Mississippi State University
Scholars Junction

Theses and Dissertations Theses and Dissertations

1-1-2013

The Role of Habit in Information Security Behaviors

Kalana Malimage

Follow this and additional works at: https://scholarsjunction.msstate.edu/td

Recommended Citation
Malimage, Kalana, "The Role of Habit in Information Security Behaviors" (2013). *Theses and Dissertations*. 4635.
https://scholarsjunction.msstate.edu/td/4635

This Dissertation - Open Access is brought to you for free and open access by the Theses and Dissertations at Scholars Junction. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of Scholars Junction. For more information, please contact scholcomm@msstate.libanswers.com.

www.manaraa.com

The role of habit in information security behaviors

By

Kalana Malimage

A Dissertation
Submitted to the Faculty of
Mississippi State University
in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy
in Business Information Systems
in the Department of Management & Information Systems

Mississippi State, Mississippi

December 2013

www.manaraa.com

Copyright by

Kalana Malimage

2013

المنارة للاستشارات

www.manaraa.com

The role of habit in information security behaviors

By

Kalana Malimage

Approved:

Merrill Warkentin
(Director of Dissertation)

Robert F. Otondo
(Committee Member)

Kent Marett
(Committee Member)

Robert E. Crossler
(Committee Member)

Joe Sullivan
(Committee Member)

Rebecca G. Long
(Graduate Coordinator)

Sharon L. Oswald
Dean
College of Business

المنارة للاستشارات
www.manaraa.com

Name: Kalana Malimage

Date of Degree: December 14, 2013

Institution: Mississippi State University

Major Field: Business Information Systems

Major Professor: Dr. Merrill Warkentin

Title of Study: The role of habit in information security behaviors

Pages in Study: 327

Candidate for Degree of Doctor of Philosophy

The purpose of this present study is to understand the role of habit in information security behaviors. The automatic aspect of habit and its impact on secure behavior and the intention-behavior relationship was explored in this dissertation through the lens of protection motivation theory. Three secure behaviors were selected for the investigation after following a rigorous process to identify habitual secure behaviors. The three behaviors that were investigated are: locking the PC when leaving it unattended, verifying the recipient email addresses before sending email and visiting only verified websites. Separate pilot studies were conducted for each of the behaviors followed by a main investigation. Habit was measured with a first-order reflective and second-order formative scale that captured the multidimensional aspects of habit: Lack of Awareness, Uncontrollability and Mental Efficiency.

Data were collected for each of the behaviors separately via separate online surveys using Amazon Mechanical-Turk. The results of the data analyses indicate that habit significantly influence the performance of secure behavior while negatively moderating the intention-behavior relationship for each of the three behaviors. The

www.manaraa.com

findings also confirm that when certain behaviors are habitual, the cognitive resources needed to make decisions on performing behavior reduce. Several alternate models were analyzed as a part of the post hoc phase of the study.

The findings of this study provide several contributions to the IS research and practice. This study investigated the role of habit in an information security context using a second-order formative scale. The findings indicate that habit play a significant role in the performance of secure behaviors and verifies the relationship between intention and behavior in an information security context. The findings provide directions to organizations in understanding habits of their employees and to foster positive habits while breaking negative habits. The findings of this study provide several future research directions and highlight the importance of further exploration of habit in an information security context.

www.manaraa.com

DEDICATION

I would like to dedicate this dissertation to my wife, Nirmalee; my parents, Asoka and Ruwan; my sister, Anu, my in-laws Piyatissa, Lilamani and Upul, my friends and my professors. This dissertation could not have been completed without the support from all of you. Thank you for your understanding and patience during the completion of my dissertation.

المنارة للاستشارات

www.manaraa.com

ACKNOWLEDGEMENTS

I would like to thank everyone who has supported me during my years in the doctoral program at Mississippi State University. First, I would like to thank my wife, Nirmalee, who first got me interested in pursuing a doctoral degree and supported me throughout the whole time. Without her encouragement and support this dissertation would not have been possible. I also like to thank my parents and in-laws who patiently supported me through this journey

I like to extend my sincere gratitude to my dissertation committee who contributed immensely to make this dissertation a success. Dr. Robert Otondo provided his extensive insights into information systems theory and methods. Dr. Kent Marett extended his expertise and guidance in information security in instrument development and theory. Dr. Joe Sullivan tirelessly and exceptionally guided me through the statistical analysis and provided inspiration to achieve high standards of quantitative analysis while providing me ideas on how to solve difficulties during my dissertation. Dr. Robert Crossler, inspired me to reach greater lengths in creative thinking and provided excellent guidance, feedback and support to shape my dissertation to be a success.

My deepest appreciation goes to the chair of my dissertation committee, Dr. Merrill Warkentin. I would like to thank him for his patience, support and wisdom in transforming me from a student to a scholar. I also like to thank him for his guidance throughout my dissertation and providing me great feedback and support, while always

المنارة للاستشارات
www.manaraa.com

encouraging me to strive for high quality and rigor. His passion for research and excellence has inspired me immensely throughout the years in this doctoral program. Through his leadership and guidance, I have been able to successfully complete this program. I would be forever grateful to him for being a great mentor, coauthor and friend.

I would also like to thank the entire faculty of the Management and Information Systems Department for their support and encouragement. A very special acknowledgement goes to my fellow doctoral students: Phil Menard, Jim Lee, Shwadhin Sharma, Dustin Ormond, Mike Pope and Leigh Mutchler. Thank you for your encouragement and support during this journey. I look forward to continuing our friendships in the future. I also like to thank Ms. Nadine Rosinski and Angella Baker who were very helpful whenever I needed any assistance.

المنارة للاستشارات
www.manaraa.com

TABLE OF CONTENTS

المنـــارة للاستشارات

www.manaraa.com

المنارة للاستشارات
www.manaraa.com

APPENDIX

المنارة للاستشارات
www.manaraa.com

المنارة للاستشارات

www.manaraa.com

LIST OF TABLES

www.manaraa.com

المنارة للاستشارات

www.manaraa.com

المنارة للاستشارات
www.manaraa.com

LIST OF FIGURES

المنارة للاستشارات

www.manaraa.com

المنارة للاستشارات

www.manaraa.com

CHAPTER I

INTRODUCTION

Organizations continue to struggle protecting their information systems daily from various threats and spend billions of dollars to build defenses to counter these threats. Some of these threats include natural and manmade disasters, errors by internal employees, acts of competitors with malicious intent, hackers, spyware and viruses (Loch et al. 1992; Willison and Warkentin 2013). The reliance of organizations on information systems and the increased connectivity of organizational information systems to the internet has increased the exposure to threats from hackers, spyware and viruses (Whitman 2003). These increased threats have caused many organizations to enforce strong countermeasures to deter and prevent them, including technical and behavioral controls. Although technical controls were the primary form of information security in the past, organizations have realized that technology tools alone cannot secure their information systems. An increased focus on insiders (e.g. employees) and their behavior has resulted in organizations implementing security education, training, and awareness (SETA) campaigns (D’Arcy et al. 2009; Puhakainen and Siponen 2010), strict information security policies and procedures (Warkentin and Johnston 2008), and sanctions to deter policy violations (D’Arcy and Devaraj 2012; D’Arcy and Herath 2011; D’Arcy et al. 2009; Xu et al. 2013) to counter threats to their information systems.

www.manaraa.com

However, these controls and security policies are only effective to the extent that employees and others follow them.

Organizations have implemented information security policies that require their employees to perform many secure behaviors on a routine basis. Some of these enforced behaviors include technical aspects such as backing up data, running anti-virus software, encrypting sensitive data before sending it over the internet, locking workstations and behavioral aspects such as being cautious about opening email attachments, visiting only verified or known websites and avoiding discussing sensitive information in public areas (Posey et al. 2013). These behaviors, performed on a routine basis by employees, provide organizations with significantly reduced information security risks that originate inside the workplace. Employees may initially perform these secure behaviors due to sanctions being in place for non-compliance or due to threat awareness. However, employees may perform these behaviors automatically after successful repetition.

Information security policies that are properly implemented would most likely be unsuccessful if employees do not follow them. With the critical nature of information security, it only requires one incident or lapse of following security measures for an information security breach to occur. Thus, employees are identified as the weakest security link in an organization (Crossler et al. 2013; Warkentin and Willison 2009). Security policy violations or noncompliant behavior can be malicious or non-malicious in nature (Guo et al. 2011), but both types of behavior will open an organization to information security threats. Organizations continuously attempt to reduce malicious behavior through security controls, deterrence and organizational policies. Non-malicious behavior or "human error" is known to be the reason for the majority of policy violations

المنارة للاستشارات
www.manaraa.com

and security incidents at organizations (Plamondon 2011). Organizations have increased their efforts to curtail these non-malicious employee behaviors through measures such as information security training and behavioral shaping (e.g., creating habitual security practices) (Harnesk and Lindström 2011).

It is important to understand that most of these positive or negative behaviors performed by employees may be a part of their work routine, performed frequently and automatically. When certain behaviors are performed successfully on a routine basis and in a stable context, employees may perform these behaviors automatically or habitually (Limayem et al. 2007). Habit is defined as "learned sequences of acts that become automatic responses to specific situations, which may be functional in obtaining certain goals or end states" (Verplanken et al. 1997, p. 540). Therefore, when information security behaviors are performed as automatic responses to certain environmental situations, in order to achieve goals (securing information), they can be called 'habitual.' For example, an employee may frequently and automatically lock his or her computer every time he or she leaves the terminal unattended, which exhibits a habitual compliant behavior or a positive habit (Siponen et al. 2010). On a similar note, even though the organizational policy states otherwise, an employee may intentionally share his or her password to a secure system with a colleague (Siponen and Vance 2010). Continuously sharing of passwords, however, may become a habitual (automatic) non-compliant behavior or a negative habit. Several research studies also identified that habits can be formed in password construction, changing passwords and writing down passwords (Brown et al. 2004; Florencio and Herley 2007; Morris and Thompson 1979). It is also important to note that some employees may not lock their computer due to negligence.

المنارة للاستشارات
www.manaraa.com

The employee does not fail to lock the computer due to any malicious intentions, thus it is non-malicious (Guo et al. 2011; Willison and Warkentin 2013). The negligent behavior cannot be considered habitual since is not initiated intentionally and does not initiate the habit formation process. Therefore, habitual behaviors can be either positive or negative and not all behaviors form habits. Extant research on information security focuses more on behavioral intention and behavior, and most of these studies have ignored the influence of these habitual behaviors related to security.

The remainder of the chapter provides an overview of information security risks and organizational security policies followed by descriptions of threat avoidance, Protection Motivation Theory (PMT) and Habit Theory. These theories provide the foundation for the conceptual model that seeks to explain and predict the direct effect of habit on actual secure behavior and the moderating effect habit on the relationship between behavioral intention and actual behavior. An overview of the conceptual model, the research objective and research methods are described, followed by statements about the significance of the study and the organization of the rest of the chapters.

Information Security Risks

Information security risks have become a cause of major concern to most organizations. The security risks have multiplied with the information explosion that has been experienced globally by organizations especially in the last decade. These security-related issues have been complicated with more users having ubiquitous access to computers and the internet. With a plethora of data available, organizations have been struggling to keep the data organized, easily accessible, and most importantly, highly secured (Whitman 2003). Organizations also rely on data as a strategic asset. Maintaining

المنارة للاستشارات

www.manaraa.com

the integrity of that data is a primary goal of information assurance and security of each organization. In order to secure the information from external parties, such as hackers and thieves, organizations have employed different technical controls such as firewalls, intrusion detection systems, honeypots, honeynets and other security mechanisms (Whitman 2003). These mechanisms are effective in securing company information only from external parties such as hackers. The Information Systems(IS) Threat Taxonomy (Willison and Warkentin 2013), as illustrated in Figure 1.1, provides valuable insights into how the threats to information systems can be categorized.

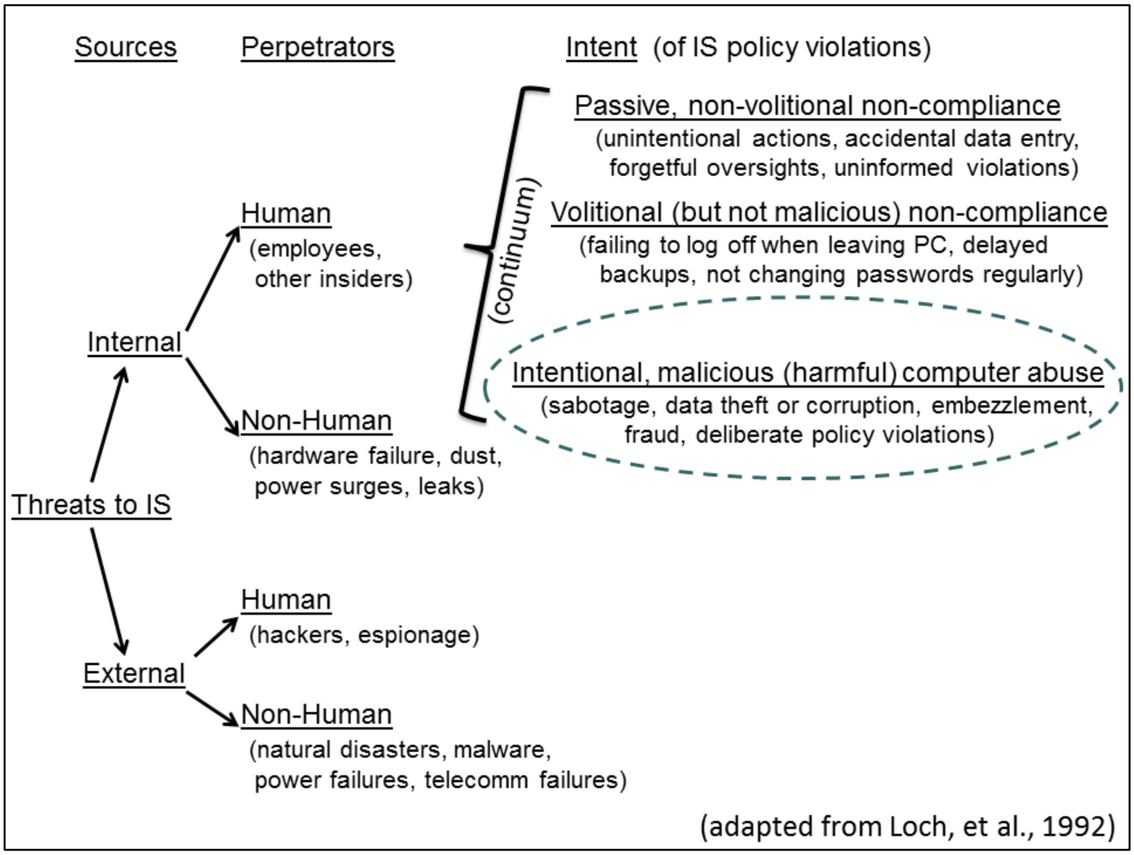

Sources
Perpetrators
Intent (of IS policy violations)
Passive, non-volitional non-compliance
(unintentional actions, accidental data entry, forgetful oversights, uninformed violations)
Volitional (but not malicious) non-compliance
(failing to log off when leaving PC, delayed backups, not changing passwords regularly)
Intentional, malicious (harmful) computer abuse
(sabotage, data theft or corruption, embezzlement, fraud, deliberate policy violations)
(continuum)
Human
(employees, other insiders)
Internal
Non-Human
(hardware failure, dust, power surges, leaks)
Threats to IS
Human
(hackers, espionage)
External
Non-Human
(natural disasters, malware, power failures, telecomm failures)
(adapted from Loch, et al., 1992)

Figure 1.1 IS Threat Taxonomy (Willison and Warkentin 2013)

www.manaraa.com

Threats to information systems were formerly considered to be only external to the organizations. However the threat landscape has become more complicated such that internal threats have become a major area of concern. Both internal and external threats to IS, can be divided into two categories: human and non-human threats. Non-human external threats such as natural disasters (e.g., hurricanes, floods, and earthquakes), power failures or telecommunication failures have resulted in billions of losses to organizations. Non-human internal threats such as hardware failure, power surges and leaks are similar in nature to external threats. Although these types of threats are not controllable, organizations have taken measures such as creating redundant servers at remote locations, redundant backup systems in different locations and investing in more reliable fail-proof hardware to reduce the repercussions from these threats.

The most serious external and internal threats to information systems of organizations originate from humans (Warkentin and Willison 2009; Willison and Warkentin 2013). In terms of external human threats, intentional malicious acts by external parties such as espionage and hackers have become an increasing threat to secure or sensitive information stored on corporate servers. The goal of most hackers who operate with malicious intent is to gain access to secure corporate data in order to carry out espionage or make the secure information public in order to degrade a company's ability to secure its data (Hu et al. 2011). Recent developments indicate that hacking groups or 'hacktivists' such as Anonymous and LulzSec operate to simply gain access to sensitive data from corporations and governments and make them public in order to "publicize the corruption and illicit activities" taking place in the organizations (Gjelten 2012). Hacking groups use techniques such as distributed denial of service (DDoS)

المنارة للاستشارات
www.manaraa.com

attacks to disable corporate and government websites and employ sophisticated hacking techniques to gain access to data and deface the websites.

Malicious software (malware) such as viruses and spyware pose another extreme threat to organizational data (Luo and Warkentin 2008). While most viruses or spyware are utilized for installing adware programs, to wipe out personal data or impose software or hardware restrictions on personal computers, some malware are programmed to take an extra step of accessing and transmitting secure data that belongs to organizations. According to the Computer Crime and Security Survey (2011), malware attacks were reported as the most common threat to corporate information security. Recent developments in the malware threat landscape suggests that malware are becoming increasingly sophisticated and used as a weapon to conduct espionage on other governments or corporations and counter-terrorism activities. In a recent *New York Times* article, it was revealed that 'Stuxnet,' which was a virus that disabled nuclear enrichment equipment in Iran, was created by the collaboration between the United States and Israel (Sanger 2012). Another virus called 'Flame,' which is known to "exceed those of all other cyber menaces known to date," has been discovered in Iran (Kaspersky 2012, p. 1). The Flame virus has the ability to capture the content on a user's screen, turn on a computer's microphone to record conversations, detect who and what is on a network, collect lists of vulnerable passwords, and transfer users computer files to another server (Goldman 2012). If a virus were to infect a corporate or government server with highly sensitive data, it would have damaging consequences. It is interesting to note that the Stuxnet and possibly the Flame virus were infected through an employee plugging in a USB drive from an unknown source to a corporate or organizational computer and not by

المنارة للاستشارات

www.manaraa.com

hacking activity that penetrated through the server security defenses. This shows how the internal threats can be a major concern to many organizations.

According to the 2011 Computer Crime and Security Survey (Richardson 2012), respondents from government, financial, medical, business, and higher education institutions reported malware and insider abuse (internal threat) comprised the most frequent forms of information security breaches. Willison and Warkentin (2013) categorize the internal human threats into passive (non-volitional), volitional (non-malicious), and intentional (malicious) in terms of security policy violations of an organization. Intentional malicious threats include data theft, intentional data corruption, deliberate policy violations and fraud. These types of threats cannot be prevented completely but they can be reduced through stringent technical controls in place that will alert the management of any illicit actions that are taking place using IS. Although intentional and malicious violations of security policy can occur, their occurrence is rare (Richardson 2012). The more common occurrences of internal threats in an organization are the volitional and passive threats (Willison and Warkentin 2013). In passive or non-volitional non-compliance of security polices, employees may violate security policies unintentionally by acts such as accidental data entry or deletion, forgetful oversights or any other unintentional acts. Although these acts may be unintentional, they can be detrimental to the information security of the organization. Volitional but non-malicious acts that are performed frequently by employees can also have serious repercussions on information security. Some of these volitional acts may include delaying backups, not changing passwords regularly or failing to log off or lock the computer when leaving it unattended as required by the company security policy.

المنارة للاستشارات
www.manaraa.com

The increased threats from insiders have resulted in organizations implementing security education, training, and awareness (SETA) (D'Arcy et al. 2009; Puhakainen and Siponen 2010), strict information security policies and procedures (Warkentin and Johnston 2008), and sanctions to deter policy violations (D'Arcy and Devaraj 2012; D'Arcy and Herath 2011; D'Arcy et al. 2009; Xu et al. 2013) to counter threats to their information systems. With the increased focus on insider threats to organizations, scholars have conducted various research studies on all three categories of internal threats. One of the most frequently studied areas in IS security research is the organizational security compliance and the factors that influence employees to comply or violate these policies (Bulgurcu et al. 2010; Herath and Rao 2009; Ifinedo 2012; LaRose et al. 2008; Pahnila et al. 2007; Vance et al. 2012).

While some employees may comply with the security policies and perform the recommended secure behaviors, other employees may intentionally violate these policies. These compliant or positive behaviors and the previously discussed negative behaviors, when practiced on a routine basis, may become habitual. Organizations should strive to influence their employees to practice secure behaviors automatically or habitually since it significantly reduces the chances of non-compliance by employees due to negligence. Therefore, organizations should encourage their employees perform secure behaviors habitually. Similarly, organizations would prefer their employees to refrain from forming non-compliant habitual behaviors. If certain non-compliance behaviors are performed habitually by employees, the organizations should attempt to break those habits. SETA programs can be effective solutions to form positive habits and break negative habits of employees through frequently administered security communications such as pop-up

www.manaraa.com

messages, sidebar in a newsletter or post-it notes with encouragement to comply with security policies. Recent research seems to suggest that both positive and negative habits are formed similarly (Neal et al. 2013). Although behaviors performed habitually by employees can be either positive or negative, the focus of this present study is on positive habits related to information security at the workplace.

Threat Avoidance

Criminology research and a plethora of psychology research suggest that it is human nature to seek rewards and avoid punishment (Becker 1968; McCarthy 2002; Paternoster and Pogarsky 2009; Paternoster and Simpson 1996; Piquero et al. 2005; Westland 1997). Rational Choice Theory (RCT) provides the foundation to this view by arguing that an individual undergoes a cognitive process that balances the costs and benefits of his or her actions before a course of action is taken (Beccaria 1770; Bentham 1781; Paternoster and Simpson 1996). Behavioral theories based on reinforcement suggest that an individual who is satisfied by performing a certain behavior is likely to repeat the same behavior. Similarly, an individual is likely to avoid repeating a behavior that had resulted in unsatisfactory outcomes (Freud 1915). These threats that humans typically try to avoid (Witte 1992) can be in the form of health-related threats, natural disasters, terrorism and information technology threats, to name a few.

Based on Cybernetic Theory (Wiener 1948), which posits that humans self-regulate their behaviors through feedback loops, Liang and Xue (2009) developed the Technology Threat Avoidance Theory (TTAT). TTAT explains individual behavior of avoiding certain IS security threats by utilizing positive feedback loops. In these positive loops, an anti-goal is the threat or occurrence that needs to be averted. TTAT posits that

المنارة للاستشارات
www.manaraa.com

individuals perform secure behaviors to distance themselves from these anti-goals. Threat and coping appraisals are recognized as major components of the threat avoidance process and process view of TTAT affirms that threat appraisal occurs first (Liang and Xue 2009). This is consistent with theories such as the Extended Parallel Process Model (EPPM) posit that threat appraisals need to occur prior to coping appraisals (Witte 1992). If the threat is not perceived first, individuals will have no necessity to apply coping mechanisms. If a threat is perceived, it will lead to coping appraisal, which may be either emotional-based coping or problem-based coping. Emotional-based maladaptive coping may be in the form of religious faith or denial of the presence of a threat. Problem-based coping is performing an adaptive response such as following the recommended response. However, the variance theory view of TTAT, which provides a cross-sectional view of the threat avoidance process, suggests that threat and coping appraisals can occur in parallel. The view that threat and coping appraisal could occur in parallel was initially suggested by Rogers (1983) and many recent IS security studies have followed this view.

According to TTAT, when an individual faces a threat, a threat appraisal process is activated, followed by the coping appraisal process, and adaptive or maladaptive behavior is performed as a result. This process continues on a feedback loop. However, TTAT does not consider the outcome of the feedback loop being repeated many times in a stable context. When the adaptive behavior is repeated in a stable context, habits may be formed, developing a habit loop. The habit loop consists of a cue, routine and a reward. A cue or environmental trigger will initiate the automatic behavior, which results in a reward or satisfaction (Duhigg 2012). The habit loop will continue until there is a disturbance in the environment or a trigger causing the process to return to the positive

المنارة للاستشارات
www.manaraa.com

feedback loop. The automatic nature of habit and the variance theory view of TTAT provide a sound theoretical basis for this present study to investigate the role of habit in information security behaviors and explore the primary research question as shown below.

The primary research question that is explored in this study is:

RQ: What role does habit play in individuals' performance of information security behaviors in the workplace?

While exploring the primary research questions, the findings of this study are utilized for additional analysis. The impact of threat and coping appraisals on the performance of secure behavior in various levels of habit strength, was investigated in this study. Furthermore, this study explored the direct effect of habit on secure behaviors and the moderating effect of habit on the intention-behavior relationship.

Protection Motivation Theory

Protection Motivation Theory (Rogers 1975), which was drawn from expectancy value theories and cognitive processing theories, suggests that individuals act to avoid and prevent threats to their safety and security if and when they perceive that the threat is sufficiently severe and if they perceive that they are susceptible to the threat. Individuals are also likely to form perceptions about their ability to respond to the threat (self-efficacy), conduct an assessment about the effectiveness of the recommended response (response efficacy), and analyze the costs involved in performing the recommended behavior (response cost) (Bandura and Adams 1977). These two appraisals: threat appraisal and coping appraisal, form the foundation for the individual user's behavioral intention to carry out or execute the recommended response to a threat (Witte 1992, Witte

المنارة للاستشارات

www.manaraa.com

1996). A substantial amount of research studies using PMT have revealed both threat and coping appraisals to be significantly correlated with behavioral intention. However, coping appraisal variables have been shown to have a stronger relationship with behavioral intention than threat appraisal variables (Milne et al. 2000). While PMT suggests that the threat and coping appraisals may occur concurrently, theories such as Extended Parallel Process Model (EPPM) suggest that threat appraisals occur prior to coping appraisals. Johnston and Warkentin (2010) utilized the view of EPPM in their study, which investigated the influence of PMT variables on behavioral intention to use anti-spyware software. This dissertation focused on the original view of PMT where threat and coping appraisals can occur simultaneously.

Previous studies have suggested that threat appraisal and coping appraisal variables, which are the foundation of the Protection Motivation Theory (PMT), influence security behavior of individuals (Ifinedo 2012; Johnston and Warkentin 2010; LaRose et al. 2008; Lee and Larsen 2009; Woon et al. 2005; Workman et al. 2008). When individuals face a threat, they are likely to adopt protective technologies to deter the threat. These protective technologies help users avoid harm from a growing number of negative technologies, such as malware (Johnston and Warkentin 2010; Lee and Larsen 2009; Liang and Xue 2010). PMT has also been utilized to investigate the impact of threat and coping appraisal on security policy compliance (Herath and Rao 2009; Ifinedo 2012; LaRose et al. 2008; Pahnila et al. 2007), backing up data (Crossler 2010; Malimage and Warkentin 2010) and risky online behavior (Marett et al. 2011) .

Protection Motivation Theory, which has been widely used in information security research, provides a highly validated theory to test the role of habit in

المنارة للاستشارات

www.manaraa.com

information security behaviors. The cognitive mediating process provides an excellent background to explore the influence of habit, since habitual behaviors reduce cognitive processing. Pahnila et al. (2007) and Vance et al. (2012) tested PMT and habit in the context of information security, but both studies failed to capture the automaticity of habit. This study investigated the role of habit in information security behaviors utilizing PMT while capturing the multidimensional and automatic nature of habit.

Role of Habit

Behavioral Theories such as the Theory of Reasoned Action (TRA) (Fishbein and Ajzen 1975) and the Theory of Planned Behavior (TPB) (Ajzen 1991) are well established theories that have provided a core foundation to most behavioral research studies across many disciplines (Conner et al. 2003; Liao et al. 2007). These theories operate under the assumption that actions are guided by a rational and intentional decision-making process. However, these underlying theories do not address that, over time, habitual patterns are developed when certain behaviors are repeated successfully in a stable context. These formed habits will decrease the role of rationality and intentionality of the decision making process, therefore, theories such as TRA and TPB do not provide the best theoretical foundation for the study of behaviors, which are already habituated (Guinea and Markus 2009).

Triandis (1977), who was one of the first scholars to integrate habit into behavioral research, states that habit and intentions are at the opposite ends of a continuum, where the more habitual an action becomes, the less intentional it would be. However, the true meaning of habit has been a topic of much debate among researchers. There are clearly two definitions of habit. One group of researchers argue that habits are

المنارة للاستشارات
www.manaraa.com

equal to the frequency of past behavior (Bagozzi and Warshaw 1990; Bagozzi 1981; Beck and Ajzen 1991; Landis et al. 1978; Quine and Rubin 1997; Tuorila and Pangborn 1988). Under this definition, any behavior when performed frequently would become a habit. Another group of researchers asserts that while frequency is a component of habit formation, frequency itself does not constitute habit. They state that habit is a form of goal-oriented automaticity (Aarts and Dijksterhuis 2000; Bargh and Ferguson 2000; Neal et al. 2011; Sheeran et al. 2005; Verplanken and Orbell 2003; Wood and Neal 2007). This dissertation followed the view that habitual behaviors are performed automatically and defines habit as "learned sequences of acts that become automatic responses to specific situations, which may be functional in obtaining certain goals or end states" (Verplanken et al. 1997, p. 540). The automaticity aspect of habit is multidimensional and consists of dimensions such as lack of awareness, uncontrollability and mental efficiency.

The power of habit has been utilized by many organizations to foster positive habits and to break negative habits of their employees. Several organizations such as Starbucks have developed training programs to instill positive habits in their employees, which has resulted in great success (Simon 2011). Companies such as Proctor and Gamble have taken advantage of consumers' habitual urges to create highly profitable products like Febreze (Bittar 2000). Non-profit organizations such as Alcoholics Anonymous have used the power of habit to reform lives by breaking habits that lead to alcoholism and providing individuals with alternative positive habits.

Technology adoption models such as the Technology Acceptance Model (TAM) (Davis 1989) and the Unified Theory of Acceptance and Use of Technology (UTAUT) (Venkatesh et al. 2003) were based on TRA, which assumes that individuals only

المنارة للاستشارات
www.manaraa.com

perform behaviors after a formal decision-making process. When a routine or repetitive task needs to be performed, this formal decision making process may not be beneficial since there is no need to weigh costs and benefits of the same action (Guinea and Markus 2009). Kim and Malhotra (2005) and Venkatesh et al. (2000) suggests that over time, the decision-making process and intentions change and that the influence of intentions on behavior decreases. When habits are formed, the predictive power of behavioral intention reduces and over time habit becomes the main driver of actual behavior while suppressing the intention-behavior relationship. While habit has been modeled as a mediator and a direct effect on behavior, Limayem et al. (2007) posits that the automatic aspect of habits can only be captured by including habit as a moderator of the intention-behavior relationship. The moderating effect of habit was initially suggested by James (1890) and received support from several other researchers (Landis et al. 1978; Montano and Taplin 1991; Ronis et al. 1989). Aarts et al. (1998) suggests that individuals do not consume cognitive resources when performing a habitual behavior and therefore, TRA and TPB may not be applicable in situations where habitual behaviors are performed. Figure 1.2 illustrates the operationalization of habit as a moderator.

المنارة للاستشارات
www.manaraa.com

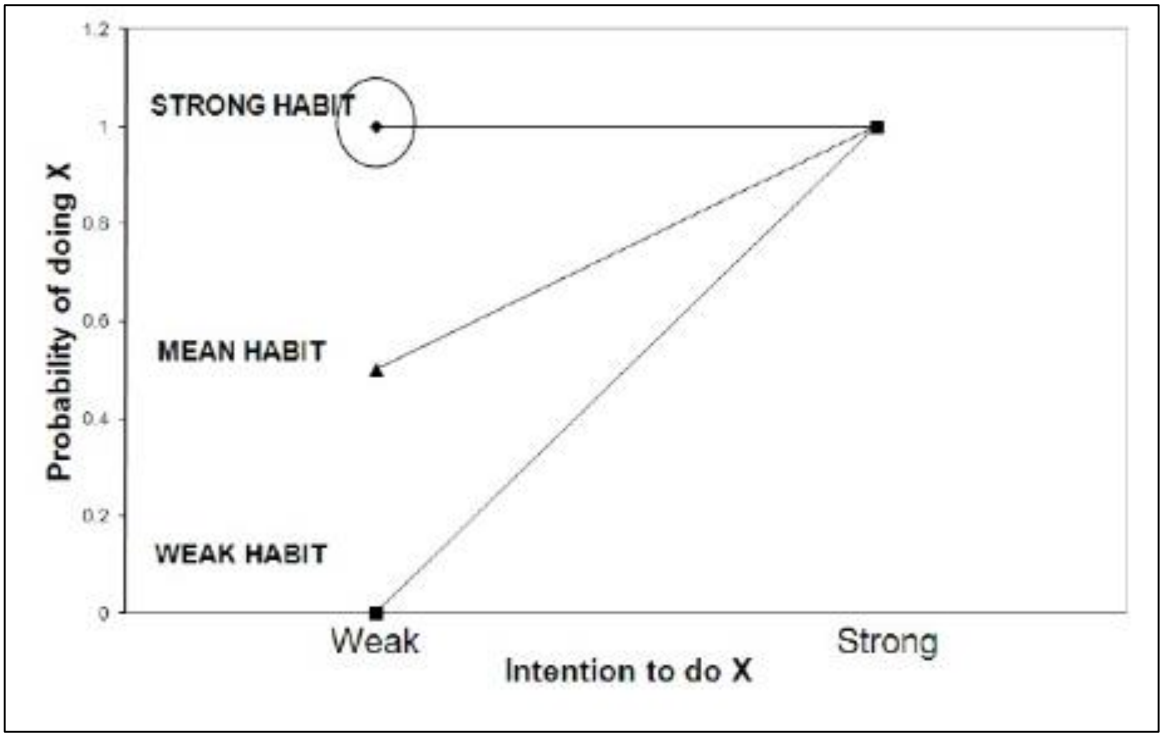


Figure 1.2 Habit as a Moderator (Sood 2012)

Theorizing habit as a moderator is suggested as the best way to capture the automaticity nature of habitual behaviors. However, scholars have found empirical evidence that habit and intention are independent constructs, which predict actual behavior in the contexts of blood donation, seatbelt usage and food consumption (Charng et al. 1988; Mittal 1988; Tuorila and Pangborn 1988). Limayem et al. (2007) also found habit to have a significant direct influence on actual behavior. These findings suggest that habit exhibits a moderating influence on the intention-behavior relationship and also acts as a direct influence on actual behavior.

Habit has been investigated heavily in social psychology using both the frequency of past behavior and automaticity views. With more than 40 percent of daily behaviors

www.manaraa.com

performed by an individual being habitual (Duhigg 2012; Neal et al. 2006), and information systems being used heavily on a daily basis, it stands to reason that habit plays an important role in behaviors related to information systems. Habits have been shown to influence our daily behaviors related to sending emails, online shopping, web browsing, smartphone usage and using information systems in general (Oulasvirta et al. 2012). Given the applicability of habit to IS related behaviors, it is surprising that only a few researchers have investigated the role of habit in IS research.

Table 1.1 Recent Empirical IS Research Investigating Habit

Study	Behavioral Context
Cheung and Limayem (2005)	Student use of Blackboard
Chiu et al. (2012)	Online purchaces
Gefen (2003)	Online CD/book vendors
Khalifa & Liu (2007)	Online shopping
Khalifa et al. (2002)	Online grocery shopping
Kim and Malhotra (2005)	Web based information system
Limayem and Cheung (2011)	Student use of Blackboard
Limayem and Hirt (2003)	Student use of WebBoard
Limayem et al. (2001)	Student use of WebBoard
Limayem et al. (2007)	World Wide Web
Pahnila et al. (2007)	Security policy compliance
Polites and Karahanna (2012)	Student use of GoogleDocs
Siponen et al. (2010)	Security policy compliance (qualitative)
Vance et al. (2012)	Security policy compliance
Wu and Kuo (2008)	Google searches
Ye and Potter (2011)	Student use of web browsers

Reflecting on that void in IS research, Benbasat and Barki (2007) called for scholars to consider investigating the role of habit in information systems. Scholars in the IS continuance and discontinuance area have utilized habit in their research to a certain degree since it is highly applicable. There has been an increase in the number of IS

المنارة للاستشارات
www.manaraa.com

articles exploring the influence of habit, which is highlighted by the Unified Theory of Acceptance and Use of Technology (UTAUT) 2 model integrating habit as one of the exogenous variables (Venkatesh et al. 2012). Table 1.1 lists some recent research in IS that has utilized habit as a construct in their investigations.

Extant research in IS that has utilized habit is scarce, which is baffling given the applicability of habits in routine usage of information systems by individuals. Even more surprisingly, there have been only a few studies to our knowledge where habit was investigated in the context of information security. Several information security research studies have identified habit to be a key factor in secure behaviors. Some of the secure behaviors identified to be habitual in these studies were password creation and usage (Bellman et al. 1999; Farn et al. 2004; Florencio and Herley 2007; Herath and Rao 2009; Morris and Thompson 1979; Yang and Shieh 1999), data backup (Chunli and Donghui 2012; Dunnavant and Childress 2010; S.B.Thorat et al. 2010; Spennemann and Atkinson 2002), locking or logging off computer terminal when leaving them unattended (Morgan et al. 2007; Siponen et al. 2010), clicking web links or visiting websites (Chen and Halsey 2009; Frøkjær and Hornbæk 2002) and behaviors related to emailing such as reviewing the addresses of recipients before sending email (Etchells 2008; Vandermeer 2006) and exercising care when opening email attachments (Ng et al. 2009). Other information security studies have identified habit as a possible antecedent to actual behavior and have suggested scholars investigate the influence of habit on secure behaviors in the future (Anderson and Agarwal 2010; Herath and Rao 2009).

Although many information security studies have identified habit as a key factor, only a few research studies have actually tested habit in an information security context.

المنارة للاستشارات
www.manaraa.com

Pahnila et al. (2007) modeled habit and other variables related to PMT and Deterrence Theory to investigate security policy compliance. They hypothesized that habit has a direct influence of behavioral intentions to comply with security policies. Siponen et al. (2010) followed a qualitative approach to test the influence of habit on security related behaviors such as secure use of the internet, writing down passwords and locking one's PC. Vance et al. (2012) used scenarios to test the influence of habit in the presence of PMT. They hypothesized that threat and coping appraisal mediated the relationship between habit and policy compliance intention. Pahnila et al. (2007) and Vance et al. (2012) found empirical evidence to support their hypotheses related to habit, utilizing the cognitive mediating process to mediate the relationship between habit and intention (Vance et al. 2012) and modeling habit as a direct influence of behavioral intentions (Pahnila et al. 2007). However, these investigations are in contrast to the automaticity nature of habit and follow the notion that habits are equal to frequency of past behavior.

Information security behaviors are performed routinely, on a repetitive basis in stable contexts by employees at the workplace. Over time these behaviors can become habitual. Several information security research studies have identified that habit is a key factor in secure behaviors. However, only a few studies that investigated the role of habit in information security behaviors and those studies do not capture the automatic aspect of habit. This study attempted to fill this research gap by developing a research model to explore the role of habit in information security behaviors with a focus on the automaticity view of habit.

المنارة للاستشارات

www.manaraa.com

Conceptual Research Model

This study proposed a research model to test the influence of the threat appraisal process and coping appraisal on behavioral intentions and to test the role of habit in moderating the intention-behavior relationship. Technology Threat Avoidance Theory (TTAT), Protection Motivation Theory (PMT) and Habit Theory provide the theoretical basis for the research model. The main research model for this study is shown on Figure 1.3.

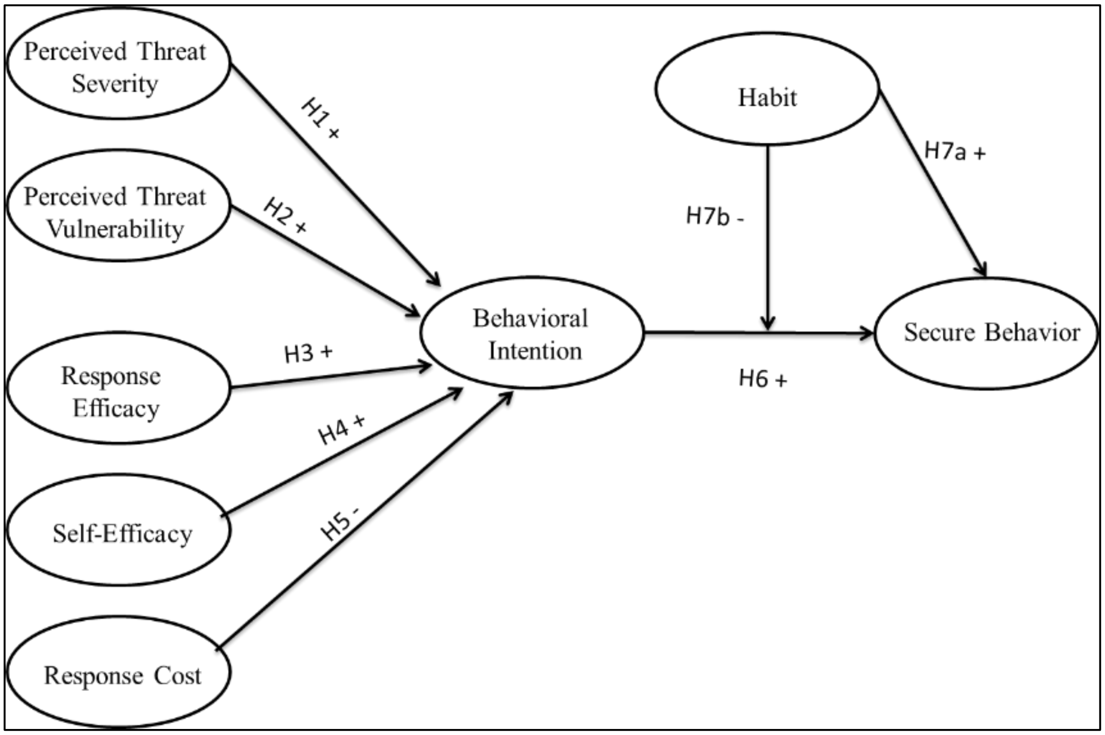


Figure 1.3 Conceptual Research Model

It was hypothesized that perceived threat severity and vulnerability will positively influence intention to perform a secure behavior. Coping appraisal variables, response efficacy and self-efficacy were hypothesized to positively influence intentions while

www.manaraa.com

response cost was hypothesized to negatively influence intentions. Behavioral intentions were hypothesized to influence actual behavior. Habit was hypothesized to directly influence behavior while negatively moderating the intention-behavior relationship. The suppressing effect of habit on relationship between intention and behavior was explored by Limayem and Hirt (2003) and Limayem et al. (2007) in the context of IS continuance. This study investigated the suppressing relationship in the context of information security with the presence of threat and coping appraisal variables.

Research Objectives

The primary purpose of this study was to explore the role of habit in information security behaviors while capturing the automatic nature of habit. With the increasing severity and frequency of information security threats, a single incident can jeopardize the security of a whole organization. Therefore, identifying the role of habit in the performance of information security behaviors by employees at the workplace is critical. There have been only a few studies in the information security domain that utilized habit as a construct to predict secure behaviors or intentions to perform secure behaviors. This present study filled this research gap by developing a comprehensive research model that can be applied in the information security context to test the role of habit in information security behaviors in the workplace.

In order to confirm that the research model presented in this study is appropriate, comparisons of the path coefficients and variance explained are conducted with several other alternative models that investigate PMT and habit. Research models positioning habit as an indirect effect (Vance et al. 2012), direct effect on intentions (Gefen 2003),

المنارة للاستشارات
www.manaraa.com

and direct effect of behavior (Limayem et al. 2007) were analyzed and compared with the proposed conceptual model of this study.

Research Methods

The initial challenge of this present study was to identify which information security behaviors were habitual. Due to the lack of prior research in information security that utilized habits, a rigorous process had to be followed to identify behaviors that are habitual. As mentioned previously, habitual behaviors can be positive or negative. For the purposes of this study, only positive habits related to information security were considered. After compiling a list of forty-nine positive secure behaviors, a subject-matter expert panel was convened to identify which of those behaviors their employees performed habitually. An employee panel was also convened to identify which of those behaviors they performed habitually. The responses were compiled and members of a measurement panel were requested to identify three behaviors that the panelists identified as habitual, but still were practical to be measured through an online survey.

Three online survey instruments were developed for the three distinct behaviors and the content validity was assessed by a panel of instrument experts. After several rounds of modifications, the panel agreed on the content validity of the instrument. The surveys were hosted on Qualtrics and respondents randomly received one of the three surveys that tested a secure behavior. A pilot test was conducted using the same respondent pool that was utilized for the full scale study. Pilot study data were analyzed for the construct validity and reliability and after some required refinements were conducted, the full-scale study was deployed. The sampling frame for the pilot test and the full scale study was corporate employees across a diverse range of industries.

المنارة للاستشارات

www.manaraa.com

Although many research studies use students as their respondents, for the purposes of this study and to measure the role of habit, a corporate sampling frame was deemed more appropriate due to generalizability and realism (Compeau et al. 2012). Structural Equation Modeling (SEM) techniques were used to analyze the data collected from the full-scale study.

Significance of the study

The findings of this present study contribute to research as well as practitioners. The findings are expected to empirically confirm the role of habit has a key factor in information security behaviors as identified by prior information security research. While extending the findings of prior research that investigated habit and PMT, this study captured the true nature of habit: automaticity. Prior information security research utilizing PMT has suggested that threat and coping appraisals significant influence behavioral intention. The findings of this study indicate that while the PMT variable exert their influence on behavioral intentions, when habit is present, the influence of behavioral intentions on the performance of actual behavior reduces. This in-turn reduces the influence of the PMT variables on actual behavior.

For organizations, the findings mean that they should strive to ensure that their employees form habits to perform secure behaviors, which are critical to the security of the organization. When a certain behavior becomes habitual, it is less likely that the employees will forget to perform that behavior since the behaviors are automatically triggered. With information security, it requires only a single incident to compromise security, thus habitual performance of secure behaviors such as locking the computer whenever it is left unattended would reap great benefits to organizations.

المنارة للاستشارات

www.manaraa.com

Organization

This dissertation proposal is comprised of five chapters. The first chapter provides a brief introduction and an overview about this dissertation. Chapter II provides a detailed literature review on TTAT, PMT and habit, resulting in the development of the conceptual model and hypotheses. Chapter III presents a detailed description of the research method that was employed for this dissertation study. Chapter IV presents the results of the data analyses and Chapter V concludes the study with a discussion of the findings, theoretical and practical implications and a presentation of the limitations and suggestions for future research.

المنارة للاستشارات
www.manaraa.com

CHAPTER II

LITERATURE REVIEW

The purpose of this chapter is to review the extant literature regarding the primary theories addressed in this study and to articulate the formation of the research model along with the hypotheses. First, the background literature on threat avoidance is reviewed along with the Technology Threat Avoidance Theory (TTAT). Next, Protection Motivation Theory (PMT) and the extant literature utilizing PMT in information systems (IS) research are reviewed. Habit is defined, followed by explorations of the formation of habit and extant literature that apply habit in psychology and IS. After the background on current habit research, how habit can be applied in IS security research is presented. The research model is then discussed in detail along with the constructs that are tested in the model. Finally, paths from the independent variables to the dependent variables and the moderating relationships are theoretically justified and the associated hypotheses are defined.

Threat Avoidance

Psychology research on human behavior has provided ample evidence that humans' motivational foundation is to seek pleasure and avoid pain. Some of the prolific researchers and founders of behavioral psychology such as Sigmund Freud and William James have agreed with the notion that human behavior revolves around setting goals to

المنارة للاستشارات

www.manaraa.com

achieve positive outcomes and distance themselves from negative outcomes (Freud 1915; James 1890). Behavioral theories, based on reinforcement, assert that when humans receive rewards or satisfaction after performing a certain behavior they are more likely to repeat the same or similar behavior while punishments or unsatisfactory behavior will reduce the chances of that behavior being repeated. A threat can be identified as a negative outcome which humans would typically try to avoid. Threats faced by humans can be of different forms in contexts such as health-related issues, natural disasters, terrorism and information technology. Whatever the threat may be, individuals are likely to take action to deter the threat if and when they perceive it (Witte 1992).

Cybernetic Theory, which was created by Wiener (1948), asserts that humans self-regulate their behaviors through feedback loops. These feedback loops are also called cybernetic loops. There are two feedback loops presented in the cybernetic theory: positive feedback loops and negative feedback loops.

المنارة للاستشارات
www.manaraa.com

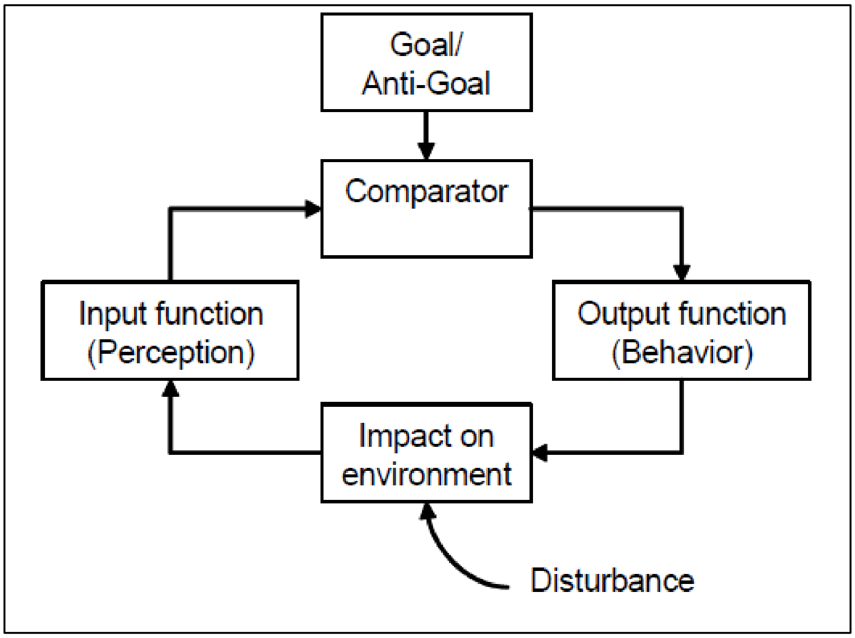


Figure 2.1 Cybernetic Loop (Liang and Xue 2009)

The cybernetic loop, which may be positive or negative, is activated by a disturbance in the environment, which will be captured by the input function and perceptions created. The cybernetic loop is presented in Figure 2.1. The comparator in the cybernetic loop compares the present state, as signaled by the input function, with the values set by the goal or anti-goal. This is called a positive feedback loop or a positive cybernetic loop. In a negative feedback loop or negative cybernetic loop, if the comparator finds the values between the goal and present state are different, the output function activates a behavior in order to reduce the difference. This behavior will impact the environment changing the present state and it will then be sent to the comparator by the input function to decide whether the behavior needs to continue. This process functions as a negative feedback loop since it "functions to decrease the discrepancy between the present state and the desired end state" (Liang and Xue 2009, p.74).

المنارة للاستشارات
www.manaraa.com

Technology acceptance theories such as the Technology Acceptance Model (TAM) (Davis 1989) operate under the assumption that human behaviors are goal directed and that through cognitive processes they chose the behavior that results in the best outcome. However, the technology acceptance theories explain only the link between the comparator and the output function. These theories ignore the reasons why the goal was initially formed and does not even test the actual goal of the individual.

The positive feedback loop is applicable to assess humans' propensity to avoid threats since it describes how individuals may try to increase the discrepancy between the present state and the anti-goal. When the comparator finds that a present value is too close to the undesired goal, the output function activates a behavior that continues until "the discrepancy is sufficiently large" (Carver and Scheier 1982; Liang and Xue 2009, p.77). The positive feedback loop can be utilized to describe the phenomena of how individuals behave to avoid certain threats. In the IS security context, this loop explains how individuals may avoid security threats such as computer viruses, spyware and data loss by following a recommended response or by simply ignoring the threat. For example, losing data may be the anti-goal or occurrence that an individual wants to prevent. When the threat of data loss is perceived by the input function through a disturbance in the environment, such as witnessing the computer behaving abnormally or hearing about a colleague losing data, the comparator may find that the current state is in close proximity to the anti-goal. The output function moves the current state away from the anti-goal by activating avoidance behavior, such as backing up your data. Cybernetic theory was used as a foundation by Liang and Xue (2009) to develop the Technology

المنارة للاستشارات
www.manaraa.com

Threat Avoidance Theory (TTAT), which explains individual behavior of avoiding certain IS Security threats.

Technology Threat Avoidance Theory

With the number of information technology threats such as viruses and spyware increasing on a daily basis, individuals as well as organizations are likely to experience at least some of these threats at some point. In order to deter these threats lurking in any IT environment, evasive actions need to be taken by end users. According to the Technology Threat Avoidance Theory (TTAT), users go through two cognitive processes: threat appraisal to evaluate threats and coping appraisal to decide how to cope with those threats (Liang and Xue 2009). Based on the theories rooted in the psychology discipline that suggest humans seek pleasure and avoid pain, TTAT posits that approach behavior, which is represented by the negative feedback loop in cybernetic theory is different from threat avoidance behavior. Neurological research also supports this position by identifying that the left prefrontal cortex is associated with approach behavior while the right prefrontal cortex is associated with avoidance behavior (Louis and Sutton 1991; Sutton and Davidson 1997). It is important to note that acceptance and avoidance are cognitive processes that involve decision making, utilizing the prefrontal cortex of the brain. Thus, when a certain behavior is learned or becomes habitual, the decision making that was conducted in the prefrontal cortex part of the brain will cease, and a part of the brain which is responsible for routine and automatic behavior, basal ganglia, will take precedence (Ashby et al. 2010). The latter part of this chapter will discuss how a successful repetition of a similar behavioral feedback loop may result in habitual behavior, which is automatic and unconscious.

المنارة للاستشارات

www.manaraa.com

The process view of TTAT, while stating that threat and coping appraisals are significant parts of the threat avoidance process, asserts that threat perception activates the coping appraisal. This implies that the threat appraisal occurs before coping appraisal. As it is illustrated in Figure 2.2, once the environment changes with the emergence of malicious IT, threat perceptions are created. These threat perceptions depend on the perceived probability of the threat's occurrence and the perceived severity of the consequences if the threat was to occur. Threat appraisal evaluates the threat and activates coping appraisal where the user analyzes which options are available to deter the threat before deciding on the behavior to avoid the threat. Therefore, if an individual perceives no threat, there will be no requirement for the analysis of coping mechanisms or behavior to cope with a threat. However, the variance view of TTAT, which describes the threat avoidance process in a cross-sectional manner, utilizes the original approach taken by (Maddux and Rogers 1983) where threat and coping appraisals may occur concurrently.

Once an individual perceives a threat and analyzes the different options available to cope with the threat, actual coping behavior takes place as a form of problem-focused coping or emotion-based coping. In problem based coping, an individual moves away from the anti-goal by performing a behavior that deals directly with threats, such as installing anti-virus, installing anti-spyware software or backing up data. In emotion-focused coping, individuals "create a false perception of the environment without actually changing it" (Liang and Xue 2009, p.78), which reduces the threat perceptions or motivation of coping without actually changing the present state. Some emotion-focused coping may include belief that God will remove the danger (religious faith), acceptance

المنارة للاستشارات

www.manaraa.com

of a threat or a risky situation (fatalism), denial of the presence of the threat, or self-blame for not being able to control the threat (Rippetoe and Rogers 1987). Individuals are likely to select only one of the coping methods for most situations, but high threat situations may influence individuals to select both types of coping methods.

In the process view of TTAT, Liang and Xue (2009) presents several propositions. In proposition 1 (P1), they propose that once users become aware of a certain threat in the environment, they would perform avoidance behavior to distance themselves from the anti-goal or the undesired end state. In proposition 2 (P2), it is proposed that individuals need to appraise the threat before they assess available behavioral options to cope with the threat. This is consistent with the Extended Parallel Process Model (EPPM), where threat perception is a necessary condition for individuals to keep methods to cope with the threats. Proposition 3 (P3) suggests that individuals may perform problem-focused or emotion-focused coping to reduce a threat that they perceive. Individuals may evaluate several options available to avert the perceived threat before selecting one of the options in problem-focused coping (P3a). Emotion-based coping (P3b) creates a false perception of the environment without changing the reality. However, the process view of TTAT fails to identify that once a coping mechanism or secure behavior is repeated successfully, over time a habit loop may be created, which bypasses the feedback loops until there is a change in the environment or the anti-goal.

المنارة للاستشارات
www.manaraa.com

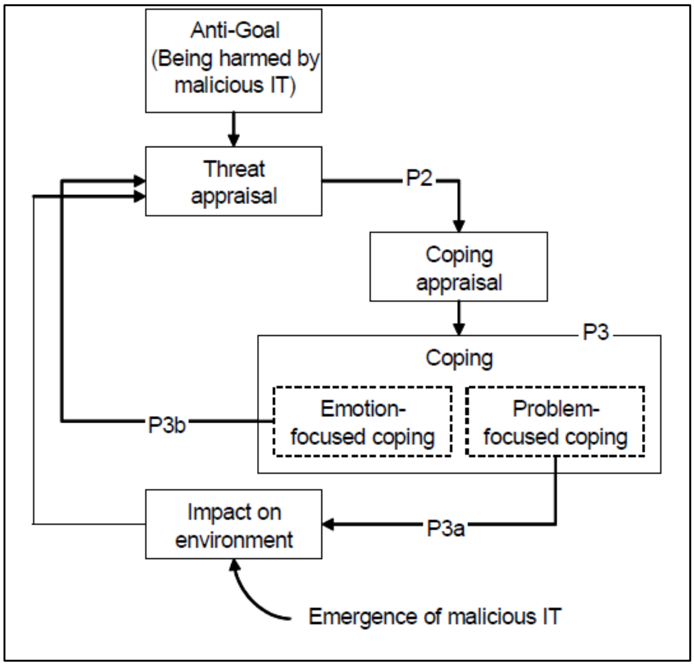


Figure 2.2 Process of IT Threat Avoidance (Liang and Xue 2009)

Liang and Xue (2010) utilized TTAT on a variance model where they hypothesized that perceived threat and perceived avoidability will positively influence avoidance motivation and that avoidance motivation will positively influence avoidance behavior. They found empirical evidence to validate their research model, which was derived from TTAT, with all but one of their hypotheses being supported. Their findings are largely consistent with the Protection Motivation Theory where individual's threat appraisal and coping appraisals lead to protective behaviors or recommended responses.

Although tested as a variance model, their paper utilizing TTAT provides valuable insight into how behavioral feed-back loops work in the context of threat avoidance. However, consistent with similar studies, their study did not take into account that when the feed-back loop is repeated many times in a stable context, coping behavior

المنارة للاستشارات
www.manaraa.com

may become habitual by creating a habit loop instead of the positive feedback loop. The habit loop will be initiated by a trigger, followed by the actual coping behavior before approaching the rewards stage. TTAT along with habit provide a theoretical foundation for this study.

Protection Motivation Theory

Protection Motivation Theory was originally developed by Rogers (1975) to demonstrate how fear appeals affect health attitudes and behaviors. Fear appeals are defined as “persuasive messages designed to scare people by describing the terrible things that will happen to them if they do not do what the message recommends” (Witte 1992, p. 329). A successful fear appeal will heighten the awareness of a threat by increasing the threat severity and vulnerability levels of an individual and by increasing the coping appraisal to the recommended response. A plethora of research studies have found that fear-arousing messages contribute to the increased acceptance of recommended response or secure behavior (Sutton 1982). As identified by the fear appeals theory (Johnston and Warkentin 2010; Witte 1992), certain adaptive responses can be associated with certain threats. Table 2.1 illustrates threat-response pairs related to health-awareness campaigns and IS security in organizations. Crossler and Belanger (2012) posit that although a threat is usually associated with a single recommended response, individuals may perform alternative responses to avert a threat.

Perceived threat vulnerability, perceived threat severity and response efficacy were identified as the main components of PMT by Rogers (1975), while self-efficacy was included as a core component of PMT at a later stage (Maddux and Rogers 1983; Rogers 1983). PMT suggests that once an individual receives information about a threat,

www.manaraa.com

a cognitive mediation process causes that individual to evaluate the threat. If the individual perceives that the threat is sufficiently severe and that he or she is susceptible to the threat, he or she will act to avoid or prevent the threat (Rogers 1975).

Table 2.1 Threat-Response Pairs

Threat	**Recommended Response**	**Source**
Health-related		
Injury due to a Car Crash	Wear seat belts	(Schwarzer et al. 2007)
Lung cancer/smoke related death	Smoking cessation	(Rogers 1975)
HIV infection	Condom usage	(Abraham et al. 1994)
IS Security Related		
Loss of Data	Backing up data Changing password Keeping software updated Set up user access controls	(Crossler and Belanger 2012; Crossler 2010; Malimage and Warkentin 2010)
Computer Virus Infection	Anti-Virus software usage	(Ng et al. 2009)
Spyware Infection	Anti-Spyware software usage	(Johnston and Warkentin 2010)
Unauthorized access to user account	Changing password frequently	(Zhang and McDowell 2009)
Corporate data breach	Encrypting corporate data	(Vance et al. 2012)
Unauthorized use of user credentials	Locking the computer	(Vance et al. 2012)

In addition to the cognitive appraisal of threat severity and threat susceptibility, individuals also form perceptions of the recommended response to the threat by assessing their own individual capabilities (self-efficacy), coupled with an assessment of the effectiveness of the response (response efficacy) (Bandura 1977; Witte 1992; Witte et al. 1996). Individuals also assess the cost related to performing a selected coping behavior (response cost). Response costs can be in the form of time, money and/or effort expended while performing the adaptive coping behavior (Floyd et al. 2000). PMT

المنارة للاستشارات

www.manaraa.com

consists of two cognitive mediating processes; threat appraisal and coping appraisal. The threat appraisal process consists of perceived threat vulnerability and perceived threat severity while the coping appraisal process consists of response efficacy, self-efficacy and response costs. The perceptions created in the threat appraisal and coping appraisal processes will increase the likelihood of an individual performing a recommended response (Floyd et al. 2000). Figure 2.3 demonstrates the cognitive mediating processes of PMT.

When an individual perceives a threat, he or she may accept the recommended response (adaptive coping) or choose to ignore the threat or react negatively (maladaptive coping). Adaptive coping results from an individual perceiving an average threat or fear appeal. Maladaptive coping results from a very high or very low threat perception or fear appeal, where an individual may ignore the threat or perform a behavior, which is the opposite of the recommended response. Therefore, the relationship between threat perception or fear and motivation to carry out the recommended response is suggested to have an inverted U-shaped relationship (Janis 1967).

المنارة للاستشارات
www.manaraa.com

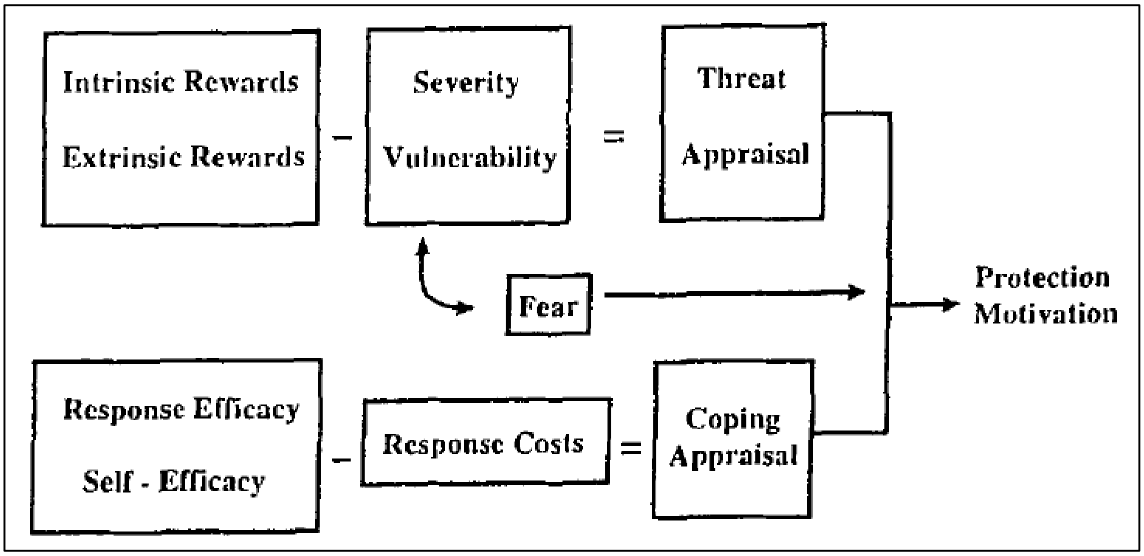


Figure 2.3 PMT Cognitive Mediating Process (Floyd et al. 2000)

PMT has been widely used in health research domains such as smoking cessation, sunscreen usage, moderate alcohol consumption and dietary improvements and the four primary variables have been found to be significantly correlated with the behavioral intention. According to a meta-analysis of extant PMT studies, coping appraisal variables were strongly related to behavioral intention and behavior of the adaptive response compared to threat appraisal variables (Floyd et al. 2000; Milne et al. 2000). Response cost has only been utilized as a PMT variable in the research models on a limited number of studies (Vance et al. 2012). This may be due to validity or reliability issues or simply because it was not applicable to the context of those studies in question. For this present study, response cost is included as a PMT variable in the research model as secure behaviors may involve a degree of cost to the individual performing them.

PMT has provided the foundation to several behavioral information security research studies conducted in different contexts to explain how individuals are motivated

المنارة للاستشارات
www.manaraa.com

in response to perceptions of certain threats. The different contexts and different adaptations of PMT in these studies have yielded contrasting findings. Woon et al. (2005) used PMT to find factors that influenced home users' behavior to protect their wireless networks. They found that all the PMT variables except perceived vulnerability had a significant impact on the probability of an individual enabling security in their wireless network. Lee and Larsen (2009) utilized PMT to investigate factors effecting small and medium sized business executives' decision to adopt anti-malware software for organizations. Their findings indicated that threat severity had the strongest impact on the executives' intention to adopt anti-malware software. Herath and Rao (2009) hypothesized that PMT variables had a direct effect on attitudes, which then had a direct effect on behavioral intention to comply with security policies. Their findings indicate that the perceived severity of a security breach was significantly related to security breach concern level.

Johnston and Warkentin (2010) employed PMT along with the Extended Parallel Process Model (EPPM) where they hypothesized threat appraisal to directly affect coping appraisal and the coping appraisal to directly affect behavioral intention to adopt anti-spyware when faced with the threat of spyware. Their Fear Appeals Model (FAM) indicated that perceived threat severity significantly influenced response efficacy when fear appeals were provided. They also found that response efficacy and self-efficacy significantly influenced individuals' intentions to use anti-spyware software. Liang and Xue (2010) utilized PMT to test a variance model of TTAT also utilized the threat of spyware in their study. They hypothesized that while threat and coping appraisal had a direct influence on behavioral intention (motivation), an interaction effect between

المنارة للاستشارات
www.manaraa.com

perceived threat and response efficacy constructs. Their data showed significant relationships in all of their hypothesized relationships except the interaction effect of threat severity and vulnerability on perceived threat.

Lee (2011) investigated the factors effecting the adoption of anti-plagiarism software by university faculty with PMT variables. He found that threat appraisals had a stronger influence on anti-plagiarism software adoption by faculty members than coping appraisal. Moral obligation was also found to be a factor that influenced the adoption of the software while social influence did not have a significant effect. Marett et al. (2011) investigated the risky online behavior of internet users using PMT and fear appeals. They found that PMT explained both adaptive and maladaptive responses. Ng et al. (2009) investigated the influence of threat and coping appraisals on email related security behavior and found that perceived severity moderated the effects of self-efficacy on secure behavior. A list of recent research studies that applied PMT in information security contexts are presented in Table 2.2.

Use of behavioral intentions as the ultimate dependent variable has been criticized as incomplete (Lee 2011), but measuring actual secure behavior is very challenging and in most cases impossible (Crossler et al. 2013; Warkentin et al. 2012). Due to these challenges, behavioral security researchers have measured actual secure behavior through self-reports. Even though significant limitations exist in self-reported actual behavior, it provides researchers the ability to test the intention-behavior relationship in secure behaviors and test the direct impacts of PMT variables on actual behavior. Only a very few research studies have collected actual secure behavior through computer logs that

المنارة للاستشارات
www.manaraa.com

reflected behaviors such as password changes, security patch updates, backups and software usage (Lee 2011; Workman et al. 2008).

Table 2.2 InfoSec PMT Empirical Studies and Contexts

Study	Context	Ultimate DV	Int-Behavior relationship	Self-reported Actual Behavior
Anderson & Agarwal (2010)	Security related behavior	Intention	N/A	N/A
Crossler (2010)	Backing up data	Behavior	No	Yes
Gurung et al. (2009)	Anti-spyware usage	Behavior	No	Yes
Herath & Rao (2009)	Security policy compliance	Intention	N/A	N/A
Ifinedo (2012)	Security policy compliance	Intention	N/A	N/A
Johnston & Warkentin (2010)	Anti-spyware usage	Intention	N/A	N/A
LaRose et al. (2008)	Security policy compliance	Intention	N/A	N/A
Lee & Larsen (2009)	Anti-spyware adoption	Behavior	Yes	Yes
Lee (2011)	Anti-plagarism tool adoption	Behavior	Yes	No
Liang & Xue (2010)	Anti-spyware usage	Behavior	Yes	Yes
Malimage & Warkentin (2010)	Backing up data	Intention	N/A	N/A
Marett et al. (2011)	Risky online behavior	Intention	N/A	N/A
Ng et al. (2009)	Opening Email attachments	Behavior	No	Yes
Pahnila et al. (2007)	Security policy compliance	Behavior	Yes	Yes
Vance et al. (2012)	Security policy compliance	Intention	N/A	N/A
Woon et al. (2005)	Wireless security enabling	Behavior	No	Yes
Workman et al. (2008)	Secure computing practices	Behavior	No	Yes with actual

It is important to note that behavioral intentions change over time (e.g., through repetition) and may not be the driving factor of actual behavior (Guinea and Markus 2009). Several other variables may directly impact actual behavior and other variables such as habit may negatively moderate the intention-behavior relationship of PMT constructs. Most of the extant information security literature that investigate factors influencing secure behaviors, do not take into account that these behaviors may have

www.manaraa.com

already been habituated. Measuring the factors that influence secure behaviors without considering the influence of habit would have serious repercussions to the findings of these studies. This study attempted to address that gap by investigating the role of habits in information security behaviors and how habits moderate the intention-behavior relationship in a PMT model.

Concept of Habit

Recent behavioral research has made significant progress in our understanding and prediction of the initiation of human behaviors by applying theories such as Theory of Reasoned Action (TRA) (Fishbein and Ajzen 1975) and Theory of Planned Behavior (TPB) (Ajzen 1991). Both theories focus on actions guided by an intentional decision making process. Although TRA, TPB, and other theories that explain human decision making have been heavily utilized, validated, and proven their strengths in predicting behavior across many disciplines and in many paradigms, they are weak in one aspect. They lack the concept of repeated actions and habitual patterns of humans and how these habitual actions may influence behavior.

The earliest investigation of habit dates back to James (1890) and Watson (1914) where they investigated instinct, which was equated to habit in a biological perspective, focusing on learned associations between stimuli and responses in the context of the repetitive behavior of animals. The concept of habit was adjusted to be used in the context of human behavior by Abelson (1981) and Schank and Abelson (1977) where they introduced the idea of cognitive schema and scripts. These scripts represent standard events or behavioral sequences, which are frequently practiced under unchanging circumstances (Polites and Karahanna 2012). Since human cognitive resources are

المنارة للاستشارات
www.manaraa.com

limited, these scripts provide useful cognitive mechanisms that can make decisions mostly automatically utilizing only a few environmental cues.

Building on the previous behavioral research on habit, where habit was conceived as learned behavior that was triggered by the environment (Dewey 1922) and consistency of behavior across time (Landis et al. 1978), Triandis (1977, 1980) was one of the first to integrate habit into his research model. Triandis states that habit and intention are at the opposite end of a continuum where the more habitual an action becomes, the less intentional it is. He also stated the possibility that in extreme situations, an action is determined only by habit on one end and only by intention on the other. It is important to note the significance of habit in human behavior when trying to integrate it into behavioral research models. According to William James (1899), "all our life, so far as it has definite form, is but a mass of habits." James further states that about 99 percent of what we do each day are habitual, which may be somewhat extreme. Recent scholarly research suggests that more than 40 percent of the actions people performed each day are habitual in nature, which did not consist of a formal decision making process (Duhigg 2012; Neal et al. 2006). Thus, habit is an important factor to consider whenever behavioral research is conducted.

Definition of Habit

The true definition of habit has been a topic of much debate for decades among scholars, which has also resulted in researchers viewing habit from different theoretical lenses. There has been a general consensus that habit is a learned sequence related to routine behavior and that habit provides an individual the benefit of behavior while only

المنارة للاستشارات

www.manaraa.com

using a limited amount of cognitive resources. However, a debate revolves around the formation of habit, resulting in a debate on the overall definition of habit as well.

Habit was initially conceptualized as equal to the frequency of past behavior and that when a certain behavior is carried out on a routine basis it was defined as the formation of habit. The notion that habit is formed when an individual performs a certain act on a repetitive basis in a stable environment was evaluated and the findings published by many scholars (Bagozzi and Warshaw 1990; Bagozzi 1981; Beck and Ajzen 1991; Landis et al. 1978; Quine and Rubin 1997; Tuorila and Pangborn 1988). However, latest developments in social psychology research view habit as a form of goal-oriented automaticity (Aarts and Dijksterhuis 2000; Bargh and Ferguson 2000; Neal et al. 2011; Sheeran et al. 2005; Verplanken and Orbell 2003; Wood and Neal 2007) . These goals are defined as “desired, or anticipated, outcomes and end states” (Aarts and Dijksterhuis 2000, p. 54) or anticipated, desired effect guiding the performance behavior (Sheeran et al. 2005). Research conducted defining habit as frequency of past behavior and automaticity are described in detail in the next section. While frequency and past behavior are critical to the formation of habit, those alone cannot constitute habit since past behavior is a construct that has no explanatory value (Ajzen and Fishbein 2000). For the purpose of this study, while recognizing that frequency of past behavior is a major predictor of habit, habit is defined as “learned sequences of acts that become automatic responses to specific situations, which may be functional in obtaining certain goals or end states” (Verplanken et al. 1997, p. 540).

المنارة للاستشارات
www.manaraa.com

Frequency of Past Behavior

The habit construct has been commonly tested through measuring the frequency of past behavior. Ouellette and Wood (1998) state that when certain behaviors occur in domains where habits can develop, frequent past performance reflects habitual patterns that are likely to predict future behavior. They conducted a meta-analysis of prior studies and found that studies, which examined behaviors performed annually or biannually did not find past behavior to be a strong predictor of future behavior even though the relationship was significant. They also indicated that studies which examined routine behaviors (performed daily or weekly) in stable contexts found past behavior to be a strong predictor of future behavior. These studies also indicated that behavioral intention was significant but did not have a strong influence. Their structural model is shown in Figure 2.4 where Panel A represents studies on behavior performed annually or biannually and Panel B represents studies on behaviors performed on a daily or weekly basis.

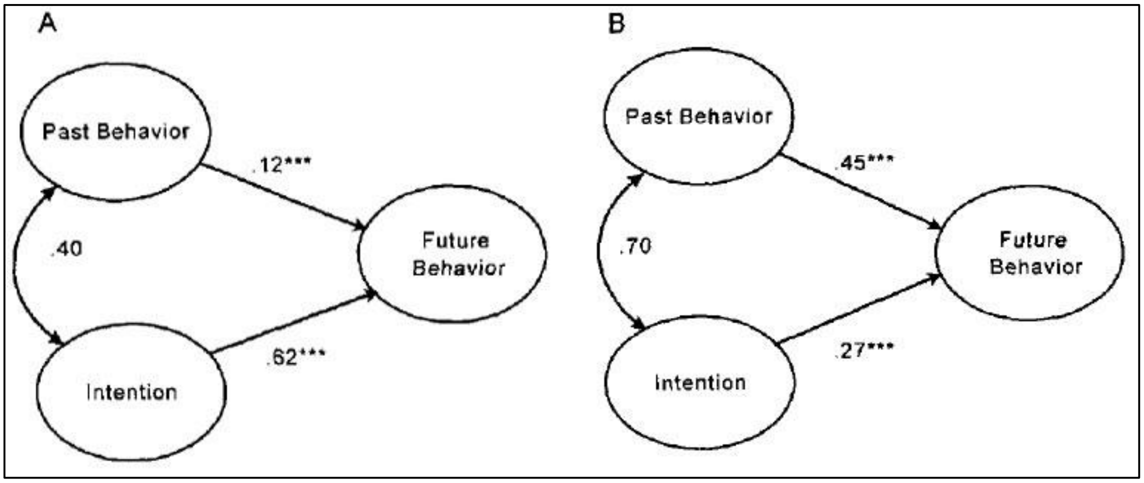


Figure 2.4 Ouellette & Wood Structural Model (Ouellette and Wood 1998)

www.manaraa.com

Past behavior and frequency of past behavior are the most frequently used methods to measure habits with the theoretical lens that for the development of habits, it requires a certain amount of repetition and practice. With the repetition of a behavior, it is "learned", thus reducing or removing the need for intentions to form for the actual behavior. For example, an email user who checks his/her email regularly each day will eventually create the habit of checking email while another user who checks email only occasionally may never create the habit of checking email and will always go through the decision making process in order to check email (Limayem et al. 2007). However, Gardner et al. (2012) suggests that once habits are formed, the habitual behavior does not need to be performed frequently. These formed habits are elicited only as frequently as a trigger is encountered. For example, an individual may have formed a habit of eating popcorn when visiting a cinema but the habit is elicited only when he/she visits the cinema.

When a behavior is performed repetitively, an individual gains adequate practice and increased familiarity with the behavior, providing that individual with the ability to perform future behavior without a significant cognitive process. Reflecting on findings of Ouellette and Wood (1998), Aarts and Dijksterhuis (2000) highlighted that the strength of habit created through repetitious past behavior is directly related to the frequency of the past behavior that was performed. Therefore, when a certain behavior such as checking email is performed on a daily basis, there is a higher likelihood to form stronger habits than a behavior performed on a weekly or monthly basis. Table 2.3 lists a summary of previous research conducted where they defined habit as past behavior or frequency of past behavior.

www.manaraa.com

Table 2.3 Prior Research on Habit With Past Behavior Dimension (Limayem et al. 2007)

Study	**Area**	**Purpose**
Ajzen (1991)	Human decision process	To review research on various aspects of the theory of planned behavior.
Bagozzi (1981)	Actual blood Donation behavior	Test attitude- behavior relation in the context of a longitudinal field study.
Bagozzi and Warshaw (1990)	Goal pursuit	To revise and extend the TPB to better explain goal pursuit.
Beck and Ajzen (1991)	Dishonest Action	Self-reports of behavior with respect to cheating on a rest, shoplifting, and lying to get out of assignments.
Bergeron et al. (1995)	Use of executive information systems (EIS)	Explore various factors related to EIS utilization.
Fredricks and Dossett (1983)	Model Comparison: Attitude-behavior relations	To compare the Fishbein-Ajzen (1975) model with the Bentler-Speckart (1979) model.
Landis et al. (1978)	Social behavior	Assess the relative impact of habit and behavioral intentions in predicting teacher behavior.
Montano and Taplin (1991)	Mammography participation	To test an expanded TRA to predict mammography participation.
Quine and Rubin (1997)	Use of hormone replacement therapy	To examine women's attitude towards the use of hormone replacement therapy and try to predict intention to use it using TPB.
Trafimow (2000)	Intention to use condoms	Study how habit relates to intentions.
Tuorila and Pangborn (1988)	Consumption of selected foods.	To compare predictions based on TRA and Triandis' model.

However, the notion that past behavior or frequency of past behavior forms habit has been criticized by several scholars (Gardner 2012; Ouellette and Wood 1998; Verplanken and Orbell 2003). They state that behavioral frequency or the number of times the past behavior was performed does not recognize the automatic nature of habit (Verplanken and Orbell 2003). While frequency and past behavior are critical to the formation of habit, those alone cannot constitute habit since past behavior is a construct

www.manaraa.com

that has no explanatory value (Ajzen and Fishbein 2000). Due to these arguments, it is recommended that studies using frequency of past behavior or past behavior as a "proxy measure of habit should be considered with caution" (Limayem et al. 2007, p. 714).

Automaticity

Latest developments in social psychology research views habit as a form of goal-oriented automaticity (Aarts and Dijksterhuis 2000; Bargh and Ferguson 2000; Gardner 2012; Limayem et al. 2007; Neal et al. 2011; Sheeran et al. 2005; Verplanken and Orbell 2003; Wood and Neal 2007). A clear definition that is accepted widely among many disciplines states that habits are "learned sequences of acts that become automatic responses to specific situations, which may be functional in obtaining certain goals or end states" (Verplanken et al. 1997). With the recent definition of habit as an explanatory force in understanding current behavior, several important points are clarified on how habit influences behavior. First, habitual behaviors are "learned sequences of acts." Thus there is a requirement that the behavior has been repeated previously in a successful manner for an individual to learn the behavior and be familiar with it. Therefore, it is implied in the definition that habit occurs in the context of routine behavior. Second, habits are "automatic responses", which distance themselves from normative decision making process using cognitive resources. Due to the automatic nature of habit, habitual behavior occurs outside of awareness, where an individual may not be aware of a reason that led him or her to perform a certain behavior (Polites and Karahanna 2012). Behavioral intentions play a minor role when habits are strong, and it frees the cognitive resources of an individual to do other things (Bargh 1994; Verplanken and Orbell 2003), thus habits are mentally efficient (Polites and Karahanna 2012). Third,

المنارة للاستشارات

www.manaraa.com

habitual behaviors are performed automatically as a result of specific situations, environmental cues or a trigger. With repetition of behaviors, individuals, while familiarizing themselves with the behavior, will also learn to associate environmental cues or triggers with particular behavioral responses. These triggers can be in different forms for different individuals, but yet these triggers should occur in stable contexts (Verplanken et al. 1997). When an individual performs a certain behavior in similar environmental cues and goals across consecutive situations, it is considered to be in a stable context (Limayem et al. 2007). An example of a stable situation that triggers a user to lock the computer may be simply leaving it unattended or going back home from work at the end of the day.

Habitual behavior is also about obtaining "goals and end-states". These goals are defined as "desired, or anticipated, outcomes or end states" (Aarts and Dijksterhuis 2000, p. 54) or anticipated, desired effect guiding the performance of behavior (Sheeran et al. 2005). Obtaining the goals or end states successfully through repetition is also equally important. If an individual performs a behavior to obtain a certain goal and accomplishes success, he or she is more likely to perform the same behavior again when the need to obtain the same end state arises, given that a similar stable context and environmental cues exist. Aarts et al. (1997) who conducted research on habitual health behaviors such as physical exercise, posit that satisfactory experiences increase the tendency of an individual to repeat the same behavior. Thus satisfaction is a key condition of habit development.

المنارة للاستشارات

www.manaraa.com

Table 2.4 Prior Research on Habit With Automaticity Dimension (Limayem et al. 2007)

Study	Area	Purpose
Aarts and Dijksterhuis (2000)	Travel mode choice	To explore when travel choice behavior is habitual.
Aarts et al. (1997)	Health related behavior	To describe a theoretical model of exercise habit formation.
Bargh (2002)	Consumer behavior	To examine the role of non-conscious influences in real life in decisions and behavior.
Louis and Sutton (1991)	Cognitive processing	To propose a view of cognitive processing that involves automatic and cognitive modes.
Mittal (1988)	Seat belt usage	To examine the role of habit in seat belt usage.
Orbell et al. (2001)	Ecstasy consumption	To explore to what extent variables specified by the TPB can predict ecstasy use intentions and behavior.
Ronis et al. (1989)	Repeated health-related behaviors	To propose that repeated behavior is largely determined by habits rather than by attitudinal variables.
Verplanken (2006)	3 studies: eating snacks, mental habits, word processing	To test and distinguish habit from frequency of Occurrence.
Verplanken and Aarts (1999)	Review of previous studies on travel mode choices	To synthesize past work in support of the argument that habit is a concept worth studying.
Verplanken et al. (1994)	Travel mode choices	To test a model of travel mode choice predicting behavior from the attitudes toward choosing a car, choosing an alternative mode and car choice habit.
Verplanken et al. (1997)	Travel mode choices	To examine in 3 studies the role of habit in information acquisition concerning travel mode choices.
Verplanken et al. (1998)	Travel mode choices	To investigate (in a field experiment) the prediction and change in repeated behavior in the domain of travel mode choices.

As it was discussed previously, it is important to note that several components need to exist for habitual patterns to form. These components which are clearly defined in

المنارة للاستشارات
www.manaraa.com

the automaticity definition of habit itself are very similar to the three components of the habit loop: trigger, routine, and reward, which will be discussed later in the chapter.

Several studies have been conducted across many disciplines with the view of habit as a form of goal-directed automaticity. All these studies concur to the notion that habit is a learned action sequence, which was originally intentional that may be repeated without conscious intention when triggered by environmental cues in a stable context (Guinea and Markus 2009). From the automatic dimension of habit, past behavior or frequency of past behavior is indicative of only a portion of the habit construct, where the repetition helped an individual to learn a behavior to attain certain goals. Table 2.4 illustrates a summary of previous research conducted with a view of habit as a form of goal-directed automaticity. It is important to note that habit studies related to IS were excluded from this table and will be shown in a later section.

Habit and Behavior

Behavioral researchers have utilized TRA and TPB extensively in their conceptual models to predict behavioral intentions across many disciplines. The link between behavioral intention and actual behavior has been evaluated and established extensively, such that some researchers only utilize behavioral intention as their ultimate dependent variable. These studies imply that a significant relationship between behavioral intention and behavior already exists. For example, in technology adoption literature, research has revealed that behavioral intention to adopt a certain technology explains a significant amount of variance in actual usage of the technology. In TAM-based IS research, behavioral intention explained 40 percent of the variance of actual usage in Davis (1989), 27 percent in Venkatesh and Davis (2000) and 25 percent in

المنارة للاستشارات

www.manaraa.com

Venkatesh et al. (2000). These findings are consistent with the meta-analysis study of 87 TRA-based studies that found behavioral intention to explain about 28 percent of the variance of actual behavior (Sheppard et al. 1988). Most behavioral research models including Technology Acceptance Model (TAM) and Unified Theory of Acceptance and Use of Technology (UTAUT) presume that intention is formed as a result of a conscious decision making process. However, these models do not address how the decision making process and intentions change and evolve over time (Kim and Malhotra 2005) or how individual behaviors may consist of 'unreasoned actions' or actions which are not deliberate (Guinea and Markus 2009). Instead, these models imply that within each time period, new perceptions and intentions are formed without any influence of previous decisions or intentions.

The notion that behavioral intentions may not solely explain the variance in behavior has been reflected in a meta-analysis of behavioral studies where 28 percent of variance in behavior was explained by intention. The authors suggested that automatic activation of behavior may account for a portion of the remainder of unexplained variance (Sheeran 2002). Ajzen (2002) posited that past behavior has a "residual impact" on later behavior beyond what is explained by intention and perceived behavioral control. It was also suggested that most behavioral patterns are "semiautomatic response patterns" where these patterns involve a mixture of controlled and automatic behaviors. With habit being defined as "learned sequences of acts that become automatic responses to specific situations, which may be functional in obtaining certain goals or end states," it has been utilized in behavioral models in three different perspectives: as an indirect effect, as a direct effect, and as a moderator.

المنارة للاستشارات

www.manaraa.com

Scholars who postulate that actual behavior is only driven primarily by intention but yet consider the habit construct to be a significant factor in their research models, have tested habit as a predictor of intention. This perspective results in behavioral intentions mediating the influence of habit on actual behavior, which according to critics, "suffers from both theoretical and empirical shortcomings" (Limayem et al. 2007, p. 717). Its theoretical shortcomings stem from the view that habit is a form of goal-directed automaticity. The true nature of automaticity is that behavior is conducted automatically, thus not following the normative decision making process. Therefore, habit does not influence behavioral intention directly, which is in stark contrast to several studies that have modeled habit to directly influence behavioral intention. Although there are several studies that empirically support a direct relationship between habit and behavioral intention, none of the studies provide solid support and have other shortcomings such as omitting to include actual behavior in the model (Limayem et al. 2007).

Some scholars suggest that habit and intention are independent constructs that predict actual behavior. Several studies have found empirical support when habit was modeled as a direct predictor of actual behavior. Studies modeling habit as a direct predictor on actual behavior in blood donation (Charng et al. 1988), seat belt usage (Mittal 1988), and food consumption (Tuorila and Pangborn 1988) found empirical support on their assumptions. The "automaticity" view provides some support to this view because habitual behaviors reduce the influence of cognitive processes on actual behavior. With the absent or weakened behavioral intentions, habit may become the driving force of actual behavior. Limayem et al. (2007) found empirical evidence of habit

المنارة للاستشارات
www.manaraa.com

having a stronger direct influence on actual behavior than behavioral intentions. Based on the prior evidence, this study tests the direct influence of habit on actual secure behaviors.

Limayem et al. (2007) suggests that "the relationship between intention and habit is more complex" than a simple direct effect on actual behavior. Even though behavioral theories such as TRA and TPB suggest that behavioral intention is the main predictor of actual behavior, advocates of habit as early as 1890 suggested that habit reduces or eliminates conscious decision making when a behavior is performed (James 1890). Initially Triandis (1980) and later Verplanken et al. (1998) suggested that habit has an interaction effect between behavioral intention and behavior, where intentions are assumed to predict behavior when habits are weak. When habits are strong, the relationship between behavioral intention and behavior is assumed to weaken and in some instances become nonexistent. Strong empirical support exist in modeling habit has a moderator of the relationship between behavioral intention and actual behavior (Landis et al. 1978; Montano and Taplin 1991; Ronis et al. 1989; Verplanken et al. 1998). Moreover, some of these studies found that while habit is a stronger predictor of actual behavior than intentions, whenever habit was weak or not present, behavioral intentions became an important predictor of behavior, which is consistent with the idea of habit as a moderator.

While modeling habit as a moderator in a behavioral model, it is important to note that habit acts as a suppressor variable between behavioral intention and actual behavior. A suppressor variable "cancels out, reduces, or conceals a true relationship between two variables" (Limayem et al. 2007, p. 720). Habit as a moderator does not disprove the

www.manaraa.com

existence of the relationship between behavioral intention and behavior, but only suggests that the relationship is weakened depending on the strength of habit.

Formation of Habit

It is important to understand how habits are formed in different contexts before integrating into a research model. Examining the commonly accepted definition of habit, by Verplanken et al. (1997), several factors emerge as requirements for habit formation. The factors that can be easily distinguished from the definition itself are: learned sequences, specific situations, and goals or end states. There are also some factors implied in the definition, such as a stable context and satisfactory experience upon performing a behavior.

Before any habitual behavior is formed in any context, perceptions are formed that lead to behavioral intention, which is consistent with the behavioral normative decision making models. A graphical representation of how habits form was presented by Aarts et al. (1997) in their model of “physical exercise and habit formation”. For example at a given point of time (t=0), when an individual wishes to reach a certain goal or end-state, perceptions of desirability and other factors associated with the behavior are considered. According to Aarts et al. (1997), individuals who perform a certain behavior for the first time, or have little or no experience with the behavior “may seek additional information externally for further subjective validation of one’s perceptions. This external information may be collected through the forms of books, magazines websites or through consulting friends and colleagues who have experience in similar behavior. Once the behavioral goal is set and solidified, the intentions that were formed are implemented,

المنارة للاستشارات
www.manaraa.com

which results in actual behavior. This common decision making process by Aarts et al. (1997) is shown in the upper part of Figure 2.5.

Once the behavior is performed, a user will evaluate if the goal or end-state was achieved using the performed behavior and determine if the experience was satisfactory. A “satisfactory experience” with the behavior is a key component of repeating the behavior in question, thus a key factor for habit formation (Limayem et al. 2007). If the behavior was not satisfactory, perceptions are adjusted, and any new attempt to perform the behavior will initiate with the updated perceptions, which in-turn will create new behavioral intentions. An individual is more likely to perform the same behavior repeatedly when a satisfactory performance of the behavior was experienced previously. The successful outcome will also increase positive perceptions and attitudes towards the behavior, and an individual will learn that the goal or end-state can be accomplished.

This “learned” behavior will reinforce the individual to choose the “same course of action when facing the same situation next time,” increasing the chances of repeated behavior given that the desired goals are similar and behavior is performed in a stable context (Aarts et al. 1997). It is also important to note that individuals recognize that the “same or similar” behavior can be executed repeatedly in a stable context. As depicted in the habit formation model, once the same behavior is repeated over-time, memory of past behaviors will enable the creation of cognitive shortcuts that reduce the use of perceptions and attitudes to create behavioral intention to perform a behavior.

Habits are formed when certain behaviors are carried out consciously and intentionally and repeated frequently over time in a stable context with a “satisfactory experience” (Limayem et al. 2007; Polites and Karahanna 2012). According to Aarts et

المنارة للاستشارات
www.manaraa.com

al. (1997), habit is suggested to have been formed to some degree with just “a single experience” that was satisfactory and additional positive experiences with the behavior will only strengthen the habit.

المنارة للاستشارات

www.manaraa.com

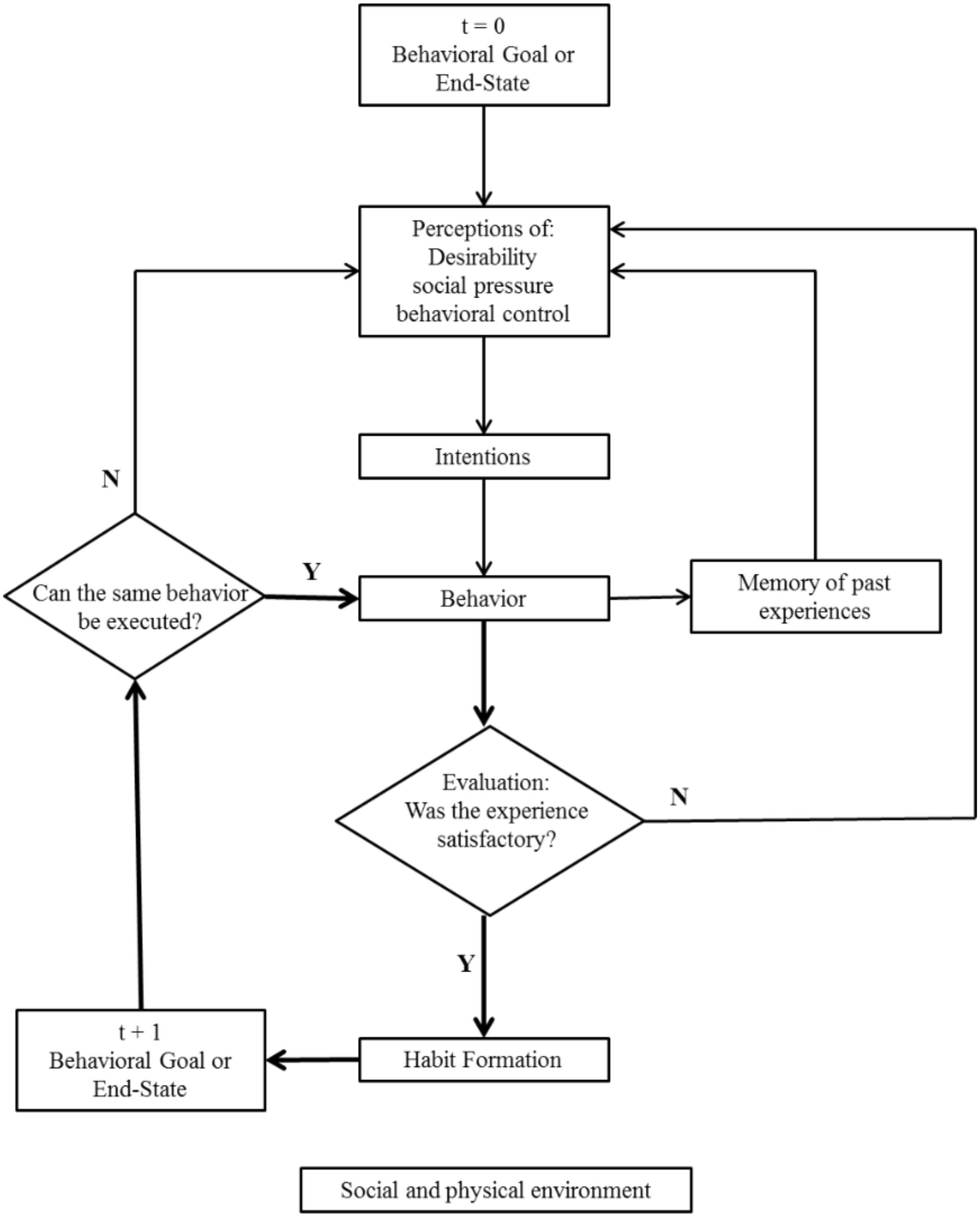

t = 0
Behavioral Goal or End-State
Perceptions of: Desirability social pressure behavioral control
Intentions
Behavior
Memory of past experiences
N
Can the same behavior be executed?
Y
Evaluation: Was the experience satisfactory?
N
Y
t + 1
Behavioral Goal or End-State
Habit Formation
Social and physical environment

Figure 2.5 Model of Habit Formation (Aarts and Dijksterhuis 2000)

www.manaraa.com

When habit is in full force, all which is needed for an automatic behavior to occur is the initiation of a goal or end-state to act in memory and a situational cue that triggers the behavior. Thus the frequency of the behavior that is performed will influence the strength of habit, where repetition of a behavior routinely (e.g., daily basis) will form stronger habits than behaviors that are practiced less often (e.g., monthly basis).

Once strong habits are formed, behaviors will no longer be guided by reasoned considerations and behavioral intentions will have very little influence on the actual behavior that is performed. This habit formation process is represented in bold arrows in the bottom left of Figure 2.5.

Habit Loop

Recently, a similar but innovative concept on habit formation called “habit loop” was introduced by Duhigg (2012). According to Duhigg, habits account for more than 40 percent of an individual’s daily routine, and every habit initiates with a psychological pattern called a "habit loop," which is a three-part process. In the first part, there's a cue, or a trigger, that tells your brain to go into automatic mode and let a behavior unfold. This is similar to the environmental cues or specific situations that are defined by Verplanken et al. (1997). Next is the routine or the behavior itself, such as brushing your teeth, locking your computer or locking your door. The third step is the reward, which is something your brain enjoys and helps it reinforce the “habit loop” in the future.

Habit-making behaviors are traced to a part of the brain called ‘basal ganglia’ by neuroscientists, while decisions are made in a different part of the brain called prefrontal cortex. But as the decision making and behavior becomes automatic or habitual, the decision making part of the brain is free or in sleep-mode, which enables the brain to use

المنارة للاستشارات

www.manaraa.com

its resources on something else. The influence of basal ganglia on creating habits was tested by Graybiel (2008) of Massachusetts Institute of Technology (MIT), when it was noticed that mice with damaged basal ganglia developed problems with tasks such as learning how to run through mazes or remembering how to open food containers. An experiment was conducted to investigate the brain activity in the basal ganglia of rats using a maze where the rats were required to find a piece of chocolate (reward) at the end of the maze. When the rats heard a click (trigger) and saw a partition disappear, they wandered through the maze and often made several wrong turns before finding the piece of chocolate. The equipment used in the experiment detected high brain activity during the time the rats were attempting to find the chocolate.

The scientists repeated the experiment several times and discovered that the brain activity of each rat changed as they moved through the same route many times. After several repetitions of the experiment, rats learned how to navigate the maze and found the chocolate quickly without making any wrong turns. Scientists also uncovered that as each rat learned the navigation of the maze, its brain activity decreased as the route became more automatic, and each rat started thinking less and less. Scientists attributed the "learned sequences" of rats' behavior to the basal ganglia, where the habits were stored and activated even when the brain activity ceased. The graphs depicting the brain activity during the initial behavior and routine behavior is portrayed on Figure 2.6. During the initial stage, the rat's brain functions are in full force when the maze is encountered and the trigger is supplied. After a week, when the behavior is routine and the rats are familiar with the path that leads to the piece of chocolate, not only did they make correct turns majority of the time, but also reached the chocolate in a very quick time. This illustrates

المنارة للاستشارات
www.manaraa.com

that when the routine behavior is performed, the brain activity of rats slow down significantly. Graybiel (2008) suggests that a similar process happens in human brains. In the initial stages of a human behavior, it is not automatic but it is goal directed similar to an animal attempting to find the food reward. But with repetition and success of obtaining the reward in each attempt, the behavior becomes automatic. These notions were confirmed in lab tests that investigated human brain activity of habitual smokers using functional Magnetic Resonance Imaging (fMRI) (Janes et al. 2009).

When behaviors are habituated, this process where the brain converts a sequence of actions into an automatic routine is known as "chunking." In this process, our neural circuits engage in some type of chunking behavior frequently. From simple automated behavior, such as putting toothpaste on the toothbrush before inserting in to the mouth, to rather complex behavior, such as getting dressed or making kids lunch, our brains are constantly involved in the chunking processes (Duhigg 2012). Chunking in our brains happen in the three steps where the habit loop is formed. An environmental cue or trigger informs the brain to go into automatic mode and select which habit to use, based on the desired goal or end state. Then the routine is performed, which is the repetitive behavior that has been "learned". Finally, a reward helps the brain to figure out if this loop is worth remembering for the future.

المنارة للاستشارات
www.manaraa.com

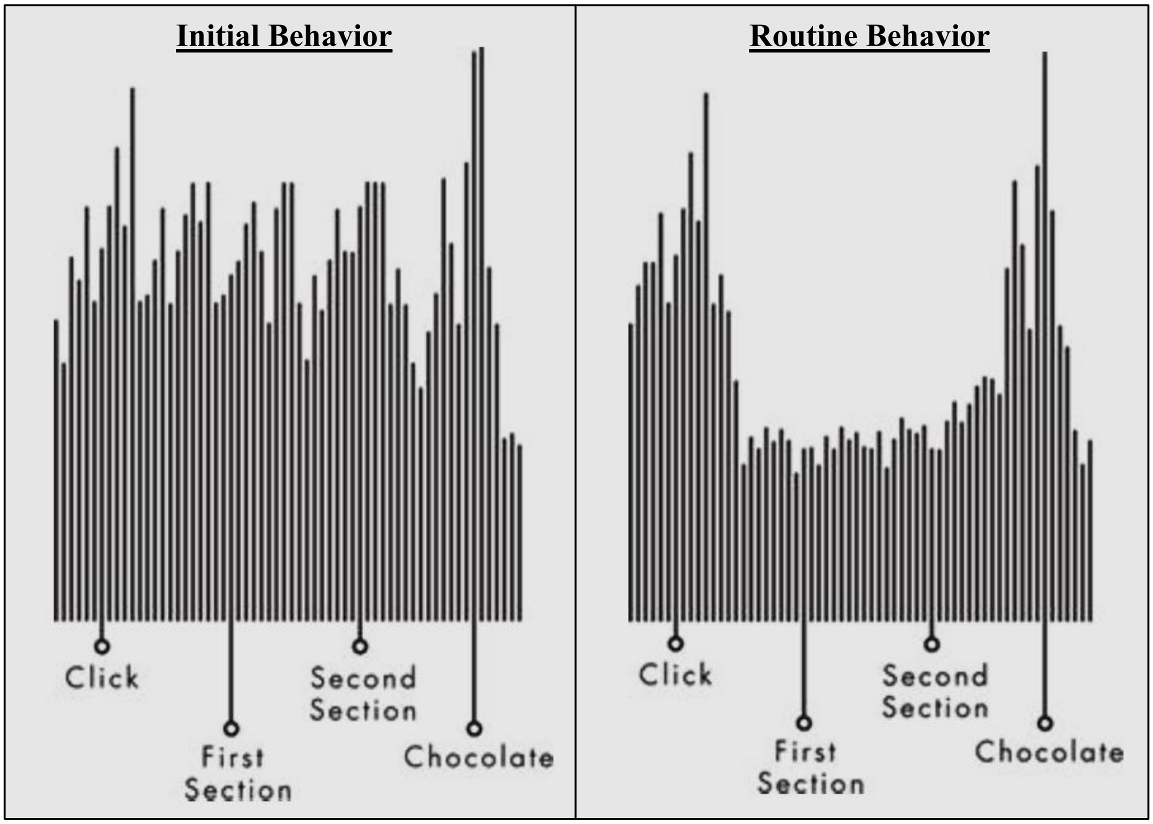


Figure 2.6 Rat’s Brain Activity With Habits (Duhigg 2012)

A habit loop can also be used to create new habits or break current habits. An appropriate example for a situation where a habit needs to be broken is when one wants to stop smoking. By identifying the cues and rewards that are associated with cigarettes and then choosing new routines that provide similar rewards, the habit of smoking can be broken while replacing it with a newly created habit, such as a piece of Nicorette or a quick series of push-ups (Duhigg 2012). Organizations such as Microsoft and Google are spending millions to understand the neurology and psychology of habits, their strengths

المنارة للاستشارات
www.manaraa.com

and weaknesses, and how habits can be created and broken when necessary. For this study, the focus will be only on the routine or habitual behavior, while the rewards and cue will not be investigated. How the habit loop can be integrated in to individual threat perceptions and threat responses in information security research will be discussed later in this chapter. Figure 2.7 demonstrates the habit loop consisting of a cue, a routine, and a reward. Once this loop is repeated, habitual behavior emerges.

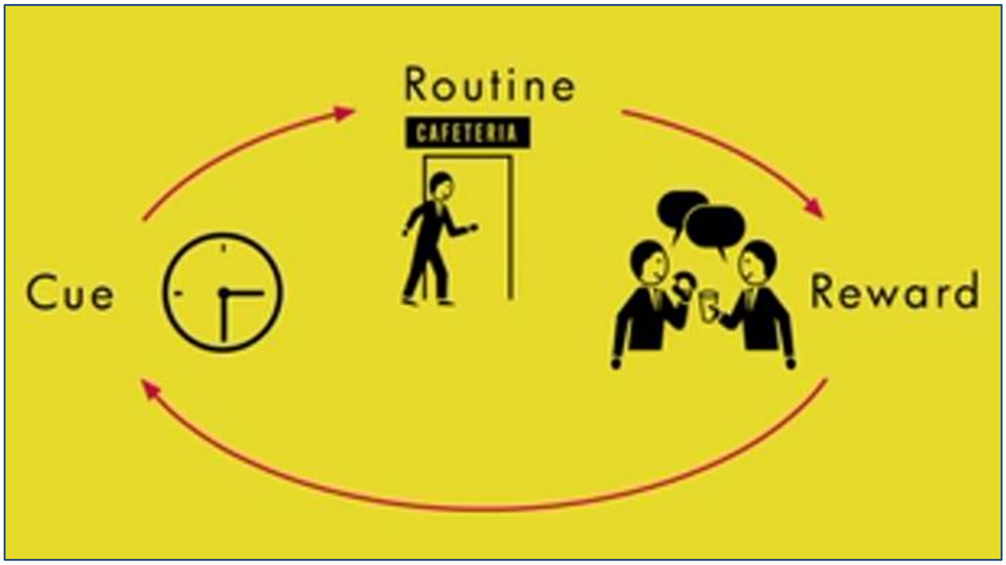


Figure 2.7 Habit Loop (Duhigg 2012)

Habit in IS Research

Although there is an abundance of behavioral research literature in the field of information systems, habit has gained little attention. As with other behavioral research, most behavioral IS research models explore behavioral intentions or behavior at a given point in time. Thus, these studies usually do not consider the importance of habit in their models. Since most behaviors are routine or habitual in nature, even when behavioral

www.manaraa.com

research studies are conducted as cross-sectional, individuals may have already formed habitual patterns for the behavior that is tested. There has been an abundance of technology adoption literature following TAM and UTAUT and various research studies that have been conducted extending these models. Attention has also been focused on post-adoption behavior, or so called IS Continuance or Discontinuance, because after the initial adoption stage, an end user will have to make the ultimate decision whether to continue using a certain technology or information system or to discontinue the usage. Individual behavior in the context of IS usage is usually repetitive or performed on a routine basis. With satisfied outcomes or experiences, individuals are likely to continue to use an IS or perform IS related behavior repetitively, which will result in the formation of habitual behavior. Karahanna et al. (1999) found that different factors affect the users to initially adopt a technology (adoption intention) and to continue or discontinue using such technology (post-adoption). Several other studies (Bhattacherjee 2001; Jasperson et al. 2005; Saga and Zmud 1994) have confirmed these findings and elaborated the importance that the success of a technology or information system depends on how many users have moved beyond the initial adoption stage and used the technology regularly. Behavioral intention may play a significant part in the initial IS adoption stage, but with repeated behavior, individuals are likely to use IS automatically because learning and stable contexts exist.

Venkatesh et al. (2000), in a longitudinal five month study of technology adoption, found that although usage of IS was heavily influenced by behavioral intentions in the initial state (t=1), as time progressed (t=2 and t=3), “behavior became more habituated” resulting in a significant decrease of the influence on IS usage from

المنارة للاستشارات

www.manaraa.com

intentions. This reflects the automaticity view of habit where habit is conceptualized to have a direct effect on actual behavior while having a suppressing effect on the relationship between behavioral intention and behavior. Although it was not included in the original Unified Theory of Acceptance and Use of Technology (UTAUT) model (Venkatesh et al. 2003), the notion of habit is reflected in the UTUAT2 model (Venkatesh et al. 2012).

Venkatesh et al. (2012) posit that in terms of continued usage, individuals will form “differing levels of habit” depending on the frequency of usage and familiarity gained with a technology or continuance behavior. In UTUAT2, habit is operationalized as a self-reported perception consistent with prior research such as Limayem et al. (2007) and Polites and Karahanna (2012a). They developed a 3-item scale to measure habit and discovered that habit, along with several other variables, explained more variance in behavioral intentions and actual behavior compared to the original UTAUT model. They also found that certain demographic characteristics such as age moderated the habit-intention and habit-usage relationships. The UTUAT2 model is presented in Figure 2.8.

المنارة للاستشارات

www.manaraa.com

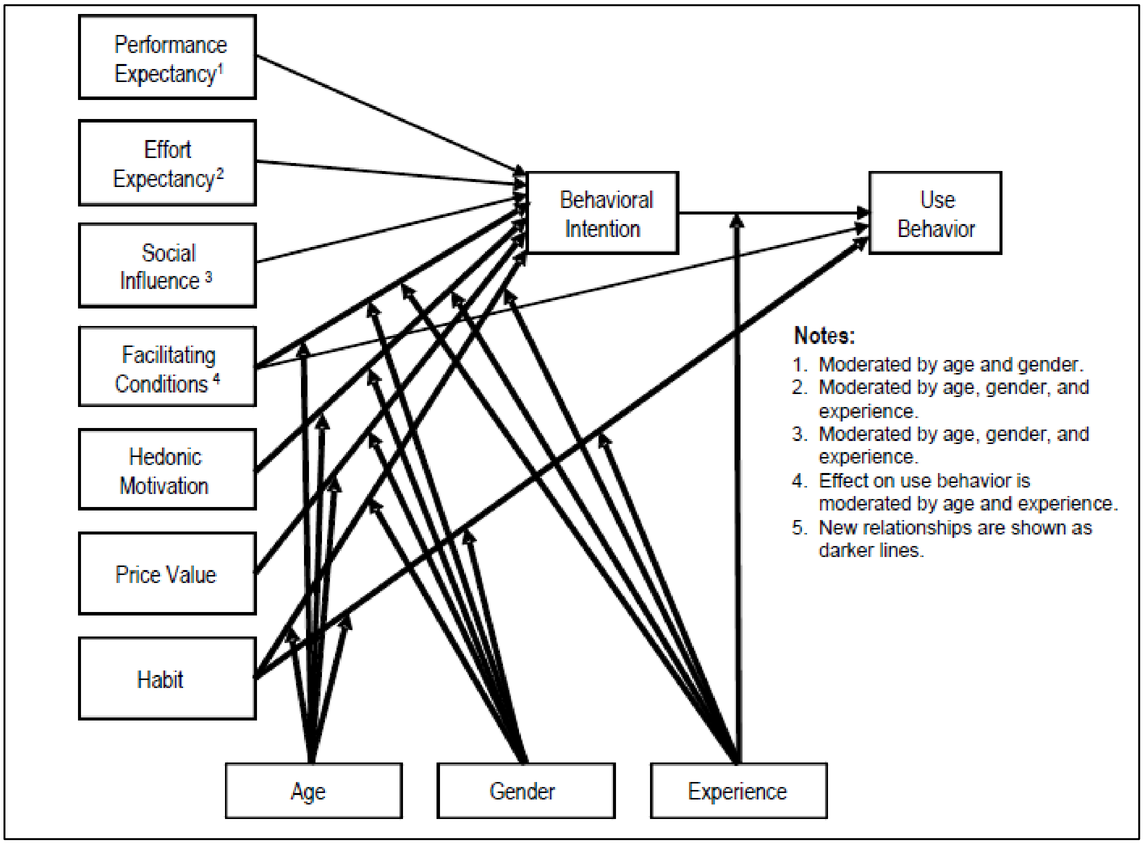

Performance Expectancy1
Effort Expectancy2
Social Influence 3
Facilitating Conditions 4
Hedonic Motivation
Price Value
Habit
Behavioral Intention
Use Behavior
Age
Gender
Experience
Notes:
1. Moderated by age and gender.
2. Moderated by age, gender, and experience.
3. Moderated by age, gender, and experience.
4. Effect on use behavior is moderated by age and experience.
5. New relationships are shown as darker lines.

Figure 2.8 UTAUT 2 Model (Venkatesh et al. 2012)

Kim and Malhotra (2005) conducted a longitudinal study on how individual users' evaluations and behaviors evolve as they gain experience with the IS. Their findings suggest that the influence of intentions on actual behavior decreased with time, which is consistent with the findings of Venkatesh et al. (2000). Although research studies conducted across many disciplines are in disagreement on how habit is defined, it is of interest to note that a majority of the recent IS literature utilizing habit are in unison with the view of habit as goal-directed automatic behavior. Cheung and Limayem (2005) and Limayem and Hirt (2003) investigated habitual behavior in the student use of WebBoard and BlackBoard systems. They collected their data utilizing a two-stage

المنارة للاستشارات
www.manaraa.com

questionnaire-based survey and found that the inclusion of habit increased the variance explained by the actual behavior construct. However, they modeled habit as a direct effect on behavior along with behavioral intention.

Kim and Malhotra (2005) defined habit as “a repeated behavioral pattern that automatically occurs outside awareness.” They observed that, Web Portals, when used frequently in a stable environment, habitual behaviors emerged that overshadowed the effect of intention on future use. Similar to previous studies, data were collected in two stages, and actual usage was measured employing a self-reported scale.

Gefen (2003) used a different approach compared to other IS literature that utilized habit. He defined habit as “previous usage preference of an IT” and suggested that repeated previous behavior often dictates current behavior independently of any rational assessments. The results suggest that habit was a strong predictor of continued purchases from a specific website through data collected from experienced shoppers. However, habit was modeled to influence behavioral intention directly, hence an implied indirect effect of actual behavior, which is theoretically challenged given the automaticity nature of habit.

Given the applicability of habit in behaviors related to information systems usage, there have been only a few studies that actually tested the role that habit plays in IS usage. Concerned by the lack of research studies applying the concept of habit, Benbasat and Barki (2007) called for more research investigating the role of habit in IS. Recently there has been an increasing trend in the number of articles published utilizing habit on IS research literature in the IS Continuance and Discontinuance area (Limayem and Cheung 2011; Limayem et al. 2007; Wu and Kuo 2008; Ye and Potter 2011).

المنارة للاستشارات
www.manaraa.com

Limayem et al. (2007, p. 705) defined habit in the context of IS usage as “the extent to which people tend to perform behaviors (use IS) automatically because of learning.” While hypothesizing that continued IS usage is not only a consequence of intention, but also habit, they tested a model where habit moderated the relationship between behavioral intention and behavior. This moderating relationship of habit captures the true nature of the habit definition, which is automaticity, where automatic responses reduce the need for cognitive processing, thus reducing the influence of intentions of behavior when habits are strong. Investigating habitual usage of the World Wide Web (WWW), habit was found to significantly suppress the relationship between behavioral intention and behavior, confirming their hypotheses. Limayem and Cheung (2011) investigated the role of habit in internet-based learning technology usage and found that habit negatively moderated the intention-behavior relationship. Some of the recent research in IS utilizing habit as a construct are listed in Table 2.5 along with their behavioral context.

المنارة للاستشارات
www.manaraa.com

Table 2.5 Recent IS Research Utilizing Habit

Source	**Method**	**DV**	**DV=Actual Behavior**	**Measurement of DV**	**Measurement of Habit**	**Usage of Habit in the Model**
Cheung and Limayem (2005)	Survey (longitudinal - 4 points of time)	Actual behavior	YES	Self-reported	Self-reported (limayem2003)	Moderator to intention-behavior.
Chiu et al. (2012)	Survey	Behavioral Intention	NO	Self-reported	Self-reported	Moderator of trust and purchase intention
Gefen (2003)	Survey	Behavioral intention	NO	Self-reported	Self-reported	Direct and indirect effect on intention.
Khalifa and Liu (2007)	Survey	Repurchase intention	NO	Self-reported	Self-reported (Limayem & Hirt 2003)	Habit positively moderates online shopping satisfaction and repurchase intention.
Khalifa et al. (2002)	Survey + online purchase tracking	Actual behavior (Repurchase)	YES	Actual behavior	Self-reported	Moderating relationship between satisfaction and repurchase.
Kim and Malhotra (2005)	Survey	Actual behavior	YES	Self-reported	N/A	N/A
Kim et al. (2005)	Survey (2 phase)	Actual behavior	YES	Self-reported	N/A	Moderator to intention-behavior and direct effect on intentions.

www.manaraa.com

Table 2.5 (continued)

Source	**Method**	**DV**	**DV=Actual Behavior**	**Measurement of DV**	**Measurement of Habit**	**Usage of Habit in the Model**
Limayem & Cheung (2011)	Survey (2 phase)	Actual behavior	YES	Self-reported	Self-reported (Limayem & Hirt 2003)	Moderator to intention-behavior.
Limayem and Hirt (2003)	Survey (longitudinal)	Actual behavior	YES	Self-reported	Self-reported	Direct influence on actual behavior and affect.
Limayem et al. (2001)	Survey (longitudinal)	Actual behavior	YES	Self-reported	Self-reported	Moderator to intention-behavior.
Limayem et al. (2007)	Survey (longitudinal - 3 points of time)	Actual behavior	YES	Self-reported	Self-reported (developed scale)	Moderator to intention-behavior.
Pahnila et al. (2007)	Survey	Actual Behavior	YES	Self-reported	Self-reported	Direct effect on intention.
Polites and Karahanna (2012)	Survey (longitudinal)	Behavioral intention	NO	Self-reported	Self-reported (developed scale-Formative)	Indirect influence on intention.
Siponen et al. (2010)	Interviews	N/A	N/A	N/A	Self-reported	Direct effect on actual behavior.
Vance et al. (2012)	Scenario/Survey	Behavioral intention	NO	Self-reported	Self-reported (Verplanken self-report)	PMT variables mediating the relationship between habit and intention.

المنارة للاستشارات
www.manaraa.com

Table 2.5 (continued)

Wu and Kuo (2008)	Survey	Behavioral intention	NO	Self-reported	Self-reported (Verplanken self-report)	Direct effect on intention.
Source	**Method**	**DV**	**DV=Actual Behavior**	**Measurement of DV**	**Measurement of Habit**	**Usage of Habit in the Model**
Ye and Potter (2011)	Survey (2 phase)	Actual behavior	YES	Self-reported	Self-reported (Limayem 2007 scale)	Indirect effect on intention and direct and indirect effect on intention.

المنارة للاستشارات
www.manaraa.com

Some of the extant literature on applying the concept of habit has modeled behavioral intention as the ultimate dependent variable (Gefen 2003; Polites and Karahanna 2012; Vance et al. 2012; Wu and Kuo 2008). This is rather contradictory to the definition of habit where habit is formed beyond behavioral intentions. Moreover, by testing a research model that does not measure behavior, researchers will not be able to capture the true strength of habit, since the link between behavioral intention and actual behavior is only implied and not tested. Most of the research models incorporating the automatic nature of habit, have modeled actual behavior as the ultimate dependent variable. Due to challenges such as Institutional Review Board (IRB) issues, denied access to server logs, and inaccessibility of information, researchers have used self-reported scales to measure actual behavior (Crossler et al. 2013; Warkentin et al. 2012). Although a subjective behavioral measure such as self-reported actual behavior is sufficient, Straub et al. (1995) suggests that it should be supplemented with other objective measures whenever possible. Several methodologies utilized by researchers to operationalize habits and their strengths and weaknesses will be discussed in Chapter III.

Habit in IS Security Research

Research studies in IS security have utilized several behavioral theories such as Protection Motivation Theory (PMT) (Anderson and Agarwal 2010; Gurung et al. 2009; Ifinedo 2012; Johnston and Warkentin 2010; Lee 2011; Liang and Xue 2010; Marett et al. 2011; Vance et al. 2012), General Deterrence Theory (GDT) (D'Arcy and Devaraj 2012; D'Arcy et al. 2009; Herath and Rao 2009; Hovav and D'Arcy 2012; Siponen and Vance 2010), Self-efficacy (SE) (Bulgurcu et al. 2010; Herath and Rao 2009; Zhang et al. 2006), Extended Parallel Processing Model (EPPM) (Johnston and Warkentin 2010),

www.manaraa.com

Fear Appeals Model (FAM) (Johnston and Warkentin 2010) and Rational Choice Theory (RCT) (Bulgurcu et al. 2010). Most of these studies utilized behavioral intention as the ultimate dependent variable. Since actual behavior is not measured, these studies can only assume that a positive relationship exists between behavioral intention and actual behavior. Furthermore, these studies only measure individual perceptions in a cross-sectional manner, thus they do not take into consideration that the relationship between intention and behavior change over time and that the behaviors become habitual.

Among many behavioral research studies utilizing theories such as PMT and Deterrence Theory in the context of information security, it is surprising that the concept of habit was investigated in only few of the behavioral research studies. There is empirical evidence in social psychology literature which suggests that many behaviors we perform are habitual (e.g., driving a car, wearing seatbelts, drinking alcohol, smoking, use of condoms, food consumption, blood donation). Recent behavioral research in IS, such as the ones listed previously, also suggest that individuals form habitual patterns of behavior in using information systems (Blackboard usage, shopping online, surfing the web, use of web browser, searching the web). With more than 40% of daily behavior of individuals being habitual (Duhigg 2012; Neal et al. 2006), it is imperative to assume that habits are very much applicable to many information security behaviors at organizations since they are performed routinely by employees in the presence of certain environmental cues in order to attain desired outcomes or end states. For example, in the behavior of backing up data, the trigger or the environmental cue may be in the form of the time (e.g. end of work day or end of week), and the routine or behavior is backing up data. The desired outcome or end state is that the data is backed up, and the reward is the feeling or

المنارة للاستشارات
www.manaraa.com

assurance that the data is secure in case of hard drive failure. Similarly, volitional but non-malicious behavior, which still violates organizational security policies (Willison and Warkentin 2013), can become habitual when performed on a routine basis.

Although habits have been tested in the context of information security only on a few occasions, several information security research studies have clearly identified habit as a major factor that drives secure behaviors. The behavior of password creation and usage was suggested as habitual by several research studies where they identified habitual patterns in password creation such as choosing the same password across multiple applications or websites, choosing an easy to guess password and the automaticity of entering passwords (Adams et al. 1997; Bellman et al. 1999; Farn et al. 2004; Florencio and Herley 2007; Herath and Rao 2009; Morris and Thompson 1979; Yang and Shieh 1999) . One study identified that programmers may form habits related to writing programming code according to IT security rules (Farn et al. 2004), while another study identified the habituation of validating all input by a programmer (Rietta 2006). The role of habit in network usage and the detection of malware such as worms were identified by Wang et al. (2005).

Backing up data, which has been a behavior of study in information security research (Crossler and Belanger 2012; Crossler 2010), was identified by several scholars as a behavior where habits can be formed (Chunli and Donghui 2012; Dunnavant and Childress 2010; S.B.Thorat et al. 2010; Spennemann and Atkinson 2002). Logging off or locking the computer terminal when leaving it unattended is one of the secure behaviors recommended by organizations (Siponen and Vance 2010). This behavior when performed repetitively and successfully in a stable context is suggested to form habits by

www.manaraa.com

some scholars (Morgan et al. 2007; Siponen et al. 2010). Clicking on unknown web links on emails and social media sites have been identified as a behavior that may compromise information security by security experts. However, some individuals evaluate the safety of the website before visiting it or clicking on a link. Chen and Halsey (2009) and Frøkjær and Hornbæk (2002) suggest that clicking on unknown web links and the evaluation of the safety of visiting websites are behaviors that can be habitual. Behaviors related to emailing such as reviewing the addresses of recipients before sending email (Etchells 2008; Vandermeer 2006) and exercising care when opening email attachments (Ng et al. 2009). Herath and Rao (2009) suggest that while actual behavior is significantly influenced by behavioral intentions, “may factors such as habits” should be considered for future studies. Anderson and Agarwal (2010) indicated that future research should identify the role of habit in secure behaviors and possibly as a moderator to their research model. These research studies provide ample support to the argument that information security behaviors can be habitual.

Although many research studies have identified habit as a key factor that influences secure behavior, only a few studies have tested the role habit plays in information security. Pahnila et al. (2007) was one of the first studies to investigate habit in the context of information security. They hypothesized that habit directly influenced behavioral intention to comply with security policies along with other independent variables such as sanctions, threat and coping appraisal, facilitating conditions and rewards. The data were collected from a single company in Finland using an online survey and habit was measured using a pre-validated self-report scale by Limayem and Hirt (2003). Their data analysis indicated that habit positively influenced behavioral

المنارة للاستشارات
www.manaraa.com

intention to comply with security policies. They suggested that organizations should get their employees “into the habit of complying with security policies.”

Using a qualitative approach, Siponen et al. (2010) suggested that habit influenced security related behaviors such as secure use of the internet, writing down passwords and locking one’s PC. They employed a grounded theory approach to identify key concepts and develop linkages between them. Interviews were conducted with employees of a global company located in Switzerland, China and United Arab Emirates (UAE). They identified secure use of the internet, writing passwords down, password selection and locking the workstation as behaviors for their study. They found habitual enactment to be a factor of locking one’s PC, writing down passwords and secure use of the internet but password selection was not associated with habit. Employees who were interviewed responded that following security procedures such as locking the PC is inconvenient and time-consuming.

Vance et al. (2012) hypothesized that PMT variables, representing threat appraisal and coping appraisal mediated the relationship between habit and behavioral intention to comply with IS security policies. They utilized a hypothetical scenario method which presented the respondents with a scenario that reflected a certain non-compliant behavior. After reading the scenario, respondents were asked to answer survey questions. After convening an expert panel, they selected five non-compliant behaviors to be investigated in their study. These behaviors were: sharing passwords, failing to lock or log off a workstation, allowing reading confidential material at printers, allowing children at home to use and install software on a work laptop, and copying highly sensitive information to a USB stick. The results of their data analysis indicated that habit directly influenced the

المنارة للاستشارات
www.manaraa.com

threat and coping appraisal variables of PMT. They also found that all the PMT variables except the threat vulnerability significantly influenced behavioral intention to comply with security policies. The research model of Vance et al. (2012) is illustrated in Figure 2.9.

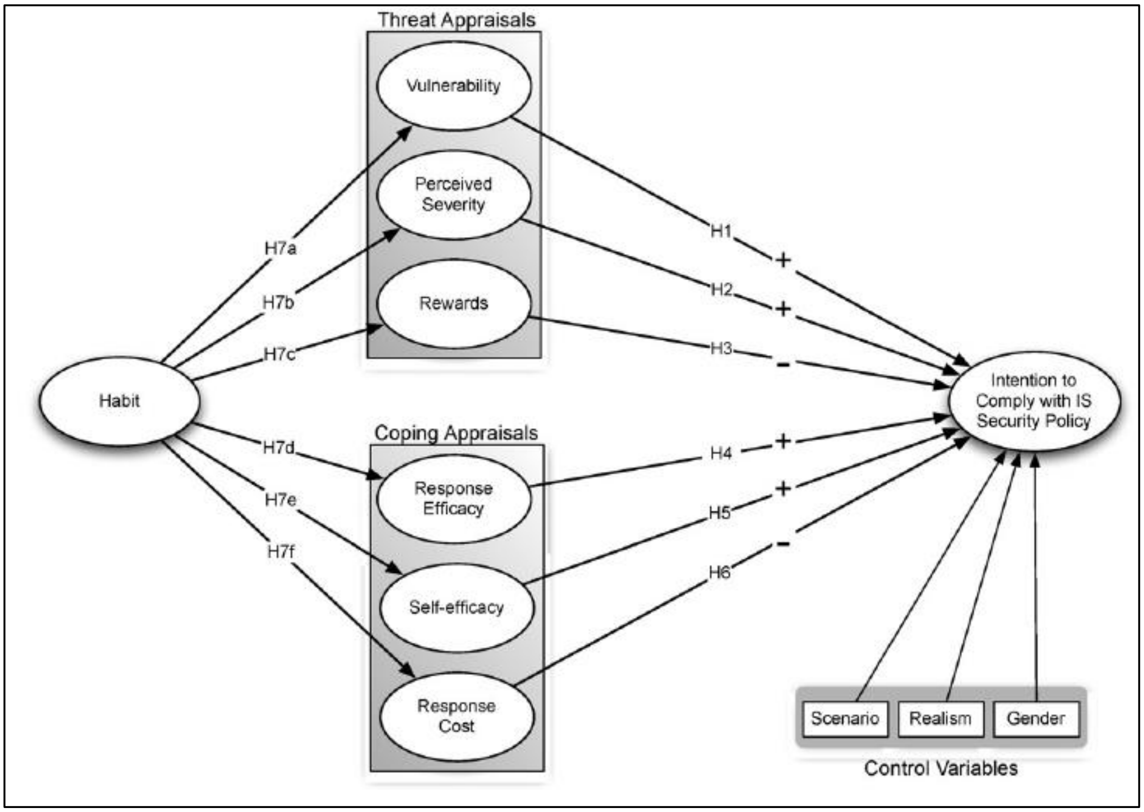


Figure 2.9 Vance et al. (2012) Research Model

This study significantly differs from previous information security studies that tested the role of habit, in many aspects such as the use of theories, hypothesized relationships, method used and expected findings and contributions. These differences are

المنارة للاستشارات
www.manaraa.com

discussed in detail on this section, while details on how this present study overcomes the shortcomings of the previous studies are explained.

Similar to the present study, both Pahnila et al. (2007) and Vance et al. (2012) utilize Protection Motivation Theory (PMT) and habit theory in an information security context. Siponen et al. (2010) utilized a grounded theory approach to construct their research model. Compared to the present study, previous studies differ significantly on how they utilized habit in their research models. Pahnila et al. (2007) and Vance et al. (2012) agree with the notion that frequency of past behavior alone does not constitute habit and recognizes that the habit construct is based on the key element of automaticity. They also agree that when habits are formed, individuals may perform certain behaviors without making conscious decisions and that these habitual behaviors may be triggered by environmental cues. However, Pahnila et al. (2007) hypothesizes that habits will directly influence behavioral intentions to comply with security policies and Vance et al. (2012) hypothesizes that awareness of threats will trigger the cognitive appraisal process of the PMT, which in turn leads to intention to behave. This contradicts their earlier notion that habitual behaviors are performed with little or no involvement of conscious decision-making. This present study follows the definition of habit by Verplanken et al. (1997), where habit is defined as a form of goal-oriented automaticity. The automatic nature of habit implies that conscious decision-making is reduced or non-existent when habitual behavior is performed. Therefore, the view that when habits are strong the influence of the cognitive process towards performing an actual secure behavior is reduced or non-existent is used for this study, which is consistent with prior psychology

المنارة للاستشارات

www.manaraa.com

research (Verplanken 2006). Siponen et al. (2010) found that habits influenced certain secure behaviors directly, which is consistent with a hypothesis of this study.

During the initiation of a new secure behavior, the threat and coping appraisal processes of PMT are activated, leading to creating behavioral intentions that will eventually lead to actual performance of the secure behavior. When this behavior is performed repetitively and successfully in a stable context, it will gradually become automatic or habitual. These habitual secure behaviors may be triggered by environmental cues or events. It is important to note that when a certain secure behavior is habitual, it may be performed simply due to habit, without going through the cognitive mediating process defined in PMT. Therefore, threat and coping appraisal processes or other perceptions such as sanctions, facilitating conditions and normative beliefs may have little or no impact on the actual performance of a behavior when behaviors have become habitual. In contrast to the previous studies, this present study clearly distinguishes the automatic nature of habit where habits reduce or negate any influence of the cognitive mediating process.

The present study modeled habit to negatively moderate the intention-behavior relationship and directly influence actual behavior. This is in contrast to Pahnila et al. (2007) who hypothesized habit to directly influence behavioral intentions and Vance et al. (2012) who hypothesized that PMT variables mediated the relationship between habit and behavioral intentions.

Protection Motivation Theory suggests that when an individual faces a threat, he or she assesses the severity and vulnerability of the threat in the threat appraisal process. In the coping appraisal process, individuals also assess their own capability and the

المنارة للاستشارات
www.manaraa.com

capability of the recommended response in deterring the threat while considering the costs involved in practicing the recommended behavior. Both threat appraisal and coping appraisal processes will lead to the formation of behavioral intentions to perform secure behavior (Rogers 1983). Intentions will then lead to actual behavior.

However, when intentions are formed based on the threat and coping appraisals, influence of habit would be at the weakest level. The influence of habit would become stronger as an individual performs the secure behavior repeatedly and eventually, the secure behavior will become an automatic response to an environmental trigger. If the threat perceptions are reduced or the behavior becomes unsatisfactory, new behavioral intentions are formed. This means that habit is weakened, and the cognitive processes therefore, become the driving force of actual behavior until the habit loop forms. Habits are automatic in nature and involve little or no cognitive power (Verplanken et al. 1998). Modeling habit in a research model as an indirect effect on actual behavior or a direct effect on behavioral intention may create theoretical issues and does not capture the true nature of habit (Limayem et al. 2007). Therefore, it can be concluded that the conceptual models of Pahnila et al. (2007) and Vance et al. (2012) are theoretically weak, at least from the automaticity point of view.

In terms of the methodology utilized, Pahnila et al. (2007) used an online survey to collect their data from a single company. They utilized a self-report scale developed by Limayem and Hirt (2003) to measure habit. They also modeled actual compliance as the ultimate dependent variable in their research model, which allowed them to test the relationship between intentions and behavior. Vance et al. (2012) collected data utilizing a hypothetical scenario, which is a common method of assessing unethical behavior

المنارة للاستشارات

www.manaraa.com

(Nagin and Pogarsky 2001). They used five scenarios of different policy violations in their study and utilized the self-report habit scale (Verplanken and Orbell 2003) to operationalize habit. Although they found that behavioral intentions to comply with security policies differed significantly depending on the scenarios received by the respondents, they analyzed data from the five different scenarios together, as one behavior. This does not allow the identification of how each behavior differs in habit strength and the differences that exist on how habit influences each behavior in the context of information security. Vance et al. (2012) also modeled the ultimate dependent variable as behavioral intention to comply with security policies but respondents were presented with a scenario relevant to one of the five security policy violations. This may have introduced serious flaws in their instrument design since an employee who may violate some sections of the security policy yet comply with other sections does not comply with security policies overall. For example, an employee may lock his or her computer every time it is left unattended but may use unencrypted portable media to copy company data. In this situation, if an employee answers that he or she intends to comply with the security policies, the responses will be erroneous. This especially applies to the way they measured habit. They measured the habit of security policy compliance in general which implied that the employees complied with all the security policies. Similarly, Pahnila et al. (2007) also tested the behavioral intentions and actual compliance of security policies in general, which may have introduced similar errors in their data as mentioned previously.

Vance et al. (2012) utilized behavioral intention as the ultimate dependent variable with their study, which is similar to other PMT related studies. However, as

المنارة للاستشارات
www.manaraa.com

discussed previously, recent information security research studies have measured self-reported actual behavior since behavioral intentions may not always be the perfect proxy for actual behavior (Lee 2011). Pahnila et al. (2007) and Vance et al. (2012) collected their data only from one organization. Collecting data from a single company provides advantages to researchers such as all respondents have the same security policy, same organizational culture, thus reducing the need to control for those factors. However, collecting data from multiple organizations across different industries makes the findings more generalizable (Compeau et al. 2012).

Pahnila et al. (2007) found that habit significantly influenced behavioral intentions to comply with security policies and the intentions significantly influenced actual policy compliance. They suggest that employers should get their employees into the habit of complying with IS security policies. Vance et al. (2012) found that habit significantly influenced threat and coping appraisals and all the variables except perceived threat vulnerability had a significant impact on behavioral intentions. They discussed the theoretical and practical implications of their findings related to the relationships between the PMT constructs and behavioral intention to comply with policies. However, they failed to discuss the theoretical and practical implications of the relationships they found on habit with relation to the PMT variables. From the discussion above, it is clear that the studies by Pahnila et al. (2007) and Vance et al. (2012) do not provide a theoretically sound argument on how habit influences secure behaviors. Our study provides a fresh perspective into investigating the role of habit in information security behaviors utilizing PMT while correcting any potential drawbacks in the Pahnila et al. (2007) and Vance et al. (2012) studies that may have biased their findings.

المنارة للاستشارات

www.manaraa.com

In terms of organizational security, firms would require their employees to form positive or secure habits while breaking their negative or mal-adaptive habits. Organizations would also prefer their employees to perform secure behaviors 100 percent of the time. This can be achieved by encouraging them to habitually or automatically perform those behaviors or perform them intentionally. This is important because it takes only one incident for an information security breach to occur (Motorola 2010). It is important to note that habits may not be applicable to every secure behavior. Certain secure behavior, such as backing up data or changing passwords, may require some cognitive processing in order to perform the behavior, thus reducing the chances of those behaviors becoming habitual. Behaviors such as backing up data and usage of anti-virus software may also be automated by the organizations where individuals do not need to perform any behavior related to them (PWC 2013). However, secure behaviors such as logging off or locking the computer terminal when leaving it unattended, if performed on a routine basis, may become automatic in nature, thus habitual. It is important to understand which secure behaviors are habitual and which are not. There are no extant studies that have investigated the automatic nature of secure behaviors. Therefore, a rigorous and exhaustive approach needs to be taken to identify secure behaviors which are habitual and worth measuring before a full-scale study is deployed.

According to the variance model on TTAT, the positive feedback loop will be used by individuals initially to assess the threat and coping mechanisms, which will eventually lead to the performance of coping behavior. This study hypothesizes that once this loop is performed repetitively, habitual behavioral patterns may emerge. When these

المنارة للاستشارات
www.manaraa.com

patterns emerge, the behavior will skip the positive feedback loop and initiate the habit loop when it reaches the coping stage.

Figure 2.10 illustrates how the habit loop will be created at the coping stage of the positive feedback loop when the same behavior is repeated under a stable context. Once the feedback loop continues at a given point of time, the coping behavior will become an automatic response to a stimuli or environmental cue. An environmental trigger will activate the habit loop instead of the threat perceptions that usually lead to coping appraisal and eventually coping behavior. The habit loop will be initiated by a trigger, followed by the actual coping behavior, before approaching the rewards stage. The loop will then continue until it is disturbed. The positive feedback loop will cease to function due to the habit loop that is created by the formation of habit.

المنارة للاستشارات

www.manaraa.com

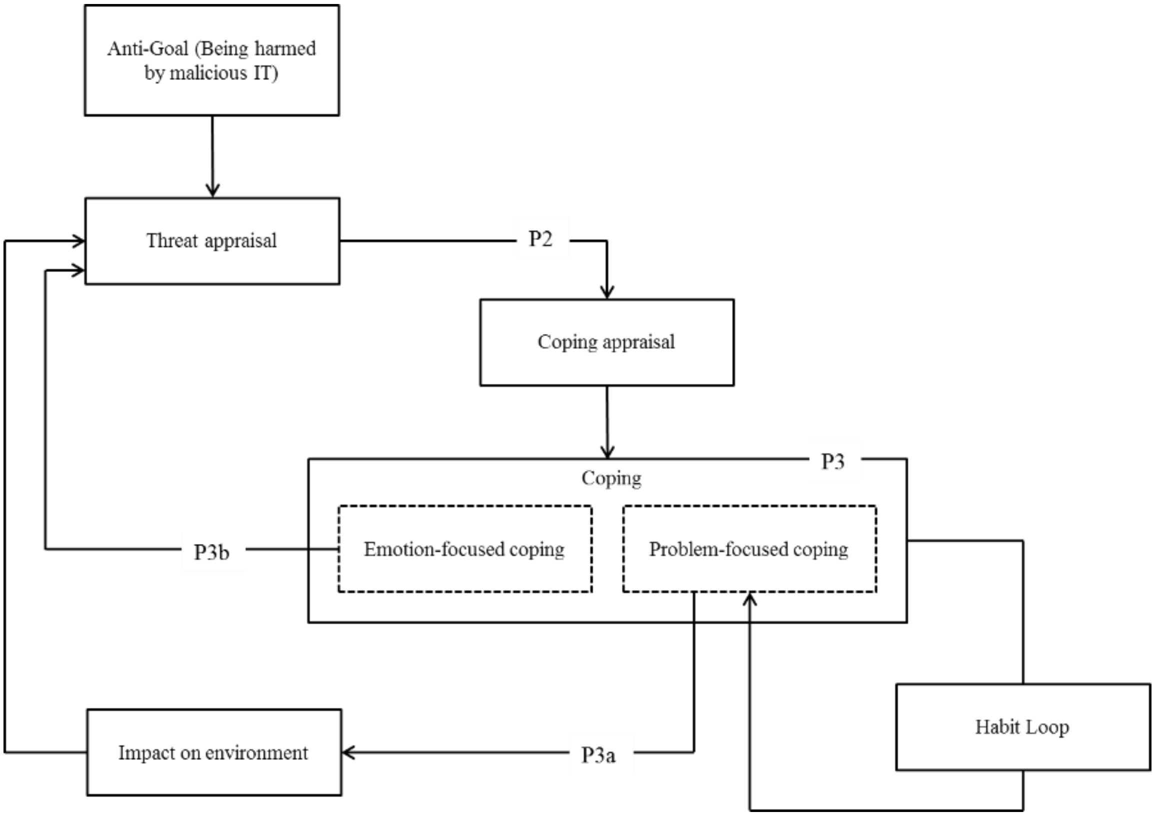


Figure 2.10 Extended TTAT Process Model

Note: Adopted from Liang and Xue (2009) and extended with habit loop

Once habits are formed, the threat and coping appraisal processes will have little impact on the actual behavior that is performed. However, the positive feedback loop will spring into action when the habit loop is disturbed. An example of a disruption in the habit loop is when an individual does not receive satisfaction or a reward following the performance of a habitual behavior. In that case, since the automatic behavior is not satisfactory or rewarding, the positive feedback loop will be reactivated, creating new threat perceptions and coping appraisals. This will be followed by coping behavior performed after intentions are created. Different individuals are likely to perceive the same threat differently. Some individuals may perceive the threat of unauthorized access

www.manaraa.com

to their computer to be severe with dire consequences. Others may view that as a minor threat not requiring any coping behavior. Similarly, some individuals are likely to form habitual behaviors quickly while others may be slow or may not develop any habitual behavior.

Model and Hypotheses

Based on the Technology Threat Avoidance Theory (TTAT), Protection Motivation Theory (PMT) and Habit Theory, this study proposed a research model to explain the influence of threat appraisal and coping appraisal on behavioral intentions and the influence of behavioral intentions on performing secure behavior. Primarily, this model assessed the moderating influence of habit on the relationship between behavioral intention and actual secure behavior. Similar to extant IS security literature where PMT is utilized in a variance model, this study tested the influence of PMT variables in a cross sectional manner to assess the influence of threat appraisal and coping appraisal on behavioral intentions. Additionally, the relationship between behavioral intention and behavior is assessed along with the influence of habit on that relationship. Figure 2.11 shows the conceptual research model that utilizes the PMT and Habit Theory. Rogers (1983) suggests that threat appraisal variables: perceived threat vulnerability and severity, will positively influence behavioral intentions along with coping appraisal variables: response efficacy, self-efficacy and response cost.

المنارة للاستشارات
www.manaraa.com

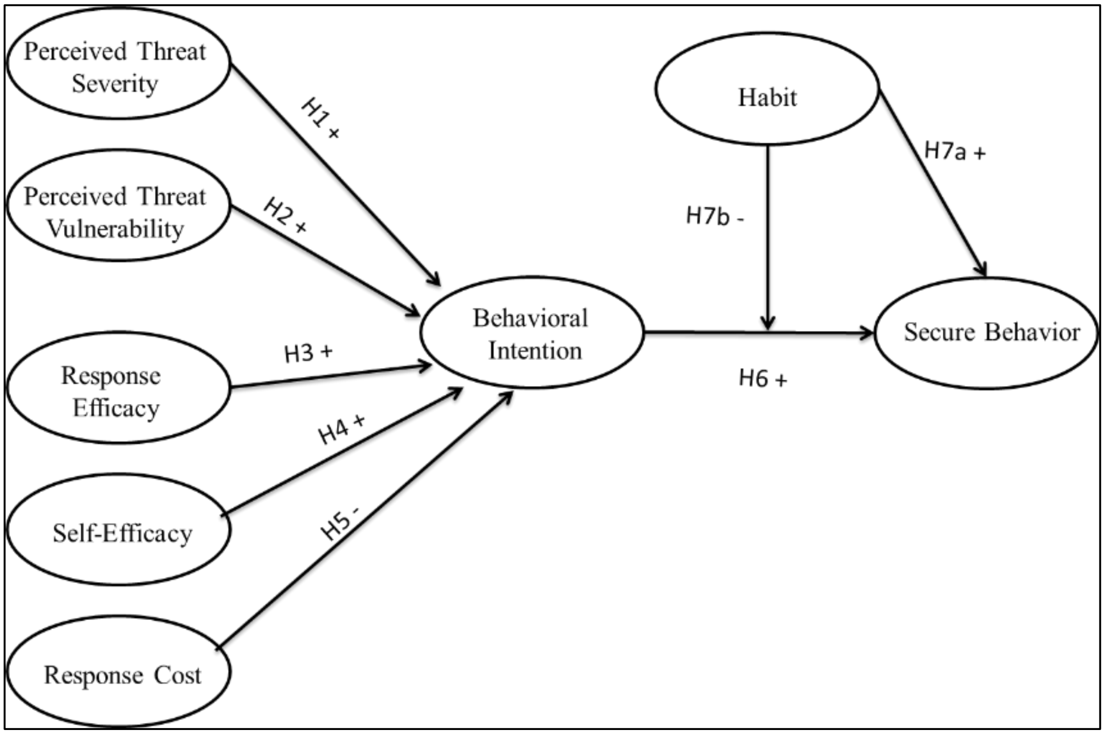


Figure 2.11 Conceptual Research Model

The present study included the threat and coping appraisal variables as direct antecedents of behavioral intention. Similarly, the relationship between behavioral intention and actual behavior relationship as posited by TRA and TPB, is reflected in the research model. This is consistent with PMT (Rogers 1983) and several other research studies in information security that utilized PMT.

In order to measure the role of habit on information security behaviors, habit is positioned in two different ways. First, habit is positioned to directly influence actual behavior. TRA and TPB suggest that behavioral intentions influence actual behavior and a meta-study found that 28 percent of the variance of actual behavior was explained by behavioral intentions (Sheppard et al. 1988). This also means that other factors may

المنارة للاستشارات
www.manaraa.com

influence behavior directly. Habit has been studied as a variable that directly influenced behavior, and in some cases it was found to be a stronger predictor of actual behavior than behavioral intentions (Saba et al. 2000; Towler and Shepherd 1991). It is conceivable that habit would influence behavior directly in the context of information security. Therefore, habit is positioned as a direct effect on secure behavior.

Habit is also positioned as a moderator variable that suppresses the intention-behavior relationship. Prior research on habits suggest that when behaviors are performed repetitively and in a satisfactory manner, they "may lose its reasoned character" (Verplanken et al. 1998, p. 113). These studies also suggest that when habits are strong, intentions were not a strong predictor on behavior, but when habits were weak or nonexistent, behavioral intentions played a major role in predicting behavior (Wood et al. 2002). Consistent with those findings, Limayem and Hirt (2003) and Limayem et al. (2007) suggested that the most appropriate way to capture automaticity is to position habit as a suppressor variable of the intention-behavior relationship. Similarly, habit is also positioned as a moderator variable of the intention-behavior relationship in the research model of this study. Thus, when a certain information security behavior becomes habitual, the influence of threat and coping appraisals would have minor impacts on the actual behavior mediated by intentions.

Threat Appraisal

In the research model model, threat appraisal, which comprises of perceived severity and perceived vulnerability, is articulated as a direct determinant of behavioral intent. Perceived threat severity refers to the extent to which an individual perceives that negative consequences caused by the threat will be severe. Therefore, when a person

المنارة للاستشارات

www.manaraa.com

believes that the threat is severe, he or she is more likely to follow the recommended actions (Rogers 1975; Witte 1992). In this study, it was expected that individuals will identify threats such as unauthorized access of their computer at work, computers getting infected by malware or an unintended individual receiving an email with sensitive data. Previous literature suggests that perceived threat severity is a factor that significantly influences behavioral intent to perform secure behavior in order to deter threats. Although some studies had inconsistent findings (Ifinedo 2012), Crossler (2010), Herath and Rao (2009), Johnston and Warkentin (2010), Lee and Larsen (2009), Lee (2011), Liang and Xue (2010) and Woon et al. (2005) found that perceived threat severity was a significant predictor of their dependent variable. Once a threat is identified, and an individual perceives that threat to be severe, it is expected that he or she would perform the recommended actions to avert the threat. Hence, it is hypothesized:

H1: Perceptions of threat severity will positively influence end user intentions to perform a secure behavior.

Perceived threat vulnerability, which is the perception of the probability of encountering a threat, was also included by Rogers (1975) in the PMT model. A person is likely to adopt the recommended or threat aversive behavior if the individual assesses the probability of exposure to the adverse threat. Perceived vulnerability has been tested extensively in PMT research where perceptions of increased likelihood for a threat to occur have been found to significantly influence intentions to perform the recommended actions (Witte et al. 1996). In the context of this study, it was expected that perceptions of the likelihood of the threats such as unauthorized access to their computer at work, computers being infected with malware, or an unintended individual receiving an email

المنارة للاستشارات
www.manaraa.com

with sensitive data would influence an individual to take evasive action. Previous perceived threat vulnerability is also a factor that significantly influences behavioral intent to perform secure behavior in order to deter threats. However, the results are mixed in different studies, which may be attributed to the context of the studies or simply due to the studies being tested at only one point in time where perceptions may have been changed previously. Ifinedo (2012),Lee and Larsen (2009), and Liang and Xue (2010) found perceived threat vulnerability to be a significant factor, while some other studies did not (Herath and Rao 2009; Johnston and Warkentin 2010; Woon et al. 2005). However, exploration of previous literature on PMT suggests that perceived threat vulnerability, while context specific, significantly influences the behavioral intention to perform secure behavior. Therefore, it is hypothesized:

H2: Perceptions of threat vulnerability will positively influence end user intentions to perform secure behavior.

Coping Appraisal

In addition to the severity of a threat and the vulnerability of a threat, an individual evaluates the effects or efficacy of adopting the recommended behavior in coping appraisal. Response efficacy refers to the extent to which a person believes that by adopting the recommended behavior, a threat can be prevented (Rogers 1975; Witte et al. 1996). If individuals perceive a threat, such as unauthorized access to their computers when left unattended will result in negative consequences, they are likely to consider ways to protect their computers from unauthorized access. Locking the computer terminal is a known method to prevent unauthorized access to the computer terminal when it is left unattended (Microsoft 2012). Since locking a computer terminal is perceived as an

المنارة للاستشارات
www.manaraa.com

effective method to avert the threat of unauthorized access to a computer, the greater perceived response efficacy will result in increased likeliness of adopting the recommended behavior. Most of the prior studies that utilized PMT in the context of information security found that response efficacy had a significant impact on behavioral intentions to perform secure behavior (Anderson and Agarwal 2010; Crossler 2010; Herath and Rao 2009; Ifinedo 2012; Johnston and Warkentin 2010; Lee and Larsen 2009; Workman et al. 2008). PMT literature also suggests that augmented levels of response efficacy are associated with increased behavioral intentions. With this argument, response efficacy is hypothesized as follows:

H3: Response efficacy will have a positive effect on end user intentions to perform secure behavior.

In coping appraisal, self-efficacy also directly influences behavioral intent. If an individual believes that an action is easy to perform and is confident in his or her ability to adopt and perform a recommended action, they are more likely to adopt that action (Bandura and Adams 1977). Rogers (1983) extended the PMT model with self-efficacy, where it was viewed as a determinant of intent concerning a recommendation to address a threat. Several studies have found that self-efficacy has a significant impact on behavioral intent of conducting protective actions. Milne et al. (2000) suggests that self-efficacy was the PMT variable that had the strongest relationship with behavioral intention in a meta-analysis of past PMT research studies. Several research studies in the context of information security found significant relationship between self-efficacy and behavioral intentions (Anderson and Agarwal 2010; Crossler 2010; Herath and Rao 2009; Ifinedo 2012; Johnston and Warkentin 2010; Lee and Larsen 2009; Lee 2011; Liang and Xue

المنارة للاستشارات
www.manaraa.com

2010; Woon et al. 2005; Workman et al. 2008). If an individual perceives that the behavior of locking the computer whenever leaving it unattended is not difficult to perform, they are more likely to adopt that behavior. Hence it can be hypothesized:

> *H4: Self-efficacy will have a positive effect on end user intentions to perform secure behavior.*

Response cost refers to any costs, such as time, money, and inconvenience associated with performing a secure behavior to cope with a threat (Floyd et al. 2000). When an individual perceives the related costs of performing a behavior, it will lead to reduced behavioral intentions. Previous IS security literature suggests that response cost is a significant factor that influences behavioral intention negatively (Herath and Rao 2009; Lee and Larsen 2009; Liang and Xue 2010; Woon et al. 2005). Several studies that utilized PMT in the context of information security did not employ response cost in their research models (Anderson and Agarwal 2010; Johnston and Warkentin 2010). However, for the purposes of this study, response cost is regarded as an appropriate variable which needs to be tested. While habits are formed when a behavior is performed repetitively in a successful manner, when individuals perceive costs related to the behavior performed, they are less likely to form behavioral intentions that will eventually lead to habit formation. Therefore, response cost is hypothesized as follows:

> *H5: Response Cost will have a negative effect on end user intentions to perform secure behavior.*

Behavioral Intention and Behavior

Prominent research models such as TRA and TPB suggest that once behavioral intentions are formed by an individual, they are likely to perform a behavior based on

المنارة للاستشارات
www.manaraa.com

those intentions. Behavioral research theories in IS such as TAM and UTAUT have confirmed these suggestions by finding empirical support of the intention-behavior relationship. This relationship has also been confirmed by a large number of IT adoption studies as well as many other behavioral studies in psychology (Fishbein and Ajzen 1975; Venkatesh et al. 2003). Consistent with prior research, it is argued that users who have stronger behavioral intentions are more likely to engage in the performance of secure behavior. Therefore, it is hypothesized:

H6: Behavioral intention will have a positive effect on secure end user behavior.

Direct and Moderating Effects of Habit

Previous research utilizing PMT has modeled behavioral intention as the dependent variable and has tested the influence of threat and coping appraisal along with other possible independent variables on behavioral intention. One of the most important aspects that has been overlooked in PMT research is that many of the behaviors studied are repetitive in nature and may have already been a routine or habitual behavior at the time of study, given that users were in a post-adoption stage (Verplanken et al. 1997). Failing to capture this important element in fact may have biased the findings of previous PMT research. For example, studies that measured individuals' behavioral intentions to perform secure behaviors, such as anti-spyware usage or backing up data in a cross-sectional manner, may have flawed findings since the behavior may have been repeated many times previously in a successful manner (Crossler 2010; Johnston and Warkentin 2010; Lee 2011; Malimage and Warkentin 2010). The influence of behavioral intentions are weakened when habits are strong, thus the prior studies have not accounted for the influence of habit. While most of the extant IS literature including IS security research

للاستشارات المنارة

www.manaraa.com

has used behavioral intentions as a proxy for actual behavior (D'Arcy et al. 2009), the studies that measured actual behaviors have usually ignored the direct influence of habit on actual behavior. Mittal (1988) found that habit and behavioral intentions directly influenced actual behavior of wearing seatbelts. In a research related to food consumption, Tuorila and Pangborn (1988) found that both habit and behavioral intentions were predictors of actual behavior. Saba et al. (2000) and Towler and Shepherd (1991) had similar findings in their research studies related to food consumption.

Limayem and Hirt (2003), in a research that explored WebBoard usage found that habit directly influenced actual usage behavior of WebBoard. They also found that habit's influence on behavioral intention was mediated by affect. Although Limayem et al. (2007) focused primarily on the suppression effect of habit, in a comparison model they found that habit had a significant direct influence on actual behavior as well. The direct effect of habit has scarcely been explored in IS and has never been explored in the context of information security. When habits are present, it is important to note that it can be a major predictor of actual behavior along with behavioral intentions. With that argument it is hypothesized that:

H7a: Habit will have a positive effect on secure end user behavior.

Once an individual repeats the same behavior satisfactorily over and over again, the increasing automaticity of the behavior is known to suppress the need for an individual to engage in cognitive processing (James 1890). Therefore, when the previous studies measured behavioral intention to perform a certain behavior, the behavior may have already been habitual and the intentions may have been attenuated. Wood et al. (2002) found that when strong habits were present, behavioral intentions had a weak

المنارة للاستشارات

www.manaraa.com

influence on actual behavior and it was the opposite when habits were weak. The widely accepted definition of habit by Verplanken et al. (1998) implies that the automatic nature of habit creates a moderating effect on the intention-behavior relationship as well. Limayem et al. (2007) suggested that while habit has been utilized as a mediator and a direct effect, in order to capture the true essence of habit, it has to be positioned as a suppressor variable of the intention-behavior relationship. In extreme circumstances, habitual behavior may become very strong to the point that intention will not have any influence on the actual behavior. In such instances, behavioral intention becomes influential only when the threat-response becomes unsatisfactory or when behavioral conditions change such as when a fear appeal is introduced. Moreover, behavioral intention will regain its influence on actual behavior by reducing the effect of habit (Limayem et al. 2007).

This type of suppression relationship has not been studied in the context of IS security and sparsely tested in IS continuance literature. Limayem et al. (2007) and Limayem and Cheung (2011b) found that habits significantly moderated the relationship between behavioral intentions and actual behavior consistent with the widely accepted definition on habit. Based on this argument, it is hypothesized that:

H7b: Habit will negatively moderate (suppress) the relationship between behavioral intention and behavior.

Summary

From the literature review, it can be concluded that there is a significant gap in behavioral IS security research in terms of exploring the role of habit in security behaviors. The extant study that investigated the role of habit in IS security behaviors did

المنارة للاستشارات
www.manaraa.com

not take into account, the automatic nature of habit. Using PMT, which is commonly applied in many behavioral security researches, a conceptual research model was developed which served to explain the influence of threat and coping appraisals on behavioral intention and the moderating influence of habit on the intention-behavior relationship. From this model, hypotheses were developed that articulate the relationships among the different variables in the model. The next chapter will explain the method used to measure the variables in the conceptual model.

المنارة للاستشارات
www.manaraa.com

CHAPTER III

METHODS

Chapter III provides a detailed discussion of the methods that was employed in this study for analyzing the research model. The chapter begins with a review of the independent and dependent variables included in the proposed conceptual model. The review of the variables includes their definitions, original source and scale items for each of the variables. Next, a description of this study's data collection instrument design is followed by a description of data collection method. An overview of the study's two-phase investigation procedure is initiated with the description of the preliminary investigative procedure which includes details of tests of validity and reliability and the pilot test. Finally, the plan used for the primary investigation phase of this study is provided, including details of the data collection procedure and sampling frame.

Variables

The Technology Threat Avoidance Theory (TTAT), the Protection Motivation Theory (PMT) and the Habit Theory literature provides the theoretical foundation for our study. TTAT, which is developed as a process model and tested as a variance model, provides the early insights into how habits can be formed when a certain secure behavior is performed repetitively. PMT, which has been extensively studied in an information security context, provides the theoretical basis to test the role of habit on information

المنارة للاستشارات

www.manaraa.com

security behaviors. Previous information security research studies that utilized PMT did not take into account that certain security behaviors, when performed repetitively in a stable context, may become habitual. Our study aims to fill this research gap by investigating the role of habit in information security behaviors by utilizing PMT. As discussed in Chapter II, PMT consists of two main components: threat appraisal and coping appraisal. The threat appraisal process consists of perceived threat severity and vulnerability and the coping appraisal consists of self-efficacy, response efficacy and response cost (Floyd et al. 2000). Perceived threat severity refers to the level of the potential impact of the threat. When an individual believes the consequences of exposure to the threat (when not adopting the intended actions) are severe, he or she is more likely to perform secure behaviors to prevent the threat. Perceived threat vulnerability is defined as the perceived probability of encountering the threat or the degree to which an individual believes the threat is possible. A person is increasingly likely to adopt the recommended behavior if the individual assesses a high probability of exposure to the adverse threat (Witte et al. 1996).

In the coping appraisal, individuals evaluate the effects or efficacy of adopting the recommended behavior. Response efficacy refers to an individual's belief that the act of adopting the recommended behavior will prevent or avert the threat (Rogers 1975; Witte 1992). Self-efficacy is defined as the degree to which an individual believes he or she is able to perform the recommended secure behavior to avert the threat (Bandura and Adams 1977; Rogers 1983). Response cost refers to the perceived costs associated with performing a secure behavior (Floyd et al. 2000). Some individuals may perceive that performing secure behavior such as backing up data, scanning the computer for viruses or

المنارة للاستشارات
www.manaraa.com

spyware, changing passwords regularly and logging off the computers as an inconvenience, thus skipping on those secure actions.

Apart from the PMT threat and coping appraisal variables, which are independent variables predicting behavioral intention in the conceptual model, habit is another independent variable included in the conceptual model that predicts actual secure behavior and suppresses the relationship between behavioral intention and actual behavior. There is an ongoing debate about the definition of habit where certain scholars define it as the frequency of past behavior and other scholars define it as the automaticity of behavior. For the context of this study, habit is defined as "learned sequences of acts that become automatic responses to specific situations, which may be functional in obtaining certain goals or end states" (Verplanken et al. 1997). Therefore, it can be assumed that when individuals develop habits, they are more likely to perform certain secure behaviors automatically. It can also be assumed that when habits are developed, behavioral intentions will not be the major driver of actual behavior because the automaticity aspect of habit reduces cognitive processing.

In summary, this study measured six independent variables that are used in the main conceptual model. These variables are Perceived Severity (PSEV), Perceived Vulnerability (PVUL), Response Efficacy (REFF), Self-Efficacy (SEFF), Response Cost (RCST) and Habit (HABT). All the independent variables including habit were measured through pre-validated self-reported scales. Habits by definition are unconscious or automatic. Therefore, utilizing self-reports to measure habit has been questioned by some critics (Klockner and Matthies 2012). However, Verplanken and Orbell (2003) state that if appropriately measured, the degree to which an individual perceives a certain

المنارة للاستشارات
www.manaraa.com

behavior they perform to be habitual can be obtained. Use of self-reports to measure habits will be discussed later in this chapter. Table 3.1 lists each of the independent variables used in the conceptual model along with their definitions within the context of this study.

Table 3.1 Independent Variables and Their Definitions

Variable	**Definition**
Perceived Threat Severity (Johnston and Warkentin, 2010)	The degree to which an individual believes a threat to be severe.
Perceived Threat Vulnerability (Johnston and Warkentin, 2010)	The degree to which an individual believes a threat to be probable.
Response Efficacy (Johnston and Warkentin, 2010)	The degree to which an individual believes a recommended response will efficiently and effectively avert a threat.
Self-efficacy (Johnston and Warkentin, 2010)	The degree to which an individual believes he or she is able to perform a recommended action.
Response Cost (Bulgurcu et al., 2010)	The degree to which an individual believes performing a behavior would result in unfavorable consequences.
Habit (Verplanken et al. 1998)	The degree to which an individual believes he or she performs a recommended response automatically.

One of the dependent variables used in this study is behavioral intention, which is an individual's intention to perform the recommended response to avert the potential threat. Theory of Reasoned Action (TRA) by Fishbein and Ajzen (1975) posits attitude as one of the most significant predictors of behavioral intention. However, technology acceptance models and other behavioral models have refrained from including attitude as a main predictor of intentions due to lack of predictive power (Davis 1989; Venkatesh et

www.manaraa.com

al. 2003, 2012). Herath and Rao (2009) ascertained that attitude was not a significant predictor of intentions to comply with security policies when tested with PMT variables. Most of the prior research across all disciplines that utilized PMT has modeled the threat and coping appraisal to directly predict behavioral intention but not mediate attitude. Similarly, this study also hypothesizes that threat and coping appraisal variables will directly influence behavioral intention.

Most extant IS security literature utilizing PMT has measured behavioral intention rather than actual behavior as the ultimate dependent variable. This study measured both intention and actual behavior in order to test the relationship between the two variables. These variables also assisted in measuring the suppressing effect of habit on the intention-behavior link and the direct effect of habit on actual behavior. Although behavioral intentions have been measured through self-reports, measuring actual behavior in a similar manner has been criticized by researchers. Actual behavior is usually difficult to measure and in the information security context, it is almost impossible to collect actual data related to secure behaviors (Crossler et al. 2013; Warkentin et al. 2012). Recent information security studies that utilized actual behavior as a dependent variable have operationalized it using self-reported scales (Crossler 2010; Gurung et al. 2009; Lee and Larsen 2009; Lee 2011; Liang and Xue 2010; Ng et al. 2009; Pahnila et al. 2007; Woon et al. 2005; Workman et al. 2008). This is an indication that self-reports for actual usage is gaining acceptance in the information security research, especially due to the challenges of measuring actual secure behaviors. Therefore, actual behavior for our study is measured utilizing self-reported scales which were previously validated. Table 3.2 provides the two dependent variables included in this study.

المنارة للاستشارات
www.manaraa.com

Table 3.2 Dependent Variables

Construct	**Definition**
Behavioral Intention (Johnston and Warkentin, 2010)	An individual's intention to perform the recommended response.
Actual Behavior (Myyry et al. 2009)	The self-report of performing a recommended behavior.

Instrument Design

A total of eight constructs were measured in this study using an online survey methodology: actual behavior, behavioral intention, habit, perceived threat severity, perceived threat vulnerability, response efficacy, self-efficacy, and response cost. The constructs were be measured using multi-item scales adopted from validated measures used in IS security research and extant literature on habit. These items were adopted to reflect the context of this study. Table 3.3 summarizes the scale items used for each variable. All these items except for habit were reflective and were measured using a five-point likert scale. The automaticity nature of habit is represented as a second-order formative and first-order reflective scale (Polites and Karahanna 2012; Verplanken and Orbell 2003). The formative habit construct consists of three dimensions: lack of awareness, mental efficiency and uncontrollability. The anchors for the Likert scales range from "Strongly Disagree" to "Strongly Agree." It is also important to note that the dependent variable "actual behavior" was measured using a self-reported scale. The items that are listed in Table 3.3 have been deemed to possess content validity by a panel of instrument experts.

المنارة للاستشارات
www.manaraa.com

Table 3.3 Constructs and Measures of PMT Variables

Construct	Items
Perceived Threat Severity (PSEV) (Witte et al. 1996)	**PSEV1**: If an unauthorized individual accesses my computer, it will be a severe problem.
	PSEV2: It would be a significant problem for me if an unauthorized individual accesses my computer.
	PSEV3: If an unauthorized individual accesses my computer, it will be serious.
Perceived Threat Vulnerability (PVUL) (Witte et al. 1996)	**PVUL1**: Chances of an unauthorized individual accessing my computer are high.
	PVUL2: It is likely that an unauthorized individual may accesses my computer.
	PVUL3: There is a possibility that an unauthorized individual may access my computer.
Response Efficacy (REFF) (Witte et al. 1996)	**REFF1**: Locking the computer will successfully prevent an unauthorized individual accessing my computer.
	REFF2: Locking the computer is an effective solution to prevent an unauthorized individual accessing my computer.
	REFF3: I can prevent an unauthorized individual accessing my computer by locking it.
Self-efficacy (SEFF) (Bulgurcu et al. 2012)	**SEFF1**: I am confident that I have the skills to lock the computer.
	SEFF2: I know I can successfully lock the computer.
	SEFF3: I believe that I have the knowledge necessary to lock the computer.
Response Cost (RCST) (Bulgurcu et al. 2012)	**RCST1**: Locking the computer is a burden.
	RCST2: Locking the computer is inconvenient.
	RCST3: Locking the computer is time consuming.
Behavioral Intention (BINT) (Venkatesh et al. 2003)	**BINT1**: I intend to log off the computer every time I leave it unattended.
	BINT2: I predict that I would log off the computer every time I leave it unattended.
	BINT3: I plan to log off the computer every time I leave it unattended.
Actual Behavior (BEHV) (Myyry et al. 2009; Workman et al. 2008)	**BEHV1**: I always log off the computer every time I leave it unattended.
	BEHV1: I make sure that the computer is locked every time I leave it unattended.
	BEHV1: Locking the computer is something I do, every time I leave it unattended.

www.manaraa.com

Operationalizing Habit

Previous research studies have operationalized habit using different methods. Some studies have measured habit by measuring the self-reported frequency of past behavior. This operationalization has been criticized for several reasons. Although the history of repetition may be a key component of habit formation, repetition itself does not habituate behaviors. It is also unlikely that a linear relationship between habits and behavioral frequency exists, since that would imply that the more times an individual have repeated a behavior, the more habitual it would be (Chiu et al. 2012). Self-reported frequency measures can also be unreliable since respondents are required to recall performances of their past behavior. For example, respondents may not be able to remember how many times they locked the computer when it was left unattended.

Response frequency (RF) measure has also been utilized by researchers to measure habit (Verplanken et al. 1994). Using this measure, respondents are presented with hypothetical choice situations and within a limited time period (e.g. 10 seconds), they are required to choose behavioral options (Verplanken 2006). This measure also has its limitations. It is not practical to employ self-administered questionnaires in a controlled environment where the respondents are under time pressure and it requires pretesting for every new habit (Chiu et al. 2012). The RF measure strains the respondents due to the limited time frame which biases the results (Klockner and Matthies 2012). Other methods to measure habit such as experiments, Electroencephalogram (EEG) and functional Magnetic Resonance Imaging (fMRI) have been suggested (Dimoka 2012), but all these methods have limitations such as lack of realism. Behaviors are habituated when they are performed successfully and repetitively in a stable context. When habit is

المنارة للاستشارات
www.manaraa.com

measured with any of the above mentioned methods, the behavior will be measured in a controlled and unrealistic environment (Dennis and Valacich 2001), which removes the stable context required for habits to be performed.

With the given limitations of alternate methods and a highly validated self-report scale, operationalizing habit as a self-reported perception appears to be gaining acceptance in the IS discipline (Limayem and Cheung 2011; Limayem et al. 2007; Polites and Karahanna 2012; Vance et al. 2012; Venkatesh et al. 2012). Self-report habit index (SHRI) is a 12-item instrument scale developed by Verplanken and Orbell (2003), that has been used by many researchers to measure habit. The SHRI has been revalidated by many scholars showing excellent internal reliability and convergent validity. For the purposes of this study, a scale developed by Polites and Karahanna (2012), which is based on the SHRI, is utilized to measure habit. As mentioned previously, habit is positioned as a second-order formative and first-order reflective scale. By the definition and the automatic nature of habit, it constitutes of the following three dimensions which are measured as the first-order reflective constructs (Polites and Karahanna 2012). Figure 3.1 illustrates this multi-dimensional nature of habit.

1. **Lack of awareness** - The behavior is performed automatically or without much awareness. (e.g., I lock the computer every time I leave it unattended, without being aware of doing it)

2. **Mental efficiency** - The behavior is performed without thinking or using less cognitive processing. (e.g., I lock the computer without thinking, every time I leave it unattended)

المنارة للاستشارات
www.manaraa.com

3. **Uncontrollability** - The behavior is hard to control. (e.g., I would find it hard not to lock the computer, every time I leave it unattended)

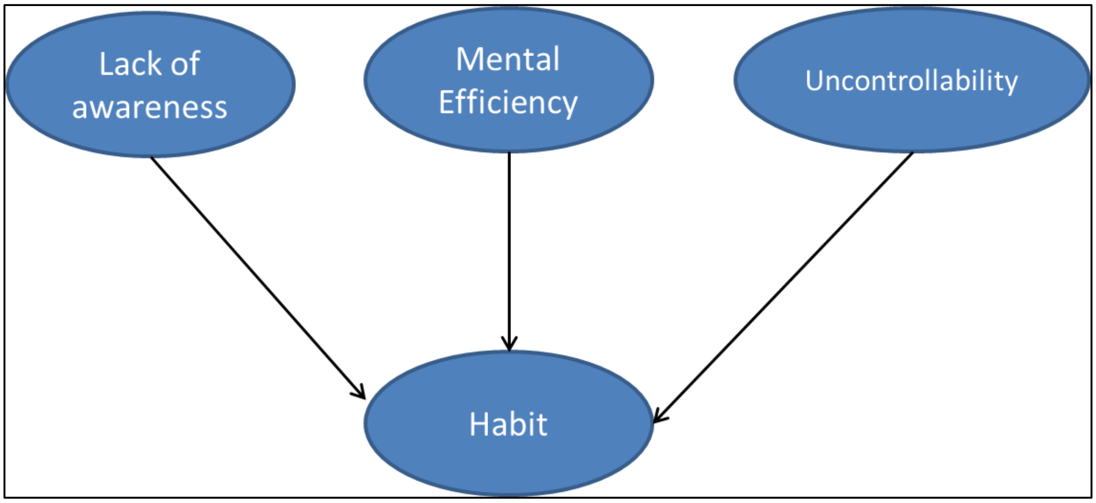


Figure 3.1 Multi-dimensional Nature Of Habit

Although there are several validated scales to measure habit through self-reports such as the self-report habit index (SHRI) by Verplanken and Orbell (2003), the developed habit scale by (Limayem et al. 2007) and the UTAUT2 habit scale by Venkatesh et al. (2012), items to measure habit were primarily adopted from Polites and Karahanna (2012) since they capture the multidimensional nature of habit. Habit is conceptualized as a second-order formative and first-order reflective construct similar to Polites and Karahanna (2012). Habit was also conceptualized and validated as a three-item reflective scale by Limayem et al. (2007). Although the multi-dimensional scale of habit was primarily utilized in this study, items from the reflective scale of habit were also measured to increase the validity of the research model. The items from Polites and Karahanna (2012) and Limayem et al. (2007) were modified to fit the context of IS

www.manaraa.com

security and to reflect the behavior that was being measured. These items are shown in Table 3.4.

Table 3.4 Measures of The Habit Variable

Construct	**Items**
Lack of Awareness (AWAR) (Polites and Karahanna 2012)	**AWAR1**: Every time I leave my computer unattended, I choose to lock it without even being aware of doing it.
	AWAR2: Every time I need to leave my computer unattended, I unconsciously lock it.
	AWAR3: Locking the computer every time I leave it unattended is something I do without being aware.
	AWAR4: Locking the computer every time I leave it unattended is something I do unconsciously.
Uncontrollability (CTRL) (Polites and Karahanna 2012)	**CTRL1**: I (would) find it difficult to overrule my impulse to lock the computer every time I leave it unattended.
	CTRL 2: I (would) find it difficult to overcome my tendency to lock the computer every time I leave it unattended.
	CTRL 3: It would be difficult to control my tendency to lock the computer every time I leave it unattended.
	CTRL 4: It is [would be] hard to restrain my urge to lock the computer every time I leave it unattended.
Mental Efficiency (EFFCH) (Polites and Karahanna 2012)	**EFFCH1**: I do not need to devote a lot of mental effort to decide to lock the computer every time I leave it unattended.
	EFFCH 2: It would require effort not to lock the computer every time I leave it unattended.
	EFFCH 3: Choosing to lock the computer every time I leave it unattended requires little mental energy.
	EFFCH 4: I have no need to think about locking the computer every time I leave it unattended.
Habit (HBT) (Limayem et al. 2007)	**HBT1**: Locking the computer every time I leave it unattended has become automatic to me.
	HBT2: Locking the computer every time I leave it unattended is natural to me.
	HBT3: When leaving the computer unattended, locking it is an obvious choice for me.

Habit is conceptualized as a second-order formative and first-order reflective construct similar to Polites and Karahanna (2012). Habit was also conceptualized and

المنارة للاستشارات
www.manaraa.com

validated as a three-item reflective scale by Limayem et al. (2007). Although the multi-dimensional scale of habit was primarily utilized in this study, items from the reflective scale of habit were also measured to increase the validity of the research model. The items from Polites and Karahanna (2012) and Limayem et al. (2007) were modified to fit the context of IS security and to reflect the behavior that is being measured.

Habit and Inertia

Polites & Karahanna (2012) investigated how incumbent system usage negatively impacted new system perceptions and usage intentions, using status quo bias and habit literature to theoretically guide their study. One of the key constructs in their research model is inertia. Inertia is defined as the "attachment to, and persistence of, existing behavioral patterns (i.e., the status quo), even if there are better alternatives or incentives to change" (Polites and Karahanna 2012, p. 24). They hypothesize that habitual use of an incumbent system, rationalization due to perceived transition costs, and psychological commitment due to perceived sunk costs, influence the development of inertia.

While incumbent system habit may lead to inertia, and inertia may negatively influence the adoption of a new system in the context of a post-adoption setting, there is a clear distinction between the motivation and context of Polites & Karahanna and this dissertation. Polites & Karahanna (2012) investigates the role of habit in inhibiting change while this dissertation investigates the role of habit in information security behaviors in the workplace. Another distinction between the two studies is that Polites & Karahanna (2012) test the influence of inertia of an 'old' behavior (using email) in inhibiting the adoption of a 'new' behavior (using GoogleDocs), while this dissertation study simply focused on three current secure behaviors performed by employees. These

المنارة للاستشارات

www.manaraa.com

three behaviors are recommended responses to three different threats and the sole purpose of investigating different behaviors is to identify if habit impacts these behaviors differently. Each of the response behaviors is related to a specific threat. These behaviors are not interchangeable and not presented with another alternative behavior in mind.

Polites & Karahanna (2012) have hypothesized that habit will positively influence inertia and that inertia will negatively influence intention to use a new system. While they recognized that habitual behaviors occur outside of awareness, they have modeled inertia to mediate the habit-intention relationship. Limayem et al. (2007, p. 717) posits that modeling habit as an indirect effect of actual behavior has both "theoretical and empirical shortcomings." This dissertation modeled habit as an antecedent of actual behavior while it is hypothesized that habit negatively moderates the intention-behavior relationship, which reflects the automatic nature of habit. Polites & Karahanna (2012, p. 38) recognized this limitation in their study and suggested that future studies examine the impact of habit "on actual new system usage, via the intention-behavior link." They suggest that there would be a stronger direct link between habit and actual behavior than the habit-intention relationship being mediated though inertia. This dissertation tested the habit-behavior relationship as recommended by Polites & Karahanna (2012).

This dissertation study is a cross-sectional study that focused on existing habits or current habitual behaviors. Habit is a process; therefore, it is ideally investigated through a longitudinal study. When a new behavior is performed, behavioral intentions play a significant part in the performance of that behavior. Once this behavior is performed successfully and repetitively in a stable context, over time it will become habitual and the power of intentions dissipates. Polites & Karahanna (2012) suggested that inertia is more

المنارة للاستشارات
www.manaraa.com

evident in the persistence of inefficient practices. In terms of secure behaviors, investigation of inertia in the context of breaking habits or forming habits would be applicable in a longitudinal study, especially when it concerns negative habits (inefficient practices).

Polites & Karahanna (2012) also identified that habit and inertia are clearly distinct constructs while criticizing the use of these two constructs interchangeably by past literature. The definition of inertia as "attachment to, and persistence of, existing behavioral patterns," however, may imply a relationship with habit. Habits are also routine behaviors or behavioral patterns that are carried out repetitively. Polites & Karahanna (2012, p. 25) clearly defines habit as automatic but states that "inertia may have both conscious and subconscious origins." They also state that the existence of better alternatives is not a necessary condition for the existence of inertia. Although inertia may not be applicable in the context of this dissertation, considering the possible relationship between inertia and habit, inertia was be measured and utilized for post hoc analysis of this study. Polites and Karahanna (2012) measures inertia from three different aspects: behavior-based, cognitive-based and affective-based. Behavior-based inertia is defined as the continuance of a behavior without giving it much thought, simply because it is part of a routine. Cognitive-based inertia is defined as the conscious decision to continue performing a behavior even when an individual is aware that the behavior is not the most effective way of doing things. Affective-based inertia is defined as the continuance of a behavior since it is stressful to chance, enjoyable and an emotional attachment exists to that behavior. However, only behavior-based inertia and affective-based inertia will be measured since cognitive-based inertia construct is not applicable in

المنارة للاستشارات
www.manaraa.com

the context of this study.However, only behavior-based inertia and affective-based inertia will be measured since cognitive-based inertia construct is not applicable in the context of this study.

During the post hoc analysis, the influence of habit on inertia and the influence of inertia on a current behavior in an information security context can be tested. Moreover, tests can be performed to investigate the moderating influence of habit on the intention-behavior relationship, in the presence of inertia as an antecedent of behaviors intentions.

The items to measure inertia are shown below. The language was modified to reflect the secure behavior of locking the computer when leaving it unattended.

Table 3.5 Measures of Inertia

Construct	**Items**
Inertia – Affective Based (Polites and Karahanna 2012)	I continue to lock my computer whenever I leave it unattended
	INAF1: because it would be stressful to change.
	INAF2: because I am comfortable doing so.
	INAF3: because I enjoy doing so.
Inertia – Behavioral Based (Polites and Karahanna 2012)	I continue to lock my computer whenever I leave it unattended
	INBB1: simply because it is what I have always done.
	INBB2: simply because it is part of my normal routine.
	INBB3: simply because I have done so regularly in the past.

Identification of Habitual Secure Behaviors

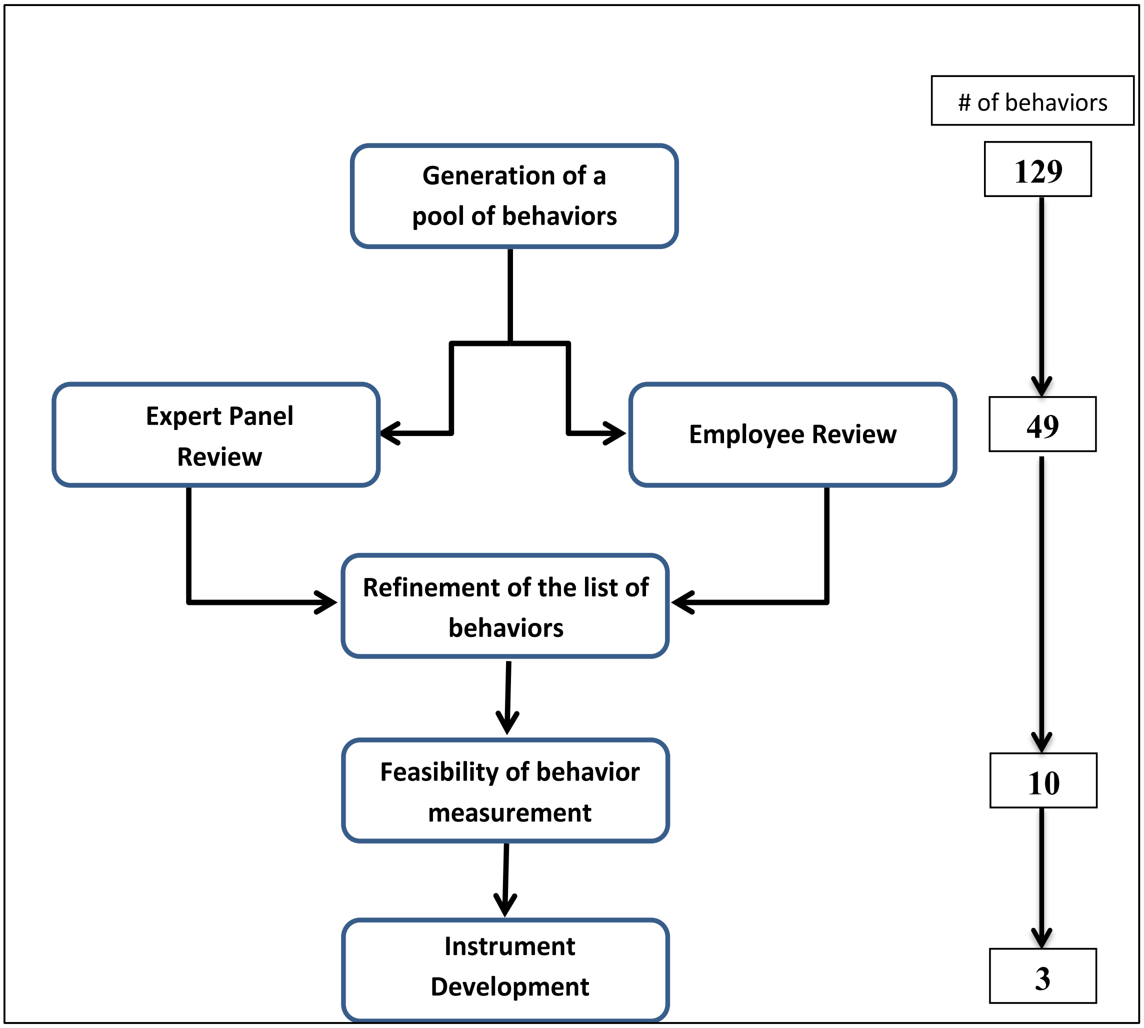
Information security behaviors can be routine and repetitive and when they are performed successfully in a stable context they can become automatic, therefore habitual. As discussed in chapter II, repetition or frequency itself does not make a certain behavior habitual. Habit formation requires a repetition of a certain behavior successfully, in a

المنارة للاستشارات
www.manaraa.com

stable context where the behavior is initiated through environmental triggers. If all these factors are not present, habits may not be formed. Therefore, it can be assumed that not all secure behaviors are habitual. Even when certain behaviors can be habitual, the strength of habit can significantly vary between different individuals. Due to the lack of previous information security research that investigated habits, it is challenging to identify behaviors to test the role of habit. Vance et al. (2012) investigated the top five security violations utilizing PMT and habit. They derived a list from security experts and management on the basis of security policy violations and did not consider whether those behaviors were habitual. In terms of behaviors that are investigated, our study differs from the study by Vance et al. (2012) in two important ways. First, our study focused only on positive habitual behaviors related to information security. Vance et al. (2012) followed a hypothetical scenario-based method due to the context of policy violations in their study. Scenario based methods are commonly used in criminology to assess unethical or criminal behavior since it allows the respondents to disassociate themselves from the unethical or non-compliance behavior tested in the instrument (Hovav and D'Arcy 2012; Taylor 2006). The other study which utilized habit in an information security context (Pahnila et al. 2007), collected their data using a web-based survey. Our study focused on positive habits, thus a survey methodology would be able to capture generalizable perceptions of the respondents successfully, although potential limitations such as acquiescence bias exists (Dennis and Valacich 2001; McGrath 1982, 1995; Wyatt 2000). Second, an alternative process was followed to identify information security behaviors that can be habitual from which three behaviors are selected to explore the role

www.manaraa.com

of habit. Figure 3.2 illustrates this exhaustive process which will be discussed in the subsequent pages.



# of behaviors
Generation of a pool of behaviors
129
Expert Panel Review
Employee Review
49
Refinement of the list of behaviors
Feasibility of behavior measurement
10
Instrument Development
3

Figure 3.2 Selection of Habitual Behaviors

Due to the lack of extant literature investigating habitual secure behaviors, it was challenging to identify habitual information security behaviors among employees, which could be utilized to test the research model. In similar challenging situations, Moore and

www.manaraa.com

Benbasat (1991) recommended conducting a step-by-step procedure to select which items to be used in a research instrument. Their recommendations were followed in selecting the behaviors that are relevant to this study. Whereas there are many behaviors that can be investigated, in order to have a parsimonious research design, three behaviors were identified to be utilized for testing the research model. Strength of habits can differ among respondents, thus selecting just one behavior does not provide generalizable results when investigating the role of habit in information security behaviors. The measurement panel was asked to select three secure behaviors, which were deemed to have sufficient range of properties to provide a generalizable and an accurate representation on the role of habit. This rigorous process as recommended by Moore & Benbasat (1991) follows five steps starting from generating a pool of positive secure behaviors and ending with the development of the research instrument. The procedure followed in each step is discussed below.

Step 1: Generation of a pool of behaviors

Churchill (1979) and Moore & Benbasat (1991) recommended compiling a list of items from an exhaustive literature review as the initial stage of instrumentation. Their recommendations were applied in the context of secure behaviors for this study. The first step of the procedures to identify the habitual secure behaviors relevant to this study involved two phases. The first phase was to conduct a thorough literature review of all the information security research studies and identify information security behaviors performed at the workplace that have been explored. The review included articles in prominent journals and research presentations at AMCIS, ICIS and security workshops such as the Dewald Roode Workshop on Information Systems Security Research. The

المنارة للاستشارات

www.manaraa.com

secure behaviors identified from these articles were utilized extensively for the compilation of the list of secure behaviors. The second phase involved a review of practitioner articles on information security such as whitepapers. Secure behaviors that are recommended for corporations by industry experts to be integrated into company-wide security policies were also considered. The behaviors compiled in the two lists were combined which totaled to 129 secure behaviors. A list of secure behaviors and their academic and practitioner sources can be found on Appendix B. After eliminating similar and overlapping behaviors, a final list of 49 secure behaviors was identified. The list of 49 secure behaviors selected to be presented to an expert panel and an employee panel review is shown in Table 3.6.

Table 3.6 List of Behaviors For Expert Panel

#	Behavior
01	Avoid sharing passwords with co-workers.
02	Use anti-spyware software.
03	Backup data regularly.
04	Set up strong passwords to login to systems.
05	Verify regularly that anti-virus and/or anti-spyware software is auto updated.
06	Change passwords often.
07	Locking the computer when leaving it unattended.
08	Always encrypt sensitive information.
09	Immediately apply software updates when they become available.
10	Logoff or shutdown the computer when leaving the office for the day.
11	Shred sensitive documents.
12	Complying with information security policies.
13	Being cautions of emails from unknown sources.
14	Avoid coping sensitive data to portable media (e.g., USB, portable HDD).
15	Avoid revealing sensitive information to outsiders.
16	Avoid installing unauthorized software on your computer.
17	Avoid reading confidential documents that does not belong to you.
18	Report a computer virus immediately.

المنارة للاستشارات
www.manaraa.com

Table 3.6 (Continued)

19	Avoid using a laptop for personal use.
20	Avoid writing down sensitive information on paper.
21	Avoid visiting unknown/suspicious websites.
22	Avoid opening email attachments from unknown senders.
23	Avoid posting sensitive information on social networking sites.
24	Encrypt corporate data before copying to portable media.
25	Avoid leaving sensitive documents at the printer.
26	Avoid clicking URLs on social media links.
27	Always use the most updated version of the browser.
28	Encrypt emails with sensitive data.
29	Regularly verify that the firewall on the computer is active.
30	Always lock the office door when leaving for the day.
31	Avoid leaving important documents at the working area/desk.
32	Avoid responding to emails from unknown sources.
33	Avoid inserting portable media that is not yours into the computer.
34	Keep all sensitive information secure to prevent loss or theft.
35	Avoid using public networks to connect to corporate servers remotely.
36	Avoid discussing sensitive information in public areas (e.g., hallway, elevator).
37	Avoid connecting personal devices (e.g., laptop, tablet) to company network.
38	Ensuring sensitive data entered into the system is accurate.
39	Use corporate email only for work-related activities.
40	Always verify that email is sent only to the intended recipients.
41	Set computer file permissions to prevent unauthorized access.
42	Avoid leaving active computers unattended.
43	Always lock sensitive physical documents in a secure location when not in use.
44	Immediately inform authorities if you discover an information security problem.
45	Do not perform work on a computer under a co-worker’s login session.
46	Always verify with the sender if the email content seem suspicious.
47	Document any changes made in the computer system.
48	Avoid downloading files from unknown websites.
49	Always secure keys and ID badges.

المنارة للاستشارات

www.manaraa.com

Step 2: Expert Panel Review & Employee Panel Review

Step two involved identifying security behaviors that may be habitually performed in the workplace. Churchill (1979) has recommended using experts or focus groups to identify items/behaviors to be used in an instrument. Verplanken and Orbell (2003), used a similar method, where they distributed a list of behaviors to a sample of respondents to identify which of those behaviors are more habitual. This study followed a similar procedure but complemented the primary data with views of an expert panel on which behaviors of their employees were habitual. In order to initiate this step, an online survey that presented the forty-nine secure behaviors was sent to a panel of security experts and information security managers. They were asked to select the behaviors which they thought are performed habitually by their employees. The survey was sent to 18 experts and a total of 12 experts responded.

A similar survey was sent to some selected employees or end users across different corporations who used a computer to complete their daily job tasks. The employee responses were gathered through personal contacts and through Amazon Mechanical Turk. The behaviors that were most selected by the respondents were considered to be habitual and in turn were selected to become candidates for the behaviors to be measured in the final instrument. Utilizing feedback from both a subject-matter expert review panel and an employee panel provides better insights in to habitual behaviors in the workplace and differentiates our study from Vance et al. (2012), where they utilized only an expert panel to select their behaviors. The responses from the expert panel and employee panel are included in Appendix B.

المنارة للاستشارات
www.manaraa.com

Step 3: Refinement of the list of behaviors

Using the data from the expert panel and employee panel reviews, twenty positive secure behaviors that were most selected by the panelists were identified. The respondent scores for each behavior by the expert panel and employee panel was used for this procedure. The identification of several behaviors that varied in habitual strength was similar to the study conducted by Verplanken and Orbell (2003).

From the twenty selected behaviors, information security behaviors that had overlapping similarities in terms of the security context were grouped together as suggested by Petter et al. (2007). For example, the behaviors of locking the door, locking the computer, and logging off the computer were similar and served the same purpose, thus were grouped together.

Expert researchers and members of the committee reviewed the list of behaviors and based on their recommendations the "avoidance" behaviors were rephrased to reflect positive behaviors. The rationale for this change was that an avoidance of a certain behavior did not necessarily constitute habit. By avoiding a certain behavior, an individual may perform an opposite behavior which may be habitual. For example, instead of the behavior "avoid opening email attachments from unknown senders," it was rephrased with "open email attachments only from known/verified senders." The twenty behaviors identified from the two panels and the modified language for the behaviors can be found in Appendix B.

Step 4: Feasibility of behavior measurement

Step four involved presenting the twenty behaviors, which were grouped in the previous stage, to a measurement panel. The measurement panel consisted of three

المنارة للاستشارات
www.manaraa.com

professors with several years of experience in conducting research and data collection utilizing different methodologies. Some of the behaviors which were deemed to be habitual by an expert panel and an employee panel could not have been measured accurately through a survey. Therefore, certain behaviors that were impractical to be measured through a survey needed to be removed. Although it would have been ideal to select several behaviors for the study, members of the measurement panel were asked to select the top three behaviors from the list of twenty that were practical to be measured through a self-reported method such as a survey. The panel was also requested to ensure that no two behaviors from the same group were selected in order to avoid any overlapping behaviors being selected. The measurement panel suggested removing certain behaviors such as 'being cautious not to discuss sensitive information in public areas' as being more relevant to healthcare organizations and not relevant in corporate environments where the data for this study would be collected. They also suggested removing certain behaviors which they believed were not practical to be measured through a survey. Finally, they agreed on three behaviors that they thought were practical to be measured through a survey. The three behaviors selected were not the top behaviors identified by the respondents, instead the measurement panel selected behaviors that are feasible and varied in habit strength such that there would be sufficient variance for data analysis. Table 3.7 lists the three behaviors selected, along with the percentage of respondents that selected these behaviors to be habitual in the expert panel and employee panel.

المنارة للاستشارات
www.manaraa.com

Table 3.7 Behaviors Selected For The Study

#	Behavior	Expert Panel	Employee Panel
7	Lock the computer when leaving it unattended.	64%	67%
40	Verify that email is sent only to the intended recipients.	45%	63%
21	Visit only known/verified websites.	55%	56%

Step 5: Instrument Development

After the three behaviors appropriate to be measured for this study were selected, an initial draft of the three instruments was created. The instrument consists of pre-validated scales for each of the constructs included in the research model. The items were modified to fit the context and the behavior studied. Existing literature recommends that content validity, reliability and discriminant validity tests to be conducted even when pre-validated scales are utilized (Netemeyer et al. 2003). Content validity was established through an instrument panel that consisted of four doctoral students from Information Systems, one professor from the Department of Management & Information Systems and one professor from the School of Accountancy. The panel was guided through the content validation process and each panelist analyzed the language and accuracy of the items and whether all the items were reflective of the construct they measured. This approach is suggested by Podsakoff et al. (2003) as a proactive method to minimize Common Method Variance. Based on the recommendations of the panel, several items in the threat and coping appraisal scales were modified. A second panel was convened to verify whether the changes were accurate. A few more adjustments to the language of the items were made. The revised instrument was again reviewed by the panel and they agreed on the content validity of the scales used in the instrument.

www.manaraa.com

Preliminary Investigation

Prior to the main data collection, a preliminary investigation consisting of instrument content validity was conducted. This was followed by a pilot test to measure construct validity and reliability as suggested by Podsakoff et al. (2003) . Although this study utilized previously validated and well established scales, it was necessary to ensure that the construct validity and reliability still holds after modifications were made to the items to reflect the context of this study.

Instrument Content Validity

According to Straub et al. (2004), content validity of the instrument needs to be investigated in order to confirm that the instrument completely and accurately represents the behavioral domain. The content validity assessment will also reduce the chances of measurement error in the instrument since such occurrences will be identified and corrected. The scale of habit has scarcely been utilized in the IS security context along with the scale of actual behavior. Thus, it is important that content validity is assessed to make sure the scales were adopted accurately to reflect the IS security domain.

As mentioned in step 5, content validity was established through an instrument panel that consisted of several doctoral students and professors. Each panelist analyzed the language and accuracy of the items and whether all the items were reflective of the construct it measured. Several items in the threat and coping appraisal scales were modified upon recommendations of the instrument panel. The instrument panel was reconvened to verify whether the changes were applied accurately. A few more adjustments to the language of the items were made. The revised instrument was reviewed by the panel again and they came to a consensus that the measures properly

المنارة للاستشارات
www.manaraa.com

reflected the constructs being measured. These steps ensured that a highly valid instrument was developed prior to the data collection being initiated (Netemeyer et al. 2003; Straub et al. 2004). Following the decision rules recommended by Petter et al. (2007), it was also concluded that all the constructs except habit was reflective. Habit is included in the research model as a first-order reflective and second-order formative construct.

Construct Validity and Reliability

In order to assess construct validity and reliability, a pilot test was conducted with a sample from the same pool of respondents that is used for the full-scale study. Conducting a pilot test from the same population significantly increases the initial construct validity and reliability and to some degree would be reflective of the responses of the final study as well. This would provide the opportunity to understand the accuracy of the scale items and if the measurement model reflects the expected findings.

The data was be analyzed through principal component analysis (PCA). All the items used in this proposed study were previously validated items and were reflective. First a measurement model analysis was conducted to examine the psychometric properties of all the constructs included in the research model. There are three processes generally used for assessing reliability of reflective scales. The first is Cronbach's alpha coefficient (Cronbach 1951; Nunnally and Bernstein 1994), where alpha scores that exceed 0.70 would indicate reliability. Another method is the measurement of internal consistency developed by Fornell and Larcker (1981) and preferred in Partial Least Square (PLS) analysis (Chin 1998). The goal of this method is to achieve a composite reliability score of above 0.70 which demonstrates reliability (Fornell and Larcker 1981;

www.manaraa.com

Gefen and Straub 2005). Finally, reflective items were tested for scale reliability by examining the item loadings of at least 0.70.

Convergent validity is demonstrated when (1) the item loadings exceed 0.70 on their respective constructs and (2) Average Variance Extracted (AVE) for each construct is above 0.50 (Gefen and Straub 2005), which suggests that the principal constructs capture a much higher construct-related variance than error variance. Discriminant validity, which is the extent to which different constructs diverge from each other, can be demonstrated if the square root of each construct's AVE is greater than the absolute value of the inter-construct correlations (Gefen and Straub 2005). If the square roots of the AVEs of all constructs are found to be larger than all cross-correlations of the other constructs, it will demonstrate discriminant validity of the constructs used in this study.

Common Method Variance (CMV) Tests

This research used an online survey to collect self-reported data which presents the potential to introduce common method variance (CMV) that might bias the results of this study. Podsakoff et al. (2003) suggests proactive methods to minimize CMV and statistical methods to test for CMV after the data is collected. Proactive measures that can reduce CMV include random selection of subjects, random organization of items in the questionnaire, expert panels, pilot tests and anonymity. All the recommended proactive measures to reduce CMV as suggested by Podsakoff et al. (2003), are utilized for the full-scale study. Statistical analysis using two tests will be conducted to check for the presence of and severity of CMV in the collected data. For the first test, the Harmon one-factor test (Podsakoff and Organ 1986; Podsakoff et al. 2003) can be used, where an exploratory factor analysis (EFA) was conducted on all variables used in the research

المنارة للاستشارات
www.manaraa.com

model and the un-rotated factor solution was examined. It is assumed that CMV exists if a single factor emerges from un-rotated factor solutions or a first factor explains the majority of the variance in the variables (Podsakoff and Organ 1986). In this study, ideally ten factors emerged with no single factor accounting for a majority of the variance.

For the second test, a more rigorous statistical approach suggested by Podsakoff et al. (2003) to check for common method bias was utilized. This approach was first applied using PLS by Liang et al. (2007) and was replicated recently by Bulgurcu et al. (2010). The same procedure was used to test for common method bias in this study. To use this technique, a single-indicator construct for each indicator in the measurement model was created. Each major construct is then linked with their appropriate single-indicator constructs. A common method construct that contains all the indicators of the model is created and linked to each single-indicator constructs. This allows the major constructs and the common method constructs to become second-order reflective constructs. This approach compares the influence of a common method factor on each indicator used in our model against the influence of the constructs on their respective indicators. The average of the substantive factor variance explained was compared to the method factor variance explained. Moreover, the method factor loadings can be inspected, to test if common method bias was unlikely a serious concern in the data (Williams et al. 2003).

Main Investigation

The main investigation of this study was conducted subsequent to the pilot study and after ensuring the validity and reliability of the measures. The survey instrument was

المنارة للاستشارات

www.manaraa.com

developed on Qualtrics and panels of respondents from Amazon Mechanical Turk were utilized. Qualtrics is a company that allows researchers to create powerful surveys online (Qualtrics 2013). Amazon Mechanical Turk (AMT) is a popular crowdsourcing website that is gaining in popularity among researchers as a cheaper alternative to Qualtrics and other survey panel providers (Mason and Suri 2012). AMT respondents are demographically diverse and majority of the respondents are located in the United States or India (Buhrmester et al. 2011). Using the AMT, researchers can collect reliable and high quality data at a range of $0.20-$1 per survey compared to the survey panel providers who charge $5-20 per survey. Researchers have found that, even though the respondents are willing to accept a low payment for each survey completed, the quality of the data did not vary depending on the reward offered (Paolacci et al. 2010). In a comparative study, where an identical survey was distributed to different sources such as the AMT, students at a Midwestern university and visitors of online discussion boards. The results indicate that the data collected from AMT do not differ significantly from the other sources and are reliable providing evidence that AMT is a suitable source to collect data for behavioral research (Berinsky et al. 2012; Mason and Suri 2012; Paolacci et al. 2010).

Initial power analysis using the G-power software indicated that a sample size of 308 would be required for each behavior to achieve a medium effect size (0.15), an alpha of 0.05 and a power of 0.95. Three separate surveys that reflect each of the three behaviors selected for the study was developed. The respondents were randomly presented with one of those surveys. The data were collected from respondents who were employed in different organizations across different industries, compared to Vance et al.

للاستشارات المنارة
www.manaraa.com

(2012), who collected their data only from one organization. Collecting data from multiple companies may introduce some biases to the collected data since different organizations have different organizational cultures, information security policies and sanctions. These factors needed to be controlled during the data analysis stage to alleviate any biases previously mentioned. However, collecting data from multiple organizations across different industries makes the findings more generalizable (Compeau et al. 2012). The full-scale study for our study was conducted from the same pool of respondents as the pilot study, which also increased the validity of the data.

After the data collection procedure was completed, survey sets that reflected each of the three distinct behaviors were analyzed separately. Compared to Vance et al. (2012), this separate analysis informed us on how each distinct behavior differs in habit strength and if differences that exist on how habit influences each behavior in the context of information security. Similar to the pilot study, construct reliability and validity tests were conducted followed by CMV tests. SPSS and Partial Least Squares (PLS) software tool SmartPLS were used to analyze the data as they provided tools to conduct confirmatory factor analysis, path analysis and provided the ability to measure structural and measurement models simultaneously (Chin 1998).

Similar to Limayem et al. (2007), three different models were tested to identify the role of habit in the three information security behaviors selected. First a baseline model was tested that includes only the PMT variables, behavioral intention and actual behavior. Second, habit was tested as a direct effect on actual behavior. Finally, habit was tested as a moderator of the intention-behavior relationship. By comparing the variance explained in the dependent variable which is self-reported secure behavior, the overall

المنارة للاستشارات
www.manaraa.com

effect sizes of the three models were calculated. Cohen (1988) has suggested different thresholds to determine if the effect size is small, medium or large. Depending on the effect size, the impact of habit on the intention-behavior relationship can be identified.

Our study differs significantly from Vance et al. (2012) in the expected findings. While they found empirical support for their research model, they do not capture the automaticity nature of habit. Our study theorized that habit will negatively moderate the intention-behavior relationship while directly influencing behavior. When habits are strong, influence of threat appraisal and coping appraisal would not drive the actual behavior. Our study was the first attempt to utilize a second-order formative and first-order reflective scale to measure habit in an information security context. Practitioners can use the findings of our study to foster positive habits in their employees, such as the recommended secure behaviors which are performed automatically. They can also use the findings to break negative habits through the use of fear appeals and increase of threat appraisals. Researchers can use the findings of our study to further investigate the role of habit on an information security context and identify factors that contribute to the forming and breaking of habits.

Summary

This chapter described the variables used, methodology implemented and an exhaustive process followed to select three information security behaviors investigated for this study. The next two chapters will discuss the data analysis and discussion of findings.

المنارة للاستشارات

www.manaraa.com

CHAPTER IV

DATA ANALYSES AND RESULTS

This chapter first reports the analyses and results for the preliminary study, then those for the main study and finally interpretation of the findings. It is important to note that there are three different behaviors that are investigated in this study and the methodology and analyses are similar for all three. Each behavior is considered separately, but greater detail is given with the first one and not repeated for the subsequent behaviors.

The pilot study was conducted to test the validity and reliability of the survey instrument. An Exploratory Factor Analysis (EFA) was conducted to perform validity and reliability tests for each measurement scale. The main investigation with a larger sample size was conducted by a repeat of the EFA and testing of the measurement model with the use of SmartPLS software.

Preliminary Investigation (Pilot Study)

As discussed on Chapter III, the purpose of the preliminary investigation was to test the validity and reliability of the constructs and their respective items that were part of the survey instrument. The data were collected using the Amazon Mechanical Turk service. Each behavior was investigated with a separate survey. The demographics and

المنارة للاستشارات
www.manaraa.com

the results of the tests conducted to assess the validity and reliability of the scales used in the instruments are reported separately for each behavior.

Behavior 1: Locking the PC

The first behavior investigated was locking the PC when leaving it unattended. The survey was taken by 141 respondents, and after removing incomplete responses, 123 usable responses remained for the pilot test. Over half (61.8 percent) of the respondents were male, nearly half (48.8 percent) were in 25-34 age category, about half (50.4 percent) had a 4-year College Degree, and the most prevalent industry classification was information (24.4 percent). The complete demographic information in the pilot study for this behavior is shown in Table 4.1.

An exploratory factor analysis (EFA) was conducted to test the validity and reliability of the items and their respective constructs. A principal component analysis (PCA) with a Varimax rotation was conducted to complete the EFA (Hair et al. 2010; Netemeyer et al. 2003; Tabachnick and Fidell 2007). The initial EFA analysis revealed cross-loadings for items BINT3, AWAR1, BEHV1, BEHV2 and BEHV3. According to TPB and most behavioral research, intentions and actual behavior are highly correlated. Therefore, these cross-loadings are not surprising. After removing BINT3 and AWAR1 from the analysis, behavioral intention and actual behavior items loaded cleanly on their separate constructs. However, some items for response efficacy and self-efficacy also cross-loaded. This was surprising as the items were pre-validated by many studies in the past. SEFF1 and SEFF2, which cross-loaded significantly with response efficacy, were removed, significantly improving the loadings of the two constructs. The loadings are shown in Table 4.2.

المنارة للاستشارات
www.manaraa.com

Table 4.1 Lock PC: Demographics of Pilot Study

Demographic		Frequency
Gender	Male	76 (61.8%)
	Female	47 (38.2%)
Age	18-24	34 (27.6%)
	25-34	60 (48.8%)
	35-44	22 (17.9%)
	45-54	4 (3.3%)
	55-64	2 (1.6%)
	65 and older	1 (0.8%)
Education	High School	4 (3.3%)
	Some College	16 (13%)
	2-year College Degree	7 (5.7%)
	4-year College Degree	62 (50.4%)
	Masters Degree	32 (26.0%)
	Doctoral Degree	1 (0.8%)
	Professional Degree	1 (0.8%)
Industry	Forestry, fishing, hunting or agriculture support	1 (0.81%)
	Mining	1 (0.81%)
	Utilities	0 (0%)
	Construction	3 (2.44%)
	Manufacturing	15 (12.2%)
	Wholesale trade	1 (0.81%)
	Retail trade	8 (6.5%)
	Transportation or warehousing	1 (0.81%)
	Information	30 (24.39%)
	Finance or insurance	12 (9.76%)
	Real estate or rental and leasing	3 (2.44%)
	Professional, scientific or technical services	11 (8.94%)
	Management of companies or enterprises	5 (4.07%)
	Admin, support, waste management or remediation serv	4 (3.25%)
	Educational services	10 (8.13%)
	Health care or social assistance	9 (7.32%)
	Arts, entertainment or recreation	2 (1.63%)
	Accommodation or food services	1 (0.81%)
	Other services (except public administration)	6 (4.88%)

المنارة للاستشارات
www.manaraa.com

Table 4.2 Lock PC: EFA Results of Pilot Study

Rotated Component Matrix

	Component									
	1	2	3	4	5	6	7	8	9	10
AWAR2	.771									
AWAR3	.808									
AWAR4	.831									
BEHV1		.837								
BEHV2		.789								
BEHV3		.857								
BINT1			.756							
BINT2			.780							
CTRL1				.835						
CTRL2				.871						
CTRL3				.883						
CTRL4				.835						
EFFC1					.632					
EFFC2					.760					
EFFC3					.710					
EFFC4					.794					
PSEV1						.886				
PSEV2						.689				
PSEV3						.789				
PVUL1							.844			
PVUL2							.791			
PVUL3							.904			
RCST1								.818		
RCST2								.780		
RCST3								.812		
RCST4								.799		
REFF1									.741	
REFF2									.729	
REFF3									.734	
REFF4									.817	
SEFF3										.704
SEFF4										.620

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
Correlations lower than 0.4 in absolute value were suppressed.

المنارة للاستشارات

www.manaraa.com

Table 4.3 Lock PC: Construct Reliability of Pilot Study

Construct	Construct Name	Cronbach's Alpha
AWAR	Lack of Awareness	0.796
BEHV	Self-Reported Actual Behavior	0.910
BINT	Behavioral Intention	0.856
CTRL	Lack of Control	0.910
EFFC	Mental Efficiency	0.754
PSEV	Perceived Threat Severity	0.833
PVUL	Perceived Threat Vulnerability	0.866
RCST	Response Cost	0.903
REFF	Response Efficacy	0.884
SEFF	Self-efficacy	0.847

Once the items that cross-loaded were removed, all the items of each construct loaded on a separate factor without any cross-loadings above 0.4, with majority of the items loading above 0.7. Convergent validity of the items was demonstrated with all the items loading significantly on each of their respective factors. Discriminant validity was demonstrated by all items loading on their respective constructs without cross-loadings above the 0.40 threshold. This meets the threshold recommended by Hair et al. (2010), to demonstrate convergent and discriminant validity of the instrument items and their respective scales. Some of the items, such as PSEV2, EFFC1, and SEFF4 had loadings slightly below 0.7. These items did not load on any other factors and had loadings very close to the recommended threshold. Therefore, they were retained since they did not pose a threat to the discriminant and convergent validity of the items. Cronbach’s Alpha values exceeded the 0.70 threshold for each of the constructs demonstrating good scale reliability for all measurement scales. Item loadings that exceeded the 0.70 threshold for each constructs without cross-loadings demonstrated discriminant validity.

المنارة للاستشارات
www.manaraa.com

Behavior 2: Verify Email Recipients

The first behavior investigated was the lock computer behavior. The survey was taken by 170 respondents, and, after removing incomplete responses, 154 usable responses remained for the pilot test. Over half (63.6 percent) of the respondents were male, about half (50.6 percent) were in the 25-34 age category, about half (46.8 percent) had a 4-year College Degree, and the most prevalent Industry classification was Information (24 percent). The complete demographic information in the pilot study for this behavior is shown in Table 4.4.

An exploratory factor analysis (EFA) was conducted to test the validity and reliability of the items and their respective constructs. A principal component analysis (PCA) with a Varimax rotation was conducted to complete the EFA (Hair et al. 2010; Netemeyer et al. 2003; Tabachnick and Fidell 2007).

The initial EFA analysis revealed cross-loadings for items REFF1, REFF2, SEFF1, SEFF2 and SEFF4. It seems that the respondents were not able to distinguish between the response efficacy and self-efficacy items. REFF2 with the lowest loading was removed and the loadings for REFF improved significantly. However, REFF1 continued to cross-load with SEFF. The cross-loading was only slightly above 0.4, thus REFF1 was retained. SEFF1 and SEFF2 items still cross-loaded and were removed from the analysis.SEFF1 and SEFF2 items had cross-loading issues in the first behavior as well, indicating that those items have issues. The languages of the two items were slightly changed for the full scale study. The results of the EFA are shown in Table 4.5.

www.manaraa.com

Table 4.4 Verify Email Recipients: Demographics of Pilot Study

Demographic		Frequency
Gender	Male	98 (63.6%)
	Female	56 (36.4%)
Age	18-24	42 (27.3%)
	25-34	78 (50.6%)
	35-44	22 (14.3%)
	45-54	7 (4.5%)
	55-64	3 (1.9%)
	65 and older	2 (1.3%)
Education	High School	9 (5.8%)
	Some College	19 (12.3%)
	2-year College Degree	7 (4.5%)
	4-year College Degree	72 (46.8%)
	Masters Degree	44 (28.6%)
	Doctoral Degree	0 (0.0%)
	Professional Degree	3 (1.9%)
Industry	Forestry, fishing, hunting or agriculture support	1 (0.6%)
	Mining	1 (0.6%)
	Utilities	0 (0.0%)
	Construction	3 (1.9%)
	Manufacturing	13 (8.4%)
	Wholesale trade	1 (0.6%)
	Retail trade	5 (3.2%)
	Transportation or warehousing	3 (1.9%)
	Information	37 (24.0%)
	Finance or insurance	14 (9.1%
	Real estate or rental and leasing	1 (0.6%)
	Professional, scientific or technical services	7 (4.5%)
	Management of companies or enterprises	7 (4.5%)
	Admin, support, waste management or remediation serv	17 (11.0%)
	Educational services	6 (3.9%)
	Health care or social assistance	1 (0.6%)
	Arts, entertainment or recreation	1 (0.6%)
	Accommodation or food services	15 (9.7%)
	Other services (except public administration)	4 (2.6%)

المنارة للاستشارات
www.manaraa.com

Table 4.5 Verify Email Recipients: EFA results of Pilot Study

Rotated Component Matrix

	Component									
	1	2	3	4	5	6	7	8	9	10
AWAR1	.737									
AWAR2	.780									
AWAR3	.803									
AWAR4	.843									
BEHV1		.793								
BEHV2		.727								
BEHV3		.805								
BINT1			.745							
BINT2			.687							
BINT3			.707							
CTRL1				.835						
CTRL2				.871						
CTRL3				.883						
CTRL4				.835						
EFFC1					.770					
EFFC2					.606					
EFFC3					.708					
EFFC4					.646					
PSEV1						.767				
PSEV2						.739				
PSEV3						.886				
PVUL1							.809			
PVUL2							.863			
PVUL3							.846			
RCST1								.766		
RCST2								.764		
RCST3								.780		
RCST4								.750		
REFF1									.614	
REFF3									.751	.421
REFF4									.776	
SEFF3										.753
SEFF4										.632

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
Correlations lower than 0.4 in absolute value were suppressed.

المنارة للاستشارات

www.manaraa.com

Table 4.6 Verify Email Recipients: Construct Reliability of Pilot Study

Construct	Construct Name	Cronbach's Alpha
AWAR	Lack of Awareness	0.867
BEHV	Self-Reported Actual Behavior	0.869
BINT	Behavioral Intention	0.812
CTRL	Lack of Control	0.933
EFFC	Mental Efficiency	0.774
PSEV	Perceived Threat Severity	0.856
PVUL	Perceived Threat Vulnerability	0.907
RCST	Response Cost	0.871
REFF	Response Efficacy	0.826
SEFF	Self-efficacy	0.856

Once the items that cross-loaded were removed, all the items of each construct loaded on a separate factor with only one cross-loading above 0.4. As illustrated in Table 4.5, majority of the items loaded above the 0.7. This meets the threshold recommended by Hair et al. (2010), to demonstrate convergent and discriminant validity of the instrument items and their respective scales. Items such as BINT2, EFFC2, EFFC4, REFF1 and SEFF4 indicated loadings slightly below the recommended threshold, they did not pose a threat to the discriminant and convergent validity of the other items. Therefore, those items were retained. Convergent validity of the items was demonstrated with all the items loading significantly on each of their respective factors. Discriminant validity was demonstrated by all items loading on their respective constructs without any major cross-loadings above the 0.40 threshold. As shown in Table 4.6, Cronbach's Alpha values exceeded the 0.70 threshold for each of the constructs demonstrating good scale reliability for all measurement scales.

المنارة للاستشارات

www.manaraa.com

Behavior 3: Visit Verified Websites

The third behavior investigated was visiting only verified websites. The survey was taken by 165 respondents, and after removing incomplete responses, 143 usable responses remained for the pilot test. Over half (60.8 percent) of the respondents were male, about half (45.5 percent) were in 35-44 age category, about half (44.1 percent) had a 4-year College Degree, and the most prevalent industry classification was information (23.8 percent). The complete demographic information in the pilot study for this behavior is shown in Table 4.7.

An exploratory factor analysis (EFA) was conducted to test the validity and reliability of the items and their respective constructs. A principal component analysis (PCA) with a Varimax rotation was conducted to complete the EFA (Hair et al. 2010; Netemeyer et al. 2003; Tabachnick and Fidell 2007). The initial EFA analysis revealed cross-loadings for items EFFC4, BINT1, SEFF2 and REFF4. EFFC4 was removed eliminating the cross-loading with BINT1. After removing SEFF2 from the analysis, all the items loaded cleanly on their separate constructs. Majority of the items loaded above 0.7 and the loadings are shown in Table 4.8. This meets the threshold recommended by Hair et al (2010), to demonstrate convergent and discriminant validity of the instrument items and their respective scales. Items such as AWAR1, EFFC2, PVUL1 and REFF2 indicated loadings below the recommended threshold, but they were retained since they did not pose a threat to the discriminant and convergent validity of the other items.

www.manaraa.com

Table 4.7 Visit Verified Websites: Demographics of Pilot Study

Demographic		Frequency
Gender	Male	87 (60.8%)
	Female	56 (39.2%)
Age	18-24	0 (0.0%)
	25-34	42 (29.4%)
	35-44	65 (45.5%)
	45-54	29 (20.3%)
	55-64	7 (4.8%)
	65 and older	0 (0.0%)
Education	High School	7 (4.8%)
	Some College	18 (12.6%)
	2-year College Degree	6 (4.2%)
	4-year College Degree	63 (44.1%)
	Masters Degree	47 (32.9%)
	Doctoral Degree	0 (0.0%)
	Professional Degree	2 (1.4%)
Industry	Forestry, fishing, hunting or agriculture support	3 (2.1%)
	Mining	1 (0.7%)
	Utilities	4 (2.8%)
	Construction	2 (1.4%)
	Manufacturing	16 (11.2%)
	Wholesale trade	1 (0.7%)
	Retail trade	1 (0.7%)
	Transportation or warehousing	1 (0.7%)
	Information	34 (23.8%)
	Finance or insurance	12 (8.4%)
	Real estate or rental and leasing	2 (1.4%)
	Professional, scientific or technical services	13 (9.1%)
	Management of companies or enterprises	8 (5.6%)
	Admin, support, waste management or remediation serv	6 (4.2%)
	Educational services	15 (10.5%)
	Health care or social assistance	8 (5.6%)
	Arts, entertainment or recreation	4 (2.8%)
	Accommodation or food services	1 (0.7%)
	Other services (except public administration)	11 (7.7%)

المنارة للاستشارات
www.manaraa.com

Table 4.8 Visit Verified Website: EFA Results of Pilot Study

Rotated Component Matrix

	Component									
	1	2	3	4	5	6	7	8	9	10
AWAR1	.605									
AWAR2	.794									
AWAR3	.773									
AWAR4	.739									
BEHV1		.848								
BEHV2		.844								
BEHV3		.858								
BINT1			.864							
BINT2			.810							
BINT3			.836							
CTRL1				.861						
CTRL2				.855						
CTRL3				.806						
CTRL4				.777						
EFFC1					.769					
EFFC2					.657					
EFFC3					.729					
PSEV1						.770				
PSEV2						.734				
PSEV3						.770				
PVUL1							.684			
PVUL2							.810			
PVUL3							.775			
RCST1								.841		
RCST2								.815		
RCST3								.824		
RCST4								.830		
REFF1									.691	
REFF2									.773	
REFF3									.819	
REFF4									.726	
SEFF1										.792
SEFF3										.789
SEFF4										.759

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
Correlations lower than 0.4 in absolute value were suppressed.

www.manaraa.com

Convergent validity of the items was demonstrated with all the items loading significantly on each of their respective factors. Discriminant validity was demonstrated by all items loading on their respective constructs without cross-loadings above the 0.40 threshold. As shown in Table 4.9, Cronbach's Alpha values except for EFFC exceeded the 0.70 threshold for each of the constructs demonstrating good scale reliability. EFFC showed an alpha value of 0.677 which is still acceptable since it is quite close to the minimum threshold of 0.7.

Table 4.9 Visit Verified Websites: Construct Reliability of Pilot Study

Construct	Construct Name	Cronbach's Alpha
AWAR	Lack of Awareness	0.789
BEHV	Self-Reported Actual Behavior	0.916
BINT	Behavioral Intention	0.901
CTRL	Lack of Control	0.897
EFFC	Mental Efficiency	0.677
PSEV	Perceived Threat Severity	0.719
PVUL	Perceived Threat Vulnerability	0.771
RCST	Response Cost	0.884
REFF	Response Efficacy	0.806
SEFF	Self-efficacy	0.829

Power Analysis

A power analysis was conducted using the G-power software to identify a suitable sample size for this study. *A priori* type of power analysis was used to compute the required sample size with an effect size (f^2) of 0.15 (medium effect), alpha of 0.05 and a power of 0.95. It was calculated that a sample size of 308 would be required for each of the behaviors with the number of predictors as 45 (total number of items). The results of the power analysis procedure are shown on Appendix C.

المنارة للاستشارات
www.manaraa.com

Main Investigation

This section describes the results of the main study with a larger sample size than used in the pilot study and the support of the hypothesized relationships. Following the format for the pilot study results, results for each of the three studied behaviors are reported separately, but with some details given only for the first one and omitted in the other two for brevity. Each behavior is tested according to the proposed research model followed by post hoc analyses that test the alternative models. It is also important to note that data for all three behaviors were collected using the Amazon Mechanical-Turk. The reward amount paid to the respondents per each survey completed during the pilot study phase and the main investigation phase was the same. Restrictions were placed to limit each respondent from completing more than one survey.

Behavior 1: Locking the PC (n=421)

The first behavior tested was “locking the PC when leaving it unattended” and from now on will be referred to as the ‘Lock PC’ behavior. A total of 500 responses were collected for this behavior, and the surveys were completed in an average time of four minutes. Responses that were incomplete or failed the response validity check item were removed. This resulted in a usable sample of 421 responses, which exceeded required sample size of 308 as calculated through the power analysis.

المنارة للاستشارات

www.manaraa.com

Table 4.10 Lock PC: Demographics of Main Investigation

Demographic	Category	Frequency
Gender	Male	254 (60.3%)
	Female	167 (39.7%)
Age	18-24	105 (24.9%)
	25-34	214 (50.8%)
	35-44	73 (17.3%)
	45-54	18 (4.3%)
	55-64	8 (1.9%)
	65 and older	3 (0.7%)
Education	Less than High School	1 (0.2%)
	High School / GED	17 (4%)
	Some College	68 (16.2%)
	2-year College Degree	25 (5.9%)
	4-year College Degree	199 (47.3%)
	Masters Degree	102 (24.2%)
	Doctoral Degree	4 (1%)
	Professional Degree (JD, MD)	5 (1.2%)
Industry	Forestry, fishing, hunting or agriculture support	2 (0.5%)
	Mining	2 (0.5%)
	Utilities	2 (0.5%)
	Construction	7 (1.7%)
	Manufacturing	43 (10.2%)
	Wholesale trade	6 (1.4%)
	Retail trade	25 (5.9%)
	Transportation or warehousing	4 (1%)
	Information	83 (19.7%)
	Finance or insurance	42 (10%)
	Real estate or rental and leasing	6 (1.4%)
	Professional, scientific or technical services	48 (11.4%)
	Management of companies or enterprises	17 (4%)
	Admin, support, waste management or remediation services	17 (4%)
	Educational services	39 (9.3%)
	Health care or social assistance	31 (7.4%)
	Arts, entertainment or recreation	7 (1.7%)
	Accommodation or food services	3 (0.7%)
	Other services (except public administration)	31 (7.4%)
	Unclassified establishments	6 (1.4%)

المنارة للاستشارات
www.manaraa.com

Of the usable responses, 254 (60.3%) were male and 167 (39.7%) were female. There were 105 (24.9%) respondents who were between the ages of 18 and 24, 214 (50.8%) were between the ages of 25 and 34, 73 (17.3%) were between the ages of 35 and 44, 18 (4.3%) were between the ages of 45 and 54, 8 (1.9%) were between the ages of 55 and 64 and 3 (0.7%) were age 65 or above. In terms of the education of the respondents, 111 (26.37%) had a 2-year college degree or lesser, 199 (47.3%) had a 4-year college degree, 102 (24.2%) had a master's degree and 9 (2.2%) had a doctoral degree or a professional degree. The respondents were employed in various industries and the majority of the respondents belonged to the categories of information (19.7%), professional, scientific or technical services (11.4%) and manufacturing (10.2%). Table 4.10 provides the demographic details of the respondents who participated in this study.

Many scholars believe that if an Exploratory Factory Analysis (EFA) is conducted during a preliminary investigation phase, a repeat of the EFA is not required during the data analysis of the full scale study. However, since minor language changes were made to a few items in the instrument after the pilot study, an EFA was repeated for the full scale study. The results confirm the pilot study findings. The items demonstrated an acceptable response spread with no unusual patterns in the means or standard deviations. Bartlett's Test of Sphericity was significant at 0.000 and Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy was 0.897, indicating that factor analysis was appropriate for this sample (Hair et al. 2010).

The EFA was conducted using the Principal Component Analysis (PCA) technique with a Varimax rotation. Ten factors with an eigenvalues of one or greater were extracted, and those factors explained a total of 78% of the variance, which is above

المنارة للاستشارات
www.manaraa.com

the minimum of 65% recommended by Hair et al. (2010). The communalities of the items were well above the accepted minimum threshold of 0.03. All the items loaded cleanly on their respective factors except AWAR1 and BINT1, which cross-loaded with the items of BEHV. This was not a surprise as the items in the formative habit construct, behavioral intentions, and behavior were quite similar. After the preliminary study, wording of AWAR1 was slightly modified for the main investigation. However, it was removed from the analysis again since it continued to cross-load with a value of 0.619. EFFC2, which loaded cleanly along with other EFFC items, had a loading of less than 0.5 and was removed as well. This improved the factor loadings, and all remaining items loaded cleanly on their respective factors. The results of the EFA are shown in Table 4.11 with the correlations than 0.4 in absolute value suppressed for clarity.

The EFA factor loadings for the main study were very similar to those of the pilot study. All the items loaded cleanly on their respective constructs. The results provide strong evidence that the measurement scales were reliable and we can move to the analysis of the measurement model.

المنارة للاستشارات
www.manaraa.com

Table 4.11 Lock PC: EFA Results of Main Investigation

Rotated Component Matrix

	Component									
	1	2	3	4	5	6	7	8	9	10
AWAR2	.796									
AWAR3	.762									
AWAR4	.842									
BEHV1		.779								
BEHV2		.762								
BEHV3		.786								
BINT1			.680							
BINT2			.765							
BINT3			.722							
CTRL1				.857						
CTRL2				.870						
CTRL3				.866						
CTRL4				.846						
EFFC1					.738					
EFFC3					.795					
EFFC4					.773					
PSEV1						.843				
PSEV2						.803				
PSEV3						.833				
PVUL1							.830			
PVUL2							.810			
PVUL3							.883			
RCST1								.871		
RCST2								.834		
RCST3								.826		
RCST4								.839		
REFF1									.778	
REFF2									.780	
REFF3									.767	
REFF4									.745	
SEFF1										.767
SEFF2										.805
SEFF3										.823
SEFF4										.831

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
Correlations lower than 0.4 in absolute value were suppressed.

المنارة للاستشارات

www.manaraa.com

Measurement Model

SmartPLS was used to test both the measurement model and structural model (Ringle et al. 2005). As mentioned in Chapter III, partial least squares (PLS) allows the simultaneous testing of both the measurement and structural models. PLS is frequently used in IS research, especially in IS security research, and is the preferred tool of data analysis when formative scales are included (Limayem et al. 2007). PLS is also better suited to test moderation effects than covariance based tools such as LISREL or AMOS (Limayem et al. 2007) since those methods use a grouping technique without considering the complete data set together. The research model of this study is fairly complex with habit conceptualized as a first-order reflective and a second-order formative construct. Moreover, the core of this study is based on detecting the moderating effects of habit. Therefore, SmartPLS was the best tool for the data analysis of this study.

A measurement model analysis was conducted to examine the psychometric properties of all the reflective constructs included in the research model. PLS validation procedures outlined by Gefen and Straub (2005) were followed to establish the validity and reliability of the measurement model. Reliability of reflective scales can be tested with three different analyses. The most commonly used method to test reliability is to examine the Cronbach's alpha coefficient. According to Cronbach (1951) and Nunnally and Bernstein (1994), when the alpha score of a scale exceeds 0.70, it would indicate reliability. All the scales had alpha values larger than the recommended threshold with the lowest alpha value being 0.723 for EFFC. Composite reliability scores of 0.70 for each of the scales would indicate good reliability as well (Fornell and Larcker 1981; Gefen and Straub 2005). All the scales demonstrated composite reliability values much

المنارة للاستشارات
www.manaraa.com

higher than the recommended values with the lowest reliability being 0.860 for the scale PVUL. The values of the reliability tests such as composite reliability and Cronbach's alpha are shown in Table 4.12.

Table 4.12 Lock PC: Reliability Statistics

Construct		AVE	C-alpha	CREL	Mean (St. dev)	Min/Max
AWAR	Lack of Awareness	0.825	0.894	0.934	3.29 (1.084)	1.00/5.00
BEHV	Actual Behavior	0.885	0.935	0.959	3.65 (1.160)	1.00/5.00
BINT	Behavioral Intention	0.860	0.919	0.949	3.75 (1.050)	1.00/5.00
CTRL	Uncontrollability	0.833	0.933	0.952	3.09 (1.117)	1.00/5.00
EFFC	Mental Efficiency	0.643	0.723	0.844	3.47 (0.908)	1.00/5.00
PSEV	Perceived Severity	0.797	0.873	0.922	3.75 (0.973)	1.00/5.00
PVUL	Perceived Vulnerability	0.781	0.860	0.915	2.83 (1.091)	1.00/5.00
RCST	Response Cost	0.781	0.907	0.935	2.55 (1.108)	1.00/5.00
REFF	Response Efficacy	0.730	0.877	0.915	4.08 (0.731)	1.00/5.00
SEFF	Self-Efficacy	0.755	0.892	0.925	4.27 (0.724)	1.00/5.00

Convergent validity indicates the "extent to which the items of a scale that are theoretically related are also related in reality" (Gefen and Straub 2005; Limayem et al. 2007, p. 724). Convergent validity can be demonstrated when (1) the item loadings exceed 0.70 on their respective constructs and (2) Average Variance Extracted (AVE) for each construct is above 0.50 (Gefen and Straub 2005), which suggests that the principal constructs capture a much higher construct-related variance than error variance. As shown in Table 4.14 all the item loadings exceeded 0.70 on their respective constructs. Table 4.12 shows that all the scales demonstrated AVE values well above 0.5. Therefore, all the scales of this study demonstrate convergent validity values that are beyond the recommended thresholds.

المنارة للاستشارات
www.manaraa.com

Table 4.13 Lock PC: Inter-Construct Correlations

	AWAR	BEHV	BINT	CTRL	EFFC	PSEV	PVUL	RCST	REFF	SEFF
AWAR	0.908									
BEHV	0.610	0.941								
BINT	0.562	0.732	0.927							
CTRL	0.479	0.409	0.404	0.913						
EFFC	0.333	0.217	0.288	0.338	0.802					
PSEV	0.374	0.440	0.470	0.265	0.169	0.893				
PVUL	0.251	0.106	0.118	0.342	0.080	0.105	0.884			
RCST	-0.070	-0.293	-0.304	0.147	0.030	-0.211	0.329	0.884		
REFF	0.170	0.307	0.417	0.005	0.201	0.435	-0.180	-0.341	0.855	
SEFF	0.084	0.218	0.326	0.051	0.204	0.291	-0.235	-0.357	0.607	0.869

* The highlighted diagonal elements are square-roots of the AVE

Discriminant validity refers to the extent to which different constructs diverge from each other. This can be demonstrated if the square root of each construct's Average Variance Extracted (AVE) is greater than the absolute values of the inter-construct correlations (Gefen and Straub 2005). As it is shown in Table 4.13, the square roots of the AVEs of all constructs were found to be larger than all cross-correlations of the other constructs, demonstrating discriminant validity of the constructs used in this study. Discriminant validity is also demonstrated when items load on their respective constructs and substantially less on all other constructs. Although all the items load significantly higher on their respective constructs, a few cross-loadings above 0.60 are present. BEHV and BINT items cross-load, with BINT1 having the highest cross-loading of 0.711 on BEHV. PLS loadings and cross-loadings for all the items are shown in Table 4.14.

www.manaraa.com

Table 4.14 Lock PC: PLS loadings for the Main Investigation

	Aware	BEHV	BINT	CTRL	EFFC	PSEV	PVUL	RCST	REFF	SEFF
AWAR2	0.914	0.578	0.507	0.449	0.324	0.368	0.207	-0.081	0.154	0.091
AWAR3	0.886	0.551	0.506	0.425	0.277	0.350	0.248	-0.052	0.166	0.079
AWAR4	0.925	0.532	0.518	0.430	0.306	0.301	0.229	-0.055	0.144	0.060
BEHV1	0.566	0.945	0.681	0.387	0.207	0.414	0.102	-0.275	0.302	0.224
BEHV2	0.567	0.931	0.689	0.372	0.186	0.414	0.109	-0.283	0.277	0.180
BEHV3	0.589	0.947	0.697	0.396	0.220	0.414	0.088	-0.269	0.289	0.210
BINT1	0.560	0.711	0.939	0.393	0.290	0.457	0.108	-0.287	0.398	0.322
BINT2	0.494	0.667	0.915	0.379	0.256	0.398	0.129	-0.233	0.336	0.271
BINT3	0.507	0.659	0.928	0.353	0.255	0.452	0.091	-0.322	0.424	0.314
CTRL1	0.440	0.370	0.370	0.917	0.319	0.250	0.338	0.150	-0.005	-0.033
CTRL2	0.435	0.369	0.373	0.918	0.297	0.238	0.298	0.128	-0.013	-0.030
CTRL3	0.410	0.384	0.348	0.913	0.319	0.237	0.311	0.144	0.020	-0.047
CTRL4	0.462	0.372	0.386	0.904	0.301	0.245	0.301	0.116	0.017	-0.075
EFFC1	0.267	0.277	0.334	0.292	0.802	0.224	0.016	-0.032	0.273	0.238
EFFC3	0.273	0.198	0.241	0.272	0.815	0.145	0.068	0.012	0.174	0.151
EFFC4	0.262	0.036	0.108	0.249	0.789	0.028	0.114	0.098	0.025	0.095
PSEV1	0.341	0.381	0.385	0.237	0.134	0.883	0.101	-0.176	0.360	0.214
PSEV2	0.310	0.400	0.418	0.226	0.184	0.880	0.082	-0.203	0.411	0.306
PSEV3	0.350	0.396	0.452	0.247	0.135	0.914	0.099	-0.185	0.393	0.257
PVUL1	0.265	0.089	0.110	0.344	0.082	0.114	0.901	0.312	-0.173	-0.226
PVUL2	0.203	0.084	0.104	0.288	0.070	0.061	0.862	0.307	-0.163	-0.216
PVUL3	0.192	0.109	0.097	0.269	0.060	0.103	0.889	0.249	-0.139	-0.176
RCST1	-0.090	-0.274	-0.306	0.131	0.028	-0.225	0.281	0.926	-0.310	-0.343
RCST2	-0.098	-0.285	-0.247	0.127	0.054	-0.174	0.260	0.859	-0.306	-0.251
RCST3	-0.008	-0.248	-0.218	0.101	-0.010	-0.175	0.345	0.855	-0.315	-0.314
RCST4	-0.041	-0.232	-0.288	0.156	0.028	-0.167	0.289	0.893	-0.282	-0.345
REFF1	0.139	0.248	0.362	0.010	0.166	0.379	-0.164	-0.300	0.863	0.491
REFF2	0.159	0.249	0.338	-0.036	0.145	0.380	-0.202	-0.275	0.860	0.537
REFF3	0.178	0.281	0.356	0.051	0.224	0.338	-0.085	-0.270	0.851	0.548
REFF4	0.107	0.270	0.368	-0.010	0.151	0.390	-0.167	-0.318	0.845	0.500
SEFF1	0.060	0.181	0.263	-0.057	0.198	0.244	-0.233	-0.307	0.548	0.848
SEFF2	0.064	0.184	0.284	-0.040	0.166	0.262	-0.212	-0.308	0.540	0.873
SEFF3	0.089	0.207	0.305	-0.047	0.182	0.245	-0.169	-0.308	0.517	0.882
SEFF4	0.078	0.184	0.281	-0.033	0.163	0.261	-0.206	-0.319	0.506	0.872

المنارة للاستشارات
www.manaraa.com

The BINT2, BINT3, BEHV1, BEHV2, and BEHV3 items cross-loaded at values of 0.6 or higher. Language of BINT3 was slightly modified following the cross-loadings during the pilot study phase. However, similar issues with the behavior and intention items exist in the main study as well. Behavior and behavioral intention constructs, which stem from TRA and TPB, are highly correlated in nature and the measurement scales have items that are quite similar. Therefore, cross-loadings among the intention and behavior items were not a complete surprise. However, it can be argued that these cross-loadings are not sufficiently high to negate the validity of the items and constructs. While it is recommended to have no cross-loadings among items of separate constructs, some researchers suggest that discriminant validity is still demonstrated if the cross-loadings are at least 0.2 less than the loading on the correct construct, as is the case with this study. Although BINT1 cross-load with BEHV at 0.711, the factor loading of BINT1 on its intended construct BINT is 0.939. Therefore, the cross-loadings differ by more than 0.2, which still demonstrates discriminant validity.

Gefen and Straub (2005), suggests that discriminant validity is demonstrated when an item loads higher on its intended construct by at least 0.10 more than any of the loadings on other constructs. Their suggestion is similar to Chin (1998), who suggested that, if the item loadings are higher on the intended construct than the items that were used to measure other constructs, it is a good indication of discriminant validity. Limayem et al. (2007), who investigated the role of habit in IS continuance, found much higher cross-loadings of their items than in this study, but they retained those items in their data analyses citing Chin (1998). The correlations between BINT and BEHV are evident in the inter-construct correlations table as well (0.732). However, the square root

www.manaraa.com

of the AVE is well above the inter-construct correlations, demonstrating high discriminant validity. Overall, the results of the reliability and validity tests provide strong empirical support of the scales used in this study.

Tests for Common Method Variance

This study utilized an online survey that collected self-reported data at one point in time with similar Likert scales, which has the potential to introduce common method variance (CMV). Podsakoff et al. (2003) defines CMV as "variance that is attributable to the measurement method rather than to the constructs the measures represent." If CMV is high, it may lead to incorrect inferences about the relationships among constructs. To reduce the possibility of common method variance, proactive measures such as random selection of subjects and random organization of items in the questionnaire were utilized in the survey. However, there is still a possibility of CMV being introduced to the data because the dependent variables and independent variables were measured using the same instrument and at the same time (Siponen and Vance 2010). We conducted statistical analysis using three tests to check for the presence of and severity of CMV in our data.

For the first test, we used the Harmon single-factor test (Podsakoff and Organ 1986; Podsakoff et al. 2003), where an exploratory factor analysis (EFA) was conducted on all the variables used in our model and the unrotated factor solution was examined. It is assumed that CMV exists if a single factor emerges from unrotated factor solutions or a first factor explains the majority of the variance in the variables (Podsakoff and Organ 1986). Ten factors emerged from the EFA, which accounted for 78.41% of the variance.

المنارة للاستشارات
www.manaraa.com

The greatest variance explained by one factor was 27.33%, demonstrating that common method variance is unlikely to bias the results.

The Harmon single-factor test is increasingly questioned on its ability to detect common method bias and often criticized by scholars if used as the sole method to test for CMV (Podsakoff et al. 2003). A second test suggested by Pavlou et al. (2007) recommends the examination of the inter-construct correlation matrix to determine whether any of the constructs correlate extremely high, defined as being above 0.90, with such “extremely high” correlations indicative of potential CMV. Extremely high correlations indicate potential CMV. Examining the inter-construct correlations in Table 4.13, the highest correlation among constructs is 0.732 which does not exceed the threshold of 0.9 suggested by Pavlou et al. (2007). This rules out the potential for CMV in this study.

For the third test, we used the rigorous statistical approach suggested by Podsakoff et al. (2003) to check for common method bias. This approach was first applied using PLS by (Liang et al. 2007) and the same procedure was used to test for common method bias in this study. To use this technique, we created a single-indicator construct for each indicator in the measurement model resulting in 36 single indicator constructs. The major constructs then linked with their appropriate single-indicator constructs. A common method construct that contained all the indicators of the model was created and linked to each single-indicator constructs, transforming the major constructs and the common method constructs to second-order reflective constructs. This approach compares the influence of a common method factor on each indicator used in our model against the influence of the constructs on their respective indicators.

المنارة للاستشارات
www.manaraa.com

Table 4.15 Lock PC: CMV Test Results

Construct	Indicator	Substantive Factor Loading (λs)	Substantive Factor Variance Explained (λs2)	Method Factor Loading (λm)	Method Factor Variance Explained (λm2)
Awareness	AWAR2	0.893	0.797	0.030	0.001
	AWAR3	0.874	0.764	0.018	0.000
	AWAR4	0.957	0.916	-0.047	0.002
Behavior	BEHV1	0.945	0.893	0.000	0.000
	BEHV2	0.943	0.889	-0.015	0.000
	BEHV3	0.935	0.874	0.014	0.000
Behavioral Intention	BINT1	0.866	0.749	0.085**	0.007
	BINT2	1.008	1.016	-0.107**	0.011
	BINT3	0.912	0.831	0.019	0.000
Uncontrollability	CTRL1	0.918	0.842	-0.001	0.000
	CTRL2	0.920	0.847	-0.005	0.000
	CTRL3	0.918	0.842	-0.008	0.000
	CTRL4	0.896	0.802	0.014	0.000
Mental Efficiency	EFFC1	0.734	0.539	0.143***	0.020
	EFFC3	0.812	0.659	0.013	0.000
	EFFC4	0.863	0.744	-0.160***	0.026
Perceived Severity	PSEV1	0.921	0.849	-0.045	0.002
	PSEV2	0.853	0.728	0.037	0.001
	PSEV3	0.904	0.816	0.008	0.000
Perceived Vulnerability	PVUL1	0.896	0.802	0.011	0.000
	PVUL2	0.859	0.738	-0.018	0.000
	PVUL3	0.897	0.805	0.006	0.000
Response Cost	RCST1	0.909	0.826	-0.026	0.001
	RCST2	0.863	0.745	0.000	0.000
	RCST3	0.875	0.765	0.013	0.000
	RCST4	0.890	0.791	0.014	0.000
Response Efficacy	REFF1	0.872	0.760	-0.015	0.000
	REFF2	0.884	0.781	-0.029	0.001
	REFF3	0.827	0.684	0.038	0.001
	REFF4	0.835	0.697	0.006	0.000
Self-Efficacy	SEFF1	0.855	0.732	-0.003	0.000
	SEFF2	0.875	0.765	-0.002	0.000
	SEFF3	0.871	0.759	0.008	0.000
	SEFF4	0.874	0.765	-0.004	0.000
Average		**0.8868**	**78.9%**	**-0.0002**	**0.2%**

المنارة للاستشارات

www.manaraa.com

Table 4.15 shows the factor loadings for each major construct and factor loadings for the common method construct captured through this procedure. The results explain that the average loading of the indicators is 0.887 while the average loading of the method indicators is -0.0002. The average variance explained by the substantive constructs is 78.9 percent compared to the 2 percent average variance explained by the method construct. Moreover, all the method factor loadings were statistically non-significant, except for four indicators that had small loadings all less than 0.160 in absolute value (although statistically different from zero). Items that indicated significant method factor loadings are shown with '**' for p<0.01 and '***' for p<0.001. It is important to note that BINT1 and BINT2, which had small but statistically significant method factor loadings, also had cross-loading issues in the CFA. This may indicate some problems with those items. Since almost all of the method factor loadings are statistically not significant and the indicators' substantive variances are substantially greater than their method variances, it can be concluded that common method bias is unlikely to be a serious concern in the data of this study (Williams et al. 2003). Therefore, based on the three separate tests to measure CMV, we concluded that common method bias was not a concern for this study.

Structural Model

The structural models were tested with the SmartPLS software as well. Habit was conceptualized as a first-order reflective and a second-order formative construct. Therefore, before the final structural model was tested, we generated factor scores for each of the first-order dimensions of Habit: Lack of Awareness, Uncontrollability and Mental Efficiency. These factors scores were used as formative measures of the second-

المنارة للاستشارات
www.manaraa.com

order aggregate construct of Habit (Chin et al. 2003; Polites and Karahanna 2012). To achieve this, we followed the two-stage approach for formative hierarchical constructs as recommended by Ringle et al. (2012). The first stage was to run the full research model on SmartPLS with the constructs disaggregated. The resulting PLS latent scores for each dimension were used as the formative measures of the Habit construct (Polites and Karahanna 2012).

Reliability and validity tests performed on the first-order reflective dimensions of Habit were described previously. However, these tests do not apply to formative scales because "the measurement model does not predict that the sub-dimensions will be correlated" (Bollen and Lennox 1991; Edwards 2003; MacKenzie et al. 2011, p.314). This view has also been suggested by prominent marketing research articles as well (Diamantopoulos and Winklhofer 2001; Jarvis et al. 2003). Item weights of the formative constructs can be examined to identify their individual influence in forming each construct (Chin 1998; Petter et al. 2007). The weights for the three habit dimensions were 0.866 for Lack of Awareness, 0.249 for Uncontrollability and -0.025 for Mental Efficiency. The weight for Mental Efficiency was not significant while Lack of Awareness and Uncontrollability were significant at p<0.001.

The formative dimensions of the habit construct were tested for multicollinearity next. Although multicollinearity between construct items is preferred in reflective scales, "excessive multicollinearity in formative constructs can destabilize the model" (Petter et al. 2007, p.641). To test for multicollinearity, the variance inflation factor (VIF) statistics for the three dimensions of habit were examined. VIF values higher than 10 are considered indicative of multicollinearity, but Diamantopoulos and Siguaw (2006)

المنارة للاستشارات
www.manaraa.com

recommended VIF values of 3.3 or lesser to indicate no issues with multicollinearity. As shown in Table 4.16, all the VIF values are well below the recommended threshold value of 3.3, which indicates no serious multicollinearity issues with the formative dimensions of Habit. Individual weights of the formative dimensions of Habit also indicate that multicollinearity is not a concern.

Table 4.16 Lock PC: Weights of the Formative Habit Construct

Construct	Dimension	Weight	VIF
Habit	Lack of Awareness	0.866 (****)	1.129
	Uncontrollability	0.249 (****)	1.125
	Mental Efficiency	-0.025 (n.s.)	1.297

Note: ****p<0.001

Although two of the formative dimensions of Habit are significant, the dimension of mental efficiency is not significant. There is an ongoing debate among researchers whether formative indicators with non-significant weights should be removed from the analysis. MacKenzie et al. (2011, p. 316) recommend that sub-dimensions should be eliminated only if “all of the essential aspects of the focal construct domain are captured by the remaining sub-dimensions” and suggest that such instances are rare. Content validity of formative scales is affected if one of the indicators that represent one of the formative dimensions is removed. Therefore, it is recommended that removal of any indicators from a formative construct should be theoretically justified rather than relying only on empirical results (Diamantopoulos and Siguaw 2006; Diamantopoulos and Winklhofer 2001; MacKenzie et al. 2011; Petter et al. 2007; Polites and Karahanna 2012). Since mental efficiency is one of the three dimensions that constitute habit, it was retained for the structural model analysis although its weight was not significant. The

www.manaraa.com

model was reanalyzed without the non-significant Mental Efficiency dimension yielded similar results. To test the role of habit in information security behaviors, data analyses were performed in three stages, following the recommendations by Limayem et al. (2007). First, we ran a baseline research model with only the PMT variables. The next model added habit as a direct effect on behavior. The final model added the possibility of habit moderating the relationship between behavioral intention and behavior.

Lock PC Behavior: Baseline Model

A baseline model without the incorporation of the habit construct was tested first and the results are shown in Figure 4.1. All the hypothesized relationships were significant at p<0.01 or better except self-efficacy, which was significant at p<0.10.

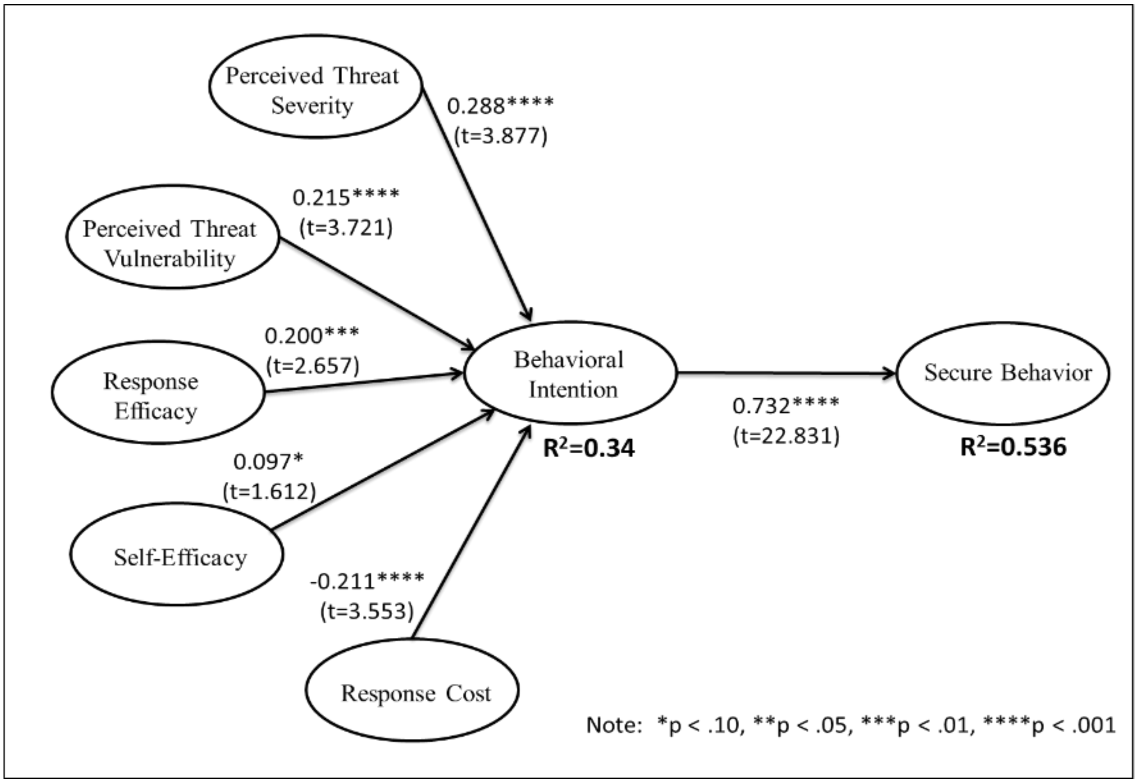


Figure 4.1 Lock PC: Baseline Model (Without Habit)

www.manaraa.com

This model accounts for 53.6 percent of the variance of self-reported actual behavior and 34 percent of the variance in behavioral intention to perform a secure behavior. The p-value for self-efficacy was slightly more than 0.05 ($p=0.0539$) and the majority of the previous PMT related studies have found self-efficacy to significantly influence behavioral intentions. Therefore, we looked for a suppressor effect, which is defined as a situation where "one independent variable hides or suppresses the true effect of another" (Vance et al. 2012). We found that both response efficacy and response cost acted as suppressors for self-efficacy in our model. When self-efficacy was considered without the suppressor variables, it positively influenced intention with a path coefficient of 0.246 at $p<0.001$, which is consistent with PMT.

Lock PC Behavior: Habit as a Direct Effect

In the second research model, habit is hypothesized to have a direct effect on secure behavior. The results for this model are shown on Figure 4.2. Similar to the first model, self-efficacy was significant at the 0.10 level with a p-value of 0.06, while all of the other hypothesized relationships significant at $p<0.001$.

The introduction of habit as a direct effect on behavior increased variance explained from 53.6 percent to 59.6 percent, with a path coefficient of 0.301, supporting H_{7a}. The path coefficient between behavioral intention and secure behavior decreased from 0.732 to 0.558, but remained significant. These values confirm the definition of habit adopted by this study, such that when habit is established, it reduces the importance of behavioral intention in the performance of actual behavior.

المنارة للاستشارات

www.manaraa.com

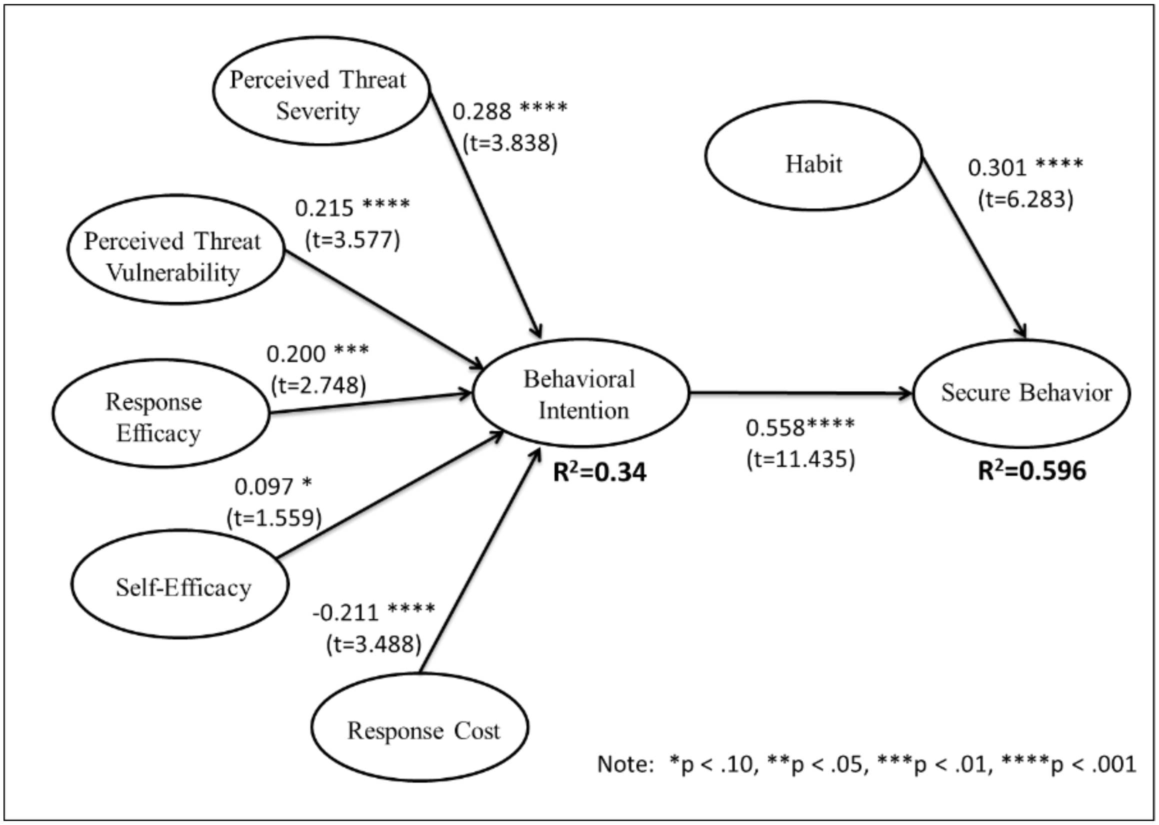


Figure 4.2 Lock PC: Habit as a Direct Effect

Lock PC Behavior: Habit as a Moderator and a Direct Effect

In the third and final research model, habit is included as a direct effect on secure behavior and in addition as moderating the relationship between behavioral intention and behavior. The results for this model are shown in Figure 4.3.

www.manaraa.com

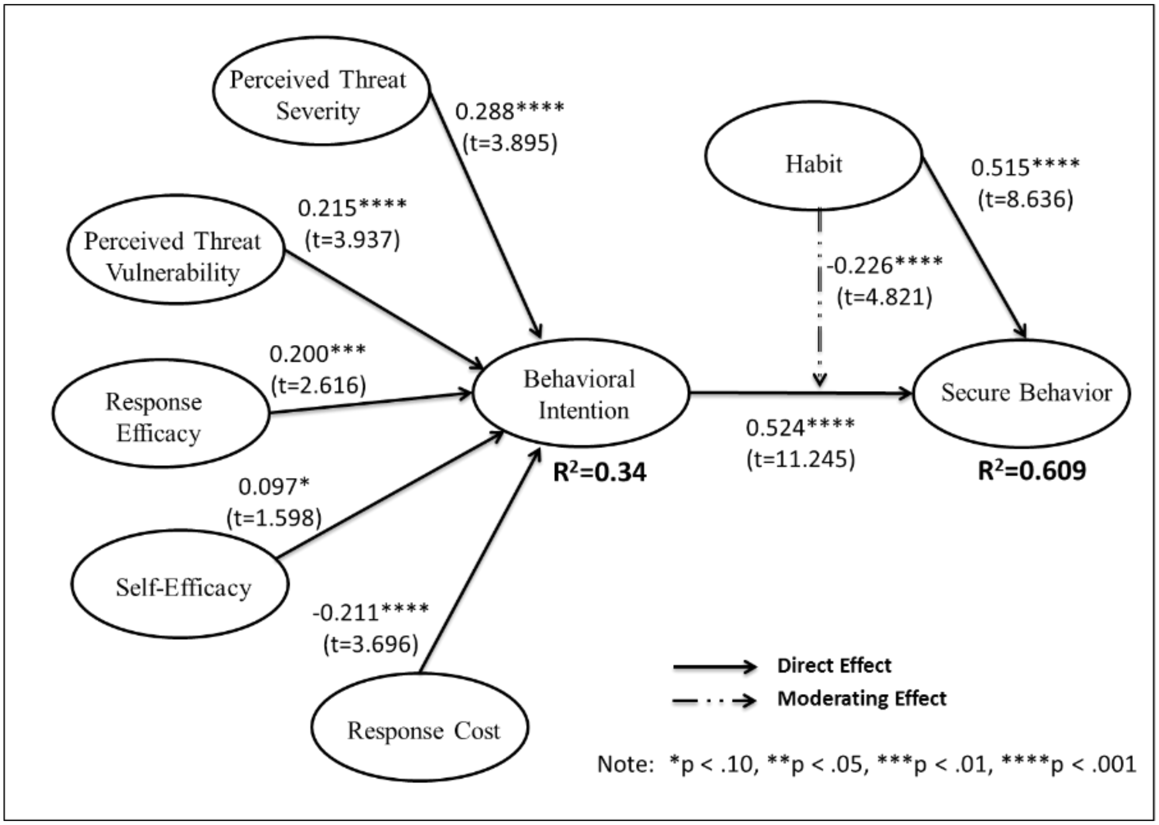


Figure 4.3 Lock PC: Habit as a Moderator

The introduction of habit as a moderator increased the total variance explained by secure behavior slightly from 59.6 percent to 60.9 percent. The moderating effect of habit on the relationship between behavioral intention and secure behavior had a path coefficient of -0.226 at p<0.001 supporting H_{7b}. The path coefficient between behavioral intention and secure behavior also decreased slightly from 0.558 to 0.524, but the relationship was still significant. A summary of the results for the third (complete) research model is shown in Table 4.17. It is also evident that when the moderation effect is taken into account, the direct effects of habit and behavioral intention on actual behavior are nearly equal for the Lock PC behavior. Tests for significance of control

www.manaraa.com

variables indicated that education significantly influenced habit such that higher educated individuals demonstrated higher habits. However, education did not have significant effects behavioral intention or behavior. Other control variables such as age, gender and industry had non-significant effects on habit, behavioral intention or behavior.

Table 4.17 Lock PC: Summary of Findings

Hypothesis (with direction)	**Path Coefficient (β)**	**T Value**	**P-Value**	**Support**
H_1: PSEV → BINT (+)	0.288	3.895	$p < 0.001$	Supported
H_2: PVUL → BINT (+)	0.215	3.937	$p < 0.001$	Supported
H_3: REFF → BINT (+)	0.200	2.616	$p < 0.001$	Supported
H_4: SEFF → BINT (+)	0.097	1.598	$p <0.100$ ($p=0.06$)	Supported
H_5: RCST → BINT (-)	-0.211	3.696	$p < 0.001$	Supported
H_6: BINT → BEHV (+)	0.524	11.245	$p < 0.001$	Supported
H_{7a}: HBT → BEHV (+)	0.515	8.636	$p < 0.001$	Supported
H_{7b}: HBT * INT (-)	-0.226	4.821	$p < 0.001$	Supported

To test for moderation using PLS, Chin et al. (1996) suggested comparing the R-square values of a model that includes the interaction construct with a model that does not include the interaction construct. The overall effect size f^2 for the moderation can be calculated from the difference in R-squares of the two models. Cohen (1988) has suggested that overall effect size for the interaction of 0.02 or below to be a small effect, 0.02-0.15 to be a medium effect and 0.15 or above to be a large effect. However, “it is important to understand that a small f^2 does not necessarily imply an unimportant effect” (Limayem et al. 2007, p. 729) . The overall effect size of the moderation (f^2) can be calculated by the following formula:

$$f^2 = (R^2_{\text{included}} - R^2_{\text{excluded}}) / 1 - R^2_{\text{included}} \qquad (4.1)$$

المنارة للاستشارات
www.manaraa.com

Based on the R-square difference tests between the models with habit modeled as only a direct effect and habit additionally modeled as a moderator, the additional moderation effect was found to have a value of 0.033, which is a medium effect (Chin et al. 2003; Cohen 1988). It is also evident that the third (complete) model demonstrates higher explanatory power than previous two models. Therefore, the research model where habit is hypothesized to moderate the relationship between behavioral intentions and secure behavior and the model where habit is hypothesized to have only a direct effect on secure behaviors have significantly higher explanatory power than the baseline model that does not consider habit. The research model also has slightly better explanatory power than the model in which habit is hypothesized to have only a direct effect on secure behavior. The results of the R-square difference tests are shown in Table 4.18.

Table 4.18 Lock PC: Effect Size Calculations

Model	**R^2**	**f-statistics**	
Baseline Model (Without Habit)	0.536	0.187	
Research Model (Habit as a Moderator)	0.609		0.033
Habit as a Direct Effect	0.596		

Post hoc Analyses

To further test the validity of using habit as a formative measure, several alternative models were analyzed as a post hoc step. Scholars suggest that post hoc analysis could be performed to test alternative models that may strengthen the statistical findings or assist in developing a model that has better explanatory power. The construct

المنارة للاستشارات
www.manaraa.com

of habit has been a topic of much debate among scholars, and has been modeled in different ways, which we review next and compare our research model.

Habit conceptualized as Limayem et al. 2007

Habit has not yet received much attention in IS research and has received even less attention in information security research. Limayem et al. (2007) investigated the role of habit as a moderator of the intention-behavior relationship in the context of IS continuance. While they tested a research model similar to our study, they tested habit with a reflective scale that failed to capture the true multi-dimensional nature of habit. However, as a part of this study, data were collected for the reflective scale of Limayem et al. (2007) which allows comparison of the research model of this study using both formative and reflective scales for habit.

The two models for habit were tested using SmartPLS, and the results are shown in Table 4.19. The path coefficients of the PMT variables of both models remained the same and are not displayed in the table. The magnitude of the path coefficient of the intention-behavior relationship was higher (0.524) in our research model with the formative scale, compared to the same model tested with the reflective scale (0.275).

www.manaraa.com

Table 4.19 Lock PC: Formative vs. Reflective Habit Measures

Hypothesis (with direction)	Habit as Second-Order Formative	Habit as Conceptualized in Limayem et al. 2007
H_6: BINT → BEHV (+)	0.524**** (t=11.245)	0.275**** (t=3.379)
H_{7a}: HBT → BEHV (+)	0.515**** (t=8.636)	0.750**** (t=11.019)
H_{7b}: HBT → INT-BEHV (-)	-0.226**** (t=4.821)	-0.143* (t=1.386)
R^2 of BINT	0.340	0.340
R^2 of BEHV	0.609	0.710
Effect Size (Moderator vs. Base Model)	0.187	0.600
Effect Size (Moderator vs. Direct Effect)	0.033	0.003

Note: *p < .10, **p < .05, ***p < .01, ****p < .001

Habit demonstrated a higher direct impact on secure behavior when tested with reflective scales, even though both relationships were significant at p<0.001. Both models demonstrated that habit was a significant negative moderator of the intention-behavior relationship. However, with the formative construct, the moderation coefficient was higher (-0.226) and highly significant (p<0.001) compared with the reflective the reflective scale results (0.143, and p<0.01). This indicates that when habit is conceptualized as a formative construct, which accurately captures the habit domain, the negative moderating effect of habit is stronger compared to the 3-item reflective scale. The R-square value of secure behavior was higher with the reflective scale, demonstrating better explanatory power. One of the reasons for the higher explanatory power may be due to the language of the reflective items being closely related to the items that measure behavioral intention and behavior. The fact that the respondents could not distinguish between the different constructs, may have caused the correlations to increase resulting in a higher R-square value. The formative habit scale contains

المنارة للاستشارات
www.manaraa.com

measurement items that are clearly different from the behavioral intention and behavior scale items.

The effect sizes of the moderation were compared between the two models. Both models had a large effect size when comparing the baseline model to the model with habit has a moderator. However, the effect size, when comparing the model of habit as a direct effect to the model with habit as a moderator, was medium when tested with the formative scale and was very small when tested with the reflective scale. This provides further evidence that the negative moderating effect of habit is stronger when habit is conceptualized as a second-order formative construct.

Habit as a Mediator of the PMT-Intention Relationship

Vance et al. (2012), one of the few studies in information security that has explored the role of habit, modeled PMT variables as mediators of the relationship between habit and behavioral intention. As mentioned previously, any indirect relationship of habit towards actual behavior does not reflect the definition of habit, where habit is defined to be a form of automaticity. However, since the Vance et al. (2012) study is closely related to our study, we decided to test their model in the post hoc analysis. It is important to note that Vance et al. (2012) measured habit with a 12-item self-report habit index (SRHI), which was a reflective scale developed by (Verplanken and Orbell 2003). We tested the Vance et al. (2012) research model with both the formative and the reflective habit measures separately.

First we tested the Vance et al. (2012) research model with the first-order reflective and second-order formative habit scale and the results are shown in Figure 4.4. Path coefficients of the PMT-intention and intention-behavior relationships remained the

المنارة للاستشارات

www.manaraa.com

same as the previous models. The formative habit construct demonstrated significant influence on the threat appraisal variables: perceived threat severity and perceived threat vulnerability. However, none of the coping appraisal variables were significantly influenced by the formative habit construct.

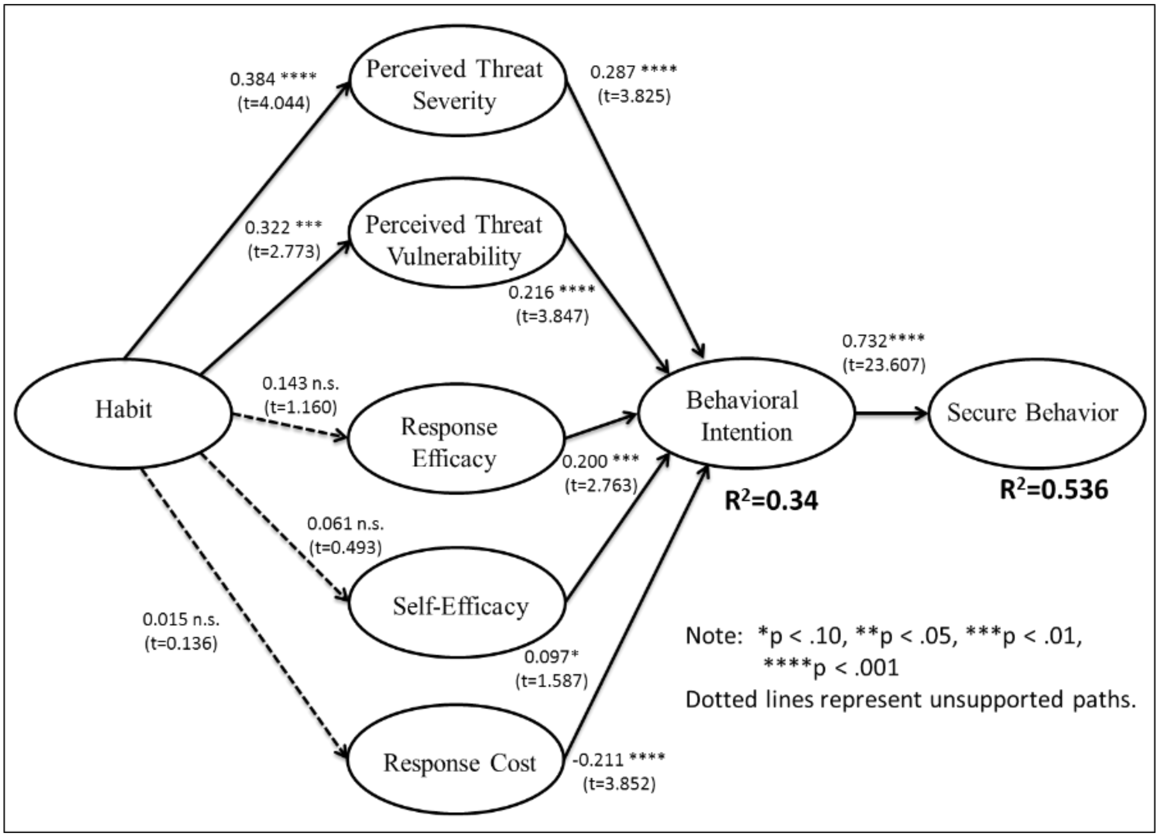


Figure 4.4 Lock PC: Habit (Formative) as an Indirect Influence

Next, we tested the Vance et al. (2012) research model with the 3-item reflective scale developed by Limayem et al. (2007) and the results are shown in Figure 4.5. The test results were identical to the findings of the Vance et al.'s (2012) study. Habit significantly influenced all the PMT variables with the highest path coefficient being

www.manaraa.com

0.470 (p<0.001) between habit and perceived threat severity. It is also important to note that habit negatively influenced response cost, which demonstrates that habitual secure behaviors decreases the perceived response costs associated with the behavior. This was consistent with the findings of Vance et al. (2012). However, the research model of Vance et al. (2012) demonstrated a higher explanatory power with an R-square of 44 percent compared to 34 percent in each of our research models where habit was measured formatively and reflectively.

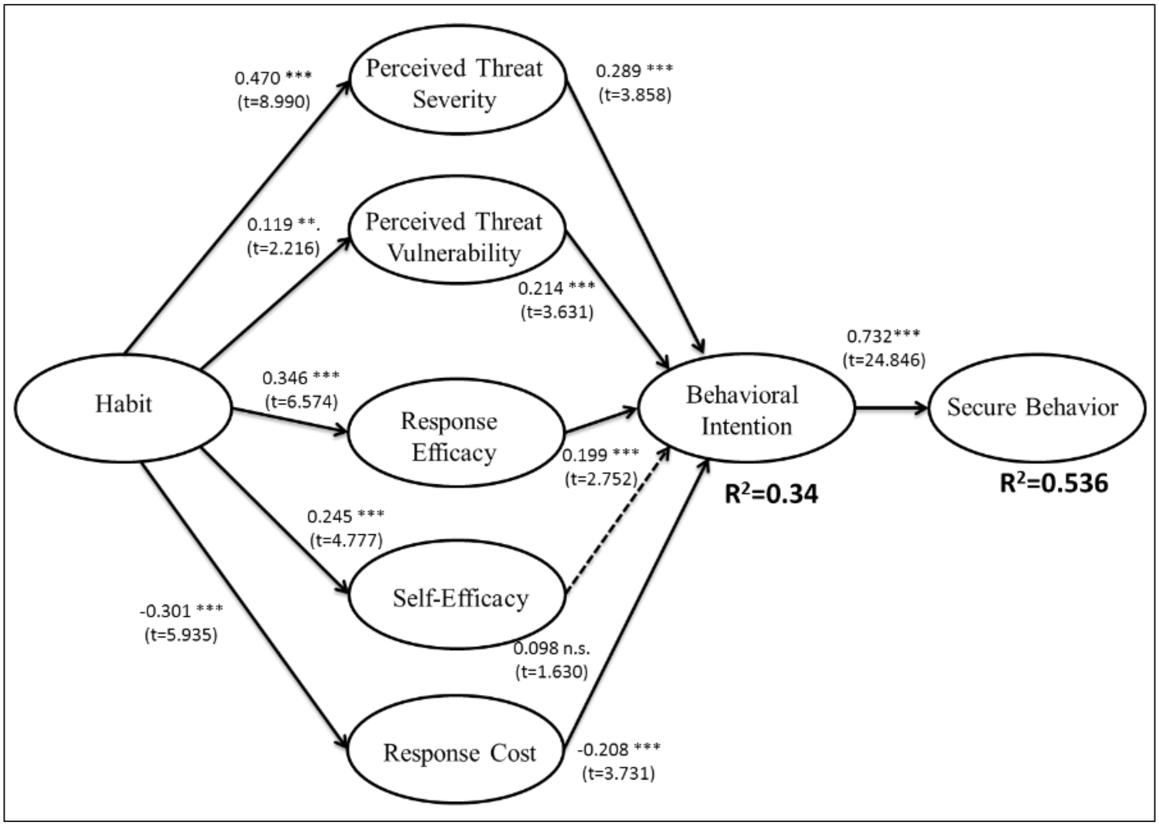


Figure 4.5 Lock PC: Habit (Reflective) as an Indirect Influence

www.manaraa.com

This may indicate that the language of the reflective items may be similar and highly correlated to behavioral intention and PMT variables. However, when the formative items are used to test the same model, several paths were not supported. The formative habit construct makes the language of different dimension items more distinct such that respondents may be more likely to recognize the distinction from the behavioral intention items.

Inertia as a mediator of Habit-Intention Relationship

This study adopted the first-order reflective and second-order habit construct scale from Polites and Karahanna (2012). Inertia is defined as the "attachment to, and persistence of, existing behavioral patterns (i.e., the status quo), even if there are better alternatives or incentives to change" (Polites and Karahanna 2012, p. 24). They hypothesized that habit will positively influence inertia and that inertia will negatively influence intention to use a new system. Although the applicability of inertia to this study was not immediately evident, it seemed fruitful to consider the possible relationship between inertia and habit. Accordingly, inertia was measured as part of the data collection and an alternative model was tested as a part of the post hoc analysis. As discussed in Chapter III, inertia was considered to be a first-order reflective and second-order formative construct. However, only the behavior-based inertia and affective-based inertia components were measured here, since the cognitive-based inertia component is not applicable in the context of this study.

Similar to the formative habit construct, a two stage approach was followed where the PLS latent scores for each dimensions were used as weights for the formative measures of the inertia construct (Polites and Karahanna 2012). Affective-based inertia

المنارة للاستشارات

www.manaraa.com

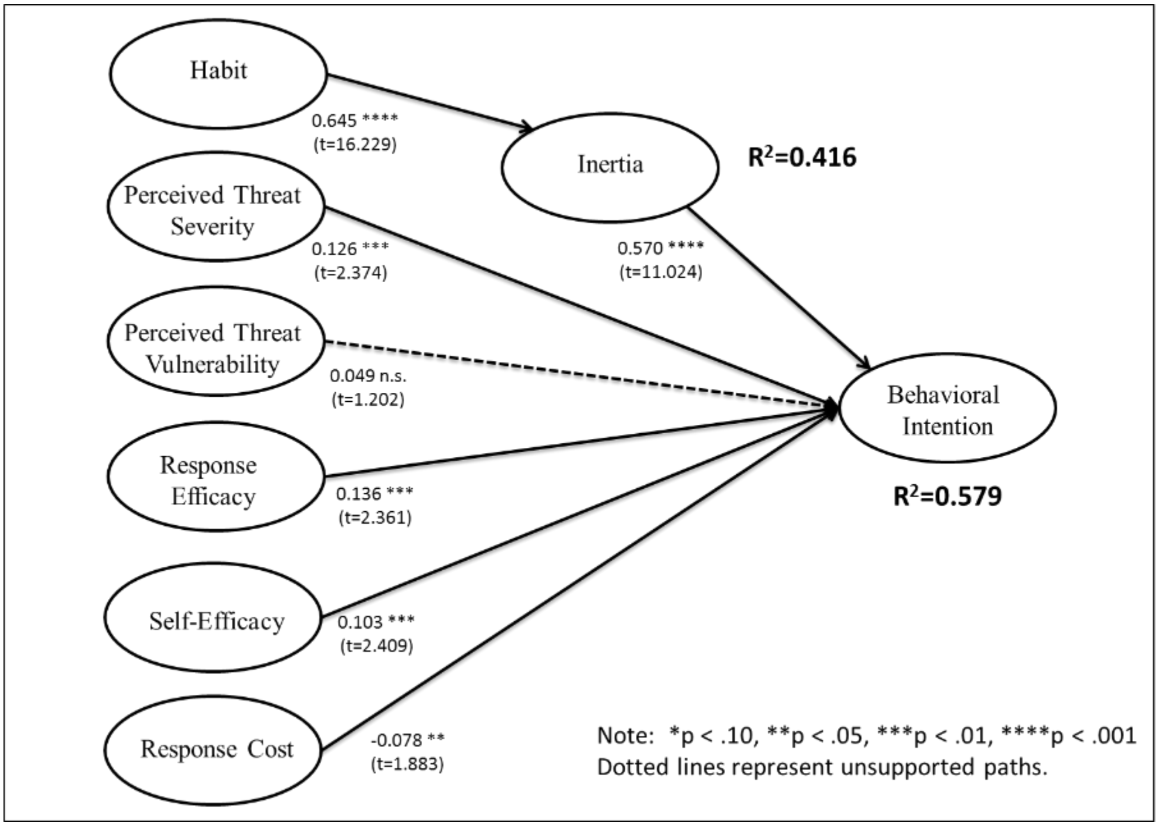
demonstrated a weight of 0.262 (p<0.01) and behavior-based inertia demonstrated a weight of 0.786 (p<0.001), and thus were suitable to be included in the data analysis. Habit was modeled as positively influencing inertia and inertia was modeled as positively influencing behavioral intention, which corresponds to the research model of Polites and Karahanna (2012).

The results of the data analysis are shown in Figure 4.6. All the PMT variables significantly influenced behavioral intention except perceived threat vulnerability. Habit significantly influenced inertia with a path coefficient of 0.645 (p<0.001) and inertia significantly influenced behavioral intention with a coefficient of 0.570 (p<0.001). Habit also explained 41.6 percent of the variance in inertia. Inertia was hypothesized to negatively influence behavioral intentions by Polites and Karahanna (2012) and they found support for their hypothesis. However, the results of this alternative model found that path to be significant, but positive, which means that increased levels of inertia leads to increased behavioral intention to perform secure behavior. R-square of the behavioral intention was 57.9 percent. Mediation tests revealed that inertia partially mediated the relationship between habit and behavioral intention. Another research model where a reflective habit construct was utilized yielded similar results with similar explanatory power.

A research model that included direct paths to behavioral intention from both habit and inertia demonstrated an R-square value of 61 percent, slightly increasing the explanatory power of the model due to the direct influence of habit on behavioral intention. The results suggest that inertia increased the explanatory power of the research model, indicating that it may play a role in the performance of secure behaviors, although

المنارة للاستشارات
www.manaraa.com

the path was significant in the opposite direction compared to the results of Polites and Karahanna (2012). This discrepancy of the results will be discussed in detail on Chapter V.



Note: *p < .10, **p < .05, ***p < .01, ****p < .001
Dotted lines represent unsupported paths.

Figure 4.6 Lock PC: Inertia as a Mediator of Habit and Intention

Habit as a Direct Influence of Behavioral Intention

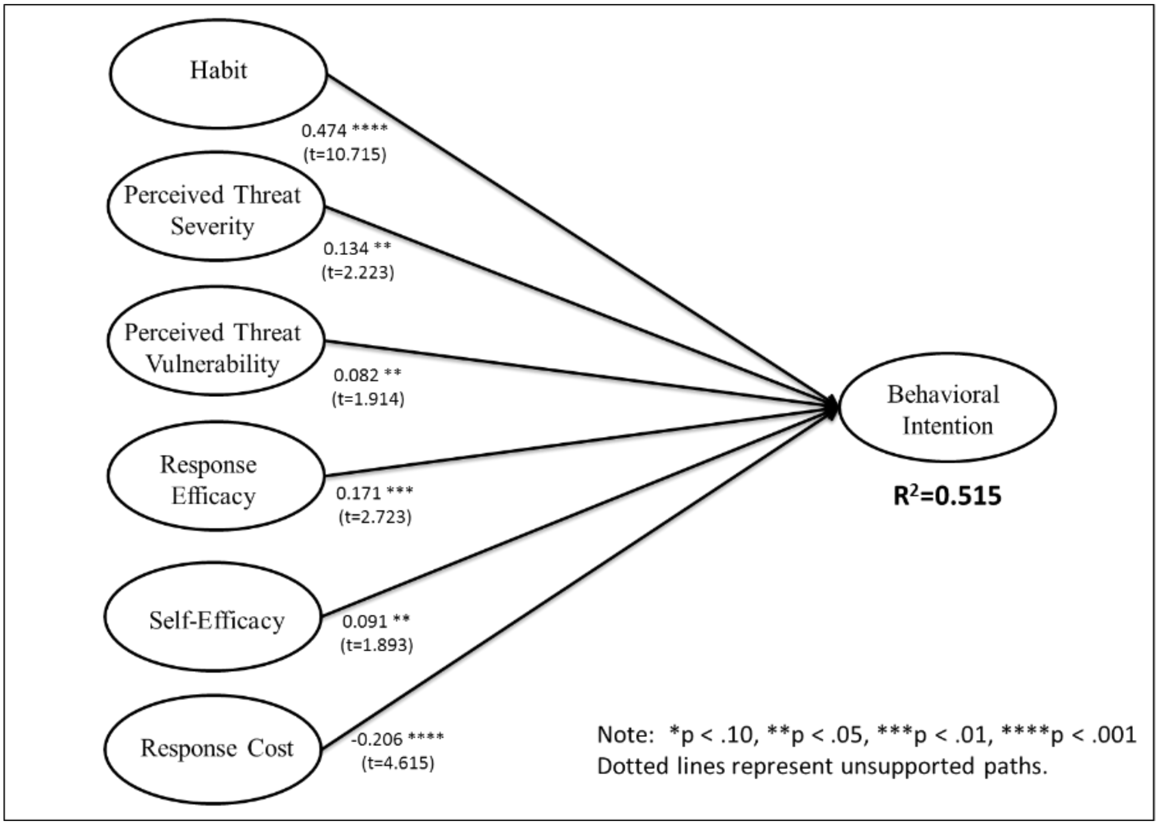
Several IS research studies that investigated the role of habit on information systems usage modeled habit as a direct influence on behavioral intention (Gefen 2003; Lankton et al. 2012; Wu and Kuo 2008). This is rather contradictory to the definition of habit where it is defined as a form of automaticity (Verplanken et al. 1997). This

المنارة للاستشارات
www.manaraa.com

dissertation also defines habit as a form of automaticity. Therefore, modeling habit as a direct influence on behavioral intention is contradictory. However, since previous IS studies have modeled habit as a direct influence of behavioral intention, a similar alternative model was tested as a part of the post hoc analysis.

First, the path between habit and behavioral intention was tested with the first-order reflective and second-order formative habit construct. The results of this analysis are shown in Figure 4.7. The path from habit to behavioral intention was significant with a path coefficient of 0.474 ($p<0.001$). All the paths from PMT variables to behavioral intention were significant with the lowest significant path being self-efficacy and behavioral intention ($p<0.01$). R-square value of behavioral intention was 51.5 percent explaining considerably more explanatory power than a baseline model without habit.

المنارة للاستشارات
www.manaraa.com



Note: *p < .10, **p < .05, ***p < .01, ****p < .001
Dotted lines represent unsupported paths.

Figure 4.7 Lock PC: Direct Influence of Habit on Behavioral Intention

Next, the same model was tested with the reflective habit scale. The paths from perceived severity to behavioral intention and response cost to behavioral intention were non-significant. Paths from perceived vulnerability, response efficacy, and self-efficacy to behavioral intention were significant. The path from habit to behavioral intention was significant with a path coefficient of 0.673 (p<0.001). R-square of behavioral intention was 65.5 percent compared to the R-square of 51.5 percent when the model was tested with the formative habit scale. Therefore, the model with a reflective habit scale demonstrated higher explanatory power than the model with a formative habit scale when habit was modeled as a direct influence of behavioral intention.

www.manaraa.com

Habit as a Moderator of the PMT-Behavior Relationship

Information security literature suggests that measuring actual behavior is preferred rather than intentions (Anderson and Agarwal 2010; Crossler et al. 2013; Mahmood et al. 2010; Warkentin et al. 2012). As discussed previously, actual behaviors are of more importance in information security since behavioral intentions do not necessarily lead to actual secure behavior. Therefore, it is recommended that researchers collect data on actual behavior whenever possible since most information security studies utilize behavioral intention as a proxy for actual behaviors (Crossler et al. 2013).

As a part of the post hoc study, an alternative model where PMT variables directly influenced actual behavior was tested. Habit was hypothesized to directly influence secure behavior while moderating the relationships between the PMT variables and actual behavior. The results of this analysis are shown in Figure 4.8.

Paths from perceived threat severity, response efficacy, self-efficacy, response cost, and habit to secure behavior were significant. Path from perceived threat vulnerability to secure behavior were insignificant. Similarly, habit did not significantly moderate the paths from perceived threat vulnerability and response efficacy to secure behavior. Habit significantly moderated the paths from perceived threat severity, self-efficacy and response cost to secure behavior. It is important to note that habit negatively moderated the path between perceived threat severity and secure behavior demonstrating that when a certain behavior is habitual, the perceived severity of the threat is lesser. Similarly, when a certain behavior is habitual, self-efficacy and response cost increases. This is demonstrated in habit significantly moderating the paths between response cost and self-efficacy with secure behavior.

www.manaraa.com

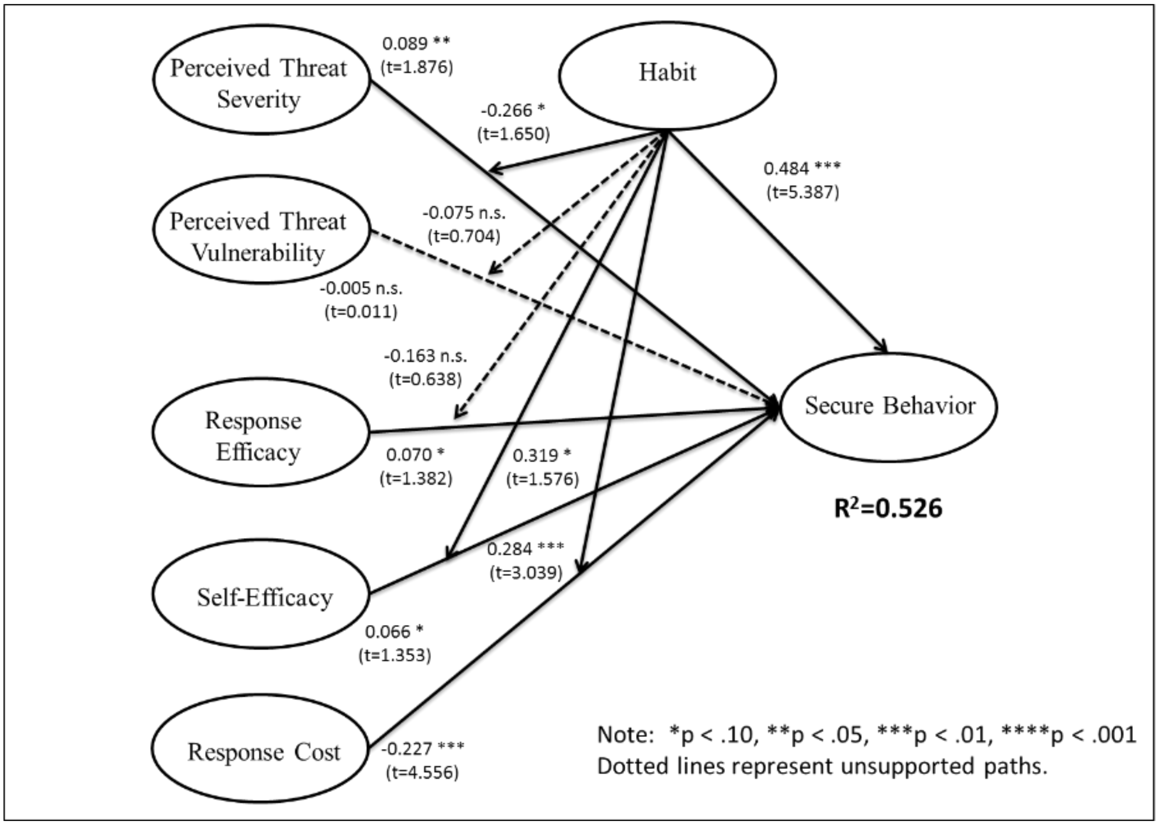


Figure 4.8 Lock PC: Habit as a Moderator of PMT Behavior

Behavior 2: Verify Email Recipients (n=443)

The second behavior tested was "verifying the email recipient addresses before sending email." A total of 500 responses were collected for this behavior, and the surveys were completed in an average of four minutes and twenty-one seconds. Responses that were incomplete or failed the response set item were removed. This resulted in a usable sample of 443 responses, which exceeded the required sample size of 308 as calculated through the power analysis.

Of the usable responses, 288 (65%) were male and 155 (35%) were female. There were 117 (26.4%) respondents who were between the ages of 18 and 24, 216 (48.8%)

المنارة للاستشارات
www.manaraa.com

were between the ages of 25 and 34, 74 (16.7%) were between the ages of 35 and 44, 20 (4.5%) were between the ages of 45 and 54, 15 (3.4%) were between the ages of 55 and 64 and 1 (0.2%) were age 65 or above. In terms of the education of the respondents, 142 (32.1%) had a 2-year college degree or lesser, 201 (45.4%) had a 4-year college degree, 94 (21.2%) had a master’s degree and 6 (1.35%) had a doctoral degree or a professional degree.The respondents were employed in various industries and the majority of the respondents belonged to the categories of Information (18.5%), professional, scientific or technical services (12.0%) and educational services (10.4%). Table 4.20 provides the demographic details of the respondents who participated in this study.

المنارة للاستشارات
www.manaraa.com

Table 4.20 Verify Email Recipients: Demographics of Main Investigation

Demographic	Category	Frequency
Gender	Male	288 (65.0%)
	Female	155 (35.0%)
Age	18-24	117 (26.4%)
	25-34	216 (48.8%)
	35-44	74 (16.7%)
	45-54	20 (4.5%)
	55-64	15 (3.4%)
	65 and older	1 (0.2%)
Education	Less than High School	2 (0.5%)
	High School / GED	29 (6.5%)
	Some College	72 (16.3%)
	2-year College Degree	39 (8.8%)
	4-year College Degree	201 (45.4%)
	Masters Degree	94 (21.2%)
	Doctoral Degree	2 (0.5%)
	Professional Degree (JD, MD)	4 (0.9%)
Industry	Forestry, fishing, hunting or agriculture support	2 (0.5%)
	Mining	3 (0.7%)
	Utilities	4 (0.9%)
	Construction	15 (3.4%)
	Manufacturing	32 (7.2%)
	Wholesale trade	7 (1.6%)
	Retail trade	22 (5.0%)
	Transportation or warehousing	8 (1.8%)
	Information	82 (18.5%)
	Finance or insurance	37 (8.4%)
	Real estate or rental and leasing	7 (1.6%)
	Professional, scientific or technical services	53 (12.0%)
	Management of companies or enterprises	16 (3.6%)
	Admin, support, waste management or remediation services	15 (3.4%)
	Educational services	46 (10.4%)
	Health care or social assistance	30 (6.8%)
	Arts, entertainment or recreation	13 (2.9%)
	Accommodation or food services	5 (1.1%)
	Other services (except public administration)	37 (8.4%)
	Unclassified establishments	9 (2.0%)

المنارة للاستشارات
www.manaraa.com

As with the previous behavior, an EFA was repeated for the main investigation with a sample size of 443, since minor changes were made to the language of certain items following the preliminary investigation phase. The items demonstrated an acceptable response spread and no unusual patterns in the means and standard deviations were found. Bartlett's Test of Sphericity was significant at 0.000 and Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy test result of 0.883 indicated that factor analysis was appropriate for this sample (Hair et al. 2010).

The EFA was conducted using the Principal Component Analysis (PCA) technique with a Varimax rotation. Ten factors with an Eigenvalue of one or greater, were extracted and those factors explained a total of 74.66% of the variance, which is above the 65% recommended by Hair et al. (2010). The communalities of the items were well above the accepted threshold of 0.30.

All the items loaded cleanly on their respective factors except EFFC2, which had a loading of 0.437. EFFC2 had a similar cross-loading issue during the EFA of behavior 1 as well, indicating that it may be a problematic item. EFFC2 was removed, and the EFA was re-run. This improved the factor loadings, and the remaining items loaded cleanly on their respective factors. The results of the EFA are shown in Table 4.21. Correlations lower than 0.40 in absolute value were suppressed for clarity. BINT1 had a loading of 0.599, which is lower than the recommended 0.70 loadings. However, BINT1 did not cross-load with any other factors and the removal of BINT1 from the EFA did not contribute to better loadings. Therefore, BINT1 was retained for the data analysis.

المنارة للاستشارات
www.manaraa.com

Table 4.21 Verify Email Recipients: EFA results of Main Investigation

Rotated Component Matrix[a]

	Component									
	1	2	3	4	5	6	7	8	9	10
AWAR1	.809									
AWAR2	.797									
AWAR3	.802									
AWAR4	.842									
BEHV1		.799								
BEHV2		.825								
BEHV3		.704								
BINT1			.599							
BINT2			.787							
BINT3			.707							
CTRL1				.859						
CTRL2				.870						
CTRL3				.866						
CTRL4				.848						
EFFC1					.799					
EFFC3					.719					
EFFC4					.704					
PSEV1						.829				
PSEV2						.777				
PSEV3						.875				
PVUL1							.804			
PVUL2							.827			
PVUL3							.808			
RCST1								.844		
RCST2								.842		
RCST3								.788		
RCST4								.819		
REFF1									.728	
REFF2									.785	
REFF3									.717	
REFF4									.767	
SEFF1										.731
SEFF2										.685
SEFF3										.784
SEFF4										.723

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

المنارة للاستشارات

www.manaraa.com

Measurement Model

SmartPLS was used again to test both the measurement model and structural model similar to the previous behavior that was tested. A measurement model analysis was conducted to examine the psychometric properties of all the reflective constructs included in the research model. PLS validation procedures outlined by Gefen and Straub (2005) were followed to establish the validity and reliability of the measurement model. All the scales except EFFC had alpha values larger than the recommended threshold. EFFC had an alpha value of 0.669, which was still acceptable. All the scales demonstrated composite reliability values much higher than the recommended ones with the lowest value being 0.819 for the scale EFFC.

Table 4.22 Verify Email Recipients: Reliability Statistics

Construct		**AVE**	**C-Alpha**	**CREL**	**Mean (St. dev)**	**Min/Max**
AWAR	Lack of Awareness	0.707	0.862	0.906	3.44 (0.888)	1.0/5.0
BEHV	Actual Behavior	0.802	0.877	0.924	4.00 (0.782)	1.0/5.0
BINT	Behavioral Intention	0.742	0.827	0.896	3.91 (0.771)	1.0/5.0
CTRL	Uncontrollability	0.797	0.915	0.940	3.22 (0.988)	1.0/5.0
EFFC	Mental Efficiency	0.602	0.669	0.819	3.44 (0.774)	1.0/5.0
PSEV	Perceived Severity	0.753	0.836	0.901	3.76 (0.853)	1.0/5.0
PVUL	Perceived Vulnerability	0.767	0.858	0.908	2.84 (1.123)	1.0/5.0
RCST	Response Cost	0.762	0.897	0.928	2.80 (1.035)	1.0/5.0
REFF	Response Efficacy	0.707	0.863	0.906	4.00 (0.725)	1.0/5.0
SEFF	Self-Efficacy	0.683	0.845	0.896	4.13 (0.685)	2.0/5.0

All the items demonstrated loadings well above 0.7 showing above acceptable reliability. The values of the reliability tests such as composite reliability and Cronbach's alpha are shown in Table 4.22 and item loadings are shown in Table 4.23. These values indicate that the scales satisfy the reliability requirements.

www.manaraa.com

Convergent validity requirements such as item loadings that exceed 0.70 on their respective constructs and Average Variance Extracted (AVE) above 0.50 (Gefen and Straub 2005) for each construct were examined. As shown in Table 4.24 all the item loadings exceeded 0.70 on their respective constructs. Table 4.22 shows that all the scales demonstrated AVE values well above 0.5. Therefore, all the scales of this study demonstrate convergent validity values that are beyond the recommended thresholds.

Table 4.23 Verify Email Recipients: Inter-Construct Correlations

	AWAR	BEHV	BINT	CTRL	EFFC	PSEV	PVUL	RCST	REFF	SEFF
AWAR	0.841									
BEHV	0.313	0.895								
BINT	0.272	0.646	0.861							
CTRL	0.347	0.208	0.281	0.893						
EFFC	0.252	0.219	0.276	0.321	0.776					
PSEV	0.185	0.349	0.337	0.242	0.090	0.868				
PVUL	0.138	-0.163	-0.151	0.171	0.020	0.055	0.876			
RCST	0.113	-0.225	-0.233	0.136	0.107	-0.004	0.555	0.873		
REFF	0.156	0.510	0.539	0.087	0.163	0.369	-0.266	-0.311	0.841	
SEFF	0.085	0.440	0.491	0.029	0.179	0.295	-0.318	-0.348	0.638	0.826

* The highlighted diagonal elements are square-roots of the AVE

Discriminant validity can be demonstrated if the square root of each construct's AVE is greater than the absolute value of the inter-construct correlations. As it is shown in Table 4.23, the square roots of the AVEs of all constructs were found to be larger than all cross-correlations of the other constructs, demonstrating discriminant validity of the constructs used in this study (Gefen and Straub 2005). Discriminant validity is also demonstrated when items load on their respective constructs more than any other construct, as it did in this study. PLS loadings and cross-loadings for all the items are shown in Table 4.24.

المنارة للاستشارات
www.manaraa.com

Table 4.24 Verify Email Recipients: PLS loadings for the Main Investigation

	AWAR	BEHV	BINT	CTRL	EFFC	PSEV	PVUL	RCST	REFF	SEFF
AWAR1	0.826	0.276	0.272	0.255	0.175	0.130	0.104	0.074	0.157	0.083
AWAR2	0.833	0.293	0.232	0.309	0.215	0.164	0.065	0.091	0.148	0.075
AWAR3	0.835	0.242	0.207	0.301	0.253	0.188	0.152	0.126	0.133	0.079
AWAR4	0.869	0.245	0.206	0.302	0.202	0.140	0.142	0.087	0.090	0.051
BEHV1	0.272	0.895	0.575	0.179	0.170	0.302	-0.138	-0.237	0.429	0.386
BEHV2	0.276	0.898	0.556	0.188	0.170	0.298	-0.136	-0.170	0.460	0.352
BEHV3	0.292	0.894	0.603	0.192	0.244	0.334	-0.163	-0.197	0.479	0.441
BINT1	0.250	0.610	0.882	0.225	0.191	0.315	-0.154	-0.269	0.531	0.463
BINT2	0.231	0.521	0.825	0.249	0.278	0.244	-0.100	-0.134	0.382	0.376
BINT3	0.221	0.532	0.876	0.257	0.256	0.306	-0.131	-0.185	0.466	0.423
CTRL1	0.317	0.213	0.247	0.888	0.259	0.201	0.171	0.125	0.043	-0.043
CTRL2	0.309	0.186	0.276	0.902	0.292	0.245	0.137	0.103	0.126	0.016
CTRL3	0.328	0.182	0.241	0.902	0.300	0.221	0.162	0.131	0.085	-0.026
CTRL4	0.285	0.161	0.240	0.878	0.295	0.198	0.141	0.125	0.056	-0.054
EFFC1	0.191	0.191	0.249	0.259	0.815	0.068	-0.088	-0.041	0.176	0.197
EFFC3	0.158	0.296	0.311	0.220	0.746	0.118	-0.065	-0.003	0.261	0.269
EFFC4	0.233	0.039	0.097	0.265	0.765	0.029	0.187	0.280	-0.038	-0.031
PSEV1	0.153	0.316	0.313	0.235	0.088	0.880	0.059	-0.008	0.327	0.223
PSEV2	0.181	0.283	0.292	0.208	0.069	0.840	0.073	0.015	0.304	0.298
PSEV3	0.148	0.308	0.268	0.184	0.075	0.882	0.008	-0.017	0.331	0.249
PVUL1	0.135	-0.107	-0.116	0.168	0.022	0.072	0.875	0.515	-0.225	-0.310
PVUL2	0.205	-0.093	-0.072	0.173	0.059	0.093	0.825	0.465	-0.217	-0.241
PVUL3	0.080	-0.193	-0.173	0.132	-0.003	0.016	0.924	0.490	-0.252	-0.283
RCST1	0.089	-0.240	-0.233	0.108	0.094	-0.028	0.513	0.911	-0.296	-0.303
RCST2	0.063	-0.173	-0.213	0.114	0.042	-0.012	0.414	0.860	-0.249	-0.294
RCST3	0.119	-0.129	-0.137	0.104	0.116	0.094	0.500	0.820	-0.188	-0.267
RCST4	0.133	-0.220	-0.210	0.147	0.133	-0.031	0.524	0.899	-0.327	-0.347
REFF1	0.095	0.412	0.446	0.072	0.147	0.288	-0.261	-0.307	0.835	0.561
REFF2	0.150	0.407	0.417	0.055	0.087	0.306	-0.191	-0.242	0.838	0.514
REFF3	0.172	0.452	0.519	0.101	0.161	0.357	-0.222	-0.251	0.863	0.561
REFF4	0.102	0.441	0.420	0.058	0.149	0.283	-0.220	-0.247	0.828	0.504
SEFF1	0.050	0.392	0.387	-0.025	0.165	0.220	-0.296	-0.343	0.527	0.829
SEFF2	0.088	0.377	0.445	-0.039	0.170	0.239	-0.265	-0.228	0.560	0.835
SEFF3	0.074	0.334	0.379	0.000	0.106	0.251	-0.264	-0.316	0.469	0.813
SEFF4	0.067	0.351	0.408	-0.030	0.148	0.266	-0.230	-0.276	0.546	0.829

المنارة للاستشارات

www.manaraa.com

Tests for Common Method Bias

Similar to the previous behavior, CMV tests were performed to assess any biases resulting from the use of the same method to collect data. We conducted statistical analysis using three tests to check for the presence of and severity of CMV in our data.

For the first test, we used the Harmon one-factor test (Podsakoff and Organ 1986; Podsakoff et al. 2003), where an exploratory factor analysis (EFA) was conducted on all the variables used in our model and the unrotated factor solution was examined. It is assumed that CMV exists if a single factor emerges from unrotated factor solutions or a first factor explains the majority of the variance in the variables (Podsakoff and Organ 1986). Ten factors emerged from the EFA, which accounted for 74.66% of the variance. The greatest variance explained by one factor was 24.38%, demonstrating that common method variance is unlikely to bias the results. A second test suggested by Pavlou et al. (2007) was conducted. Examining the inter-construct correlations in Table 4.23, the highest correlation among constructs is 0.646, which is not extremely high as suggested by Pavlou et al. (2007), thus ruling out CMV in this study.

For the third test, we used a more rigorous statistical approach suggested by Podsakoff et al. (2003) to check for common method bias. Table 4.25 shows the factor loadings for each major construct and factor loadings for the common method construct captured through this procedure.

للاستشارات المنارة
www.manaraa.com

Table 4.25 Verify Email Recipients: CMV Test Results

Construct	Indicator	Substantive Factor Loading (λs)	Substantive Factor Variance Explained (λs2)	Method Factor Loading (λm)	Method Factor Variance Explained (λm2)
Awareness	AWAR1	0.831	0.692	0.031	0.001
	AWAR2	0.822	0.676	-0.007	0.000
	AWAR3	0.834	0.696	-0.033	0.001
	AWAR4	0.878	0.771	-0.052	0.003
Behavior	BEHV1	0.915	0.837	-0.024	0.001
	BEHV2	0.951	0.903	-0.065	0.004
	BEHV3	0.821	0.674	0.089**	0.008
Behavioral Intention	BINT1	0.762	0.580	0.139	0.019
	BINT2	0.928	0.861	-0.118**	0.014
	BINT3	0.903	0.815	-0.030	0.001
Uncontrollability	CTRL1	0.892	0.796	-0.015	0.000
	CTRL2	0.892	0.795	0.041	0.002
	CTRL3	0.902	0.813	-0.002	0.000
	CTRL4	0.885	0.783	-0.025	0.001
Mental Efficiency	EFFC1	0.804	0.646	0.058	0.003
	EFFC3	0.726	0.527	0.154**	0.024
	EFFC4	0.803	0.645	-0.235**	0.055
Perceived Severity	PSEV1	0.873	0.762	0.002	0.000
	PSEV2	0.829	0.688	0.012	0.000
	PSEV3	0.901	0.811	-0.013	0.000
Perceived Vulnerability	PVUL1	0.891	0.795	-0.002	0.000
	PVUL2	0.908	0.824	0.060	0.004
	PVUL3	0.849	0.720	-0.059	0.003
Response Cost	RCST1	0.885	0.782	-0.034	0.001
	RCST2	0.849	0.720	0.001	0.000
	RCST3	0.889	0.791	0.083*	0.007
	RCST4	0.875	0.766	-0.045	0.002
Response Efficacy	REFF1	0.798	0.637	0.046	0.002
	REFF2	0.923	0.852	-0.095	0.009
	REFF3	0.762	0.580	0.106**	0.011
	REFF4	0.885	0.783	-0.059	0.003
Self-Efficacy	SEFF1	0.814	0.663	0.0268	0.001
	SEFF2	0.798	0.637	0.0301	0.001
	SEFF3	0.866	0.750	-0.0577	0.003
	SEFF4	0.828	0.686	0.0292	0.001
Average		**0.8571**	**73.7%**	**-0.0028**	**0.5%**

المنارة للاستشارات

www.manaraa.com

The results explain that the average loading of the indicators is 0.8571 while the average loading of the method indicators is -0.0028. The average variance explained by the substantive constructs is 73.7 percent compared to the 0.5 percent average variance explained by the method construct. Moreover, except for six indicators, all the method factor loadings were insignificant. Since the most of the method factor loadings are insignificant and the indicators' substantive variances are substantially greater than their method variances, it can be concluded that common method bias is unlikely to be a serious concern in the data of this study (Williams et al. 2003). Therefore, based on the three separate tests to measure CMV, we concluded that common method bias was not a concern for this study.

Structural Model

The structural models were then tested with the SmartPLS software. Factor scores for each of the first-order dimensions of habit were generated. These factors scores were used as formative measures of the second-order aggregate construct of habit (Chin et al. 2003; Polites and Karahanna 2012).

Reliability and validity tests that were performed on the first-order reflective dimensions of habit previously do not apply to formative scales because "the measurement model does not predict that the sub-dimensions will be correlated" (Bollen and Lennox 1991; Edwards 2003; MacKenzie et al. 2011, p.314). Item weights of the formative constructs can be examined to identify their individual influence in forming each construct (Chin 1998; Petter et al. 2007). The weights for the three habit dimensions were 0.719 for Lack of Awareness, 0.223 for Uncontrollability and 0.368 for Mental

المنارة للاستشارات
www.manaraa.com

Efficiency. The weight for Uncontrollability was not significant while Lack of Awareness and Mental Efficiency were significant at p<0.001.

The formative dimensions of the habit construct were tested for multicollinearity next. To test for multicollinearity, the variance inflation factor (VIF) statistics for the three dimensions of habit were examined. As shown in Table 4.26, VIF values are well below the recommended threshold value of 3.3 Diamantopoulos and Siguaw (2006), which indicates no serious multicollinearity issues with the formative dimensions of habit. Individual weights of the formative dimensions of habit also indicate that multicollinearity is not a concern.

Table 4.26 Verify Email Recipients: Weights of the Formative Habit Construct

Construct	**Dimension**	**Weight**	**VIF**
Habit	Lack of Awareness	0.719 (****)	1.115
	Uncontrollability	0.223 (n.s.)	1.068
	Mental Efficiency	0.368 (****)	1.137

Note: ****p<0.001

Although two of the formative dimensions of habit are significant, the dimension of Uncontrollability is not significant. Content validity of formative scales is affected if one of the indicators that represent one of the formative dimensions is removed. Since uncontrollability is one of the three dimensions that constitute habit, it was retained for the structural model analysis although its weight was not significant.

To test the role of habit in information security behaviors, data analyses were run in three stages, following the recommendations by Limayem et al. (2007). First, we ran a baseline research model with only the PMT variables. The next model added habit as a

المنارة للاستشارات
www.manaraa.com

direct effect on behavior. The final model added the possibility of habit moderating the relationship between behavioral intention and behavior.

Verify Email Recipient Behavior: Baseline Model

A baseline model, without the incorporation of the habit construct was tested first and the results are shown on Figure 4.9. Paths from perceived threat severity, response efficacy and self-efficacy to behavioral intention were significant (p<0.001) while paths from perceived threat vulnerability and response cost were not significant. The path from behavioral intention to secure behavior was also significant at p<0.001.

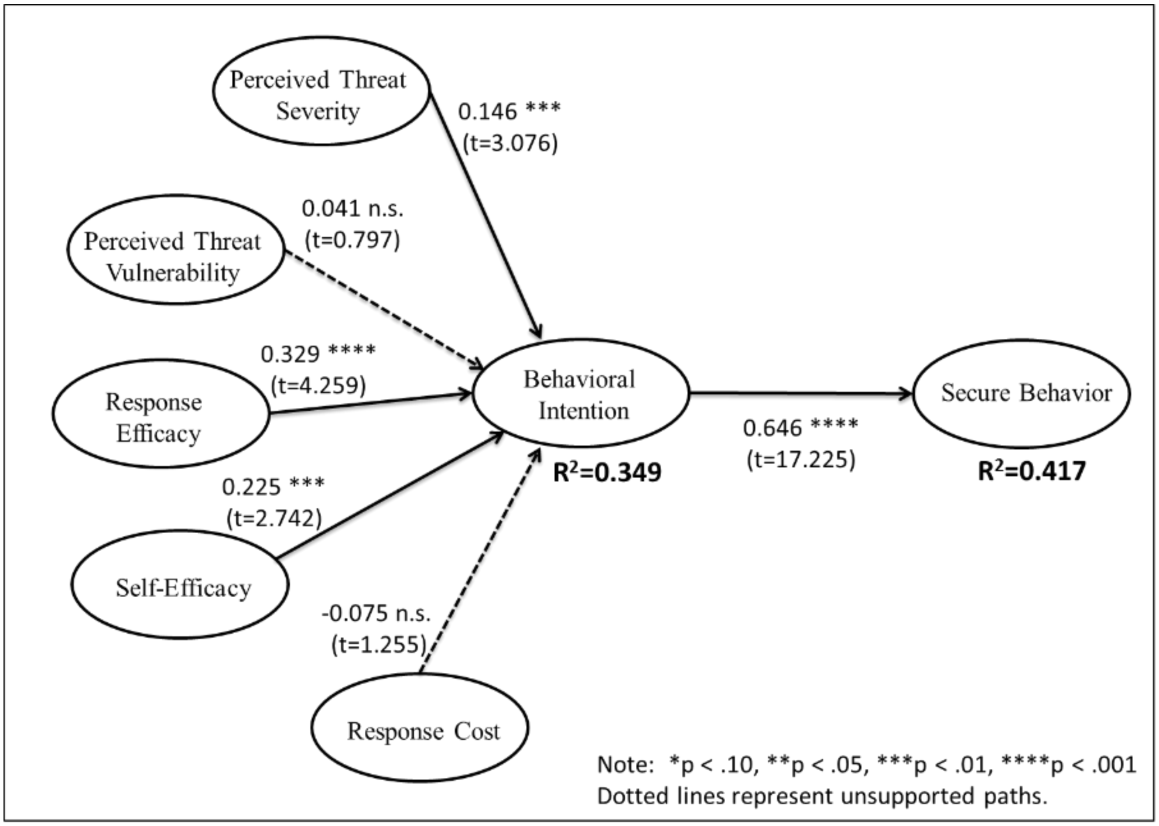


Figure 4.9 Verify Email Recipients: Baseline Model (Without Habit)

www.manaraa.com

This model accounts for 41.7 percent of the variance of self-reported actual behavior and 34.9 percent of the variance in behavioral intention to perform a secure behavior. Perceived threat vulnerability was not found to have a significant influence on behavioral intention, indicating that the respondents perceived the possibility of sending an email with sensitive company information to a wrong recipient as low. However, the results indicate that the respondents perceive it to be a severe problem, if an unintended recipient receives an email with sensitive company information. The non-significant path from perceived threat vulnerability to behavioral intention is was similar to the results of Johnston and Warkentin (2010), Malimage and Warkentin (2010) and Woon et al. (2005). The non-significant path from response cost and behavioral intention also indicates that the perceived costs of verifying the recipient email addresses before sending email are not significant enough to influence their intentions to perform that behavior.

Verify Email Recipient Behavior: Habit as a Direct Effect

In the second research model, habit is hypothesized to have a direct effect on secure behavior. The results for this model are shown on Figure 4.10. Similar to the first model, paths from perceived threat vulnerability and response cost were non-significant while the remaining paths were significant.

The introduction of habit as a direct effect on secure behavior increased variance explained by the self-reported behavior from 41.7 percent to 43.4 percent. Habit significantly influenced secure behavior with a path coefficient of 0.137 at p<0.01, supporting H7a. The path coefficient between behavioral intention and secure behavior reduced marginally from 0.646 to 0.597, but the relationship was still significant.

المنارة للاستشارات

www.manaraa.com

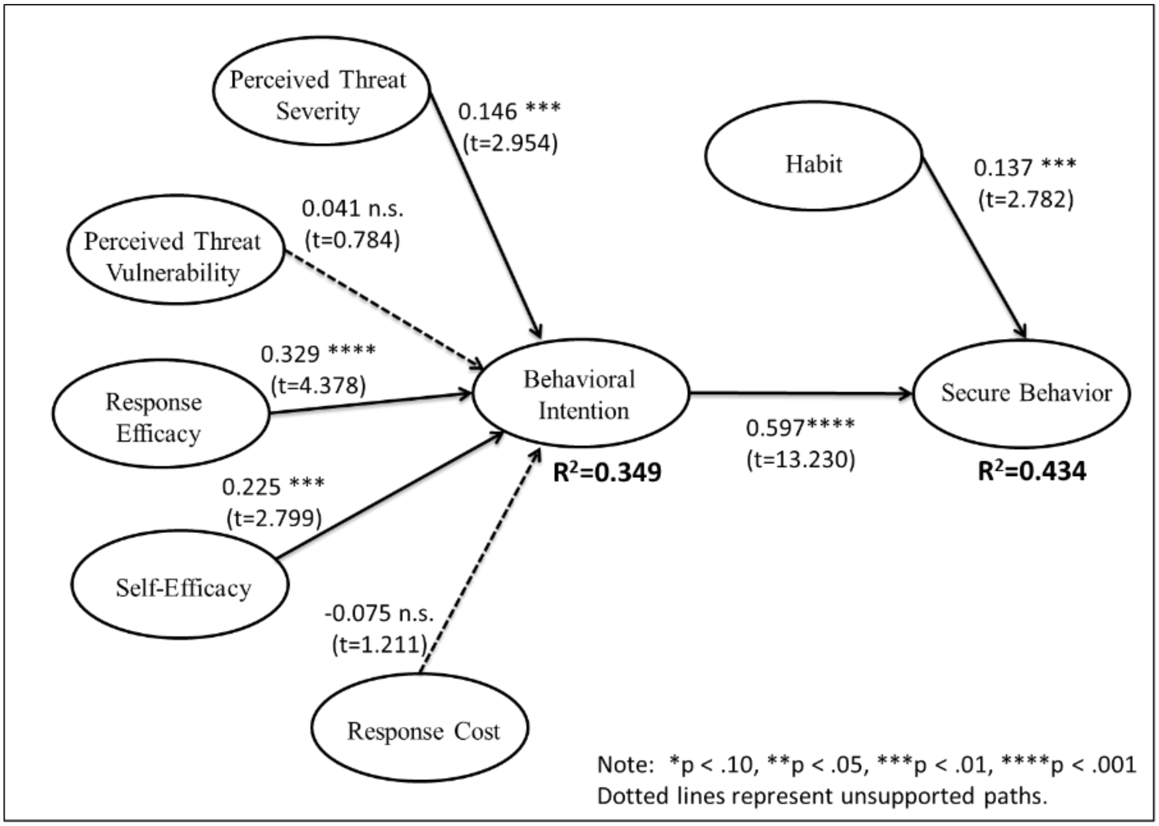


Figure 4.10 Verify Email Recipients: Habit as a Direct Effect

Verify Email Recipient Behavior: Habit as a Moderator and Direct Effect

In the third and final research model, habit is included as a direct effect on secure behavior and in addition as moderating the relationship between behavioral intention and behavior. The results for this model are shown in Figure 4.11.

The introduction of habit as a moderator increased the total variance explained by secure behavior slightly from 43.4 percent to 44.5 percent. The moderating effect of habit on the relationship between behavioral intention and secure behavior had a path coefficient of -0.114 at p<0.01 supporting H7b. The path coefficient between behavioral intention and secure behavior also reduced marginally from 0.597 to 0.551, but the

المنارة للاستشارات
www.manaraa.com

relationship was still significant. Tests for significance of control variables indicated that none of the control variables of age, gender, education and industry significantly influenced habit, behavioral intention or behavior. A summary of the results for the third (complete) research model is shown in Table 4.27.

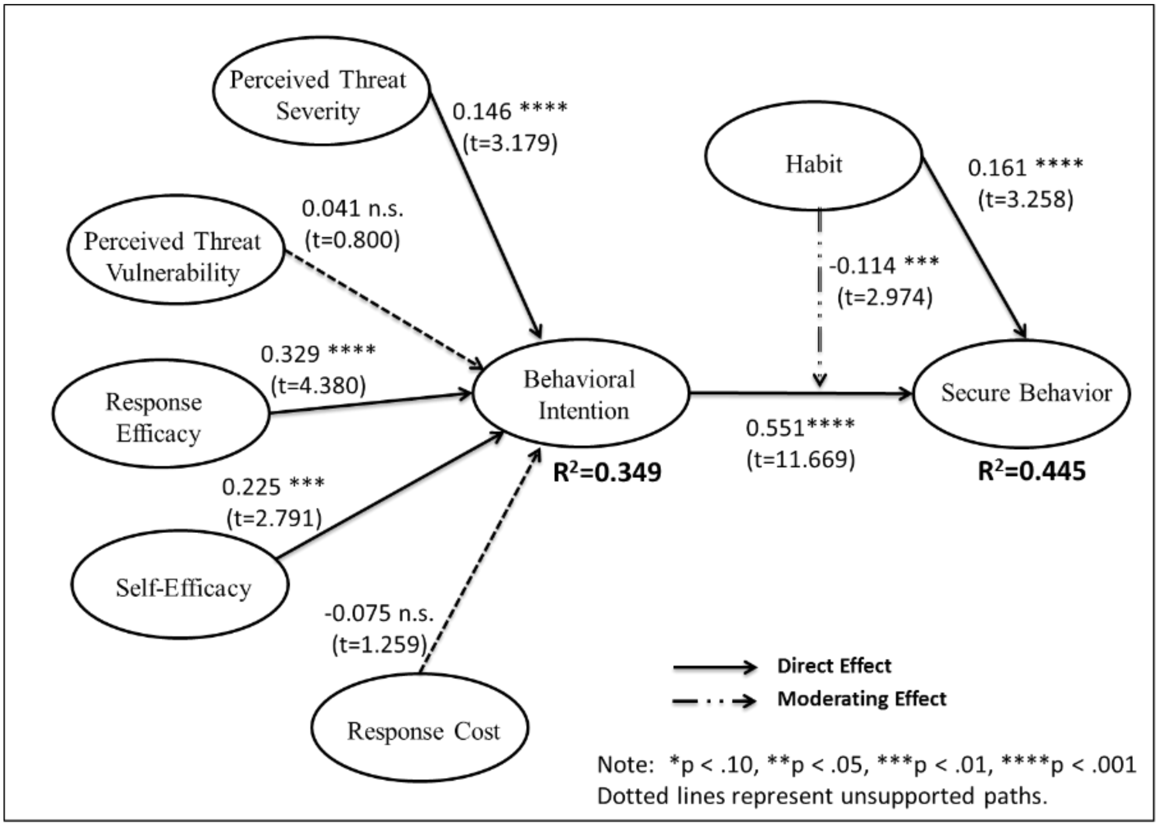


Figure 4.11 Verify Email Recipients: Habit as a Moderator

المنارة للاستشارات
www.manaraa.com

Table 4.27 Verify Email Recipients: Summary of Findings

Hypothesis (with direction)	Path Coefficient (β)	T Value	P-Value	Support
H_1: PSEV → BINT (+)	0.146	3.179	$p < 0.001$	Supported
H_2: PVUL → BINT (+)	0.041	0.800	$p < 0.10$	Not Supported
H_3: REFF → BINT (+)	0.329	4.380	$p < 0.001$	Supported
H_4: SEFF → BINT (+)	0.225	2.791	$p < 0.001$	Supported
H_5: RCST → BINT (-)	-0.075	1.259	$p < 0.10$	Not Supported
H_6: BINT → BEHV (+)	0.551	11.669	$p < 0.001$	Supported
H_{7a}: HBT → BEHV (+)	0.161	3.258	$p < 0.001$	Supported
H_{7b}: HBT → INT-BEHV (-)	-0.114	2.974	$p < 0.001$	Supported

Based on the R-square difference tests between the models with habit modeled as a direct effect and habit additionally modeled as a moderator, the additional moderation effect was found to have a value of 0.019, which is a small effect (Chin et al. 2003; Cohen 1988). It is also evident that the third (complete) model demonstrates higher explanatory power than previous two models. Therefore, the research model where habit is hypothesized to moderate the relationship between behavioral intentions and secure behavior and the model where habit is hypothesized to only have a direct effect on secure behaviors have significantly higher explanatory power than the baseline model that does not consider habit. The results of the R-square difference tests are shown in Table 4.28.

Table 4.28 Verify Email Recipients: Effect Size Calculations

Model	R^2	f-statistics	
Baseline Model (Without Habit)	0.417	0.050	
Research Model (Habit as a Moderator)	0.445		0.019
Habit as a Direct Effect	0.434		

المنارة للاستشارات
www.manaraa.com

Post hoc Analyses

To further test the validity of using habit as a formative measure, several alternate models were analyzed as a post hoc step. The construct of habit has been a topic of much debate among scholars, and has been modeled in many different ways. We compare our research model to some of these models that tested habit.

Habit conceptualized as Limayem et al. 2007

Data were collected for the reflective scale of Limayem et al. (2007) as a part of this study, which allowed comparison of the research model of this study using both formative and reflective scales of habit. The two models were tested using SmartPLS and the results are shown in Table 4.29. The path coefficients of the PMT variables of both models remained the same and are not displayed in the table. The magnitude of the path coefficient of the intention-behavior relationship was higher (0.551) in our research model that tested habit as a second-order formative construct, compared to the alternate research model where habit was conceptualized using the reflective scale from Limayem et al. (2007).

Habit demonstrated a higher direct impact on secure behavior when tested with reflective scales, even though both relationships were significant at $p<0.001$. Only the model tested with the formative scales demonstrated that habit was a significant negative moderator of the intention-behavior relationship. Although the path coefficient was higher (-0.242) in the model tested with reflective scales, the moderation effect was non-significant. This indicates that when habit is conceptualized as a formative construct, which accurately captures the habit domain, the negative moderating effect of habit is stronger compared to the 3-item reflective scale. The R-square value of secure behavior

المنارة للاستشارات

www.manaraa.com

was higher in the research model with the reflective scale demonstrating that when habit was tested using the reflective scale of Limayem et al. (2007), the model had better explanatory power. As discussed previously, this may be due to the higher correlations between habit and other constructs due to the language of the reflective items being closely related to the items that measure behavioral intention and behavior.

Table 4.29 Verify Email Recipients: Formative vs. Reflective Habit Measures

Hypothesis (with direction)	**Habit as Second-Order Formative**	**Habit as Conceptualized in Limayem et al. 2007**
H_6: BINT → BEHV (+)	0.551 **** (t=11.669)	0.452 *** (t=2.935)
H_{7a}: HBT → BEHV (+)	0.161 **** (t=3.258)	0.616 **** (t=4.561)
H_{7b}: HBT → INT-BEHV (-)	-0.114 *** (t=2.974)	-0.242 n.s. (t=1.024)
R^2 of BINT	0.349	0.349
R^2 of BEHV	0.445	0.550
Effect Size (Moderator vs. Base Model)	0.050	0.300
Effect Size (Moderator vs. Direct Effect)	0.019	0.002

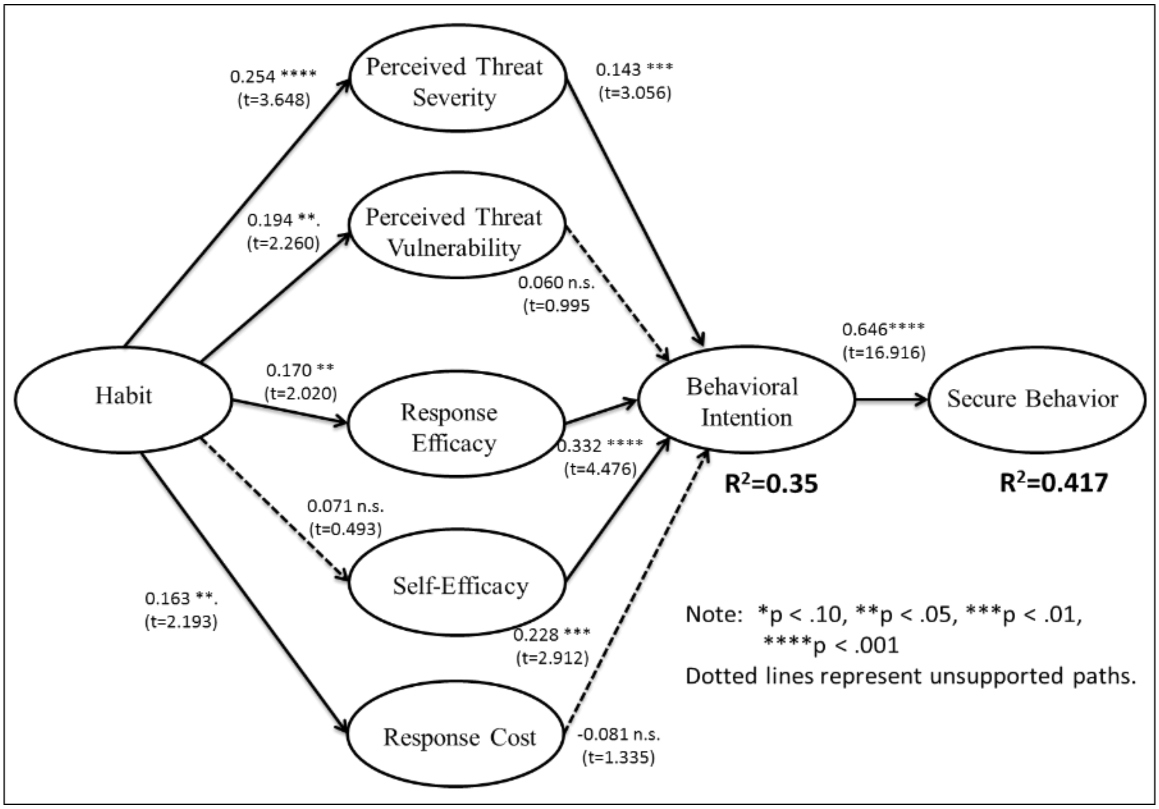
Note: *p < .10, **p < .05, ***p < .01, ****p < .001

The effect sizes of the moderation were compared between the two models. The model tested with the formative scale had a small effect size compared to the model with reflective scales, which had a large effect size when comparing the baseline model to the model with habit has a moderator. However, the effect size, when comparing the model of habit as a direct effect to the model with habit as a moderator was medium when tested with the formative scale and the effect size was very small in when tested with the reflective scale. This provides further evidence that the negative moderating effect of habit is stronger when habit is conceptualized as a second-order formative construct.

المنارة للاستشارات
www.manaraa.com

Habit as a Mediator of the PMT-Intention Relationship

As an alternative model, we tested Vance et al. (2012) research model with both the formative and the reflective habit measures separately. First we tested the Vance et al. (2012) research model with the first-order reflective and second-order formative habit scale and the results are shown on Figure 4.12. Perceived threat severity and response cost had non-significant relationships with behavioral intention while the remaining PMT variables had significant relationships. The formative habit construct demonstrated significant influence on the threat appraisal variables: perceived threat severity and perceived threat vulnerability and coping appraisal variables: response efficacy and response cost.

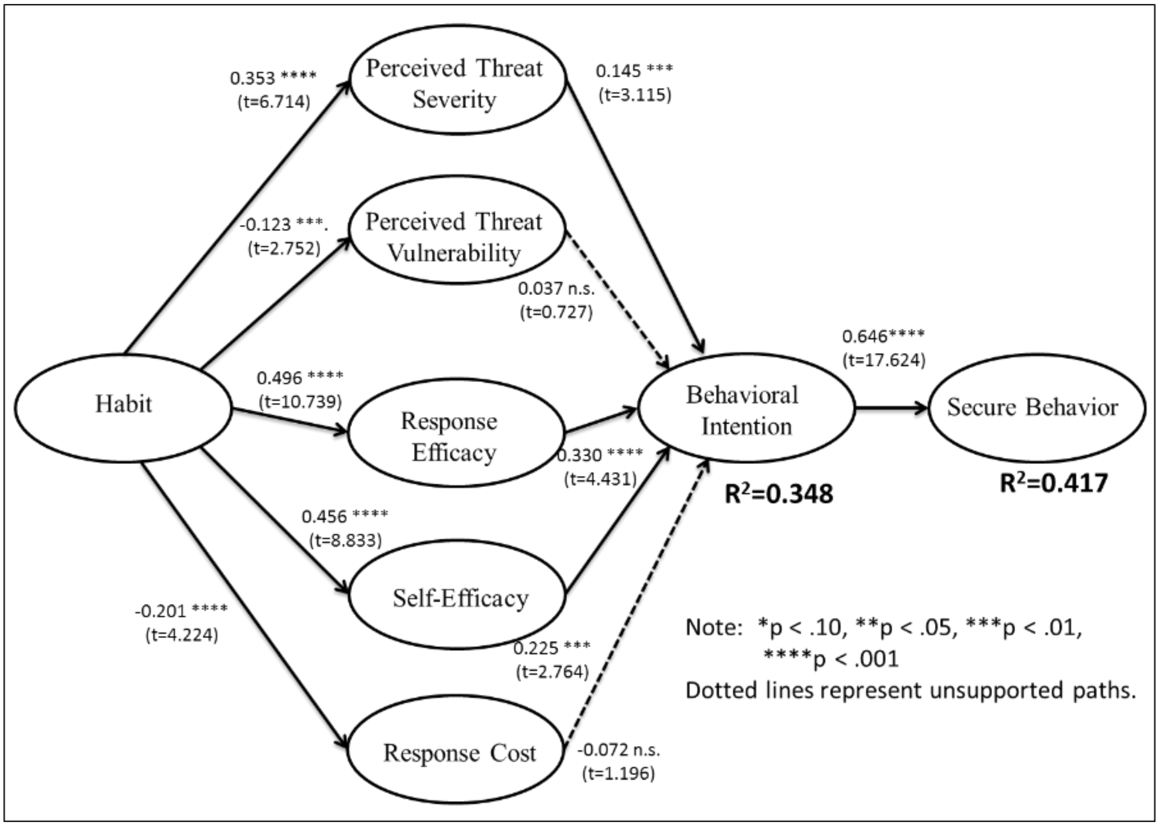


Note: *p < .10, **p < .05, ***p < .01, ****p < .001
Dotted lines represent unsupported paths.

Figure 4.12 Verify Email Recipients: Habit (Formative) as an Indirect Influence

www.manaraa.com

Next, we tested the Vance et al. (2012) research model with the 3-item reflective scale developed by Limayem et al. (2007) and the results are shown on Figure 4.13. Habit significantly influenced all the PMT variables, with the highest path coefficient being 0.496 (p<0.001) between habit and perceived threat vulnerability. The support for the hypotheses are consistent with the findings of Vance et al. (2012). However, the research model of Vance et al. (2012) demonstrated a higher explanatory power with a R-square of behavioral intention at 44 percent compared to the R-square value of 35 percent in each of our research models where habit was measured formatively and reflectively.



Note: *p < .10, **p < .05, ***p < .01, ****p < .001
Dotted lines represent unsupported paths.

Figure 4.13 Verify Email Recipients: Habit (Reflective) as an Indirect Influence

المنارة للاستشارات
www.manaraa.com

Inertia as a mediator of Habit-Intention Relationship

An alternative model, where habit directly influenced inertia and inertia directly influenced behavioral intention, was tested. Similar to the formative habit construct, a two stage approach was followed where the PLS latest scores for each dimensions were used as the formative measures of the inertia construct (Polites and Karahanna 2012). Affective-based inertia demonstrated a weight of 0.349 (p<0.01) and behavior-based inertia demonstrated a weight of 0.741 (p<0.001), thus were suitable to be included in the data analysis. Habit was modeled as positively influencing inertia and inertia was modeled as positively influencing behavioral intention, which reflects the research model of Polites and Karahanna (2012).

The results of the data analysis are shown on Figure 4.14. All the PMT variables significantly influenced behavioral intention except perceived threat vulnerability and response cost. Habit significantly influenced inertia with a path coefficient of 0.440 (p<0.001) and inertia significantly influenced behavioral intention with a coefficient of 0.445 (p<0.001). Habit also explained 19.4 percent of the variance in inertia. The relationship between inertia and behavioral intention was positive for the verify email recipient behavior too, which is in contrast to the hypothesis by Polites and Karahanna (2012). This means that increased levels of inertia leads to increased behavioral intention to perform secure behavior. R-square of the behavioral intention was 50.4 percent. Mediation tests revealed that inertia partially mediated the relationship between habit and behavioral intention. Another research model where a reflective habit construct was utilized yielded similar results with similar explanatory power.

المنارة للاستشارات
www.manaraa.com

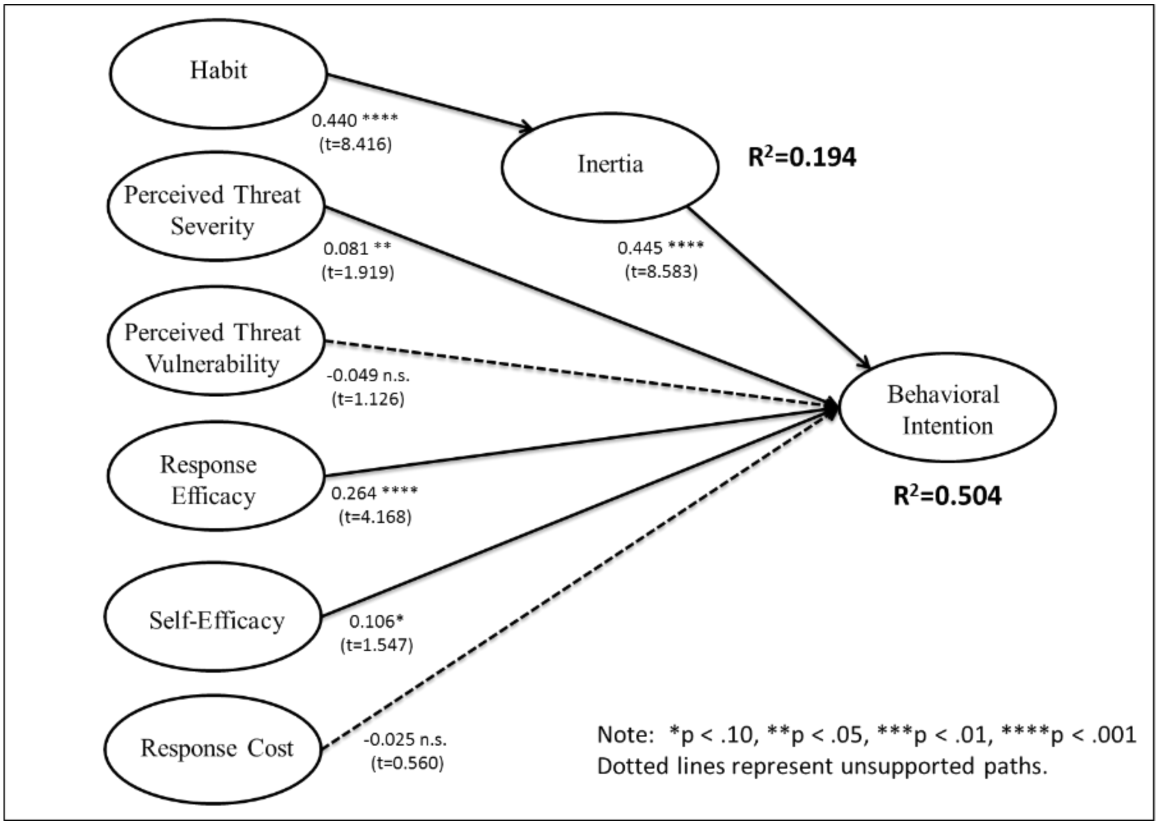


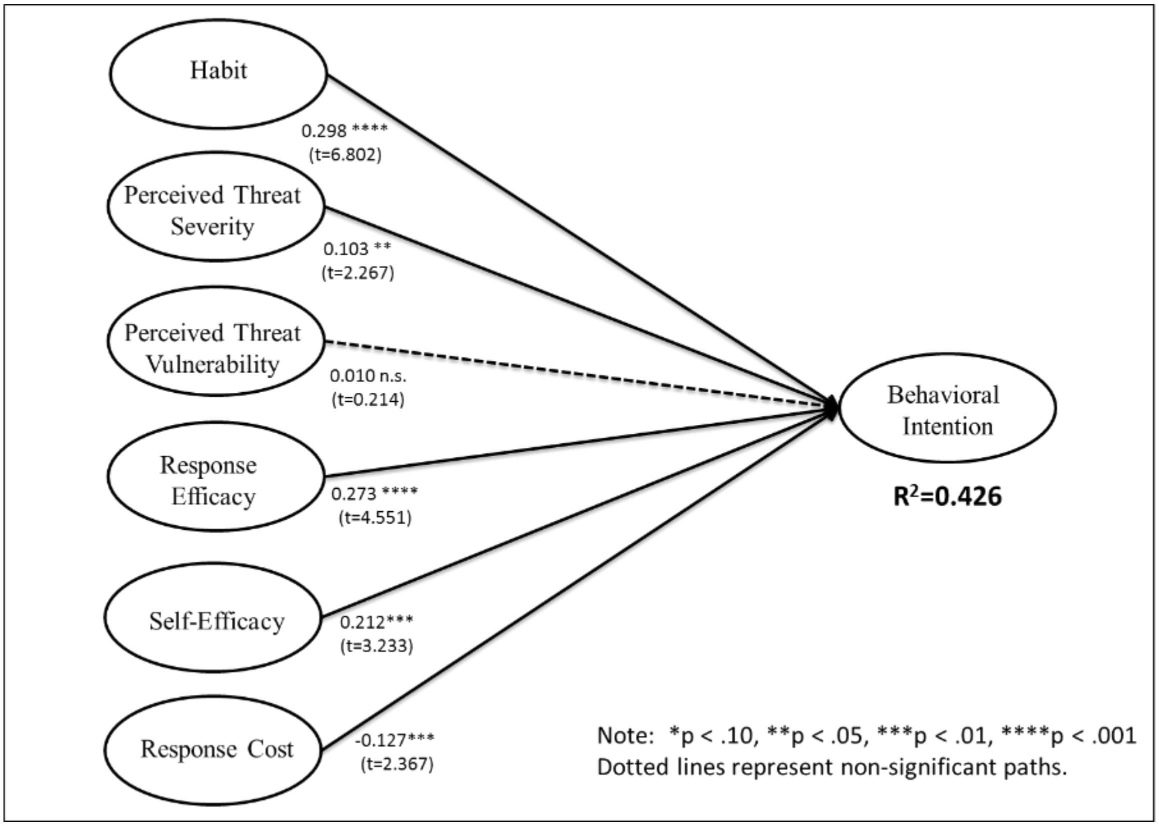
Figure 4.14 Verify Email Recipients: Inertia as a Mediator of Habit and Intention

A research model that included direct paths to behavioral intention from both habit and inertia demonstrated a R-square value of 52.2 percent, slightly increasing the explanatory power of the model due to the direct influence of habit on behavioral intention. The results suggest that inertia increased the explanatory power of the research model indicating that it may play a role in the performance of secure behaviors, although the path was significant in the opposite direction compared to the results of Polites and Karahanna (2012). This discrepancy of the results will be discussed in detail on Chapter V.

www.manaraa.com

Habit as a Direct Influence of Behavioral Intention

An alternative model where habit was modeled as a direct influence of behavioral intention was tested as a part of the post hoc analysis. First, the path between habit and behavioral intention was tested with the first-order reflective and second-order formative habit construct. The results of this analysis are shown on Figure 4.15. The path from habit to behavioral intention was significant with a path coefficient of 0.298 (p<0.001). All the paths from PMT variables to behavioral intention were significant except for perceived threat vulnerability. R-square value of behavioral intention was 42.6 percent explaining considerably more explanatory power than the baseline model without habit.



Note: *p < .10, **p < .05, ***p < .01, ****p < .001
Dotted lines represent non-significant paths.

Figure 4.15 Verify Email Recipients: Direct Influence of Habit on Behavioral Intention

www.manaraa.com

Next, the same model was tested with the reflective habit scale. The paths from perceived severity, perceived threat vulnerability and response cost to behavioral intention were non-significant. Only the paths from response efficacy and self-efficacy to behavioral intention were shown to be significant. The path from habit to behavioral intention was significant with a path coefficient of 0.499 ($p<0.001$). R-square of behavioral intention was 52 percent compared to the R-square of 42.6 percent when the model was tested with the formative habit scale. Therefore, the model with a reflective habit scale demonstrated higher explanatory power than the model with a formative habit scale when habit was modeled as a direct influence of behavioral intention.

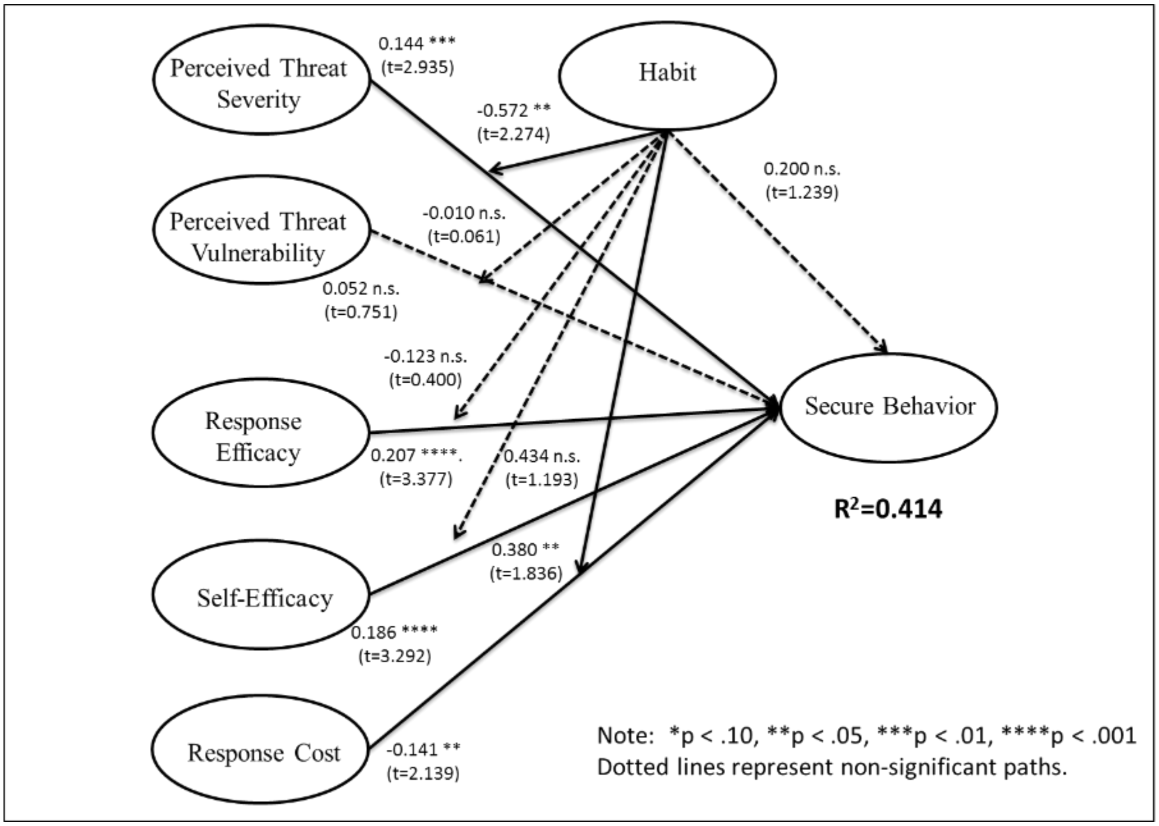
Habit as a Moderator of the PMT-Behavior Relationship

As a part of the post hoc study, an alternative model where PMT variables directly influenced actual behavior was tested. Habit was hypothesized to directly influence secure behavior while moderating the relationships between the PMT variables and actual behavior. The results of this analysis are shown on Figure 4.16.

Paths from perceived threat severity, response efficacy, self-efficacy and response cost to secure behavior were significant. Paths from perceived threat vulnerability and habit to secure behavior were insignificant. Similarly, habit did not significantly moderate the paths from the PMT variables to secure behavior except for the paths between perceived threat severity and response cost with secure behavior. It is important to note that habit negatively moderated the path between perceived threat severity and secure behavior demonstrating that when a certain behavior is habitual, the perceived severity of the threat is lesser. Similarly, when a certain behavior is habitual, response

المنارة للاستشارات
www.manaraa.com

cost increases. This is demonstrated in habit significantly moderating the path between response cost and secure behavior.



Note: *p < .10, **p < .05, ***p < .01, ****p < .001
Dotted lines represent non-significant paths.

Figure 4.16 Verify Email Recipients: Habit as a Moderator of PMT-Behavior

Behavior 3: Visit Verified Websites (N=395)

The third behavior tested was "visiting only verified websites." A total of 500 responses were collected for this behavior, and the surveys were completed in an average of four minutes and twenty seconds. Responses that were incomplete or failed the response set item were removed. This resulted in a usable sample of 395 responses, which exceeded the required sample size of 308 as calculated through the power analysis.

المنارة للاستشارات
www.manaraa.com

Of the usable responses, 241 (61%) were male and 154 (39%) were female. There were 120 (30.4%) respondents who were between the ages of 18 and 24, 185 (46.8%) were between the ages of 25 and 34, 54 (13.7%) were between the ages of 35 and 44, 25 (6.3%) were between the ages of 45 and 54, 9 (2.3%) were between the ages of 55 and 64 and 2 (0.5%) were age 65 or above. In terms of the education of the respondents, 110 (27.8%) had a 2-year college degree or lesser, 174 (44.1%) had a 4-year college degree, 102 (25.8%) had a masters degree and 9 (2.27%) had a doctoral degree or a professional degree.

The respondents were employed in various industries and the majority of the respondents belonged to the categories of Information (20.3%), finance and insurance (11.6%) and professional, scientific or technical services (8.6%). Table 4.30 provides the demographic details of the respondents who participated in this study.

المنارة للاستشارات
www.manaraa.com

Table 4.30 Visit Verified Websites: Demographics of Main Investigation

Demographic	Category	Frequency
Gender	Male	241 (61.0%)
	Female	154 (39.0%)
Age	18-24	120 (30.4%)
	25-34	185 (46.8%)
	35-44	54 (13.7%)
	45-54	25 (6.3%)
	55-64	9 (2.3%)
	65 and older	2 (0.5%)
Education	Less than High School	0 (0%)
	High School / GED	28 (7.1%)
	Some College	57 (14.4%)
	2-year College Degree	25 (6.3%)
	4-year College Degree	174 (44.1%)
	Masters Degree	102 (25.8%)
	Doctoral Degree	5 (1.3%)
	Professional Degree (JD, MD)	4 (1.0%)
Industry	Forestry, fishing, hunting or agriculture support	3 (0.5%)
	Mining	0 (0%)
	Utilities	2 (0.5%)
	Construction	5 (1.3%)
	Manufacturing	28 (7.1%)
	Wholesale trade	6 (1.5%)
	Retail trade	14 (3.5%)
	Transportation or warehousing	9 (2.3%)
	Information	80 (20.3%)
	Finance or insurance	46 (11.6%)
	Real estate or rental and leasing	2 (0.5%)
	Professional, scientific or technical services	34 (8.6%)
	Management of companies or enterprises	12 (3.0%)
	Admin, support, waste management or remediation services	18 (4.6%)
	Educational services	41 (10.4%)
	Health care or social assistance	24 (6.1%)
	Arts, entertainment or recreation	11 (2.8%)
	Accommodation or food services	3 (0.8%)
	Other services (except public administration)	36 (9.1%)
	Unclassified establishments	21 (5.3%)

المنارة للاستشارات
www.manaraa.com

As with the previous behavior, an EFA was repeated for the main investigation with a sample size of 395, since minor changes were made to the language of certain items following the preliminary investigation phase. The items demonstrated an acceptable response spread and no unusual patterns in the means and standard deviations were found. Bartlett's Test of Sphericity was significant at 0.000 and Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy test result of 0.791 indicated that factor analysis was appropriate for this sample (Hair et al. 2010).

The EFA was conducted using the Principal Component Analysis (PCA) technique with a Varimax rotation. Ten factors with an Eigenvalue of one or greater, were extracted and those factors explained a total of 71.90% of the variance, which is above the 65% recommended by Hair et al. (2010). The communalities of the items were well above the accepted threshold of 0.30.

All the items loaded cleanly on their respective factors except EFFC2 and EFFC4, which had loadings of 0.532 and 0.599. EFFC2 had a similar cross-loading issue during the EFA of behavior 1 as well, indicating that it may be a problematic item. EFFC2 was removed, and the EFA was re-run. This improved the factor loadings, but EFFC4 still had low loadings. Once EFFC4 was removed, the remaining items loaded cleanly on their respective factors. The results of the EFA are shown in Table 4.31. Correlations lower than 0.40 in absolute value were suppressed for clarity. BINT1 had a loading of 0.653 and PSEV3 had a loading of 0.695, which were marginally lower than the recommended 0.70 loadings. However, both the items did not cross-load with any other factors, thus they were retained for the data analysis.

المنارة للاستشارات
www.manaraa.com

Table 4.31 Visit Verified Websites: EFA Results of Main Investigation

Rotated Component Matrix[a]

	Component									
	1	2	3	4	5	6	7	8	9	10
AWAR1	.816									
AWAR2	.803									
AWAR3	.817									
AWAR4	.844									
BEHV1		.804								
BEHV2		.798								
BEHV3		.804								
BINT1			.653							
BINT2			.704							
BINT3			.724							
CTRL1				.846						
CTRL2				.858						
CTRL3				.867						
CTRL4				.823						
EFFC1					.788					
EFFC3					.780					
PSEV1						.790				
PSEV2						.854				
PSEV3						.695				
PVUL1							.733			
PVUL2							.823			
PVUL3							.788			
RCST1								.832		
RCST2								.833		
RCST3								.801		
RCST4								.836		
REFF1									.709	
REFF2									.810	
REFF3									.729	
REFF4									.745	
SEFF1										.754
SEFF2										.785
SEFF3										.744
SEFF4										.739

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
Correlations lower than 0.4 in absolute value were suppressed..

المنارة للاستشارات

www.manaraa.com

Measurement Model

SmartPLS was used again to test both the measurement model and structural model similar to the previous behavior that was tested. A measurement model analysis was conducted to examine the psychometric properties of all the reflective constructs included in the research model. PLS validation procedures outlined by Gefen and Straub (2005) were followed to establish the validity and reliability of the measurement model. All the scales except EFFC had alpha values larger than the recommended threshold. EFFC had an alpha value of 0.645, which was still acceptable. All the scales demonstrated composite reliability values much higher than the recommended ones with the lowest value being 0.753 for the scale RCST.

Table 4.32 Visit Verified Websites: Reliability Statistics

Construct		**AVE**	**C-Alpha**	**CREL**	**Mean (St. dev)**	**Min/Max**
AWAR	Lack of Awareness	0.727	0.875	0.914	3.22 (0.988)	1.0/5.0
BEHV	Actual Behavior	0.817	0.888	0.930	3.76 (0.853)	1.0/5.0
BINT	Behavioral Intention	0.689	0.774	0.869	3.91 (0.771)	1.0/5.0
CTRL	Uncontrollability	0.767	0.899	0.929	3.22 (0.988)	1.0/5.0
EFFC	Mental Efficiency	0.697	0.645	0.815	2.84 (1.123)	1.0/5.0
PSEV	Perceived Severity	0.702	0.787	0.876	3.76 (0.853)	1.0/5.0
PVUL	Perceived Vulnerability	0.712	0.797	0.881	2.80 (1.035)	1.0/5.0
RCST	Response Cost	0.527	0.831	0.753	4.00 (0.725)	1.0/5.0
REFF	Response Efficacy	0.637	0.811	0.875	4.13 (0.685)	1.0/5.0
SEFF	Self-Efficacy	0.668	0.835	0.890	3.84 (0.984)	1.0/5.0

Almost all the items demonstrated loadings well above 0.7 showing above acceptable reliability. The values of the reliability tests such as composite reliability and Cronbach’s alpha are shown in Table 4.32 and item loadings are shown in Table 4.34. These values indicate that the scales satisfy the reliability requirements.

المنارة للاستشارات

www.manaraa.com

Convergent validity requirements such as item loadings that exceed 0.70 on their respective constructs and Average Variance Extracted (AVE) above 0.50 (Gefen and Straub 2005) for each construct were examined. As shown in Table 4.34 all the item loadings exceeded 0.70 on their respective constructs. Table 4.32 shows that all the scales demonstrated AVE values well above 0.5. Therefore, all the scales of this study demonstrate convergent validity values that are beyond the recommended thresholds.

Table 4.33 Visit Verified Websites: Inter-Construct Correlations

	AWAR	BEHV	BINT	CTRL	EFFC	PSEV	PVUL	RCST	REFF	SEFF
AWAR	0.853									
BEHV	0.434	0.904								
BINT	0.323	0.497	0.830							
CTRL	0.220	0.283	0.233	0.876						
EFFC	0.284	0.125	0.219	0.247	0.829					
PSEV	0.188	0.100	0.315	0.134	0.105	0.838				
PVUL	0.129	0.047	0.255	0.206	0.087	0.468	0.844			
RCST	0.084	0.057	0.078	0.238	-.001	0.147	0.246	0.726		
REFF	0.188	0.335	0.497	0.110	0.104	0.329	0.135	0.094	0.798	
SEFF	0.268	0.517	0.534	0.093	0.219	0.171	0.059	0.036	0.477	0.817

* The highlighted diagonal elements are square-roots of the AVE.

Discriminant validity can be demonstrated if the square root of each construct's AVE is greater than the absolute value of the inter-construct correlations. As it is shown in Table 4.33, the square roots of the AVEs of all constructs were found to be larger than all cross-correlations of the other constructs, demonstrating discriminant validity of the constructs used in this study (Gefen and Straub 2005). Discriminant validity is also demonstrated when items load on their respective constructs more than any other construct, as it did in this study. PLS loadings and cross-loadings for all the items are shown in Table 4.34.

المنارة للاستشارات
www.manaraa.com

Table 4.34 Visit Verified Websites: PLS loadings for the Main Investigation

	AWAR	BEHV	BINT	CTRL	EFFC	PSEV	PVUL	RCST	REFF	SEFF
AWAR1	0.871	0.415	0.281	0.185	0.258	0.197	0.134	0.056	0.191	0.259
AWAR2	0.836	0.359	0.312	0.211	0.219	0.139	0.094	0.074	0.157	0.248
AWAR3	0.847	0.359	0.250	0.198	0.242	0.160	0.128	0.008	0.133	0.196
AWAR4	0.857	0.345	0.260	0.156	0.249	0.143	0.082	0.046	0.159	0.211
BEHV1	0.399	0.910	0.444	0.258	0.109	0.081	0.011	0.062	0.290	0.464
BEHV2	0.396	0.915	0.470	0.271	0.136	0.102	0.073	0.035	0.349	0.497
BEHV3	0.381	0.886	0.431	0.237	0.092	0.087	0.042	0.084	0.266	0.439
BINT1	0.226	0.414	0.856	0.162	0.215	0.306	0.220	0.092	0.472	0.501
BINT2	0.345	0.454	0.806	0.228	0.169	0.212	0.199	0.068	0.363	0.387
BINT3	0.240	0.370	0.827	0.195	0.156	0.261	0.214	0.099	0.397	0.434
CTRL1	0.148	0.259	0.198	0.869	0.227	0.095	0.177	0.181	0.074	0.078
CTRL2	0.189	0.223	0.216	0.887	0.235	0.131	0.183	0.146	0.059	0.058
CTRL3	0.181	0.220	0.188	0.881	0.225	0.120	0.181	0.161	0.121	0.076
CTRL4	0.249	0.288	0.214	0.865	0.179	0.123	0.180	0.167	0.130	0.112
EFFC1	0.255	0.102	0.116	0.209	0.846	0.010	0.089	0.017	0.049	0.155
EFFC3	0.214	0.106	0.253	0.200	0.812	0.171	0.054	0.038	0.126	0.211
PSEV1	0.188	0.074	0.260	0.152	0.105	0.833	0.391	0.149	0.311	0.170
PSEV2	0.150	0.145	0.270	0.117	0.045	0.874	0.380	0.148	0.296	0.163
PSEV3	0.135	0.030	0.260	0.069	0.116	0.805	0.405	0.062	0.219	0.097
PVUL1	0.165	0.034	0.224	0.240	0.091	0.438	0.860	0.203	0.077	0.018
PVUL2	0.098	0.055	0.208	0.170	0.053	0.351	0.861	0.185	0.161	0.062
PVUL3	0.059	0.030	0.212	0.107	0.075	0.392	0.809	0.079	0.105	0.070
RCST1	0.072	0.005	-.008	0.294	0.098	0.101	0.277	0.519	0.076	0.005
RCST2	0.110	0.003	-.026	0.205	0.070	0.066	0.229	0.995	0.032	-.038
RCST3	0.087	0.054	0.072	0.256	0.011	0.149	0.261	0.565	0.097	0.035
REFF1	0.154	0.255	0.367	0.066	0.108	0.283	0.100	0.033	0.769	0.422
REFF2	0.077	0.222	0.362	0.072	0.075	0.167	0.079	0.044	0.784	0.301
REFF3	0.192	0.296	0.407	0.118	0.090	0.301	0.118	0.070	0.813	0.439
REFF4	0.169	0.290	0.443	0.091	0.063	0.289	0.127	0.146	0.827	0.363
SEFF1	0.176	0.404	0.451	0.087	0.198	0.147	0.040	0.070	0.406	0.824
SEFF2	0.225	0.390	0.400	0.072	0.138	0.172	0.055	0.081	0.401	0.797
SEFF3	0.232	0.433	0.474	0.102	0.176	0.192	0.073	0.054	0.386	0.827
SEFF4	0.247	0.465	0.413	0.038	0.202	0.043	0.021	-.009	0.369	0.820

المنارة للاستشارات
www.manaraa.com

Tests for Common Method Bias

Similar to the previous behavior, CMV tests were performed to assess any biases resulting from the use of the same method to collect data. We conducted statistical analysis using three tests to check for the presence of and severity of CMV in our data.

For the first test, we used the Harmon one-factor test (Podsakoff and Organ 1986; Podsakoff et al. 2003), where an exploratory factor analysis (EFA) was conducted on all the variables used in our model and the unrotated factor solution was examined. It is assumed that CMV exists if a single factor emerges from unrotated factor solutions or a first factor explains the majority of the variance in the variables (Podsakoff and Organ 1986). Ten factors emerged from the EFA, which accounted for 71.9% of the variance. The greatest variance explained by one factor was 17.24%, demonstrating that common method variance is unlikely to bias the results. A second test suggested by Pavlou et al. (2007) was conducted. Examining the inter-construct correlations in Table 4.23, the highest correlation among constructs is 0.497, which is not extremely high as suggested by Pavlou et al. (2007), thus ruling out CMV in this study.

For the third test, we used a more rigorous statistical approach suggested by Podsakoff et al. (2003) to check for common method bias. Table 4.35 shows the factor loadings for each major construct and factor loadings for the common method construct captured through this procedure.

المنارة للاستشارات
www.manaraa.com

Table 4.35 Visit Verified Websites: CMV Test Results

Construct	Indicator	Substantive Factor Loading (λs)	Substantive Factor Variance Explained (λs2)	Method Factor Loading (λm)	Method Factor Variance Explained (λm2)
Awareness	AWAR1	0.872	0.692	0.000	0.001
	AWAR2	0.816	0.676	0.028	0.000
	AWAR3	0.861	0.696	-0.026	0.001
	AWAR4	0.888	0.771	-0.048	0.003
Behavior	BEHV1	0.925	0.837	-0.021	0.001
	BEHV2	0.951	0.903	0.060	0.004
	BEHV3	0.918	0.674	-0.041	0.008
Behavioral Intention	BINT1	0.832	0.580	0.021	0.019
	BINT2	0.780	0.861	0.036	0.014
	BINT3	0.878	0.815	-0.058	0.001
Uncontrollability	CTRL1	0.884	0.796	-0.022	0.000
	CTRL2	0.898	0.795	-0.022	0.002
	CTRL3	0.889	0.813	-0.013	0.000
	CTRL4	0.831	0.783	-0.058	0.001
Mental Efficiency	EFFC1	0.845	0.646	-0.045	0.003
	EFFC3	0.814	0.645	0.045	0.055
Perceived Severity	PSEV1	0.819	0.762	0.036	0.000
	PSEV2	0.873	0.688	0.009	0.000
	PSEV3	0.820	0.811	-0.047	0.000
Perceived Vulnerability	PVUL1	0.849	0.795	0.024	0.000
	PVUL2	0.870	0.824	0.003	0.004
	PVUL3	0.813	0.720	-0.028	0.003
Response Cost	RCST1	0.851	0.782	0.015	0.001
	RCST2	0.850	0.720	-0.036	0.000
	RCST3	0.810	0.791	0.058	0.007
	RCST4	0.867	0.766	-0.035	0.002
Response Efficacy	REFF1	0.766	0.637	0.013	0.002
	REFF2	0.869	0.852	-0.115**	0.009
	REFF3	0.764	0.580	0.072*	0.011
	REFF4	0.796	0.783	-0.027	0.003
Self-Efficacy	SEFF1	0.823	0.637	-0.003	0.000
	SEFF2	0.807	0.580	-0.002	0.002
	SEFF3	0.783	0.766	0.048	0.000
	SEFF4	0.857	0.762	-0.043	0.000
Average		**0.8461**	**71.79%**	**-0.0065**	**0.17%**

المنارة للاستشارات

www.manaraa.com

The results explain that the average loading of the indicators is 0.8461 while the average loading of the method indicators is -0.0065. The average variance explained by the substantive constructs is 71.8 percent compared to the 0.2 percent average variance explained by the method construct. Moreover, except for two indicators, all the method factor loadings were insignificant. Since the most of the method factor loadings are insignificant and the indicators' substantive variances are substantially greater than their method variances, it can be concluded that common method bias is unlikely to be a serious concern in the data of this study (Williams et al. 2003). Therefore, based on the three separate tests to measure CMV, we concluded that common method bias was not a concern for this study.

Structural Model

The structural models were then tested with the SmartPLS software. Factor scores for each of the first-order dimensions of habit were generated. These factors scores were used as formative measures of the second-order aggregate construct of habit (Chin et al. 2003; Polites and Karahanna 2012).

Reliability and validity tests that were performed on the first-order reflective dimensions of habit previously do not apply to formative scales because "the measurement model does not predict that the sub-dimensions will be correlated" (Bollen and Lennox 1991; Edwards 2003; MacKenzie et al. 2011, p.314). Item weights of the formative constructs can be examined to identify their individual influence in forming each construct (Chin 1998; Petter et al. 2007). The weights for the three habit dimensions were 0.840 for Lack of Awareness, 0.430 for Uncontrollability and -0.082 for Mental

المنارة للاستشارات
www.manaraa.com

Efficiency. The weight for Mental Efficiency was not significant while Lack of Awareness and Mental Efficiency were significant at p<0.001.

The formative dimensions of the habit construct were tested for multicollinearity next. To test for multicollinearity, the variance inflation factor (VIF) statistics for the three dimensions of habit were examined. As shown in Table 4.36, VIF values are well below the recommended threshold value of 3.3 Diamantopoulos and Siguaw (2006), which indicates no serious multicollinearity issues with the formative dimensions of habit. Individual weights of the formative dimensions of habit also indicate that multicollinearity is not a concern.

Table 4.36 Visit Verified Websites: Weights of the Formative Habit Construct

Construct	**Dimension**	**Weight**	**VIF**
Habit	Lack of Awareness	0.840 (****)	1.121
	Uncontrollability	0.430 (****)	1.092
	Mental Efficiency	-0.082 (n.s.)	1.312

Note: ****p<0.001

Although two of the formative dimensions of habit are significant, the dimension of mental efficiency is not significant. Content validity of formative scales is affected if one of the indicators that represent one of the formative dimensions is removed. Since mental efficiency is one of the three dimensions that constitute habit, it was retained for the structural model analysis although its weight was not significant.

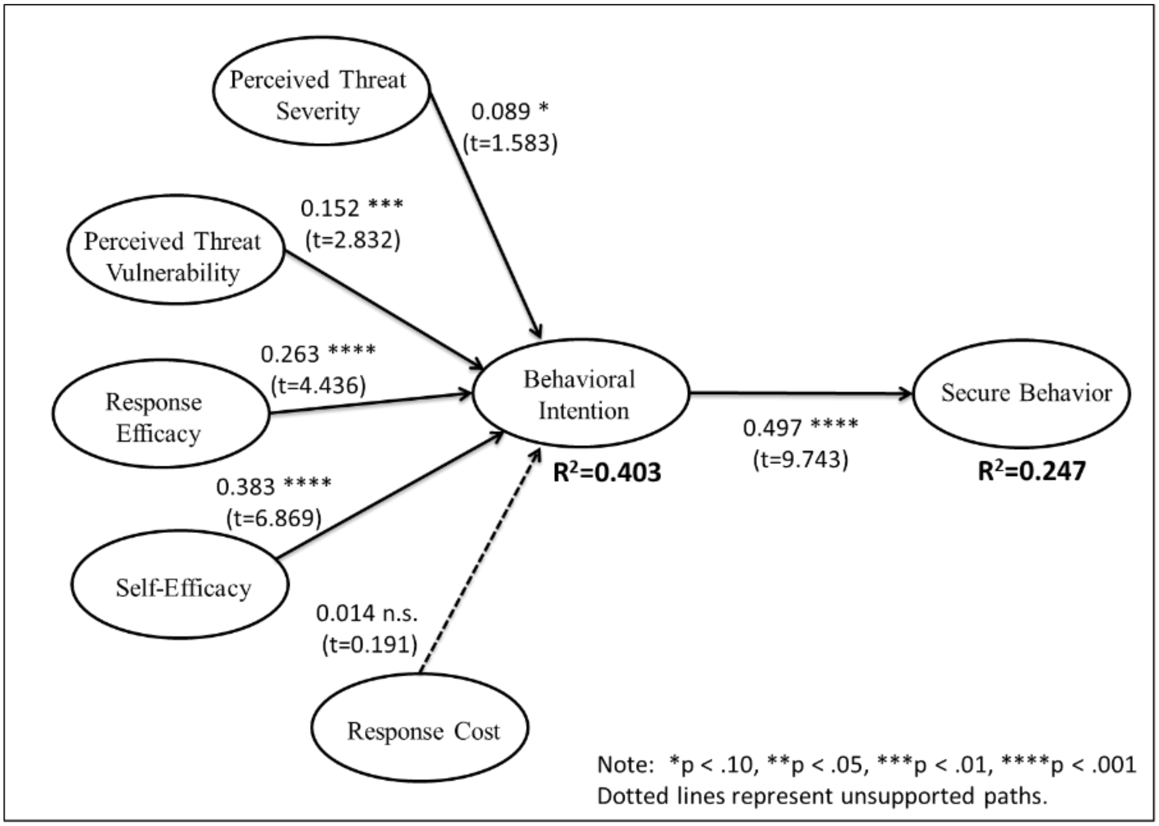
To test the role of habit in information security behaviors, data analyses were run in three stages, following the recommendations by Limayem et al. (2007). First, we ran a baseline research model with only the PMT variables. The next model added habit as a

المنارة للاستشارات
www.manaraa.com

direct effect on behavior. The final model added the possibility of habit moderating the relationship between behavioral intention and behavior.

Visit Verified Websites: Baseline Model

A baseline model, without the incorporation of the habit construct was tested first and the results are shown on Figure 4.17. Paths from perceived threat severity, perceived threat vulnerability, response efficacy and self-efficacy to behavioral intention were significant (p<0.10 or higher) while the paths from response cost was not significant. The path from behavioral intention to secure behavior was also significant at p<0.001.



Note: *p < .10, **p < .05, ***p < .01, ****p < .001
Dotted lines represent unsupported paths.

Figure 4.17 Visit Verified Websites: Baseline Model (Without Habit)

www.manaraa.com

This model accounts for 27.7 percent of the variance of self-reported actual behavior and 40.3 percent of the variance in behavioral intention to perform a secure behavior. Response cost was found to have a non-significant influence on behavioral intention, indicating that the respondents' intentions to visit only verified websites were not affected by any costs or inconvenience involved with that behavior . In the contrary, individuals perceive that a threat of their computers getting infected with malware is severe and they are vulnerable to it infection. They also perceive that if they visit only verified or known websites, the threat of malware infections can be reduced.

Visit Verified Websites: Habit as a Direct Effect

In the second research model, habit is hypothesized to have a direct effect on secure behavior. The results for this model are shown on Figure 4.18. Similar to the first model, the path from response cost was non-significant while the remaining paths were significant.

المنارة للاستشارات
www.manaraa.com

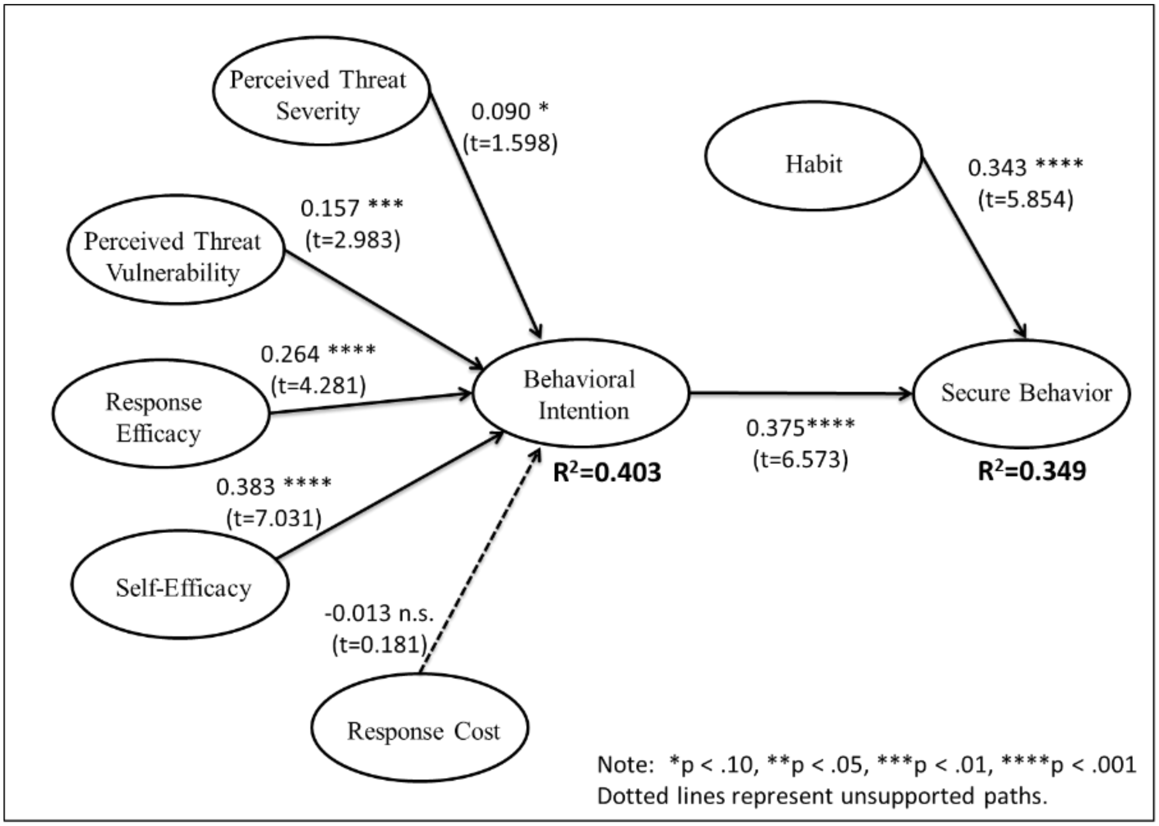


Figure 4.18 Visit Verified Websites: Habit as a Direct Effect

The introduction of habit as a direct effect on secure behavior increased variance explained by the self-reported behavior from 24.7 percent to 34.9 percent. Habit significantly influenced secure behavior with a path coefficient of 0.343 at p<0.001, supporting H_{7a}. The path coefficient between behavioral intention and secure behavior reduced marginally from 0.497 to 0.375, but the relationship remained significant.

Visit Verified Websites: Habit as a Moderator and a Direct Effect

In the third and final research model, habit is included as a direct effect on secure behavior and in addition as moderating the relationship between behavioral intention and behavior. The results for this model are shown in Figure 4.19.

www.manaraa.com

The introduction of habit as a moderator increased the total variance explained by secure behavior slightly from 34.9 percent to 36 percent. The moderating effect of habit on the relationship between behavioral intention and secure behavior had a path coefficient of -0.273 at $p<0.001$ supporting H_{7b}. The path coefficient between behavioral intention and secure behavior remained the same at 0.375, while still being significant. Tests for significance of control variables indicated that none of the control variables of age, gender, education and industry significantly influenced habit, behavioral intention or behavior. A summary of the results for the third (complete) research model is shown in Table 4.37.

Table 4.37 Visit Verified Websites: Summary of Findings

Hypothesis (with direction)	**Path Coefficient (β)**	**T Value**	**P-Value**	**Support**
H_1: PSEV → BINT (+)	0.090	1.683	$p < 0.05$	Supported
H_2: PVUL → BINT (+)	0.157	3.126	$p < 0.01$	Supported
H_3: REFF → BINT (+)	0.264	4.560	$p < 0.001$	Supported
H_4: SEFF → BINT (+)	0.383	7.217	$p < 0.001$	Supported
H_5: RCST → BINT (-)	-0.013	0.183	$p < 0.10$	Not Supported
H_6: BINT → BEHV (+)	0.375	6.534	$p < 0.001$	Supported
H_{7a}: HBT → BEHV (+)	0.596	6.089	$p < 0.001$	Supported
H_{7b}: HBT*INT → BEHV (-)	-0.273	3.182	$p < 0.001$	Supported

المنارة للاستشارات
www.manaraa.com

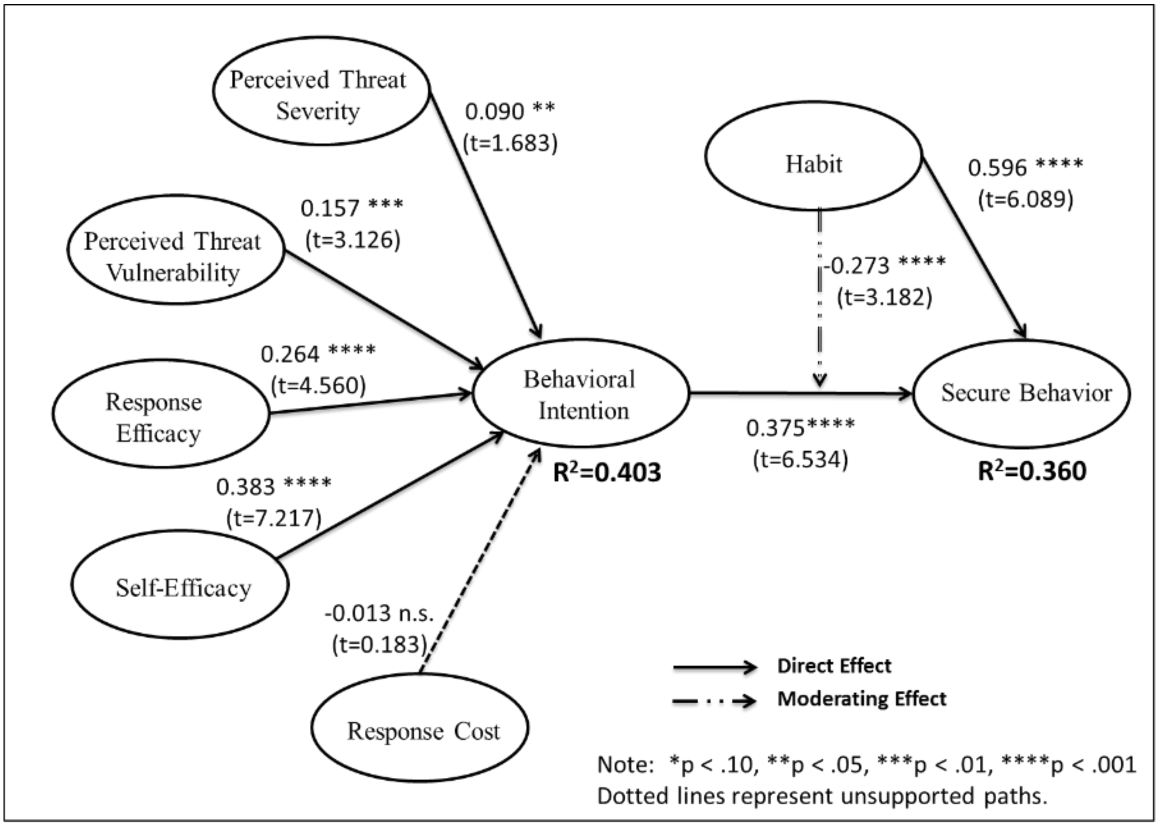


Figure 4.19 Visit Verified Websites: Habit as a Moderator

Based on the R-square difference tests between the models with habit modeled as a direct effect and habit additionally modeled as a moderator, the additional moderation effect was found to have a value of 0.017, which is a small effect (Chin et al. 2003; Cohen 1988). It is also evident that the third (complete) model demonstrates higher explanatory power than previous two models. Therefore, the research model where habit is hypothesized to moderate the relationship between behavioral intentions and secure behavior and the model where habit is hypothesized to only have a direct effect on secure behaviors have significantly higher explanatory power than the baseline model that does not consider habit. The results of the R-square difference tests are shown in Table 4.38.

المنارة للاستشارات
www.manaraa.com

Table 4.38 Visit Verified Websites: Effect Size Calculations

Model	**R^2**	**f-statistics**	
Baseline Model (Without Habit)	0.247	0.177	
Research Model (Habit as a Moderator)	0.360		0.017
Habit as a Direct Effect	0.349		

Post hoc Analyses

To further test the validity of using habit as a formative measure, several alternate models were analyzed as a post hoc step. The construct of habit has been a topic of much debate among scholars, and has been modeled in many different ways. We compare our research model to some of these models that tested habit.

Habit conceptualized as Limayem et al. 2007

Data were collected for the reflective scale of Limayem et al. (2007) as a part of this study, which allowed comparison of the research model of this study using both formative and reflective scales of habit. The two models were tested using SmartPLS and the results are shown in Table 4.39. The path coefficients of the PMT variables of both models remained the same and are not displayed in the table. The magnitude of the path coefficient of the intention-behavior relationship was somewhat higher (0.375) in our research model that tested habit as a second-order formative construct, compared to the alternate research model where habit was conceptualized using the reflective scale from Limayem et al. (2007).

Habit demonstrated a higher direct impact on secure behavior when tested with reflective scales, even though both relationships were significant at $p<0.001$. Only the model tested with the formative scales demonstrated that habit was a significant negative

المنارة للاستشارات
www.manaraa.com

moderator of the intention-behavior relationship. Although the path coefficient was high (-0.264) in the model tested with reflective scales, the moderation effect was non-significant. This indicates that when habit is conceptualized as a formative construct, which accurately captures the habit domain, the negative moderating effect of habit is stronger compared to the 3-item reflective scale. The R-square value of secure behavior was higher in the research model with the reflective scale demonstrating that when habit was tested using the reflective scale of Limayem et al. (2007), the model had better explanatory power. As discussed previously, this may be due to the higher correlations between habit and other constructs due to the language of the reflective items being closely related to the items that measure behavioral intention and behavior.

Table 4.39 Visit Verified Websites: Formative vs. Reflective Habit Measures

Hypothesis (with direction)	**Habit as Second-Order Formative**	**Habit as Conceptualized in Limayem et al. 2007**
H_6: BINT → BEHV (+)	0.375**** (t=6.534)	0.303 * (t=1.487)
H_{7a}: HBT → BEHV (+)	0.596**** (t=6.089)	0.744 **** (t=3.593)
H_{7b}: HBT → INT-BEHV (-)	-0.273**** (t=3.182)	-0.264 n.s. (t=0.771)
R^2 of BINT	0.403	0.403
R^2 of BEHV	0.36	0.487
Effect Size (Moderator vs. Base Model)	0.177	0.443
Effect Size (Moderator vs. Direct Effect)	0.017	0.002

Note: *p < .10, **p < .05, ***p < .01, ****p < .001

The effect sizes of the moderation were compared between the two models. The model tested with the formative scale had a small effect size compared to the model with reflective scales, which had a large effect size when comparing the baseline model to the model with habit has a moderator. However, the effect size, when comparing the model

www.manaraa.com

of habit as a direct effect to the model with habit as a moderator was medium when tested with the formative scale and the effect size was very small in when tested with the reflective scale. This provides further evidence that the negative moderating effect of habit is stronger when habit is conceptualized as a second-order formative construct.

Habit as a Mediator of the PMT-Intention Relationship

As an alternative model, we tested Vance et al. (2012) research model with both the formative and the reflective habit measures separately. First we tested the Vance et al. (2012) research model with the first-order reflective and second-order formative habit scale and the results are shown on Figure 4.20. All the hypothesized paths of this model were significant. The formative habit construct demonstrated significant influences on all of the PMT variables and the PMT variables on behavioral intention.

المنارة للاستشارات

www.manaraa.com

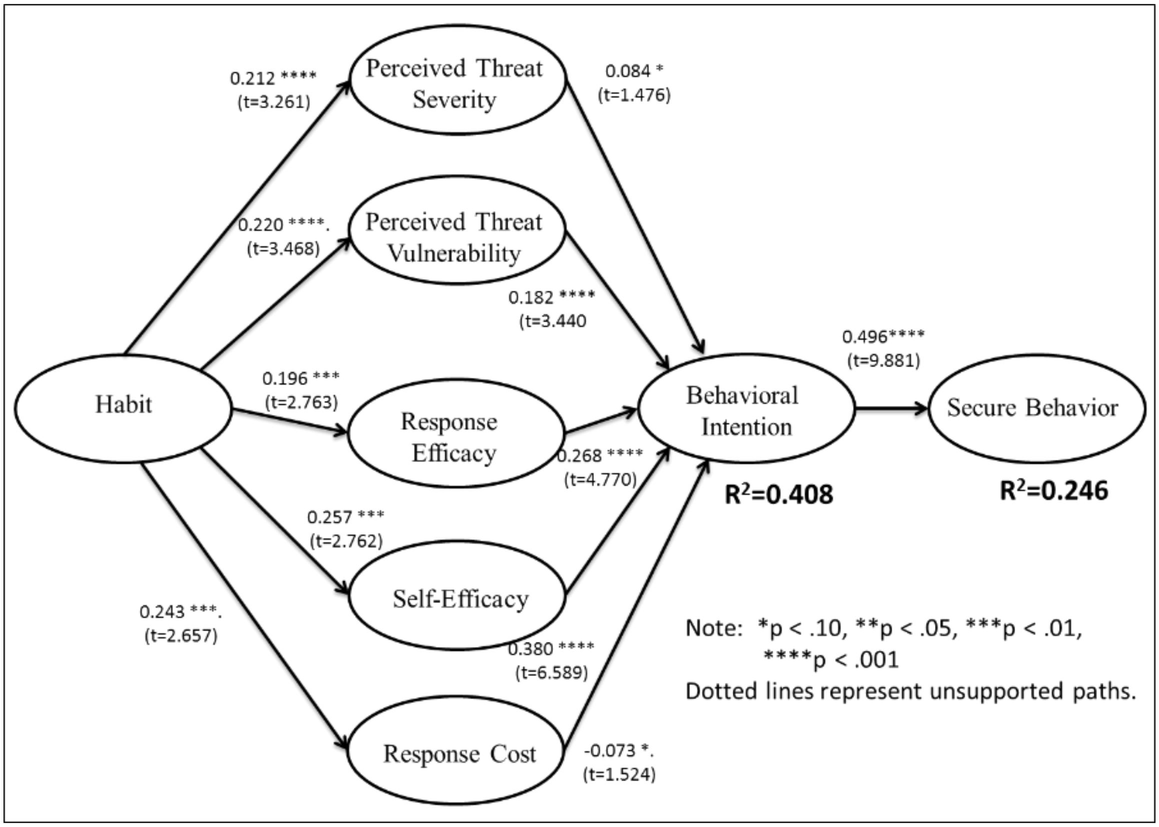


Figure 4.20 Visit Verified Websites: Habit (Formative) as an Indirect Influence

Next, we tested the Vance et al. (2012) research model with the 3-item reflective scale developed by Limayem et al. (2007) and the results are shown on Figure 4.21. Habit significantly influenced all the PMT variables except for response cost, with the highest path coefficient being 0.470 (p<0.001) between habit and self-efficacy. The supports for the hypotheses are consistent with the findings of Vance et al. (2012). However, the research model of Vance et al. (2012) demonstrated slightly higher explanatory power with an R-square of behavioral intention at 44 percent compared to the R-square value of 40 percent in each of our research models where habit was measured formatively and reflectively.

www.manaraa.com

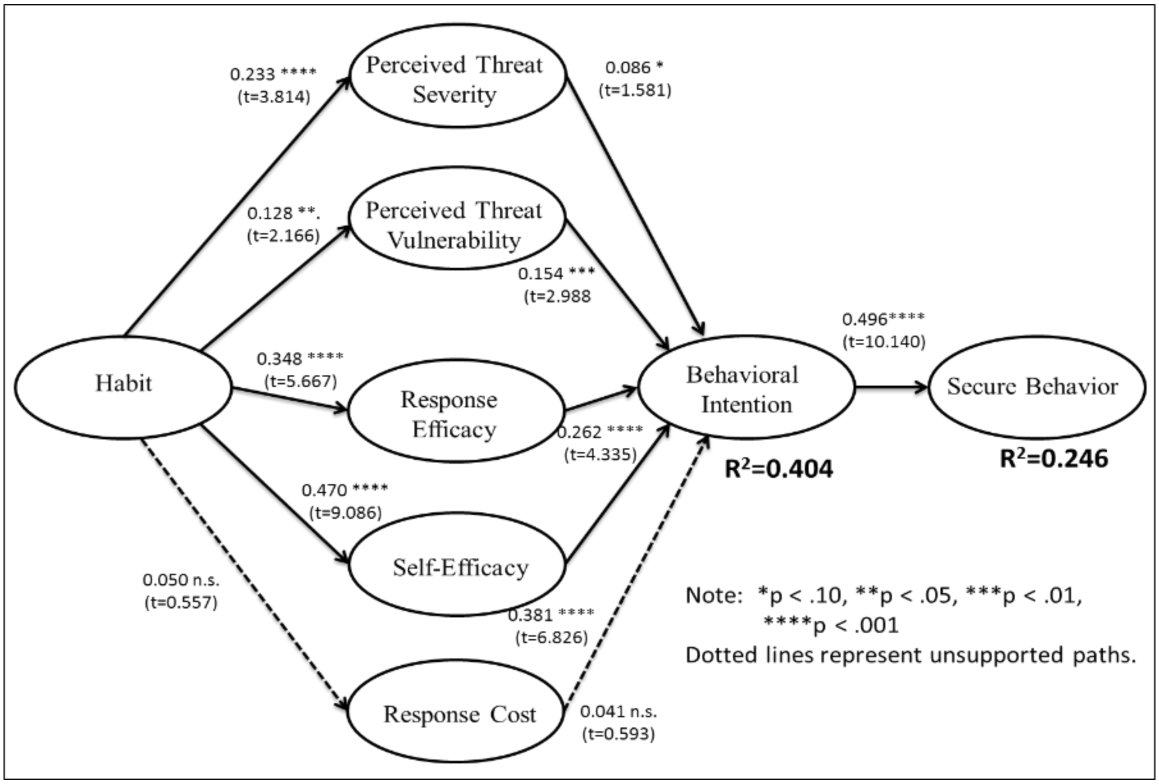


Figure 4.21 Visit Verified Websites: Habit (Reflective) as an Indirect Influence

Inertia as a mediator of Habit-Intention Relationship

An alternative model, where habit directly influenced inertia and inertia directly influenced behavioral intention, was tested. Similar to the formative habit construct, a two stage approach was followed where the PLS latest scores for each dimensions were used as the formative measures of the inertia construct (Polites and Karahanna 2012). Affective-based inertia demonstrated a weight of 0.369 (p<0.01) and behavior-based inertia demonstrated a weight of 0.709 (p<0.001), thus were suitable to be included in the data analysis. Habit was modeled as positively influencing inertia and inertia was modeled as positively influencing behavioral intention, which reflects the research model of Polites and Karahanna (2012).

www.manaraa.com

The results of the data analysis are shown on Figure 4.22. All the PMT variables significantly influenced behavioral intention except response cost. Habit significantly influenced inertia with a path coefficient of 0.512 ($p<0.001$) and inertia significantly influenced behavioral intention with a coefficient of 0.338 ($p<0.001$). Habit also explained 26.3 percent of the variance in inertia. The relationship between inertia and behavioral intention was positive for the visiting only verified websites too, which is in contrast to the hypothesis by Polites and Karahanna (2012). This means that increased levels of inertia leads to increased behavioral intention to perform secure behavior. R-square of the behavioral intention was 49.5 percent. Mediation tests revealed that inertia partially mediated the relationship between habit and behavioral intention. Another research model where a reflective habit construct was utilized yielded similar results with similar explanatory power.

A research model that included direct paths to behavioral intention from both habit and inertia demonstrated a R-square value of 49.8 percent, slightly increasing the explanatory power of the model due to the direct influence of habit on behavioral intention. The results suggest that inertia increased the explanatory power of the research model indicating that it may play a role in the performance of secure behaviors, although the path was significant in the opposite direction compared to the results of Polites and Karahanna (2012). This discrepancy of the results will be discussed in detail on Chapter V.

المنارة للاستشارات

www.manaraa.com

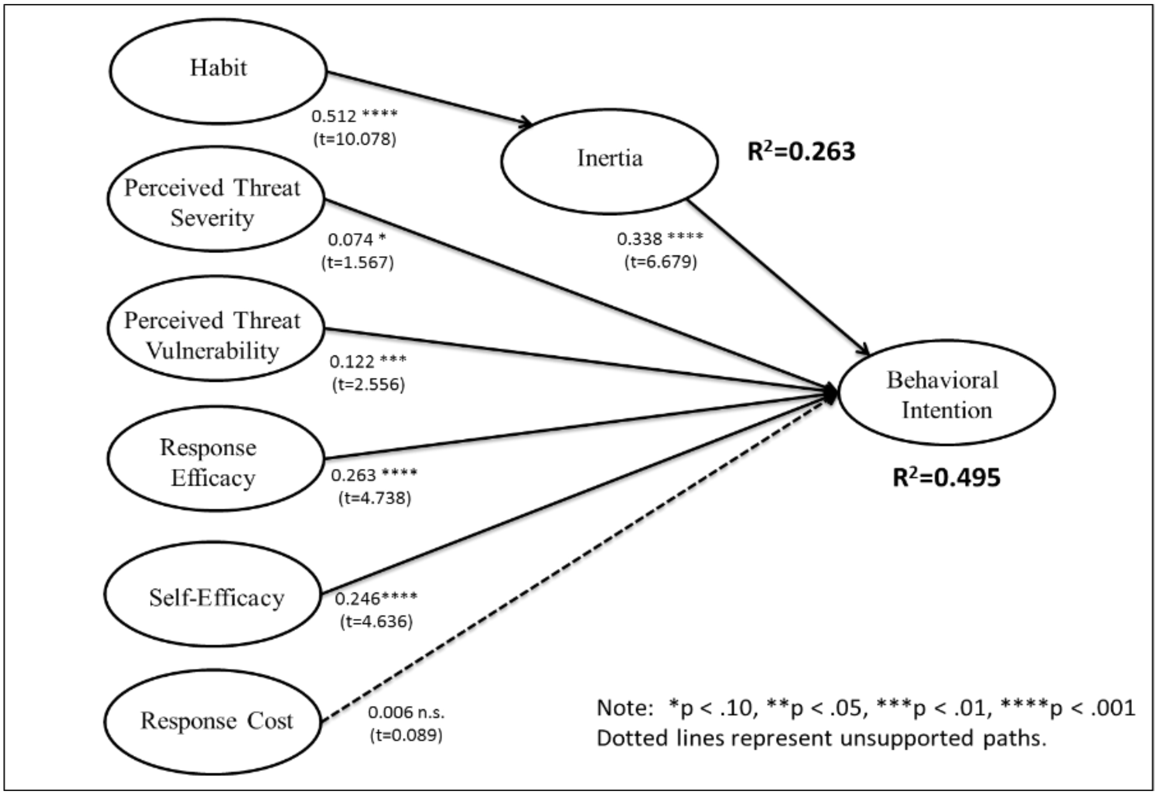


Figure 4.22 Visit Verified Websites: Inertia as a Mediator of Habit and Intention

Habit as a Direct Influence of Behavioral Intention

An alternative model where habit was modeled as a direct influence of behavioral intention was tested as a part of the post hoc analysis. First, the path between habit and behavioral intention was tested with the first-order reflective and second-order formative habit construct. The results of this analysis are shown on Figure 4.23. The path from habit to behavioral intention was significant with a path coefficient of 0.187 (p<0.001). All the paths from PMT variables to behavioral intention were significant except for response cost. R-square value of behavioral intention was 43.5 percent explaining more explanatory power than the baseline model without habit.

المنارة للاستشارات
www.manaraa.com

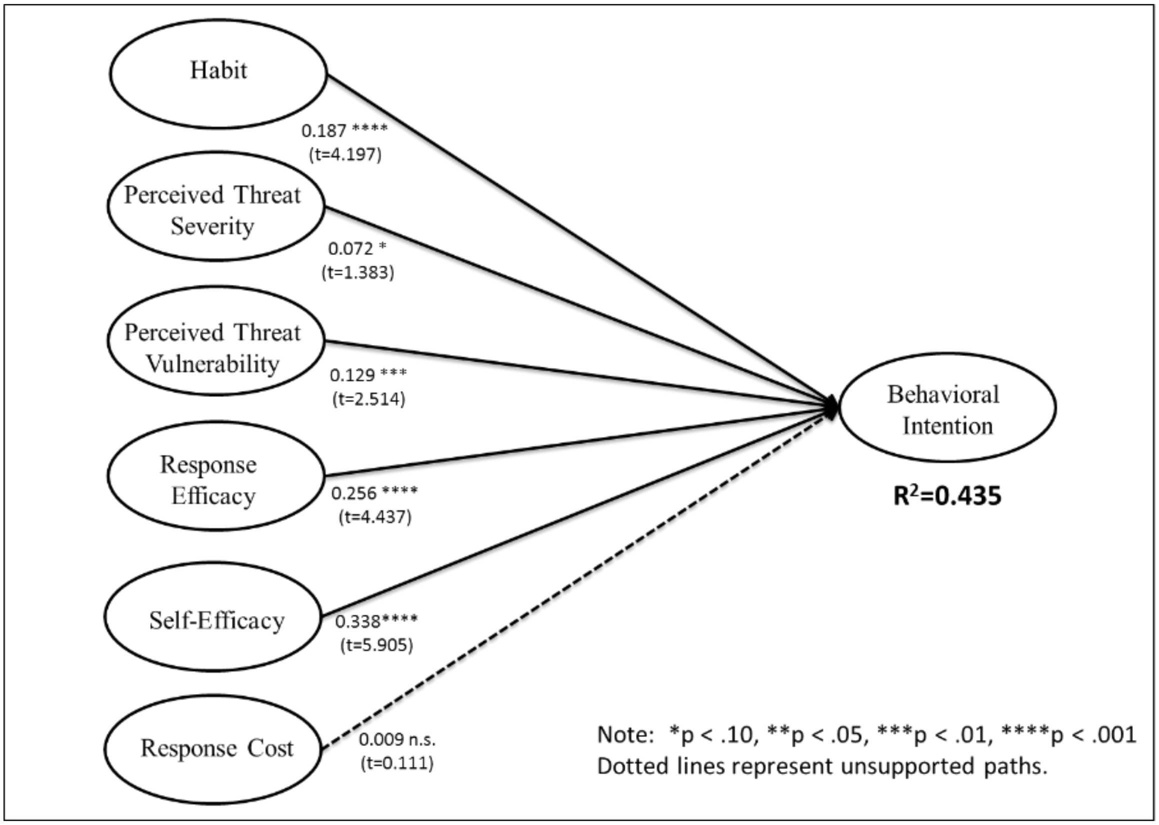


Figure 4.23 Visit Verified Websites: Direct Influence of Habit on Behavioral Intention

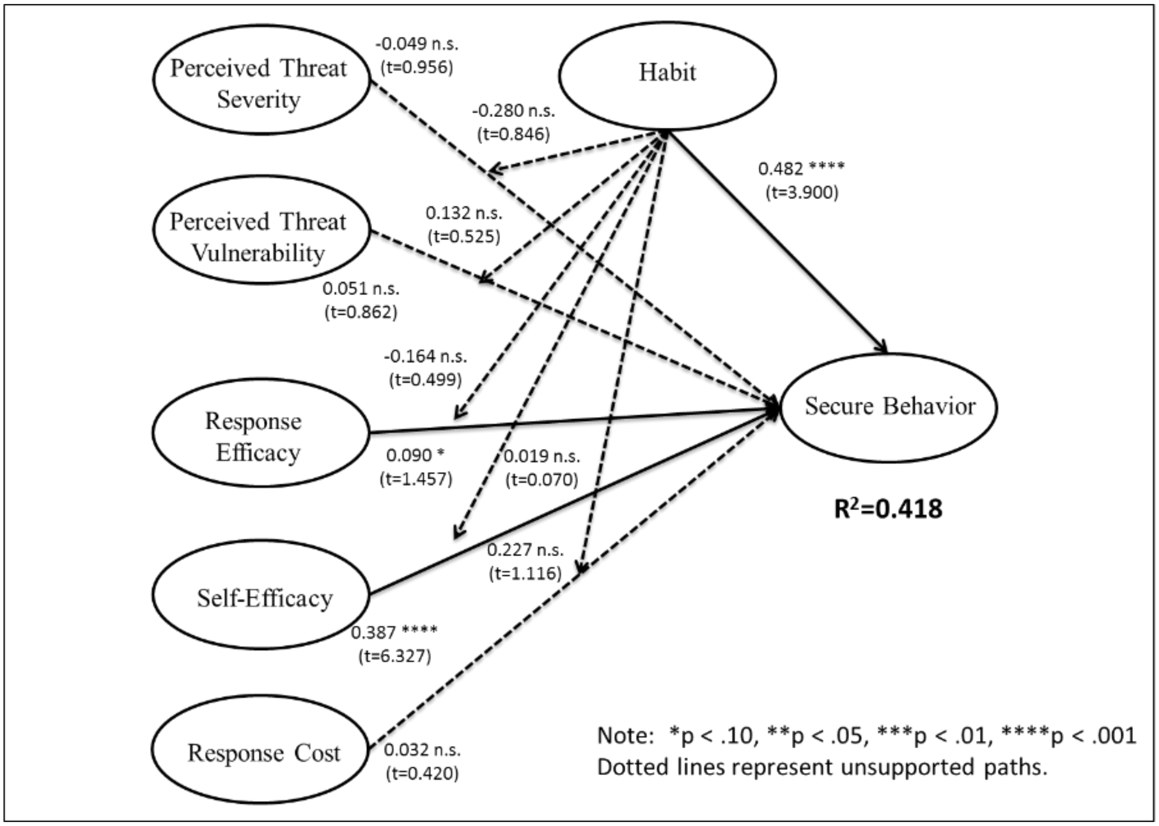
Next, the same model was tested with the reflective habit scale. The paths from perceived severity, perceived threat vulnerability and response cost to behavioral intention were non-significant. Only the paths from response efficacy and self-efficacy to behavioral intention were shown to be significant. The path from habit to behavioral intention was significant with a path coefficient of 0.334 (p<0.001). R-square of behavioral intention was 48.6 percent compared to the R-square of 43.5 percent when the model was tested with the formative habit scale. Therefore, the model with a reflective habit scale demonstrated higher explanatory power than the model with a formative habit scale when habit was modeled as a direct influence of behavioral intention.

www.manaraa.com

Habit as a Moderator of the PMT-Behavior Relationship

As a part of the post hoc study, an alternative model where PMT variables directly influenced actual behavior was tested. Habit was hypothesized to directly influence secure behavior while moderating the relationships between the PMT variables and actual behavior. The results of this analysis are shown on Figure 4.24.

Paths from perceived threat severity, response efficacy, self-efficacy and response cost to secure behavior were significant. Paths from perceived threat severity, perceived threat vulnerability and response cost were insignificant. Habit had a significant direct effect on secure behavior at p<0.001. However, habit did not significantly moderate any of the paths from the PMT variables to secure behavior.



Note: *p < .10, **p < .05, ***p < .01, ****p < .001
Dotted lines represent unsupported paths.

Figure 4.24 Visit Verified Websites: Habit as a Moderator of PMT-Behavior

المنارة للاستشارات
www.manaraa.com

Summary

This chapter discussed the EFA results of the preliminary investigation as well as the statistical analyses of the main investigation of three different secure behaviors. Using SmartPLS, tests of the measurement and structural models were performed for all three behaviors. Tests for moderations effects of habit on the intention-behavior relationship were conducted in three stages. The first stage included testing a baseline model without the incorporation of habit. The second stage included modeling habit as a direct effect on behavior. In the final stage, the complete research model was tested by including habit as a moderating relationship between the intention-behavior relationships. Several alternative models were tested in the post hoc analysis that allowed the comparison of the results of our research model with others.

المنارة للاستشارات

www.manaraa.com

CHAPTER V

DISCUSSION

The purpose of this dissertation is to identify the role of habit in information security behaviors in the workplace. In order to achieve this goal, a research agenda that consisted of three phases was executed. The first phase involved the identification of habitual behaviors related to information security. After a thorough review of academic publications and practitioner articles, a list of 49 unique secure behaviors was created. This list of behaviors was presented to a subject-matter expert panel and an employee expert panel, who were asked to select the behaviors they perceived to be habitual. Their responses were compiled and presented to members of a measurement panel. The measurement panel was requested to identify three behaviors that the panelists previously identified to be habitual. They were also requested to select behaviors that were practical to be measured through an online survey.

The second phase involved tests to ensure that the three instruments developed to investigate the three secure behaviors demonstrated content validity, reliability, discriminant validity and convergent validity. Preliminary tests were conducted for each of the three behaviors. The third phase or the main investigation phase involved the development and testing of a conceptual research model for each of the three behaviors. Usable sample sizes of 421, 443 and 395 were used to test the three corresponding research models of the three secure behaviors using SmartPLS. While the support for

المنارة للاستشارات
www.manaraa.com

hypotheses varied somewhat among the three behaviors tested, in all three behaviors habit was shown to have a significant direct influence on actual secure behavior and was shown to negatively moderate the intention-to-behavior relationship.

This chapter examines the results of the present study separately for each of the three behaviors followed by a discussion on the findings of the post hoc analyses. Next, the implications of this study, its findings and how they are related to both practice and theory in IS are discussed. Finally the limitations of this study are discussed followed by a discussion of future research directions.

Behavior 1: Lock PC

The first secure behavior investigated was locking the PC when leaving it unattended. Following the recommendations by Limayem et al. (2007), data analyses were performed in three stages. First analyzed was a baseline research model with only the PMT variables. The second model added habit as a potential direct effect on secure behavior. The third and final model added the possibility of habit negatively moderating the relationship between behavioral intention and secure behavior.

The tested models, investigated direct relationships from threat appraisal and coping appraisal variables to the behavioral intention to lock a PC when leaving it unattended. Perceived threat severity and perceived threat vulnerability demonstrated a significant positive relationship in determining whether individuals intended to lock their computers when leaving them unattended at the workplace. This provides support for H_1 and H_2. Crossler (2010), Herath and Rao (2009), Johnston and Warkentin (2010), Lee and Larsen (2009), Lee (2011), Liang and Xue (2010) and Woon et al. (2005) found that perceived threat severity was a significant predictor of their dependent variable of

المنارة للاستشارات

www.manaraa.com

different secure behaviors. Our findings are consistent with their results. The support for H_1 explains that the higher individuals perceive the threat of someone else accessing their computers without permission, the more likely they are to develop intentions to lock their computers to secure them when leaving them unattended. In organizations, employees often have access to sensitive data and their computers are setup to easily access this data. If an unauthorized person accesses this data while an employee is logged onto the computer with his or her credentials, it is very likely that the individual who was authenticated will be held responsible for any unauthorized access or modification of the sensitive company data. Therefore, a severe threat of unauthorized access to sensitive company data exists if the computers are left unattended without being locked. The data suggests that the perceived severity of the threat influences the employees to develop intentions to lock their computers whenever they leave it unattended.

Ifinedo (2012), Lee and Larsen (2009), and Liang and Xue (2010) found perceived threat vulnerability to be a significant factor that influences behavioral intention to perform secure behavior. This study had similar findings. The support for H_2 explains that the higher individuals perceive the probability of someone else accessing their computers without permission, the more likely they are to develop intentions to lock their computers to secure them when leaving them unattended. Many employees in many organizations work in open office areas or cubicles where other employees or unauthorized individuals can easily access any computer if they are not locked or logged off. Only a few employees have their own offices where the doors can be locked to secure their assets in the office. These results show that if the employees perceive that

www.manaraa.com

they are vulnerable to the threat of someone else accessing their computer if they leave their work area, then they are more likely to lock their computers.

Coping appraisal variables such as response efficacy, self-efficacy and response cost were tested for direct relationships with behavioral intention. Response efficacy and response cost were found to have significant relationships with behavioral intention to lock the computers when leaving them unattended supporting H_3 and H_5. Support for H_3, which hypothesized that response efficacy will positively influence behavioral intention, suggests that individuals are more likely to develop intentions to lock their computers as they gain confidence in the effectiveness of locking their computer to protect them from unauthorized access. This is consistent with the findings of prior research studies in an information security context (Anderson and Agarwal 2010; Crossler 2010; Herath and Rao 2009; Ifinedo 2012; Johnston and Warkentin 2010; Lee and Larsen 2009; Workman et al. 2008). Response cost, which refers to any costs, such as time, money, and inconvenience associated with performing a secure behavior to cope with a threat, was also found to have a significant negative relationship with behavioral intention to lock the PC when leaving it unattended, therefore supporting H_5. This finding is also consistent with the findings of prior research in information security (Herath and Rao 2009; Lee and Larsen 2009; Liang and Xue 2010; Woon et al. 2005). While locking the PC when leaving it unattended may not cost money, it may cost time to individuals who are not savvy with using shortcuts to perform the locking task and it may also cause inconvenience to employees in having to lock their computers every time they leave it unattended and having to unlock it once they return. The findings suggest that when an

المنارة للاستشارات
www.manaraa.com

employee perceives response cost to be higher, they are less likely to develop intentions to lock their computers when leaving them unattended.

In contrast to previous findings of information security research studies (Anderson and Agarwal 2010; Crossler 2010; Herath and Rao 2009; Ifinedo 2012; Johnston and Warkentin 2010; Lee and Larsen 2009; Liang and Xue 2010; Woon et al. 2005; Workman et al. 2008), self-efficacy was only shown to have a weak significant relationship with behavioral intention at $p<0.10$. Self-efficacy refers to the confidence of an individual in his or her ability to perform the specific secure behavior (locking the computer when leaving it unattended for this study). Examining the mean values for the self-efficacy construct, it seems that most of the respondents reported high self-efficacy with a mean of 4.27 out of 5. There was also little variability in this scale (standard deviation of 0.724), which could help explain the lack of an explanatory relationship. To test if the low significance between self-efficacy and behavioral intention was due to correlations with response efficacy, we examined if a suppressor effect from response efficacy was present in our model. We found that both response efficacy and response cost acted as suppressors for self-efficacy in our model. When self-efficacy was considered without the suppressor variables, it positively influenced behavioral intention with a path coefficient of 0.246 at $p<0.001$, which is consistent with PMT.

The hypothesized positive relationship between behavioral intention and self-reported actual behavior was significant, supporting H_6. This relationship has also been confirmed by a large number of IT adoption studies as well as many other behavioral studies in psychology (Fishbein and Ajzen 1975; Venkatesh et al. 2003). The results suggest that individuals are more likely to lock their computers when leaving them

المنارة للاستشارات

www.manaraa.com

unattended when they have formed behavioral intentions to perform that behavior. PMT variables explained 34 percent of the variance in behavioral intentions. 53.6 percent of the variance in self-reported actual behavior was explained by behavioral intentions. While the high R-square value of actual behavior may be due to somewhat high correlations with behavioral intention, a significant portion of the variance in actual behavior has been explained by behavioral intentions in prior studies (Liang and Xue 2010; Limayem et al. 2007; Venkatesh and Davis 2000; Venkatesh et al. 2000, 2003).

A second model investigated the influence of habit only as a direct effect on actual behavior. H_{7a}, in which habit was hypothesized to have a positive direct effect on actual behavior, was supported at $p<0.001$. Although this relationship has not been tested previously in an information security context, Moody and Siponen (2013) and Limayem et al. (2007) found habit to significantly influence actual behavior. The findings of this study are consistent with the findings of those studies. It was also examined that the path coefficient between behavioral intentions and actual behavior reduced from 0.732 to 0.558 when habit was introduced into the model as a direct determinant of actual behavior. This explains that when habit is included as a direct determinant of actual behavior, it reduces the influence of intentions in determining actual behavior. The R-square value of actual behavior increased to 59.6 percent, increasing the explanatory power of the research model.

The final and complete research model hypothesized habit as a negative moderator of the intention-behavior relationship. The results indicate that habit does negatively moderate the intention-behavior relationship significantly at $p<0.001$ supporting H_{7b}. The inclusion of habit as a moderator in the research model increased the

المنارة للاستشارات

www.manaraa.com

R-square value of actual behavior to 60.9 percent while further reducing the coefficient value of the intention-behavior relationship to 0.524. However, the relationship between behavioral intention and actual behavior remained significant, which shows that intention still plays a significant role even when habit is present. As discussed in the literature review section, in extreme circumstances, habitual behavior may become very strong to the point that intention will not have any influence on the actual behavior. It is clear that in this behavior, habit was not sufficiently strong to completely negate the influence of behavioral intentions. This indicates that the respondents perform the lock PC behavior habitually, but the strength of their habit is at a medium level. However, less cognitive effort is utilized to perform the lock PC behavior due to the behavior being habitual as it is apparent in the reduced influence on behavioral intentions on actual behavior. These findings are consistent with Limayem et al. (2007) in which habit negatively moderated the intention-behavior relationship. R-square difference tests between the models where habit was modeled as only a direct effect and where habit was also a moderator indicate that the moderation has a value of 0.033, which is a medium effect (Chin et al. 2003; Cohen 1988). This is consistent with the findings of Limayem et al. (2007), who also found that the negative moderation effect was at a medium level.

Habit was operationalized as a first-order reflective and second-order formative construct in this study. Statistical tests conducted to examine the weights of the formative dimensions of habit indicate that the lack of awareness and uncontrollability dimensions were significant factors in forming the habit construct while mental efficiency was non-significant. However, based on recommendations of prior research studies (Bollen and Lennox 1991; Diamantopoulos and Siguaw 2006; Diamantopoulos and Winklhofer 2001;

المنارة للاستشارات

www.manaraa.com

Diamantopoulos et al. 2008; Petter et al. 2007), mental efficiency was retained for further data analysis. Respondents of this study demonstrated that mental efficiency was high (mean=3.47) when the lock PC behavior is performed (e.g., I do not need to devote a lot of mental effort to decide to lock the computer every time I leave it unattended). However, it was not a significant contributor to the formation of habit. Polites and Karahanna (2012) found that awareness was not a significant factor that formed habit in their study. The non-significant dimensions in our study and the study of Polites and Karahanna (2012) may be due to the specific contexts of the studies or due to inconsistencies of the habit scale. However, the second-order habit construct consistently demonstrated significant effects on the dependent variable in this dissertation and the study by Polites and Karahanna (2012).

Behavior 2: Verify Email Recipient

The second secure behavior investigated was the verification of the recipient email address before sending email. Similar to behavior 1, data analyses were conducted in three stages: a baseline model with only the PMT variables, a model with PMT variables and habit as only a direct effect and a full research model where habit was hypothesized to influence secure behavior directly and negatively moderate the relationship between behavioral intention and secure behavior.

The models tested, considered direct relationships from threat appraisal and coping appraisal variables to the behavioral intention to verify the email addresses of the recipients before sending email. Perceived threat severity demonstrated a significant positive relationship, supporting H_1, which is consistent with many prior studies that found similar results (Crossler 2010; Herath and Rao 2009; Johnston and Warkentin

المنارة للاستشارات
www.manaraa.com

2010; Lee and Larsen 2009; Lee 2011; Liang and Xue 2010; Woon et al. 2005). The support for H_1 explains that the higher an individual perceives the threat of an unintended recipient receiving an email with sensitive company data, the more likely he or she is to check the recipient addresses before sending email. In organizations, daily tasks of most employees involve communicating with other employees, clients and other interested parties through email. These emails may sometimes contain sensitive company information such as budgetary data, patent information, or corporate secrets where if an unintended recipient were to receive such an email, the company will have to suffer dire consequences. Therefore, most employees make sure that they verify recipient addresses before sending an email whether or not the email contains sensitive company information. The data suggests that the respondents perceive an unintended recipient receiving an email with sensitive corporate data as a severe threat, which in turn influences them to verify the recipient email addresses before sending an email.

The hypothesized relationship between perceived threat vulnerability and behavioral intention (H_2) was not supported. As discussed previously in the literature review section, the relationship between perceived threat vulnerability and behavioral intention has inconclusive results. While results of some previous studies indicate a significant relationship between perceived threat vulnerability and behavioral intention (Ifinedo, 2012; Lee and Larsen 2009; Liang and Xue 2010; Ng et al., 2009; Pahnila et al., 2007; Woon et al., 2005), some studies indicate non-significant relationships (Herath and Rao 2009; Johnston and Warkentin 2010; Malimage & Warkentin, 2010; Woon et al. 2005). The data suggests that on average, respondents perceived that the possibility of an unintended recipient receiving an email with sensitive company information is low

المنارة للاستشارات
www.manaraa.com

(mean=2.84). However, if an unintended recipient were to receive an email with sensitive company data, they perceived it would be severe. The results may indicate that the respondents are very careful when sending emails with sensitive data such that they check the recipient addresses often. It may also mean that they are not involved in sending emails with any sensitive data.

Coping appraisal variables such as response efficacy, self-efficacy and response cost were tested for direct relationships with behavioral intention. H_3, where it was hypothesized that response efficacy will significantly influence behavioral intention, was supported. This suggests that individuals are more likely to develop intentions to verify email addresses of the recipients before sending email, as they gain in confidence that the verification of email addresses will result in reducing the chances of an unintended recipient receiving an email with sensitive company information. Support for H_3 is also consistent with the findings of prior research studies (Anderson and Agarwal 2010; Crossler 2010; Herath and Rao 2009; Ifinedo 2012; Johnston and Warkentin 2010; Lee and Larsen 2009; Workman et al. 2008). Self-efficacy was found to have a significant influence on behavioral intention, supporting H_4. This is consistent with the findings of prior research studies as well (Anderson and Agarwal 2010; Crossler 2010; Herath and Rao 2009; Ifinedo 2012; Johnston and Warkentin 2010; Lee and Larsen 2009; Liang and Xue 2010; Woon et al. 2005; Workman et al. 2008). This suggests that individuals are more likely to verify the recipient email addresses before sending email as they gain confidence in their ability to verify the recipient email addresses are the intended ones.

Response cost was not shown to have a significant relationship with behavioral intention. Although the path co-efficient was negative (-0.075) as hypothesized, the path

المنارة للاستشارات
www.manaraa.com

was not significant. Some of the previous studies found that response cost was a significant factor influencing behavioral intention (Herath and Rao 2009; Lee and Larsen 2009; Liang and Xue 2010; Vance et al. 2012; Woon et al. 2005). The findings of this study are consistent with the findings of Ifinedo (2012) and (Crossler 2010) where the path between response cost and behavioral intention was not significant. This suggests that individuals do not associate costs, such as time, money, and inconvenience with verifying the recipient email addresses before sending email. Compared to locking a PC when leaving it unattended, verifying the email addresses before sending an email involves very little time or effort resulting in less inconvenience to the employees. This is reflected by the findings of this study as well.

The hypothesized positive relationship between behavioral intention and self-reported actual behavior was significant, supporting H_6. This relationship has also been confirmed by a large number of IT adoption studies as well as many other behavioral studies in psychology (Fishbein and Ajzen 1975; Venkatesh et al. 2003). The results suggest that individuals are more likely to verify email addresses of the recipients before sending email, when they have formed behavioral intentions to perform that behavior. PMT variables explained 34.9 percent of the variance in behavioral intentions while 41.7 percent of the variance in self-reported actual behavior was in turn explained by behavioral intentions. This is consistent with previous studies where a significant portion of the variance in actual behavior was explained by behavioral intentions (Liang and Xue 2010; Limayem et al. 2007; Venkatesh and Davis 2000; Venkatesh et al. 2000, 2003).

A second model investigated the influence of habit only as a direct effect on actual behavior. H_{7a}, where habit was hypothesized to have a positive direct effect on

المنارة للاستشارات
www.manaraa.com

actual behavior, was supported at $p<0.01$. Although this relationship has not been tested previously in an information security context, Moody and Siponen (2013) and Limayem et al. (2007) found habit to significantly influence actual behavior. The findings of this study are consistent with the findings of those studies. The path coefficient between behavioral intentions and actual behavior was reduced from 0.646 to 0.597 when habit was introduced into the model as a direct predictor of actual behavior. The R-square value of actual behavior increased to 43.4 percent, increasing the explanatory power of the research model.

The final and complete research model hypothesized habit as a negative moderator of the intention-behavior relationship. The results indicate that habit does negatively moderate the intention-behavior relationship significantly at $p<0.001$ supporting H_{7b}. The inclusion of habit has a moderator in the research model increased the R-square value of actual behavior to 44.5 percent while further reducing the coefficient of the intention-behavior relationship to 0.551. However, the relationship between behavioral intention and secure behavior remained significant, which explains that intention still has a significant role even with habit as a direct predictor of this behavior. As discussed in the literature review section, in extreme circumstances, habitual behavior may become very strong to the point that intention will not have any influence on the actual behavior. It is clear in our study that habit is not sufficiently strong to make the influence of behavioral intentions non-significant. This indicates that the respondents habitually verify the recipient email addresses before sending email, but the strength of their habit is at a medium level. However, less cognitive effort is utilized to verify the email addresses due to the behavior being habitual as it is apparent in the reduced

المنارة للاستشارات

www.manaraa.com

influence on behavioral intentions on actual behavior. These findings are consistent with those of Limayem et al. (2007) showing habit to negatively moderate the intention-behavior relationship. R-square difference tests between the models where habit was modeled as a direct effect and habit was modeled as a moderator indicate that the moderation has an effect size value of 0.02, which is a small effect (Chin et al. 2003; Cohen 1988). This is somewhat consistent with the findings of Limayem et al. (2007), who found a negative moderation effect that was at the medium level. However, it is important to note that when an effect size is small, it does not mean that the change in R-square is unimportant (Abelson 1985; Prentice and Miller 1992).

Habit was operationalized as a first-order reflective and second-order formative construct in this study. Statistical tests conducted to examine the weights of the formative dimensions of habit indicate that lack of awareness and mental efficiency dimensions were significant factors in forming the habit construct while uncontrollability was not significant. However, based on recommendations of prior research studies (Bollen and Lennox 1991; Diamantopoulos and Siguaw 2006; Diamantopoulos and Winklhofer 2001; Diamantopoulos et al. 2008; Petter et al.2007), uncontrollability was retained for further data analysis. Respondents of this study demonstrated that uncontrollability was above neutral (mean=3.22) when the recipient email addresses are verified (e.g., It would be difficult to control my tendency to verify the recipient email addresses before sending email). However, it was not a significant contributor to the formation of habit. Polites and Karahanna (2012) found that awareness was not a significant factor that formed habit in their study. The insignificant dimensions in our study and the study of Polites and Karahanna (2012) may be due to the specific contexts of the studies or due to

المنارة للاستشارات
www.manaraa.com

inconsistencies of the habit scale. However, the second-order habit construct consistently demonstrated significant effects on the dependent variable in both the studies.

Behavior 3: Visit Verified Websites

The third secure behavior investigated was visiting only verified websites. Similar to behavior 1 and 2, data analyses were run in three stages: a baseline model with only the PMT variables, a model with PMT variables and habit as only a direct effect, and a full research model where habit was hypothesized to influence secure behavior directly while negatively moderating the relationship between behavioral intention and secure behavior.

The model tested, investigated direct relationships from threat appraisal and coping appraisal variables to the behavioral intention to visit only verified websites. Perceived threat severity and perceived threat vulnerability demonstrated significant positive relationships in determining whether individuals intended to visit only verified websites at the workplace. This provides support for H_1 and H_2. Threats of visiting unverified or unknown websites include virus or spyware infection of the computer at the workplace, which may expose the company network and data to outsiders. Crossler (2010), Herath and Rao (2009), Johnston and Warkentin (2010), Lee and Larsen (2009), Lee (2011), Liang and Xue (2010) and Woon et al. (2005) found that perceived threat severity was a significant predictor of their dependent variable of different secure behaviors and our findings are consistent with their results. The support for H_1 explains that the higher an individual perceives the threat of getting infected with malware by visiting unknown websites, the more likely he or she is to develop intentions to visit only verified websites. In organizations, employees have access to sensitive data and their

المنارة للاستشارات
www.manaraa.com

computers are setup to easily access this data. If a computer gets infected with a virus or other type of spyware, the information stored on that computer and on the company network will be at risk of being compromised. Therefore, a severe threat of data breach or compromise exists, if the computers get infected with virus or spyware because of visiting unknown websites. The data suggests that employees understand this threat to be severe and it influences them to develop intentions to visit only verified websites.

Ifinedo (2012), Lee and Larsen (2009), Liang and Xue (2010) and Workman et al. (2008) found perceived threat vulnerability to be a significant factor that influences behavioral intention to perform secure behavior. This study had similar findings. The support for H_2 shows that the higher an individual perceives the probability of their computer getting infected with malware by visiting unknown websites; the more likely they are to develop intentions to visit only verified websites. The findings of the relationships between the threat appraisal and coping appraisal variables suggest that individuals perceive that a severe threat of getting their work computer infected with malware is severe and the possibility of that happening is high. Therefore, they are more likely to visit only verified websites to protect their computers from malware infections.

Coping appraisal variables such as response efficacy, self-efficacy and response cost were tested for direct relationships with behavioral intention. H_3, where it was hypothesized that response efficacy will significantly influence behavioral intention, was supported. This suggests that individuals are more likely to develop intentions to visit only verified websites as they gain in confidence that visiting only verified websites will prevent them from getting infected with malware. Support for H_3 is also consistent with the findings of prior research studies (Anderson and Agarwal 2010; Crossler 2010;

www.manaraa.com

Herath and Rao 2009; Ifinedo 2012; Johnston and Warkentin 2010; Lee and Larsen 2009; Workman et al. 2008). Self-efficacy was found to have a significant influence on behavioral intention, supporting H_4. This is consistent with the findings of prior research studies as well (Anderson and Agarwal 2010; Crossler 2010; Herath and Rao 2009; Ifinedo 2012; Johnston and Warkentin 2010; Lee and Larsen 2009; Liang and Xue 2010; Woon et al. 2005; Workman et al. 2008). This suggests that individuals are more likely to visit only verified websites as they gain confidence in their ability to identify websites or web-links that are safe and do not pose a threat of malware.

Response cost did not demonstrate a significant relationship with behavioral intention. Although the path co-efficient was negative (-0.013) as hypothesized, the path was not significant. Some of the previous studies found that response cost was a significant factor influencing behavioral intention (Herath and Rao 2009; Lee and Larsen 2009; Liang and Xue 2010; Vance et al. 2012; Woon et al. 2005). The findings of this study are consistent with the findings of Ifinedo (2012) and (Crossler 2010) where the path between response cost and behavioral intention was not significant. This suggests that individuals do not associate any costs, such as time, money, or inconvenience with visiting only verified websites. Compared to locking a pc when leaving it unattended, visiting only verified websites involves very little time or effort resulting in less inconvenience to the employees. This is reflected by the findings of this study as well.

The hypothesized positive relationship between behavioral intention and self-reported actual behavior was significant, supporting H_6. This relationship has also been confirmed by a large number of IT adoption studies as well as many other behavioral studies in psychology (Fishbein and Ajzen 1975; Venkatesh et al. 2003). The results

المنارة للاستشارات
www.manaraa.com

suggest that individuals are more likely to visit only verified websites when they have formed behavioral intentions to perform that behavior. PMT variables explained 40.3 percent of the variance in behavioral intentions. Only 24.7 percent of the variance in self-reported actual behavior was explained by behavioral intentions. While the high R-square value of actual behavior may be somewhat low compared to behavior 1 and 2, it is still a relatively high percentage. A significant portion of the variance in actual behavior has been explained by behavioral intentions in prior studies (Liang and Xue 2010; Limayem et al. 2007; Venkatesh and Davis 2000; Venkatesh et al. 2000, 2003).

A second model investigated the influence of habit only as a direct effect on actual behavior. H_{7a}, where habit was hypothesized to have a positive direct effect on actual behavior, was supported at $p<0.001$. Although this relationship has not been tested previously in an information security context, Moody and Siponen (2013) and Limayem et al. (2007) found habit to significantly influence actual behavior. The findings of this study are consistent with the findings of those studies. It was also examined that the path coefficient between behavioral intentions and actual behavior reduced from 0.497 to 0.375 when habit was introduced into the model as a direct effect of actual behavior. This explains that when habit is present, it reduces the influence of intentions as the driving force of actual behavior. When habit was introduced into the model, the R-square value of actual behavior increased to 34.9 percent, increasing the explanatory power of the research model.

The final and complete research model hypothesized habit as a negative moderator of the intention-behavior relationship. The results indicate that habit does negatively moderate the intention-behavior relationship significantly at $p<0.001$

المنارة للاستشارات

www.manaraa.com

supporting H_{7b}. The inclusion of habit as a moderator in the research model increased the R-square value of actual behavior to 36 percent, while the coefficient value of the intention-behavior relationship remained constant at 0.375. However, the relationship between behavioral intention and secure behavior remained significant, which shows that intentions still play a significant role even when habit is present. As discussed in the literature review section, in extreme circumstances, habitual behavior may become very strong to the point that intention will not have any influence on the actual behavior. It is clear that in our study, habit is not extremely strong to make the influence of behavioral intentions non-significant. This indicates that the respondents visit only verified websites habitually, but the strength of their habit is at a medium level. However, less cognitive effort is utilized to visit only verified websites due to the behavior being habitual as it is apparent in the reduced influence on behavioral intentions on actual behavior. These findings are consistent with Limayem et al. (2007), where they found habit to negatively moderate the intention-behavior relationship. R-square difference tests between the models where habit was modeled as a direct effect and habit was modeled as a moderator indicate that the moderation has an effect size value of 0.02, which is a small effect (Chin et al. 2003; Cohen 1988). This is somewhat consistent with the findings of Limayem et al. (2007), who also found a negative moderation effect that was at the medium level. Again, it is also important to note that when an effect size is small, it does not mean that the change in R-square is unimportant (Abelson 1985; Prentice and Miller 1992).

Habit was operationalized as a first-order reflective and second-order formative construct in this study. Statistical tests conducted to examine the weights of the formative dimensions of habit indicate that lack of awareness and uncontrollability dimensions

المنارة للاستشارات
www.manaraa.com

were significant factors in forming the habit construct, while mental efficiency was non-significant. This is consistent with the findings of lock PC behavior where mental efficiency was not a significant factor that formed the habit construct. However, based on recommendations of prior research studies (Bollen and Lennox 1991; Diamantopoulos and Siguaw 2006; Diamantopoulos and Winklhofer 2001; Diamantopoulos et al. 2008; Petter et al.2007), mental efficiency was retained for further data analysis. Respondents of this study demonstrated that mental efficiency was high when the visiting only verified websites behavior is performed (e.g., I do not need to devote a lot of mental effort to decide to visit only verified websites). However, it was not a significant contributor to the formation of habit. Polites and Karahanna (2012) found that awareness was not a significant factor that formed habit in their study. The insignificant dimensions in our study and the study of Polites and Karahanna (2012) may be due to the specific contexts of the studies or due to inconsistencies of the habit scale. However, the second-order habit construct consistently demonstrated significant effects on the dependent variable in both the studies.

Post hoc Analyses

To further test the validity of using habit as a formative measure, several alternative models were analyzed as a post hoc step. This section discusses the findings of the post hoc alternative models that tested the behaviors of locking the PC, verifying email address of recipients and visiting only verified websites respectively. It is important to note that all the statistical analyses of the structural models of this dissertation were conducted with SmartPLS. PLS software such as SmartPLS, does not provide any fit statistics similar to covariance based SEM tools such as AMOS or LISREL. A goodness-

المنارة للاستشارات
www.manaraa.com

of-fit (GoF) index was recently suggested by some scholars, but it has been heavily criticized due to the over reliance on the R-square value and communality values. Chin (1998) also criticizes the overreliance of fit indices and posits that a model with high goodness-of-fit may still yield low R-square values and low path coefficients resulting in a model with low predictive power. Moreover, he suggests that research models with formative measures would not enable researchers to accurately calculate goodness-of-fit. Therefore, the post hoc analyses compared the R-square values and path coefficient values between models instead of GoF values.

Behavior 1 or locking the computer when leaving it unattended was tested with alternative models. Habit was measured with a 3-item reflective scale developed by Limayem et al. (2007), and the reflective scale was used to test the main research model. The alternative model with the reflective scale demonstrated higher explanatory power than our research model with the alternative model demonstrating an R-square value of 71 percent for the actual behavior compared to the main research model R-square value of 60.9 percent. The habit coefficient in the alternative model also demonstrated a higher predictive ability on actual behavior compared to the main research model. The coefficient value of the relationship between habit and actual behavior in the main research model was 0.515 and the value increased to 0.75 in the alternative model. However, it is important to note that the path coefficient of the moderating path of habit on intention-behavior relationship was lower in the alternative model compared to the main research model (-0.143 vs. -0.226). Although the alternative model with the reflective habit scale may demonstrate higher predictive power than the main research model, it is important to consider that the reflective scale fails to accurately capture the

المنارة للاستشارات
www.manaraa.com

multidimensional nature of habit (Polites and Karahanna 2012). Therefore, a formative scale that takes the different dimensions of habit would still be preferred to measure habit.

Lock PC behavior was tested on another alternative model where PMT was modeled to mediate the habit-intention relationship as it was modeled by Vance et al. (2012). This alternative model was tested with both the formative and reflective constructs of habit. When the Vance et al. (2012) model was tested with the formative scale, habit demonstrated significant direct paths with only threat severity and threat vulnerability while all of the direct paths from habit to coping appraisal variables were found to be non-significant. When habit was tested with the reflective scale, the alternative model yielded similar results to Vance et al. (2012) with all the paths from habit to threat and coping appraisal being significant. Both alternative models showed similar predictive power with the R-square value of actual behavior being 53.6 percent, which is less than the 60.9 percent of the main research model.

Lock PC behavior was again tested on another alternative model where inertia was included as a mediator of the habit-intention relationship as it was modeled by Polites and Karahanna (2012). Although inertia is not applicable in the context of this dissertation, considering the possible relationship between inertia and habit, inertia was measured and an alternative model was tested as a part of the post hoc analysis of this study. All the paths between PMT variables and behavioral intention were significant except for perceived threat vulnerability. Habit-inertia path and inertia-intention path were significant at $p<0.001$ in the opposite direction as hypothesized by Polites and Karahanna (2012). This may indicate that inertia may be somewhat relevant to the

المنارة للاستشارات
www.manaraa.com

behavior of locking the computer when leaving it unattended, since inertia refers to the attachment of existing behavioral patterns (status-quo) even if there are better alternatives. In the study of Polites and Karahanna (2012), inertia was modeled to negatively influence behavioral intention, where the higher the inertia, the lesser an individual would intend to perform an alternate behavior. However, for the context of this study, no alternative behaviors were suggested to the respondent; therefore in the context of our study, the higher the inertia of an individual, the more likely he or she would intend to perform the lock PC behavior as the data suggested.

Two more alternative models were tested with the from the lock PC behavior. One of the alternative models tested the direct influence of habit along with PMT variables on behavioral intention. The R-square value of the behavioral intention yielded 51.5 percent, which was much higher than the R-square value of the behavioral intention in the main research model. However, the two models cannot be compared since the alternative model omitted the variable of actual behavior. However, it is interesting to see that all the paths of this research model were significant. Another alternative model tested the influence of PMT variables on actual behavior while habit moderated the paths between the PMT variables and behavior. The dependent variable of this research model, actual behavior, had an R-square value of 52.6, but most of the paths were not significant. Perceived threat severity and response cost were found to have significant paths on actual behavior while habit significantly moderated those paths. All other paths were found to be non-significant. The results suggest that while actual behavior may matter the most in information security, it may not be influenced by threat and coping variables when a behavior is habituated.

المنارة للاستشارات
www.manaraa.com

Behavior 2 or verifying the recipient email addresses before sending email was tested with alternative models. Habit was measured with a 3-item reflective scale developed by Limayem et al. (2007), and the reflective scale was used to test the main research model. The alternative model with the reflective scale demonstrated lower explanatory power than our main research model. The calculated R-square value for the actual behavior of the alternative model was 55 percent compared to the main research model R-square value of 60.9 percent. The habit coefficient in the alternative model demonstrated a higher predictive ability on actual behavior compared to the main research model. The coefficient value of the relationship between habit and actual behavior in the main research model was 0.515 and the value increased to 0.616 in the alternative model. However, it is important to note that the path coefficient of the moderating path of habit on intention-behavior relationship was not significant in the alternative model ($p>0.05$). This indicates that when investigating the role of habit in verifying the email recipient before sending email, the formative scale better captures the habit.

Verifying email recipients was tested on another alternative model where PMT was modeled to mediate the habit-intention relationship as it was modeled by Vance et al. (2012). This alternative model was tested with both the formative and reflective constructs of habit. When the Vance et al. (2012) model was tested with the formative scale, habit demonstrated significant direct paths from habit to PMT variables except for the path from habit to self-efficacy. When habit was tested with the reflective scale, the alternative model yielded similar results to Vance et al. (2012) with all the paths from habit to threat and coping appraisal being significant. Both alternative models showed

المنارة للاستشارات
www.manaraa.com

similar predictive power with the R-square value of actual behavior being 41.7 percent, which is less than the 44.5 percent of the main research model.

Verifying email recipients was again tested on another alternative model where inertia was included as a mediator of the habit-intention relationship as it was modeled by Polites and Karahanna (2012). All the paths between PMT variables and behavioral intention were shown to be significant. Habit-inertia path and inertia-intention path were significant at $p<0.001$ in the opposite direction as hypothesized by Polites and Karahanna (2012). This may indicate that inertia may be somewhat relevant to the behavior of verifying email recipients before sending email. Since no alternative behaviors were suggested to the respondent, in the context of our study, inertia should increase the behavioral intentions to verify the recipient email addresses before sending email as the data suggested.

Two more alternative models were tested with the behavior of verifying email recipients. One of the alternative models tested the direct influence of habit along with PMT variables on behavioral intention. The R-square value of the behavioral intention yielded 42.6 percent, which is lesser than the R-square value of the behavioral intention in the main research model. However, the two models cannot be compared since the alternative model omitted the variable of actual behavior. It is interesting to see that all the paths of this research model were significant except for perceived threat vulnerability. Another alternative model tested the influence of PMT variables on actual behavior while habit moderated the paths between the PMT variables and behavior. The dependent variable of this research model, actual behavior, had an R-square value of 41.4. All the paths between the PMT variables and behavior were significant except for the path

المنارة للاستشارات
www.manaraa.com

between perceived threat vulnerability and behavior. Paths between perceived threat severity and response cost with behavior were shown to be significantly moderated by habit, which other relationships were not significantly moderated. Interestingly, the relationship between habit and behavior was non-significant for this study. The results suggest that when considering the behavior of verifying email recipients before sending email, threat and coping appraisals are strong determinants of actual behavior than habit.

Behavior 3 or visiting only verified websites was tested with alternate models. Habit was measured with a 3-item reflective scale developed by Limayem et al. (2007), and the reflective scale was used to test the main research model. The alternate model with the reflective scale demonstrated higher explanatory power than our main research model. The calculated R-square value for the actual behavior of the alternative model was 48.7 percent compared to the main research model R-square value of 36 percent. The habit coefficient in the alternate model demonstrated a higher predictive ability on actual behavior compared to the main research model. The coefficient value of the relationship between habit and actual behavior in the main research model was 0.596 and the value increased to 0.616 in the alternative model. However, it is important to note that the path coefficient of the moderating path of habit on intention-behavior relationship was not significant in the alternate model ($p>0.05$). This indicates that when investigating the role of habit in visiting only verified websites, the formative scale better captures the habit.

Visiting only verified websites was tested on another alternative model where PMT was modeled to mediate the habit-intention relationship as it was modeled by Vance et al. (2012). This alternative model was tested with both the formative and reflective constructs of habit. When the Vance et al. (2012) model was tested with the

www.manaraa.com

formative scale, habit demonstrated significant direct paths from habit to all the PMT variables. When habit was tested with the reflective scale, the alternate model yielded similar results to Vance et al. (2012) with all the paths from habit to threat and coping appraisal being significant. Both alternative models showed similar predictive power with the R-square value of actual behavior being 24.6 percent, which is less than the 36 percent of the main research model.

Visiting only verified websites was again tested on another alternative model where inertia was included as a mediator of the habit-intention relationship as it was modeled by Polites and Karahanna (2012). All the paths between PMT variables and behavioral intention were significant except for perceived threat vulnerability. Habit-inertia path and inertia-intention path were significant at $p<0.001$ in the opposite direction as hypothesized by Polites and Karahanna (2012). For the context of this study, no alternative behaviors were suggested to the respondent; therefore, inertia should increase the behavioral intentions to visit only verified websites as the data suggested.

Two more alternative models were tested with the behavior of visiting only verified websites. One of the alternate models tested the direct influence of habit along with PMT variables on behavioral intention. The R-square value of the behavioral intention yielded 43.5 percent, which was much higher than the R-square value of the behavioral intention in the main research model. The two models cannot be compared since the alternative model omitted the variable of actual behavior. However, it is interesting to see that all the paths of this research model were significant except for the path between response cost and behavioral intention. Another alternative model tested the influence of PMT variables on actual behavior while habit moderated the paths between

المنارة للاستشارات
www.manaraa.com

the PMT variables and behavior. The dependent variable of this research model, actual behavior, had an R-square value of 41.8 percent, but most of the paths were not significant. Habit showed a significant relationship with behavior but failed to moderate any of the paths between the PMT variables and behavior. Response efficacy and self-efficacy were the only variables that showed significant paths with behavior. All other paths were found to be non-significant. The results suggest that in the behavior of visiting only verified websites, habit was a strong determinant of behavior along with response efficacy and self-efficacy.

Implications For Research

This dissertation contributes to the field of IS, especially information security by investigating the role of habit in information security behaviors. Habit theory, which has been extensively investigated in the psychology discipline, has not received much attention in the IS discipline and has received even less attention in the domain of information security. The findings of this dissertation demonstrate that habit plays a significant role in the performance of information security behaviors and provide support of that notion with results from an investigation of three secure behaviors.

To test the role of habit in the context of information security, we drew from the theoretical perspectives of a well-established and highly validated theory in information security, which is the Protection Motivation Theory (PMT). PMT has been utilized by many cross-sectional information security studies. However, most of these studies rely on the assumption that behavioral intention is the driving factor of actual behavior. Due to the theoretical background of the correlations between intentions and actual behavior and due to the challenges of collecting data on actual behavior, most researchers are content

المنارة للاستشارات
www.manaraa.com

to measure behavioral intentions as a proxy for actual behavior. This perfectly aligns with the suggestions of TRA and TPB. Behavioral intentions may be the driving force of behavior in the initial stages of performing a behavior. However, these studies fail to identify that the influence of behavioral intentions as the driving force of behavior starts to diminish over time, and most behaviors become habituated. Subjects of a research study may or may not have formed habits related to the behavior that is tested. However, by failing to capture the existence of habit during cross-sectional studies, prior studies may have left out an important antecedent that may have increased the predictive ability of their research model. More importantly, they have failed to test the role of habit in information security behaviors.

This dissertation is not the first attempt to investigate the role of habit in information security. Several information security research studies have clearly identified habit as a major factor that drives secure behaviors, but only a few of them have empirically tested it. Moody and Siponen (2013), Pahnila et al. (2007), Siponen et al. (2010) and Vance et al. (2012) have empirically tested the role of habit in information security behaviors. However, most of them hypothesized that habit will directly influence behavioral intentions, which is in contrast to the widely accepted definition of habit, as automatic behavior that requires little or no cognitive effort. This study overcame this limitation by modeling habit as a direct influence of actual behavior and a moderator of the intention-behavior relationship, similar to Limayem et al. (2007). Previous studies by Pahnila et al. (2007) and Vance et al. (2012), which explored habit in an information security context, measured habit through reflective scales. While the reflective scales they utilized to measure habit are validated and heavily tested, they fail to capture the

المنارة للاستشارات
www.manaraa.com

multi-dimensional aspects of habit. This study measured habit with a first-order reflective, second-order formative construct, therefore, capturing the multiple dimensions of habit.

The findings of this dissertation provide numerous contributions to IS theory. First, the findings of this study confirm the significant relationship between behavioral intention and actual behavior in the context of information security. While the intention-behavior relationship has been tested in many research studies, only a few information security studies have tested that relationship (Liang and Xue 2010; Workman et al. 2008). This study measured secure behavior through a self-reported scale. Measurement of actual behavior using self-reported scales has been criticized by scholars. However, due to challenges in measuring actual behavior, self-reported scales are gaining acceptance in IS research. This study investigated the intention-behavior relationship in three secure behaviors and found consistent findings where behavioral intentions significantly influenced self-reported actual behavior in all three behaviors examined. These findings should encourage researchers to measure actual behavior with self-reported scales since it provides an opportunity to increase the predictive ability of the research model. It also provides the opportunity to test other interaction and moderation effects of many variables on actual behavior, which otherwise would not have been possible.

Second, the findings of this study provide strong empirical evidence to illustrate the importance of habit in information security behaviors. In all the three behaviors examined, habit significantly influenced secure behavior directly. The inclusion of the habit variable as an antecedent of secure behavior increased the variance explained by the secure behavior significantly in all three behaviors, demonstrating the importance of

www.manaraa.com

habit. This also shows that previous information security studies have failed to capture this important aspect of habit in their research studies. If they measured habit, it could have led to richer findings. The importance of habit in information security behaviors is further highlighted by the investigation of the moderation effects. In all three behaviors examined in this study, habit was found to moderate the intention-behavior relationship significantly. The values of the effect sizes in R-square difference tests suggest that all three behaviors have a medium effect size value for the moderation effect. This finding itself is a significant contribution to information security research. Prior to this study, information security scholars have not considered the moderating effect of habit on the intention-behavior relationship (Moody and Siponen 2013; Pahnila et al. 2007; Siponen et al. 2010; Vance et al. 2012). Previous studies simply assumed that behavioral intentions will continue to be the driving force of behavior regardless of the repetitive or routine nature of the performance of that behavior. Findings of this study would provide an opportunity for information security researchers to re-evaluate their views on the intention-behavior relationship in an information security context. As discussed later on this chapter, a longitudinal study would provide better evidence on how the influence of intentions on actual behavior diminishes over time.

Third, this study contributes to information security research by adopting a first-order reflective and second-order formative habit construct in the context of information security. The first-order reflective dimensions of habit are formed of 4 items each and this study evaluated the reliability, validity and loadings of those dimensions on three different secure behaviors. These validated items can be potentially adopted by future

المنارة للاستشارات
www.manaraa.com

researchers who are interested in examining the role of habit on other secure behaviors and want to capture the multidimensional aspect of habit.

Fourth, a list of 49 secure behaviors was developed after a rigorous review of academic literature and practitioner articles. While some behaviors of this list were adopted from Posey et al. (2013), the list of 49 secure behaviors was subjected to a subject-matter expert panel and an employee panel who were asked to rate each behavior to the degree they perceived it to be habitual. Appendix B, table B.5 illustrates the results of the expert and employee panel surveys, which provide the percentage of panelists who rated each behavior to be habitual. Three of those behaviors were selected for this study. However, the list of behaviors and their habit strength as perceived by the panelists provide future researchers with a source to select the secure behaviors they need to test for the role of habit.

Finally, PMT was extended with the inclusion of habit in the research model. PMT was extended with habit by Vance et al. (2012), but this study provides an alternate method to extend PMT with habit while accounting for the moderating effects of habit and capturing the different dimensions of habit with a formative scale. Investigation of three secure behaviors that has not been tested before is also a contribution to information security research. The findings of these three studies can be utilized to extend our knowledge of secure behaviors and PMT.

Implications for Practice

Organizations continue to face dynamic threats to the security of their information systems on a daily basis. Most of these organizations have created technical controls to deter these threats and have implemented information security policies that are mandated

المنارة للاستشارات
www.manaraa.com

to all employees. However, these controls and security policies are only effective to the extent that employees and others follow them. This dissertation makes a contribution to practice by providing evidence of the role habit plays in information security behaviors and explaining how it can be utilized to the advantage of organizations to strengthen their information security practices.

The results of this study provide strong support to the existence of habit as a major factor that influences the performance of secure behavior. Most employees perform a routine set of tasks on a daily basis and some of these tasks are likely to be habituated over time. If organizations can make their employees perform secure behaviors habitually, it will reduce the need for security policies or negative sanctions for non-compliance. The first step in this process is to identify secure behaviors that are habitual. As it was discussed previously in Chapter III, not all behaviors are habitual. Thus, it is important to understand habitual secure behaviors. This dissertation provides a solid foundation to organizations in identifying habitual secure behaviors. A list of 49 secure behaviors was ranked by subject-matter experts and a panel of employees to the degree to which they perceived those behaviors to be habitual. Some behaviors were ranked highly by both the expert panel and employee panel while some behaviors were perceived differently by the two panels to the degree they thought the behaviors were habitual. Organizations can examine this list to get a general idea about which secure behaviors their employees may perform habitually. Therefore, this dissertation contributes to the practice by extending the understanding of habitual secure behaviors.

This dissertation also aids the practice by identifying that habits can be positive or negative. Positive habits are the performance of recommended secure behaviors

المنارة للاستشارات
www.manaraa.com

habitually in compliance with the organizational security policies. While organizations would want their employees to comply with the security policies, they would strive to make their employees perform compliant behavior habitually. Habituation of secure behaviors by employees provides organizations with two main benefits. First, it will provide them with peace of mind since employees are less likely to neglect performance of secure behavior (e.g., locking their computer when leaving it unattended) since the behaviors happens automatically (Oulasvirta et al. 2012; Plamondon 2011; Vandermeer 2006). Second, it will provide organizations the opportunity to have a relaxed security policy, which increases employee satisfaction (Plamondon 2011). Negative habits are non-compliant behavior that is performed habitually by employees. Negative habits are highly undesirable and organizations should quickly identify any negative habits and take immediate steps to curtail them. While this dissertation focused solely on positive habits of secure behaviors, it provides opportunities to organizations to identify possible negative habits of employees.

Following the identification of possible secure behaviors that can be habituated, organizations should find ways to influence their employees to perform these behaviors habitually. There are several methods employees can deploy to foster positive habits (Plamondon 2011). One of the methods is through enforced security policies. When the performance of certain secure behavior is mandated, it will force employees to perform these behaviors routinely. Eventually, employees will learn to associate environmental cues with these secure behaviors and perform these secure behaviors regardless of the security policies. Another method to foster positive habit is through security education, training and awareness (SETA) programs. SETA programs can be effective solutions to

www.manaraa.com

form positive habits and break negative habits of employees through frequently administered security communications such as pop-up messages, sidebar in a newsletter or post-it notes with encouragement to comply with security policies. These may eventually become environmental cues that trigger the performance of secure behavior automatically. For example, a post-it note that asks the question “did you lock your computer?” will trigger an employee who is about to leave the workspace to lock his or her computer automatically.

It was not possible to analyze the formation of habit as a part of this study because the data are cross-sectional and measurements overtime are required to study the evolution of habits. However, understanding of habit formation and habitual secure behaviors is critical in certain contexts such as the healthcare sector. The findings of this study can be applied in the healthcare sector to test if the same behaviors are performed habitually by employees in the healthcare sector. The healthcare sector has increased the need for stringent information security procedures with the adoption of digital patient records and other technology related tools (Appari and Johnson 2010; Warkentin, Johnston, and Shropshire 2011). Many reports of privacy and data breaches in the healthcare sector provide the importance of enforced security policies that require employees to perform secure behaviors.

All three behaviors investigated in this study can be related to recommended secure behaviors performed by employees in the healthcare sector. Healthcare employees are likely to have access to private patient data (Warkentin, Johnston, and Shropshire 2011), thus they should definitely lock their computer when the leave it unattended to prevent an unauthorized user gaining access to private patient data. Healthcare employees

المنارة للاستشارات
www.manaraa.com

are also likely to communicate with their superiors and colleagues through email and these emails may contain private patient data. Therefore, it is important that employees verify the email addresses of the recipients before sending email because if an unintended recipient receives an email with private patient data, it would be a severe problem. Visiting unknown websites at the workplace poses the threat of malware infection that may expose the computer access, information stored on the computer and the network to outsiders. In the case of a computer in the workplace of a healthcare employee, this poses a huge threat. Therefore, employees should be careful only to visit verified websites and avoid clicking web-links that are suspicious. It is clear that the three behaviors tested in this dissertation are highly applicable to the healthcare sector. The results indicate that habit plays a major role in the secure behaviors being performed. Superiors of the healthcare industry can utilize these findings to foster habits of secure behaviors in their employees.

The findings of this study related to the direct paths between PMT variables and behavioral intention will be beneficial to practice as well. The results of the lock PC behavior suggest that high perceptions of threat severity and vulnerability will influence individuals to form intentions to lock their computer when leaving it unattended. Organizations can use this information to educate their employees about the consequences of an unauthorized user accessing their computer if they leave it unattended without locking it and to educate them about the possibility of someone else accessing their computer since most of them work in open workspaces or cubicles. Employees can also be educated in the effectiveness of locking their computers to protect them from unauthorized access and easy ways to lock their computers. Similarly, employees can be

المنارة للاستشارات
www.manaraa.com

educated about the threat severity and vulnerability of the other two behaviors tested in this study along with the effectiveness and the ease of performing the recommended behavior.

Limitations

This study has several limitations, as do all research studies. The limitations of this study are discussed in this section. It is not feasible to remove all limitations; however, we are hopeful that these limitations will lead to opportunities for future research where they can be addressed.

One of the limitations of this study is that it was conducted in a cross-sectional manner. As discussed in Chapter II, habit is a process where individuals, to achieve a certain goal, repetitively and successfully perform a certain behavior, until it becomes habitual. Habits become stronger overtime and it is a gradual process. In extreme situations, certain habitual behaviors may be performed with no cognitive effort (Triandis 1980). The time it takes and other factors that lead to stronger habits, such as the success rate, and environmental cues will vary among individuals, resulting in varying levels of habit strength among different individuals. Certain scholars posit that a minute level of habit will be generated the first time a certain behavior is performed, and every time the same behavior is repeated, the strength of habit increases (Ouellette and Wood 1998). However, other scholars refute this argument and posit that habits are born under different circumstances for different individuals (Verplanken and Orbell 2003; Verplanken 2006). There is a widely accepted notion of habit: Behaviors when they are performed initially will be cognitive and will agree with the TPB and TRA, where behavioral intentions are created and lead to actual behavior. However, certain behaviors

المنارة للاستشارات
www.manaraa.com

may be performed repetitively and successfully in order to achieve certain goals, where individuals may associate certain environmental cues with the performance of these behaviors. When these cues are encountered, the behaviors are performed automatically or with very little cognitive effort, which is called habitual performance of the behavior.

The gradual strengthening of habit makes it a strong contender for longitudinal studies. First, the initial influence of behavioral intentions on actual behavior can be examined. At this point, habits should be non-existent or should have little influence on actual behavior. If the behavior is habitual in nature, habits will develop over time strengthening the influence of habit on actual behavior while the influence of behavioral intentions on actual behaviors reduces as habit develops. A longitudinal study would enable researchers to collect data at several points of time and examine how the strength of habit develops over time as well as the significance of behavioral intentions or cognitive process diminishes. Collecting data in a cross-sectional manner such as it was done in this study, reduces the ability of the researchers to analyze how habits materialize and gain in strength over-time. However, longitudinal studies are not easy to conduct (Venkatesh and Davis 2000) since this type of study requires access to the same sample and data collection over time such as months or years. These difficulties may explain why most of the studies that have investigated the role of habit in IS have been cross-sectional.

The data for this study was collected from respondents from multiple organizations. Although this can be considered an advantage due to greater generalizability (Compeau et al. 2012), it also introduces some limitations. Collecting data from multiple companies such as it was done in this study, may introduce some

المنارة للاستشارات
www.manaraa.com

biases to the collected data. The biases are related to the different factors that the respondents are exposed to in their organization environment. For example, different organizations may have different organizational cultures. Certain companies may have a robust security policy and stringent enforcement of that policy through negative sanctions. Respondents who are employed in these types of companies are likely to follow security policies more carefully and will have a higher likelihood to perform recommended secure behaviors (e.g., lock the computer when leaving it unattended). They are also more likely to perform these behaviors habitually due to the repetitive and successful nature of the behaviors that are triggered by environmental cues such as warnings or notices of sanctions for those who do not comply with security policies. Conversely, respondents of companies that have implemented relaxed security policies are less likely to form habits to perform secure behaviors. These factors such as organizational culture, information security policy enforcement and sanctions involved for non-compliance, were not taken into account in this study; therefore, could not be controlled. However, the type of industry, which the respondents were employed, was not found to be a significant factor during the data analysis.

All the data of this study were collected with self-reported scales utilizing an online survey, which can be considered a limitation of this study. Although survey methodology is commonly used in IS research and other disciplines, it is also criticized for its limitations and biases. It is recommended researchers measure actual behavior and investigating behavioral intentions as a proxy of actual behavior has been criticized (Lee 2011). However, measuring actual secure behavior, such as accessing computer logs of computer usage, is very challenging and in most cases impossible (Crossler et al. 2013;

المنارة للاستشارات
www.manaraa.com

Warkentin et al. 2012). Because of these challenges, researchers have measured actual behavior through self-reported scales, which provides researchers with the ability to test relationships such as intention-behavior relationship. Only a few research studies have collected actual secure behavior such as password changes, security patch updates and backups by accessing computer logs (Lee 2011; Workman et al. 2008) while most researchers have measured only behavioral intention or measured actual behaviors with self-reported scales.

The data for the study were collected through Amazon Mechanical Turk (AMT), which is a popular crowdsourcing website. The data collected were high quality and reliable. However, rewarding the respondents for completing surveys may bias the responses since they are motivated to earn the reward. Therefore, they may only provide formidable responses resulting in a lower response spread. The very low reward given for each response (20 cents) may also have encouraged respondents to complete the survey quickly, so that they can complete another task to earn more money. However, there was a good response spread in the data collected in the three studies conducted for this dissertation, but paid survey responses could still be considered a limitation of this study. There is also the possibility of the same respondent completing the same survey in order to earn more rewards. Although steps were taken to restrict an individual respondent from completing the same survey again, robust procedures do not exist in achieving this. The fact that AMT respondents have to visit a link hosted in Qualtrics to complete the survey, and having visit the AMT site again with a code to obtain the reward money, creates potential problems and loopholes.

المنارة للاستشارات
www.manaraa.com

One of the major constructs investigated in this study is habit. Prior studies have measured habit using frequency of past behavior, self-reports and response frequency measures. Past behavior and frequency of past behavior are the most frequently used methods to measure habits with the theoretical lens that for the development of habits, it requires a certain amount of repetition and practice. However some scholars conducting behavioral research argue that frequency and past behavior alone cannot constitute habit. In order to measure the automaticity of habit and to capture the whole habit domain, habit is measured in this study through a self-reported first-order reflective, second-order formative scale.

Self-reports have been the commonly used method to measure habit in the recent scholarly research. The self-reported habit index (SRHI), which was created by Verplanken and Orbell (2003), is one of the most commonly utilized scales to measure habit (Sniehotta and Presseau 2012). Limayem et al. (2007) and Polites and Karahanna (2012) developed self-reported scales to measure habit in the context of information systems. However, some critics are skeptical about measuring habit with self-reported scales and argue that these scales are not valid. Contrary to constructs used in behavioral models such as intention and attitude, which belong to conscious human cognition, habit is of an unconscious nature. Therefore, these scholars suggest that it may not be appropriate to ask people to report the strength of their habits, when an essential feature of habit is its unconscious character (Klockner and Matthies 2012). Justifying the use of self-reports to measure habits, two of the prominent researchers of habit, Verplanken and Orbell (2003, p.1316), suggest that “if measured appropriately, it is possible to have people reflect on their behavior in terms of the degree to which it is habitual.” Even

المنارة للاستشارات
www.manaraa.com

though habit is measured frequently using self-reported scales, measuring habit with only self-reported scales may still be considered as a limitation of this study.

Several potential constructs were not included in our research model in order to test a parsimonious model. This study tests the traditional PMT model with habit modeled as a direct influence of behavior and a moderator of the intention-behavior relationship. There are many possible antecedents of behavioral intention and actual behavior described in the literature we could have tested. However, the sheer number of possible antecedents makes it impractical to test all of them in our research study. Possible antecedents that could have been included in our research model will be discussed in the future research section.

Another limitation of this study is the study of only three behaviors, although many previous studies investigated antecedents of only one behavior. The three behaviors tested in this study were selected using a systematic 5-step procedure that began with a pool of 129 behaviors relevant to IS that could have been studied. 49 of these were identified to be reviewed by an expert panel and separately by employees for the extent to which habit was considered important in explaining each of the behaviors. Separately, the feasibility of accurately measuring each behavior was evaluated. Ten behaviors were identified that were feasible to measure and were rated as having high, medium to high, and medium dependence on habit. It was a deliberate choice to consider not just behaviors considered highly dependent on habit to increase the generalizability of the conclusions. Another expert panel identified the final three behaviors that were used in the pilot and main studies. This study considered three behaviors, which is an improvement upon the single behavior often studied in other research. Although these

للاستشارات المنارة
www.manaraa.com

three were carefully selected to represent high and medium relationship to habit, the study of other behaviors will be necessary to demonstrate the strength of habit in IS-related behaviors.

Another possible limitation of this study is its focus only on positive habits. In terms of information security and security policy compliance, behaviors performed by employees may be compliant or non-compliant(Bulgurcu et al. 2010; Herath and Rao 2009; Ifinedo 2012; Puhakainen and Siponen 2010; Vance et al. 2012; Warkentin, Johnston, and Shropshire. 2011). For example, an employee may frequently and automatically lock his or her computer every time he or she leaves the terminal unattended. This may demonstrate a habitual compliant behavior or a positive habit (Siponen et al. 2010). Another employee, even though the organizational policy states otherwise, may intentionally share his or her password to a secure system with a colleague (Siponen and Vance 2010). Continuously sharing of passwords, however, may become a habitual (automatic) non-compliant behavior or a negative habit. This study only focused on positive habits. However, many behaviors performed by employees in the workplace may be negative habits that affect the information security of an organization.

Future Research

The findings of this dissertation provide valuable contributions to both IS theory and practice. This study is also one of the few studies that explored the role of habit in an information security context. However, there are many possible areas where new research studies can address the limitations of this dissertation and/or expand on the findings of

www.manaraa.com

this study in order to better understand the role of habit in information security. Possible future research ideas are discussed in this section.

An important direction for future research investigating the role of habit in information security is to measure habit in a longitudinal manner instead of cross-sectional. As mentioned in the limitations section, by measuring habit in a cross-sectional manner such as it was done on this dissertation and most of the scholarly articles exploring habit, the habit formation process is ignored. Therefore, important antecedents related to habit formation cannot be captured until the study is conducted in a longitudinal manner. The formation of habit is a process where individuals repetitively and successfully perform a certain behavior to achieve a certain goal. Eventually, this behavior will be performed automatically whenever a certain situation is encountered or faced with an environmental cue, making the behavior habitual. Habits are formed gradually, making it highly applicable for a longitudinal study where different levels of habit strength can be measured at different stages of time. While intentions may play a key role in the performance of actual behavior in initial stages of performing a behavior, when the same behavior is performed routinely, the decision-making process and intentions change, and the influence of intentions on behavior decreases (Kim and Malhotra 2005; Venkatesh et al. 2000). In a five month longitudinal study on technology adoption, Venkatesh et al. (2000) found that actual usage of IS was heavily influenced by intentions in the initial stage (t=1) and identified a significant decrease of intentions on actual behavior as time progressed, which they attributed to the behaviors becoming "habituated." Similarly, future research studies should conduct longitudinal studies to understand the role of habit on information security behaviors where the initial

المنارة للاستشارات
www.manaraa.com

significance of intentions on the actual secure behavior, and the decrease of the cognitive decision making process can be examined over time.

However, it will be challenging to measure the habitual performance of a secure behavior in a longitudinal manner for several reasons. First, it would be difficult to identify when a respondent initiates the performance of a secure behavior. Second, it would be difficult to gain access to actual data such as computer logs to identify if a certain behavior was performed (e.g., logging off the computer). Finally, it would be difficult to keep track of the secure behavior performed by the respondents for a long period of time (e.g., months, years) and also to identify if the behaviors were performed automatically, when triggered by environmental cues. If these challenges can be overcome, a longitudinal study to investigate the role of habit in information security behaviors can be conducted in the future. If it is not practical to conduct a longitudinal study to investigate habit in an information security context, cross-sectional studies would still provide ample opportunities for researchers to investigate different behaviors and the influence of habit on the automatic performance of those behaviors.

We measured the survey instrument from respondents who are employed in multiple organizations across different industries. This was identified as a possible limitation previously due to the different organizational cultures that may promote different security policies and different levels of required compliance and sanctions. While respondents from multiple organizations may provide more generalizable data (Compeau et al. 2012), future studies should address some of the limitations of this study with regards to the sample. First, future studies should focus on collecting data from multiple organizations, which increases generalizability, but should take rigorous steps to

المنارة للاستشارات
www.manaraa.com

control for variables such as organizational culture differences, existence of security policies, security policy enforcement, positive or negative sanctions involved with compliant and non-compliant behavior. These controls will take into account the biases that may be introduced to the data due to different organizational factors. Second, future research should also conduct studies focusing on one organization for each study. By focusing only on one organization, any biases of data collection from multiple organizations can be avoided. Researchers can also focus more on specific security policies or secure behaviors that are unique to the organization that is on focus. While gender as a control variable did not have any influence in our study, future research should continue to test the influence of gender and how it affects the strength of habit in the context of information security behaviors.

Future research studies should collect data from multiple sources if possible. This dissertation collected data only through Amazon Mechanical Turk. While the data did not have any significant issues, data can be collected through different panel providers to provide more generalizability and also to reduce any possible biases of respondents that belong to a certain panel provider. There are several reputable survey panels available through companies such as Qualtrics, Empanel and Survey Monkey. These panels have access to respondents from different demographics and different organizations and the incentives or rewards provided to the respondents for completing a survey are different too. However, researchers may face the risk of collecting data from the same respondent completing the same survey if they are recruited by several panel providers. Due to the sheer number of members in each of these survey panels, the probability of a situation

المنارة للاستشارات
www.manaraa.com

like that happening would be low. In the same vein, it will be desirable that future studies collect from other sources than just survey panels.

Data can be collected from students, which is one of the most common sources of data for research studies. However, researchers should be careful in collecting data from students related to information security behaviors and their habits, since students have shown little concerns about the security and privacy of information that belong to them or the academic organizations. Certain secure behaviors identified in this study such as locking the PC when leaving it unattended will not be applicable to be tested with student data. Collecting data related to habitual secure behavior will provide insights into the factors that form good and bad habits among students, which will be beneficial to academic institutions and their IT services departments to enforce policies and strengthen information security. Student data will also provide researchers with the ability to compare if the factors that contribute to the formation of habit in secure behaviors are similar or different between students and organizational computer users.

Future research studies can expand the findings of this study by collecting data in different contexts as well. While, a comparison of data from organizational users with students can be beneficial, a better comparison would be to compare organizational users with home users. Organizational respondents usually perform secure behaviors because they need to protect sensitive information related to their organization and because they are required to do so by the enforced security policies. Therefore, the habit strength of these behaviors may be influenced by different factors related to the organization. In a home setting, any secure behaviors that individuals perform are done so completely voluntarily. Therefore, researchers can collect data from both home users and

المنارة للاستشارات
www.manaraa.com

organizational users for comparison purposes and to understand if differences exist on factors that influence the formation of habit in different settings. Data can also be collected from respondents (students, organizational users and home users) without any incentives or rewards. This would alleviate any potential biases introduced by the offers of incentives for completing surveys. Multi-cultural studies can also be conducted to test if differences exist among habit formation and habit strength among individuals from different cultures and countries.

This dissertation focuses only on habitual behaviors related to information security, but habit is prevalent in many behaviors that individuals perform on a daily basis. Researchers suggest that more than 40 percent of our daily behaviors are habitual (Duhigg 2012; Neal et al. 2006). Future research can study if differences exist in the factors that influence the formation of habit related to information security behaviors, IS behaviors and other daily performed behaviors. Differences that exist in the environmental cues that trigger habitual behavior and the duration it takes to form habits between daily habits and information security habits can be examined through these studies as well. Researchers will also be able to identify if habitual security behaviors are formed in a unique manner or if they are formed similar to habits of daily behaviors that are performed on a daily basis.

One of the major issues with investigating habit in academic research is the operationalization of habit. Previous studies have measured habit through frequency of past behavior and response frequency (RF) measures. The most frequently used method is using self-reported formative and reflective scales to measure habit with self-reported habit index (SRHI) being the most popular measure (Sniehotta and Presseau 2012).

المنارة للاستشارات
www.manaraa.com

Critics have questioned measuring habit through self-reported scales because by definition habit is automatic in nature and uses less cognitive resources. They argue that if habitual behaviors are performed automatically by individuals without awareness of why they performed the behavior, survey items will not be able to capture the strength of habit or if the individuals performed the behavior habitually. Although Verplanken and Orbell (2003) argue that “if appropriately measured” habit can be measured through self-reports, future studies should explore other methods to measure habit.

One of the possible methods to measure habit is through an experiment. During experimental studies, the behavior and the habit will be measured in a controlled and unrealistic environment that would reduce realism. However, a controlled environment would be more appealing for researchers where they can control for many factors and focus specifically on how habits are formed. For example, a simulated experimental environment can be created where the subjects are required to perform information security related tasks on a routine basis. Researchers can identify factors that lead to habit formation and even manipulate certain factors to see if any significant differences manifest with the habit formation process. An experiment will also be beneficial to a longitudinal study, where researchers can have access to the same set of respondents over a longer period of time.

Another possible method to measure habit is through neuro-physiological methods such as Electroencephalogram (EEG) and functional Magnetic Resonance Imaging (fMRI). EEG equipment from companies such as EMOTIV are readily available and affordable, which provides researchers with better opportunities to measure the neurological aspects of habit. FMRI is a more robust method to measure habit, but it is

www.manaraa.com

not economically feasible for most researchers to conduct research using that method. Both EEG and fRMI have been suggested by Janes et al. (2009) and Dimoka (2012) as possible methods to measure habit. Both these methods examine brain waves of subjects when they are performing certain tasks. As mentioned previously, decision making processes utilize the prefrontal cortex of the brain while routine or automatic behaviors utilize the basal ganglia of the brain. EEG and fMRI methods will be able to identify which part of the brain functions when a certain behavior is performed and researchers will be able to identify if the basal ganglia or the prefrontal cortex is activated when a certain behavior is performed. Depending on the area of the brain that is active, researchers will be able to understand if a certain behavior is performed habitually or intentionally. These neuro-physiological methods will also aid researchers in longitudinal studies.

The experiments and neuro-physiological methods to measure habits are highly beneficial to researchers in measuring habit. However, these methods may not always be practical or feasible for most researchers to measure habit. These methods also have limitations such as lack of realism. Behaviors are habituated when they are performed successfully and repetitively in a stable context. However, when habit is measured with either an experiment or a neuro-physiological method, the controlled and unrealistic environment (Dennis and Valacich 2001), removes the stable context required for habits to be performed. Therefore, researchers should not completely avoid using self-reported scales to measure habit, which is considered to be the most appropriate method.

One of the areas that future research can focus is developing a more robust self-report scale to measure habit. Currently, there are several validated self-report scales.

المنارة للاستشارات
www.manaraa.com

Self-report habit index (SRHI) by Verplanken and Orbell (2003), is a 12-item reflective scale, which is frequently utilized by researchers. Although this scale is measured reflectively, careful examination of the items suggest a formative or multi-dimensional structure that taps into dimensions such as awareness, mental efficiency, uncontrollability, frequency and self-identity. Although empirical results from the studies that measured habit with SRHI suggest of a reflective structure of the scale, the inclusion of items related to frequency and self-identify to measure habit has been questioned (Sniehotta and Presseau 2012). Limayem et al. (2007) developed and validated a 3-item reflective habit scale to measure habit in the context of IS continuance. While this scale is a parsimonious way of measuring habit, it fails to capture the multi-dimensional aspects such as lack of awareness, uncontrollability and mental efficiency.

Polites and Karahanna (2012) developed a formative scale for habit that captures the multi-dimensional aspects of habit. Their scale is one of the more robust scales developed to capture habit, where three first-order reflective constructs: lack of awareness, uncontrollability and mental efficiency form the three dimensions of the second-order formative habit construct. Their scale was validated and tested in the context of new information system acceptance. However, they found that the dimension of awareness was not a significant factor in forming the second-order habit construct. Similarly, the findings of this dissertation indicate that mental efficiency was not a significant factor in forming habit when the behaviors investigated were locking the PC when leaving it unattended and visiting only verified websites. We also found that uncontrollability was not a significant factor forming the habit construct when the behavior tested was verifying email recipients before sending emails. While this may be

المنارة للاستشارات
www.manaraa.com

due to different contexts of the investigations, this may also be due to certain limitations of the scale developed by Polites and Karahanna (2012). Future studies should re-validate their scale in many contexts in IS and other disciplines to confirm its reliability and validity. In terms of future information security research, their scale should be revalidated in different secure behaviors to ensure its applicability in an information security context. It is appropriate that future research should also focus on developing a self-reported habit scale, specifically for information security context since the current scales by Limayem et al. (2007) and Polites and Karahanna (2012) were developed to test habit in the context of IS continuance or adoption and post-adoption of technology.

Data collected though self-reported habit measures can also be supplemented with other objective measures such as experiment results, fMRI or EEG results. Straub et al. (1995) suggests that limitations of self-reported scales can be reduced by supplementing the findings with objective data. This is especially critical when actual behavior is measured through self-reported scales, where social desirability is very likely to bias the data. For example, survey items asking about actual behavior about their behavior related to locking the PC when they leave it unattended, it is highly possible that most respondents will give a favorable answer. If the survey data can be supplemented with actual data logs from the computer to check the locking activity of each respondent, it will lead to stronger findings. Similarly, if the results of the self-reported habit scale can be supplemented with data from an experiment, fMRI or EEG, it will add more reliability to the findings. Using objective measures will make it easier for researchers to identify which behaviors are actually habitual and which are not, instead of solely relying on self-reported measures.

المنارة للاستشارات
www.manaraa.com

Another appropriate direction for future research is conducting a qualitative study to investigate different aspects of habit. A qualitative study is appropriate to study habit in the context of information security since our understanding of how habit influences secure behavior is in its infancy stage. An exploratory study would provide better insights into identifying factors that influence habit formation and identify which secure behaviors are habitual and which are not. Siponen et al. (2010) used a qualitative approach to investigate the role of habit in information security behaviors. Through several interviews, they identified that several secure behaviors were influenced by habit. However, their qualitative study can be significantly improved by conducting a thorough study involving a diverse pool of subjects from different organizations, industries and countries. A future qualitative study should also involve the investigation of areas such as habit formation, factors that contribute to changes in habit strength, breaking habits, different dimensions that form habit and differences of positive and negative habits. The findings of the qualitative study can be followed by survey, experiment, or neuro-physiological methods to conduct a mixed-method research study. This merging of qualitative and quantitative data to develop a deeper understanding of a phenomenon or a research problem is called 'triangulation' (Mingers 1997, 2001; Venkatesh et al. 2013). There have been calls for mixed-method studies in IS research since only less than 5 percent of the empirical studies published between 2001 to 2007 in the AIS Basket of Journals utilized mixed-methods (Venkatesh et al. 2013). Therefore, a great opportunity exists to conduct mixed-method research studies to gain deep insights to habit while contributing significantly to IS research.

المنارة للاستشارات
www.manaraa.com

The dissertation study focused solely on the role of habit in information security behaviors utilizing PMT. However, there were several potential antecedents that were not tested in our research model for the sake of parsimony. General Deterrence Theory (GDT) constructs such as sanction severity, sanction certainty and sanction celerity are possible constructs that should be tested in the future along with habit. Although Pahnila et al. (2007) investigated sanctions and habit as antecedents of behavioral intentions, it would be appropriate to test the influence of habit on actual behavior in the presence of constructs from the deterrence theory. Siponen et al. (2010) suggested that sanctions or other deterrence factors may play a role in the habit formation. However, they did not provide any statistical evidence to support it. Enforced information security policies in organizations and negative sanctions for non-compliance are highly likely to persuade employees to perform recommended secure behaviors on a routine basis. Although initial performance of these behaviors may be performed intentionally due to the security policies that are in place, repetitive performance of the same secure behavior routinely is likely to make it habitual. General Deterrence Theory (GDT) has been tested extensively and sanction severity, sanction certainty and sanction celerity have been found to be antecedents of behavioral intention to comply with security policies (D'Arcy and Devaraj 2012; D'Arcy et al. 2009; Herath and Rao 2009; Hovav and D'Arcy 2012; Siponen and Vance 2010). As it was tested with the PMT variables in this study, habit may also be tested as a moderator of the relationships between the deterrence variables and behavioral intention. However, further research is needed to test these views with the support of empirical results.

www.manaraa.com

Social influence is another variable that warrants an investigation in future studies that test the role of habit in information security behaviors. Social influence is the willingness of an individual to perform a behavior to the degree to which he or she perceives that those whose opinions matter support the performance of that behavior (Venkatesh et al. 2003). Different variations of social influence have also been tested as subjective norms (Herath and Rao 2009) and normative beliefs (Bulgurcu et al. 2010). Johnston and Warkentin (2010) tested the relationship between social influence and behavioral intention to perform secure behaviors and found that social influence was a significant factor that influenced intentions. Similar to the deterrence variables, social influence may be a significant factor that will contribute to the development of habit. If an individual continues to perform a secure behavior due to the views of the people that matter to him or her, he or she is likely to form habitual patterns related to performing those behaviors. This provides an opportunity for future research studies to test the impact of social influence on behavioral intentions and actual behavior in the presence of PMT, deterrence factors and habit.

As discussed previously, deterrence factors related to sanctions may lead to the formation of habit. It is important to note that sanctions can be positive or negative. Positive organizational sanctions or rewards may include pay raises, performance bonuses, and praise or recognition at work. Negative organizational sanctions or punishment may include reprimands, demotions, termination of employment or public ridicule. Both positive and negative sanctions may lead to the routine performance of secure behaviors that may cause the habituation of those behaviors. Future research studies could investigate if either of the two types of sanctions has a stronger influence in

المنارة للاستشارات
www.manaraa.com

habit formation of secure behavior performance, which would provide many benefits to organizations. They can use the findings to increase either positive or negative sanctions as long as employees perform the recommended secure behaviors in the workplace.

Future research can also examine the role of past behavior on behavioral intentions and actual behavior. There have been criticism for using past behavior as a proxy of habit (Ajzen and Fishbein 2000; Limayem et al. 2007). However, the influence of past behavior may be worth exploring further especially in a longitudinal study that investigates habit formation and performance of habitual behaviors. For example, researchers can examine if subjects were performing a secure behavior such as backing up their data in the past. If that is the case, they can explore the reasons for the past behavior. If the subjects have not been backing up their data and suddenly start backing up their data, researchers can examine the causes for the new behavior and the factors that triggered it (e.g., social influence, experience of data loss).

Researchers also need to understand the influence of habit in volitional and non-volitional acts related to information security. It is easy to regard positive secure behaviors as positive habits, but it is unclear whether an omission of performing a secure behavior can be habitual and can be called a negative habit. For example, if an individual does not lock their PC when they leave it unattended volitionally, and repeatedly fail to lock his or her PC, does that lead to habituation? Since the omission of locking the PC is performed purposely by the employee, it may involve more cognitive effort; therefore it may not be considered a habit. Future research needs to explore these conundrums in order to obtain a deeper understanding of the role of habit in information security behaviors.

المنارة للاستشارات
www.manaraa.com

Conclusion

This dissertation investigated the role of habit on three different information security behaviors. The data analysis confirmed that habit plays a major role in the performance of secure behaviors supporting the hypotheses. Habit demonstrated a significant direct effect on behavior as well as a negative moderating effect on the intention-behavior relationship. The findings of this study provide several contributions to the IS theory and practice as well as several future research directions.

المنارة للاستشارات
www.manaraa.com

REFERENCES

Aarts, H., and Dijksterhuis, A. 2000. "Habits as Knowledge Structures: Automaticity in Goal-Directed Behavior," *Journal of Personality and Social Psychology* (78:1), pp. 53–63.

Aarts, H., Paulussen, T., and Schaalma, H. 1997. "Physical Exercise Habit: On the Conceptualization Formation of Habitual Health Behaviours," *Health Education Research* (12:3), pp. 363–374.

Aarts, H., Verplanken, B., and Van Knippenberg, A. 1998. "Predicting Behavior from Actions in the Past: Repeated Decision Making or a Matter of Habit?," *Journal of Applied Social Psychology1* (28:15), pp. 1355–1374.

Abelson, R. P. 1981. "Psychological Status of the Script Concept," *American Psychologist* (36), pp. 715–729.

Abelson, R. P. 1985. "A Variance Explanation Paradox: When a Little is a Lot," *Psychological Bulletin* (97:1), pp. 129–133.

Abraham, S. C. S., Sheeran, P., Abrams, D., and Spears, R. 1994. "Exploring Teenagers' Adaptive and Maladaptive Thinking in Relation to the Threat of HIV Infection," *Psychology and Health* (9), pp. 253–272.

Adams, A., Sasse, M. A., and Lunt, P. 1997. "Making Passwords Secure and Usable," in *HCI 97- People and Computers XII*, pp. 1–20.

Ajzen, I. 1991. "The Theory of Planned Behavior," *Organizational Behavior and Human Decision Processes* (50:2), pp. 179–211.

Ajzen, I. 2002. "Residual Effects of Past on Later Behavior: Habituation and Reasoned Action Perspectives," *Personality and Social Psychology Review* (6), pp. 107–122.

Ajzen, I., and Fishbein, M. 2000. "Attitudes and the Attitude-behavior Relation: Reasoned and Automatic Processes," *European Review of Social Psychology* (11), pp. 1–33.

المنارة للاستشارات
www.manaraa.com

Anderson, C., and Agarwal, R. 2010. “Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions,” *MIS Quarterly* (34:3), pp. 613–643.

Appari, A., and Johnson, M. E. 2010. “Information Security and Privacy in Healthcare: Current State of Research,” *International Journal of Internet and Enterprise Management* (6:4), pp. 279–314.

Ashby, F. G., Turner, B. O., and Horvitz, J. C. 2010. “Cortical and Basal Ganglia Contributions to Habit Learning and Automaticity,” *Trends in Cognitive Sciences* (14:5), pp. 208–215.

Bagozzi, R. P. 1981. “Attitudes, Intentions and Behavior: A Test of Some Key Hypotheses,” *Journal of Personality and Social Psychology* (41:4), pp. 607–627.

Bagozzi, R. P., and Warshaw, P. R. 1990. “Trying to Consume,” *Journal of Consumer Research* (17:2), pp. 127–140.

Bandura, A. 1977. “Self-Efficacy: Towards a Unifying Theory of Behavioral Change,” *Psychological Review* (84:2), pp. 191–225.

Bandura, A., and Adams, N. E. 1977. “Analysis of Self-efficacy Theory of Behavioral Change,” *Cognitive Therapy and Research* (1), pp. 287–308.

Bargh, J. A. 1994. “The Four Horsemen of Automaticity: Awareness, Efficiency, Intention, and Control in Social Cognition,” in *Handbook of Social Cognition*, R. S. Wyer and T. K. Srull (eds.), Hillsdale, NJ, pp. 1–40.

Bargh, J. A. 2002. “Losing Consciousness: Automatic Influences on Consumer Judgment, Behavior, and Motivation,” *Journal of Consumer Research* (29:2), pp. 280–285.

Bargh, J. A., and Ferguson, M. J. 2000. “Beyond Behaviorism: On the Automaticity of Higher Mental Processes,” *Psychological Bulletin* (126:6), pp. 925–945.

Beccaria, C. 1770. *An Essay on Crimes and Punishments*, *Criminological Theory: Past to Present (Essential Readings)*, pp. 2–3.

Beck, L., and Ajzen, I. 1991. “Predicting Dishonest Actions Using the Theory of Planned Behavior,” *Journal of Research in Personality* (25:3), pp. 285–301.

Becker, G. S. 1968. “Crime and Punishment: And Economic Approach,” *The Journal of Political Economy* (76:2), pp. 169–217.

المنارة للاستشارات

www.manaraa.com

Bellman, S., Lohse, G. L., and Johnson, E. J. 1999. “Predictors of Online Buying Behavior,” *Communications of the ACM* (42:12), pp. 32–38.

Benbasat, I., and Barki, H. 2007. “Quo Vadis, TAM?,” *Journal of the Association for Information Systems* (8:4), pp. 211–218.

Bentham, J. 1781. *An Introduction to the Principles of Morals and Legislation*, *Jeremy Bentham's economic writings*, (Werner Stark, ed.), London, UK: George Allen and Unwin.

Bergeron, F., L., R., S., R., and Gara, M. F. 1995. “Determinants of EIS Use: Testing a Behavioral Model,” *Decision Support Systems* (14:2), pp. 131–146.

Berinsky, A. J., Huber, G. A., and Lenz, G. S. 2012. “Evaluating Online Labor Markets for Experimental Research: Amazon.com's Mechanical Turk,” *Political Analysis* (20), pp. 351–368.

Bhattacherjee, A. 2001. “Understanding Information Systems Continuance: An Expectation-Confirmation Model,” *MIS Quarterly* (25:3), pp. 351–370.

Bittar, C. 2000. “P&G's Monumental Repackaging Project,” *Brandweek* , pp. 40–52.

Bollen, K. A., and Lennox, R. 1991. “Conventional Wisdom on Measurement: A Structural Equation Perspective,” *Psychological Bulletin* (110:2), pp. 305–314.

Buhrmester, M., Kwang, T., and Samuel D. Gosling. 2011. “Amazon's Mechanical Turk: A New Source of Inexpensive, Yet High-Quality, Data?,” *Perspectives on Psychological Science* (6:1), pp. 3–5.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. 2010. “Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness,” *MIS Quarterly* (34:3), pp. 523–548.

Carver, C. S., and Scheier, M. F. 1982. “Control Theory: A Useful Conceptual Framework for Personality-Social, Clinical, and Health Psychology,” *Psychological Bulletin* (92:1), pp. 111–135.

Charng, H.-W., Piliavin, J. A., and Callero, P. L. 1988. “Role Identity and Reasoned Action in the Prediction of Repeated Behavior,” *Social Psychology Quarterly* (51:4), pp. 303–317.

Chen, X., and Halsey, P. 2009. “Reading to Learn on the Internet: Challenges, Solutions and Implications,” *American Journal of Educational Studies* (2:1), pp. 51–62.

المنارة للاستشارات

www.manaraa.com

Cheung, C. M. K., and Limayem, M. 2005. “The Role of Habit in Information Systems Continuance: Examining the Evolving Relationship between Intention and Usage,” in *Twenty-Sixth International Conference on Information Systems*, Las Vegas, NV, pp. 471–482.

Chin, W. W. 1998. “The Partial Least Squares Approach for Structural Equation Modeling,” in *Modern Methods for Business Research*, G. . Marcoulides (ed.), Mahwah, NJ: Lawrence Erlbaum, pp. 295–336.

Chin, W. W., Marcolin, B. L., and Newsted, P. R. 1996. “A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and Voice Mail Emotion/Adoption Study,” in *Proceedings of the 17th International Conference on Information Systems*, Cleveland, OH, pp. 21–41.

Chin, W. W., Marcolin, B. L., and Newsted, P. R. 2003. “A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-Mail Emotion/Adoption Study,” *Information Systems Research* (14:2), pp. 189–217.

Chiu, C.-M., Hsu, M.-H., Lai, H., and Chang, C.-M. 2012. “Re-Examining the Influence of Trust on Online Repeat Purchase Intention: The Moderating Role of Habit and its Antecedents,” *Decision Support Systems* (53:4), pp. 835–845.

Chunli, L., and Donghui, L. 2012. “Computer Network Security Issues and Countermeasures,” in *IEEE Symposium on Robotics and Applications*, pp. 328 – 331.

Cohen, J. 1988. *Statistical Power Analysis for the Behavioral Sciences*, Hillsdale, NJ: Lawrence Erlbaum Associates.

Compeau, D., Marcolin, B., Kelley, H., and Higgins, C. 2012. “Generalizability of Information Systems Research Using Student Subjects—A Reflection on Our Practices and Recommendations for Future Research,” *Information Systems Research* (23:4), pp. 1–17.

Conner, M., R., P., Sparks, P., James, R., and Shepherd, R. 2003. “Moderating Role of Attitudinal Ambivalence Within the Theory of Planned Behaviour,” *British Journal of Social Psychology* (42), pp. 75–94.

Cronbach, L. J. 1951. “Coefficient Alpha and the Internal Structure of Tests,” *Psychometrika* (16), pp. 297–334.

المنارة للاستشارات

www.manaraa.com

Crossler, R., and Belanger, F. 2012. "The Quest for Complete Security Protection: An Empirical Analysis of an Individual's 360 Degree Protection from File and Data Loss," in *AMCIS 2012 Proceedings*, .

Crossler, R. E. 2010. "Protection Motivation Theory: Understanding Determinants to Backing Up Personal Data," in *43rd Hawaii International Conference on System Sciences*, pp. 1–10.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. 2013. "Future Directions for Behavioral Information Security Research," *Computers & Security* (32), pp. 90–101.

D'Arcy, J., and Devaraj, S. 2012. "Employee Misuse of Information Technology Resources: Testing a Contemporary Deterrence Model," *Decision Sciences* (43:6), pp. 1091–1124.

D'Arcy, J., and Herath, T. 2011. "A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings," *European Journal of Information Systems* (20:6), pp. 643–658.

D'Arcy, J., Hovav, A., and Galletta, D. 2009. "User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach," *Information Systems Research* (20:1), pp. 79–98.

Davis, F. D. 1989. "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS Quarterly* (13:3), pp. 319–339.

Dennis, A. R., and Valacich, J. S. 2001. "Conducting Research in Information Systems," *Communications of AIS* (7:2), pp. 1–41.

Diamantopoulos, A., and Siguaw, J. A. 2006. "Formative Versus Reflective Indicators in Organizational Measure Development: A Comparison of Empirical Illustration," *British Journal of Management* (17), pp. 263–282.

Diamantopoulos, A., and Winklhofer, H. M. 2001. "Index Construction with Formative Indicators: An Alternative to Scale Development," *Journal of Marketing Research* (38), pp. 269–277.

Dimoka, A. 2012. "How to Conduct a Functional Magnetic Resonance (fMRI) Study in Social Science Research," *MIS Quarterly* (36:3), pp. 811–840.

Duhigg, C. 2012. *The Power of Habit: Why We Do What We Do in Life and Business*, Random House.

المنارة للاستشارات
www.manaraa.com

Dunnavant, S., and Childress, M. J. 2010. “A Sideways Approach to Data Security and Privacy Awareness,” in *Proceedings of the 38th Annual Fall Conference on SIGUCCS*, Norfolk, Virginia, pp. 195–198.

Edwards, J. R. 2003. “Construct Validation in Organizational Behavior Research,” in *Organizational Behavior: The State of the Science*, Mahwah, NJ: Lawrence Erlbaum Associates, pp. 327–371.

Etchells, M. 2008. “Exposed: Email’s Worst Habits,” *Engineering & Technology* (3:9), pp. 58–60.

Farn, K.-J., Lin, S.-K., and Fung, A. R.-W. 2004. “A Study on Information Security Management System Evaluation—Assets, Threat and Vulnerability,” *Computer Standards & Interfaces* (26), pp. 501–513.

Fishbein, M., and Ajzen, I. 1975. *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research.*, Reading, MA.: Addison-Wesley Publishing.

Florencio, D., and Herley, C. 2007. “A Large-Scale Study of Web Password Habits,” in *World Wide Web Conference*, pp. 657–665.

Floyd, D. L., Prentice-Dunn, S., and Rogers, R. W. 2000. “A Meta-Analysis of Research on Protection Motivation Theory,” *Journal of Applied Social Psychology* (30:2), pp. 407–429.

Fornell, C., and Larcker, D. F. 1981. “Evaluating Structural Equations with Unobservable Variables and Measurement Error,” *Journal of Marketing Research* (18:1), pp. 39–50.

Freud, S. 1915. “Repression,” in *Complete Psychological Works of Sigmund Freud*, London: Hogarth.

Frøkjær, E., and Hornbæk, K. 2002. “Metaphors of Human Thinking in HCI: Habit, Stream of Thought, Awareness, Utterance, and Knowing,” in *Proceedings of OzCHI*, .

Gardner, B. 2012. “Habit as Automaticity, not Frequency,” *The European Health Psychologist* (14:2), pp. 32–36.

Gardner, B., Bruijn, G.-J. de, and Lally, P. 2012. “Habit, Identity, and Repetitive Action: A Prospective Study of Binge-drinking in UK Students,” *British Journal of Health Psychology* (17:3), pp. 565–581.

Gefen, D. 2003. “TAM or Just Plain Habit: A Look at Experienced Online Shoppers,” *Journal of End User Computing* (15:3), pp. 1–13.

المنارة للاستشارات

www.manaraa.com

Gefen, D., and Straub, D. W. 2005. “Practical Guide to Factorial Validity using PLS-Graph: Tutorial and Annotated Example,” *Communications of the AIS* (16:25), pp. 91–109.

Gjelten, T. 2012. “‘Anonymous’ Hacking Group Threatens The Internet,” *NPR*, .

Goldman, D. 2012. “Super-virus Flame Raises the Cyberwar Stakes,” *CNN Money*, .

Graybiel, A. M. 2008. “Habits, Rituals, and the Evaluative Brain,” *Annual Review of Neuroscience* (31), pp. 359–387.

Guinea, A. O. de, and Markus, M. L. 2009. “Why Break the Habit of a Lifetime? Rethinking the roles of Intention, Habit, and Emotion in Continuing Information Technology Use,” *MIS Quarterly* (33:3), pp. 433–444.

Gurung, A., Luo, X., and Liao, Q. 2009. “Consumer Motivations in Taking Action Against Spyware: an Empirical Investigation,” *Information Management & Computer Security* (17:3), pp. 276–289.

Hair, J. F. J., Black, W. C., Babin, B. J., and Anderson, R. E. 2010. *Multivariate Data Analysis*, (7th ed.) Saddle River, NJ: Prentice Hall.

Herath, T., and Rao, H. R. 2009. “Protection Motivation and Deterrence: a Framework for Security Policy Compliance in Organisations,” *European Journal of Information Systems* (18:2), pp. 106–125.

Hovav, A., and D’Arcy, J. 2012. “Applying an Extended Model of Deterrence Across Cultures: An Investigation of Information Systems Misuse in the U.S. and South Korea,” *Information & Management* (20:1), pp. 79–98.

Hu, Q., Zhang, C., and Xu, Z. 2011. “How Can You Tell a Hacker from a Geek? Ask Whether He Spends More Time on Computer Games than Sports!,” in *DeWald Information Security Research Workshop*, Blacksburg, Virginia.

Ifinedo, P. 2012. “Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory,” *Computers & Security* (31:1), pp. 83–95.

James, W. 1890. *The principles of psychology*, (Vol. 1.) New York, NY: Holt.

James, W. 1899. *Talks to teachers on psychology--and to students on some of life’s ideals*, New York, NY: Metropolitan Books/Henry Holt, pp. 64–78.

المنارة للاستشارات

www.manaraa.com

Janes, A. C., Frederick, B., Richardt, S., Burbridge, C., Merlo-Pich, E., Renshaw, P. F., Evins, A. E., Fava, M., and Kaufman, M. J. 2009. “Brain fMRI Reactivity to Smoking-Related Images Before and During Extended Smoking Abstinence,” *Experimental and Clinical Psychopharmacology* (17:6), pp. 365–373.

Janis, I. L. 1967. “Effects of Fear Arousal on Attitude Change: Recent Developments in Theory and Experimental Research,” in *Advances in experimental social psychology*, L. Berkowitz (ed.), New York, NY: Academic Press, pp. 166–225.

Jarvis, C. B., Mackenzie, P. M., and Podsakoff., P. M. 2003. “A Critical Review of Construct Indicators and Measurement Model Misspecification in Marketing and Consumer Research,” *Journal of Consumer Research* (30:2), pp. 199–218.

Jasperson, J., Carter, P. E., and Zmud, R. W. 2005. “A Comprehensive Conceptualization Of Post-Adoptive Behaviors Associated With Information Technology Enabled Work Systems,” *MIS Quarterly* (29:3), pp. 525–557.

Johnston, A. C., and Warkentin, M. 2010. “Fear Appeals and Information Security Behaviors: An Empirical Study,” *MIS Quarterly* (34:3), pp. 549–566.

Karahanna, E., Straub, D. W., and Chervany, N. L. 1999. “Information Technology Adoption Across Time: A Cross-sectional Comparison of Pre-adoption and Post-adoption Beliefs,” *MIS Quarterly* (23:2), pp. 183–213.

Kaspersky. 2012. “Kaspersky Lab and ITU Research Reveals New Advanced Cyber Threat,” *Kaspersky Labs*, .

Khalifa, M., Limayem, M., and Liu, V. 2002. “Online Consumer Stickiness: A Longitudinal Study,” *Journal of Global Information Management* (10:3), pp. 1–14.

Kim, S. S., and Malhotra, N. K. 2005. “A Longitudinal Model of Continued IS Use: An Integrative View of Four Mechanisms Underlying Postadoption Phenomena,” *Management Science* (51:5), pp. 741–755.

Klockner, C. A., and Matthies, E. 2012. “Two Pieces of the Same Puzzle? Script-Based Car Choice Habits Between the Influence of Socialization and Past Behavior1,” *Journal of Applied Social Psychology* (42:4), pp. 793–821.

Landis, D., Triandis, H. C., and Adamopoulos, J. 1978. “Habit and Behavioral Intentions as Predictors of Social Behavior,” *Journal of Social Psychology* (106:2), pp. 227–237.

المنارة للاستشارات

www.manaraa.com

Lankton, N. K., McKnight, D. H., and Thatcher, J. B. 2012. “The Moderating Effects of Privacy Restrictiveness and Experience on Trusting Beliefs and Habit: An Empirical Test of Intention to Continue Using a Social Networking Website,” *IEEE Transactions on Engineering Management* (59:4), pp. 654 – 665.

LaRose, R., Rifon, N. J., and Enbody, R. 2008. “Promoting Personal Responsibility for Internet Safety,” *Communications of the ACM* (51:3), pp. 71–76.

Lee, Y. 2011. “Understanding Anti-plagiarism Software Adoption: An Extended Protection Motivation Theory Perspective,” *Decision Support Systems* (50:2), pp. 361–369.

Lee, Y., and Larsen, K. R. 2009. “Threat or Coping Appraisal: Determinants of SMB Executives‟ Decision to Adopt Anti-Malware Software,” *European Journal of Information Systems* (18:2), pp. 177–187.

Liang, H., Saraf, N., Hu, Q., and Xue, Y. 2007. “Assimilation of Enterprise Systems: The Effect Of Institutional Pressures And The Mediating Role Of Top Management,” *MIS Quarterly* (31:1), pp. 59–87.

Liang, H., and Xue, Y. 2009. “Avoidance Of Information Technology Threats: A Theoretical Perspective,” *MIS Quarterly* (33:1), pp. 71–90.

Liang, H., and Xue, Y. 2010. “Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective,” *Journal of the Association for Information Systems* (11:7), pp. 394–413.

Liao, C., Chen, J.-L., and Yen, D. C. 2007. “Theory of Planning Behavior (TPB) and Customer Satisfaction in the Continued Use of E-service: An Integrated Model,” *Computers in Human Behavior* (23:6), pp. 2804–2822.

Limayem, M., and Cheung, C. M. K. 2011. “Predicting the Continued Use of Internet-based Learning Technologies: The Role of Habit,” *Behaviour & Information Technology* (30:1), pp. 91–99.

Limayem, M., and Hirt, S. G. 2003. “Force of Habit and Information Systems Usage: Theory and Initial Validation,” *Journal of the Association for Information Systems* (4:3), pp. 65–97.

Limayem, M., Hirt, S. G., and Cheung, C. M. K. 2007. “How Habit Limits The Predictive Power of Intention: The Case of Information Systems Continuance,” *MIS Quarterly* (31:4), pp. 705–737.

المنارة للاستشارات

www.manaraa.com

Limayem, M., Hirt, S. G., and Chin, W. W. 2001. “Intention Does Not Always Matter: The Contingent Role of Habit on IT Usage Behavior,” in *9th European Conference on Information Systems*, pp. 274–286.

Loch, K. D., Carr, H. H., and Warkentin, M. E. 1992. “Threats to Information Systems: Today’s Reality, Yesterday's Understanding,” *MIS Quarterly* (16:2), pp. 173–186.

Louis, M. R., and Sutton, R. I. 1991. “Switching Cognitive Gears: From Habits of Mind to Active Thinking,” *Human Relations* (44:1), pp. 55–76.

Luo, X., and Warkentin, M. 2008. “Malicious Code: Developments and Defenses,” in *Encyclopedia of Multimedia Technology and Networking*, M. Pagani (ed.), (2nd ed.) Hershey, PA: Idea Group Publishing.

MacKenzie, S. B., Podsakoff, P. M., and Podsakoff, N. P. 2011. “Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques,” *MIS Quarterly* (35:2), pp. 293–334.

Maddux, J. E., and Rogers, R. W. 1983. “Protection Motivation and Self-efficacy: A Revised Theory of Fear Appeals and Attitude Change,” *Journal of Experimental Social Psychology* (19), pp. 469–479.

Mahmood, M. A., Siponen, M., Straub, D., Rao, R., and Raghu, T. S. 2010. “Moving Toward Black Hat Research in Information Systems Security: An Editorial Introduction to the Special Issue,” *MIS Quarterly* (34:3), pp. 431–433.

Malimage, K., and Warkentin, M. 2010. “Data Loss from Storage Device Failure: An Empirical Study of Protection Motivation,” in *2010 Workshop on Information Security and Privacy (WISP)*, .

Marett, K., McNab, A. L., and Harris, R. B. 2011. “Social Networking Websites and Posting Personal Information: An Evaluation of Protection Motivation Theory,” *AIS Transactions on Human-Computer Interaction* (3:3), pp. 170–188.

Mason, W., and Suri, S. 2012. “Conducting Behavioral Research on Amazon’s Mechanical Turk,” *Behavior Research Methods* (44:1), pp. 1–23.

McCarthy, B. 2002. “New Economics of Sociological Criminology,” *Annual Review of Sociology* (28:1), pp. 417–442.

McGrath, J. E. 1982. “Dilemmatics: The Study of Research Choices and Dilemmas,” in *Judgment Calls in Research*, Beverly Hills, CA: Sage Publications, Inc., pp. 69–80.

المنارة للاستشارات

www.manaraa.com

McGrath, J. E. 1995. “Methodology Matters: Doing Research in the Behavioral and Social Sciences,” *Humancomputer interaction* (R. Baecker and W. A. S. Buxton, eds.), (26:c)Morgan Kaufmann Publishers Inc., pp. 152–169.

Microsoft. 2012. “10 Ways to Work More Securely,” *Microsoft At Work*, .

Milne, S., Sheeran, P., and Orbell, S. 2000. “Prediction and Intervention in Health-related Behavior: A Meta-analytic of Protection Motivation Theory,” *Journal of Applied Social Psychology* (30:1), pp. 106–143.

Mingers, J. 1997. “Multi-Paradigm Multimethodology,” in *Multimethodology: Theory and Practice of Combining Management Science Methodologies*, J. Mingers and A. Gill (eds.), Chichester, UK: Wiley, pp. 1–20.

Mingers, J. 2001. “Combining IS Research Methods: Towards a Pluralist Methodology,” *Information Systems Research* (12:3), pp. 240–259.

Mittal, B. 1988. “Achieving Higher Seat Belt Usage: The Role of Habit in Bridging the Attitude-Behavior Gap,” *Journal of Applied Social Psychology* (18:12), pp. 993–1016.

Montano, D. E., and Taplin, S. E. 1991. “A Test of an Expanded Theory in Reasoned Action to Predict Mammography Participation,” *Social Science and Medicine* (32:6), pp. 733–741.

Moody, G. D., and Siponen, M. 2013. “Using the Theory of Interpersonal Behavior to Explain Non-work-related Personal Use of the Internet at Work,” *Information & Management (forthcoming)* .

Moore, G. C., and Benbasat, I. 1991. “Development of an Instrument to Measure the Perceptions of Adopting an Information Technology Innovation,” *Information Systems Research* (2), pp. 192–222.

Morgan, J., Maris, J.-M., and Lorents, A. C. 2007. “Security Practices of Students,” in *Information Systems Education Conference*, .

Morris, R., and Thompson, K. 1979. “Password Security: A Case History,” *Communications of the ACM* (22:11), pp. 594–597.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. 2009. “What Levels of Moral Reasoning and Values Explain Adherence to Information Security Rules? An Empirical Study,” *European Journal of Information Systems* (18:2), pp. 126–139.

المنارة للاستشارات

www.manaraa.com

Nagin, D. S., and Pogarsky, G. 2001. "Integrating Celerity, Impulsivity,and Extralegal Sanction Threats into a Model of General Deterrence and Evidence," *Criminology* (39:4), pp. 865–891.

Neal, D. T., Wood, W., and Drolet, A. 2013. "How Do People Adhere to Goals When Will Power is Low? The Profits (and Pitfalls) of Strong Habits.," *Journal of Personality and Social Psychology* (104:6), pp. 959–975.

Neal, D. T., Wood, W., and Quinn, J. M. 2006. "Habits—A Repeat Performance," *Current Directions in Psychological Science* (15:4), pp. 198–202.

Neal, D. T., Wood, W., Wu, M., and Kurlander, D. 2011. "The Pull of the Past: When Do Habits Persist Despite Conflict With Motives?," *Personality and Social Psychology Bulletin* (37:11), pp. 1428 –1437.

Netemeyer, R. G., Bearden, W. O., and Sharma, S. 2003. *Scaling procedures: Issues and applications*, Thousand Oaks, CA: Sage Publications, Inc.

Ng, B.-Y., Kankanhalli, A., and Xu, Y. (Calvin). 2009. "Studying Users' Computer Security Behavior: A Health Belief Perspective," *Decision Support Systems* (46:1), pp. 815–825.

Nunnally, J. C., and Bernstein, I. H. 1994. *Psychometric Theory*, New York, NY: McGraw-Hill.

Orbell, S., Blair, C., Sherlock, K., and Conner, M. 2001. "The Theory of Planned Behavior and Ecstasy Use: Roles for Habit and Perceived Control over Taking Versus Obtaining Substances," *Journal of Applied Social Psychology* (31:1), pp. 31–47.

Ouellette, J. A., and Wood, W. 1998. "Habit and Intention in Everyday Life: The Multiple Processes by Which Past Behavior Predicts Future Behavior," *Psychological Bulletin* (124:1), pp. 54–74.

Oulasvirta, A., Rattenbury, T., Ma, L., and Raita, E. 2012. "Habits Make Smartphone Use More Pervasive," *Personal and Ubiquitous Computing* (16:1), pp. 105–114.

Pahnila, S., Siponen, M., and Mahmood, A. 2007. "Employees' Behavior Towards IS Security Policy Compliance," in *40th Hawaii International Conference on System Sciences*, Hawaii, USA.

Paolacci, G., Chandler, J., and Ipeirotis, P. G. 2010. "Running experiments on Amazon Mechanical Turk," *Judgment and Decision Making* (5:5), pp. 411–419.

المنارة للاستشارات

www.manaraa.com

Paternoster, R., and Pogarsky, G. 2009. “Rational Choice, Agency and Thoughtfully Reflective Decision Making: The Short and Long-Term Consequences of Making Good Choices,” *Journal of Quantitative Criminology* (25:2).

Paternoster, R., and Simpson, S. 1996. “Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime,” *Law and Society Review* (30:3), pp. 549–584.

Pavlou, P., Liang, H., and Xue, Y. 2007. “Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective,” *MIS Quarterly* (31:1), pp. 105–136.

Petter, S., Straub, D., and Rai, A. 2007. “Specifying Formative Constructs in Information Systems Research,” *MIS Quarterly* (31:4), pp. 623–656.

Piquero, N. L., Exum, M. L., and Simpson, S. S. 2005. “Integrating the Desire for Control and Rational Choice in a Corporate Crime Context,” *Justice Quarterly* (22:2), pp. 252–280.

Plamondon, S. 2011. “How to Help Your Employees Develop Better Security Habits,” *Microsoft Medium Business Centre*, .

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., and Podsakoff, N. P. 2003. “Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies,” *Journal of Applied Psychology* (88:5), pp. 879–903.

Podsakoff, P. M., and Organ, D. W. 1986. “Self-reports in Organizational Research: Problems and Prospects,” *Journal of Management* (12:4), pp. 531–544.

Polites, G. L., and Karahanna, E. 2012. “Shackled To The Status Quo: The Inhibiting Effects Of Incumbent System Habit, Switching Costs, And Inertia On New System Acceptance,” *MIS Quarterly* (36:1), pp. 21–42.

Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., and Courtney, J. F. 2013. “Insiders’ Protection of Organizational Information Assets: Development of a Systematics-Based Taxonomy and Theory of Diversity for Protection-Motivated Behaviors,” *MIS Quarterly (forthcoming)* .

Prentice, D. A., and Miller, D. T. 1992. “When Small Effects Are Impressive,” *Psychological Bulletin* (112:1), pp. 160–164.

Puhakainen, P., and Siponen, M. 2010. “Improving Employee’s Compliance Through Information Systems Security Training: An Action Research Study,” *MIS Quarterly* (34:4), pp. 757–778.

المنارة للاستشارات
www.manaraa.com

Qualtrics. 2013. “Qualtrics Survey Panels,” .

Quine, L., and Rubin, R. 1997. “Attitude, Subjective Norm and Perceived Behavioral Control as Predictors of Women’s Intentions to Take Hormone Replacement Therapy,” *British Journal of Health Psychology* (2:3), pp. 199–216.

Richardson, R. 2012. “2010 / 2011 CSI Computer Crime and Security Survey,” .

Rietta, F. S. 2006. “Application Layer Intrusion Detection for Sql Injection,” in *Annual Southeast regional conference*, , pp. 531–536.

Ringle, C. M., Sarstedt, M., and Straub, D. W. 2012. “Editor’s Comments: A Critical Look at the Use of PLS-SEM in MIS quarterly,” *MIS Quarterly* (36:1), pp. iii–xiv.

Ringle, C., Sven, W., and Alexander, W. 2005. “SmartPLS 2.0.,” Hamburg.

Rippetoe, P. A., and Rogers, R. W. 1987. “Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Coping with a Health Threat,” *Journal of Personality and Social Psychology* (52:3), pp. 596–604.

Rogers, R. W. 1975. “A Protection Motivation Theory of Fear Appeals and Attitude Change,” *The Journal of Psychology* (91), pp. 93–114.

Rogers, R. W. 1983. “Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protected Motivation,” in *Social Psychophysiology: A Sourcebook*, J. T. Cacioppo and R. E. Petty (eds.), New York: The Guilford Press, pp. 153–176.

Ronis, D. L., Yates, J. F., and Kirscht, J. P. 1989. “Attitudes, Decisions, and Habits As Determinants of Repeated Behavior,” in *Attitude, Structure and Function*, A. R. Pratkanis, S. J. Breckler, and A. G. Greenwald (eds.), Hilldale, NJ: Lawrence Erlbaum Associates, pp. 213–239.

S.B.Thorat, S.K.Nayak, and M.M.Bokhare. 2010. “Data Security : An Analysis,” *International Journal on Computer Science and Engineering* (2:4), pp. 1355–1358.

Saba, A., Vassallo, M., and Turrini, A. 2000. “The Role of Attitudes, Intentions and Habit in Predicting Actual Consumption of Fat Containing Foods in Italy,” *European Journal of Clinical Nutrition* (54:7), pp. 540–547.

Saga, V. L., and Zmud, R. W. 1994. “The Nature and Determinants of IT Acceptance, Routinization, and Infusion,” in *Diffusion, Transfer and Implementation of Information Technology*, L. Levine (ed.), Amsterdam: Elsevier Science, pp. 67–86.

المنارة للاستشارات

www.manaraa.com

Sanger, D. E. 2012, June. “Obama Order Sped Up Wave of Cyberattacks Against Iran,” *The New York Times* .

Schank, R. C., and Abelson, R. P. 1977. *Scripts, Plans, Goals and Understanding: An Inquiry Into Human Knowledge Structures*, Hillsdale, New Jersey: Lawrence Erlbaum Associates.

Schwarzer, R., Schuez, B. E. C., Ziegelmann, J. P., Lippke, S., Luszczynska, A., and Scholz, U. 2007. “Adoption and Maintenance of Four Health Behaviors: Theory-guided Longitudinal Studies on Dental Flossing, Seat Belt Use, Dietary Behavior, and Physical Activity,” *Annals of Behavioral Medicine* (33:2), pp. 156–166.

Sheeran, P. 2002. “Intention-behavior Relations: A Conceptual and Empirical Review,” in *European review of social psychology*, W. Stroebe and M. Hewstone (eds.), Chichester, UK: Wiley, pp. 1–36.

Sheeran, P., Aarts, H., Custers, R., Rivis, A., Webb, T. L., and Cooke, R. 2005. “The Goal-Dependent Automaticity of Drinking Habits,” *British Journal of Social Psychology* (44), pp. 47–63.

Sheppard, B. H., Hartwick, J., and Warshaw, P. R. 1988. “The Theory of Reasoned Action: A Meta-analysis of Past Research with Recommendations for Modifications and Future Research,” *Journal of Consumer Research* (15), pp. 325–343.

Simon, B. 2011. *Everything but the Coffee: Learning about America from Starbucks*, University of California Press.

Siponen, M., Karjalainen, M., and Sarker, S. 2010. “Unearthing Social Mechanisms that Lead Employees to Violate IS Security Procedures: An Inductive Study,” in *The Dewald Roode Information Security Workshop*, pp. 155–189.

Siponen, M., and Vance, A. 2010. “Neutralization : New Insights Into the Problem of Employee Information Systems Security Policy Violations,” *MIS Quarterly* (34:3), pp. 487–502.

Sniehotta, F. F., and Presseau, J. 2012. “The Habitual Use of the Self-Report Habit Index,” *Annals of Behavioural Medicine* (43), pp. 139–140.

Sood, B. G. 2012. “How Should We Measure Habits? (and why should we care),” *Reflect Project*, .

Spennemann, D. H. R., and Atkinson, J. S. 2002. “A Longitudinal Study of Data Management Practices Among Parks Management Students,” *Campus-Wide Information Systems* (19:4), pp. 149–155.

المنارة للاستشارات

www.manaraa.com

Straub, D., Limayem, M., and Karahanna, E. 1995. “Measuring System Usage: Implications for IS Theory Testing,” *Management Science* (41:8), pp. 1328–1342.

Straub, D. W., Boudreau, M. C., and Gefen, D. 2004. “Validation Guidelines for IS Positivist Research,” *Communications of AIS* (13:1), pp. 380–427.

Sutton, S. 1982. “Fear-arousing Communications: A Critical Examination of Theory and Research,” in *Social psychology and behavioral medicine*, London, UK: John Wiley & Sons, pp. 303–337.

Sutton, S. K., and Davidson, R. 1997. “Prefrontal Brain Asymmetry: A Biological Substrate of the Behavioral Approach and Inhibition Systems,” *Psychological Science* (8:3), pp. 204–210.

Tabachnick, B. G., and Fidell, L. S. 2007. *Multivariate Statistics*, (5th ed.) Boston, MA: Allyn and Bacon.

Taylor, B. J. 2006. “Factorial Surveys: Using Vignettes to Study Professional Judgement,” *British Journal of Social Work* (36), pp. 1187–1207.

Towler, G., and Shepherd, R. 1991. “Modification of Fishbein and Ajzen’s Theory of Reasoned Action to Predict Chip Consumption,” *Food Quality and Preference* (3:1), pp. 37–45.

Trafimow, D. 2000. “Habit as Both a Direct Cause of Intention to Use a Condom and as a Moderator of the Attitude-Intention and Subjective Norm-Intention Relations,” *Psychology and Health* (15:3), pp. 383–393.

Triandis, H. C. 1977. *Interpersonal Behavior*, Monterey, CA: Brooks/ Cole.

Triandis, H. C. 1980. “Values, Attitudes, and Interpersonal Behavior,” in *Nebraska Symposium on Motivation*, H. E. Home and M. Page (eds.), (27th ed.) Lincoln NE: University of Nebraska Press.

Tuorila, H., and Pangborn, R. M. 1988. “Prediction of Reported Consumption of Selected Fat-Containing Foods,” *Appetite* (11:2), pp. 81–95.

Vance, A., Siponen, M., and Pahnila, S. 2012. “Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory,” *Information & Management* (49:3), pp. 190–198.

Vance, A., Siponen, M., and Pahnilla, S. 2009. “How Personality and Habit Affect Protection Motivation,” in *Workshop on Information Security and Privacy (WISP)*, .

المنارة للاستشارات

www.manaraa.com

Vandermeer, J. 2006. “Seven Highly Successful Habits of Enterprise Email Managers: Ensuring that your Employees’ Email Usage is not Putting your Company at Risk,” *Information Systems Security* (15:6), pp. 64–75.

Venkatesh, V., Brown, S., and Bala, H. 2013. “Bridging the Qualitative–Quantitative Divide: Guidelines for Conducting Mixed Methods Research in Information Systems,” *MIS Quarterly* (37:1), pp. 21–54.

Venkatesh, V., and Davis, F. D. 2000. “Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies,” *Management Science* (46:2), pp. 186–204.

Venkatesh, V., Morris, M., Davis, G., and Davis, F. 2003. “User Acceptance of Information Technology: Toward a Unified View,” *MIS Quarterly* (27:3), pp. 425–478.

Venkatesh, V., Morris, M. G., and Ackerman, P. L. 2000. “A Longitudinal Field Investigation of Gender Differences in Individual Technology Adoption Decision Making Processes,” *Organizational Behavior and Human Decision Processes* (83:1), pp. 33–60.

Venkatesh, V., Thong, J. Y. L., and Xu, X. 2012. “Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology,” *MIS Quarterly* (36:1), pp. 157–178.

Verplanken, B., and Aarts, H. 1999. “Habit, Attitude, and Planned Behaviour: Is Habit an Empty Construct or an Interesting Case of Goal-Directed Automaticity?,” in *European Review of Social Psychology*, W. Stroebe and M. Hewstone (eds.), London: John Wiley & Sons, pp. 101–134.

Verplanken, B., Aarts, H., and Van Knippenberg, A. 1997. “Habit,Information Acquisition, and the Process of Making Travel Mode Choices,” *European Journal of Social Psychology* (27:5), pp. 539–560.

Verplanken, B., Aarts, H., Van Knippenberg, A., and Van Knippenberg, C. 1994. “Attitude Versus General Habit: Antecedents of Travel Mode Choice,” *Journal of Applied Social Psychology* (24:4), pp. 285–300.

Verplanken, B., Aarts, H., Van Knippenberg, A., and Moonen, A. 1998. “Habit Versus Planned Behaviour: A Field Experiment,” *British Journal of Social Psychology* (37:1), pp. 111–128.

Verplanken, B., and Orbell, S. 2003. “Reflections on Past Behavior: A Self-Report Index of Habit Strength,” *Journal of Applied Social Psychology* (33:6), pp. 1313–1330.

المنارة للاستشارات

www.manaraa.com

Verplanken, V. 2006. “Beyond Frequency: Habit as Mental Construct,” *British Journal of Social Psychology* (45:3), pp. 639–656.

Wang, P., Fang, B., and Xiaochun, Y. 2005. “A New User-Habit Based Approach for Early Warning of Worms,” *Computational Intelligence and Security* (3802), pp. 212–219.

Warkentin, M., Johnston, A. C., and Shropshire, J. 2011. “The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention,” *European Journal of Information Systems* (20:3), pp. 267–284.

Warkentin, M., Johnston, A. C., and Shropshire., J. 2011. “The Influence of the Informal Social Learning Environment on Information Privacy Policy Compliance Efficacy and Intention,” *European Journal of Information Systems* (20:3), pp. 267–284.

Warkentin, M., and Johnston, C. A. 2008. “IT Governance and Organizational Development for Security Management,” in *Information Security Policies and Practices*, D. Straub, S. Goodman, and R. L. Baskerville (eds.), Armonk, NY: M.E. Sharpe, pp. 46–68.

Warkentin, M., Straub, D., and Malimage, K. 2012. “Measuring Secure Behavior: A Research Commentary,” in *Annual Symposium on Information Assurance*, Albany , NY.

Warkentin, M., and Willison, R. 2009. “Behavioral and Policy ssues in Information Systems Security: The Insider Threat,” *European Journal of Information Systems* (18:2), pp. 101–105.

Watson, J. B. 1914. *Behavior: An Introduction to Comparative Behavior*, New York, NY: Holt.

Westland, C. 1997. “A Rational Choice Model of Computer and Network Crime,” *International Journal of Electronic Commerce* (1:2), pp. 109–126.

Whitman, M. E. 2003. “Enemy At The Gate: Threats to Information Security,” *Communications Of The ACM* (46:8), pp. 91–95.

Wiener, N. 1948. *Cybernetics: Control and Communication in the Animal and the Machine*, Cambridge, MA: MIT Press.

Williams, L. J., Edwards, J. R., and Vandenberg, R. J. 2003. “Recent Advances in Causal Modeling Methods for Organizational and Management Research,” *Journal of Management* (29:6), pp. 903–936.

المنارة للاستشارات

www.manaraa.com

Willison, R., and Warkentin, M. 2013. “Beyond Deterrence: An Expanded View Of Employee Computer Abuse,” *MIS Quarterly* (37:1), pp. 1–20.

Witte, K. 1992. “Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model,” *Communication Monographs* (59), pp. 329–349.

Witte, K., Cameron, K. A., McKeon, J. K., and Berkowitz, J. M. 1996. “Predicting Risk Behaviors: Development and Validation of a Diagnostic Scale,” *Journal of Health Communication* (1), pp. 317–341.

Wood, W., and Neal, D. T. 2007. “A New Look at Habits and the Habit–Goal Interface,” *Psychological Review* (114:4), pp. 843–863.

Wood, W., Quinn, J. M., and Kashy, D. A. 2002. “Habits in Everyday Life: Thought, Emotion, and Action,” *Journal of Personality and Social Psychology* (83:6), pp. 1281–1297.

Woon, I. M. Y., Tan, G. W., and Low, R. T. 2005. “A Protection Motivation Theory Approach to Home Wireless Security,” in *Proceedings of the 26th International Conference on Information Systems*, D. Avison, D. Galletta, and J. I. DeGross (eds.), Las Vegas, pp. 367–380.

Workman, M., Bommer, W., and Straub, D. W. 2008. “Security Lapses and the Omission of Information Security Measures: An Empirical Test of the Threat Control Model,” *Journal of Computers in Human Behavior* (24:6), pp. 2799–2816.

Wu, M.-C., and Kuo, F.-Y. 2008. “An Empirical Investigation of Habitual Usage and Past Usage on Technology Acceptance Evaluations and Continuance Intention,” *The DATA BASE for Advances in Information Systems* (39:4), pp. 48–73.

Wyatt, J. C. 2000. “When to Use Web-based Surveys,” *Journal of the American Medical Informatics Association* (7:4), pp. 426–429.

Xu, Z. C., Hu, Q., and Zhang, C. H. 2013. “Why Do Computer Talents Become Computer Hackers? A Framework for Understanding and Managing the Hacking Epidemic,” *Communications of the ACM (forthcoming)* .

Yang, W.-H., and Shieh, S.-P. 1999. “Password Authentication Schemes with Smart Cards,” *Computers & Security* (18:8), pp. 727–733.

Ye, C., and Potter, R. 2011. “The Role of Habit in Post-Adoption Switching of Personal Information Technologies: An Empirical Investigation,” *Communications of the Association for Information Systems* (28:1), pp. 585–609.

المنارة للاستشارات

www.manaraa.com

Zhang, L., and McDowell, W. C. 2009. “Am I Really at Risk? Determinants of Online Users’ Intentions to Use Strong Passwords,” *Journal of Internet Commerce* (8), pp. 180–197.

Zhang, L., Smith, W. W., and McDowell, W. C. 2006. “Examining digital piracy: self-control, punishment, and self-efficacy,” *Information Resources Management Journal* (22:1), pp. 24–44.

المنارة للاستشارات

www.manaraa.com

APPENDIX A

COMPARISON OF OTHER STUDIES

المنارة للاستشارات

www.manaraa.com

Topic	**Vance et al. 2010**	**Pahnila et al. (2007)**	**Siponen et al. (2010)**	**Present study**
Use of Theory	• Utilization of PMT and Habit Theory in an information security context. • Frequency of past behavior alone does not constitute habit. • Influence of prior experience on adaptive or maladaptive coping. • Awareness of threats triggers PMT cognitive process.	• User of PMT, Deterrence Theory, TRA and Habit in an information security context. • Habit is unconscious and automatic behavior. • Influence of habits on actual behavior increases in the long run while behavioral intention decreases.	• Grounded theory approach to identify factors that influence information security policy compliance. • Habitual enactment influences employees to follow security procedures automatically.	• Utilization of PMT and Habit Theory in an information security context. • Habit is a form of goal-oriented automaticity. • Goal-oriented behavior performed repetitively in a stable context will become habitual. • When habits are strong, influence of the cognitive process is weakened. • PMT variables and behavioral intentions have a weak influence on actual behavior when habits are strong.
Research Model	• PMT variables are hypothesized to mediate the relationship between habit and behavioral intentions.	• Habit is hypothesized to directly influence behavioral intention to comply with security policies.	• Habitual enactment is proposed to directly influence secure use of the internet, writing passwords down and locking one's pc.	• Habit is hypothesized to negatively moderate the intention-behavior relationship and directly influence behavior.
Method	• Use of hypothetical scenario method • Five scenarios of different IS policy violations • Self-report habit scale	• Use of survey methodology. • Self-report habit scale (reflective) used to operationalize habit • Self-reported actual	• Use of interviews to collect data to conduct a grounded theory approach. • Data collected from a single company but	• Use of survey methodology to investigate the role of habit on three positive secure behaviors. • Second-order formative, first-order reflective scale to

www.manaraa.com

	(reflective) used to operationalize habit • Behavioral intention was the ultimate dependent variable. • Data Collected from one organization • Intentions to comply differed significantly depending on the scenarios received. • Data from five different scenarios analyzed together as one behavior.	behavior was the ultimate dependent variable. • Data Collected from one organization	different locations in Switzerland, UAE and China. • 72 face-to-face interviews conducted in different organizational positions and countries.	measure habit using self-reported items, along with a reflective scale. • Self-reported actual behavior was the ultimate dependent variable. • Data collected from multiple organizations across different industries with the use of survey panels. • Pilot study conducted from the same pool of respondents as the full-scale study. • Data from each behavior analyzed separately in its own model.
Expected Findings and Contributions	• Habit had a significant effect on threat and coping appraisals. • All variables except perceived threat vulnerability had a significant impact on behavioral intentions. • No discussion of the role of habit for practitioners or researchers.	• Habit significantly influenced behavioral intentions to comply with security policies. • Behavioral intentions significantly influenced actual behavior. • It is recommended that organizations should get their employees to get into the habit of complying with IS security policies.	• Employees identified habit has a major factor in the performance of certain secure behaviors. • Secure use of the internet, writing down passwords and locking one's PC were found to be significantly influenced by habit. • Instead of testing theories, this study used a grounded approach to find the phenomenon of	• Habit will negatively moderate the intention-behavior relationship while directly influencing behavior. When habits are strong, influence of threat appraisal and coping appraisal would not drive the actual behavior. • First time that a habit scale is used to reflect the true automatic nature of habit and to investigate the role of habit in information security

المنارة للاستشارات
www.manaraa.com

			security policy compliance.	context. • Practitioners can use the findings to foster positive habits in their employees, such that the secure behaviors are performed automatically. They can also use the findings to break negative habits through fear appeals and increasing of threat appraisals. • Researchers can use the findings to further investigate the role of habit in an information security context and identify factors that contribute to the forming and breaking of habits.

المنارة للاستشارات
www.manaraa.com

APPENDIX B

BEHAVIOR SELECTION PROCESS

www.manaraa.com

Table B.1 Behaviors Selected From Academic References

#	Behavior	Source
1	Sharing password with co-workers.	Crossler and Belanger (2010)
2	Using anti-spyware software.	Johnston & Warkentin (2010)
3	Backing up data regularly.	Crossler and Belanger (2010)
4	Setting up strong passwords to login to systems.	Crossler and Belanger (2010)
5	Making sure the anti-virus is automatically updated.	Crossler and Belanger (2010)
6	Using caution when opening links/attachments in email.	Crossler and Belanger (2010)
7	Scanning the computer for spyware and keeping it up to date.	Crossler and Belanger (2010)
8	Writing passwords down.	Crossler and Belanger (2010)
9	Change passwords often.	Crossler and Belanger (2010)
10	Adherence to security policies.	Herath et al. (2010)
11	Good password practices.	Workman et al. (2008)
12	Locking the computer when not in use	Vance et al. (2012)
13	Encryption of sensitive information.	Vance et al. (2012)
14	Update software regularly.	Johnston & Warkentin (2010)
15	Logging off workstations.	Johnston & Warkentin (2010)
16	Shredding sensitive documents.	Johnston & Warkentin (2010)
17	Voluntary IS security training participation	Siponen et al. (2010)
18	Obeying IS security policies.	Siponen et al. (2010)
19	Constantly updating anti-virus software	Anderson & Agrwal (2010)
20	Being suspicious of e-mails from unknown sources.	Anderson & Agrwal (2010)
21	Effectively securing passwords.	Anderson & Agrwal (2010)
22	Enabling security in your wireless network.	Woon et al. (2005)
23	Avoid copying sensitive data to USB drives.	Siponen & Vance (2010)
24	Avoid revealing sensitive information to outsiders.	Siponen & Vance (2010)
25	Avoid sending confidential information unencrypted.	Siponen & Vance (2010)
26	Using unauthorized access to copy, modify or delete critical data.	D'Arcy et al. (2009)
27	Avoid downloading personal internet software to your company computers.	D'Arcy et al. (2009)
28	Avoid reading confidential documents.	Vance et al. (2012)
29	Report a computer virus immediately.	Vance et al. (2012)
30	Avoid using company laptop for personal usage.	Vance et al. (2012)

المنارة للاستشارات
www.manaraa.com

Table B.2 Behaviors Selected From Posey et al. (2013)

#	**Behavior**
1	Respond to emails, which have a legitimate business request.
2	Documents any changes made in the computer system.
3	Opens email attachments only if you know the email's sender and was expecting the email.
4	Not allowing unauthorized individuals to do your work.
5	When using a shared computer, log off the previous employee before logging in with your credentials.
6	Set up a screen saver password to protect unauthorized logins.
7	Refrain from verbally discuss sensitive information in areas where unauthorized persons may be located (e.g., a hallway, an elevator)
8	Locks your workstation when leaving the office space so that the workstation cannot be accessed by other individuals.
9	Refrain from forwarding email spam to co-workers.
10	Store information only according to the retention policies specified by his/her organization.
11	Change passwords according to the organization's security guidelines.
12	Notify your co-workers of important security information you become aware of.
13	If you identify something that looks out of the ordinary in your work environment, you immediately reports it to the proper organizational authorities.
14	Refrain from using shortcuts in the computer system that would be against the organization's accepted security protocol.
15	Refrain from connecting personal devices (e.g., laptop, smartphone, tablet devices) into the company network.
16	Properly destroys and disposes of all unneeded sensitive documents.
17	Perform a "double check" of your work to make certain that the sensitive information you enter into the computer system is accurately coded.
18	Work at a steady but cautious pace to ensure that you perform your job tasks in a secure manner.
19	Backs up important data and documents on a regular basis.
20	Avoid writing your passwords down.
21	Converts sensitive documents to Adobe PDF format so that none of the information in the document can be altered once it is finalized.
22	Avoid opening emails that you believe have a chance of containing a virus or other potentially malicious components.
23	Avoid installing software on your computer workstation unless authorized to do so.
24	Immediately apply software updates to your computer workstation when notified of the update by an authorized individual or department within your organization

المنارة للاستشارات
www.manaraa.com

Table B.2 (Continued)

#	**Behavior**
25	Pauses before responding to an email to make certain that you are responding to a valid request.
26	Uses corporate email for work-related activities only.
27	While at work, utilize the Internet for work-related tasks only.
28	Avoid discussing sensitive company information with the media unless authorized to do so.
29	Avoid allowing anyone to look over his/her shoulder when he/she works on sensitive documents.
30	Always store sensitive corporate information only on protected media or locations (e.g., a protected server)
31	When compiling a new email message, verify that you actually send the email only to the intended recipients receive the communication.
32	Avoid setting up a wireless network access point in the corporate office without proper approval.
33	Properly destroy unneeded data residing on the computer system or the computer workstation.
34	Always logs out of the computer system as soon as you are done using it.
35	Always read and pay close attention to security newsletters sent by your organization's department that is responsible for information-security matters.
36	Always verify an individual's identity prior to releasing sensitive information to them.
37	Protect your computer-system account information by never giving it to other individuals.
38	Avoid writing your system login information down.
39	Set the permissions of computer files to prevent unauthorized access.
40	Actively attempts not to accidentally disclose sensitive company information with unauthorized individuals.
41	Avoid putting sensitive information in emails or other forms of electronic communication (e.g., instant messages) unless authorized to do so as required by your job.
42	Avoid displaying sensitive documents in public (e.g., airplane or airport).
43	Always properly logs into and out of computer systems at work.
44	Always create strong passwords (i.e., passwords having a combination of lower- and upper-case letters, numbers, and special characters).
45	Avoid leaving active computers unattended.
46	Immediately report a lost access card to the proper organizational authorities.
47	Clears sensitive information off of your desk or computer before allowing someone entrance into your office or leaving at the end of the work day.
48	Always lock sensitive, physical documents in a secure location when they are not in use.

للاستشارات المنارة
www.manaraa.com

Table B.2 (Continued)

#	**Behavior**
49	Adheres to the information-security guidelines and policies adopted by your organization.
50	Avoid discussing company-specific, information-security information (e.g., internal protocols, breaches) with anyone who does not need to know.
51	Do not open emails that "just do not look right" to you.
52	Informs your co-worker if you believe that the co-worker is engaging in behaviors not accepted by their company's information-security guidelines and policies.
53	Do now allow anyone else to utilize your computer workstation.
54	Uses secured wireless and/or wired networks approved by your organization for offsite network access.
55	Reminds your fellow co-workers of information-security guidelines and protocols adopted by your organization.
56	Immediately inform your supervisor upon awareness of the physical theft of computer equipment.
57	Immediately inform the authorized individual or department within the organization if you found a potential information-security problem or loophole
58	Only accesses information in the computer system that is required for your job.
59	Do not allow anyone else to utilize a computer workstation under your account and login information
60	Do not perform work on a computer workstation with a co-worker's account information or under a co-worker's login session
61	Quickly notify the sender of an email if that email contained sensitive information that was not meant for you.
62	Immediately report a co-worker's negligent information-security behavior to the proper organizational authorities.
63	If you receive an email from someone you know but the topic or content looks suspicious, you contact the sender to verify that the communication attempt was valid.
64	Keep the laptop or other electronic devices issued to them by their organization with them at all times.

المنارة للاستشارات
www.manaraa.com

Table B.3 Behaviors Selected From Practitioner Sources

#	Behavior	Source
1	Using security software (anti-virus, anti-spyware)	1
2	Writing down sensitive information on paper	2
3	Using authorized access to copy, modify or delete critical data	2
4	Avoid using unauthorized/insecure web apps in company networks	3
5	Avoid responding to fake emails or scams.	3
6	Avoid opening attachments in emails from unknown senders	3
7	Avoid posting sensitive information on social networking sites.	3
8	Encrypt corporate data before transferring it to USB devices.	3
9	Following company security policies.	3
10	Copy confidential or sensitive business information onto USB devices	4
11	Transferred Sensitive information onto computers outside the company network	4
12	Download personal internet software to their company computers	4
13	Turn off security settings or firewalls on workplace computers	5
14	Share passwords with co workers	6
15	Collect sensitive documents from the printer as soon as it was printed.	6
16	Avoid clicking URLs on social media links.	6
17	Always use the most updated version of Internet Browser.	7
18	Encrypting emails with sensitive data.	8
19	Avoid discarding sensitive documents in the trash.	9
20	Verify the firewall in the computer is switched on.	9
21	Lock the office door when you leave for the day.	9
22	Avoid leaving important documents on your desk or printing area.	9
23	Shred documents no longer necessary with a cross-cut shredder.	9
24	When issuing data to others be sure to understand what it will be used for and send only the data required.	9
25	Avoid downloading content directly from an unknown internet site.	10

المنارة للاستشارات
www.manaraa.com

Table B.3 (Continued)

#	Behavior	Source
26	Avoid downloading content directly from an unknown internet site.	10
27	Avoid opening or responding to an email from an unrecognized source.	10
28	Always lock the screen (Ctrl + Alt + Del) when leaving a computer terminal unattended and log-off completely when leaving for the day.	10
29	Avoid inserting portable media into the computer unless you are sure of its origin.	10
30	Avoid taking sensitive or valuable information away from work unless it is essential and secured via encrypted laptops or USB devices.	10
31	When away from the premises and/ or in public areas, keep all sensitive information secure to prevent loss or theft.	10
32	Create good browsing habits.	11
33	Avoid installing unauthorized software in your computer.	12
34	Avoid sharing sensitive information on social media.	12
35	Be careful when accessing corporate data with personal mobile devices such as smartphones or tablets.	12
36	have mobile safeguards in place and ensure that no sensitive data is being transferred over unsecured Wi-Fi networks.	12

Practitioner Sources:

1. http://techcrunch.com/2012/05/29/mcafee-malwar/
2. https://www.utoledo.edu/it/ns/Security/Awareness/Sensitive_Information.html
3. http://www.enterprisenetworkingplanet.com/netsecur/top-10-information-security-threats-2010
4. http://www.infosecurity-magazine.com/view/2123/majority-break-information-security-policies-survey/
5. http://www.infosecurity-magazine.com/view/2123/majority-break-information-security-policies-survey/

المنارة للاستشارات
www.manaraa.com

6. http://www.infosecurity-magazine.com/view/2123/majority-break-information-security-policies-survey/
7. http://www.pwc.com/en_GX/gx/information-security-survey/pdf/pwcsurvey2010_cio_reprint.pdf
8. http://www.clearswift.com/data/the-importance-of-encrpyting-email/
9. http://www.prnewswire.com/news-releases/national-survey-uncovers-data-breach-vulnerabilities-in-the-workplace-143809866.html
10. http://www.cpni.gov.uk/Security-Planning/Staff-training-and-communications/workplace-security/
11. http://www.ccskguide.org/risky-behavior-data-security-practices-in-the-workplace/
12. http://www.cioinsight.com/c/a/IT-Management/Bad-Tech-Habits-8-Things-Employees-Dont-Want-You-to-Know-628887/

المنارة للاستشارات
www.manaraa.com

Table B.4 Behaviors Selected for Step 2

#	**Behavior**
01	Avoid sharing passwords with co-workers.
02	Use anti-spyware software.
03	Backup data regularly.
04	Set up strong passwords to login to systems.
05	Verify regularly that anti-virus and/or anti-spyware software is auto updated.
06	Change passwords often.
07	Locking the computer when leaving it unattended.
08	Always encrypt sensitive information.
09	Immediately apply software updates when they become available.
10	Logoff or shutdown the computer when leaving the office for the day.
11	Shred sensitive documents.
12	Complying with information security policies.
13	Being cautions of emails from unknown sources.
14	Avoid coping sensitive data to portable media (e.g., USB, portable HDD).
15	Avoid revealing sensitive information to outsiders.
16	Avoid installing unauthorized software on your computer.
17	Avoid reading confidential documents that does not belong to you.
18	Report a computer virus immediately.
19	Avoid using a laptop for personal use.
20	Avoid writing down sensitive information on paper.
21	Avoid visiting unknown/suspicious websites.
22	Avoid opening email attachments from unknown senders.
23	Avoid posting sensitive information on social networking sites.
24	Encrypt corporate data before copying to portable media.
25	Avoid leaving sensitive documents at the printer.
26	Avoid clicking URLs on social media links.
27	Always use the most updated version of the browser.
28	Encrypt emails with sensitive data.
29	Regularly verify that the firewall on the computer is active.
30	Always lock the office door when leaving for the day.
31	Avoid leaving important documents at the working area/desk.
32	Avoid responding to emails from unknown sources.
33	Avoid inserting portable media that is not yours into the computer.
34	Keep all sensitive information secure to prevent loss or theft.

المنارة للاستشارات
www.manaraa.com

Table B.4 (Continued)

#	**Behavior**
35	Avoid using public networks to connect to corporate servers remotely.
36	Avoid discussing sensitive information in public areas (e.g., hallway, elevator).
37	Avoid connecting personal devices (e.g., laptop, tablet) to company network.
38	Ensuring sensitive data entered into the system is accurate.
39	Use corporate email only for work-related activities.
40	Always verify that email is sent only to the intended recipients.
41	Set computer file permissions to prevent unauthorized access.
42	Avoid leaving active computers unattended.
43	Always lock sensitive physical documents in a secure location when not in use.
44	Immediately inform authorities if you discover an information security problem.
45	Do not perform work on a computer under a co-worker's login session.
46	Always verify with the sender if the email content seem suspicious.
47	Document any changes made in the computer system.
48	Avoid downloading files from unknown websites.
49	Always secure keys and ID badges.

المنارة للاستشارات

www.manaraa.com

Table B.5 Results of The Expert and Employee Panels

##	Secure Behavior	Expert Panel (n=12)	Employee Panel (n=43)
15	Avoid revealing sensitive information to outsiders.	91%	67%
30	Lock the office door when leaving for the day.	91%	58%
10	Logoff or shutdown the computer when leaving the office for the day.	73%	74%
36	Avoid discussing sensitive information in public areas (e.g., hallway, elevator).	73%	51%
7	Lock the computer when leaving it unattended.	64%	67%
13	Being cautious of emails from unknown sources.	64%	63%
22	Avoid opening email attachments from unknown senders.	64%	60%
1	Avoid sharing passwords with co-workers.	55%	88%
21	Avoid visiting unknown/suspicious websites.	55%	56%
25	Avoid leaving sensitive documents at the printer.	55%	60%
32	Avoid responding to emails from unknown sources.	55%	58%
42	Avoid leaving active computers unattended.	55%	40%
48	Avoid downloading files from unknown websites.	55%	70%
23	Avoid posting sensitive information on social networking sites.	9%	72%
16	Avoid installing unauthorized software on your computer.	36%	65%
40	Verify that email is sent only to the intended recipients.	45%	63%
4	Set up strong passwords to login to systems.	45%	60%
3	Use anti-spyware software.	45%	58%
49	Secure keys and ID badges.	27%	53%
27	Use the most updated version of the browser.	9%	51%

Table B.6 Behaviors Selected for Full-scale Study

##	Behavior	Expert Panel	Employee Panel
7	Lock the computer when leaving it unattended.	64%	67%
40	Verify that email is sent only to the intended recipients.	45%	63%
21	Visit only known/verified websites.	55%	56%

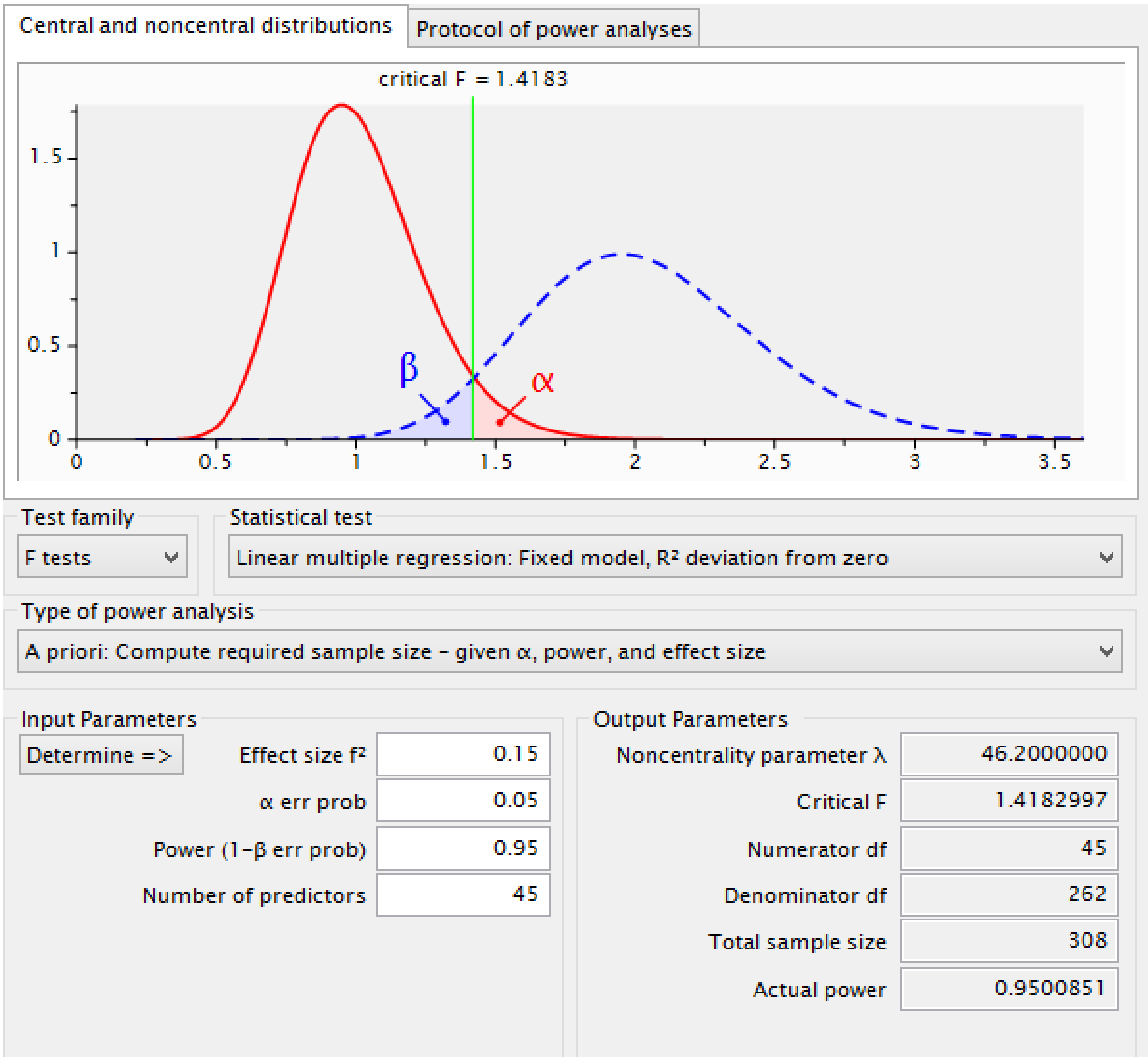
www.manaraa.com

APPENDIX C

POWER ANALYSIS

www.manaraa.com

A power analysis was conducted using the G-power software to identify a suitable sample size for this study. Using “a priori” type of power analysis to compute the required sample size, an effect size (f^2) of 0.15 (medium effect), alpha of 0.05 and a power of 0.95 required sample size was calculated with the number of predictors as 45 (total number of items). The results of the power analysis are shown below. A sample of 308 is needed to achieve a power of 0.95 and to detect a medium effect size.


Central and noncentral distributions
Protocol of power analyses
critical F = 1.4183
1.5
1
0.5
0
0
0.5
1
1.5
2
2.5
3
3.5
β
α
Determine =>

Test family: F tests

Statistical test: Linear multiple regression: Fixed model, R² deviation from zero

Type of power analysis: A priori: Compute required sample size – given α, power, and effect size

Input Parameters

Effect size f²	0.15
α err prob	0.05
Power (1-β err prob)	0.95
Number of predictors	45

Output Parameters

Noncentrality parameter λ	46.2000000
Critical F	1.4182997
Numerator df	45
Denominator df	262
Total sample size	308
Actual power	0.9500851

Figure C.1 Results of The Power Analysis

www.manaraa.com

APPENDIX D

SURVEY INSTRUMENT

المنارة للاستشارات

www.manaraa.com

Survey Instrument for the Lock PC Behavior

All items were measured using a 5 point likert scale (1-Strongly Disagree, 2-Disagree, 3-Neither Agree not Disagree, 4-Agree, 5-Strongly Agree).

Perceived Threat Severity (PSEV) - (Johnston & Warkentin, 2010)

PSEV1: If an unauthorized individual accesses my computer, it will be a severe problem.

PSEV2: It would be a significant problem for me if an unauthorized individual accesses my computer.

PSEV3: If an unauthorized individual accesses my computer, it will be serious.

Perceived Threat Vulnerability (PVUL) - (Witte et al. 1996)

PVUL1: The chances of an unauthorized individual accessing my computer are high.

PVUL2: It is likely that an unauthorized individual may access my computer.

PVUL3: It is possible that an unauthorized individual may access my computer.

Response Efficacy (REFF) - (Lee 2011)

REFF1: Locking the computer works for protection against unauthorized access to my computer.

REFF2: Locking the computer is an effective solution to prevent an unauthorized individual accessing my computer.

REFF3: I can effectively prevent an unauthorized individual accessing my computer by locking it.

REFF4: Unauthorized access to my computer can be effectively prevented by locking it.

Self-Efficacy (SEFF) - (Bulgurcu et al. 2010)

SEFF1: I am confident that I have the skills to lock my computer.

SEFF2: I know I can successfully lock my computer.

SEFF3: I believe that I have the knowledge necessary to lock my computer.

SEFF4: I personally have the skills to lock my computer.

Response Cost (RCST) - (Bulgurcu et al. 2010)

RCST1: Locking my computer is a burden.

RCST2: It is inconvenient to lock my computer.

RCST3: Locking my computer is time consuming.

RCST4: It is troublesome to lock or log-off my computer.

المنارة للاستشارات

www.manaraa.com

Behavioral Intention (BINT) - (Venkatesh et al. 2003)

BINT1: I intend to lock the computer every time I leave it unattended.

BINT2: I predict that I would lock the computer every time I leave it unattended.

BINT3: I plan to lock the computer every time I leave it unattended.

Actual Behavior (BEHV) - (Myyry et al. 2009; Workman et al. 2008)

BEHV1: I lock my computer every time I leave it unattended.

BEHV2: I always make sure that my computer is locked before I leave the computer unattended.

BEHV3: Locking my computer is something I do every time I leave it unattended.

Lack of Awareness (AWAR) - (Polites & Karahanna 2012)

AWAR1: Every time I leave my computer unattended, I choose to lock it even being aware of doing it.

AWAR2: Every time I need to leave my computer unattended, I unconsciously lock it.

AWAR3: Locking my computer, whenever I need to leave it unattended, is something I do without being aware.

AWAR4: Locking my computer whenever I leave it unattended is something I do unconsciously.

Uncontrollability (CTRL) - (Polites & Karahanna 2012)

CTRL1: I find it difficult to overrule my impulse to lock my computer whenever I leave it unattended.

CTRL2: I find it difficult to overcome my tendency to lock my computer whenever I leave it unattended.

CTRL3: It is difficult to control my tendency to lock my computer whenever I leave it unattended.

CTRL4: It is hard to restrain my urge to lock my computer whenever I leave it unattended.

Mental Efficiency (EFFC) - (Polites & Karahanna 2012)

EFFC1: I do not need to devote a lot of mental effort in deciding to lock my computer whenever I leave it unattended.

EFFC2: It would require effort not to lock my computer whenever I leave it unattended.

EFFC3: Choosing to lock my computer whenever I leave it unattended requires little mental energy.

EFFC4: I have no need to think about locking my computer whenever I leave it unattended.

المنارة للاستشارات
www.manaraa.com

Habit (HBT) - (Limayem et al. 2007)

HBT1: Locking the computer every time I leave it unattended has become automatic to me.

HBT2: Locking the computer every time I leave it unattended is natural to me.

HBT3: When leaving the computer unattended, locking it is an obvious choice for me.

Affective Based Inertia (INTA) - (Polites & Karahanna 2012)

I continue to lock my computer whenever I leave it unattended

INTA1: because it would be stressful to change.

INTA2: because I am comfortable doing so.

INTA3: because I enjoy doing so.

Behavioral Based Inertia (INTB) - (Polites & Karahanna 2012)

I continue to lock my computer whenever I leave it unattended

INTB1: simply because it is what I have always done.

INTB2: simply because it is part of my normal routine.

INTB3: simply because I have done so regularly in the past.

المنارة للاستشارات
www.manaraa.com

Survey Instrument for The Visit Only Verified Websites Behavior

All items were measured using a 5 point likert scale (1-Strongly Disagree, 2-Disagree, 3-Neither Agree not Disagree, 4-Agree, 5-Strongly Agree).

Perceived Threat Severity (PSEV) - (Johnston & Warkentin, 2010)

PSEV1: If an unintended recipient receives my email with confidential company information, it will be a severe problem.

PSEV2: It would be a significant problem for me if an unintended recipient receives my email with confidential company information.

PSEV3: If an unintended recipient receives my email with confidential company information, it will be serious.

Perceived Threat Vulnerability (PVUL) - (Witte et al. 1996)

PVUL1: Chances of an unintended recipient receiving my email with confidential company information are high.

PVUL2: It is likely that an unintended recipient will receive my email with confidential company information.

PVUL3: There is a possibility that an unintended recipient will receive my email with confidential company information.

Response Efficacy (REFF) - (Lee 2011)

REFF1: Before sending email, verifying it is sent only to the intended recipients, works for protection against an unintended recipient receiving it.

REFF2: Verifying that email is sent only to the intended recipients is an effective solution to prevent an unintended recipient from receiving it.

REFF3: I can effectively prevent an unintended recipient from receiving my email by verifying that email is sent only to the intended recipients before sending it.

REFF4: Sending sensitive information to unintended people through email can be effectively prevented by verifying the list of recipients.

Self-Efficacy (SEFF) - (Bulgurcu et al. 2010)

SEFF1: I am confident that I have the skills to verify that email is sent only to the intended recipients.

SEFF2: I know I can successfully verify that email is sent only to the intended recipients.

SEFF3: I believe that I have the knowledge necessary to verify that email is sent only to the intended recipients.

www.manaraa.com

SEFF4: I personally have the skills to check and verify the recipients of an email message before it is sent.

Response Cost (RCST) - (Bulgurcu et al. 2010)

RCST1: Having to verify that email is sent only to the intended recipients is a burden.

RCST2: It is inconvenient to verify that email is sent only to the intended recipients.

RCST3: Verifying that email is sent only to the intended recipients is time consuming.

RCST4: It is troublesome to verify that email is sent only to the intended recipients.

Behavioral Intention (BINT) - (Venkatesh et al. 2003)

BINT1: I intend to verify that email is sent only to intended recipients every time before I send email.

BINT2: I predict that I would verify email is sent only to intended recipients every time before I send email.

BINT3: I plan to verify that email is sent only to intended recipients every time before I send email.

Actual Behavior (BEHV) - (Myyry et al. 2009; Workman et al. 2008)

BEHV1: I always verify that email is sent only to intended recipients before I send email.

BEHV2: I always make sure that email is sent only to intended recipients every time before I send email.

BEHV3: Verifying that email is sent only to intended recipients is something I do, every time before I send email.

Lack of Awareness (AWAR) - (Polites & Karahanna 2012)

AWAR1: Every time I am about send an email, I verify that email is sent only to intended recipients without even being aware of doing it.

AWAR2: Every time I am about send an email, I unconsciously verify that email is sent only to intended recipients.

AWAR3: Verifying that email is sent only to intended recipients before sending an email is something I do without being aware.

AWAR4: Verifying that email is sent only to intended recipients before sending an email is something I do unconsciously.

المنارة للاستشارات
www.manaraa.com

Uncontrollability (CTRL) - (Polites & Karahanna 2012)

CTRL1: I find it difficult to overrule my impulse to verify that email is sent only to intended recipients every time I am about to send an email.

CTRL2: I find it difficult to overcome my tendency to verify that email is sent only to intended recipients every time I am about to send an email.

CTRL3: It is difficult to control my tendency to verify that email is sent only to intended recipients every time I am about to send an email.

CTRL4: It is hard to restrain my urge to verify that email is sent only to intended recipients every time I am about to send an email.

Mental Efficiency (EFFC) - (Polites & Karahanna 2012)

EFFC1: I do not need to devote a lot of mental effort in deciding verify that email is sent only to intended recipients every time I am about to send an email.

EFFC2: It would require effort not to verify that email is sent only to intended recipients every time I am about to send an email.

EFFC3: Choosing to verify that email is sent only to intended recipients every time I am about to send an email, requires little mental energy.

EFFC4: I have no need to think about verifying that email is sent only to intended recipients every time I am about to send an email.

Habit (HBT) - (Limayem et al. 2007)

HBT1: Verifying the recipients of email before sending a message has become automatic to me.

HBT2: Verifying the recipients of email before sending a message is natural for me.

HBT3: When sending email, verifying the recipients first is an obvious choice for me..

Affective Based Inertia (INTA) - (Polites & Karahanna 2012)

I continue to verify the recipients before sending emails simply because

INTA1: because it would be stressful to change.

INTA2: because I am comfortable doing so.

INTA3: because I enjoy doing so.

Behavioral Based Inertia (INTB) - (Polites & Karahanna 2012)

I continue to verify the recipients before sending emails simply because

INTB1: simply because it is what I have always done.

INTB2: simply because it is part of my normal routine.

INTB3: simply because I have done so regularly in the past.

المنارة للاستشارات
www.manaraa.com

Survey Instrument for the Verify Email Behavior

All items were measured using a 5 point likert scale (1-Strongly Disagree, 2-Disagree, 3-Neither Agree not Disagree, 4-Agree, 5-Strongly Agree).

Perceived Threat Severity (PSEV) - (Johnston & Warkentin, 2010)
PSEV1: If my computer were infected by malware, it would be severe.

PSEV2: If my computer were infected by malware, it would be serious.

PSEV3: If my computer were infected by malware, it would be serious.

Perceived Threat Vulnerability (PVUL) - (Witte et al. 1996)
PVUL1: The chances of my computer getting infected with malware are high.

PVUL2: It is likely that my computer may get infected with malware.

PVUL3: There is a possibility that my computer will get infected with malware.

Response Efficacy (REFF) - (Lee 2011)
REFF1: Visiting only known websites works for protection against my computer getting infected with malware.

REFF2: Visiting only known websites is an effective solution to prevent my computer getting infected with malware.

REFF3: I can effectively prevent my computer getting infected with malware by visiting only known websites.

REFF4: Malware infection of my computer can be effectively prevented by visiting only known websites.

Self-Efficacy (SEFF) - (Bulgurcu et al. 2010)

SEFF1: I am confident that I have the skills to visit only known websites.

SEFF2: I know I can successfully visit only known websites without much effort.

SEFF3: I believe that I have the knowledge necessary to visit only known websites.

SEFF4: I personally have the skills to visit only known websites.

Response Cost (RCST) - (Bulgurcu et al. 2010)
RCST1: Visiting only known websites is a burden.

RCST2: It is inconvenient to only visit known websites.

RCST3: Visiting only known websites is time consuming.

RCST4: It is troublesome to visit only known websites.

المنارة للاستشارات
www.manaraa.com

Behavioral Intention (BINT) - (Venkatesh et al. 2003)

BINT1: I intend to visit only known websites every time I use the internet.

BINT2: I predict that I would visit only known websites every time I use the internet.

BINT3: I plan to visit only known websites every time I use the internet.

Actual Behavior (BEHV) - (Myyry et al. 2009; Workman et al. 2008)

BEHV1: I always visit only known websites every time I use the internet.

BEHV2: I always make sure that I only visit known websites every time I use the internet.

BEHV3: Visiting only known websites is something I do, every time I use the internet.

Lack of Awareness (AWAR) - (Polites & Karahanna 2012)

AWAR1: Every time I use the internet, I choose to visit only known websites without even being aware of doing it.

AWAR2: Every time I use the internet, I unconsciously visit only known websites.

AWAR3: Visiting only known websites every time I use the internet is something I do without being aware.

AWAR4: Visiting only known websites every time I use the internet is something I do unconsciously.

Uncontrollability (CTRL) - (Polites & Karahanna 2012)

CTRL1: I find it difficult to overrule my impulse to visit only known websites every time I use the internet.

CTRL2: I find it difficult to overcome my tendency to visit only known websites every time I use the internet.

CTRL3: It is difficult to control my tendency to visit only known websites every time I use the internet.

CTRL4: It is hard to restrain my urge to visit only known websites every time I use the internet.

Mental Efficiency (EFFC) - (Polites & Karahanna 2012)

EFFC1: I do not need to devote a lot of mental effort in deciding to visit only known websites every time I use the internet.

EFFC2: It would require effort not to visit only known websites every time I use the internet.

EFFC3: Choosing to visit only known websites every time I use the internet, requires little mental energy.

المنارة للاستشارات
www.manaraa.com

EFFC4: I have no need to think about visiting only known websites every time I use the internet.

Habit (HBT) - (Limayem et al. 2007)

HBT1: Visiting only known websites every time I use the internet has become automatic to me.

HBT2: Visiting only known websites every time I use the internet is natural to me.

HBT3: When using the internet, visiting only known websites is an obvious choice for me.

Affective Based Inertia (INTA) - (Polites & Karahanna 2012)

I continue to visit only known websites simply because

INTA1: because it would be stressful to change.

INTA2: because I am comfortable doing so.

INTA3: because I enjoy doing so.

Behavioral Based Inertia (INTB) - (Polites & Karahanna 2012)

I continue to visit only known websites simply because

INTB1: simply because it is what I have always done.

INTB2: simply because it is part of my normal routine.

INTB3: simply because I have done so regularly in the past.

المنارة للاستشارات
www.manaraa.com