance.

Table 3.

Sample Distribution by College

College	Frequency	Percent
Technology	46	15
Business	144	48
Education	19	6
Arts and Sciences	45	15
Health and Human Services	48	16

Table 5.

Sample Distribution by Major

Major	Frequency	Percent
Non-IT	247	82
IT	54	18

Table 6 presents the samples' level of education distribution. Notice that 94% of the sample (including high school diploma and associate degree holders as well as upper-level undergraduates), do not have a formal college degree (BA/MS/Ph.D.) awarded by this university. Only about 6% of the sample has previously obtained university awarded formal degrees.

Table 4.

Sample Distribution Based on Level of Education

Highest Level of Education	Frequency	Percent
High School Diploma	95	31
Associate Degree	57	19
Post-Associate with No Bachelors	133	44
Bachelor's	14	5
Graduate Degree (MA/Ph.D. or Equivalent)	2	1

Table 7 displays the samples' distribution of information technology (IT) experience. Sixty-eight percent (68%) reported that they have one to five years of information technology experience. Notice that IT experience is a broad subject area, encompassing the use of computers for personal purposes on an extensive basis which is a typical feature of American college life. Therefore, many may have reported higher than expected levels of experience. Nevertheless, most respondents are traditional college aged students, and therefore. the number of those with the least amount of IT experience is of note.

Table 5.

Sample Distribution based on IT Experience

IT Level of Experience	Frequency	Percent
1-5 Years	207	68
6-10 Years	55	18
11-15 Years	23	8
16-20 Years	12	4

More than 20 Years	5	2

Table 8 presents answers by the respondents to the questions presented in the survey. The distribution of Midwestern university students with respect to computer security practices appears to be significant with a number of respondents agreeing that they embrace and practice computer security practices. For instance, question CSP1 asks respondents to indicate their agreement with the following statement: "Before I read an email I check the subject and the sender if they make sense." About 88% of the survey respondents indicated that they take the time to verify the authenticity of the subject and source of emails prior to opening them. Similarly, 77% of respondents indicated that they ensure that the filename makes sense before opening an email. Another 77% of respondents reported that they exercise caution before opening any received attachment, and 90% of the sample reported that they will not open an attachment if they are suspicious of the content of the email. This indicates that the students in this study seem to adhere to and practice computer security measures in their personal daily use of computers.

Table 8 also displays responses regarding the perceived vulnerability to items. Perceived vulnerability, PV1, refers to the agreement of students with the statement: "The chances of receiving an attachment with a virus are high." It can be observed that only 48% agree with the statement, with 16% disagreeing and an additional 36% remaining neutral toward the statement. By the same token, about 48% of respondents believe that there is "a good possibility that they will receive an attachment with a virus," whereas 26% believe that they will not likely receive a virus embedded attachment via email. Finally, 38% of survey respondents believe that they are likely to actually receive an email with an attachment containing a virus while 36% believe that

they are unlikely to receive one. This result indicates that Midwestern university students do not uniformly agree that the possibility of receiving a virus via email is an eminent threat to their personal computer usage. A significant number of students do not believe that they will be personally targeted with a virus in an attachment.

Table 8 also shows the university students' attitude toward the perceived severity of information security threats to their computers. About 58% believe that having their personal computer infected with a virus is a serious problem, whereas about 30% do not see it as such. Similarly, about 63% of respondents believe that losing data due to a virus coming through an attachment is a serious issue while 26% of respondents did not view this as a serious matter. Finally, around 73% of students reported that if they lost information due to a virus infecting their machines, their work would be negatively affected. Only 10% disagreed with this sentiment.

Students' answers concerning their response efficacy toward information security incidents are also indicated in Table 8. About 66% of respondents agreed that they could deal with an information breach or security threat effectively and timely while 14% reported a lack of response ability. Only 47% reported that they possess the necessary skills to cope with an incident, but about 32% suggested a general lack of knowledge, skills, and abilities in dealing with information security threats in the form of a virus embedded in an attachment. Finally, 52% indicated that they know what to do once they detect a serious threat to their information or computers in an email or attachment while about 30% believe they do not know exactly what to do if faced with the same scenario.

Table 8 displays student responses to computer self-efficacy items related to security and information assurance. Results indicate that about 70% of students are confident that they are

capable of identifying computer security threats, whereas less than 10% believe that they are unable. Concerning the identification of suspicious headers, 75% of respondents believe that they are capable of detecting suspicious email headers while less than 10% indicated a lack of such ability. About 75% of respondents agreed with their ability to detect suspicious titles for attached files while only 10% reported a lack of such ability. Finally, 68% of respondents reported their ability to cope with a suspicious email or attachment without requiring the help of others while 15% reported that they cannot.

Results also indicate that over 80% of respondents believe that checking emails is an effective and useful way of preventing an information security incident. Similarly, about 80% of students at the Midwestern university believe that checking the filename and exercising care before opening an attachment or checking an email prove to be useful techniques in identifying, detecting, and preventing computer security breaches. Survey results also indicate that about 76% believe that it is convenient to exercise care in checking and verifying emails before opening them. Around 70% of respondents believe that checking the filename of an attachment in an email is not time-consuming. By the same token, 73% of this university students believe that it does not require additional effort beyond investing in a bit of time to check and verify emails and attachments for security purposes. Finally, 65% of respondents believe that checking emails or attachments for security reasons does not require them to develop a new habit. All in all, the Midwestern university students believe that computer security practices are useful for protecting their computers and information while being easy to adopt and implement.

Table 8 indicates that only 37% of the sample read information security newsletters and bulletins while about 40% of the university students do not. Further, about 57% of the sample seems to be concerned with information security threats and taking actions to prevent them while

about 20% of students do not. Only 54% of the university students reported that they are interested in reading and consuming information concerning computer security. About 60% of the university students reported a constant mindfulness regarding computer security. This indicates that overall, the sample includes a large portion that is not really concerned with information security and computer risks.

Table 8 also suggests that the university students exhibit positive attitudes toward computer security, learning about risks and how to prevent them. In all three items measuring computer security attitudes among the sample, more than 75% of respondents agreed that computer security, its education, and learning how to prevent threats is important. By the same token, and to a lesser degree, students in this study indicated that their peers, family, friends, co-workers, and professors believe that computer security is important. More than 60% of the sample either agreed or strongly agreed with three statements highlighting the importance of computer security behavior and practices among their close circles.

Table 8 indicates that about 55% of respondents reported that it is difficult for them to exercise computer security practices. Similarly, 60% of the sample suggested that checking emails and files for viruses is not an easy task to learn and undertake. Finally, about 55% of the sample indicated that it is difficult for them to conduct the necessary procedure(s) to intervene in the event of facing a corrupted email with a virus. This indicates that the students in this study seem to possess low perceived behavioral control levels when it comes to computer security practices.

Table 6.

Sample Responses to Core Survey Questions

Item	Frequency and (Percent)				
Responses	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
CSP1	3 (1)	12 (4)	21 (7)	86 (28)	179 (60)
CSP2	4 (1)	22 (7)	45 (15)	90 (30)	140 (47)
CSP3	4 (1)	18 (6)	47 (16)	79 (26)	153 (51)
CSP4	5 (2)	10 (3)	18 (6)	71 (24)	197 (66)
PV1	10 (3)	40 (13)	107 (36)	91 (30)	53 (18)
PV2	10 (3)	70 (23)	79 (26)	84 (28)	58 (20)
PV3	18 (6)	87 (29)	82 (27)	75 (25)	39 (13)
PS1	35 (11)	56 (18)	35 (11)	68 (23)	107 (35)
PS2	39 (13)	40 (14)	37 (12)	61 (21)	124 (42)
PS3	8 (3)	16 (6)	36 (12)	98 (32)	143 (48)
RE1	6 (3)	33 (11)	62 (20)	117 (39)	83 (27)
RE2	30 (10)	65 (22)	64 (21)	72 (24)	70 (23)
RE3	24 (8)	61 (21)	64 (22)	76 (26)	76 (26)
SE1	2 (1)	33 (11)	54 (18)	120 (40)	92 (31)
SE2	2 (1)	25 (8)	50 (16)	125 (42)	100 (33)
SE3	2 (1)	32 (10)	58 (19)	101 (34)	100 (33)
SE4	3 (1)	39 (13)	58 (19)	101 (34)	100 (33)
PU1	0 (0)	11 (4)	46 (15)	127 (43)	11 (39)
PU2	2 (1)	4 (2)	53 (18)	125 (42)	117 (39)
PU3	2 (1)	5 (2)	37 (12)	120 (40)	137 (46)

Table 8 *continued*

Responses	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
PEU1	2 (1)	18 (6)	45 (15)	146 (46)	91 (30)
PEU2	2 (1)	30 (10)	60 (20)	130 (43)	80 (27)
PEU3	2 (1)	21 (7)	59 (19)	126 (42)	93 (31)
PEU4	6 (2)	33 (11)	67 (22)	119 (40)	76 (25)
A1	27 (9)	92 (31)	70 (23)	60 (20)	52 (17)
A2	8 (3)	46 (15)	75 (25)	106 (35)	66 (22)
A3	18 (6)	40 (13)	79 (26)	87 (29)	77 (25)
A4	14 (5)	32 (10)	71 (23)	101 (33)	83 (27)
ATT1	1 (.03)	6 (2)	19 (6.3)	100 (33.2)	175 (58.1)
ATT2	1 (.03)	2 (.07)	23 (7.6)	119 (39.5)	156 (51.8)
ATT3	1 (.03)	0 (0)	40 (13.3)	115 (38.2)	145 (48.2)
SN1	4 (1.3)	16 (5.3)	68 (22.6)	115 (38.2)	98 (32.6)
SN2	5 (1.7)	11 (3.7)	81 (26.9)	112 (37.2)	92 (30.6)
SN3	10 (3.3)	16 (5.3)	47 (15.6)	103 (34.2)	125 (41.5)
PBC1	60 (19.9)	107 (35.5)	56 (18.6)	49 (16.3)	29 (9.6)
PBC2	70 (23.3)	112 (37.2)	60 (16.6)	47 (15.6)	22 (7.3)
PBC3	71(23.6)	90 (29.9)	59 (19.6)	52 (17.3)	28 (9.3)

Instrument Reliability and Validity

Table 9 displays the constructs, their corresponding items, the corrected item total correlation for each item, and the Cronbach alpha of a scale variable composed by summing the responses across corresponding items for each construct. Cronbach's alpha are measures of internal consistency for each construct which indicate the level of reliability for the items and

scale utilized in the analysis. Higher values of alpha correspond to better reliabilities and range between 0 and 1. Any scale possessing a value of 0.7 or higher is considered reliable. Table 9 indicates that all constructs are reliable, thus making the instrument a trustworthy survey. The corrected item total correlation, or r*, represents the correlation between each item and the total score composed by the scale. Instruments with higher reliabilities should possess high correlations between the items and the total score made of the sum of the items. All items in the survey have moderate to strong correlations, 0.5 or higher, with their corresponding scales which indicates at least an adequate if not higher level of reliability for all scales and therefore for the instrument as a whole.

Table 7.

Reliability Scores for the Instrument

Construct	Items	r* (Corrected Item-Total Correlation)	Cronbach's Alpha
Computer Security Practices	CSPI	0.52	0.76
	CSP2	0.61	
	CSP3	0.65	
	CSP4	0.45	
Perceived Vulnerability	PV1	0.72	0.87
	PV2	0.83	
	PV3	0.75	
Perceived Security	PS1	0.78	0.81
	PS2	0.83	
	PS3	0.46	

Table 9 *continued*

Construct	Items	R* (Corrected Item-Total Correlation)	Cronbach's Alpha
Response Efficacy	RE1	0.65	0.87
	RE2	0.83	
	RE3	0.83	
Self-Efficacy	SE1	0.84	0.82
	SE2	0.82	
	SE3	0.81	
	SE4	0.82	
Perceived Usefulness	PU1	0.79	0.81
	PU2	0.70	
	PU3	0.60	
Perceived Ease of Use	PEU1	0.60	0.82
	PEU2	0.70	
	PEU3	0.65	
	PEU4	0.65	
Awareness	A1	0.45	0.77
	A2	0.67	
	A3	0.60	
	A4	0.60	
Attitude	ATT1	0.70	0.84
	ATT2	0.76	
	ATT3	0.70	
Subjective Norms	SN1	0.57	0.78
	SN2	0.75	
	SN3	0.57	

Table 9 *continued*

Construct	Items	R* (Corrected Item-Total Correlation)	Cronbach's Alpha
Perceived Behavioral Control	PBC1	0.78	0.89
	PBC2	0.82	
	PBC3	0.78	

Table 18 in Appendix D displays the corrected total item correlation between each item and its respective scale. This allows the assessment of convergent validity of the instrument. Convergent validity is achieved when items are highly correlated with their respective scales. None of the values in the concerned column falls below 0.5, indicating a high correlation between the items and their respected scales. This leads to concluding that the instrument possesses convergent validity. Table 18 shows the inter-correlations between all items. These allow the assessment of discriminant validity. Discriminant validity occurs when a set of items measuring a construct have low correlations with another set of items, thus measuring another construct. Most items have correlations of 0.3 and below, with the different set of items measuring distinct constructs, thus yielding an acceptable level of discriminant validity.

Demographic Factors and Computer Security Practices (ANOVA Result)

Table 10 presents the results of a one-way analysis of variance (ANOVA) between age and computer security practices indicators. The table indicates that the only statistically significant relationship is between age and CSP3 (exercising caution before opening an attachment). It seems that older individuals have a higher mean when compared to younger students, as indicated in the means plot (figure 11). Figures 9, 10 and 12 display the means of various age groups based on CSP1, CSP2, and CSP4 all showing no significant differences

among the various groups. Age and computer security practices in general, however, seems to lack any reasonably practical association given the lack of significance (high *p* values in table 10) and small differences in means between the different age groups across the various indicators of computer security practices displayed in figures 9, 10, and 12.

Table 8.

Age and Computer Security Practices (one-way/ANOVA)

		Sum of Squares	Df	Mean Square	F	Sig.
CSP1	Between Groups	.185	2	.092	.124	.884
	Within Groups	222.905	298	.748		
	Total	223.090	300			
CSP2	Between Groups	3.795	2	1.898	1.884	.154
	Within Groups	300.151	298	1.007		
	Total	303.947	300			

Table 10 *continued*

		Sum of Squares	Df	Mean Square	F	Sig.
CSP3	Between Groups	6.927	2	3.464	3.560	.030
	Within Groups	289.897	298	.973		
	Total	296.824	300			
CSP4	Between Groups	3.476	2	1.738	2.275	.105
	Within Groups	227.634	298	.764		
	Total	231.110	300			

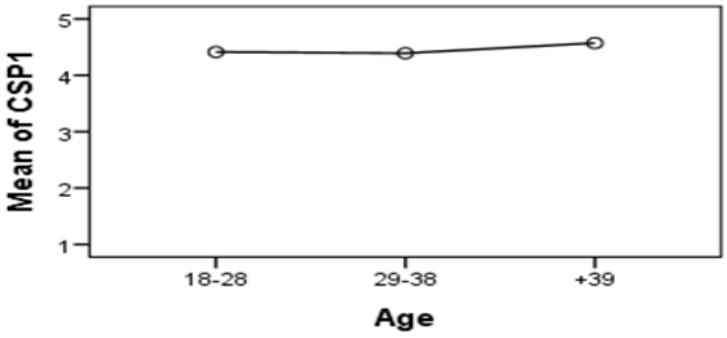

Figure 9. Mean of CSP1 (age).

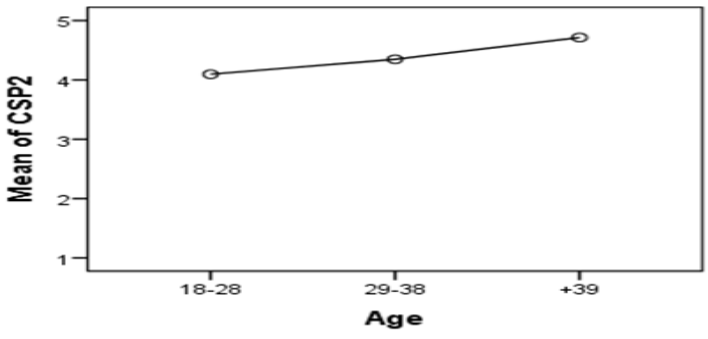

Figure 9. Mean of CSP2 (age).

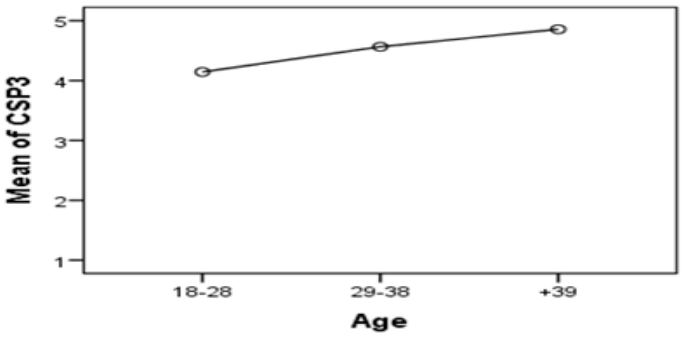

Figure 10. Mean of CSP3 (age).

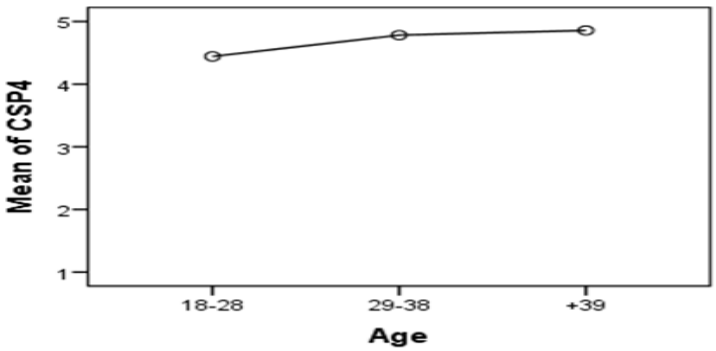

Figure 11. Mean of CSP4 (age).

Table 11 presents the results of an analysis of variance between college affiliation and computer security practices. Generally, there seems to be no relationship between the two variables given that three of the significance level values exceed conventional statistical significance levels. The only significant p-value is between college affiliation and CSP4 ("I do not open the email if the content looks suspicious"). Students in the college of business seem to be the most hesitant in trusting suspicious emails when compared to other colleges at this university as evident in Figure 16. Figures 13, 14 and 15 displays the means of the sample on

CSP1, CSP2 and CSP3 based on college affiliation. Those figures display no significant differences in the means on CSPs with respect to college affiliation.

Table 9.

College Affiliation and Computer Security Practices (one-way/ANOVA)

		Sum of Squares	Df	Mean Square	F	Sig.
CSP1	Between Groups	1.923	5	.385	.513	.766
	Within Groups	221.167	295	.750		
	Total	223.090	300			
CSP2	Between Groups	3.349	5	.670	.657	.656
	Within Groups	300.598	295	1.019		
	Total	303.947	300			
CSP3	Between Groups	4.891	5	.978	.988	.425
	Within Groups	291.933	295	.990		
	Total	296.824	300			
CSP4	Between Groups	10.469	5	2.094	2.799	.017
	Within Groups	220.641	295	.748		
	Total	231.110	300			

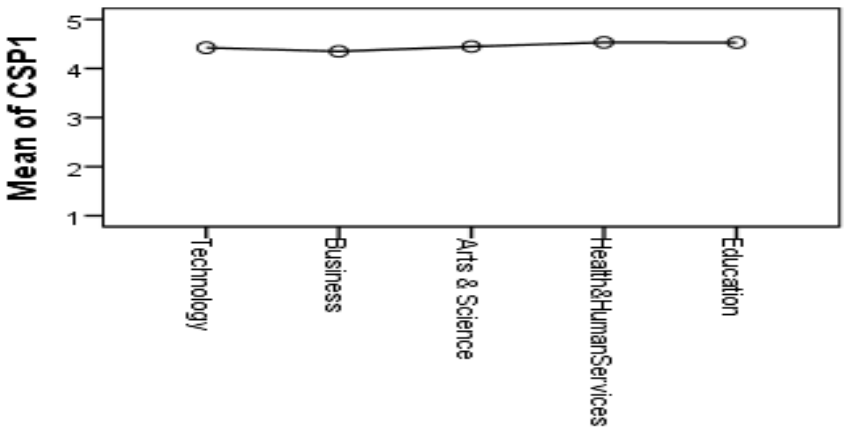

Figure 12. Mean of CSP1 (college affiliation).

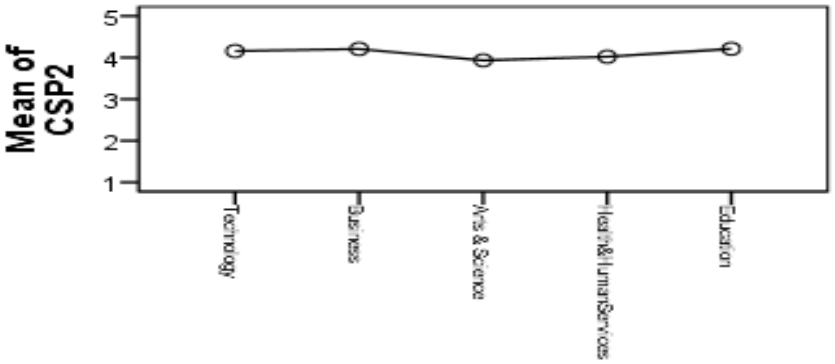

*Figure 13***.** Mean of CSP2 (college affiliation).

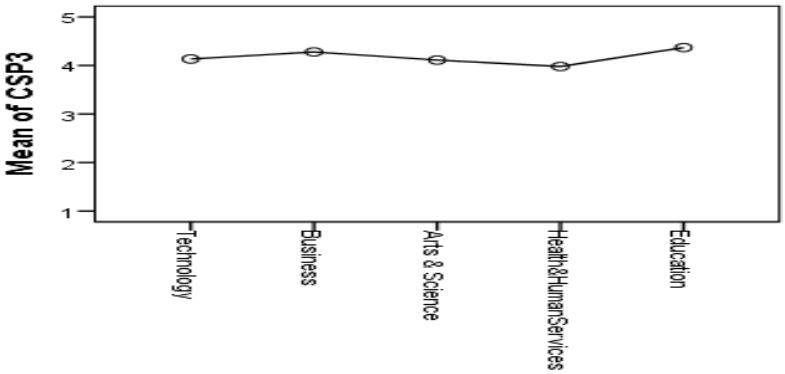

Figure 14. Mean of CSP3 (college affiliation).

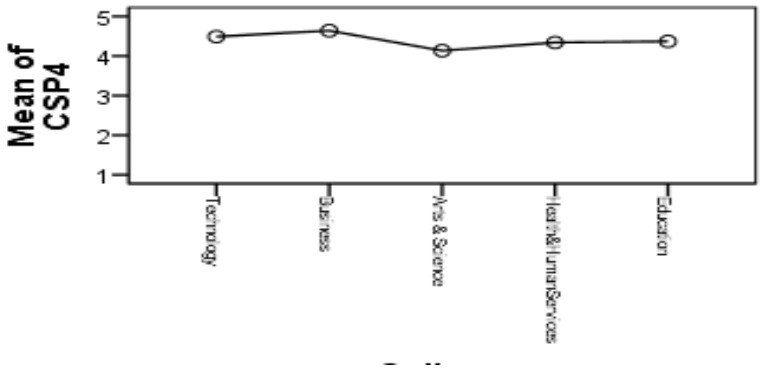

Figure 15. Mean of CSP4 (college affiliation).

Table 12 displays the results of one-way analysis (ANOVA) between academic majors (specifically whether the student has an IT or non-IT major) and the four indicators of computer security practices. In all four associations, majoring in an IT or non-IT field generates a statistically significant difference in computer security practices among students. All significant level values are well below the conventional significance levels of 0.5 or 0.10, indicating a statistical, as well as practical, significance. Figures 17-20 represents the mean differences between IT majors and non-IT majors with respect to the four indicators of computer security practices, showing that there is an observed difference in all four cases. In all cases, IT students possess a higher awareness and practice of computer security when compared to non-IT majors.

Table 10.

Major and Computer Security Practices (one-way/ANOVA)

		Sum of Squares	Df	Mean Square	F	Sig.
CSP1	Between Groups	4.159	1	4.159	5.679	.018
	Within Groups	218.931	299	.732		
	Total	223.090	300			
CSP2	Between Groups	15.259	1	15.259	15.804	.000
	Within Groups	288.688	299	.966		
	Total	303.947	300			
CSP3	Between Groups	10.524	1	10.524	10.991	.001
	Within Groups	286.300	299	.958		
	Total	296.824	300			
CSP4	Between Groups	6.650	1	6.650	8.858	.003
	Within Groups	224.460	299	.751		
	Total	231.110	300			

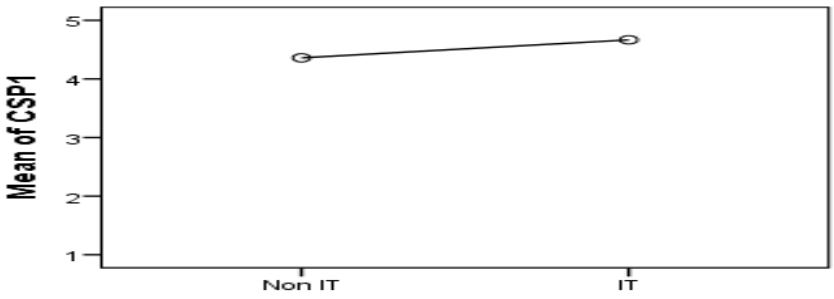

Figure 16. Mean of CSP1 (IT or non-IT).

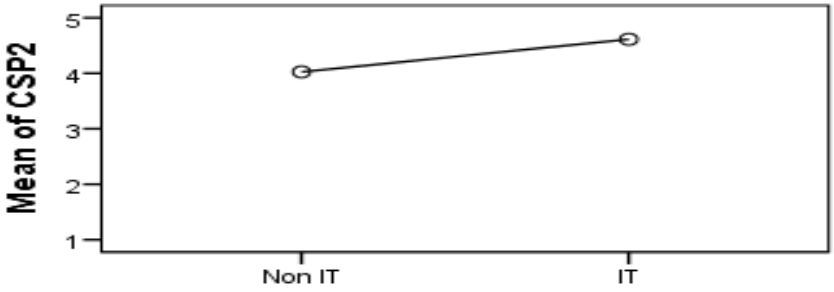

Figure 17. Mean of CSP2 (IT or non-IT).

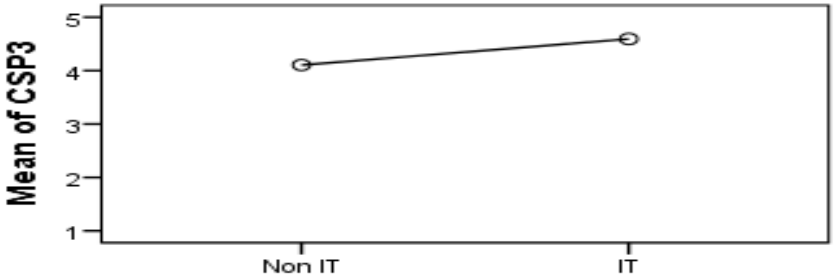

Figure 18. Mean of CSP3 (IT or non-IT).

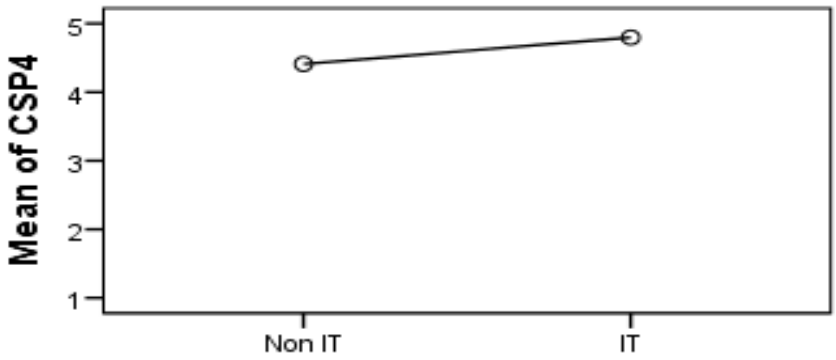

Figure 19. Mean of CSP4 (IT or non-IT).

Table 13 shows the results of the analysis of variance between level of education and computer security practices. Results indicate that there is no association between the respondents' level of education and computer security practices. P-values fall well-below the conventional levels of 0.05 and 0.01. Figures 21-24 plots the means of CSPs based on the different educational levels. It can be seen that there is little practical mean difference in each of the four indicators of computer security practices based on the level of education.

Table 11.

Variance Between Education Level and Computer Security Practices

		Sum of Squares	Df	Mean Square	F	Sig.
CSP1	Between Groups	1.180	4	.295	.393	.813
	Within Groups	221.910	296	.750		
	Total	223.090	300			
CSP2	Between Groups	4.356	4	1.089	1.076	.369
	Within Groups	299.591	296	1.012		
	Total	303.947	300			
CSP3	Between Groups	9.247	4	2.312	2.379	.052
	Within Groups	287.577	296	.972		
	Total	296.824	300			
CSP4	Between Groups	3.575	4	.894	1.163	.327
	Within Groups	227.535	296	.769		
	Total	231.110	300			

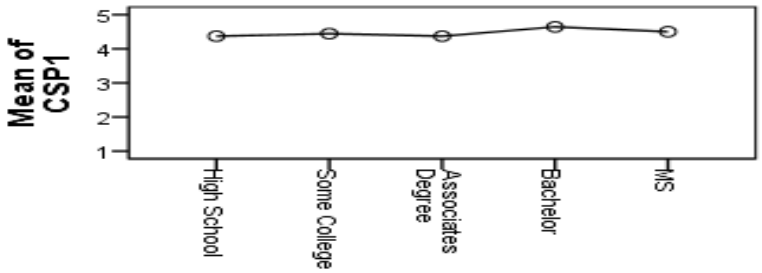

Figure 20. Mean of CSP1 (education levels).

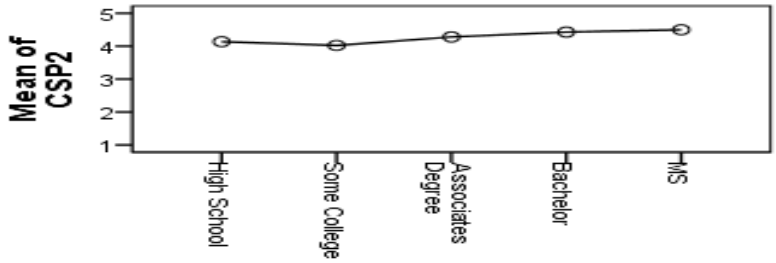

Figure 21. Mean of CSP2 (education levels).

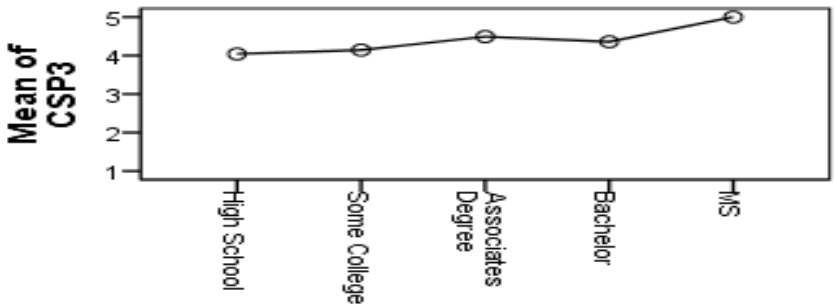

Figure 22. Mean of CSP3 (education levels).

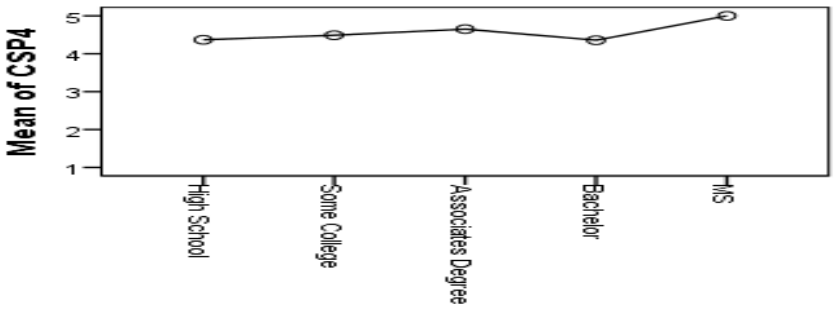

Figure 23. Mean of CSP4 (education levels).

Table 14 presents the results of a one-way analysis between IT experience and computer security practices. All in all, levels of IT experience did not generate significant differences in computer security practices. None of the significance levels values were found to be below 0.05, the most conventional statistical significance level, indicating a lack of association. Figures 25-28 confirm this result by showing the limited practical differences among the various IT experience groups and the four computer security practice indicators. Generally, there seems to be no relationship between the two variables.

Table 12.

IT Experience and Computer Security Practices (One-Way/ANOVA).

		Sum of Squares	Df	Mean Square	F	Sig.
CSP1	Between Groups	1.015	5	.203	.270	.930
	Within Groups	222.075	295	.753		
	Total	223.090	300			

Table 14 *continued*

		Sum of Squares	Df	Mean Square	F	Sig.
CSP2	Between Groups	2.805	5	.561	.550	.739
	Within Groups	301.141	295	1.021		
	Total	303.947	300			
CSP3	Between Groups	5.819	5	1.164	1.180	.319
	Within Groups	291.005	295	.986		
	Total	296.824	300			
CSP4	Between Groups	3.601	5	.720	.934	.459
	Within Groups	227.509	295	.771		
	Total	231.110	300			

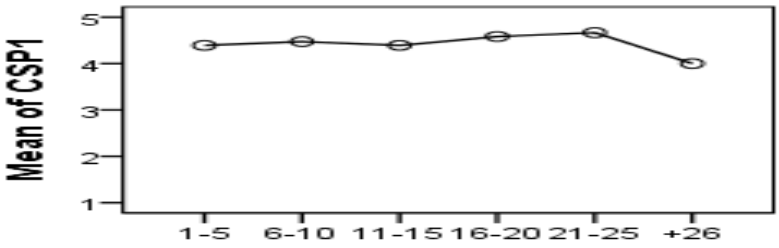

Figure 24. Means of CSP1 (IT experience).

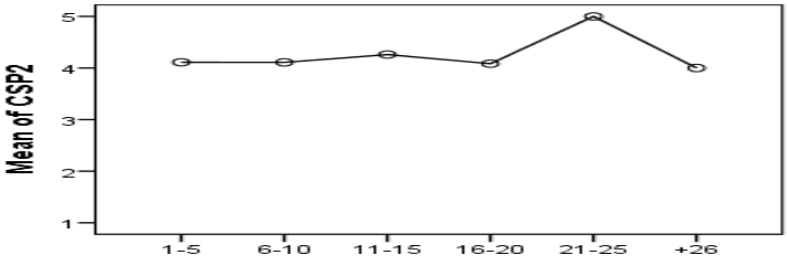

Figure 25. Means of CSP2 (IT experience).

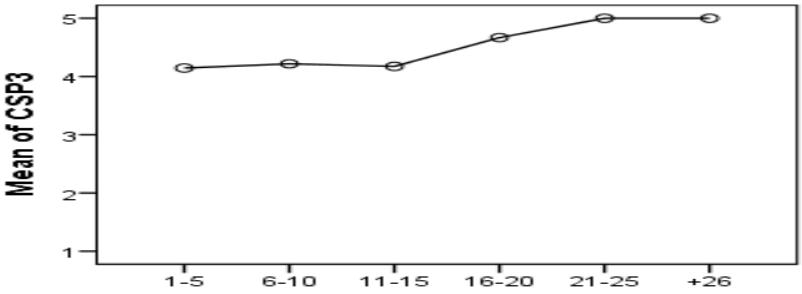

Figure 26. Means of CSP3 (IT experience).

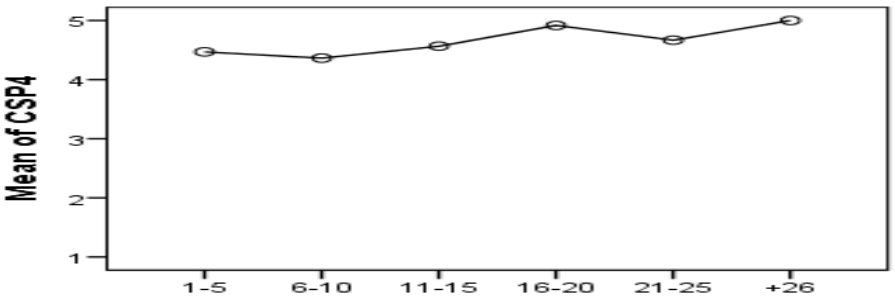

Figure 27. Means of CSP4 (IT experience).

Multiple Linear Regression Results

Table 15 displays the multiple regression analysis between perceived vulnerability, perceived severity, response efficacy, computer self-efficacy, perceived usefulness, perceived ease of use, awareness, attitudes, subjective norms, and perceived behavioral control as independent variables and computer security practices as the dependent variable. Note that all variables used in the analysis are scales composed of summing the values of all corresponding items. Table 15 shows the results of Model 1, excluding demographic indicators. Model 2, displayed in Table 16, presents the results of the regression analysis with demographic indicators included.

Model 1 is statistically significant, having F-statistic equal to 6 and a significant *p* value with a probability of less than .01. The model seems to explain about 17% of the variation in computer security practices as evident by the value of *R* squared. Results of model one indicate that without the consideration of any variable in the equation, the average computer security practice score on the scale, ranging from 1 to 5, is equal to 1.59 (the value of the constant). This result indicates a low computer security level for these university students, holding the values of all independent variables at zero. Perceived vulnerability is statistically significant in determining computer security levels among college students at this university. For every one

unit increase on the perceived vulnerability scale, an increase of 0.11 units on the computer security practice scale occurs. While statistically significant, this increase is practically miniscule. Perceived severity is not statistically or practically significant in determining the level of computer security practices. Response efficacy is not significant in determining computer security practices levels among the students, having a *p* value of just .20. Computer self-efficacy is also not significant in explaining variation in computer security practices, with a *p* value of only .29. Perceived usefulness is statistically significant, having a *p* value of .02. An increase of one unit on the scale of usefulness is associated with a 0.15 increase on the level of computer security. Despite its statistical significance, this result seems to be not practically significant in increasing students' computer security practices. Perceived ease of use seems to be statistically significant, with a *p* value of .05 and an increase of 0.11 in computer security practices for every unit increase on its scale. While awareness has a negative regression coefficient, it is not statistically significant with a *p* value of .64. Attitudes toward computer security seem to not be statistically significant in determining computer security levels, with a *p* value of .11. Finally, subjective norms and perceived behavioral control are neither statistically significant in changing the level of computer security practices among the students from this study given that their p-values exceed conventional significance levels. All in all, three indicators are significant in explaining variation in computer security levels, perceived vulnerability, perceived ease of use, and perceived usefulness.

Table 13.

MRA Model 1 (without demographics)

Dependent Variable: CSP		Unstandardized Coefficients		Standardized Coefficients			Correlations		
		B	Std. Error	Beta	T	Sig.	Zero-order	Partial	Part
	(Constant)	1.590	.418		3.802	.000			
	PV	.118	.049	.141	2.410	.017	.243	.140	.129
	PS	.002	.035	.004	.064	.949	.087	.004	.003
	RE	.067	.052	.080	1.285	.200	.241	.075	.069
	SE	.063	.060	.072	1.044	.297	.239	.061	.056
	PU	.151	.064	.143	2.347	.020	.283	.137	.125
	PEU	.119	.062	.117	1.933	.054	.260	.113	.103
	A	-.019	.041	-.027	-.460	.646	.147	-.027	-.025
	ATT	.110	.070	.093	1.566	.118	.208	.092	.084
	SN	.080	.055	.087	1.466	.144	.201	.086	.078
	PBC	.021	.040	.030	.522	.602	-.044	.031	.028
R^2 = 0.174, F= 6.0 with a p-value of less than 0.01 N= 301									

Table 14.

MRA Model 2 (with demographics)

Dependent Variable: CSP		Unstandardized Coefficients		Standardized Coefficients			Correlations		
		B	Std. Error	Beta	T	Sig.	Zero-order	Partial	Part
	(Constant)	1.656	.455		3.637	.000			
	PV	.122	.049	.146	2.487	.013	.243	.146	.132
	PS	.006	.035	.009	.160	.873	.087	.010	.009
	RE	.071	.053	.085	1.329	.185	.241	.079	.071
	SE	.061	.060	.070	1.017	.310	.239	.060	.054
	PU	.163	.066	.154	2.470	.014	.283	.145	.131
	PEU	.125	.062	.123	2.007	.046	.260	.118	.107

Table 16 *continued*

Dependent Variable: CSP		Unstandardized Coefficients		Standardized Coefficients			Correlations		
		B	Std. Error	Beta	T	Sig.	Zero-order	Partial	Part
	A	-.031	.041	-.045	-.747	.456	.147	-.044	-.040
	ATT	.081	.071	.069	1.140	.255	.208	.068	.061
	SN	.069	.055	.075	1.249	.213	.201	.074	.066
	PBC	.023	.041	.033	.565	.572	-.044	.034	.030
	Age	-.025	.129	-.011	-.193	.847	.016	-.011	-.010
	Gender	-.130	.080	-.092	-1.620	.106	-.082	-.096	-.086
	College	.073	.039	.106	1.897	.059	.075	.112	.101
	Major	.171	.130	.076	1.315	.190	.137	.078	.070
	Educational Level	.011	.057	.011	.187	.852	.039	.011	.010
	IT Experience	-.015	.056	-.016	-.272	.786	.038	-.016	-.014
R^2 = 0.196, F= 6.0 with a p-value of less than 0.01 N= 301									

Table 16 demonstrates the result of multiple linear regression analysis, including demographic factors in the model. Results show that the three variables that significantly influence computer security practices are perceived vulnerability, perceived ease of use, and perceived usefulness. None of the demographic indicators is statistically significant in changing the level of computer security practice among college students at this university. This result confirms the findings in Model 1 above.

Summary

This chapter presented the descriptive, reliability, validity, analysis of variance, and multiple linear regression analysis results of this study. Results indicated that the Midwestern university students express high levels of computer security practices. The results also indicated

that there is little connection between demographic factors and computer security practices. Multiple linear regression analysis suggested that perceived vulnerability, ease of use, and usefulness are the best indicators predicting computer security practice levels. This finding alludes to the fact that the technology acceptance model enjoys empirical support to the contrary of the theory of planned behavior and protection motivation theory, which seem to be unsupported by the results of this research in determining variation in the adoption of computer security practices among Midwestern college students.

Chapter 5: Discussion

This chapter presents an overview of the study, discussion of the findings, and analysis of the relationship between the results and previous studies as well as the significance of this research to future assessments of computer security practices.

Overview of the Study

This study investigated the relationship between protection motivation theory, theory of planned behavior, the technology acceptance model, and computer security practices among college students. The literature review identified many indicators, namely perceived vulnerability, perceived severity, response efficacy, computer self-efficacy, awareness, perceived usefulness, perceived ease of use, attitudes, subjective norms, and perceived behavioral control as independent factors that lead to changes in computer security practice among college students. This study tested a constructed model based on such constructs, using a developed survey instrument that possessed adequate reliability and validity. The assessment was conducted at Midwestern university, where the researcher distributed the survey to the university students in the five colleges composing the university. A total of 301out of 400 valid responses were collected and utilized in the statistical analysis.

Discussion

This analysis tested five hypotheses, exploring the effects of ten constructs and demographic factors (age, gender, level of education, level of IT experience, college affiliation, and whether the student has an IT or non-IT major) on computer security practices among students from a Midwestern university. Table 17 indicates that due to the data provided by the multiple linear regression analysis, three hypotheses were rejected and two were partially

rejected. Results indicated that age, gender, level of education, IT experience, and college affiliation did not bear statistical nor practical effects on computer security practices. While majoring in IT was significant in the ANOVA above, the regression analysis suggested that majoring in IT or non-IT disciplines is not significant in predicting computer security practices among college students.

College students' perceived vulnerability concerning computer security risks, perceived ease of use, and usefulness of computer security practices were significant in altering their computer security practices as demonstrated by this study. On the contrary, results indicated that perceived severity of computer security risks, students' self-efficacy in using computers, their response efficacy to computer risks, their attitudes towards computer security, their awareness of computer security risks, their subjective norms, and perceived behavioral control toward the same concept do not matter in regard to changing students' perceptions of computer security practices.

Table 15.

Rejection of Hypotheses

Hypotheses	Rejected/Not Rejected
Hypothesis 1: increased levels of perceived usefulness, perceived severity and perceived vulnerability will increase college students' likelihood of adopting computer security practices.	Partially Rejected
Hypothesis 2: increased levels of perceived ease of use, perceived computer self-efficacy, and perceived response efficacy will increase college students' likelihood of adopting computer security practices.	Partially Rejected

Table 17 *continued*

Hypotheses	Rejected/Not Rejected
Hypothesis 3: increased levels of attitudes, subjective norms, and perceived behavioral control will increase college students' likelihood of adopting computer security practices.	Rejected
Hypothesis 4: Increased levels of perceived awareness will increase college students' likelihood of adopting computer security practices.	Rejected
Hypothesis 5: Demographic variables (age, education, IT experience, major, and gender) influence college students' adoption of computer security practices.	Rejected

Findings suggest that if college students felt threatened by computer security risks, they were more likely to adopt computer security practices. College students need to feel vulnerable in the face of computer security dangers in order to infringe their sense of protection and prompt them to adopt better computer security measures. By the same token, college students need to understand that computer security practices are easy and useful for them to formulate a positive outlook toward computer security practices.

On the other end of the spectrum, a college students' experience in information technology and their awareness or attitudes toward computer security risks does not seem to influence their perception of computer security risks. Similarly, the students' ability to navigate computers and computer software and their training in intervening in cases of computer security breaches do not significantly lead them to construct a positive value for adopting and implementing computer security practices. Finally, subjective norms and the perceptions of their professors, peers, parents, and friends about computer security risks does not seem to significantly alter the students' views of computer security practices.

Results of the study demonstrate the importance of the technology acceptance model as the most useful theoretical framework for the analysis of computer security practices among home users such as college students. This is due to the significance of its main indicators, perceived usefulness, and perceived ease of use. On the other hand, the theory of planned behavior proved to not be useful in studying student perceptions of computer security practices. None of the theory's indicators were found to be significant. Protection motivation theory seems to be even less relevant than the technology acceptance model because most of its indicators were found to be non-significant, particularly computer self-efficacy, response efficacy, and the perceived severity of computer security threats.

This research study showed college students perceive computer security practices as new technologies. It appears that they evaluate the ease of use and usefulness of any practice prior to accepting the decision to adopt it. Students are surrounded with an environment filled with cyber-threats. Every day they read, hear, or are exposed to cyber-security risks because they are a vulnerable group of the population. Given this, they are likely to perceived computer security practices as useful. More importantly, checking ones' email for a suspicious title or an attached document seems to be an easy thing to do. Therefore, students are likely to consider such a useful practice in shielding themselves from cybercrime easily learned and utile. Therefore, the technology acceptance model seems to fit the logic of college students when thinking about the adoption of computer security practices.

Protection motivation theory has been found to be better at predicting health outcomes compared to technologically oriented behaviors. College students are unlikely to think of cybercrime as threatening as cancer, AIDS, or any other fatal disease. Therefore, the severity of threats or their response efficacy levels do not change much with rising cyber-threats (DiGiusto,

2008; Woon et al., 2005). This research has established that protection motivation theory is only partially supported with respect to the explanation of computer security practices. Perceived vulnerability to the risks associated with computer security has been found to positively correlate with the adoption of computer security practices. College students feel vulnerable given their perceived inability to control their systems. This significance is consistent with the finding that college students believe that computer security practices are useful in raising their security levels when it comes to their vulnerabilities.

Finally, theory of planned behavior has been found to be robust in explaining socially oriented behaviors such as socialization, commencement of romantic relationships, or networking rather than technologically oriented behaviors. College students do not think of computer security practices as social. They perceive the adoption of computer security practices as technical, thereby minimizing the effects of subject norms, attitudes, and perceived behavioral control.

One of the most noteworthy observations on the results of this research is the possible presence of social desirability. Social desirability refers to the situation when survey respondents answer questions presented in a manner that is deemed to be acceptable by the researcher or society at large. It has been documented as one of the most imminent threats to the validity of survey responses presenting researchers with hurdles in attempting the generalization of research findings.

Results indicated that this university students self-reported very high perceptions of computer security practices, prompting a modicum of suspicion in the responses. The university students may have committed social desirability in responding to the survey questions,

answering in a positive manner for whatever reason driving such a choice. Future survey-based studies on computer security practices need to ensure they account for social desirability.

Conclusions

This research proposed a total of five research questions. Answers to these questions are shown below in the same order as presented in Chapter 1.

Question 1.

To what extent do perceived usefulness, perceived severity, and perceived vulnerability toward computer security practices affect college student adoption of computer security practices?

This study found support for the hypothesis claiming a positive relationship between perceived usefulness of computer security practices and their adoption. This finding is consistent with earlier research in a variety of settings (Conklin, 2006; Jones, et al., 2010; McGregor, et al., 2015). If college students believe that computer security practices spare them greater problems, prevent the loss of their information, and increase their security over their machines, they are more likely to adopt computer security practices. This is explained by the underlying belief among students that computer security practices are useful in protecting them from imminent dangers.

Results indicated that the severity of computer security threats is unrelated to the adoption of computer security practices among college students. College students seem not to incorporate the intensity, size, or scope of computer security risks in their conceptual formulations concerning computer security practices. This result is consistent with previous research (Ng, et al. 2009; Clear, 2011). Investigating the relationship between the health belief model and computer security practices adoption by a variety of users, Ng et al. (2009) and Clear

(2011) did not find a significant relationship between the severity of computer security risks and good computer security perceptions and practice, either in organizational or home-use settings. All in all, users do not incorporate the severity of risks as a relevant indicator in their determination concerning their computer security.

A positive relationship between perceived vulnerability toward computer security risks and computer security practices was found by this study. This result is consistent with previous research DiGuisto (2008) and Woon (2005). College students' perception of imminent threats, coupled with their perception of a limited ability to control their environment, seems to increase their positive perceptions of computer security practice.

Question 2.

To what extent do perceived ease of use, perceived computer self-efficacy, and perceived response efficacy toward computer security practices affect college student adoption of computer security practices?

This study found support for the hypothesis claiming a positive relationship between perceived ease of use of computer security practices and computer security practices. This result confirms earlier findings in home, as well as organizational, settings. Computer users are found to more likely practice computer security safeguards if those are easily learned and implemented. The explanation of this relationship lies in the learning curve principle. If the learning of new technologies is easy, the adoption of such technologies becomes more prevalent.

Findings of this study suggest that there is no relationship between computer self-efficacy and computer security practices perceptions. This result is contrary to previous findings, supporting a positive relationship between computer self-efficacy and computer security practices. Users with better skills at navigating computers are expected to possess better

computer security perceptions and practice. While this claim seems intuitive and possesses empirical support from previous study, this analysis found no empirical verification for such a statement. This result may lie in the choice of items used to measure computer self-efficacy. In this study, a specific measure was utilized and applied to emails and attachments while previous analysts use more general operationalization of the construct. Additionally, the vast majority of this study's sample consists of younger individuals possessing less computer self-efficacy compared to more experienced computer users who usually tend to be older adults.

The present study is among the first to test the relationship between response efficacy and computer security practices. This is due to the heavy dependence of previous research on the health belief model, rather than the updated protection motivation theory. Results indicated that there is no significant relationship between response efficacy and computer security practices among college students. The ability of college students to prevent, intervene, and deal with post-incident scenarios does not bear a practical effect on their computer security perceptions and practice.

Question 3.

To what extent do attitudes, subjective norms, and perceived behavioral control toward computer security practices affect college student adoption of computer security practices?

This study found no support for the hypothesis claiming a positive relationship between attitudes toward computer security practices and the likelihood of their adoption among college students. Earlier research has not tested the relationship between planned behavior theory constructs and the adoption of computer security practices among college students.

This study found no support for the hypothesis claiming a positive relationship between subjective norms and computer security practices adoption among college students. Perceptions

of students, professors, peers, and friends about computer security practices did not influence the college students' decision to adopt and implement computer security practices.

This study did not find support to the hypothesis claiming a positive relationship between perceived behavioral control and computer security practices. Students' ability to control their behavior with respect to computer security practices did not bear any significance on their likelihood to adopt computer security practices.

Question 4.

To what extent does awareness toward computer security practices affect college student adoption of computer security practices?

This study did not find support for the hypothesis claiming a positive relationship between awareness about computer security practices and the likelihood of their adoption among college students. This finding is somewhat inconsistent with earlier findings (David & Shannon, 2007; Huang et al. 2011). While college students' awareness in a few areas, such as password security, has been found to positively correlate with their adoption of computer security practices, in many areas of computer security practices this correlation was not found to be significant. The result of this research may have been due to the choice of awareness measures and computer security practices, which heavily focused on one specific area of computer security: verifying the authenticity of emails and their accompanying attachments.

Question 5.

To what extent do demographic factors (age, education level, IT experience, college major, and gender) toward computer security practices affect college student adoption of computer security practices?

This study found no statistically significant relationship between age, gender, educational level, and levels of computer security practices adoption among college students. It only found a positive relationship between students who are majoring in an IT-oriented major and the likelihood of these students adopting computer security practices.

Implications

Previous research has focused heavily on technological solutions for computer security risks. Recent behavioral research has noted the importance of the human element and its role in shielding computers, the information stored on them, and users' privacy from dangerous and unauthorized penetrations. This study broadens the focus of this emerging area of scholarship by concentrating on bolstering computer security practices among college students. Previous studies have established that a significant portion of college students have been found to not practice the best standards of computer protection, such as not setting strong passwords, backing up their data regularly, and falling victim to phishing schemes. Note that such behavior positively correlates with other computer security practices such as emails verification for suspicious or infected titles or attachments (Garrison & Posey, 2006; Reznik et al. 2011). This research only focused on email verification and its conclusion are likely to apply on other computer security practices given the robust positive association with the domain of computer security practices. To strengthen users' computer security practices through the identification of factors influencing college students' likelihood of adopting said measures, this study was designed and implemented.

One of the most important implications of this research is the heightened focus on the usability and training of computer security practices. College administrators, professors, and stakeholders should design courses, workshops, and special sessions on the usefulness and ease

of use of computer security practices. As colleges like the Midwestern university already require students to enroll in a mandatory writing and composition course, they could easily require every student to finish an additional training course on computer security practices, their usefulness, and their ease of use. While the Midwestern university has launched the "THINK BEFORE CLICK" campaign, attempting to raise awareness and good practices for avoiding phishing incidents, the findings of this current study indicate that a significant portion of this university students do not follow best practices that shield them from falling victim to cyber-crime.

Another important implication of this study is the significance of perceived vulnerability with respect to adopting computer security practices. Students are found to more likely adopt computer security practices if they feel vulnerable to security threats. Colleges like the Midwestern university in this study may start a lean, cost-effective, campaign where every professor, lecturer, and staff member sends out regular emails to their students and clients which raise awareness about the risks involved with computer security practices. Students need to feel they do not have full control over their computer security practice.

Study Limitations

This research suffers from several limitations. First, the sampling design is a non-probability based technique. This threatens the representativeness of the obtained sample. While the collected responses came from 301 students, about half of the sample came from the college of business. This college was overrepresented in the obtained sample and other colleges were underrepresented such as the college of education, which only composed 6% of the sample. This does not reflect the population of students at the Midwestern university since enrollment at the college of education represents more than 6% of the total university student population.

Second, survey research presents traditional threats to the reliability and validity of

results. First, as outlined above, the university students are likely to overstate their computer security practices due to social desirability. Students are more likely to report higher levels of awareness and adoption of computer security than what they actually possess to appear smart and cautious. This generates a distribution of hopeful rather than true scores for individuals threatening the external validity of the findings generated.

Third, only nine out of fourteen teaching faculty allowed the researcher to administer the survey in their classrooms. Four out of the nine were professors at the college of business and one at the college of education. Two of the professors were at the college of arts and sciences and two at the college of technology. None of the faculty were from the college of health and human services leaving the possibility that the juniors and seniors of this college were underrepresented.

Further, most courses generating the respondents were undergraduate level courses leaving out graduate classes. This explains the overrepresented nature of the young population and the underrepresentation of graduate degree holders in the results. This may have swayed results. For instance, age and computer security practices largely were not found to be related contrary to earlier findings. This may have been due to the few respondents over thirty years of age in the sample.

More importantly, the choice of measurement in this research may have influenced the direction of results found. Computer security practices are a multidimensional construct that could be evaluated in several respects. This research only considered the checking, verifying, and exercising caution in opening emails and attachments. If other more robust measures of security practices, such as setting strong passwords, backing up data, or updating personal passwords, other results may have been produced.

Recommendations for Future Research

Future research on computer security practices should focus on the technology acceptance model more heavily. While the health belief model, protection motivation theory, and theory of planned behavior are all robust behavioral theories, computer security practices seem to be considered a new technology, and as a new technologically oriented behavior, it needs to be analyzed through the prism of the technology acceptance model.

Further, future research on computer security practices should consider using an experimental research design. Survey research and case studies can illuminate rich descriptions of students' attitudes and behaviors related to computer security practices, however they seem to be inferior to experimental research when it comes to constructing generalizable statements on the relationships between hypothesized factors and computer security practices as the dependent variable. Experimental research is likely to generate more reliable and valid measurements on computer security practices compared to survey research. This is essential in modelling computer security adoption since statistical models rely heavily on accurate data. The more accurate, precise, and valid responses are, the better results we will obtain, which allows us to generate findings across settings as well as contexts.

With such methodological recommendation, more rigorous sampling and statistical treatment should be followed. Convenience sampling is useful in many contexts, such as a small-scale research project similar to this dissertation, because it allows the researcher to access a readily available population; however, it presents well-documented dangers to the external validity of the research findings.

Summary

This chapter outlined the conclusions, implications, future research, and limitations of this dissertation. The chief findings of this work lie in the fact that the technology acceptance model is the best explanatory framework for computer security practices. Students' perceptions of the usefulness and ease of use of computer security practices determine the largest portion of explanation in the variation of students' scores on computer security. Future researchers should implement experimental designs to analyze differences in computer security practices given their superiority in producing reliable and valid data compared to survey research that is prone to the classical problem of social desirability. The most important recommendation of this research is for university administrators to devise new workshops for students, teaching them the utility of and training them about accessible methods for computer security practices. Future researchers are encouraged to use probability-based sampling techniques, multidimensional instruments measuring computer security practices, and multi-methods approaches in studying variation in the adoption of computer security practices among college students.

References

Ahmad, A., Maynard, S., & Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*, *25*(2), 357-370.

Ajzen, I. (2005). *Attitudes, personality, and behavior*. New York: McGraw-Hill Education.

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

Arachchilage, N., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, *38*, 304-312.

Ball, A., Ramim, M., & Levy, Y. (2015). Examining users' personal information sharing awareness, habits, and practices in social networking sites and e-learning systems. *Online Journal of Applied Knowledge Management*, *3*(1), 180-207

Bartsch, M., & Dienlin, T. (2016). Control your Facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, *56*, 147-154.

Boer, H., & Seydel, E. (1996). Protection motivation theory. In M. Conner, & P. Norman (Eds.), *Predicting Health Behaviour: Research and Practice with Social Cognition Models*. Maidenhead, UK: Open University Press.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548.

Celik, V., & Yesilyurt, E. (2013). Attitudes to technology, perceived computer self-efficacy

and computer anxiety as predictors of computer supported education. *Computers & Education*, *60*(1), 148-158.

Chenoweth, T., Minch, R., & Gattiker, T. (2009, January). Application of protection motivation theory to adoption of protective technologies. HICSS'09. 42nd Hawaii International Conference on System Sciences. IEEE.

Clear, C. (2011). The adoption of computer security: An analysis of home personal computer user behavior using the health belief model (Doctoral dissertation, Utah State University). Retrieved from https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=1874&context=etd

Compeau, D., & Higgins, C. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly*, 189-211.

Conklin, W. (2006). Computer security behaviors of home pc users: a diffusion of innovation approach (Doctoral Dissertation, The University of Texas at San Antonio). Retrieved from https://dl.acm.org/citation.cfm?id=1236906

Crossler, R., Johnston, A., Lowry, P., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security, 32*, 90-101.

Davidson, J. (2015). Here is How Many Internet Users There are. (2015, May 26th). Retrieved from http://time.com/money/3896219/internet-users-worldwide/

Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-340.

Davis, F., Bagozzi, R., & Warshaw, P. (1989). User acceptance of computer

technology: a comparison of two theoretical models. *Management Science, 35*(8), 982-1003.

Davis, F., & Venkatesh, V. (1996). A critical assessment of potential measurement biases in the technology acceptance model: three experiments. *International Journal of Human-Computer Studies*, *45*(1), 19-45.

Davis, F. D. (1993). User acceptance of information technology: system characteristics, user perceptions and behavioral impacts. *International journal of man-machine studies*, *38*(3), 475-487.

DiGiusto, D. (2008). A Protection Motivation Theory Approach to Home Wireless Network Security in New Zealand: Establishing If Groups of Concerned Wireless Network Users Exist And Exploring Characteristics of Behavioral Intention (Master's Thesis, University of Wellington). Retrieved from http://researcharchive.vuw.ac.nz/xmlui/handle/10063/1148

Dupuis, M., Endicott-Popovsky, B., & Crossler, R. (2013, January). An analysis of the use of amazon's mechanical turk for survey research in the cloud. In *Proceedings of the International Conference on Cloud Security Management: ICCSM 2013* (p. 10). Sonning Common, UK: Academic Conferences Limited.

Eagly, A., & Chaiken, S. (1993). *The psychology of attitudes*. San Diego, CA: Harcourt Brace Jovanovich College Publishers.

Fagan, M., & Khan, M. (2016, June). Why do they do what they do? A study of what motivates users to (not) follow computer security advice. *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. USENIX Association.

Furnell, S., Bryant, P., & Phippen, A. (2007). Assessing the security perceptions of

personal Internet users. *Computers & Security*, *26*(5), 410-417

Garrison, C., & Posey, R. (2006). Technical report: Computer security checklist for non-security technology professionals. *Journal of International Technology and Information Management*, *15*(3), 87.

Hajli, N., & Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics, 133*(1), 111.

Herath, T., & Rao, H. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154-165.

Howe, A., Indrajit, R., Roberts, M., Urbanska, M., & Byrne, Z. (2012). The psychology of security for the home computer user. *Security and Privacy (SP), 2012 IEEE Symposium on security and privacy*. IEEE, 2012.

Huang, D., Rau, P., Salvendy, G., Gao, F., & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal of Human-Computer Studies*, *69*(12), 870-883.

Huda, N., Rini, N., Mardoni, Y., & Putra, P. (2012). The analysis of attitudes, subjective norms, and behavioral control on muzakki's intention to pay zakah. *International Journal of Business and Social Science*, *3*(22), 271-279.

Hu, Q., Hart, P., & Cooke, D. (2006, January). The role of external influences on organizational information security practices: An institutional perspective. *HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on System Sciences*. IEEE.

Ion, I., Reeder, R., & Consolvo, S. (2015, July). "... No one Can Hack My Mind": comparing expert and non-expert security practices. Symposium on Usable Privacy and Security (SOUPS) 2015, July 22–24, 2015, Ottawa, Canada.

Janz, N., & Becker, M. (1984). The health belief model: A decade later. *Health Education & Behavior*, *11*(1), 1-47.

Jones, B., & Heinrichs, L. (2012). Do business students practice smartphone security? *Journal of Computer Information Systems*, *53*(2), 22-30.

Jones, C., McCarthy, R., & Halawi, L. (2010). Utilizing the technology acceptance model to assess the employee adoption of information systems security measures. *Journal of International Technology and Information Management*, *19*(2).

Keller, S., Powell, A., Horstmann, B., Predmore, C., & Crawford, M. (2005). Information security threats and practices in small businesses. *Information Systems Management*, *22*(2), 7.

Klien, A. (2017, June 2). *Data backup: Are you a hero or a zero?* Backblaze. Retrieved from: https://www.backblaze.com/blog/data-backup-survey/

KPMG International. (2011). Cybercrime-A growing challenge for governments (Vol. 8). Retrieved from https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf

Kim, E. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security*, *22*(1), 115-126.

Li, Y., & Siponen, M. (2011, July). A call for research on home users' information security behaviour. PACIS 2011 Proceedings. 112. Retrieved from https://aisel.aisnet.org/pacis2011/112

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A Threat Avoidance Perspective. *Journal of the Association for Information Systems*, *11*(7), 394.

Lomo-David, E., & Shannon, L. (2009). Information systems security and Safety measures: The dichotomy between students' familiarity and practice. *Academy of Information and Management Sciences Journal*, *12*(1/2), 29.

McGregor, S., Charters, P., Holliday, T., & Roesner, F. (2015). Investigating the computer security practices and needs of journalists. 24th USENIX Security Symposium, Washington D.C., August 12-14, 2015.

McQuade, S. (2006). *Understanding and managing cybercrime*. Boston: Pearson/Allyn and Bacon.

Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. *Academy of Information and Management Sciences Journal*, *14*(2), 91.

Merkow, M., & Breithaupt, J. (2014). *Information security: Principles and practices*. London: Pearson Education.

Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. *Journal of Information Privacy and Security*, *9*(1), 47-67.

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

Pagliery, J. (2014). Half of American Adults Hacked This Year. Retrieved from http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/

Peltier, T. (2013). *Information security fundamentals*. Boca Raton, FL: CRC Press.

Ramalingam, R., Khan, S., & Mohammed, S. (2016). The need for effective information security awareness practices in Oman higher educational institutions. 1st Symposium on Communication, Information Technology, and Biotechnology: Current Trends and Future Scope, Sur College of Applied Sciences, Ministry of Higher education, Sultanate of Oman, 12th and 13th May, 2015. Retrieved from https://arxiv.org/abs/1602.06510

Reznik, L., Buccigrossi III, V., Lewis, J., Dipon, A., Milstead, S., LaFontaine, N.... Silva, H. (2011, June). Security of computer use practice: The case of ordinary users survey. *6th Annual Symposium on Information Assurance (ASIA'11)*, Albany, NY, June 7-8, 2011.

Riley, S. (2006). Password security: What users know and what they actually do. *Usability News*, *8*(1), 2833-2836.

Rogers, R. (1983). Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation. *Social psychophysiology: A sourcebook*, 153-176.

Safa, N., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, *53*, 65-78.

Siponen, M., Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & management*, *51*(2), 217-224.

Skinner, W., & Fream, A. (1997). A social learning theory analysis of computer crime among college students. *Journal of Research in Crime and Delinquency*, *34*(4), 495-518.

Slusky, L., & Partow-Navid, P. (2012). Students information security practices and awareness. *Journal of Information Privacy and Security*, *8*(4), 3-26.

Teer, F., Kruck, S., and Kruck, G. (2007). Empirical study of students' computer security practices/perceptions. *Journal of Computer Information Systems*, *47*(3), 105-110.

Tekerek, M., & Tekerek, A. (2013). A research on students' information security awareness. *Turkish Journal of Education*, *2*(3).

Venkatesh, V., Morris, M., Davis, G., and Davis, F. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly*, 425-478.

Wash, R. (2010, July). Folk models of home computer security. Symposium on Usable Privacy and Security (SOUPS) 2010, July 14–16, 2010, Redmond, WA.

White, G., Ekin, T., & Visinescu, L. (2016). Analysis of protective behavior and security incidents for home computers. *Journal of Computer Information Systems,57*(4), 1-11.

White, G., & Long, J. (2007). Thinking globally: Incorporating an international component in information security curricula. *Information Systems Education Journal.* Retrieved from *http://isedj. org/galley/411.1913/*

Woon, I., Tan, G., & Low, R. (2005). A protection motivation theory approach to home wireless security. *ICIS 2005 proceedings*, 31. Retrieved from https://aisel.aisnet.org/icis2005/31

Xu, K., Gu, L., & Wang, F. (2013, December). Monitoring home network traffic via programmable routers. *Global Communications Conference (GLOBECOM), Atlanta Georgia, December 9-13,2013. IEEE.*

Yenisey, M., Ozok, A., & Salvendy, G. (2005). Perceived security determinants in e-

commerce among Turkish university students. *Behaviour & Information Technology*, *24*(4), 259-274.

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

Appendices

Appendix A

Informed Consent Form

The person in charge of this study is Amani Alqarni, a doctoral student at MidWestern University. Her faculty adviser is Professor Dorothy. Throughout this form, this person will be referred to as the "investigator."

Purpose of the study

The objective of this study is to explore the relationship between technology acceptance, protection motivation and planned behavior models and information security practices among college students.

What will happen if I participate in this study?

Participation in this study involves

- Completing a survey
- Spending ten minutes to fill out a written, pencil and paper, format questionnaire about your information security practices

What are the anticipated risks for participation?

There are no anticipated risks associated with participating in this study.

Are there any benefits to participating?

There are no direct personal benefits associated with participating in the study. General benefits include the increase of awareness on the risks associated with information security breaches among college students and the implementation of best practices to prevent and alleviate the consequences of such attacks.

How will my information be kept?

Your information will be anonymous. It will be kept in a password protected machine and on a password protected file. Access will not be given except to the advisor, dissertation committee members, if requested and the researcher.

Storing study information for future use

We may use the information collected for future research endeavors, publications, conference presentations or workshops. We will not sell your information to marketing agencies nor share them for any purposes unrelated to the advancement of research on information security practices.

Please initial below whether or not you allow us to store your information:

_____Yes _____No

Are there any costs to participation?

There are no costs associated with taking part in the study.

Will I be paid for participation?

There will be no compensation for participating in the study.

Study contact information

If you have any questions about the research, you can contact the Principal Investigator, Amani Alqarni, aalqarni@emich.edu or by phone at (810) 919 6668. You can also contact Professor Dorothy, dmcallen@emich.edu or by phone at (734) 487 4694.

For questions about your rights as a research subject, contact the Eastern Michigan University Human Subjects Review Committee at human.subjects@emich.edu or by phone at 734-487-3090.

Voluntary participation

Participation in this research study is your choice. You may refuse to participate at any time, even after signing this form, with no penalty or loss of benefits to which you are otherwise entitled. You may choose to leave the study at any time with no loss of benefits to which you are otherwise entitled. If you leave the study, the information you provided will be kept confidential. You may request, in writing, that your identifiable information be destroyed. However, we cannot destroy any information that has already been published.

Statement of Consent

I have read this form. I have had an opportunity to ask questions and am satisfied with the answers I received. I give my consent to participate in this research study.

Signatures

_____ _____

Signature of Subject Date

I have explained the research to the subject and answered all his/her questions. I will give a copy of the signed consent form to the subject.

_____

Name of Person Obtaining Consent

_____ _____

Signature of Person Obtaining Consent Date

Appendix B

RESEARCH @ EMU

UHSRC Determination: **EXEMPT**

Date: **August 16, 2017**

To: **Amani Alqarni**
Eastern Michigan University

Re: **UHSRC: # A20170808-1**
Category: Exempt category *2*
Approval Date: August 16, 2017

Title: **Exploring Factors that Affect Adoption of Computer Security Practices among College Students**

Your research project has been determined **Exempt** in accordance with federal regulation 45 CFR 46.102. UHSRC policy states that you, as the Principal Investigator, are responsible for protecting the rights and welfare of your research subjects and conducting your research as described in your protocol.

Renewals: Exempt protocols do not need to be renewed. When the project is completed, please submit the **Human Subjects Study Completion Form**.

Modifications: You may make minor changes (e.g., study staff changes, sample size changes, contact information changes, etc.) without submitting for review. However, if you plan to make changes that alter study design or any study instruments, you must submit a **Human Subjects Approval Request Form** and obtain approval prior to implementation.

Problems: All major deviations from the reviewed protocol, unanticipated problems, adverse events, subject complaints, or other problems that may increase the risk to human subjects **or** change the category of review must be reported to the UHSRC via an **Event Report** form.

Follow-up: If your Exempt project is not completed and closed after **three years**, the UHSRC office will contact you regarding the status of the project.

Please use the UHSRC number listed above on any forms submitted that relate to this project, or on any correspondence with the UHSRC office.

Good luck in your research. If we can be of further assistance, please contact us at 734-487-3090 or via e-mail at human.subjects@emich.edu. Thank you for your cooperation.

Sincerely,

April M Gravitt, MS
Research Compliance Analyst
University Human Subjects Review Committee

University Human Subjects Review Committee · Eastern Michigan University · 200 Boone Hall
Ypsilanti, Michigan 48197
Phone: 734.487.3090
E-mail: human.subjects@emich.edu
www.emich.edu/ord (see Research Compliance)

Appendix C

Survey Instrument

Computer Security Practices of Home Computer Users Survey

Demographics

Please indicate your age by _____.

a. 15-25
b. 26-35
c. 36+

What is your gender?

a. Male
b. Female
c. I'd rather not say.

Please list your major under the correct College:

a. College of Technology

   Major: _____

b. College of Business

   Major: _____

c. College of Arts & Science

   Major: _____

d. College of Health & Human Services

   Major: _____

e. College of Education

   Major: _____

What is your highest level of education that you have attained to date?

a. High school graduate
b. Some college
c. Associates degree
d. Bachelor
e. Masters or a professional degree

f. Doctorate

What is your IT Knowledge/Experience (in years)?

a. 1-5
b. 6-10
c. 11-15
d. 16-20
e. 21-25

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
Computer security practices					
1-Before reading an email, I will first check if the subject and the sender make sense.					
2-Before opening an email attachment, I will first check if the filename of the attachment makes sense.					
3- I exercise caution when I receive an email attachment as it may contain a virus.					
4-I do not open email attachments if the content of the email looks suspicious					
Perceived Vulnerability					
1-The chances of receiving an email attachment with virus are high					
2- There is a good possibility that I will receive an email attachment with virus.					
3- I am likely to receive an email attachment with virus.					
Perceived Severity					
1-Having my computer infected by a virus as a result of opening a suspicious email attachment is a serious problem for me					
2- Losing data as a result of opening a suspicious email attachment is a serious problem for me					
3-If my computer is infected by a virus					

as a result of opening a suspicious email attachment, my daily work could be negatively affected					
Response Efficacy					
1-In case of receiving a suspicious email, I can react effectively in a timely manner					
2-I have the necessary skills to deal with an email attachment containing a virus					
3-Once I detect a suspicious email or attachment, I know how to respond to it					
computer Self-Efficacy					
1-I am confident of recognizing a suspicious email					
2-I am confident of recognizing suspicious email headers					
3-I am confident of recognizing suspicious email attachment filename					
4-I can recognize a suspicious email attachment even if there was no one around to help me					
Perceived Usefulness					
1-Checking if the sender and subject make sense is an effective in preventing viruses from infecting my computer					
2-Checking if the filename of the email attachment makes sense is an effective in preventing viruses from infecting my computer					
3-Exercising care before opening email attachments is an effective in preventing viruses from infecting my computer					
Perceived Ease of Use					
1-Exercising care when reading emails with attachments is convenient					
2-Exercising care when reading emails with attachments is not time-consuming					
3-Exercising care when reading emails with attachments would not require considerable investment of effort other than time					
4-Exercising care when reading emails with attachments would not require starting a new habit, which is difficult					

Awareness					
1-I read information security bulletins or newsletters.					
2-I am concerned about security incidents and try to take action to prevent them					
3-I am interested in information about computer security					
4-I am constantly mindful about computer security					
Attitudes					
1-Computer security is really important					
2-Learning how to prevent security incidents is important					
3-Investing in learning and developing skills for computer security is an essential quality everyone should have					
Subjective Norms					
1-My family and friends believe that computer security is important					
2-My co-workers/classmates believe that computer security is quite essential					
3-My professors/supervisors at work believe that computer security is very important					
Perceived Behavioral Control					
1-It is difficult to exercise computer security for me					
2-It is difficult to check emails or files for viruses or suspicious material for me					
3-It is difficult to cope with a corrupted email or file sent to me					

Appendix D

Table 16.

Corrected Total Item Correlations

	CSP1	CSP2	CSP3	CSP4	PV1	PV2	PV3	PS1	PS2	PS3	RE1	RE2	RE3	SE1	SE2	SE3	SE4	PU1	PU2	PU3	PEU1	PEU2	PEU3	PEU4	A1	A2	A3	A4	ATT1	ATT2	ATT3	SN1	SN2	SN3	PBC1	PBC2	PBC3
CSP1	1.000	.565	.407	.282	.243	.249	.218	.087	.075	.206	.243	.224	.226	.242	.221	.161	.187	.293	.264	.246	.268	.212	.165	.234	.149	.224	.182	.221	.220	.209	.265	.201	.190	.198	-.047	-.007	-.011
CSP2	.565	1.000	.575	.300	.267	.280	.278	.099	.094	.198	.361	.349	.346	.330	.297	.357	.301	.318	.294	.347	.235	.259	.245	.322	.209	.325	.303	.358	.366	.344	.294	.197	.236	.216	-.193	-.134	-.080
CSP3	.407	.575	1.000	.527	.348	.294	.279	.149	.127	.170	.374	.366	.395	.454	.439	.488	.457	.293	.226	.359	.260	.257	.225	.291	.208	.372	.241	.364	.228	.215	.201	.177	.155	.138	-.297	-.309	-.246
CSP4	.282	.300	.527	1.000	.280	.319	.289	.059	.063	.157	.213	.251	.300	.423	.398	.390	.396	.235	.150	.235	.188	.166	.107	.131	.122	.194	.116	.190	.158	.140	.179	.096	.153	.115	-.264	-.232	-.238
PV1	.243	.267	.348	.280	1.000	.727	.628	.244	.217	.153	.201	.230	.282	.229	.144	.201	.167	.216	.176	.170	.176	.169	.157	.290	.244	.295	.246	.212	.127	.212	.176	.186	.218	.145	-.045	-.015	-.058

Table 18 *continued*

	CSP1	CSP2	CSP3	CSP4	PV1	PV2	PV3	PS1	PS2	PS3	RE1	RE2	RE3	SE1	SE2	SE3	SE4	PU1	PU2	PU3	PEU1	PEU2	PEU3	PEU4	A1	A2	A3	A4	ATT1	ATT2	ATT3	SN1	SN2	SN3	PBC1	PBC2	PBC3
PV2	.249	.280	.294	.319	.727	1.000	.768	.181	.226	.246	.219	.237	.285	.292	.174	.212	.271	.217	.228	.204	.153	.136	.162	.249	.267	.354	.257	.264	.229	.301	.278	.200	.235	.130	-.111	-.127	-.055
PV3	.218	.278	.279	.289	.628	.768	1.000	.181	.183	.224	.166	.199	.257	.278	.203	.215	.252	.256	.241	.231	.171	.163	.171	.212	.194	.261	.155	.202	.140	.238	.202	.123	.144	.092	-.145	-.120	.090
PS1	.087	.099	.149	.059	.244	.181	.181	1.000	.865	.411	.023	-.062	-.011	-.085	-.050	-.061	-.055	.080	.153	.134	.090	.004	.059	.059	.027	.180	.130	.122	.143	.171	.142	.204	.209	.114	.086	.133	.167
PS2	.075	.094	.127	.063	.217	.226	.183	.865	1.000	.483	.064	-.034	.012	-.028	.005	.047	.025	.110	.161	.145	.148	.058	.110	.099	.051	.218	.093	.114	.112	.131	.139	.188	.214	.092	.085	.129	.160
PS3	.206	.198	.170	.157	.153	.246	.224	.411	.483	1.000	.255	.066	.079	.116	.141	.094	.136	.194	.202	.254	.260	.211	.210	.171	.079	.234	.098	.055	.191	.137	.134	.096	.118	.074	-.041	-.048	.029
RE1	.243	.361	.374	.213	.201	.219	.166	.023	.064	.255	1.000	.627	.630	.461	.412	.443	.423	.292	.256	.257	.304	.316	.315	.358	.218	.260	.266	.353	.219	.272	.276	.128	.155	.079	-.154	-.205	.213

Table 18 *continued*

	CSP1	CSP2	CSP3	CSP4	PV1	PV2	PV3	PS1	PS2	PS3	RE1	RE2	RE3	SE1	SE2	SE3	SE4	PU1	PU2	PU3	PEU1	PEU2	PEU3	PEU4	A1	A2	A3	A4	ATT1	ATT2	ATT3	SN1	SN2	SN3	PBC1	PBC2	PBC3
RE2	.224	.349	.366	.251	.230	.237	.199	-.062	-.034	.066	.627	1.000	.855	.513	.478	.485	.505	.207	.143	.161	.292	.224	.240	.271	.315	.285	.214	.370	.185	.249	.204	.076	.131	.069	-.244	.223	.334
RE3	.226	.346	.395	.300	.282	.285	.257	-.011	.012	.079	.630	.855	1.000	.603	.521	.538	.555	.249	.155	.201	.274	.253	.240	.285	.294	.296	.257	.357	.181	.246	.223	.096	.136	.057	-.229	.227	.284
SE1	.242	.330	.454	.423	.229	.292	.278	-.085	-.028	.116	.461	.513	.603	1.000	.787	.765	.777	.381	.238	.332	.325	.333	.273	.281	.212	.223	.107	.287	.149	.146	.154	.088	.128	.061	-.352	.316	.339
SE2	.221	.297	.439	.398	.144	.174	.203	-.050	-.005	.141	.412	.478	.521	.787	1.000	.764	.731	.324	.262	.291	.272	.236	.242	.291	.213	.299	.095	.236	.094	.101	.093	.082	.109	.066	-.317	.272	.323
SE3	.161	.357	.488	.390	.201	.212	.215	-.061	-.047	.094	.443	.485	.538	.765	.764	1.000	.797	.319	.248	.274	.292	.283	.256	.322	.222	.273	.150	.282	.153	.168	.086	.037	.068	.003	-.336	.306	.352
SE4	.187	.301	.457	.396	.167	.271	.252	-.055	-.025	.136	.423	.505	.555	.777	.731	.797	1.000	.392	.281	.357	.352	.331	.286	.312	.223	.265	.116	.340	.161	.165	.125	.081	.117	.031	-.336	.324	.336

Table 18 *continued*

	CSP1	CSP2	CSP3	CSP4	PV1	PV2	PV3	PS1	PS2	PS3	RE1	RE2	RE3	SE1	SE2	SE3	SE4	PU1	PU2	PU3	PEU1	PEU2	PEU3	PEU4	A1	A2	A3	A4	ATT1	ATT2	ATT3	SN1	SN2	SN3	PBC1	PBC2	PBC3
PU1	.293	.318	.293	.235	.216	.217	.256	.080	.110	.194	.292	.207	.249	.381	.324	.319	.392	1.000	.691	.555	.322	.279	.259	.296	.235	.279	.073	.173	.160	.245	.203	.156	.184	.176	-.128	-.104	.062
PU2	.264	.294	.226	.150	.216	.228	.241	.153	.161	.202	.256	.143	.155	.238	.262	.248	.281	.691	1.000	.534	.307	.221	.209	.268	.265	.224	.087	.143	.114	.167	.186	.116	.122	.101	-.108	.067	.042
PU3	.246	.347	.359	.235	.170	.204	.231	.134	.145	.254	.257	.161	.201	.332	.291	.274	.357	.555	.534	1.000	.357	.370	.278	.240	.113	.278	.099	.223	.196	.205	.252	.111	.184	.180	-.202	.186	-.146
PEU1	.268	.235	.260	.188	.176	.153	.171	.090	.148	.260	.304	.292	.274	.325	.272	.292	.352	.322	.307	.357	1.000	.604	.449	.458	.294	.251	.040	.148	.158	.156	.222	.166	.199	.112	-.033	.046	.144
PEU2	.212	.259	.257	.166	.169	.136	.163	.004	.058	.211	.316	.224	.253	.333	.236	.283	.331	.279	.221	.370	.604	1.000	.558	.554	.264	.185	.055	.140	.148	.126	.191	.136	.124	.079	-.031	.046	-.107
PEU3	.165	.245	.225	.107	.157	.162	.171	.059	.110	.210	.315	.240	.240	.273	.242	.256	.286	.259	.209	.278	.449	.558	1.000	.607	.296	.260	.123	.275	.222	.233	.216	.149	.208	.111	-.067	-.086	-.095

Table 18 *continued*

	CSP1	CSP2	CSP3	CSP4	PV1	PV2	PV3	PS1	PS2	PS3	RE1	RE2	RE3	SE1	SE2	SE3	SE4	PU1	PU2	PU3	PEU1	PEU2	PEU3	PEU4	A1	A2	A3	A4	ATT1	ATT2	ATT3	SN1	SN2	SN3	PBC1	PBC2	PBC3
PEU4	.234	.322	.291	.131	.290	.249	.212	.059	.099	.171	.358	.271	.285	.281	.291	.332	.312	.296	.268	.240	.458	.554	.607	1.000	.337	.234	.175	.208	.237	.250	.284	.135	.197	.098	-.006	-.037	-.075
A1	.149	.209	.208	.122	.244	.267	.194	.027	.051	.079	.218	.315	.294	.212	.213	.222	.223	.235	.265	.113	.294	.264	.296	.337	1.000	.518	.322	.291	.182	.268	.248	.239	.180	.092	-.009	.027	-.053
A2	.224	.325	.372	.194	.295	.354	.261	.180	.218	.234	.260	.285	.296	.223	.229	.273	.265	.279	.224	.278	.251	.185	.260	.234	.518	1.000	.502	.547	.337	.399	.367	.283	.243	.134	-.132	.032	.012
A3	.182	.303	.241	.116	.246	.257	.155	.130	.093	.098	.266	.214	.257	.107	.095	.150	.116	.073	.087	.099	.040	.055	.123	.175	.322	.502	1.000	.603	.390	.480	.442	.286	.239	.153	-.007	.048	.059
A4	.221	.358	.364	.190	.212	.264	.202	.122	.114	.055	.353	.370	.357	.288	.236	.282	.340	.173	.143	.223	.148	.140	.275	.208	.291	.547	.603	1.000	.410	.420	.381	.297	.256	.108	-.171	.113	.124
ATT1	.220	.366	.228	.158	.127	.229	.140	.143	.112	.191	.219	.185	.181	.149	.094	.153	.161	.160	.114	.196	.158	.148	.222	.237	.182	.337	.390	.410	1.000	.709	.601	.359	.341	.220	-.132	.180	.091

Table 18 *continued*

	CSP1	CSP2	CSP3	CSP4	PV1	PV2	PV3	PS1	PS2	PS3	RE1	RE2	RE3	SE1	SE2	SE3	SE4	PU1	PU2	PU3	PEU1	PEU2	PEU3	PEU4	A1	A2	A3	A4	ATT1	ATT2	ATT3	SN1	SN2	SN3	PBC1	PBC2	PBC3
ATT2	.209	.344	.215	.140	.212	.301	.238	.171	.131	.137	.272	.249	.246	.146	.101	.168	.165	.245	.167	.205	.156	.126	.233	.250	.268	.399	.480	.420	.709	1.000	.686	.384	.352	.247	-.084	-.146	-.047
ATT3	.265	.294	.201	.179	.176	.278	.202	.142	.139	.134	.276	.204	.223	.154	.093	.086	.125	.203	.186	.252	.222	.191	.216	.284	.248	.367	.442	.381	.601	.686	1.000	.412	.402	.328	-.029	-.064	-.039
SN1	.201	.197	.177	.096	.186	.200	.123	.204	.188	.096	.128	.076	.096	.088	.082	.037	.081	.156	.116	.111	.166	.136	.149	.135	.239	.283	.286	.297	.359	.384	.412	1.000	.643	.408	.072	.089	.129
SN2	.190	.236	.155	.153	.218	.235	.144	.209	.214	.118	.155	.131	.136	.128	.109	.068	.117	.184	.122	.184	.199	.124	.208	.197	.180	.243	.239	.256	.341	.352	.402	.643	1.000	.631	-.001	.050	.018
SN3	.198	.216	.138	.115	.145	.130	.092	.114	.092	.074	.079	.069	.057	.061	.066	.031	.063	.176	.101	.180	.112	.079	.111	.098	.092	.134	.153	.108	.220	.247	.328	.408	.631	1.000	.066	.113	.110
PBC1	-.047	-.193	-.297	-.264	-.045	-.111	-.145	.086	.085	-.041	-.154	-.244	-.229	-.352	-.317	-.336	-.336	-.128	-.108	-.202	-.033	-.031	-.067	-.006	-.009	-.132	-.107	-.171	-.132	-.084	-.029	.072	-.001	.066	1.000	.761	.717

Table 18 *continued*

	CSP1	CSP2	CSP3	CSP4	PV1	PV2	PV3	PS1	PS2	PS3	RE1	RE2	RE3	SE1	SE2	SE3	SE4	PU1	PU2	PU3	PEU1	PEU2	PEU3	PEU4	A1	A2	A3	A4	ATT1	ATT2	ATT3	SN1	SN2	SN3	PBC1	PBC2	PBC3
PBC2	-.007	-.134	-.309	-.232	-.015	-.127	-.120	.133	.129	-.048	-.205	-.223	-.227	-.316	-.272	-.306	-.324	-.104	-.067	-.186	-.046	-.046	-.086	-.037	.027	-.032	.048	-.113	-.180	-.146	-.064	.089	.050	.113	.761	1.000	.764
PBC3	-.011	-.080	-.246	-.238	-.058	-.055	-.090	.167	.160	-.029	-.213	-.334	-.284	-.339	-.323	-.352	-.336	-.062	-.042	-.146	-.144	-.107	-.095	-.075	-.053	-.012	-.059	-.124	-.091	-.047	-.039	.129	.018	.110	.717	.764	1.000