MIND THE GAP: PERCEIVED SELF- EFFICACY, DOMAIN KNOWLEDGE AND THEIR EFFECTS ON RESPONSES TO A CYBERSECURITY COMPLIANCE MESSAGE

By

Ruth Jay Shillair

A DISSERTATION

Submitted to
Michigan State University
in partial fulfillment of the requirements
for the degree of

Information and Media- Doctor of Philosophy

2018

ABSTRACT

MIND THE GAP: PERCEIVED SELF- EFFICACY, DOMAIN KNOWLEDGE AND THEIR EFFECTS ON RESPONSES TO A CYBERSECURITY COMPLIANCE MESSAGE

By

Ruth Jay Shillair

This experimental research uses the framework of protection motivation theory (PMT) to understand user response to a cybersecurity message. The findings provide empirical evidence of the negative consequences that arise from a sense of self-efficacy in technology use when it is not accompanied by domain knowledge. This research found that even though cybersecurity messages motivated individuals to increase their protections, when shown how to perform a security task (checking for browser updates) there was a significant drop in self-efficacy. This would suggest that other factors, such as usability, are inhibiting motivated individuals from enacting security protections. This research consisted of three phases for rigor and to increase validity. First, the appropriateness of using PMT in this domain was tested through reviewing previous literature. Next, PMT a set of focus group transcripts (n=18 groups, ~10 people each) was explored to look for new constructs and emerging threats to improve scales. From the previous literature and focus group review, a research instrument was developed and tested. Next, a pilot study (n=70) was run using a college student sample. The results informed revisions of the research instrument, which was then used on a larger sample of online workers (n= 820). The model increases specificity in the use of PMT by adding new constructs including domain knowledge. Unexpectedly, the experimental stimulus (i.e., a cybersecurity compliance message with a training component) resulted in a significant decline in self-efficacy and lower protection motivation than the control group.

This was especially true for those with high self-efficacy pre-message who were lacking domain knowledge. As this response is quite different from other domains, where vicarious learning usually increases motivation, this finding has significant theoretical and practical implications. The lower motivation to protect, and the decline in self-efficacy after being shown how to complete a security task, suggests that usability is a critical issue in enacting protections. Previous experiences with cybersecurity threats, current protective actions, and protection habit strength were also explored. Implications for cybersecurity education efforts and improvements in cybersecurity usability are discussed.

This is dedicated to my husband, children and grandchildren, who have supported me and helped throughout the long process of research and writing.

ACKNOWLEDGEMENTS

I want to acknowledge the support of Michigan State University's College of Communication Arts & Sciences for their generous support though a research fellowship that funded most phases of this research: the development of a message, the pilot study and the full study. I also want to acknowledge the support of the National Science Foundation (Grant #1318885) for their support of the research project that collected the focus group materials. It is impossible to thank everyone who had a part in the completion of this research and supported the completion of my degree. Not only do I appreciate my husband, children, their spouses, and grandchildren who supported me with their encouragement and prayers, but also my friends and extended family who were a tremendous support.

I also want to thank my advisors and mentors, the individuals who believed in me and offered support and guidance. Special thanks to Dr. Wietske VanOsch, Dr. Nora Rifon, Dr. David Ewoldsen, and Dr. William Dutton. Also special thanks to Dr. Robert LaRose whose support and help was crucial in guiding me to this research.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1
Overview of this research:

1.1 The need for this research

When boarding an underground train in London, there is the ubiquitous recording, “mind the gap” as the crowds step on to the train. There is a gap between where they are and where they want to be–and that gap can be dangerous. However, if one wants to move forward they need to negotiate the gap; making many calculated adjustments as they move through the crowd to get safely on the train and eventually arrive at their destination. Today, computing systems are much like the train arriving at the station. They promise to take us to places where we want to go, and everyone is pressing forward to get on. However, there is a cybersecurity gap that is dangerous if we ignore it. In this research we are looking at the gaps in cybersecurity practices for end users-specifically the gap between what they feel they know (e.g., self-efficacy) and what they actually know (e.g., domain knowledge). We will explore how this gap influences attitudes about what threats are out there and how those threats could personally impact them. We will also explore how previous experiences with cyber security threats have impacted that self-efficacy/ domain knowledge gap. This gap may also impact beliefs about the efficacy of current protections and their ability to enact these protections. Then, we experimentally test a cybersecurity compliance message to see how the gap between self-efficacy and domain knowledge impact the response to a message. Finally, we discuss the causes of this gap and what changes can be made to increase the cyber safety of our systems.

The human factor continues to be the weak point in cybersecurity, even though there are constant advances in technological solutions to protect, detect intrusions, and mitigate damage to computer systems (Anderson & Agarwal, 2010; IBM Security, 2016). Sometimes stakeholder organizations (e.g., governments, educational coalitions, and

businesses) will use cybersecurity campaigns to make individuals aware of emerging threats and encourage better practices. These initiatives sponsor messages to encourage better personal cyber safety practices. This would include having stronger passwords, updating their software, and not falling for phishing emails. but little is known about how these messages impact end users. Unfortunately, the responses to these efforts are usually not encouraging with little change in user practices (Bada & Sasse, 2014). Complicating the issue is the wide range of training and domain knowledge that end users already have about cybersecurity issues and how that knowledge may be impacting their responses to cybersecurity compliance messages. Developing theoretically based and empirically tested frameworks to understand user response would help improve efficacy of these efforts tremendously.

Many groups and individual researchers have studied dimensions of the problem, using theoretical frameworks that come from disciplines as diverse as criminology, education, psychology, human-computer interaction (HCI), and health communications (Floyd, Prentice-Dunn, & Rogers, 2000; Holt, 2017; Randolph, 2017; Wiederhold, 2014). This marketplace of ideas has produced substantive research; however, there are still huge gaps in our understanding of how attitudes, experiences, and knowledge impact how individuals perceive a message and thus decide to respond to it. In order to make more effective initiatives, we need to have a better theoretical understanding of how end users process and respond to these messages. This is especially true since cybersecurity messages go out to large and diverse populations.

Cybersecurity is a very technical and rapidly changing domain, so it is unreasonable to expect novice users to understand its complexities. However, having a

basic grasp of threats and how to enact basic protections would allow users to better understand cybersecurity communications, and make informed decisions to protect themselves. Thus, this research explores the impact(s) of domain knowledge in the reaction to cybersecurity communications. Domain knowledge is defined as a basic understanding of online threats and personal protections that users can enact. This would include knowing the importance of having strong and unique passwords for accounts, updating one's software, having protective software (e.g., anti-virus or anti-malware), knowing why using public wi-fi might be dangerous, and not clicking on phishing emails. The operational measures used in this research to assess domain knowledge were developed by Pew Research (Pew Research Center, 2014).

Looking at domain knowledge alone will not allow a holistic understanding of the processes that individuals go through as they decide how to respond to a cyber based threat. Thus, I use domain knowledge as a new construct within a theoretical framework that is widely used in communications studies, the protection motivation theory (PMT; Floyd et al., 2000; Milne, Sheeran, & Orbell, 2006; Sommestad, Karlzén, & Hallberg, 2015). PMT posits that when individuals are confronted with a trigger (e.g., a message about a new cybersecurity threat), they go through a process of evaluating the likelihood of that threat harming them (i.e., threat vulnerability) and how seriously it would impact them if it did happen (i.e., threat severity), this process is called the threat appraisal process (Rogers, 1975). They also evaluate their options of how to respond to the threat, which would include how effective that response will be in protecting them (i.e., response efficacy) and how hard it will be to enact those protections (i.e., response cost). This process is called the coping appraisal process (Rogers, 1975). Another component to

the coping and threat appraisal process is the belief that they can indeed enact the coping measures and protect themselves (i.e., self-efficacy). Self-efficacy is usually seen as the key to individuals actually reaching the point where they intend to enact protections (i.e., protection motivation) and change their behavior (Ajzen, 2002; Bandura, 1977; Rogers, 1975). This process is not only based on careful evaluation of one's options, fear is also seen as an element that is triggered when individuals face a threat. This is especially true if self-efficacy is low, or if the potential solutions are not effective (e.g., low response efficacy). They may have maladaptive behaviors, instead of protecting themselves they may take even more risks or ignore the risk altogether (Maloney, Lapinski, & Witte, 2011; Witte & Allen, 2000). Thus, the PMT framework helps us understand complex psychological processes. This research explores if the additional construct of domain knowledge as part of the PMT processes will add even more understanding to responses to cybersecurity messages.

Understanding the impacts of low domain knowledge is especially important as many users have never had formal basic training in digital safety. Improved usability of computing devices has increased adoption of technology across age and economic backgrounds (Mchenry et al., 2016) thus reducing the digital divide of use or non-use of technology. However, there are growing concerns about the impacts of second level digital divides which are often caused by demographics such as age, economic background or education (Dutton & Reisdorf, 2016; Hargittai, 2002; Reisdorf & Groselj, 2015; Tsai, Shillair, & Cotten, 2017). The second level divide would include low domain knowledge about cyber threats and protections, which may put vulnerable populations at a higher risk. The "school of hard knocks" or personal experiences with online threats

might be a major source of domain knowledge for many people. Depending on the severity and outcomes of threat experiences, the PMT processes of threat and coping assessments may be impacted.

Previous research by leading scientists have brought great insights (e.g., (Anderson & Agarwal, 2010; Johnston & Warkentin, 2010; Liang & Xue, 2009). Yet, there is still a call for a more unified model that can produce effective strategies in information security compliance messages (Moody, Siponen, & Pahnila, 2018). This research is in response to this critical need for a better understanding of how users respond to compliance messages. Furthermore, it adds better understanding to how the interplay of past experiences, domain knowledge, and self-efficacy interact in the response to a cybersecurity compliance message. Gaining insights in these fields will help stakeholders to develop better interventions, design more effective messages, justify holistic cybersecurity education, and promote policies that will work towards a safer cyber secure environment for all.

1.2 The guiding research questions

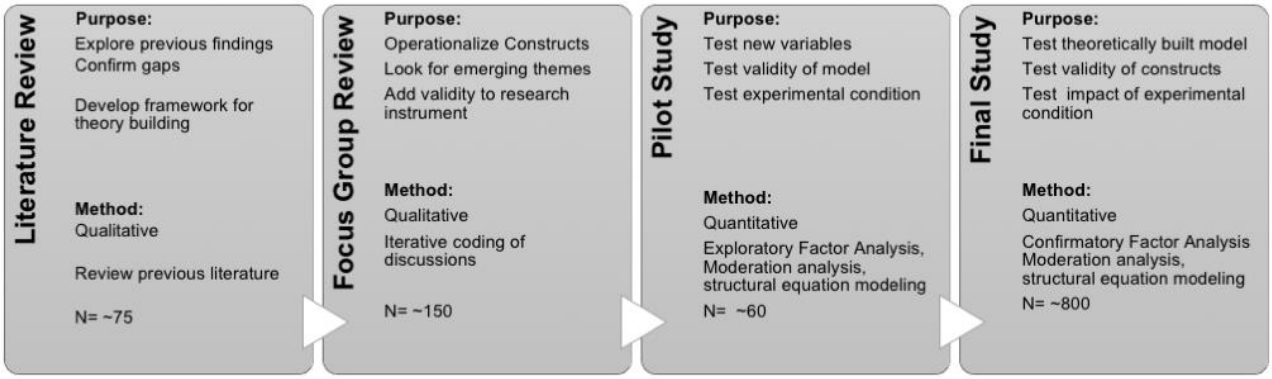
The new dimension, domain knowledge, will be center to the overarching research questions-

- Does domain knowledge impact self-efficacy in the cybersecurity domain?
- Does domain knowledge impact the threat appraisal and/or coping appraisal process in the cybersecurity domain?
- Does domain knowledge impact how users respond to a cybersecurity message?
- Does domain knowledge reduce fear in the cybersecurity domain?
- Does the gap between domain knowledge (what individuals actually know) and self-efficacy (what individuals feel confident in) help explain lack of response to cybersecurity initiatives?

1.3 Study overviews

This research takes a holistic approach to understanding end users and seeing how their attitudes, experiences, and knowledge work towards how a cybersecurity message could motivate them towards protection. This study is built upon previous studies that have focused on individual pieces of the message evaluation process and builds them together to construct a model that has a deeper understanding of users and thus, more predictive power. Development and testing of the theoretical model is done iteratively and using multiple methods to increase validity. Each step of the research is designed to inform future steps and test previous assumptions to increase rigor of the analysis. The phases of this research are illustrated in Figure 1.

Figure 1.1: Overview of study



1.3.1 Phase one: Literature review and theoretical development

First, previous literature in this domain was examined to explore what has already been done in this field, and where there are gaps. The research was then placed within the growing corpus of work on human behavior in cybersecurity, as well as communications research in a high-risk and technically complex domain. The insights from this review are in Chapter 2. I also discuss the hypotheses, an initial theoretical model, and the need for a multi-phase testing. This review process helped develop the overall research model and situate the hypotheses.

1.3.2 Phase two: Focus group review

The second phase of the research was to refine the research instrument and improve validity through a qualitative process. This was done through a review of focus group materials to look for how individuals express their domain knowledge and how that impacts their perceptions of and responses to cyber threats. A previous research project collaborated with a major credit union that helped organize eighteen focus groups, with each group having about ten individuals. They were organized by age cohort (i.e.,

Millennials, Baby Boomers, and Older Adults) and by use or non-use of online banking (e.g., high-risk online activities). The transcripts of these groups were examined for deeper insights into the coping and threat appraisal process of the participants. Statements that would indicate how their domain knowledge helped them make security decisions were of special interest. The semi-structured nature of the focus group protocol allowed free expression of the participants' experiences and attitudes.

During the analysis of the focus group material, additional salient literature was reviewed and included for better understanding of emerging concepts and themes. Details of the literature that helped form a framework for understanding the focus group material and for developing the experimental instrument are also in Chapter 3.

1.3.3 Phase three: Pilot study

The next phase of the research was a pilot study using the new items and constructs suggested by the focus group analysis and the literature review. This research instrument includes: a) a pre-exposure survey, b) exposure to an experimental stimulus (i.e., the control or training tutorial) in both a control and experimental condition, and c) a post-exposure survey. New scale items developed from the focus group review are also included. Operationalization of constructs in this unique domain of cybersecurity are refined. In order to test response using a message that would have as few external effects as possible (e.g., the message for the experiment is similar to one recently seen at work) A little known, but nonetheless important, issue is explored: software updates for browsers. The cybersecurity message about browser updates was developed after examining the focus groups transcripts. The final research instrument was then tested as a pilot study with 60 college students. The results were then evaluated to further refine

the testing instrument and the experimental compliance message. This chapter also addresses the theory behind using a tutorial for teaching a concept, the phases of usability testing for the prototype, and the various steps of data analyses.

1.3.4 Phase four: Large scale study

Before doing the large-scale study (n ~ 800 individuals) it was important to fully test all elements to improve validity and strength of the findings. After reviewing the data gathered from the pilot study, expert feedback was sought to improve the message. Major revisions of the experimental stimulus (i.e., the compliance tutorial) were done and further usability tests helped improve the final research instrument. Full details about the results of the pilot study and the subsequent modifications are in Chapter 5.

The large-scale study had a pre-test, an experimental stimulus, and a post-test. The pre-test assessed user characteristics (e.g., experiences, coping appraisal process, and threat appraisal process). Included in this pre-test were variables to find participants' self-efficacy, fear, and basic domain knowledge. Next, all participants were exposed to an experimental stimulus, a cybersecurity compliance message. Randomly selected participants were exposed to the compliance message with an additional component allowing vicarious learning to increase domain knowledge and self-efficacy. All participants, after exposure to the respective message, were given a post-test to find potential changes in the coping and threat appraisal process as well as their intention to enact protections. Any changes in attitudes towards protective actions were measured.

This phase of the study allowed enough participants for robust data analysis to test the various constructs and the experimental cybersecurity compliance message. The sample population was 800 MTurk workers. Details about the MTurk data collection

sample as well as results of confirmatory factor analysis, correlations, and structural equation modeling (SEM) and multi-group analysis are in Chapter 5. Further analysis of the large-scale data, including moderation analysis of key constructs is in Chapter 6. Chapter 7 discusses the implications of the findings of this research and limitations. Next steps for research in this field are also discussed.

1.4 The timeliness and potential impacts of this research

This research has theoretical value in that it probes how individuals process cybersecurity messages. Furthermore, it offers practical value in that better theoretical understanding can offer guidance to developing more effective interventions. This research is also novel, in that it is the first to examine the gap between perceived efficacy and actual domain knowledge and to theoretically understand how this gap may be impacting how users process and respond to cyber security messages.

The growing ubiquity of computing devices and the increased usability of interfaces often mixes ease of use with a perception of safety. Security and privacy controls are often obscured, and it is easy for end users to not be aware of the impacts of their actions. Although media reports and online safety programs in schools try to alert individuals to cybersecurity dangers, often these reports give few details to inform users what to do to protect themselves. Users can't be expected to be fully informed about all the potential threats and technical solutions (Wash & Rader, 2015). However, users are expected to invest money, time and effort in protecting themselves and the networks they use, with little support. Educational institutions often teach very little about cybersecurity, leaving it for "experts" (Mcgettrick, 2013). This research explores if helping end users to learn vicariously about security will increase their motivation and self-confidence in carrying out

protections. To achieve this goal, this research: explores current theoretical approaches in this environment, tests a typical cybersecurity compliance message and examines the reactions to the message. This allows us to gain a richer understanding of the challenge users face and gain insights into potential solutions. Thus, this research offers value in that it refines and tests a theoretical model empirically as well as testing a potential intervention. The goal is to help end users avoid the dangers of the gap between self-efficacy and domain knowledge.

WORKS CITED

WORKS CITED

Ajzen, I. (2002). Perceived Behavioral Control, Self-efficacy, Locus of Control, and the Theory of Planned Behavior. Journal of Applied Social Psychology, 32(4), 2918–2940. http://doi.org/10.1111/j.1559-1816.2002.tb00236.x

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

Bada, M., & Sasse, A. (2014). Cyber Security Awareness Campaigns Why do They Fail to Change Behaviour? Global Cyber Security Capacity Centre, (July). Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Awareness CampaignsDraftWorkingPaper.pdf

Bandura, A. (1977). Self-efficacy: Toward a Unifying Theory of Behavioral Change. Pyschological Review, 84(2), 191–215. http://doi.org/http://dx.doi.org/10.1037/0033-295X.84.2.191

Dutton, W. H., & Reisdorf, B. C. (2016). Cultural Divides and Digital Inequalities: Attitudes Shaping Internet and Social Media Divides. 44th Annual Telecommunication Policy Research Conference, (October 2016).

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. Journal of Applied Social Psychology, 2000, 30, 2, Pp. 407-429., 30,(2,), 407–429. http://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Hargittai, E. (2002). Second Level Digital Divide: Differences in People's Online Skills. First Monday, 7(4), 1–15. http://doi.org/10.5210/fm.v7i4.942

Holt, T. J. (2017). Cybercrime Through an Interdisciplinary Lens. (T. Holt, Ed.). New York, New York: Routledge.

IBM Security. (2016). Reviewing a Year of Serious Data Breaches , Major Attacks and New Vulnerabilities Analysis of Cyber Attack and Incident Data. Somers, NY.

Johnston, B. A. C., & Warkentin, M. (2010). Fear Appeals and Information Security

Behaviors: An Empirical Study. MIS Quarterly, 34(3), 549–566.

Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. MIS Quarterly, 33(1), 71–90. http://doi.org/Article

Maloney, E. K., Lapinski, M. K., & Witte, K. (2011). Fear Appeals and Persuasion: A Review and Update of the Extended Parallel Process Model. Social and Personality Psychology Compass. http://doi.org/10.1111/j.1751-9004.2011.00341.x

Mcgettrick, A. (2013). Toward Curricular Guidelines for Cybersecurity. Report of a Workshop on Cybersecurity Education and Training. ACM.

Mchenry, G., Carlson, E., Lewis, M., Goldberg, R., Goss, J., & Chen, C. (2016). The Digital Divide is Closing , Even as New Fissures Surface. Washington, D.C.

Milne, S., Sheeran, P., & Orbell, S. (2006). Prediction and Intervention in Health Related Behavior: A Meta Analytic Review of Protection Motivation Theory. Journal of Applied Social Psychology, 30(1), 106–143. http://doi.org/10.1111/j.1559-1816.2000.tb02308.x

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a Unified Model of Information Security Policy Compliance. MIS Quarterly, 42(1), 285–311. http://doi.org/10.25300/MISQ/2018/13853

Pew Research Center. (2014). Public Perceptions of Privacy and Security. Pew Research Center.

Randolph, A. B. (2017). Toward a More Secure HRIS: The Role of HCI and Unconscious Behavior. Transactions on Human-Computer Interaction, 9(1), 59–73.

Reisdorf, B. C., & Groselj, D. (2015). Internet (Non-)use Types and Motivational Access: Implications for Digital Inequalities Research. New Media & Society. http://doi.org/10.1177/1461444815621539

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. Journal of Psychology, 91(1), 93–114.

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A Meta-Analysis of Studies on

Protection Motivation Theory and Information Security Behaviour. International Journal of Information Security and Privacy, 9(1), 26–46. http://doi.org/10.4018/IJISP.2015010102

Tsai, H. S., Shillair, R., & Cotten, S. R. (2017). Social Support and “Playing Around.” Journal of Applied Gerontology, 36(1), 29–55. http://doi.org/10.1177/0733464815609440

Wash, R., & Rader, E. (2015). Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users. Eleventh Symposium On Usable Privacy and Security (SOUPS 2015), 309–325. Retrieved from https://www.usenix.org/conference/soups2015/proceedings/presentation/wash

Wiederhold, B. K. (2014). The Role of Psychology in Enhancing Cybersecurity. Cyberpsychology, Behavior and Social Networking, 17(3), 131–2. http://doi.org/10.1089/cyber.2014.1502

Witte, K., & Allen, M. (2000). A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns. Health Education & Behavior, 27(5), 591–615. http://doi.org/10.1177/109019810002700506

Chapter 2
Literature review, theory development and hypotheses

2.1 Introduction

Multiple stakeholders are interested in improving the cybersecurity practices of individuals. Governments, companies and all types of organizations want their employees to not only follow mandatory safety protocols, but to have a positive, proactive attitude towards cybersecurity (e.g., SANS security training for employees). Many of these organizations routinely send out cybersecurity compliance messages, telling individuals how to better protect themselves and the organization. Yet, little is known how domain knowledge, previous experiences, self-efficacy, or other characteristics might contribute to their response to these messages. This chapter will review research that examines the process of response to cybersecurity communications, where there are gaps, and detail how this research fits in to the overall narrative of communications research in cybersecurity.

The domain of cybersecurity communications research is a relatively nascent domain. For example, a Google Scholar search of “cybersecurity communications” in May of 2018 yielded only 101 results, all but a handful of which were technical papers geared towards systems solutions. A search for “cyber security communications” also yielded only 67 results. Using the terms “cybersecurity” and “communications” (not together) yielded over 37,000 results, but in checking the first 150 there were only a few that were dealing with the human aspects of cybersecurity, and none of the articles were looking specifically at responses to cybersecurity communications. In other domains, there is substantive research on communication processes. A similar Google Scholar search for “health communications” yielded over 37,000 results, and the first 100 were all specifically looking at the health communications process. Thus, a review of previous research in

understanding how individuals process cybersecurity communications will necessitate exploring salient literature from closely related domains. However, this should be done with caution, as there is little empirical evidence that individuals process messages coming from different domains in the same manner.

2.2 Methods

A review of salient literature was undertaken to improve theoretical understanding of the responses to cybersecurity threats, and to increase validity in developing a model that could bring better understanding to how individuals respond to a cybersecurity compliance message. This process included preliminary research using five major databases: Academic One File, Ebsco Host, Proquest, JStor, and Google Scholar. Starting with broad terms such as, “online safety”, “cybersecurity”, and “cyber security” there were thousands of articles, predominantly about technical solutions to cybersecurity with a small percentage about the human dimensions of cybersecurity. A common concept throughout many human-centered cybersecurity studies is the need for individuals to have a sense of self-efficacy to be willing to enact protections (Boss, Galletta, Lowry, Moody, & Polak, 2015; Hanus & Wu, 2015; Jansen & van Schaik, 2017; Liang & Xue, 2010; Sommestad, Karlzén, & Hallberg, 2015; Vance, Siponen, & Pahnila, 2012). This indicates that the starting point should be to come to a better understanding of self-efficacy. Self-efficacy is very broadly defined (Bandura, 1971). Thus, to better specify its function in this domain will offer both theoretical and practical insights. Following the taxonomy by Cooper (1988), this literature review has a focus on the theories under consideration, the goal of identification of central issues, a perspective that is neutral, coverage that is representational, conceptually organized, and geared for an

audience of scholars and practitioners. The concepts proposed by this review will be tested both qualitatively and empirically. As the research unfolds, the model will be further refined and tested. First, I will discuss a theory widely used in risk or threat communications, protection motivation theory (PMT), and discuss why this may be an appropriate framework for examining cybersecurity communications. Then, I will explain the proposed new construct of domain knowledge and how it may be interacting with self-efficacy in the threat appraisal and coping appraisal process. Finally, I discuss how this construct adds specificity and can help inform and add more power to the mode and how I propose to test the revised model. Thus, I demonstrate how this research contributes to theory. Through the process of examining the model I will explain the basis for my hypotheses for the experiment.

2.3 Theoretical framework for cybersecurity risk communication

Developing, or choosing, a theoretical framework to understand a process as complex as cybersecurity communications starts with first deciding the research questions and the overall goal of the research. The goal of a cybersecurity compliance message is to persuade individuals take protective action. The message seeks to inform and motivate individuals to behaviors that will protect them and the networks or systems they use. There normally is a gap in time from when the message is given and when the individual makes the decision to protect themselves, so we need a theoretical framework that deals with not only motivation but also behavioral intentions.

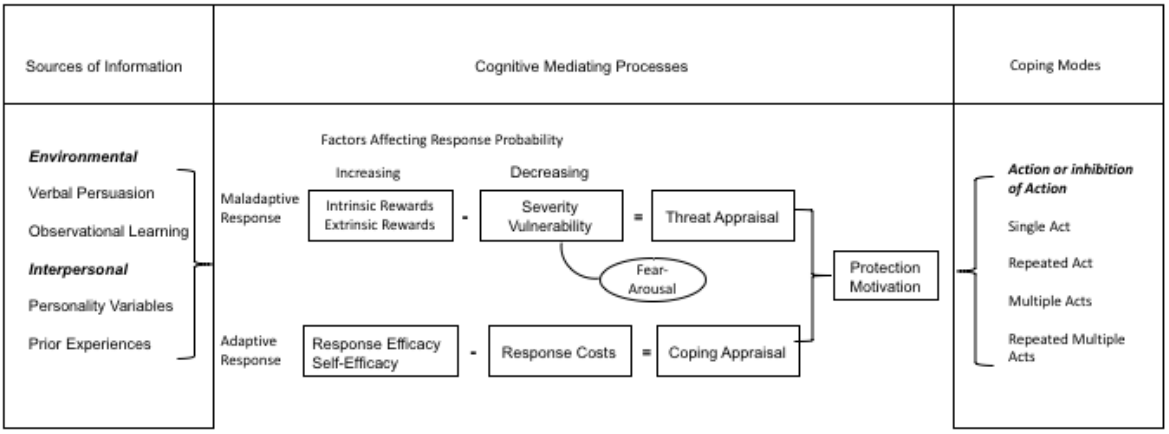
The theory of reasoned action is a framework that deals specifically with how intentions are connected to behaviors. According to Fishbein and Ajzen (1975), “when appropriately assessed (and barring unforeseen events), intentions serve as the primary

determinants of overt behavior" (pg. 511). In this theory they saw attitudes towards a behavior and subjective norms as primary determinants of the behavior. Later, Azjen refined theory of reasoned action to include perceived behavioral control and called it the theory of planned behavior (TPB; Ajzen, 2005; Madden, Ellen, & Ajzen, 1992). The framework of predicting behaviors through intentions was based on earlier learning theories and has been tested for over forty years and is validated in numerous domains (Ajzen, 2002; Armitage & Conner, 2001; Icek Ajzen, Sparks, Ajzen, & Hall-box, 2002; Lee, 2009; Rhodes & Courneya, 2003). TPB looks at how attitudes, social norms and perceived behavioral control work together to help individuals plan to carry out and perform a behavior.

With the TPB in mind, messages are designed that try to encourage protective behaviors. Sometimes these messages might try to increase a sense of imminent or serious threat, these are known as fear appeals (Rogers, 1975). Examples of fear appeals are advertisements warning people of the dangers of smoking or messages encouraging frequent exercise. Cybersecurity compliance messages fall in to this category as they remind individuals of the threats they face and the need to make a change in their behavior. Fear appeals are strongly tied to TRA and TPB as they seek to change behavioral intentions, often trying to improve attitudes towards the desired behavior (e.g., subjective norms) and improving the sense of perceived behavioral control (Lee, Larose, & Rifon, 2008). Researchers have frequently used the protection motivation theory (PMT) to understand psychological responses to fear appeals (Rogers, 1975; Tanner, Day, & Crask, 1989). This theory, as postulated by (Rogers, 1975), envisions how an individual who perceives a threat will make a cognitive evaluation of the implications of that threat

and potential responses to that threat. This is different than other persuasive communications theories, such as the elaboration likelihood model, where the goal is to change attitudes towards an action (Briñol & Petty, 2015; Carpenter, 2015). ELM is an appropriate model in studying behaviors where there might be a perceived positive aspect to a behavior that should be changed for the individual's benefit. For example, some people see smoking as relaxing, socially beneficial and culturally acceptable. A message to persuade them to give up smoking would have to help change those attitudes and give them the confidence to achieve that goal. In cybersecurity, individuals' goals are fairly universal in wanting to be safe and protected from cyber criminals. The goal of cybersecurity messages is often to inform individuals of emerging threats and motivate them to take protective actions. Figure 2.1 is adapted from Maddux and Rogers (1983) seminal work on protection motivation theory.

Figure 2.1: Protection motivation theory*



*(Rippetoe & Rogers, 1987)

2.3.1 The threat appraisal process

PMT posits that individuals' first reaction to a threat is the threat appraisal process, which includes the constructs of threat severity (e.g., how severe are the consequences) and threat susceptibility (e.g., how likely the threat is to happen to the individual). Threat severity would include seeing impacts from the threat as quite serious to one's privacy, finances, mental condition, or physical safety. Not all individuals will see the same potential outcome as having the same severity. For example, say someone downloads ransomware and their computer is locked up. They get a message demanding money to access their files. Some people would be devastated, they may have family pictures, important work files, or other irreplaceable items on their computers. Others might not have much on the computer that they care about, so they would not have as serious a personal impact for the same event. There are those who routinely back up files and keep them on a disconnected drive, so the ransomware would be annoying but not that serious.

Threat vulnerability is how likely an individual is to encounter a threat. A common example is a phishing email. Most individuals who have an email account have seen at least one of these, so vulnerability is quite high to this type of threat. There are other threats where people are vulnerable, but they might not realize it. For example, many types of malware can be delivered just by visiting a compromised web page. Legitimate web pages, including news sites, in the past have been infected through ads running in the background. These ads can put malware on computers without individuals clicking on anything within the site. So, there are both vulnerabilities that are well known, and others that not as many people are aware of. A message may try to arouse awareness to start the threat appraisal process.

2.3.2 The coping appraisal process

The second process is the coping appraisal process, which includes the constructs of response efficacy (e.g., how effective the response), response cost (e.g., how difficult or expensive the solution is), and coping self-efficacy (e.g., if the individual thinks they have the ability to carry out a task). Response efficacy includes how effective individuals feel the protective action will be to protect again the threat. Software that protects against viruses and malware is a common solution to protect operating systems from common threats. However, not all software has a good reputation for actually protecting. Some virus/ malware protection software is suspected of harboring weaknesses that criminals or national level actors control. If individuals are suspicious of the response efficacy of a protective action, they are less likely to use it.

The response cost is more than just the monetary cost of implementing a protective solution. It can also include how much effort a response takes to enact, or the inconvenience that it may cause. Software updates are notorious for sometimes taking quite a long time to download, or when installed causing features that previously worked to not work (Vaniea, Rader, & Wash, 2014). Response cost works opposite to response efficacy in that it makes the individual less likely to enact a protection if they feel the cost is greater than the benefit.

Coping self-efficacy, the belief that one can enact the protections successfully is also a positive factor in adopting protections. Self-efficacy will be looked at more in depth later in this chapter because it is such an important part of the PMT model and it is impacted by the proposed additions to the model.

2.3.3 Protection Motivation

If protection motivation is triggered, then protective action would be generally expected and individuals would evaluate their course of action for their best interest (Ajzen, 2002). This concept of protection motivation builds upon TRA and TPB that were discussed earlier in this chapter. It is the intention to follow through and take protective action. However, this process relies heavily on individuals cognitively processing a threat and having a sense of control or self-efficacy in a situation (Ajzen, 2002). Over many studies, protection motivation was supported as a predictor to protective actions with it having the strong predicative power not only for single acts, but also a predictor for repeated acts (Tannenbaum, Heiler, & Zimmerman, 2015).

2.3.4 Fear

Despite the wide use of this theory, it was observed that while some messages triggered protection motivation in some individuals, the same message may trigger a negative, or maladaptive response in another. When fear was strong, individuals often acted unpredictably, and not always in their best interests (Witte, 1994). This phenomenon was explored with the extended parallel processing model (EPPM; Lewis, Watson, & White, 2013; Maloney, Lapinski, & Witte, 2011; Witte, 1994). The EPPM visualizes response to threats as dual process, where there is both a cognitive process and an emotive process. The cognitive processing of a threat (i.e., threat response) allows for the individual to make a response based on reason and their knowledge of the threat, the needed response and the efficacy of their response, which was named danger control. At the same time, there is an emotive reaction to the threat (i.e., fear response). This fear reaction is not based on cognitive reasoning to reach the best options, but an emotive

reaction to the threat, the immediate goal is fear control. The fear control response can include a maladaptive action that might actually increase the risk, or just ignoring the threat altogether (Maloney et al., 2011; Roskos-Ewoldsen, Yu, & Rhodes, 2004; Tanner et al., 1989). Messages that increased the threat response, but also include higher coping self-efficacy and belief in response efficacy, brought much higher intentions to protect than those that solely increased the fear response (Roskos-Ewoldsen et al., 2004).

All of these previously mentioned studies on cognitive versus emotive processing are in the health communications domain. Because research in response to cybersecurity threats is still in its infancy, researchers have looked to health communication studies since there are many psychological similarities (e.g., protective actions) and health communication studies are more theoretically developed (Anderson & Agarwal, 2010; Floyd, Prentice-Dunn, & Rogers, 2000). Therefore, cyber security researchers frequently use PMT to understand response to threats (Boss et al., 2015; Shillair et al., 2015; Vance et al., 2012). Despite the cybersecurity domain having many similarities to health communications, there are some striking differences. One of these is the technological complexity of cybersecurity and despite the fact that technology is widely used, only a small portion of the population has more than a rudimentary understanding of how cyber threats work (Mcgettrick, 2013; Olmstead & Smith, 2017). This lack of knowledge may be impacting individual's ability to cognitively process a message, thus it would help explain the difficulty in getting improved behaviors (Bada & Sasse, 2014).

2.4 Domain knowledge as a proposed construct of PMT

When an individual is faced with threat message they need to have at least some understanding of the domain to be able to assess if the threat is valid and to respond

cognitively rather than simply emotionally react (Ajzen et al., 2002; Witte & Allen, 2000). Even though it would be unrealistic to expect the novice user to understand the technical details of emerging threats, would having a basic overview of how they can protect themselves have an impact on how they understand and respond to a message? For this research, as mentioned in Chapter 1, the definition of domain knowledge is the basic understanding of online threats and the basic tools that are available for the end user to protect themselves. These were operationalized by the Pew Internet Research Project (Olmstead & Smith, 2017). The ten items include: being able to recognize a strong password, being able to identify the dangers of an open wifi and recognizing a two-factor log-in system. Sample items are in Appendix 2.1.

The PMT model as proposed by Maddux and Rogers (1983) includes dimension of "previous experiences" as a potential independent variable that impacts threat processing. Domain knowledge is a type of "previous experience" can be increased through communication and educational efforts. For example, password strength, unlike some other security behaviors, has been widely discussed. News reports that talk about data breaches frequently mention the importance of strong passwords. Programs that teach online safety in schools and the workplace also start with the importance of a strong password (e.g., staysafeonline.org). Many web services now have contextual demonstrations on password strength and require a certain length or variety of characters. For example, as people are setting up a new password, some services have a little red, yellow or green bar as it is entered to indicate password strength. Thus, domain knowledge fits within the model and yet adds specificity in the dynamic field of cybersecurity. This research, using the PMT framework, will explore how domain

knowledge impacts the processing of cybersecurity messages and will specifically look at the gap between the dimension of self-efficacy and domain knowledge and how that impacts users' responses to cyber security messages.

2.5 The PMT process in cybersecurity: Hypotheses

2.5.1 Domain knowledge

As mentioned before, Witte's (1994) EPPM posited that individuals processed a message both emotively and cognitively. The cognitive process, which resulted in danger control looked at how to proactively respond to the danger. I posit that domain knowledge is an important part of the cognitive processing of danger. By knowing the basics of how cyber threats operate and what protective options are available, this should lower fear levels and increase self-confidence. Also, individuals should be more likely to habitually enact protections.

Nabi et al. (2008), tested this concept in the health domain and found that when individuals had domain knowledge (e.g., knew how to self-screen for cancer) they were able to cognitively process the protective messages and they would follow through on behavioral intentions. On the other hand, those who just had a vague idea of protective actions (e.g., didn't know how to self-screen for cancer) would either 1) not respond positively to the message, or 2) not follow through even if they claimed to be motivated to take a protection action. This informative study was in the health domain (i.e., cancer self-screening) and these concepts have not been testing in the cyber security domain up to this point.

Based on these previous studies, domain knowledge should increase compliance and reduce fear and resistance.

Domain knowledge: Since having knowledge about a topic increases a sense of self-efficacy, it also decreases fear. Thus, I hypothesize, as **domain knowledge** increases-

self-efficacy will increase (H1a)

fear will decrease (H1b)

Also, knowing about how to enact protections will make the impact of threats seem less severe and even though there may be an increased awareness of the wide range of threats, confidence in one's ability to enact protections will decrease the sense of severity and vulnerability. I hypothesize, as **domain knowledge** increases-

threat severity will decrease (H1c)

threat vulnerability will decrease (H1d)

2.5.2 Time online

It is one thing to know about an issue, it is another thing to act upon it. Often cybersecurity safety decisions are made in a millisecond rather than a careful deliberation of what is the best course of action. Fazio (1990), explored how attitudes impacted the processing and subsequent impact of messages, especially as they pertain to behavioral changes. Fazio found that a key to understanding behavioral change was that some decisions were cognitive and allowed individuals to think rationally about their options and follow through on their intentions. When decisions were under time pressure, the individual would respond to whatever attitude came first to mind (e.g., attitude accessibility). The motivation and opportunity as determinants (MODE) model found that along with time to process a response to a message, the motivation (e.g., caring about an outcome) was crucial to how messages were processed (Ewoldsen, Rhodes, & Fazio, 2015).

In cybersecurity, the purpose for being online might be tied to motivation for enacting protections. For example, if an individual is working on their computer, doing banking transactions or shopping they may be more careful about security than when someone is simply going online to watch a video or read the news. The dilemma is that often the same person will go on the same machine for widely varying reasons. While they are focused on work they may be very careful, but when they go back on the computer later in the evening they may just be seeking relaxation, it is unknown how the impacts of purpose for use may be interacting with protection motivation. Thus, the more they are online, even for work, the more likely they are to be exposed to common threats. However, these experiences may cause them to search for more information. The construct, time online, is the difference between overall time online for work beyond the time online for relaxation.

Time online: Thus, the more time an individual is investing online in work or productive pursuits, the more likely they are to value the information on their computing device. Thus, they will seek more information about how to protect themselves, also increasing their self-efficacy. Thus, I hypothesize that as **time online** increases-

domain knowledge will increase (H2a)

self-efficacy will increase (H2b)

Also, as they are purposefully online they will be more careful about their actions and have fewer experiences with common threats.

I hypothesize that as **time online** increases-

experiences with common threats will decrease (H2c)

Since the individual doing primarily work online would be more careful they will be more aware of the likelihood that they might be attacked (i.e., threat vulnerability) and if they do encounter threats these would be of more consequence.

I hypothesize that as **time online** increases-

threat severity will increase (H2d)

threat vulnerability will increase (H2e)

2.5.3 Previous threat experiences as a type of domain knowledge

Not everyone has had the benefit of formal training about online threats and how to protect themselves. Domain knowledge could be acquired through learning from friends and family or through the "school of hard knocks," personal experiences with online threats. These can be as common as accidently opening a phishing email or it could be something as serious as having someone take control of one's camera and being threatened. The impact of previous threats within the PMT framework was explored in the ordered protection model (OPM: Eppright, Tanner, & Hunt, 1994). This research, in the health domain, saw previous experiences as impacting the threat evaluation processes. However, pseudo domain knowledge gained through making poor choices can lead to future poor choices. Tanner, Hunt, and Eppright (1991) found if fear was triggered in the absence of self-efficacy then a maladaptive response would ensue, and this response tended to be repeated.

In cybersecurity, previous experiences are not all created equal. As just mentioned, a minor issue (e.g. clicking on a phishing email) may lead to the individual changing their password, then seeking out more information to make sure they are safe. Subsequently, they would be more vigilant in avoiding phishing links. On the other hand,

an experience with a serious threat such as having one's camera hacked may lead to a feeling of loss of control, and not knowing how the breech started. Thus, a lowered belief in the effectiveness of protective actions (i.e., lower response efficacy). Previous research showed that experiences with serious threats led to lower self-efficacy and a lack of trust in solutions (Shillair, 2015). These negative experiences may also trigger fear, the PMT construct that Witte (1994) saw as triggering an emotional response to a threat rather than a cognitive response. Given that both common and serious threats could potentially trigger fear, self -doubt, and a lower trust in technical solutions, a fear process would be triggered. According to the EPPM this may lead to a heightened threat appraisal process, but a lower coping appraisal process. Thus, we will include previous threat experiences, both serious and common as part of the model to explore how this type of domain knowledge impacts the threat and coping appraisal process.

2.5.3.1 Common threat experiences:

Thus, exposure to common threats may undermine confidence in being able to protect oneself (i.e., self-efficacy). At the same time the awareness of a gap in one's knowledge may spur individuals to seek for more information and ultimately increase their domain efficacy. As exposure to **common threat experiences** increases, I hypothesize that-

self-efficacy will decrease (H3a)

domain knowledge will increase (H3b)

Although exposure to more common threats will naturally increase the awareness of vulnerability, dealing with these threats may at the same time lull individuals into a sense of false security, actually making a sense of the seriousness of the threat to go down.

I hypothesize that as **common threat experiences** increase-

threat severity will decrease (H3c)

threat vulnerability will increase (H3d)

The more an individual has to deal with threat violations, the more frustrated they may become in carrying out protections as they feel they are not working. Thus, the attitude towards response cost will increase and response efficacy will decrease.

I hypothesize that as **common threat experiences** increase-

response cost will increase (H3e)

response efficacy will decrease (H3f)

Since the individuals with experiences with common threat experiences may have poor cyber safety practices I also hypothesize that as **common threat experiences** increase-

experiences with serious threats will increase (H3g)

2.5.3.2 Serious threat experiences:

In serious cybersecurity attacks it is not always easy to see who is really behind an attack. Clicking on a phishing email may be easy to understand for the novice user. Understanding how serious malware got on one's computer is harder to understand. The loss of control may undermine their confidence in their ability to protect themselves. Finding solutions may be difficult as they may not know even the terminology to look for solutions. It may be embarrassing to ask for help. Yet, continuing to use computers for work, entertainment, and to communicate is almost required in order not to be marginalized in today's digital society. Thus, ignoring the threat to normalize their lives

(Germeni & Schulz, 2014), it is easy to see that serious threats may cause maladaptive behavior.

Thus, as exposure to serious threat experiences increases, individuals feeling of being able to protect themselves will decrease. Major threats are rather ambiguous and often technically hard to understand so it would not naturally lead to finding out more information about the threat. Also, major threat experiences are sometimes not the fault of the individual, it may be the fault of a company or remote party that didn't protect personal information. This would lead to a further sense of loss of control. Thus, I hypothesize that as **serious threat experiences** increase-

self-efficacy will decrease (H4a)

domain knowledge will not change (H4b)

The sense of being vulnerable would naturally increase after experiencing a serious threat. However, having a serious threat happen and being able to continue to use computers and interact online would involve a mental mitigation of the threat, thus perception of severity would go down. Thus, I also hypothesize that as **serious threat experiences** increase-

threat severity will decrease (H4c)

threat vulnerability will increase (H4d)

Dealing with the aftermath of a serious threat violation can be tedious. For example, a stolen identity could lead to fraud and fighting to restore one's credit rating. Since enacting protections on one's computer is comparatively easy, perceptions of response cost will go down. However, because of the failure of previous protections the

belief that protection solutions are effective would also go down. Thus, I hypothesize that as **serious threat experiences** increase-

response cost will decrease (H4e)

response efficacy will decrease (H4f)

2.5.4 The threat appraisal process

The threat appraisal process itself is different in cybersecurity than in other domains such as health communications, and yet there are many similarities. Even though the domain is quite different from health, the emotional impact and response to threats are similar. I have already discussed how domain knowledge, time online, and previous experiences with threats might impact fear, and trigger the emotive rather than the cognitive processing of a threat. If perceptions threat severity is too high, then individuals respond with increased fear and a sense of being vulnerable. Thus, I hypothesize that as **threat severity** increase-

Fear will increase (H5a)

Also, as **threat vulnerability** increases-

Fear will increase (H6a)

2.5.5 The coping appraisal process

The coping appraisal process in cybersecurity often includes having to learn new processes and apply new protections. This takes time, effort and keeps people away from the task that they wanted to do. Thus, only if individuals feel that the response is efficacious will they actually use it. Also, if it is too difficult to use, or takes too much time (i.e., response cost) then they won't enact that protection. Thus, I hypothesize that as **response cost** increases-

Protection motivation will go down (H6a)

And as **response efficacy** increases-

Protection motivation will increase (H7a)

2.5.6 Self-efficacy as central to the coping process

Bandura and others explored many different facets of self-efficacy. The perception of efficacy is crucial to behavioral change, it provides a sense of confidence and control (Bandura, 2012). The concept of self-efficacy is widely discussed in numerous domains. It is seen as an essential component to learning and foundational for human agency and education (Bandura, 2001; Bandura, 1989, 1991; Deture, 2004), behavioral change (Ajzen, 2002; Armitage & Conner, 2001; Bandura, 1977), technology acceptance (Hsu & Chiu, 2004; Liang & Xue, 2009), participation in online political action (Di Gennaro & Dutton, 2006), successful aging (Tsai, Shillair, Cotten, Winstead, & Yost, 2015; Yagil, Cohen, & Beer, 2013), entrepreneurship (van Osch & Coursaris, 2010), self-care in the health domain (Roskos-Ewoldsen et al., 2004), and important for following cyber security practices (Arachchilage & Love, 2014; Boehmer, LaRose, Rifon, Alhabash, & Cotten, 2015; Vance et al., 2012; Waddell, McLaughlin, LaRose, Rifon, & Wirth-Hawkins, 2014). Self-efficacy is usually encouraged in the teaching/ communication process. Increasing individuals' confidence and perceptions of efficacy is used widely in health communication, safety communication, behavioral change programs, and education (Bandura, 1977, 1992; Deture, 2004; Ajzen et al., 2002). Self-efficacy can be somewhat transient, not just a blanket attitude, it responds to the environment and encouragement of others, and it can be very domain specific (Bandura, 1977, 2001, 2012). Self-efficacy

is recognized as being a multi-dimensional, especially in the complex environment of computer use (Agarwal, Sambamurthy, & Stair, 2000).

Self-efficacy increases as individuals successfully perform tasks and use their devices (Bandura, 2012). Improved usability in computing devices have created increased usage across many demographics. However, increased self-efficacy can lead to higher risk taking (Cox, 2012; Silvia, 2003). If the individual truly doesn't understand potential threats, but thinks that they do, risk taking could have disastrous results. This attitude can lead to inattentiveness and carelessness among those who think they know what they are doing (Workman, Bommer, & Straub, 2008). This risk taking can also take the form of ignoring a risk. Silvia (2003), found that levels of self-efficacy were tied to levels of declared interest. When levels of self-efficacy were low, participants would feel overwhelmed by a potential task and claim to not be interested in it. At the same time, participants who had extremely high self-efficacy found the task boring and were not interested. This study indicated that the benefits of self-efficacy might be much like a Gaussian distribution, with those on either end being less likely to carry out tasks they deem too difficult, or too boring.

The combination of domain knowledge and self-efficacy in other domains is a powerful combination. In the health domain, Nabi, Roskos-Ewoldsen, and Carpentier, (2008) found that individuals who had high perceived efficacy claim that they would take protective actions, but only those who also had domain specific knowledge enacted those protective measures. This combination is found as important in health communication research, and as a result there is a growing emphasis on increasing health literacy to improve patient outcomes (Bauer, Thielke, Katon, Unützer, & Areán, 2014; Ellis, Mullan,

Worsley, & Pai, 2012; Montaño & Kasprzyk, 2008). Surprisingly, there is not as widespread an effort in cybersecurity (Bauer et al., 2014; Ellis et al., 2012). Perhaps part of this problem is the complexity of cybersecurity.

In all of these approaches that examine response to perceived threat, coping self-efficacy is a crucial component to the intention to comply with the safety or security steps in the domains tested. The higher the coping self-efficacy an individual has, the more they are able to cognitively process a message and respond positively to it (Roskos-Ewoldsen et al., 2004). However, the construct of self-efficacy is often measured through questions of self-perceptions rather than a test of actual knowledge about a subject (i.e., domain knowledge). Certainly, having the confidence to carry out a procedure is an important component to actually doing it (Ajzen, 2002; Bandura, 1977); but individuals may claim self-efficacy, that they know how to do a task, when they really don't know how to do it (Nabi et al., 2008).

Self-efficacy: As just discussed, self-efficacy helps individuals see threats as less overwhelming, but rather as a challenge that they can conquer. Thus, I hypothesize that as **self-efficacy** increases

threat severity will decrease (H8a)

threat vulnerability will decrease (H8b)

Also, self-efficacy would make response cost seem less as they feel they can implement protections and more confident that the actions they take will be successful. Thus, I hypothesize that as **self-efficacy** increases-

response cost will decrease (H8c)

response efficacy will increase (H8d)

fear will decrease (H8e)

2.6 The impact of a message to increase domain knowledge

2.6.1 Using a message as a trigger for protection motivation

The triggers to the protection motivation process have been studied by many researchers for many decades. Often these triggers are something that happens to a person personally. They may find a lump or have a persistent cough that triggers them to take protective action and go to a doctor. However, wider efforts to change behaviors are often based on communications and messages. For example, Floyd et al., (2000) looked at over 65 studies that spanned 20 years and engaged over 30,000 participants to find that “PMT components may be useful for individual and community interventions.” Thus, PMT has been used in cybersecurity compliance research to better understand and predict characteristics and environments that will help increase security compliance (Sommestad et al., 2015). A message that is designed with a deep understanding of the PMT process has the potential to be more efficacious and truly motivate individuals to safer practices. This means not triggering fear, but rather triggering a cognitive protective determination.

2.6.2 Using a message to increase domain knowledge

As we previously discussed, there are many negative outcomes tied to lower domain knowledge. Not understanding cybersecurity protections is likely to lead to minimization of threat, in order to continue without change and normalize their online interactions (e.g., Germeni & Schulz, 2014 in health crisis). Also, lack of familiarity with protective tools will often lead to excusing lack of use by claiming they are too difficult

(Silvia, 2003). Lower domain knowledge will make processing of the message more difficult and more likely to result in a maladaptive response (Nabi et al., 2008).

Domain knowledge can be gained through educational efforts and vicarious experiences (Bandura, 1977). Those who are able to learn vicariously what to do to protect themselves (e.g., Bandura's social cognitive theory) could overcome their deficiencies in domain knowledge. A carefully designed message could not only trigger the protection motivation process, it could also increase domain knowledge.

2.6.3 Potential impacts of a message

A message that triggers an awareness of a threat, but at the same time increases domain knowledge has to the potential to trigger protection motivation while helping prevent many potential negative outcomes. It would increase knowledge about an issue and inform users of effective and achievable outcomes. If an individual's self-efficacy level is low, based on a realistic appraisal of their knowledge and attitudes, then self-efficacy should go up when given clear and specific details of how to do a task. Thus, being presented with a message that first arouses the threat appraisal, then affirms the coping appraisal process and then being given the details on how to perform the specific task should increase domain knowledge and ultimately increase protection motivation.

2.7 A test of the theory

In this research I present a cybersecurity compliance message in an experimental form. All participants are first given a survey to appraise their domain knowledge, their previous experiences, and how much time they spend online both for work and pleasure. Then, the PMT constructs are measured including fear and self-efficacy. The participants are asked which of four browsers they use the most (Chrome, Firefox, Internet Explorer,

or Safari). Then all participants are presented with a short video that discusses the importance of browser software updates. This is presented by a professional voice actress using screen shots and clip art typical of a cybersecurity awareness video. The control condition has this video alone. The experimental (training) condition has an additional part to their video that includes a clear demonstration of how to perform the security task. This is done using the browser that they most frequently use, so it is contextual and allows a familiar setting to learn about the safety task. It also allows the participants to learn vicariously as they see each step of the process. After watching the video, the participants answer questions about their protection motivation and it measures the potential changes in fear, self-efficacy, response efficacy, and response cost.

Full details of the message development are in Chapter 4 and the revision process is in Chapter 5. Fear is measured before and after the message as this is the attitude that overrides the cognitive, danger control, process and triggers the fear control process as described in EPPM (Nabi et al., 2008; Witte, 1994). The elements of the coping appraisal process are also measured after being exposed to the message, these are: self-efficacy, response efficacy, and response cost.

Post message control condition: Since the message includes awareness of a cybersecurity risk that they may not be familiar with, the message may increase fear somewhat. The message discusses the importance of performing this task, so beliefs in response efficacy should go up. Thus, I hypothesize- for those in the **control condition**-

Post **fear** will be strongly correlated to from pre-message **fear** (H9a)

As **fear** levels increase, **protection motivation** will decrease (H9b)

As the message doesn't show how to perform the task, but does address it specifically, self-efficacy should increase. Also, as self-efficacy increases protection motivation should also increase. Thus, for those in the **control condition-**

Post **self-efficacy** will increase from pre-message **self-efficacy** (H10a)

As post **self-efficacy** measures increase, **protection motivation** will increase (H10b)

The message encourages software updates and tells the importance of having one's browser in the latest version. Since the strengths of this task are given and not any details on how to enact this protection, Participants will probably agree that this is effective and after hearing the dangers of out-of-date browser software the response cost of updating them will seem fairly low. Thus, I hypothesize that for those in the **control condition-**

Post **response cost** measures will be weakened (e.g., not as strong a correlation) from pre-message **response cost** (H11a)

As post **response cost** measures increase, **protection motivation** will decrease (H11b)

Post **response efficacy** measures will increase from pre-**response efficacy** (H12a)

As post **response efficacy** measures increase, **protection motivation** will also increase (H12b)

Experimental (training) condition: Since the experimental condition includes clear details on how to protect themselves, I expect that participants will increase in their domain knowledge and that will reduce fear. This is because once the individuals see

how to actually perform the task, they be reassured and fear should be less of a problem. Thus, I hypothesize for those in the **experimental (e.g., training) condition**-

Post **fear** measures to pre-**fear** measures will have less correlation than in the control condition (H9d)

As post-**fear** measures increase, **protection motivation** will decrease (H9e)

As just discussed, if one's self-efficacy measures were not based on true skills, but more because of comfort in using computers, once they realize how to actually perform the task, their self-efficacy will probably go down. If there is a large decrease of self-efficacy after seeing how to actually perform a task, this would indicate that self-efficacy is based more on usability (e.g., perceived ease of use) rather than actual knowledge. Thus, hypothesize that-

Post **self-efficacy** measures to pre **self-efficacy** measures will have lower correlation than in the control condition (H10d)

As post **self-efficacy** measures increase, **protection motivation** will increase (H10e)

There will probably be a slight decrease in response efficacy since participants will see how the browser updates sometimes don't automatically work. Also, those in the experimental condition will get training on how to do the task, they may find it is harder than they anticipated. Thus, I hypothesize that for those in the **experimental condition-**

Post **response cost** measures to pre-**response cost** measures will have less correlation than in the control condition (H11d)

As post **response cost** measures increase, **protection motivation** will decrease (H10e)

Post **response efficacy** measures to pre-**response efficacy** measures will have greater correlation than in the control condition (H12d)

As post **response efficacy** measures increase, **protection motivation** will also increase (H12e)

Domain knowledge could totally change one's future interactions with that topic. Once someone knows how something works, it is never quite the same. A person with at least a basic understanding of how to protect themselves online may not be impacted by a video that would more deeply impact those who didn't know about a topic. Thus, I feel, that the higher the domain knowledge is, the less of an impact a message will make on their protection motivation. It may act as a reminder, but it won't be as crucial to those who don't know about an issue. Fear is not as much of an issue and even though self-efficacy might be lower, it is probably a more accurate assessment of one's abilities. Thus, I predict an interaction effect for either condition. I hypothesize, in all conditions, that as **domain knowledge increases**-

Post fear will decrease (H1e)

Post self-efficacy will decrease (H1f)

Since those with higher domain knowledge know how to perform a task, response cost will decrease, and they are familiar with the efficacy of the action, thus response efficacy will increase. Finally, knowing how to protect themselves, and what it takes to perform the action, their overall protection motivation will increase. Thus, I hypothesize that as **domain knowledge** increases-

Post response cost will decrease (H1g)

Post response efficacy will increase (H1h)

Protection motivation will increase (H1i)

2.8 Discussion

This conceptually organized literature review and hypothesis development shows the centrality of self-efficacy to the learning and behavioral change process, both generally and specifically in the domain of cybersecurity. It also shows potential influence of domain knowledge and previous experiences and discusses how these could impact the threat and coping appraisal process as described in PMT. This research will experimentally test the new additions to the PMT model and add specificity and validity to using PMT to better understand end user behavior in cybersecurity. This should, in turn, help stakeholders to develop better, more effective interventions to improve cybersecurity initiatives.

Self-efficacy, as discussed in this chapter, is crucial to compliance since, "…even when people know of a way to avoid a threat, they might not engage in the protective behavior because they did not think they could engage in the behavior" (Krcmar, Ewoldsen, & Koerner, 2016, p 293). Increased self-efficacy is tied closely with a sense of confidence and perceived behavioral control (Ajzen et al., 2002). True self-efficacy would normally include rational understanding of one's abilities, as well as the limits of one's abilities, which would lead to behavioral control (Bandura, 1992). However, with increased usability in computing devices there is often a sense of self-efficacy that is induced by the design of the device or the design of the software. This lulls users into a confidence that they are in control and safe, even when they are not. Thus, we have a gap between perceived self-efficacy and actually domain knowledge. If self-efficacy is based on false impressions, then users being encouraged to perform a task may agree to take action,

but in the end, they won't do it (Nabi et al., 2008). Especially in cyber safety actions, the individual may think they can perform a task and may honestly plan to do it (e.g., TPB, TRA). However, when they go to actually carry out the task it may prove more difficult or time consuming than they anticipated. It may prove to be difficult, if not impossible to carry out. Hence, the danger of a gap between self-efficacy and domain knowledge. The rest of this research is to test if that gap is indeed there, and if a message that includes the opportunity to increase domain knowledge through vicarious learning can help close that gap.

Figure 2.2: The research model

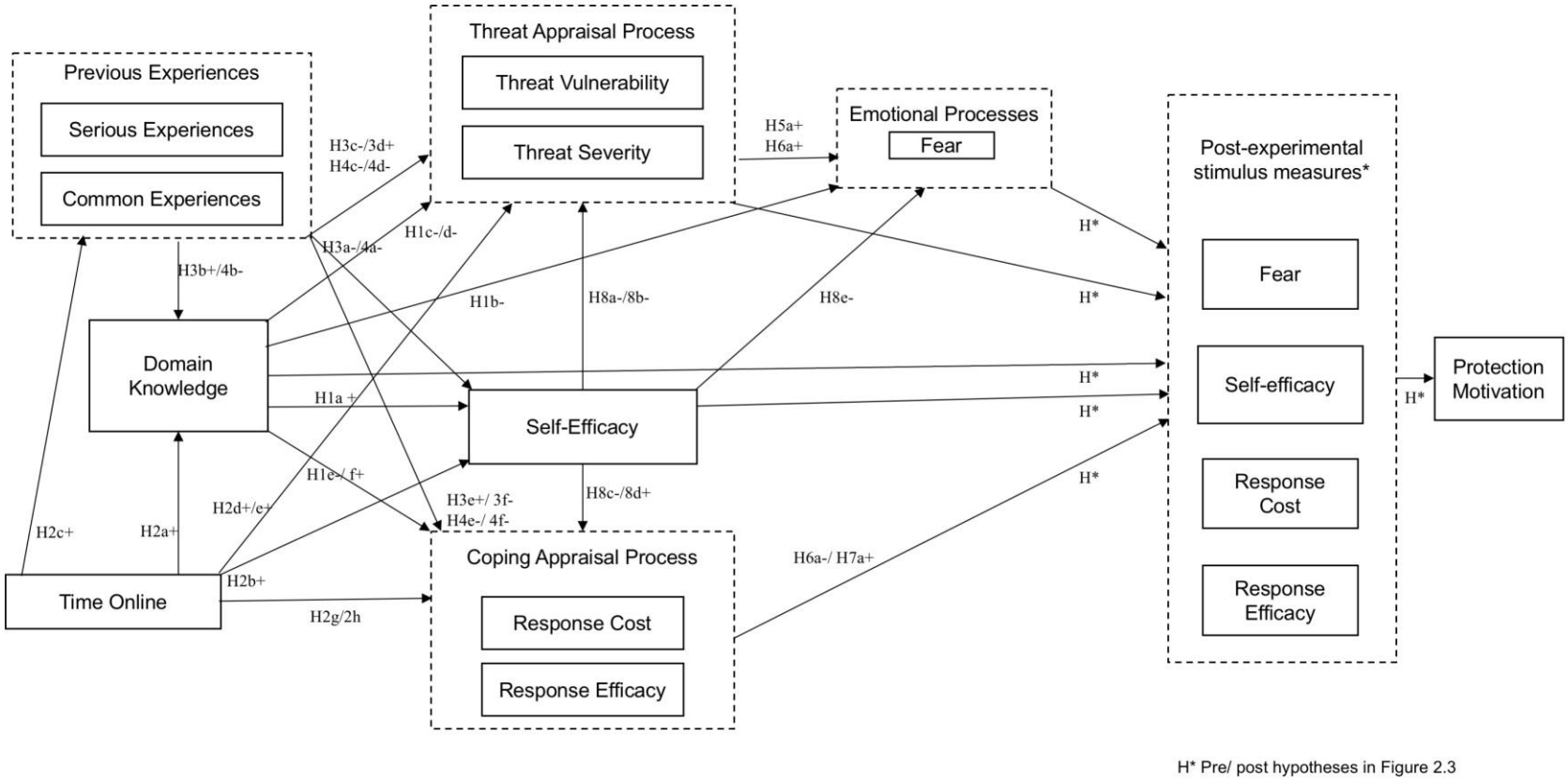
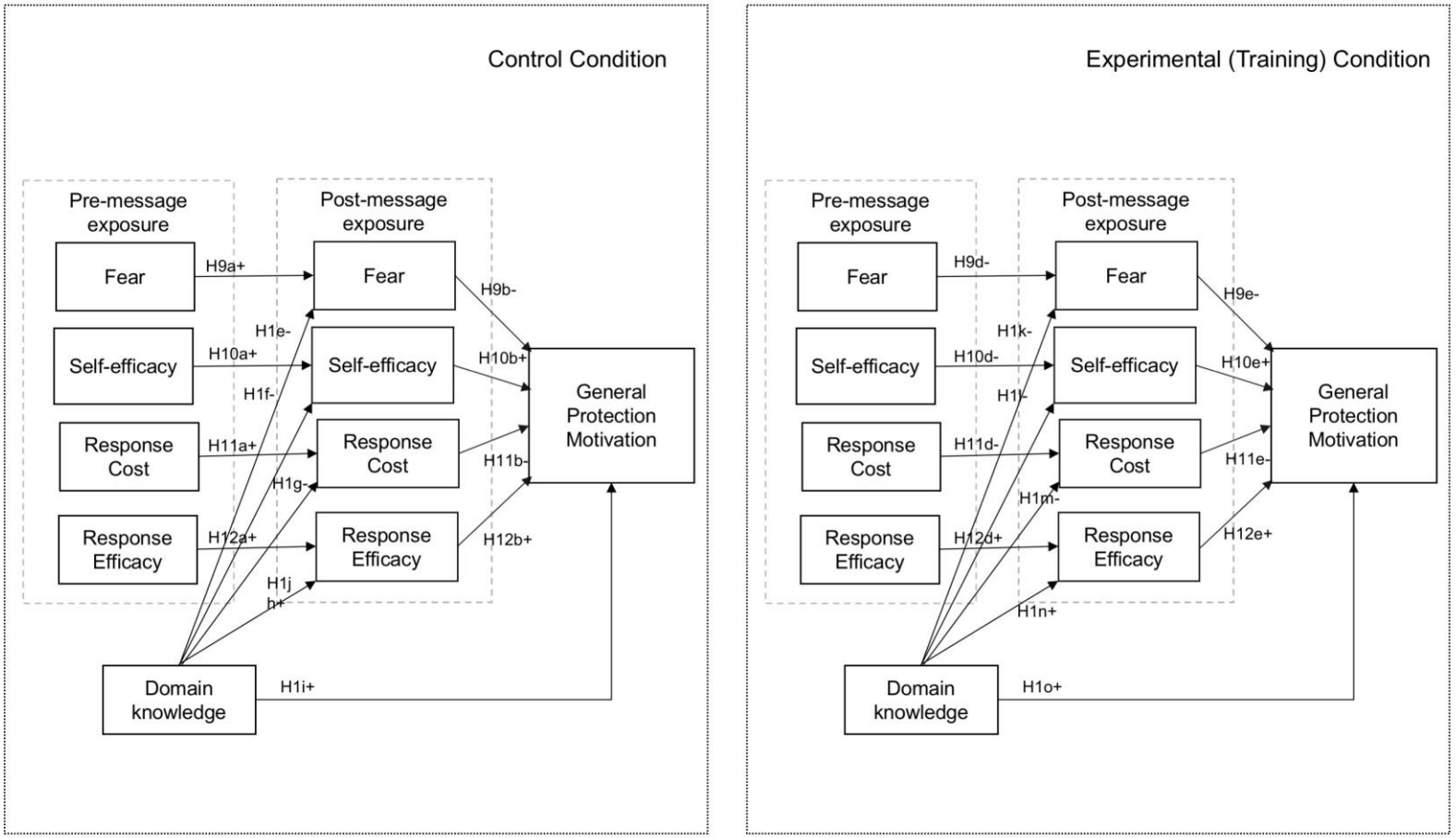


Figure 2.3: The experimental stimulus hypotheses



APPENDIX

Appendix 2.1 Examples of Domain Knowledge Measures

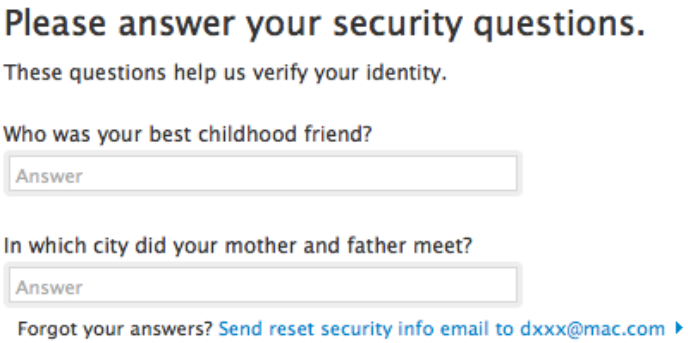
Used with permission (Olmstead & Smith, 2017)

1. Some websites and online services use a security process called two-step authentication. Which of the following images is an example of two-step authentication? (randomized)

A.

B.

C.



D.

E. None of these
F. Not sure

2. **Which of the following four passwords is the most secure?**

A. WTh!5Z
B. into*48
C. Boat123
D. 123456
E. Not sure

WORKS CITED

WORKS CITED

Agarwal, R., Sambamurthy, V., & Stair, R. M. (2000). Research Report: The Evolving Relationship Between General and Specific Computer Self-efficacy—An Empirical Assessment. Information Systems Research, 11(4), 418–430. https://doi.org/10.1287/isre.11.4.418.11876

Ajzen, I. (2002). Perceived Behavioral Control, Self-efficacy, Locus of Control, and the Theory of Planned Behavior. Journal of Applied Social Psychology, 32(4), 2918–2940. https://doi.org/10.1111/j.1559-1816.2002.tb00236.x

Ajzen, I., Sparks, P., Ajzen, I., & Hall-box, T. (2002). Perceived Behavioral Control, Self-efficacy, Locus of Control, and the Theory of Planned Behavior1. Journal of Applied Social Psychology, 80(6), 2918–2940. https://doi.org/10.1111/j.1559-1816.2002.tb00236.x

Alhabash, S., Jiang, M., Brooks, B., Rifon, N. J., LaRose, R., & Cotten, S. R. (2015). Online Banking for the Ages: Generational Difference in Institutional and System Trust. In L. Robinson, S. R. Cotten, J. Schulz, T. M. Hale, & A. Williams (Eds.), Communication and Information Technologies Annual (Vol. 10, pp. 145–171). Emerald Group Publishing, Ltd. http://dx.doi.org/10.1108/02683940010305270

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

Arachchilage, N. A. G., & Love, S. (2014). Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective. Computers in Human Behavior, 38, 304–312. https://doi.org/10.1016/j.chb.2014.05.046

Armitage, C. J., & Conner, M. (2001). Efficacy of the Theory of Planned Behaviour: A Meta-Analytic Review. The British Journal of Social Psychology / the British Psychological Society, 40(Pt 4), 471–499.

Bada, M., & Sasse, A. (2014). Cyber Security Awareness Campaigns Why do They Fail to Change Behaviour? Global Cyber Security Capacity Centre, (July).

Bandura, A. (2001). Social Cognitive Theory: an Agentic Perspective. Annual Review of Psychology, 52, 1–26. https://doi.org/10.1146/annurev.psych.52.1.1

Bandura, A. (2012). On the Functional Properties of Perceived Self-efficacy Revisited. Journal of Management, 38(1), 9–44. https://doi.org/10.1177/0149206311410606

Bandura, A. (1971). Social Learning Theory. Social Learning Theory. https://doi.org/10.1111/j.1460-2466.1978.tb01621.x

Bandura, A. (1977). Self-efficacy: Toward a Unifying Theory of Behavioral Change. Pyschological Review, 84(2), 191–215. http://dx.doi.org/10.1037/0033-295X.84.2.191

Bandura, A. (1989). Regulation of Cognitive Processes Through Perceived Self-efficacy. Developmental Psychology, 25(5), 729–735.

Bandura, A. (1991). Social Cognitive Theory of Self-Regulation. Organizational Behavior and Human Decision Processes, 50, 248–287.

Bandura, A. (1992). Exercise of Personal Agency Through the Self-efficacy Mechanism. In R. Schwarzer (Ed.), Self-Efficacy: Thought Control of Action (pp. 3–38). New York, New York: Taylor & Francis Group.

Bandura, A. (2001). Social Cognitive Theory : An Agentic Perspective. Annual Review of Psychology, 52, 26.

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of Online Safety Behavior: Towards an Intervention Strategy for College Students. Behaviour & Information Technology, 3001(July), 1–14. https://doi.org/10.1080/0144929X.2015.1028448

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. MIS Quarterly, 39(4), 837–864.

Brown, J. S., Collins, A., Duguid, P., & Seely, J. (2007). Situated cognition and the culture of learning. Educational Researcher, 18(1), 32–42.

Cadzow, S. (2017). Overcoming Fear of Threat Model. In T. Tryfonas (Ed.), HCI International: Human aspects of Information Security, Privacy and Trust (pp. 14–24). Vancouver, BC, Canada: Springer.

Cooper, H. M. (1988). Organizing Knowledge Syntheses: A Taxonomy of Literature Reviews. Knowledge in Society, 1(1), 104–126. https://doi.org/10.1007/BF03177550

Cox, J. (2012). Information Systems User Security: A Structured Model of the Knowing–Doing Gap. Computers in Human Behavior, 28(5), 1849–1858. https://doi.org/10.1016/j.chb.2012.05.003

Deture, M. (2004). Cognitive Style and Self-efficacy: Predicting Student Success. American Journal of Distance Education, 18(1), 21–38.

Ellis, J., Mullan, J., Worsley, A., & Pai, N. (2012). The Role of Health Literacy and Social Networks in Arthritis Patients' Health Information Seeking Behavior: A Qualitative Study. International Journal of Family Medicien, 2012, 6. https://doi.org/10.1155/2012/397039

Eppright, D. R., Tanner, J. F., & Hunt, J. B. (1994). Knowledge and the Ordered Protection Motivation Model : Tools for Preventing AIDS. Journal of Business Research, (30), 13–24.

Ewoldsen, D. R., Rhodes, N., & Fazio, R. H. (2015). The MODE Model and Its Implications for Studying the Media. Media Psychology, 18(3), 312–337. https://doi.org/10.1080/15213269.2014.937440

Fazio, R. H. (1990). Multiple Processes by Which Attitudes Guide Behavior : The MODE Model as an Integrative Framework. Advances in Experimental Psychology (Vol. 23), 23(July 1990), 75–109. https://doi.org/10.1016/S0065-2601(08)60318-4

Fazio, R. H., & Towles-Schwen, T. (1999). The MODE Model of Attitude-Behavior Processes. In S. Chaiken & Trope (Eds.), Dual-Process Theories in Social Psychology (pp. 97–115). Guilford Press.

Fishbein, M., & Ajzen, I. (1975). Belief, attitude, intention and behavior: an introduction to theory and research. Reading, MA: Addison-Wesley.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-Analysis of Research on Protection Motivation Theory. Journal of Applied Social Psychology, 2000, 30, 2, Pp. 407-429., 30,(2,), 407–429. https://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Germeni, E., & Schulz, P. J. (2014). Information Seeking and Avoidance Throughout the Cancer Patient Journey: Two Sides of the Same Coin? A Synthesis of Qualitative Studies. Psycho-Oncology, 23(12), 1373–1381. https://doi.org/10.1002/pon.3575

Hauser, R., Paul, R., & Bradley, J. (2012). Computer Self-efficacy, Anxiety, and Learning in Online Versus Face to Face Medium. Journal of Information Technology Education: Research, 11.

Hoadley, C. (2007). Learning Sciences Theories and Methods for E-Learning Researchers. In R. Andrews & C. Haythornthwaite (Eds.), The Sage handbook of e-learning research (pp. 139–157). 1 Oliver's Yard, 55 City Road, London EC1Y 1SP United Kingdom: SAGE Publications Ltd. https://doi.org/10.4135/9781848607859

Hsu, M.-H., & Chiu, C.-M. (2004). Internet Self-efficacy and Electronic Service Acceptance. Decision Support Systems, 38(3), 369–381. https://doi.org/10.1016/j.dss.2003.08.001

Jia, H., Wisniewski, P., Rosson, M. B., & Carroll, J. M. (2015). Risk-Taking as a Learning Process for Shaping Teen's Online Information Privacy Behaviors. In Computer Supported Cooperative Work (CSCW) (pp. 583–599).

Johnston, B. A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly, 34(3), 549–566.

Krueger, N. F. J., & Dickson, P. R. (1994). "How Believing in Ourselves Increases Risk Taking: Perceived Self-efficacy and Opportunity Recognition." Decision Sciences, 25(3), 385–400. https://doi.org/10.1111/j.1540-5915.1994.tb00810.x

Lewis, I., Watson, B., & White, K. M. (2013). Extending the Explanatory Utility of the EPPM Beyond Fear-Based Persuasion. Health Commun. https://doi.org/10.1080/10410236.2013.743430

Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. MIS Quarterly, 33(1), 71–90. https://doi.org/Article

Luarn, P., & Lin, H.-H. (2005). Toward an Understanding of the Behavioral Intention to use Mobile Banking. Computers in Human Behavior, 21(6), 873–891. https://doi.org/10.1016/j.chb.2004.03.003

Maloney, E. K., Lapinski, M. K., & Witte, K. (2011). Fear Appeals and Persuasion: A Review and Update of the Extended Parallel Process Model. Social and Personality Psychology Compass. https://doi.org/10.1111/j.1751-9004.2011.00341.x

Milne, S., Sheeran, P., & Orbell, S. (2006). Prediction and Intervention in Health Related Behavior: A Meta Analytic Review of Protection Motivation Theory. Journal of Applied Social Psychology, 30(1), 106–143. https://doi.org/10.1111/j.1559-1816.2000.tb02308.x

Montaño, D., & Kasprzyk, D. (2008). Theory of Reasoned Action, Theory of Planned Behavior, and the Integrated Behavioral Model. Health Behaviour and Health Education. Theory, Research, and Practice. https://doi.org/10.1016/S0033-3506(49)81524-1

Muhire, B. (2012). Employee Compliance with Information Systems Security Policy in Retail Industry. Case: Store Level Employees. Honors Thesis Program in the College of Management.

Multon, K. D., Brown, S. D., & Lent, R. W. (1991). Relation of Self-efficacy Beliefs to Academic Outcomes: A Meta-Analytic Investigation. Journal of Counseling Psychology, 38(1), 30–38. https://doi.org/10.1037/0022-0167.38.1.30

Nabi, R. L., Roskos-Ewoldsen, D., & Carpentier, F. D. (2008). Subjective Knowledge and Fear Appeal Effectiveness: Implications for Message Design. Health Communication, 23, 191–201. https://doi.org/10.1080/10410230701808327

Nadler, J., Thompson, L., & Boven, L. Van. (2003). Learning Negotiation Skills: Four Models of Knowledge Creation and Transfer. Management Science, 49(4), 529–540. https://doi.org/10.1287/mnsc.49.4.529.14431

Padayachee, K. (2012). Taxonomy of Compliant Information Security Behavior. Computers & Security, 31(5), 673–680. https://doi.org/10.1016/j.cose.2012.04.004

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' Behavior Towards IS Security Policy Compliance. Proceedings of the Annual Hawaii International Conference on System Sciences, 1–10. https://doi.org/10.1109/HICSS.2007.206

Purdie, N., & Boulton-Lewis, G. (2003). the Learning Needs of Older Adults. Educational Gerontology, 29(2), 129–149. https://doi.org/10.1080/713844281

Reiser, B. J. (2004). Scaffolding Complex Learning: The Mechanisms of Structuring and Problematizing Student Work. Journal of the Learning Sciences, 13(3), 273–304. https://doi.org/10.1207/s15327809jls1303_2

Rippetoe, P. A., & 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), 596–604. http://doi.org/10.1037//0022-3514.52.3.596

Rogers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. Journal of Psychology, 91(1), 93–114.

Roskos-Ewoldsen, D. R., Yu, H. J., & Rhodes, N. (2004). Fear Appeal Messages Affect Accessibility of Attitudes Toward the Threat and Adaptive Behaviors. Communication Monographs, 71(1), 49–69. https://doi.org/10.1080/0363452042000228559

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., Larose, R., & Rifon, N. J. (2015). Online Safety Begins with You and Me: Convincing Internet Users to Protect Themselves. Computers in Human Behavior, 48. https://doi.org/10.1016/j.chb.2015.01.046

Shillair, R. J. (2013). Three Constructs Examined: Theoretical Forces That Could Affect Retention in Online College Classes. Michigan State University.

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., Larose, R., & Rifon, N. J. N. J. (2015). Online Safety Begins With You and Me : Convincing Internet Users to Protect Themselves. Computers in Human Behavior, 48, 199–207. https://doi.org/10.1016/j.chb.2015.01.046

Shillair, R., LaRose, R., Jiang, M., Rifon, N. J., & Cotten, S. R. (2017). The Role of Habits and Prior Experience in Motivating User Cybersecurity Behavior. International Communication Association (p. 30). San Diego, California.

Silvia, P. J. (2003). Self-efficacy and Interest: Experimental Studies of Optimal Incompetence. Journal of Vocational Behavior, 62(2), 237–249. https://doi.org/10.1016/S0001-8791(02)00013-1

Stajkovic, A. D., & Luthans, F. (1998). Self-efficacy and Work-Related Performance Meta Analysis. Psychological Bulletin, 124(2), 240–261.

Tanner, J. F., Day, E., & Crask, M. R. (1989). Protection Motivation Theory An Extension of Fear Appeals Theory in Communication, 276, 267–276.

Tsai, H.-Y. S., Shillair, R., Cotten, S. R., Winstead, V., & Yost, E. (2015). Getting Grandma Online: Are Tablets the Answer for Increasing Digital Inclusion for Older Adults in the U.S.? Educational Gerontology, 41(10). https://doi.org/10.1080/03601277.2015.1048165

Tudge, J. R. H., & Winterhoff, P. A. (1993). Vygotsky, Piaget, and Bandura: Perspectives on the Relations between the Social World and Cognitive Development. Human Development, 36(2), 61–81. https://doi.org/10.1159/000277297

van Osch, W., & Coursaris, C. K. (2010). Self, Network, or Society: Exploring Their Relative Effects on Entrepreneurial Self- Efficacy, Attitude, and Intentions.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Vancouver, J. B., & Kendall, L. N. (2006). When Self-efficacy Negatively Relates to Motivation and Performance in a Learning Context. Journal of Applied Psychology, 91(5), 1146–1153. https://doi.org/10.1037/0021-9010.91.5.1146

Vaniea, K., Rader, E., & Wash, R. (2014). Betrayed By Updates : How Negative Experiences Affect Future Security. In CHI 2014, One of a CHInd (pp. 2671–2674).

Vygotsky, L. S., & Rieber, R. W. (1997). The Collected Works of L. S. Vygotsky: Problems of the Theory and History of Psychology. Springer Science & Business Media.

Waddell, J. C., McLaughlin, C., LaRose, R., Rifon, N., & Wirth-Hawkins, C. (2014). Promoting Online Safety Among Adolescents: Enhancing Coping and Self-efficacy and Protective Behaviors Through Enactive Mastery. In Communication and Information Technologies Annual: Doing and Being Digital: Mediated Childhoods (pp. 133–157). Emerald Group Publishing.

Wang, A. Y., & Newlin, M. H. (2002). Predictors of Web-Student Performance: The Role of Self-efficacy and Reasons for Taking an Online Class. Computers in Human Behavior, 18(2), 151–163. https://doi.org/10.1016/S0747-5632(01)00042-5

Witte, K., & Allen, M. (2000). A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns. Health Education & Behavior, 27(5), 591–615. https://doi.org/10.1177/109019810002700506

Witte, Kim. (1994). Fear Control and Danger Control: A Test of the Extended Parallel Process Model (EPPM). Communication Monographs. https://doi.org/10.1080/03637759409376328

Workman, M., Bommer, W. H., & Straub, D. (2008). Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test. Computers in Human Behavior, 24(6), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Yagil, D., Cohen, M., & Beer, J. D. (2013). Older Adults' Coping With the Stress Involved in the Use of Everyday Technologies. Journal of Applied Gerontology, 20(10). https://doi.org/10.1177/0733464813515089

Yeo, G. B., & Neal, A. (2006). An Examination of the Dynamic Relationship Between Self-efficacy and Performance Across Levels of Analysis and Levels of Specificity. Journal of Applied Psychology, 91(5), 1088–1101. https://doi.org/10.1037/0021-9010.91.5.1088

Chapter 3
Focus group study

3.1 Introduction

It is important to listen to the voices of individuals who are impacted by an issue if we are to develop research instruments with high validity. Only by listening to their expressed needs and struggles can we develop research models that reflect their reality. Research should be accurate and rigorous, yet compassionate and aware of potential long-term impacts of findings. Through analysis of the focus group materials I moved towards this goal and improved the research instrument. This phase of research has three goals:

1) To improve validity for using PMT as a framework for analyzing responses to cybersecurity messages by comparing it to other closely related theories. This compare-and-contrast method allows a deeper understanding of PMT and its appropriateness for understanding response to cyber threats.

2) To look for other potential constructs that are part of individuals' processes when dealing with online threats. There may be domain specific issues that are not covered in previous research.

3) To look for ways to refine current operationalizations of constructs. Threats are evolving there may be new terms or phrases that capture the sense of threat.

There are many things that are threats to validity in a research study, making assumptions about the subject population without careful observation is a major threat to validity. Learning deeply from the subject can not only add validity, it can improve overall understanding of the research topic(s) and even lead to unexpected results. This research uses a review of the transcripts of 18 focus groups to accomplish this goal. Each focus group lasted about an hour and had an average of 10 participants. The topic of the

discussion was online threats and why the participants did (or did not) do online banking. This is a high-risk activity online and the individuals' understanding of threats and how they could protect themselves is closely tied to my research topic. As people discuss their reasons for their choices of online activities it should reveal their understanding of threats, their threat mitigating processes, their domain knowledge, and their confidence in dealing with online threats. In this chapter I will review how the data was collected, how I reviewed it for this research, and findings from the review.

3.2 Methods

3.2.1 The Focus Group Data Collection

The past few decades have brought seismic changes in how almost everything is done. These changes are primarily a result of advances in computer technology. As waves of innovation hit society, different age cohorts dealt with these changes at different points in their lives. The age at which a technology was widely adopted impacts their use and attitudes towards the potential use (and threats) that the technology offers (Czaja & Barr, 1989; Czaja & Sharit, 1998; Mitzner et al., 2010; Tsai, Shillair, & Cotten, 2017). The source of my data is a National Science Foundation funded study, NSF Grant #1318885, that worked collaboratively with a credit union that is affiliated with my university. The credit union has over 250,000 members so its reach is quite wide. The project looked at online banking and through the focus groups we wanted to better understand the issues that made individuals choose to do online banking or to not participate. Part of the research was to look at age cohort differences and how these would impact these decisions. To examine these differences one phase of the research ran 18 focus groups with an average size of about ten people. There were three groups for each category of

user/ non-user of online banking and for each of the age cohorts of: Millennials/ Gen X (born between 1965 and 1992), Boomers (1946-1964), and Silent/ GI generation (born before 1945), resulting in a 2 x3 research design (see Table 3.1).

Table 3.1: Focus group design

	Millennial/ Gen X	Baby Boomers	Silent/ GI
Used online banking	3 groups	3 groups	3 groups
Did not use online banking	3 groups	3 groups	3 groups

3.2.2 Solicitation of participants

The IRB approved study worked closely with the credit union at each step of the research. To protect participant privacy, the credit union selected the members to invite to the focus groups based on the research criteria. Potential participants were selected based on age cohort and if they used online banking. These participants were then contacted via mail and they were encouraged to register to participate by phone. There were follow up mailings by post card and reminder phone calls. This type of recruitment, using multi-modal channels was following Dillman method (Millar & Dillman, 2011) in order to improve diversity and fuller participation. These efforts resulted in well attended groups of people that are not normally reached by group panels or primarily online solicitation samples. This unique data set allowed me to probe deeper and gain insights from individuals who are not often represented in cybersecurity research, especially older adults and those of all ages who purposefully limit their use of technology.

To complete all the groups by age and category some individuals were recruited through libraries and community outreach organizations. Participants were offered $20

incentive for participation. Many of the initial focus group meetings were at credit union branches in their large meeting rooms. Further meetings were at our lab space at the university, libraries and community meeting rooms. The particular value of this data is the wide range of participants gathered through the rigorous solicitation process. They bring insights from a population that does not normally volunteer for a focus group, thus their voices are often underrepresented.

3.2.3 Structure of focus group sessions

The focus groups were guided by a research protocol that was semi-structured to encourage participants to freely share their experiences with and attitudes towards online threats. The protocol is in Appendix 3.1. The protocol opened with going over informed consent and giving guidelines about respectfully listening to others. Each group was led by a team of two to three researchers with one facilitating the discussion and the other(s) taking notes and helping facilitate the logistics of each meeting. The logistics included passing out and collecting consent forms, preparing refreshments, and welcoming latecomers. The group facilitators were trained to follow the protocol, ask probing questions to bring deeper insights, and to assure that all participants had an opportunity to share freely. Immediately after the session the research assistants would write notes about the meeting and pay special attention to things that might not be caught just listening to the tape. For example, a comment by one member may cause most of the others to show strong affirmation with body language (e.g., nodding, leaning forward). The research assistants taking notes about the meetings could write down details not fully captured in the recordings. The recording from the groups were transcribed by a transcription service.

3.2.4 Other potential theoretical frameworks

There are many potential theoretical frameworks that could be used to help bring insight into individuals' cybersecurity beliefs, practices, and specifically their responses to messages. Since this research is seeking to understand the response to a trigger, specifically a cybersecurity message, this narrows the potential theoretical frameworks to those within the communications and persuasion family. Within the communications framework there are many theories that heavily rely on social norms, such as social cognitive theory (SCT; Bandura, 2001), and social norms approach (SNA; Berkowitz, 2005). There are other frameworks that include how communications could impact planned behavior, such as the theory of reasoned action (TRA; Madden, Ellen, & Ajzen, 1992) or theory of planned behavior (TPB; Madden et al., 1992). Also, there are the theoretical frameworks that deal with how emotions, such as fear, could override behavioral intentions. These include technology threat avoidance theory (TTAT; Liang & Xue, 2009) and extended parallel processing model (EPPM; Witte & Allen, 2000). There are also the theories that deal with how individuals process a message, such as the elaboration likelihood model (ELM; Petty, Briñol, & DeMarree, 2007).

These theories are precedents to PMT (e.g., TRA, TPB) or have elements of PMT as their base (e.g., EPPM, TTAT). The basis of PMT is that individuals have a threat appraisal process as well as a coping appraisal process before deciding how to respond to a trigger. Since security decisions are often based on a trigger (e.g., an emerging threat or performing a high-risk action) PMT works well to understand responses. Thus, the research protocol was designed to facilitate discussions of individuals' threat and coping processes.

Even though the protocol used questions that would trigger discussion of PMT elements, there may be other theoretical frameworks that could be used to bring further insights. For example, if participants discussed that they simply avoided technology to avoid threats, this would suggest that a framework such as TTAT would provide rich insights. If individuals discussed that their protections were the results of what they saw as social norms, then perhaps SCT or SNA would be a fruitful framework. If individuals discussed messages or training their had received and why they made thoughtful choices to follow training at work or school, this could indicate ELM may bring additional insight. None of these would preclude PMT, but they would indicate that another model may provide better explanation of how individuals feel towards online threats and why they make the choices they do to protect themselves. However, even though other theoretical frameworks may emerge through the analysis, the primary focus was to look for new constructs that would improve PMT by adding specificity and new variables that would improve construct validity.

3.2.5 Coding of focus group materials

To have clear digital documentation of each step, I used NVivo software as I coded the transcript. This allows collection and organization of the data as well as providing a tool to collect coding and increase quality and validity of the coding process. I used several of the processes from Miles, Huberman, & Saldana (2014) to gain insight into how these participants dealt with perceived threats. The coding process used iterative cycles to first find “chunks” of information and then refined these chunks into smaller parts in order to deepen insights.

First, I reviewed session notes and I did an overview of the session for higher level coding. Then I did a more thorough examination of the transcript. This included looking for evidence of the individuals' coping strategies, threat appraisal strategies and their protective strategies. Notes were taken during coding process about insights and trends. This includes indicators of domain knowledge and how this was tied to the participants' coping strategies. The results of the coding were compared to the literature guiding this research, then the data iteratively accessed.

3.2.6 Organizing the coding

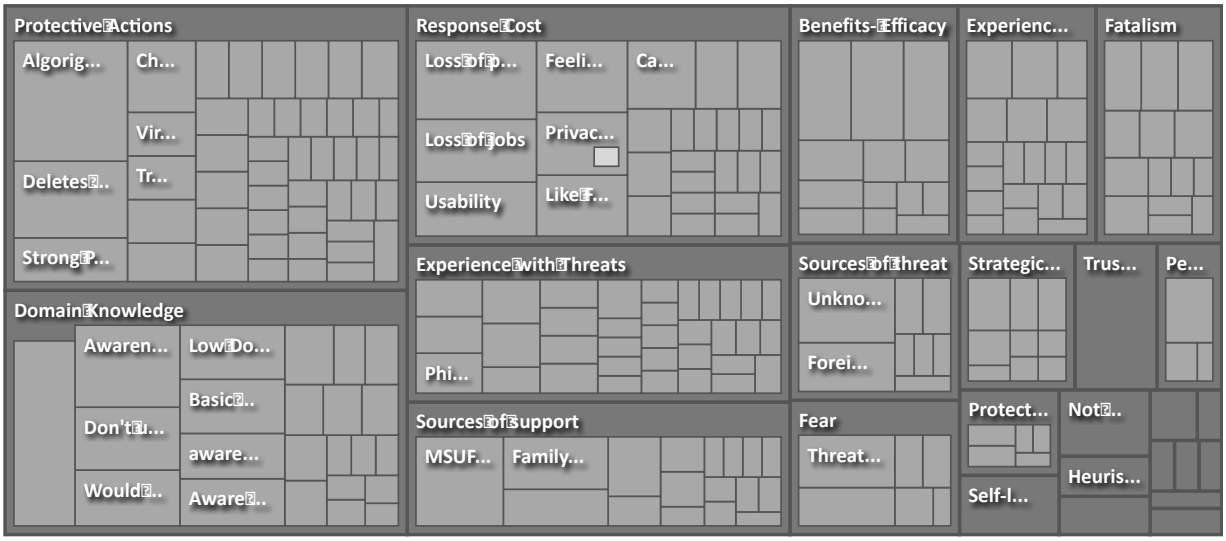
Since the goal of this research was not an exhaustive study of the focus group data, but rather a step to enrich and increase validity of the research instrument, the analysis was done "tightly," looking for "well-delineated constructs" (Miles et al., 2014, p 18). The first phase of coding was highlighting examples that satisfied the three goals of the research. The second phase was organizing the examples into nodes. The nodes were then organized into concepts. Many of the concepts were noted with comments that led to insights. Finally, the insights were checked again against the goals for the chapter. The process was iterative and repeated until redundancy. An example of this process is in Table 3.2. Notes were taken during the coding process to capture the insights gained from coding.

Table 3.2: Example of coding process

Example	Nodes	Concept	Notes
“I have a question on the first one, the downloading updates, there's one place that I was always unsure. I've always heard you gotta be careful what you download or upload, whatever. So, I never know which ones are 100% critical for a computer or no. So yeah, Windows, whatever, Microsoft, you get this, there's 14 updates, three are critical, so if you look and read through the explanation for it, and it says nothing to me. I had no idea. That's the thing I'm most worried about.” (Boomer, User)	Awareness of need for updates	Domain Knowledge	Fairly high digital literacy Aware of terminology and trying to learn more. Lack of knowledge causes worry. Shows threat and coping appraisal by evaluating efficacy of response.

The concepts were easy to visualize using the software. An example of a visualization is in Figure 3.1. The coding process produced several concepts to probe in the future, but staying focused on answering the research goals helped bring more narrow, but richly layered insights.

Figure 3.1: Example of node hierarchy



Since the review of the focus group material was to achieve the three goals stated, akin to Miles et al. (2014) “first cycle” coding and not to examine the material exhaustively, it was appropriate to code with only one researcher. Coding was done until redundancy, indicating that there was saturation of the concepts being examined.

3.3 Results

Each session started with many participants sharing their experiences of threat and how they dealt with it. The focus group facilitator started each session with an opening statement that included-

> Just about everyone who uses the Internet has encountered problems at one time or another… (different possible problems were mentioned) … As a result, some people would describe the Internet as a risky place, while others might say that the Internet is relatively safe. I’d like to ask each one of you to use the paper and pencil we provided to write down an incident that particularly sticks out in your mind. Then we’ll go around and ask you to tell us about it and how you dealt with it. If you have never had any of these problems, congratulations! But please write

down the threat you have heard about that worries you the most. (Research Protocol)

After waiting for the participants to finish writing down their experiences, the facilitator encouraged everyone to share. Most had first-hand experiences with threats, and everyone had at least one story of something that happened to others. There were many differences by age cohort, the Boomers and SG/GI groups were more concerned about financial threats, many discussed concerns about the security of their bank and credit card accounts.

3.3.1 Comparing PMT to other theoretical frameworks

The first step of analysis was to analyze the data looking for evidence of other theoretical frameworks, and to examine PMT's explanatory value. The transcripts were coded looking for elements of the theories previously mentioned, especially use/ non-use of technology (TTAT), mentions of social norms (SCT, SNA), fear (EPPM), and how they learned to protect themselves. As individuals described their threat analysis and coping analysis methods, these were coded as PMT processes. Phrases that were repeated or items that could improve validity of previously used scales were also noted. The focus group data also helped inform the construction of the cybersecurity compliance message.

3.3.1.1 Use and non-use of technology

Their protective strategies varied widely. This went all the way from non-use, which was reminiscent of the technology threat avoidance theory (TTAT; Liang & Xue, 2009) to hiring professional services to increase their protections. Those who ended up with non-use often led to reliance on others to perform tasks that required computer access. For example, one older lady shared that she had a chain of events starting with a phishing

email and ending up with threatening phone calls and even the police getting involved (SGI non-user group 3). She no longer used computers at all and relied on family members to help her with functions that she needed to do online. Non-use, or more commonly limited use, was a more prevalent option for older adults.

However, even within the non-users of all ages, there was an acknowledgement of the inevitability of having to do many functions online.

> There is no answer, but I agree with you. Eventually, everybody's gonna do everything online. The post office is gonna disappear. You gotta be aware of that. (SGI non-user, group 13).

As just mentioned, there was evidence of TTAT, especially in the older adult groups (i.e., Boomers, SGI/GI). However, even those who said they limited their exposure online often later discussed how they had a family member help them pay bills online, shop online or perform other functions. Younger participants (i.e., some Boomers, Millennials) did not seem to see non-participation as an option. TTAT as a framework was present, but those who “avoided” technology ended up relying on others to carry out sensitive functions, thus the efficacy TTAT as a security choice was very self-limiting. Even though individuals displayed TTAT, overall there was a sense that they would have to eventually accept using online access to accomplish basic tasks. Therefore, TTAT alone would have limited value in understanding response to cybersecurity communications.

3.3.1.2 Threat appraisal process

There was evidence of the threat appraisal process. Participants made decisions on what they did online based on a calculation of both threat vulnerability and threat

severity. Sometimes, even if they realized that they were vulnerable (i.e., likely to face a threat); however, they did not feel that facing the threat would be severe enough for them to change their current behaviors. For example, a Millennial shared that he was not too concerned about online threats because he did not feel that he had much to protect. Thus, he had low threat severity. He also felt that given his age he was not as much of a target so he also had low threat vulnerability.

> But I guess the thing with me is, I think I'd be more concerned if I had money to protect, but I guess, I'm not really that concerned about people stealing my information because there's not a lot to steal. It's funny, this happened to my grandparents and they have lots of money, and I think seniors are typically more of a target because they're less technologically educated about things. So, they gave all their account information to some guy, and thousands of dollars gone. So, I guess, if I was sitting on a lot of money, I would be a lot more paranoid about someone trying to take it. I guess, maybe that's my standpoint on it. (Millennial User/ Group 4)

This user also mentioned that he felt older adults were less technologically savvy than his age group. Thus, his perceived domain knowledge gave him self-efficacy in protecting himself. Many mentioned that they were aware of threats, and that it would be serious, but they didn't feel that they were particularly vulnerable to a threat. On the other hand, some individuals felt threats were more serious than most people realized.

> I think a lot of times, you feel like, you hear about all these cases where it happens, but you never think it's gonna happen to you. So, it's like, "Wow, that's too bad" until it happens to you. Then it's like, "Oh that was really serious, I didn't realize,"

so until something happens, you don't really realize how threatened you really are. Like you were saying, you're just on there doing what you feel you need to do, saying, "Oh okay, yeah it happened, but it's not gonna happen to me. (Boomer Non-user/ Group 16).

Both of these examples illustrate clear threat severity and threat vulnerability assessment by individuals as they make choices on how to protect themselves, thus PMT gives insights into this process.

3.3.1.3 Coping appraisal process

The coping appraisal process would include both assessing if the response is effective and how difficult or costly it is to use the protection. Many described how they tried to improve their security, but they were often frustrated with poor usability and they weren't sure if the protections were working correctly. For example, one couple shared,

> Wife: There are other times... Is that our browser won't support this thing, and it'll say to update or download...What are some of those other things, George, when we click on it, we've never been able to figure out how to install some of our other updates.
>
> Husband: Like the little Flash Player updates or Silverlight
>
> Wife: Yeah, you click on it and nothing happens or you keep going into it, and then we've never been able to get those updates to work. And they just go on. They take forever, don't they? I mean, even if you do something...Well, ours have just never been successful, so some of that Flash Player we've probably been getting that message for one or two years... (SGI Non-user/ Group 3)

Others did try their best to protect themselves but expressed their uncertainty and desire to know more.

> It isn't even so much that. It's just the whole thing is frustrating because of lack of instructions. They more or less assume that people know more than they may know. There needs some more basic instruction maybe (SGI non-user/ Group 3)

Wanting to know more information to make good protective choices is evidence of the coping appraisal process. Wanting to know how effective a response is, and what it would take to implement the response is evidence of response efficacy and response cost evaluations, again supporting PMT as a rich framework to explore response to cyber threats.

3.3.1.4 Self-efficacy

What frequently hindered the coping process, was stated uncertainties about their own self-efficacy or understanding how things worked (i.e., domain knowledge). These individuals often ended up relying on others (e.g., family members or friends) to help them. For example, this Millennial knew a lot of terminology such as firewalls, anti-virus, and updates. However, she was not sure of how it worked so she was afraid to install updates to protect herself.

> My boyfriend, he built our computer and so he's pretty computer-savvy and he wants to go into IT. So, I turn to him if I have any questions about anything because I'm pretty clueless when it comes to this stuff. And once or twice to use something, he's had to mess around and put the firewalls down or whatever, [chuckle] take the anti-virus off for an hour or something so we could use something, I don't know why that happens. But where it comes to downloading updates, I tend to not

> download updates because I feel like, "Oh, maybe it's just telling me that I need to update something and maybe it would be a bad thing. (Millennial non-user/ Group 15)

Self-efficacy was often reflected in the confidence of the speakers sharing how they were able to deal with threats and sometimes help others.

3.3.1.5 PMT as a theoretical model to bring rich insights

Overall, the review of the focus group material gave support for the choice of the PMT model. There was evidence of the threat appraisal process: estimating the vulnerability of certain actions or inactions. There was also evidence of the coping appraisal process. Individuals frequently discussed the protections they took, how effective they thought they might be, and how difficult they were to follow. The other elements of PMT, self-efficacy and fear were also evident. Even though there were elements from other frameworks (e.g., ELM, TTAT, SCT), these were not as widely evident nor pervasive. PMT brought rich insights into how individuals went through constant assessments of what to do as they were making security decisions. However, it also became apparent that their natural desires to protect themselves were hampered by frustrations when they tried to enact protections. Thus, it became apparent that there was a need to add constructs to PMT to help improve its explanatory value in cybersecurity.

Table 3.3: Protection motivation elements

Threat appraisal process

Construct	Comment	Group	Insight
Threat vulnerability	Well everybody is, I think it's subject to the same risk as everybody. As long as you can take certain care. I don't have a password 1-2-3-4-5, like that. I've got a real combination, letters and numbers and that kind of stuff.	Group 11 Boomer User	Lower personal threat vulnerability through personal safety practices
Threat vulnerability	I've worked for the state government for years and I thought we had shoddy coverage as far as security we were always getting stuff that there was they're gonna come around, they're gonna do this and they're gonna do that and I'm going "Really? You have guys have lousy coverage and why isn't this better and why is this happening so often?"	Group 09 Boomer non-user	Higher threat vulnerability because of poor system design
Threat severity	I'm just always afraid of anybody getting into it and not only stealing your identity; but wiping your accounts clean.	Group 11 Boomer User	High threat severity
Threat severity	Well, and especially banking. Banking is so personal and so private….to have something happen with your bank account with everything, that just doesn't seem to me, wise or secure. It just doesn't.	Group 09 Boomer non-user	High threat severity

Table 3.3: (cont'd)

Coping appraisal process

Construct	Comment	Group	Insight
Response efficacy	I use BitDefender because I read and I researched that company, and I feel like they actually do a good job …they actually manage a lot of the security roles that I would have to spend more time doing myself like firewalls, full system scans, checking what connections you come in contact with, things like that.	Group 07 Millennial User	High response efficacy/ personally researches to find answers
Response efficacy	I've also talked to my friend who was studying something with, along cyber... I don't understand, whatever, but I called him up, and was like, "Hey, do you know about this?" And he was like, "Oh yeah, that's just a debunked firewall, it's easy to get around," he told me, and I was like, "Oh, okay."	Group 04, Millennial users	Seeks help from those with expertise to verify response efficacy
Response cost	Java is the most irritating one for me, because it keeps blinking and blinking and it slows the computer down unless you can take the time to do it again... I don't want to deal with it then. And it'll keep coming up and coming up and coming up and as I say, it will pop up, it will slow down the computer and everything till I'm dealing with it.	Group 5 Boomer user	Response cost of time, irritation, uncertainty
Self-efficacy	Be careful, as careful as I can be in my limited sphere of understanding and knowledge. Now that we're all so interconnected there's a price to pay for that. There's so many benefits to it, I wouldn't trade it, but I sure do wish there were more ways to be safe.	Group 09 Boomer non-user	Self-efficacy realistic/ aware of limited knowledge

Table 3.3: (cont'd)

Construct	Comment	Group	Insight
Self-efficacy	So, I don't know if this is relevant or not. But sometimes, things online are very frustrating. I tried to join LinkedIn, when I was asked by a friend to be friends with them on LinkedIn or whatever. So, I had an acquaintance help me set up an account. But I still can't figure it out.	Group 03 SGI non-users	Lower self-efficacy
Self-efficacy	I use the FSF's which is the Free Software Foundation's rebranding of Firefox, which is basically just Firefox. I recommend running no script on it if you can deal with just HTML pages and no JavaScript. A lot of websites will stop working but you can whitelist the ones that you know are good…[in Firefox the] JavaScript engine is sandboxed within the browser…I run Linux, Gentoo specifically. I compile it myself,	Group 06 Millennial User	High self-efficacy/ high domain knowledge

3.3.2 Constructs to enhance PMT

In order to enhance PMT's value as a model to examine cybersecurity attitudes and practices, the data was examined to look for how individuals learned about online threats, and other potential constructs are unique to the cybersecurity domain.

3.3.2.1 Gaining domain knowledge

Participants discussed their process of learning about how to deal with threats (e.g., gaining domain knowledge). This was primarily through three channels: learning from the experiences of others, personal experiences, and formal training. Those who learned from others were often through stories, sometimes told by friends and things they

heard on social media. Those who described learning from stories tended to express fear and not narrate any strategic (i.e., cognitive) response. Their response to the threat was often fairly strong. One participant shared,

> I have a friend who they went online, had the bank take over their life, which I would never do. That's why I don't do online banking (SGI non-user, group 3).

The threat turned out to be the friend had signed up for a monthly auto-payment of $29 and did not know how to stop it. The lack of control, and not understanding what to do had frightened this participant away from almost all online financial activities.

The surprising thing was that as individuals described the experiences of others they often used the word “scary” or “frightening”

> One was about a friend, he was setting someone's computer and someone just started taking over his computer. The mouse was moving and he had like no control over it which I thought was very scary… (Millennial User/ Group 6)

Yet, this same person had fairly serious things happened to them personally, and yet they didn’t seem to express that much fear

> Also, one time at work actually I got locked out of my username and this government message came up but obviously it wasn't a government message and it wanted me to pay $500 or something to this random place… it wouldn't let me log out or anything it was so weird. And then just one time on Facebook they emailed me and told me someone was logging in from a random country on my account and that was like, "That's not me." So, changed my passwords and stuff… But nothing ever bad happened, just weird activity. (Millennial User/ Group 06)

This shows the need to examine the issue of fear, which could potentially override planned protections and result in a fear control response as described in EPPM.

Many had personal experiences with online threats, they didn't discuss having any formal training, but they know about general threats.

> Yeah, and [there are] dangerous programs to download. Sometimes, like today, [this] afternoon, I got a message saying that, "Your computer is about to crash. Download this to rescue your computer from crashing." And the first time you get such a message, you're like, "Hmm." And then maybe the second thought will tell you, "No, you shouldn't." But sometimes, it's tricky to... You just find yourself downloading dangerous programs that can expose your information" (Millennial User/ Group 4)

There were a few mentions of training at work,

> Well, at work, I work for the State for the Department of Transportation, so we do have all the courses that we have to take on the computer security every so often. (S/GI non-user/ Group 3)

This individual continued with describing their training in detail, which was predominantly "how to…" do things, but there seemed to be no mention of how it connected to them personally nor was there discussion that the presentation was attractive or interesting.

Those who did describe training seemed to appreciate how it had helped them. However, our participants often wanted to know more. Most cybersecurity training described by participants was focused on the "how to" and not trying to persuade them to a changed attitude. Most training was alone, using online modules. Also, most security

procedures are done alone, with no one watching so there is little sharing of cybersecurity norms. The social learning aspect, which is important to SCT and SNA, seemed fairly absent. Yet, the participants shared they were doing the best they know how to do. There was an overall feeling of vulnerability and the hope that protections could minimize the damage at best. For example, one participant said,

> What people can really benefit from is knowing in general, where your primary risks are and having strategies for minimizing risk on your own simply for that fact that everyone is using the internet in different ways. But, I think, going back to what we we've talked about earlier, and that is we don't necessarily understand where we're at most risk. And if there was more information about how to minimize it rather than ensuring it. It's a lesser standard of security, but I feel that's probably the most viable alternative. At this stage, anyway. (Boomer user/ Group 8)

3.3.2.2 Protective actions

Most training at work was geared towards “how to” do functions. This type of training may improve end users’ practices, but it is unknown how it impacts attitudes. For example, individuals may be trained at work to always follow a process (e.g., log in to VPN when doing work remotely), but just do it because they are supposed to and not have the belief (or attitude) that this process actually improves their protections (i.e., response efficacy). Those who had fairly sophisticated understanding of threats (i.e., higher domain knowledge) were able to adapt better to emerging threats and discussed their concern for others who did not understand as much. For example, when talking about the safety of using wifi networks, one participant discussed his use of open wifi,

> And wanting to do that I know that I really should not be doing that at those places because it's so easy to intercept those wireless signals. But there's no real indication on your phone. And for somebody like me who is pretty tech savvy, it's pretty clear. But for an awful lot of people, it's not. It is clearly not a... It is a threat that is out there and clearly not one that most people would be aware of. My wife who's not very technical, and does use an iPhone, she wouldn't have a clue. I mean, she wouldn't have a clue that somehow this was not a secured network. I just logged into the network here, and it's not a secure network. It's an open network (Boomer user, Group 8).

It would be enlightening to see how these actions and habitual practices were tied to the attitudes addressed in the PMT model. Could actually performing actions help improve attitudes towards coping response efficacy? Also, could these actions be tied to protection motivation? It would be logical that if someone is already doing an activity it will be more likely that they will continue to perform it, unless there is a change in either the efficacy of the action or the nature of the threat that the protective activity is no longer needed. Thus, I propose adding a construct, protective actions to help measure what individuals currently do to protect themselves. Measuring these, along with domain knowledge, might bring understanding to the attitudes that are tied to better security practices. Protective actions could include items such as clearing cookies from browsers, deleting browser history, changed passwords to stronger versions, check for https, and other activities end users can do to protect themselves

3.3.2.3 Protection Habit Strength

Along with discussing what choices they made in protections, there were many comments that dealt with how comfortable individuals felt doing those actions.

> [I] Have some knowledge taken from different places…for example, our church… tried to get people to use e-mail so that they could communicate with one another, but there are some concern because people are uncomfortable, they're not knowledgeable, and different organizations that encourages different organizations like the [redacted] and the community group that provides knowledge (S/GI user, Group 1)

Some talked about protective habits that they routinely did for protections,

> I also have the habit of clear the history…very regularly so that no information is stored in the [browser]…because the browser actually sought out the information… but I just make sure that I clear everything so my personal things aren't public. (Millennial user, Group 6)

Others discussed how they usually would do a security task, but if it came at an inconvenient time they might not do it, but then they felt guilty not following their normal security practices

> My computer, I swear, it pops up every two days, like, "Oh, you have a new update." And I try to do it because I know it's good for the computer because it keeps up-to-date with everything, and then it'll block off more things if you update it your computer. But it's just so time-consuming. It's always when you're like writing a paper or something, and you're like, "Oh gosh, are you serious?" And then you'll have to update it. (Participant 1)

Ignore, ignore. [chuckle] (Participant 2)

Yeah, I know, and then you ignore it, but I know it's important. (Participant 1) (Millennial non-users, Group 18)

So, not only knowing if individuals routinely performed certain tasks, finding out how comfortable or routinely they did them would help improve the model. Stronger, habitual use would require less cognitive processing and allow a faster evaluation of threat/coping (Boehmer, LaRose, Rifon, Alhabash, & Cotten, 2015; Shillair, LaRose, Jiang, Rifon, & Cotten, 2017). Having a deeper understanding of how behaviors (i.e., protective behaviors) and how routine those behaviors are (i.e., protection habit strength) within the PMT framework could help bring further insights and strengthen the predictability power of the model.

3.3.2.4 Fatalism

A common attitude was that of fatalism, in that every group discussed that they, at some point, expected to suffer consequences from a cybersecurity attack. A frequent hope was to minimize damage. For example, one participant said,

> What people can really benefit from is knowing in general, where your primary risks are and having strategies for minimizing risk on your own simply for that fact that everyone is using the internet in different ways. But, I think, going back to what we we've talked about earlier, and that is we don't necessarily understand where we're at most risk. And if there was more information about how to minimize it rather than ensuring it. It's a lesser standard of security, but I feel that's probably the most viable alternative. At this stage, anyway. (Boomer user, Group 8).

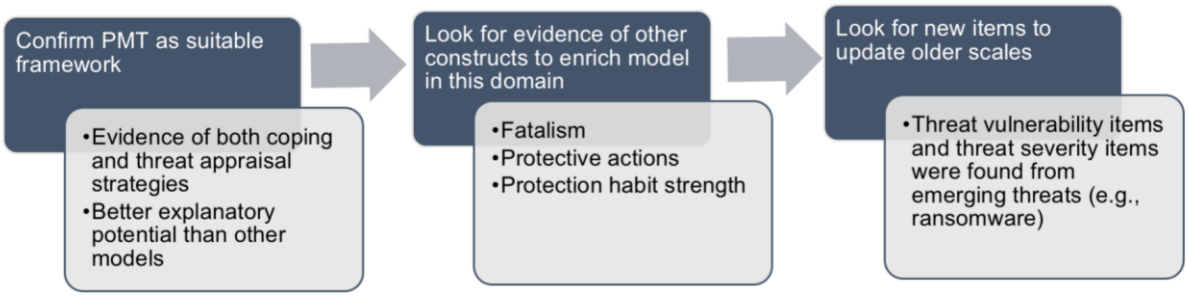
Those who expressed fatalism shared that they felt there was no way to absolutely protect against threats. The common response to fatalism was usually to still keep using technology but with lowered expectations of security. This was different than the fear response where individuals would often disengage from participating online after a frightening experience. Fear seemed to be more closely tied to lower domain knowledge and not understanding the source of threats. Also, fear often led to maladaptive behavior (e.g., never using the computer again or not taking protective actions). This echoes what researchers found in the health domain, as suggested by the EPPM (Witte & Allen, 2000; Witte, 1994). Fatalism, on the other hand, led to continued use and it is unknown how it impacts security precautions. Having items to measure fatalism should also bring insights into how this impacts the coping and threat appraisal process.

3.3.2.5 New items for threat vulnerability and threat severity

Since the landscape for online threats is changing, it would be important to ask participants about what they feel they are vulnerable to, and how severe those threats are. For example, in the mid 1990s, cookies were seen as the newest threat to privacy and potentially, security. Later, cookies became widespread in websites to give individuals a more “personalized” experience, and there was less general concern about cookies (Hill, 2015). Therefore, trying to ascertain threat vulnerability from asking question about an issue such as cookies may be an issue that was important a few years ago, but not relevant to younger users. Questions about today’s concerns about new threats like malware and ransomware may trigger stronger responses. Thus, new items should include these newer threat vectors.

Figure 3.2 illustrates the tasks completed in this section of this research.

Figure 3.2: Completed tasks for this phase of the research



3.4 Discussion and additional hypotheses

The examination of the focus group materials helped improve the research in several ways. First, it supported PMT as a model that brings insights to understand cybersecurity practices of individuals, especially when compared with other potential communications theoretical models. Secondly, the examination of the transcripts showed the need to examine constructs that are unique to cybersecurity. The participants frequently expressed a desire to know more about what they are doing. This also supports the need to explore the impact that lack of domain knowledge may be making on individuals' security choices. I saw that domain knowledge (e.g., knowing how threats actually worked) was connected with clear dialog on possible protective actions. This was in contrast with those who had lower domain knowledge and were relying on hearsay and stories from the experiences of friends to know how to protect themselves.

Protective actions and protection habit strength also emerged as an important issue to explore as this would represent not just abstract "knowledge" about threats and solutions, but actually knowing how to carry out a range of protections. Also, the comments from participants showed the wide range of things that they see as threats, showing the importance of updating threat vulnerability scales and threat severity scales.

3.4.1 Hypotheses about new constructs

The constructs not frequently associated with PMT: fatalism, protective actions, and protection habits are detailed in the next section.

3.4.1.1 Hypotheses about fatalism

As fatalism is tied to ways of coping when facing a threat in other domains (McCrae, 1984), given today's potential threat vectors it may actually be fairly realistic to have a sense of fatalism that a cyber security threat will personally touch each individual in some way (Microsoft, 2016). However, there are other components within this model that could impact a person's possible perception of fatalism. This includes domain knowledge, self-efficacy, and fear. As discussed in Chapter 2, domain knowledge could help inform end users and let them know about potential solutions.

So, I hypothesize that as **domain knowledge** increases, **fatalism** will decrease (H14a).

Also, since **self-efficacy** increases a sense of control, I hypothesize that as **self-efficacy** increases, **fatalism** will decrease (H14b).

Furthermore, since, **fear** often results from a lack of control, which is tied to fatalism, I hypothesize that as **fear** increases, **fatalism** will also increase (H14c).

3.4.1.2 Hypotheses about protective actions

In the health domain, increased protective actions commonly emerge from learning about threats and how to protect oneself (Miller, 2016). In the cyber domain this appears to be also generally true. Individuals discussed protective actions that they learned without having a deep understanding of how online threats and protections work. As they perform these protective actions, they feel more confident in carrying them out, increasing

their self-efficacy. Self-efficacy may work as a reinforcing circle as individuals enact these protections they feel confident in their ability to face future threats.

I hypothesize that as **self-efficacy** increases, **protective actions** will also increase (H15a).

Those who have more experiences with common threats are probably not taking protective actions.

I hypothesize that as **experiences with common threats** increases **protective actions** decrease (H15b)

Individuals do not usually continue to perform a task if they feel it is useless, especially if it is something that is inconvenient (Zipf, 1949). If individuals feel that enacting a protection is worthwhile, they are more likely to do it.

Thus, I hypothesize that as **response efficacy** increases, **protection actions** will also increase (H15c).

3.4.1.3 Hypotheses about protection habit strength

A habit is something that is done without debating a great deal. It is something that is done routinely. Even though at one time the action took cognitive processing to perform, it has become so routine that it takes very little thought (LaRose, 2010; Larose, Lin, & Eastin, 2003; Shillair et al., 2017). Thus, habits are often performed comfortably and are connected with self-efficacy with an action. Many of those in the focus groups who had experienced common threats seemed to have developed protective routines that they used to keep safe in the future.

Thus, I hypothesize that as **common threat** experiences increase, **protection habit strength** will also increase (H16a).

Also, that as confidence in these routines goes up, it will further increase in habit strength. Thus, I hypothesize that as **self-efficacy** goes up, **protection habit strength** will also go up (H16b).

Furthermore, as individuals understand more about how protections work, they will feel more comfortable about their actions.

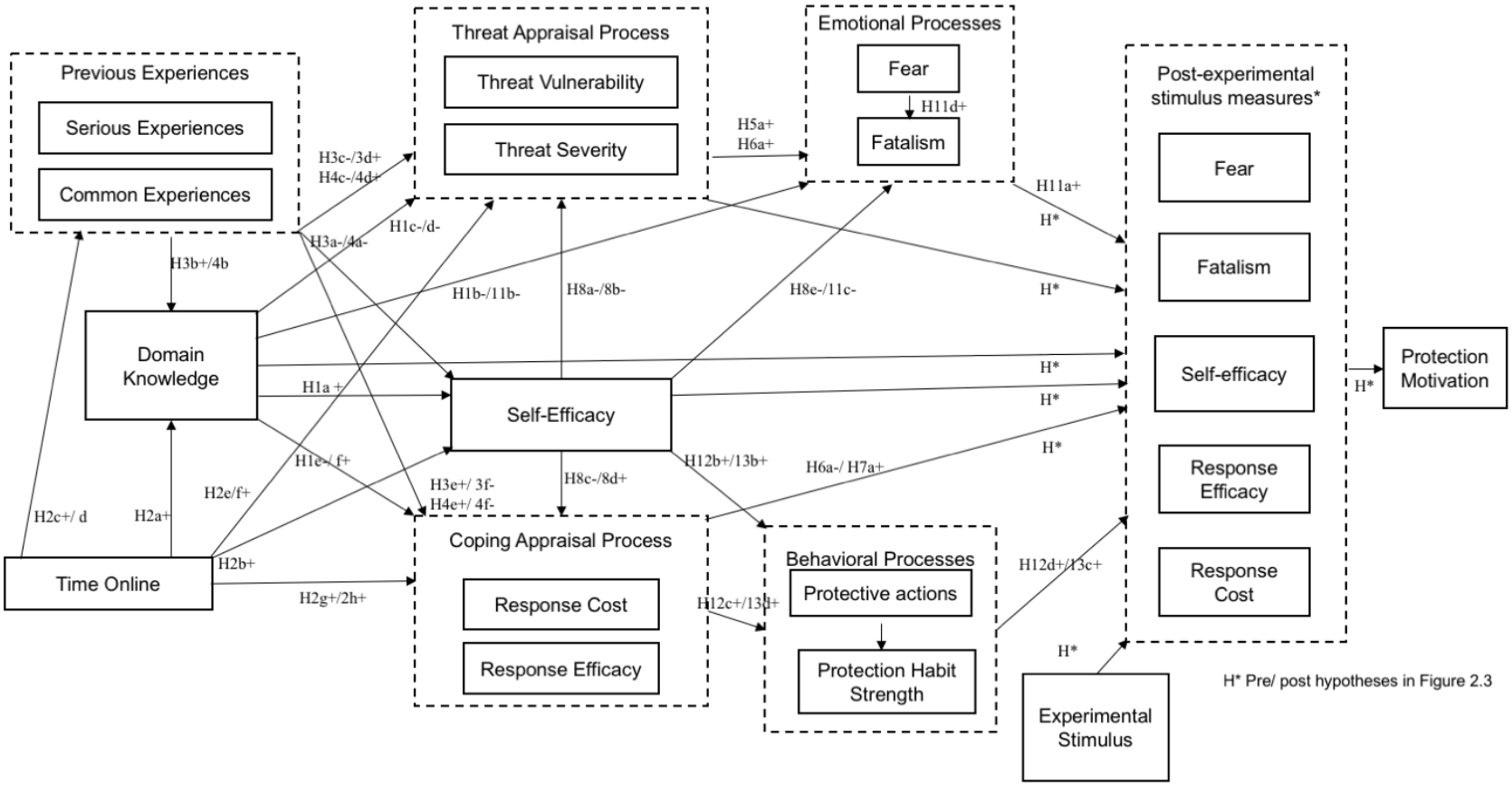
Thus, I hypothesize that as **domain knowledge** increases, **protection habit strength** will also increase (H16c).

As just mentioned, Individuals do not usually continue to perform a task if they feel it is useless. Thus, I hypothesize that as **response efficacy** increases, **protection habit strength** will also increase (H16d).

Finally, if someone routinely performs a task, it is very likely that they will continue to perform it (Boehmer et al., 2015).

Thus, I hypothesize that as **protection habit strength** increases, **protection motivation** will also increase (H16e). The hypotheses are shown in the model in Figure 3.3.

Figure 3.3: Revised model and hypotheses



3.4.2 Post message hypotheses

As the message will hopefully impact many of the key attitudes discussed in the previous chapter: fear, self-efficacy, response cost, and response efficacy. There is also the importance of examining if the message, which targets a specific cybersecurity behavior, will increase general protection motivation, or if it will only impact the specific behavior addressed in the message. This could be similar to health communications, where increasing domain knowledge about self-screening for cancer greatly improved compliance for this protective action (Nabi, Roskos-Ewoldsen, & Carpentier, 2008). On the other hand, if the motivation for the target behavior is lower than general protection motivation, this could indicate a usability issue- that individuals want to protect themselves but actually carrying out the task is difficult (Mannan & Van Oorschot, 2007). Thus, for all of the post message constructs we will look at both the general protection motivation and the target protection motivation.

3.4.2.1 Hypotheses about fatalism when exposed to a message

Since fatalism is a process that is often tied to inaction in some domains (McCrae, 1984), it would be informative to see if a message that triggers the threat and coping appraisal process would impact fatalism, especially in a complex environment as cybersecurity. Messages that inform users about emerging threats may serve to only strengthen fatalism. Yet, knowing the details of a specific threat may actually work to reduce fatalism. Learning about how they can specifically address a threat might reduce fatalism and increase the likelihood of enacting protections.

Thus, I hypothesize in the control condition that pre-message **fatalism** will be strongly correlated to post-message **fatalism** (H13a). Also, as **fatalism** increases,

general protection motivation will go down (H13b). I also predict that the **target protection motivation** will go down (H13c)

For those who get the experimental (training) message, I also hypothesize that pre-message **fatalism** will not be as strongly correlated as post-message **fatalism** in the control condition (H3d). Also, as **fatalism** increases, **protection motivation** will go down (H13e). Also, the **target protection** motivation will go up (H13f). These hypotheses are shown in Figure 3.4.

3.4.2.2 Hypotheses for other constructs to target protection motivation

Normally we would expect that if a message is able to encourage overall motivation, it would be successful at motivating towards the target behavior as well. However, given how frequently individuals in the focus groups discussed how frustrated they were performing security tasks despite their desire to protect themselves, I think that there might be higher general protection motivation and lower target protection motivation for many of these constructs. If there is a problem with usability of a security protection, then it will be apparent in the experimental condition as that is where they will see a demonstration of how to perform the task. If it is a motivational issue, then it will be apparent in both conditions, but especially the control condition.

For the **control condition**

Therefore, I hypothesize that as **fear** increases, **target protection motivation** will decrease (H9c).

I also hypothesize that as **self-efficacy** increases **target protection motivation** will also increase (H10c).

Also, as **response cost** increases I hypothesize that **target protection motivation** will decrease.

Finally, as **response efficacy** increases, I hypothesize that **target protection motivation** will increase.

For the **experimental (training) condition,** I predict the demonstration will help reduce fear compared to the control condition. However, I hypothesize the training will reduce **self-efficacy** compared to the control condition as they will see exactly what to do. I think that **response cost** will be higher compared to the control condition and that **response efficacy** will be lower. However, overall, I predict the following relationships-

I hypothesize that as **fear** increases, **target protection motivation** will decrease (H9cf).

I also hypothesize that as **self-efficacy** increases **target protection motivation** will also increase (H10c).

Also, as **response cost** increases I hypothesize that **target protection motivation** will decrease.

Finally, as **response efficacy** increases, I hypothesize that **target protection motivation** will also increase.

3.4.2.3 Hypotheses for domain knowledge on target protection motivation

Domain knowledge is the “people don’t know what they don’t know” quandary. Procedures that were considered “best practices” just a few months ago are routinely made obsolete by new exploits and weaknesses. Even though domain knowledge should act as a foundation that will only serve to make the impact of the message stronger, at higher levels it may act to mitigate a message. However, if individuals have a basic

understanding of threat vectors and solutions, being reminded of how them can protect themselves should serve to increase constructs that tend to increase protection motivation. This should be true for both conditions, with the experimental (training) condition serving to be tool to refresh their memory and reinforce positive attitudes.

Thus, I hypothesize for both **control** and **experimental** conditions-

As **domain knowledge** increases-

post fear will decrease (H1e)

post fatalism will decrease (H1j)

post-self-efficacy will decrease (H1f)

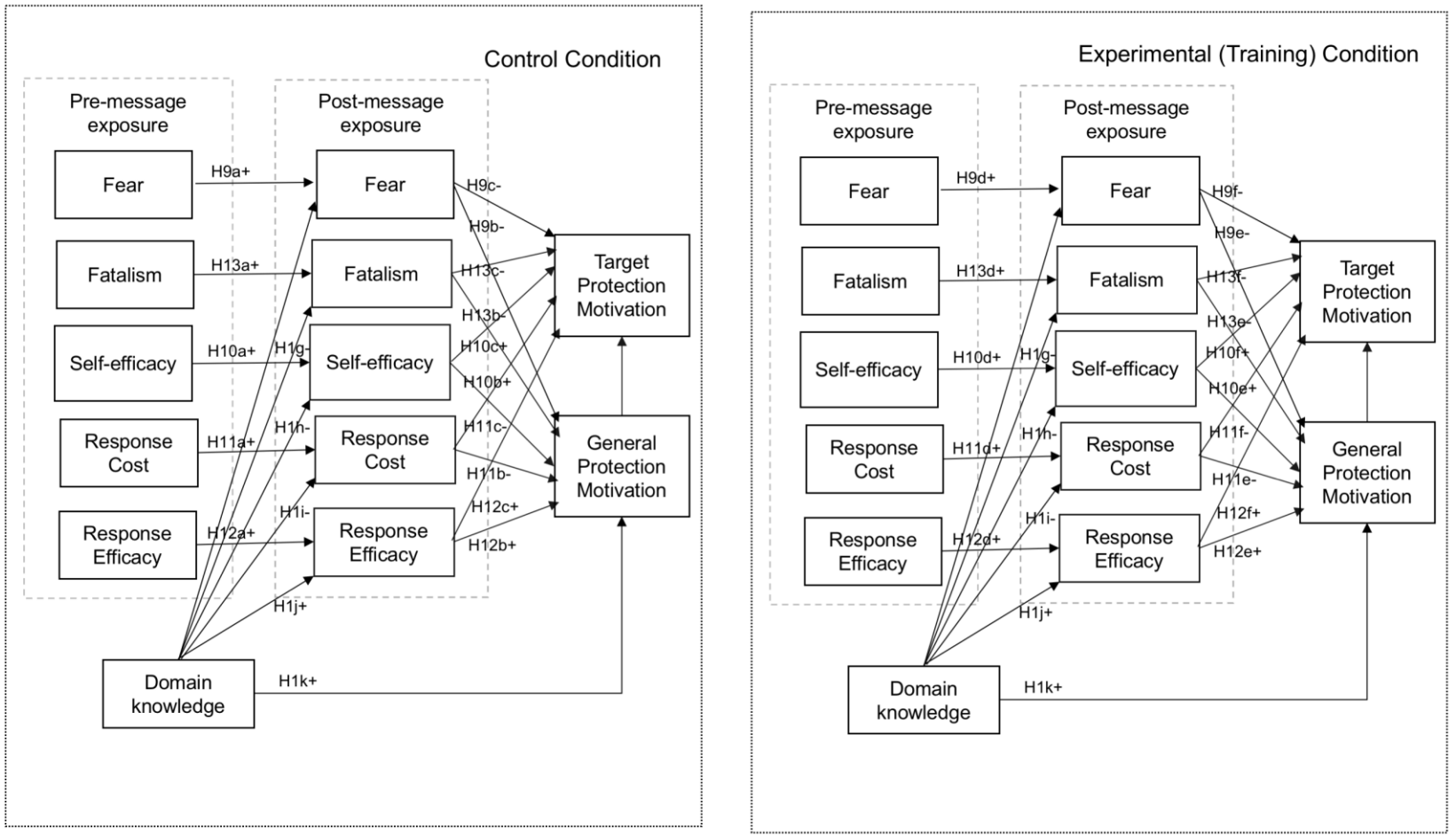
post response cost will decrease (H1g)

and **post response efficacy** will increase (H1h).

Also, since those with higher levels of **domain knowledge** should be familiar with many standard protective measures and thus more motivated to use them.

Thus, I hypothesize that as **domain knowledge** increases, both **general protection motivation** (H1i) and **target protection motivation** (H1k) will also increase.

Figure 3.4: Revised post message hypotheses



APPENDICES

Appendix 3.1: Focus group protocol

Focus Group Research Questions:

1. What are the perceived threats to online safety? (e.g., viruses, worms, hackers, spyware, browser hijackers
2. What do consumers do to improve online safety? (Their protection measures, behaviors, preparation, software, hardware, downloading)?
3. What do consumers believe that they can do to protect themselves? What resources do they use?
4. When consumers use take protective measures, what are the reasons for consumers' online safety behaviors (motivations, involvement levels, outcome expectations, bad experiences, campaigns, social norms)?
5. What are consumers' specific beliefs about the perceived positive and negative consequences of online safety behaviors?
6. What are the beliefs about specific skills that influence consumers' online safety self-efficacy?
7. What are the constraints that affect consumers' online safety (barriers)?
8. What specific threats and protections are relevant to online banking?
9. How do threats and protections vary by generation?

Questioning Strategy:

Welcome, Ground Rules, and Overview

Hello and welcome. We are about to get started. Let me make sure I have the right interview on my schedule! Everyone here was born [before 1946/between 1946 and 1954/between 1977 and 1992] and [is/is not currently banking online with REDACTED], is that right? Before we begin we have consent forms we would like you to review.

Hello and welcome.

Thank you for taking the time to join our discussion. My name is ____ and these are my assistants _____. We are researchers at Michigan State University.

We have asked you to come tonight to discuss your experiences with the dangers of the Internet and how you cope with them. Tonight, there are no right or wrong answers. We expect that you will have different experiences and differing points of view. Please feel free to share your point of view even if it differs from what other have said.

We are taping the session because we don't want to miss any of your comments. None of your names will be included in any reports. Your comments are confidential. Keep in mind that we're just as interested in negative comments as positive comments.

We have name tents here in front of us tonight. They help me remember names, but they can also help you. If you want to follow up on something that someone has said, if you want to agree, or disagree, or give an example, feel free to do that. Don't feel like

you have to respond to me all the time. Feel free to have a conversation with one another about these questions. I am here to ask questions, listen, and make sure everyone has a chance to share. We're interested in hearing from each of you. So if you're talking a lot, I may ask you to give others a chance. And if you aren't saying much, I may call on you. We just want to make sure we hear from all of you.

We are specifically interested in the technical threats risks that affect your computer or your ability to use your computer while online. So, I'll try to steer you away from talking about online stalkers, pornography, and other dangers that may threaten you or your loved ones, but not necessarily your computer or the information stored on it.

Feel free to get up and get more refreshments if you would like and remember we have incentive payments for you later. [PAUSE AND WAIT.]

[NOTE: ITEMS APPEARING IN ITALICS IN BRACKETS BELOW ARE CONCEPTS RELATED TO OUR THEORETICAL MODEL TO PROMPT THE FOCUS GROUP LEADER AND WILL NOT BE READ TO THE RESPONDENTS].

Focal Exercise

Let's begin. Just about everyone who uses the Internet has encountered problems at one time or another. You may have received requests for personal information or passwords, sometimes disguised as email from a reputable source. Or you many have had your browser hijacked by a website that they did not expect to see. Other times,

computer functions may be seriously affected by viruses and worms that enter our computers through email or hacker attacks. Or hackers may break into computers and steal personal information or leave behind destructive programs. Or they may interrupt you with a phony scan of your computer and offer to sell you a protection program on the spot. Or computers may secretly send personal information as a result of a program they downloaded or a web page they visited. As a result, some people would describe the Internet as a risky place, while others might say that the Internet is relatively safe. I'd like to ask each one of you to use the paper and pencil we provided to write down an incident that particularly sticks out in your mind. Then we'll go around and ask you to tell us about it and how you dealt with it. If you have never had any of these problems, congratulations! But please write down the threat you have heard about that worries you the most. [PAUSE WHILE WRITING]

Is everybody ready? Let's start over here with [NAME].If someone mentions a threat you are not familiar with, please stop us for an explanation. [PROBE FOR RISKS AND COPING MECHANISMS THAT HAVE NOT BEEN MENTIONED PREVIOUSLY, AVOID REPETITION.]

Online Banking

Online banking can be a particularly risky online activity since your identity can be stolen and your accounts drained in the worst case. [Whether or not you use online banking] which of the threats we have talked about especially concern you when you think about online banking?

a. For some, online banking is complicated, for others it is easy. Where do you stand on that? What are the barriers?
b. Online banking can also have important benefits. Which, if any, do you see?
c. What role do you think your credit union should play in protecting you online if you bank with them?
d. Do you think your credit union can protect you from threats while banking with them? [PROBE: WHY OR WHY NOT?]

[INTERMISSION. PAUSE FOR REFRESHMENTS.]

Coping with Online Threats

A lot of us are concerned about online threats but don't do anything about them, while others do. Tell me what you do or don't do to defend against threats of this type and to recover from them? Can you describe them to me? How routinely do you do them? What is your approach? [PROBE FOR]

a. Downloading patches
b. Running and updating anti-virus software
c. Installing personal firewall
d. Screening emails
e. Downloading spyware, popup or hijack blockers
f. Withholding personal information
g. Changing passwords
h. Other

Protection Resources

Preserving our online security is never-ending task as new threats emerge. Of the protections we have mentioned, which do you feel are most effective and least effective?

a. Which ones do you wish you knew more about?

b. Which ones require the most cost or effort to use?

c. Where do you turn for help when you run into a problem you can't solve?

d. Do others rely on you to solve their online problems?

Summary

Let me summarize what I heard tonight.

Closing Thoughts

If you could make a recommendation about protecting people like yourselves and your home computers better, what would it be?

Any last comments you would like to make?

Thanks for coming.

We have envelopes for you as you exit.

Appendix 3.2: IRB approval for focus group research

MICHIGAN STATE UNIVERSITY

Initial IRB Application Determination *Exempt*

June 11, 2013

To: Nora Rifon
309 Comm. Arts Building
MSU

Re: **IRB# x13-582e** Category: Exempt 1-2
Approval Date: June 11, 2013

Title: Online Safety for the Ages Focus Groups

The Institutional Review Board has completed their review of your project. I am pleased to advise you that **your project has been deemed as exempt** in accordance with federal regulations.

The IRB has found that your research project meets the criteria for exempt status and the criteria for the protection of human subjects in exempt research. **Under our exempt policy the Principal Investigator assumes the responsibilities for the protection of human subjects** in this project as outlined in the assurance letter and exempt educational material. The IRB office has received your signed assurance for exempt research. A copy of this signed agreement is appended for your information and records.

Renewals: Exempt protocols do not need to be renewed. If the project is completed, please submit an ***Application for Permanent Closure***.

Revisions: Exempt protocols do not require revisions. However, if changes are made to a protocol that may no longer meet the exempt criteria, a new initial application will be required.

Problems: If issues should arise during the conduct of the research, such as unanticipated problems, adverse events, or any problem that may increase the risk to the human subjects and change the category of review, notify the IRB office promptly. Any complaints from participants regarding the risk and benefits of the project must be reported to the IRB.

Follow-up: If your exempt project is not completed and closed after three years, the IRB office will contact you regarding the status of the project and to verify that no changes have occurred that may affect exempt status.

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

Good luck in your research. If we can be of further assistance, please contact us at 517-355-2180 or via email at IRB@msu.edu. Thank you for your cooperation.

Sincerely,

H. McGee

Harry McGee, MPH
SIRB Chair

c: Robert LaRose, Saleem Alhabash

Office of Regulatory Affairs
Human Research Protection Programs

Biomedical & Health Institutional Review Board (BIRB)

Community Research Institutional Review Board (CRIRB)

Social Science Behavioral/Education Institutional Review Board (SIRB)

Olds Hall
408 West Circle Drive, #207
East Lansing, MI 48824
(517) 355-2180
Fax: (517) 432-4503
Email: irb@msu.edu
www.humanresearch.msu.edu

WORKS CITED

WORKS CITED

Arachchilage, N. A. G., & Love, S. (2014). Security Awareness of Computer Users: A Phishing Threat Avoidance Perspective. Computers in Human Behavior, 38, 304–312. http://doi.org/10.1016/j.chb.2014.05.046

Bandura, A. (2001). Social Cognitive Theory : An Agentic Perspective. Annual Review of Psychology, 52, 26.

Berkowitz, A. (2005). An Overview of the Social Norms Approach. Changing the Culture of College Drinking: A Socially Situated Prevention Campaign, (January 2005), 1–29. http://doi.org/10.1080/13552074.2016.1194020

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of Online Safety Behaviour: Towards an Intervention Strategy for College Students. Behaviour & Information Technology, 3001(July), 1–14. http://doi.org/10.1080/0144929X.2015.1028448

Czaja, S. J., & Barr, R. a. (1989). Technology and the Everyday Life of Older Adults. The ANNALS of the American Academy of Political and Social Science, 503(1), 127–137. http://doi.org/10.1177/0002716289503001010

Czaja, S. J., & Sharit, J. (1998). Age Differences in Attitudes Toward Computers. The Journals of Gerontology. Series B, Psychological Sciences and Social Sciences, 53(5), P329–P340. http://doi.org/10.1093/geronb/53B.5.P329

Hill, S. (2015, March). Are Cookies Crumbling our Privacy? Digital Trends. Retrieved from https://www.digitaltrends.com/computing/history-of-cookies-and-effect-on-privacy/

Icek Ajzen, Sparks, P., Ajzen, I., & Hall-box, T. (2002). Perceived Behavioral Control, Self-efficacy, Locus of Control, and the Theory of Planned Behavior. Journal of Applied Social Psychology, 80(6), 2918–2940. http://doi.org/10.1111/j.1559-1816.2002.tb00236.x

LaRose, R. (2010). The Problem of Media Habits. Communication Theory, 20(2), 194–222. http://doi.org/10.1111/j.1468-2885.2010.01360.x

Larose, R., Lin, C. A., & Eastin, M. S. (2003). Unregulated Internet Usage: Addiction, Habit, or Deficient Self-Regulation? Media Psychology, 5(3), 225–253. http://doi.org/10.1207/S1532785XMEP0503_01

Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. MIS Quarterly, 33(1), 71–90. http://doi.org/Article

Madden, T. J., Ellen, P. S., & Ajzen, I. (1992). A Comparison of the Theory of Planned Behavior and the Theory of Reasoned Action. Personality and Social Psychology Bulletin, 18(1), 3–9. http://doi.org/10.1177/0146167292181001

Mannan, M., & Van Oorschot, P. C. (2007). Security and Usability: The Gap in Real-World Online Banking. IEEE Technology and Society Magazine, 26, 1–14. http://doi.org/10.1109/MTAS.2007.335568

McCrae, R. R. (1984). Situational Determinants of Coping Responses: Loss, Threat, and Challenge. Journal of Personality and Social Psychology, 46(4), 919–928. http://doi.org/10.1037/0022-3514.46.4.919

Microsoft. (2016). Microsoft Security Intelligence Report, 21, 7–8. Retrieved from https://www.microsoft.com/security/sir/story/default.aspx#!10year_timeline

Miles, M. B., Huberman, A. M., & Saldana, J. (2014). Qualitative Data Analysis (3rd ed.). Washington, D.C.: SAGE Publications.

Millar, M., & Dillman, D. (2011). Improving Response to Web and Mixed-Mode Surveys. Public Opinion Quarterly, 75(2), 249–269.

Miller, T. A. (2016). Health Literacy and Adherence to Medical Treatment in Chronic and Acute Illness: A Meta-Analysis. Patient Education and Counseling, 99(7), 1079–1086. http://doi.org/10.1016/j.pec.2016.01.020

Mitzner, T. L., Boron, J. B., Fausset, C. B., Adams, A. E., Charness, N., Czaja, S. J., … Sharit, J. (2010). Older Adults Talk Technology: Technology Usage and Attitudes. Computers in Human Behavior, 26(6), 1710–1721. http://doi.org/10.1016/j.chb.2010.06.020

Nabi, R. L., Roskos-Ewoldsen, D., & Carpentier, F. D. (2008). Subjective Knowledge and Fear Appeal Effectiveness: Implications for Message Design. Health

Communication, 23, 191–201. http://doi.org/10.1080/10410230701808327

Petty, R. E., Briñol, P., & DeMarree, K. G. (2007). The Meta–Cognitive Model (MCM) of Attitudes: Implications for Attitude Measurement, Change, and Strength. Social Cognition, 25(5), 657–686. http://doi.org/10.1521/soco.2007.25.5.657

Shillair, R., LaRose, R., Jiang, M., Rifon, N. J., & Cotten, S. R. (2017). The Role of Habits and Prior Experience in Motivating User Cybersecurity Behavior. In International Communication Association (p. 30). San Diego, California.

Tsai, H. S., Shillair, R., & Cotten, S. R. (2017). Social Support and “Playing Around.” Journal of Applied Gerontology, 36(1), 29–55. http://doi.org/10.1177/0733464815609440

Witte, K. (1994). Fear Control and Danger Control: A Test of the Extended Parallel Process Model (EPPM). Communication Monographs. http://doi.org/10.1080/03637759409376328

Witte, K., & Allen, M. (2000). A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns. Health Education & Behavior, 27(5), 591–615. http://doi.org/10.1177/109019810002700506

Zipf, G. K. (1949). Human Behavior and the Principle of Least Effort. Addison-Wesley Press.

Chapter 4
Pilot study

4.1 Introduction

4.1.1 Developing and refining a PMT instrument

As indicated by the review of the focus group materials in the previous chapter, participants in the focus groups discussed the threat appraisal process and their coping strategies when reflecting on past experiences with online threats. This fits well with Maddux and Rogers (1983) model of how individuals cognitively processed threats and planned their potential responses to these threats. Thus, using protective motivation theory (PMT) in research dealing with cybersecurity is appropriate. As discussed in the previous chapter, there were some constructs that have not been addressed up to this point in cybersecurity PMT research. This included the constructs of fatalism, protective routines, and protection habits. In this chapter I will detail the operationalization of these constructs, the development and testing of a message, and the results of a pilot test to test the measurement instrument.

4.1.2 Fatalism

As individuals recount their experiences with a past cyber threat to a group, it expected that they might explain their actions very rationally and not express fear. So, if fear is expressed months, or even years, after an event it must be very profound. This would support the importance of measuring fear both before and after presenting a cybersecurity compliance message. However, as discussed in the previous chapter, participants discussed fatalism, that everyone would be touched by an attack at some point. Fatalism, is seen in previous studies as a “defensive reaction to a fear appeals message” in the health domain (Roskos-Ewoldsen, Yu, & Rhodes, 2004 p 57). This could be either non-use of protections or using protections but having lower expectations of

efficacy. The focus group indicated that fatalism does not seem to uniformly cause inaction in the cybersecurity realm in this research. By examining it further, as a separate construct, then it is possible to test if it produces a similar response as fear. Given the myriad of potential ways that individuals face risk from cyberattacks, a small dose of fatalism might be a way to realistically deal with breaches and improve one's protections in the future. Or, fatalism could be a maladaptive response that excuses inaction or poor digital hygiene. Measuring fatalism and seeing how it impacts the protection motivation process should help bring insights.

4.1.3 Threat vulnerability and threat severity new items

Online threats are constantly changing as well as how seriously they would impact our lives. In the late 1990s, major cyber threats were viruses and having one's computer slow down, or a file get corrupted because of malicious software. Phishing emails were pretty obvious with multiple grammar errors, misspellings and grainy images. Today's threats and threat actors are much more sophisticated. The potential severity of attacks is ever increasing as not just computers, but household systems and even vehicles are connected to the Internet. Previously, reflective scales examining one or two common dimensions of online threats were very good at capturing perceptions of threat vulnerability and severity, expanded items should help improve capturing attitudes towards threat vulnerability and severity in today's environment. New threat vulnerability items include asking participants how likely they think: My email or social media (e.g., Facebook) account will be compromised, my files or my computer might get encrypted and held hostage (i.e., ransomware), I might eventually have to have the computer hard drive wiped and reinstall my programs, and I might be threatened with information gained from someone monitoring my computer activities (e.g., spyware). New threat severity items include asking how

serious it would be to them if: their email account was hacked, and they had to reset passwords; malware was on their computer and criminals could use it; if spyware was on their computer and others could watch what they typed; and it their computer files got locked up and they couldn't access them. Full items are in Appendix 4.1.

4.1.4 Protective Behaviors

In the focus groups, many of the participants discussed routine steps that they followed to protect themselves. In measuring the impact of a message and future intentions, it would be very helpful to know participants current protections and also how comfortable and routinely they perform those protections. Many of the participants in the focus groups mentioned they had training in the workplace on how to perform some cyber safety routines. It was not clear if those training efforts included the why and increased domain knowledge. It would be important to find if the actions they perform are tied to wider understanding of threat issues (i.e., domain knowledge). Protective actions measured include: having protective software on one's computer (e.g., anti-virus or anti-malware), changing to a stronger password, and checking for https. Protection habits, how comfortable a person feels in carrying out these tasks is more focused, thus previously used measures are appropriate (Shillair, LaRose, Jiang, Rifon, & Cotten, 2017).

4.1.5 Protection Motivation

Protection motivation is assessed with items that included general protections such as using hard to guess and unique password and updating virus protection software. Since the message targets a specific behavior it would be helpful to measure if the message impacts an overall, general intention to protect, or if it impacts intentions

towards the specific behavior. Thus, in addition to the general protection motivation construct, a three-item scale that assesses the motivation to follow through on the specific behavior(s) of updating one's browser is assessed as target protection motivation. All items for the previous constructs are in Appendix 4.1.

4.1.6 Developing an effective cybersecurity compliance message

In order to provide pragmatic guidance to stakeholders who want to improve communications strategies it is important to develop more than just a tool, but a strategy and methodology to make future tools. Health compliance messages that are successful usually include "how to" do something rather than just "you should" do something, making the "correct" behavior more readily memorable (Rhodes, Roskos-Ewoldsen, Edison, & Bradford, 2008; Roskos-Ewoldsen et al., 2004). A typical cybersecurity compliance message includes awareness of the threat, reminder of the severity and a call to action (e.g., here is a problem, it is bad, you should protect yourself). According to many learning theories, a message that includes training, with an additional demonstration of exactly how to perform that task, has to potential to increase protection motivation (Bandura, 1971, 1977; Gioia & Manz, 1985). However, in a highly technical environment, making individuals aware of a new threat often means admitting the previous solution they were trusting to protect themselves is no longer sufficient. This may produce a lower trust in response efficacy, actually diminishing the likelihood of compliance. Demonstrating how to carry out the task may greatly improve likelihood of compliance, but only an experiment could test if this is true.

This research takes a typical cybersecurity compliance message and present the base message as a control. The message with contextual training is the experimental

condition. By randomly assigning participants to the control or training condition and testing changes in key attitudes, the experimental design should help give fresh insights. This would allow better understanding of how message design impacts some of the key cognitive and emotional processes in encouraging protection motivation. Since there is a combination of new variables and constructs to test, it is important to test the research instrument rigorously to assure that the new items have good internal and external validity and check the proposed cybersecurity compliance message for effect.

4.1.7 Elements of the message

The goal of the message is to first help the viewer to identify with the problem, to see if it impacts them personally. Next, is the step to make them aware of an outside threat. The third step is to make them aware that the browser has weaknesses as threats evolve. The message reminds them that there are others working to improve their safety, but they need to personally check to make sure things are working correctly. Finally, the message ends with a call to action. Visuals were made using clip art and the experimental condition also includes a contextual demonstration of how to perform the task and encouragement to improve confidence. Visuals and clip are paced to maintain viewers' attention and engagement without being distracting. They are selected to increase awareness without eliciting high levels of fear. Full text of the message is in Appendix 4.4.

4.2 Methods

4.2.1 Construction of a research instrument

This study builds upon previous research in PMT, thus whenever possible, and appropriate, previously used and tested scales are utilized. Since many of the scales were developed a few years ago and online threats, user interfaces, and ubiquity of computing

devices have significantly changed, it was necessary to verify each scale with exploratory factor analysis (EFA) methods to test for validity with a current population sample. Variables for each construct, sources for traditional scales and the newly developed items are in the appendix for this chapter. The results of the EFAs are in the results section of this chapter.

Self-efficacy, as discussed in Chapter 2, is seen as core to individuals acting autonomously for their best interest. Thus, self-efficacy in this model is seen as the focus point in the process of evaluating and responding to threat. Both time online and domain knowledge can potentially help build confidence, therefore, building the individual's self-efficacy. The more time individuals spend online, the more likely to be self-efficacious (Hasan, 2003). Operationalization for self-efficacy is taken from Anderson and Agarwal, (2010).

As mentioned before, personal threat experiences, such as having one's social media account hacked, would most likely decrease one's self-efficacy, possibly leading to even not using certain technologies (Liang & Xue, 2009). Items for threat experiences were taken from focus group materials, my previous research and reports of current threat trends (Microsoft, 2016; Shillair, LaRose, & VanOsch, 2015). Other constructs in the model include habit strength, which is measured using variables adapted from Venkatesh, Thong, and Xu, (2012). Response efficacy and response cost are adopted from Liang & Xue, (2010) with items for response cost also taken from Vaniea, Rader, and Wash, (2014). Threat vulnerability and threat severity were adapted from Liang & Xue, (2010) with many additional variables taken from the focus group review. The constructs of fear

and fatalism were taken from Shillair, LaRose, & VanOsch (2015) and Shillair (2016), with modifications after reviewing the focus group materials.

In order for the cybersecurity compliance message to be convincing to participants in this study it would need to deal with a task that the average user could perform themselves, but they might not be aware that they should perform it. It also should be something that is rather important so that the threat and coping appraisal processes would be triggered. Some topics, like using strong passwords, are widely discussed and thus it would be hard to develop a message that would not trigger a response that was biased by any previous training, or be confounded by messages that an individual already heard. It also would help if it was a security activity that was easy to do, quick to learn, yet often neglected. Thus, the subject of checking if one's browser was up-to-date was selected as the specific context of the compliance messages. This is a simple, yet often overlooked, task.

Support for the choice of browser software updates is seen in recent research. A recent major study that tracked users actual use and then asked them about their security practices found that users often claimed their Chrome browsers were up-to-date, yet there was almost no correlation with the actual condition of their browser software (Wash, Rader, & Fennell, 2017). This is not surprising because modern browsers are supposed to update themselves, but often updates do not run for a variety of reasons. To check for browser updates is usually within several layers of menus, thus it is often overlooked.

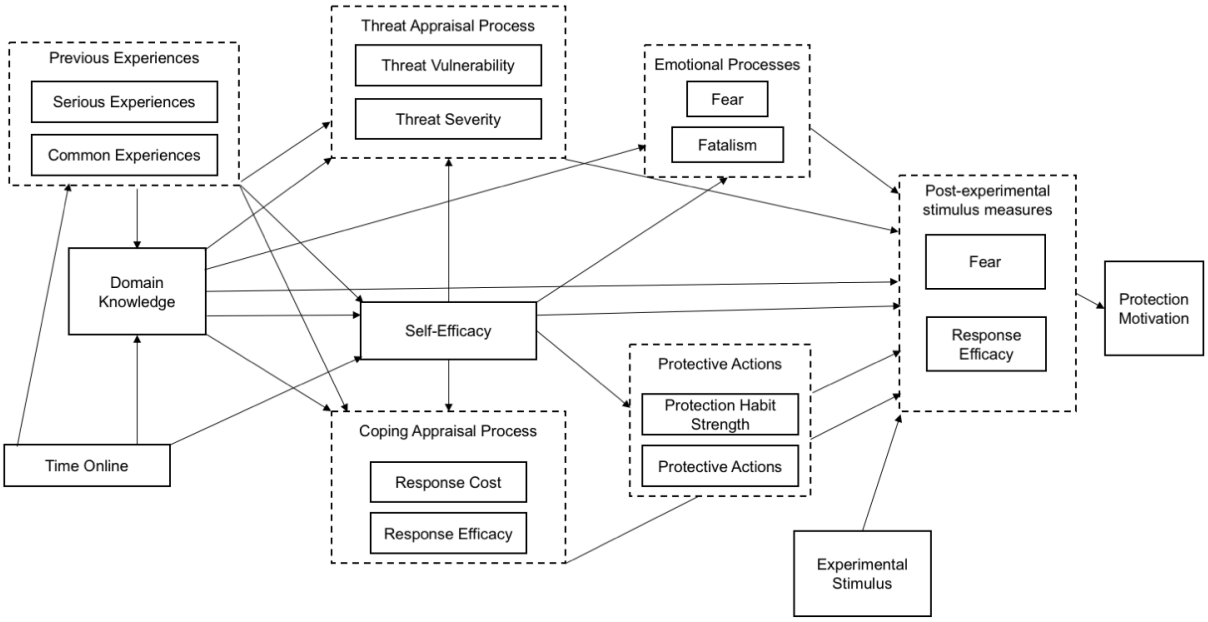
Encouraging users to update their browsers once they are aware of the dangers should initiate the threat/coping appraisal process and it is obscure enough that the fear process might be triggered in those with lower domain knowledge, leading to lower

motivation to protect themselves as proposed by Witte (1994). For those who have higher domain knowledge (e.g., they know how to check their browser software status), the cognitive processes should prevail, and they should be motivated to continue protecting themselves as proposed by Rippetoe and Rogers (1987).

The research model includes the traditional PMT constructs, several of these having a few new items as indicated by the review of the focus groups. It also includes the previous experiences that the user had with online threats and the amount of time they spend online as feeding into perceptions of self-efficacy. The construct of domain knowledge is new to the PMT model. The model is shown in Figure 4.1. Only the paths from the basic processes and practices are included for simplicity. The results of the full path model are presented in the results section of this chapter. The items for each construct and the results of the exploratory factor analysis are also discussed in the results section of this chapter. The core of the newly proposed model, the moderation interaction of the message condition (i.e., control or vicarious training), is analyzed separately and also discussed in the results section.

Since this phase of the research is to test the research instrument, the pre-post measures were limited to the two that had the greatest impact(s) in many previous studies. These were fear since it was tied to the EPPM and bypassing a cognitive response (Roskos-Ewoldsen et al., 2004; Witte & Allen, 2000; Witte, 1994) and response efficacy, since it is closely tied to both the cognitive process and domain knowledge (Hanus & Wu, 2015; Lee, Larose, & Rifon, 2008). This allowed the testing to be more focused and acknowledges the limits of the smaller student sample in testing a complex model. The model for the pilot test is shown in Figure 4.1.

Figure 4.1: Model for pilot test



4.2.2 Construction of the cybersecurity message and experimental condition

To have a more robust and rigorous testing of the potential impact of domain knowledge on the threat and coping appraisal process, the message itself will be presented using an experimental design. The control condition includes a cybersecurity compliance message, and the experimental condition has the same compliance message, but also includes a vicarious learning element. This allows participants will learn how to actually perform the task. Since there are several major browsers (i.e., Google Chrome, Firefox, Safari, and Microsoft Edge) the vicarious learning element was presented using the browser software that participants indicated they commonly use.

The message was recorded by a professional voice actor and the visual snippets were primarily clip art that were designed for simplicity. The training condition included

screen grabs of the participants' commonly used browser and how to check for updates. For this particular study, there was not an accessible (subtitles) version made as this would add a layer of complexity to the current study. However, the author would welcome future collaborations to test this in material using ways that increase accessibility for visual and auditory special needs audiences. The final video was tested informally with participants from ages and skill levels to test for clarity, interest, and comprehension.

4.2.3 Pilot test sample

To test the instrument, we wanted a population that would probably have basic knowledge about computer threats and who frequently used computers in their daily lives. A college student sample was appropriate to meet these criteria. The goal of the pilot test was to check the research instrument, especially the new constructs and the new scale items. Also, this phase of the research is needed to test the message to see how large a sample is needed for the final wave of data collection. A sample size of 60 for the pilot test was selected since this would allow for approximately 30 individuals in each condition (control or vicarious learning) and allow for EFA of new items.

I utilized our university's SONA research system to recruit participants for the study. The SONA program supports researchers by recruiting participants from both student and community populations for research projects. After getting IRB approval (#i054781) for the pilot study, students were recruited from the SONA pool and were compensated for their time through extra credit in their classes. The SONA system helps protect the anonymity of participants as well as facilitating the assembly of a data pool. Since it was expected that some students might not finish the survey or that their data

might be incomplete or not pass quality controls, 72 participants were solicited to ensure collection of at least 60 valid surveys.

All completed surveys were screened for quality. Those that had extensive sections missing, or were completed in an extremely short time, or had multiple questions with the same answer, or if they did not pass the attention check question were deleted. The remaining 69 surveys were first analyzed using SPSS v. 25 for frequencies and exploratory factor analysis. Each new item was developed from analysis of focus group interviews, thus increasing external validity as expressed opinions of participants. Internal reliability was tested using exploratory factor analysis (EFA). The EFA for each construct included first testing for Bartlett's test of sphericity, which tests the null hypothesis, running a correlation matrix, Kaiser-Meyer-Okin (KMO), and looking for Eigenvalues of over 1.0 and by examining a scree plot. The variables were all tested using a Principal Component Analysis which reduces the number of items while retaining as much of the variance as possible (Meulman, Anita., & Heiser, 2004). The resulting pattern matrix and structure matrix were examined to confirm where the variables lined up as factors. Finally, Cronbach's alpha (α) was run on the refined constructs to test for internal reliability. After eliminating items that did not load well for internal validity the revised constructs were examined using Pearson's Zero Order Correlation and the results are in Table 4.1.

For path analysis of the full model, it was tested using SmartPLS 3.1.8 (Ringle, Wende, & Becker, 2015), item loadings were noted on reflective constructs and only items loading higher than .500 were retained. Formative constructs were checked for variance inflation factors (VIF) and any over 3.3 were dropped (Diamantopoulos, Riefler, & Roth,

2008). The final moderation analysis of the impact of domain knowledge and the experimental condition was done using Hayes PROCESS v. 3 (2017).

4.3 Results

4.3.1 Results of exploratory factor analysis

Previous experiences (n=18), were based on items developed by (Shillair, 2015) and items from the focus group review, based on experiences that individuals reported as having happened to them. This included both common experiences (e.g., getting a phishing email) to more serious incidents (e.g., having one's computer camera controlled by someone else and having their pictures taken). Each of these items was measured with seven possible choices: never, once, a couple times, several times, many times, frequently, and always. All items for scales are in Appendix 4.3. When these items were factored based on Eigenvalues of over 1 and checked by a scan of a scree table output, led to 4 factors. To eliminate single item factors and factors that had variables with weak loadings, the items were run again, and the resulting 2 factor answer had a KMO of .783, Bartlett's Test of Sphericity had Chi-Square 892.384, df 190 and significance of <.001. The two factors were **common threat experiences** (n=7, α=.739) and **serious threat experiences** (n=11, α=.934) .

Time online was two items, 1) time spent on a laptop or desktop computer and 2) time spent on the Internet on all computing devices. Given that this was a college student sample, time on desktops or laptops was used as a proxy for study or work related time online. This ranged with 24.1% reporting being on desktop or laptop computers at least 1 hour but less than 3 daily, 36.2% reporting 3-5 hours daily, and 27.6% reporting 5-8 hours. Time spent online on all devices would indicate comfort of using devices and activities

online. This were 13.8% being online 1-3 hours daily, 32.8% online 3-5 hours, 31% 5-8 hours daily, and 15.5% being online 8-10 hours daily.

All of the following items were measured with a seven-point scale of strongly disagree to strongly agree.

Self-efficacy (n=3, a=.821) was based on the items by Anderson and Agarwal (2010).

Threat severity and **threat vulnerability** were based on work by Liang and Xue, (2009) and enriched by new items from the focus group insights. Threat severity's (n=6, α=.965) had a KMO of .881, Bartlett's Test of Sphericity had Chi-Square 411.744, df 15 and significance of <.001. Threat vulnerability (n=8) had a KMO of .775, passed a Bartlett's Test of Sphericity with a Chi-Square 239,591, df 28 and significance of <.001. It formed two factors, vulnerability to common items (n=4, α=.804) and vulnerability to serious items (n=4, α=.804).

Response Cost, of following online safety procedures was explored by Liang and Xue (2009) and more recently by others (Shillair, 2016; Shillair et al., 2015; Vaniea et al., 2014) were further modified by items from the focus group. The new items focused on the frequent complaints about difficulties in remembering hard to guess passwords and managing multiple passwords. As discussed in the previous chapter, time pressures and seeing security precautions as detracting from what the user intends to do were discussed more frequently than the cost of purchasing security software. Response cost items had a KMO of .750, Bartlett's Test of Sphericity had Chi-Square 135.169, df 36 and significance of <.001. Using the structure matrix, Eigenvalue over 1.0, and scree plot it was determined that these formed one construct (n=5, α =.835).

Response efficacy (n=7) items had a KMO of .907, Bartlett's Test of Sphericity had Chi-Square 310.363, df 21 and significance of <.001. Using the structure matrix, Eigenvalue over 1.0, and scree plot it was determined that these formed two constructs with only two items on the second construct. These items were dropped. The items for response efficacy (n=5, a=.920) were also measured post-message exposure, with **post response efficacy** (n=5, α=.963).

Fear and Fatalism: The items for fear and fatalism (n=n) items were tested together to assure that the items strongly loaded on each construct. The items had a KMO of .677, Bartlett's Test of Sphericity had Chi-Square 326.776, df 78 and significance of <.001. Using the structure matrix, Eigenvalue over 1.0, and scree plot it was determined that these formed two constructs, with fatalism (n=4, a=.693), fear (n=5, a=.858). Post exposure to the message the same items for fear were used as **post fear** (n=5, a=.891).

Protection Habit Strength: The items for protection habit strength (n=5, a=.965) were a KMO of .887, Bartlett's Test of Sphericity had Chi-Square 346.889, df 10 and significance of <.001. Using the structure matrix, Eigenvalue over 1.0, and scree plot it was determined that these formed one construct.

Protection Motivation: The items for protection motivation (n=9, α=.936) were a KMO of .858, Bartlett's Test of Sphericity had Chi-Square 465.072, df 36 and significance of <.001. Using the structure matrix, Eigenvalue over 1.0, and scree plot it was determined that these formed one construct.

Protective Actions: The items for protective actions were formative, thus they were tested for discriminant validity. See Table 4.3 for weight, standard error, t-statistics, p-values, and VIF.

Domain knowledge: These items were developed by Pew Internet Research and used with permission (Olmstead & Smith, 2017). These items cover a range of basic information about end user cybersecurity, such as recognizing a strong password and recognizing two-factor identification. Two additional items were added that specifically dealt with browser software updates and was information specifically covered in the test message. The specific two items were tested after the message to check for learning.

The constructs were run in a Pearson's Zero-order correlation. The results are in Table 4.1. For this pilot study only one construct from the cognitive dimension of PMT (i.e., response efficacy) and one construct from the emotional process (i.e., fear) were tested both before and after the exposure to the message.

Table 4.1: Pearson's zero order correlations of constructs

	Self-Efficacy	Domain Knowledge	Threat Severity	Threat Vulnerability	Response Efficacy	Response Cost	Fear	Fatalism	Protective Actions	Protection Habits	Post Fear	Post Response Efficacy	Protection Motivation
Self-Efficacy	1												
Domain Knowledge	.036	1											
Threat Severity	.158	-.167	1										
Threat Vulnerability	.100	-.163	.378**	1									
Response Efficacy	.287*	.131	.102	.171	1								
Response Cost	-.019	-.059	.361**	.419**	.072	1							
Fear	.056	-.016	.176	.373**	.364**	.240*	1						
Fatalism	.060	-.224	.107	.080	.064	.256*	.263*	1					
Protective Actions	-.001	.304*	-.197	.035	-.035	-.213	.025	-.295*	1				
Protection Habit	.144	-.011	.035	.150	.439**	-.052	.098	.067	.066	1			
Fear POST	-.146	.022	.049	.294*	.249*	.087	.614**	.195	-.010	.180	1		
Response Efficacy POST	.364**	.324**	.156	.124	.514**	-.052	.391**	-.001	.069	.030	.194	1	
Protection Motivation	.335**	.196	.194	.212	.563**	.085	.334**	.044	-.005	.344**	.307*	.704**	1

*. Correlation is significant at the 0.05 level (2-tailed). **. Correlation is significant at the 0.01 level (2-tailed).

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

The average variance extracted from the analysis of the constructs is in AVE of reflective constructs are in Table 4.2 All of the items except Fatalism were above the .500 level as suggested by Fornell and Larcker (1981).

Table 4.2: AVE of constructs

	AVE
Threat Severity	0.840
Threat Vulnerability	0.557
Response Efficacy	0.780
Response Cost	0.572
Fear	0.604
Fatalism	0.483
Protection Habits	0.878
Fear POST	0.710

Formative items were tested for discriminant validity using several methods. The variance inflation factor (VIF) was well below the 5.0 maximum as suggested by O'Brien, (2007), although several items were above the 3.3 limits suggested by (Diamantopoulos et al. (2008). The items over 3.3 were kept in the model as this phase was only a test of the model and the final population would probably have a more varied set of experiences and habits than a sample from one university. However, overall the items seemed to load well with minimal VIF issues.

Table 4.3: Discriminant validity for formative constructs

Construct	Item	Weight	Std. Error	T-Stat.	p-value	VIF
Protective Actions	Q24_11	0.390	0.227	3.475	0.001	1.581
	Q24_12	0.326	0.285	2.686	0.007	1.855
	Q24_13	0.211	0.242	1.936	0.053	3.624
	Q24_2	0.160	0.238	1.974	0.049	1.187
	Q24_4	-0.232	0.339	1.130	0.259	3.351
	Q24_7	0.498	0.268	2.682	0.007	1.332
Protection Motivation	Q47_1	0.543	0.051	18.296	0.000	2.291
	Q47_3	0.086	0.155	3.685	0.000	2.409
	Q47_4	0.128	0.101	7.327	0.000	2.387
	Q47_5	0.461	0.078	10.858	0.000	3.792
	Q47_6	-0.044	0.078	10.174	0.000	4.052

Table 4.3: (cont'd)

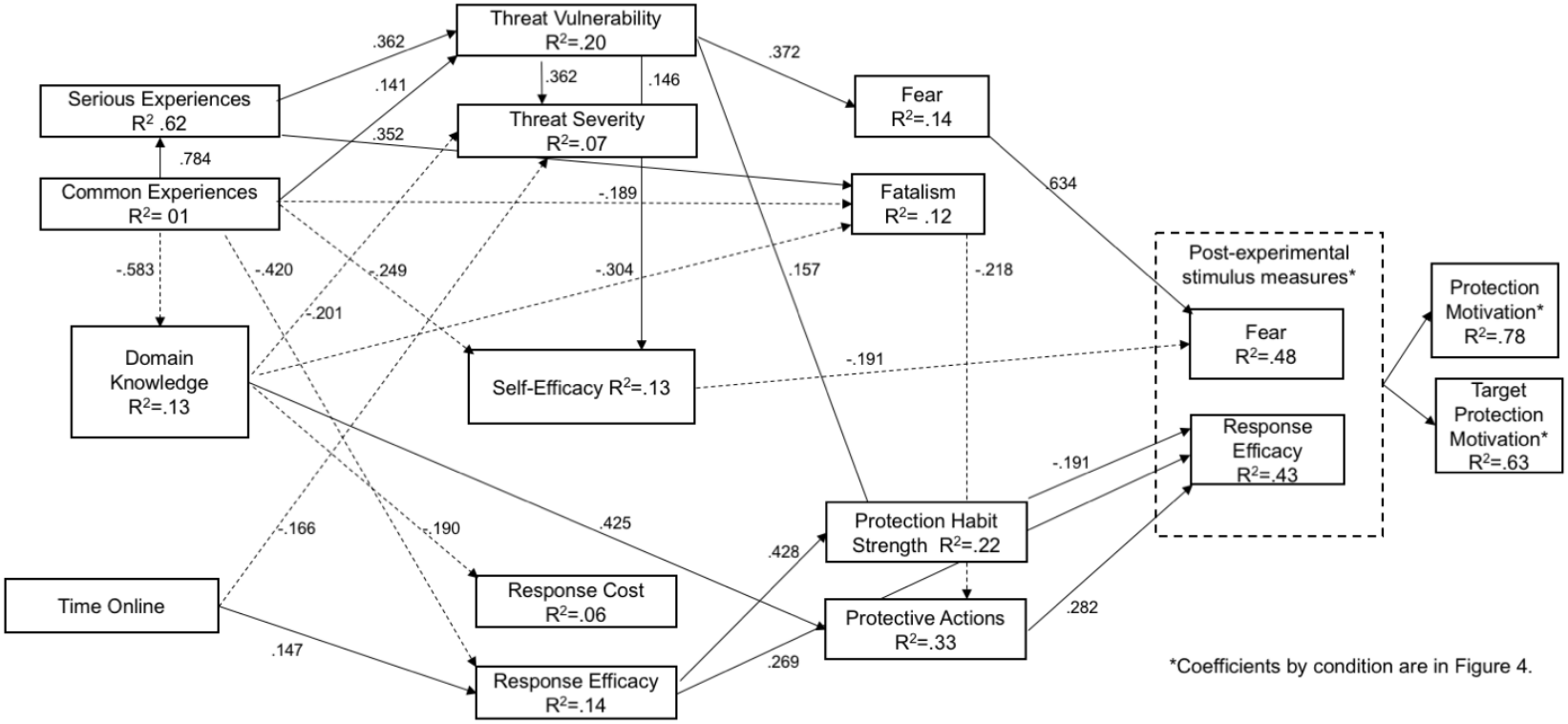
Construct	Item	Weight	Std. Error	T-Stat.	p-value	VIF
Target Protection Motivation	Q48_1	0.271	0.063	14.164	0.000	2.810
	Q48_2	0.406	0.047	20.060	0.000	3.807
	Q48_3	0.396	0.033	28.413	0.000	3.989
Common Threat Experiences	Q7_3	0.098	0.321	1.443	0.149	1.423
	Q7_5	-0.022	0.303	1.673	0.095	1.533
	Q7_9	0.518	0.321	2.702	0.007	2.436
Serious Threat Experiences	Q8_1	0.43	0.335	2.272	0.023	2.243
	Q8_2	-0.278	0.244	1.778	0.076	1.878
	Q8_3	0.356	0.330	2.632	0.009	4.114
	Q9_2	0.336	0.386	2.290	0.022	2.671
	Q9_3	0.304	0.408	2.067	0.039	2.011
	Q9_4	0.099	0.354	2.481	0.013	3.988
	Q9_6	0.396	0.343	2.652	0.008	3.359

The Fornell- Larker Table of constructs is in appendix 4.5.

4.3.2 Results of path analysis

The model was run using Smart PLS to determine the amount of variance explained in the endogenous constructs and also to check the significance of path coefficients in order to see which constructs were contributing to higher protection motivation and which constructs were inhibiting protection motivation. The number of participants was low for the degrees of freedom in the model so the PLS algorithm rather than the consistent PLS algorithm was used for the analysis. The strength of the consistent PLS algorithm is that it helps correct potential inflation in reflective measures (Ringle et al., 2015), but the PLS algorithm is sufficient at this point to test the research instrument. The PLS algorithm tested the complete data set and the control condition and the experimental (training) condition. Figure 4.2 illustrates the adjusted R-square values of the constructs for the complete model and coefficients for most of the paths. Paths that were obviously not significant were not included.

Figure 4.2: Adjusted R^2 values and path coefficients (complete)



The impacts of the message in the control (message only) and experimental (message and training) condition showed some interesting differences by condition.

Figure 4.3: Pre and post measures for the control condition

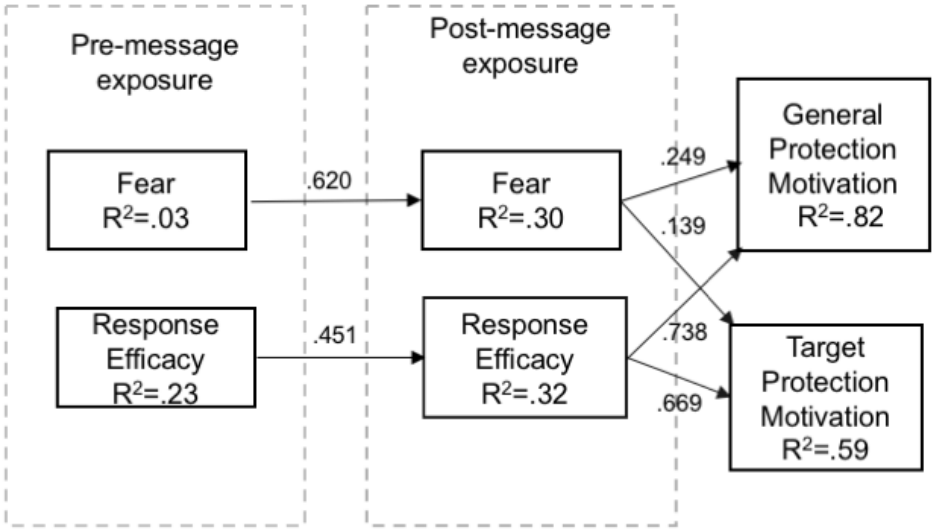
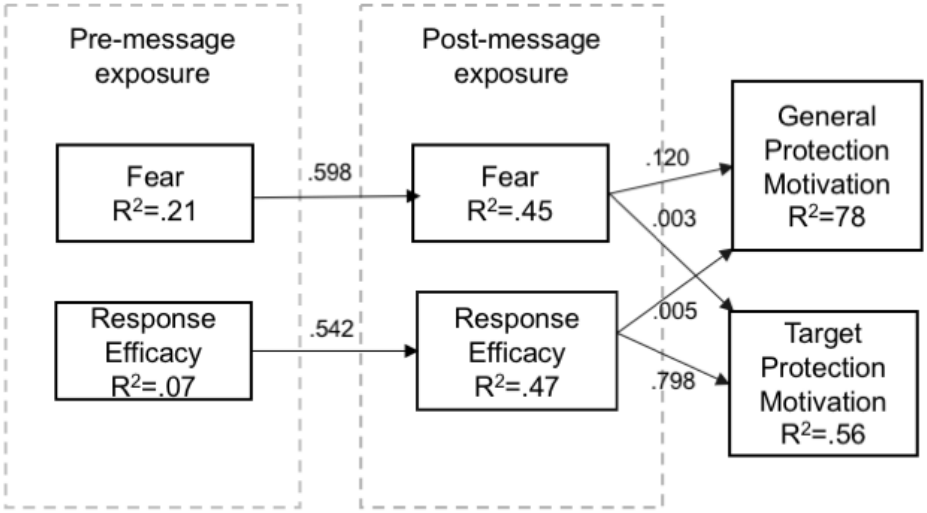


Figure 4.4: Pre and post measures for the experimental condition

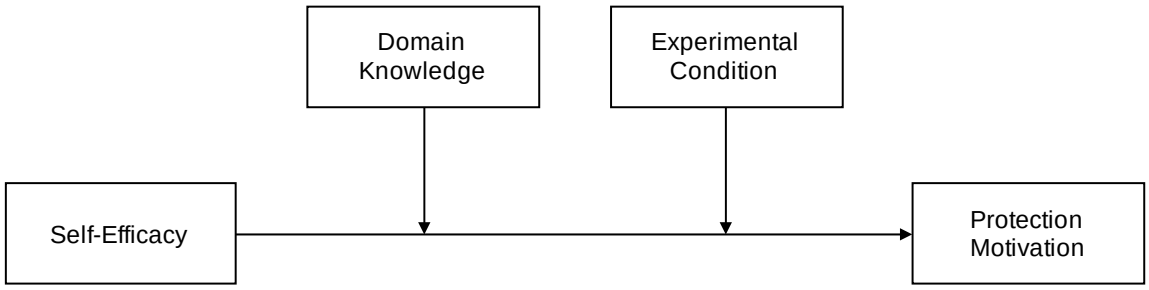


Even though I was not able to do the full multi-group analysis given the small sample size for the number of variables, there were indicators that the message had an impact. Those in the control condition, who got the message to update their browser software but didn't have instruction on how to do it showed strong intentions to perform the target behavior (fear → protection motivation b=.249 and response efficacy → protection motivation b=.738). Those in the experimental (training) condition showed lower protection motivation (fear →protection motivation b=.120 and response efficacy → protection motivation b=.005). However, those in the experimental condition were highly motivated for the target behavior (response efficacy→target protection motivation b=.798). This would indicate that the training tutorial should be revised to make sure that the pacing is slow enough to easily understand, and the message is clear.

4.3.3 Results of moderation analysis

Even though a partial least squares analysis allows a test on the impacts of a message, it is not able to analyze the potential moderation that different levels of a specific construct might have. To determine the potential moderation impacts of different levels of domain knowledge and self-efficacy, the data was analyzed using Hayes PROCESS v. 3. Model Two was used which has the two items as moderators as shown in Figure 4.5. The settings were for bootstrapping at 5,000 and the detailed results are in Appendix 3.

Figure 4.5: Moderation model



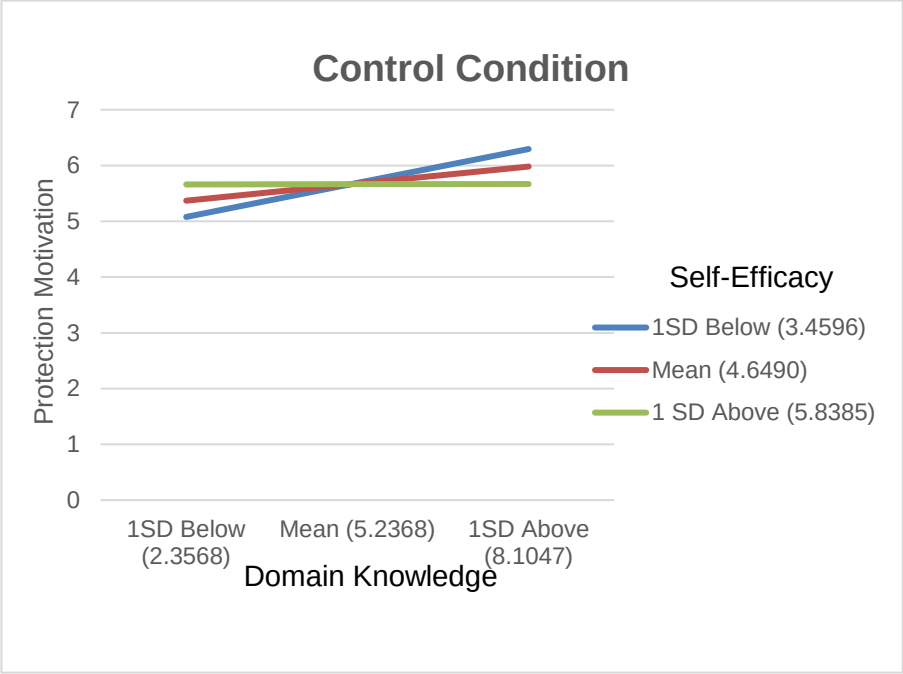
The results of the analysis revealed that the domain knowledge did interact with the experimental condition $F(5, 46) = 5.37$, $p<.001$, $R^2=0.37$. Domain knowledge had a significant positive impact $B=.52$, $t=2.67$, and $p<.05$. The training condition had a negative impact, $B=-2.21$, $t=2.33$, and $p=<.05$. The interaction of self-efficacy and domain knowledge overall was positive and significant $F(1,46)=4.79$, $p<.05$, $R^2=0.07$. The interaction of self-efficacy and training was marginally stronger $F(1,46)= 4.99$, $p<.05$, $R^2= 0.07$.

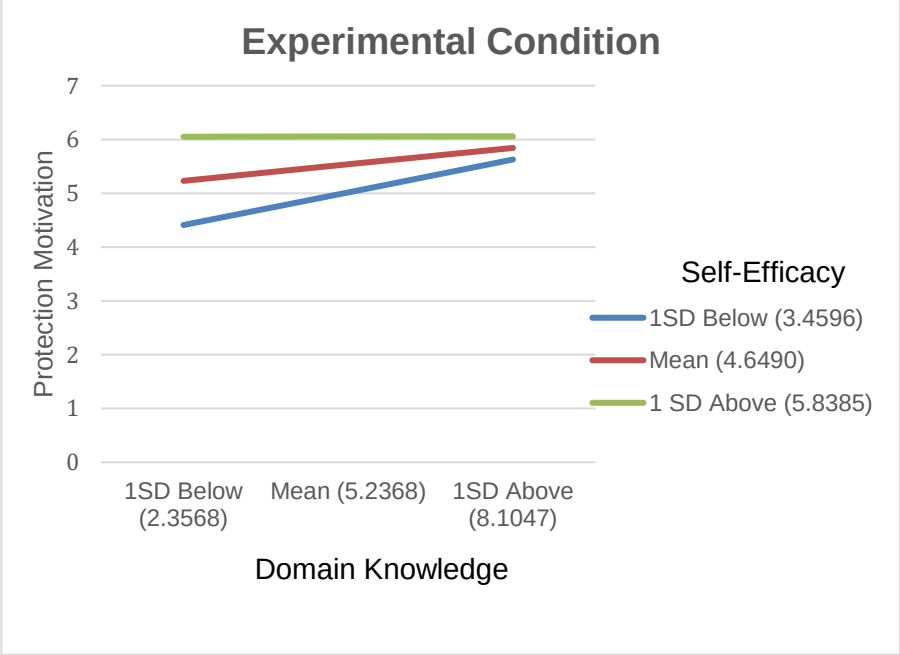
Figure 4.6, illustrates the interaction points as plotted by the Hayes PROCESS output. For those who had lower domain knowledge, and the lowest self-efficacy, even when presented with the training message were not highly motivated to protect themselves. Higher efficacy levels and at least the mean domain knowledge increased the likelihood for protection motivation. The experimental condition that showed how to perform the task was most impactful for those with at least mean or higher self-efficacy and domain knowledge.

These results indicate support for the theoretical model that domain knowledge impacts how individuals process a message. However, the negative impact of the experimental condition on all but those who had mean self-efficacy would indicate the

need to revise the message to make it more accessible. This is discussed further in the next section.

Figure 4.6: Moderation analysis of self-efficacy and domain knowledge in both conditions





4.4 Discussion

The analysis of the new items overall showed both internal and external validity. Yet there are revisions that should be made to improve the research instrument.

There was a definite impact from watching both the control message and the training message. There was also an impact depending on the individuals' level of domain knowledge. For those with extremely high self-efficacy, the training message increased their protection motivation no matter what their domain knowledge was. Those with lower self-efficacy and low domain knowledge were negatively impacted. This might indicate that the training condition gave too much information too quickly and the participants might have felt overwhelmed, leaving them with lower protection motivation. Despite being tested for usability; this issue was not seen in early testing. It may be that those who were willing to help for usability testing had either higher levels of domain knowledge or they were more interested in cybersecurity as reflected by their willingness to help test the tutorial video. Also, since the population sample for this pilot test is fairly small for each condition, there is a strong possibility of sample bias. Yet despite the small sample size, these findings do bring insights into the next round of research, the need to refine the message so that the training condition is more accessible, especially to a more diverse audience.

To increase the impact of the training condition, the script will be revised. Phrasing of the problem will be changed to make it more inclusive and avoid the "us" versus "them" attitudes. The demonstration of how to check one's browser condition will be demonstrated a second time to increase confidence of participants with lower domain efficacy. Chapter 5 will have the original script and the revised script.

The previous experiences items will be kept even though many were not widely experienced by this pool of participants. The next round of experiments will include a more diverse population than college students and their experiences with online threats will probably be more varied. The larger sample may include those who have more experiences with threat and thus it may have more impact on the threat and coping appraisal process. A few items will be slightly reworded to improve clarity in the threat vulnerability variable to make sure participants understand that these are hypothetical threats, the word “if” will precede each phrase rather than simply at the introductory phrase for the set of questions. All items will be reviewed again for clarity. Fatalism, even though it was only correlated to response cost, was kept because of the limitations of the homogenous age group of the current sample. Since they are younger the attitude of fatalism or fear might not have as much impact as it would on a more diverse age group. In the next chapter I will detail the revisions made to the instrument, the final data collection process and the results of the analysis.

APPENDICES

Appendix 4.1: Questions from survey instrument

Construct/ Source	Variable
Time Online	
	Q4 On a typical day how much time do you spend on a desktop or laptop computer?
	Q5 On a typical day how much time do you spend on the Internet on all computing devices?
Previous Threat Experience	
	Q6_1 An unexpected pop up message or pop up ad
	Q6_2 Emails trying to get me to enter personal information or passwords (phishing)
	Q6_3 A message popped up offering a free computer security scan
	Q6_4 Browser warning that a site is compromised or not safe
	Q6_5 The computer slows down or is not running as fast as it used to
	Q7_1 Fan is running and computer seems to be working hard even when I am not running many programs
	Q7_2 The computer slows down or is not running as fast as it used to
	Q7_3 New icons or programs appear out of nowhere
	Q7_4 Computer freezes up
	Q7_5 My security software won't update or run like it is supposed to
	Q7_6 My files or my computer was encrypted and held hostage (ransomware)
	Q8_1 My computer has sent out messages I didn'
	Q8_2 My email or social media (e.g., Facebook)
	Q8_3 I was locked out of my computer
	Q 9_1 Had your social security number or credit card number stolen
	Q9_2 Been the victim of an online scam and lost money
	Q9_3 Had to have the computer hard drive wiped and reinstall your programs

	Q9_4 Had to buy a new computer because of virus or malware problems Q9_5 Had someone take control of your camera and record you Q9_6 Been threatened with information gained from someone monitoring your computer activities
Threat Severity	
	How serious would any of the following be IF they happened to you- Q10_1 My email account was hacked, and I had to reset passwords Q10_2 Malware was on my computer and could use my computer for criminal purposes Q10_3 Spyware was on my computer and watching what I typed Q10_4 My computer files got locked up and I couldn't access them Q10_5 Someone could access my personal photographs Q10_6 I had to have my computer hard drive wiped and re-install my programs
Threat Vulnerability	
	Given your current protections how likely do you think the following might happen to you Q11_1 An unexpected pop-up message or pop-up ad appearing Q11_2 Getting emails that try to get me to enter personal information or passwords (phishing) Q11_3 The computer will slow down in the future and not run as fast as it used to Q11_4 New icons or programs will appear out of nowhere Q11_5 My email or social media (e.g., Facebook) account will be compromised Q11_6 My files or my computer might get encrypted and held hostage (ransomware)

	Q11_7 I might eventually have to have the computer hard drive wiped and reinstall my programs
	Q11_8 Be threatened with information gained from someone monitoring my computer activities
Self-Efficacy	
	Q13_1 I feel comfortable taking measures to secure my primary home computer
	Q13_2 Taking the necessary security measures is entirely under my control
	Q13_3 I have the resources and the knowledge to take necessary security measures
	Q13_4 Taking necessary security measures is easy
Response Cost	
	Q14_1 It is often inconvenient to take security measures
	Q14_3 Following some security measures (e.g., updating software) may cause some of my programs not to work correctly
	Q14_4 I have trouble remembering my passwords or keeping them straight
	Q15_2 I often feel time pressure when I am trying to log in to my accounts
	Q15_4 Taking security measures can slow down what I need to do
Response Efficacy	
	Q16_1 Protective software would be useful for detecting and removing malware or viruses
	Q16_2 Having hard to guess passwords that are different for my different accounts will help improve my security protections
	Q16_3 Keeping my operating systems updated will help improve my security protections
	Q16_4Keeping my Internet browser updated will help improve my security protections
	Q16_5 Keeping my software programs updated will help improve my security protections

	Q16_6 Avoiding dangerous web sites will keep me safe online
	Q16_7 Most main web sites (like news sites) are very safe
Fatalism	
	Q17_1 It doesn't matter what I do, it is random chance that people get hacked
	Q17_2 I don't worry about online safety because I don't have that much to protect
	Q17_3 Most protective actions are a waste of time, if someone wants to hack you, you are going to get hacked
	Q17_4 Hackers are very smart and they can get through most protections
Protection Habit Strength	
	Q19_1 The use of security protections has become a habit for me
	Q19_2 Using security protections has become natural to me
	Q19_3 Online security is something I do automatically
	Q19_4 Online protection is something I do without thinking
	Q19_5 Online safety protection is part of my regular routine
Protection Actions	
	Q22 Virus Protection/ Malware Software (like Norton, McAfee, Avast, or similar)
	Q23 Operating System Updates
	Q24_1 Set your browser to disable or turn off cookies
	Q24_2 Cleared cookies and browser history
	Q24_3 Use private browser windows
	Q24_4 Checked to see if your browser is up to date
	Q24_5 Encrypted your communications
	Q24_6 Changed the security settings on your Internet browser
	Q24_7 Changed to a stronger password
	Q24_8 Have different passwords for different accounts
	Q24_9 Use a spam filter to block unwanted email
	Q24_10 Check web site URL for "https"

	Q24_11 Check email address of sender before replying to a business email Q24_12 Not gone to a web site because of a security warning from the browser Q24_13 Checked to see if your browser is up to date
Fear	
	Q20_1 The trends in online security are worrisome to me Q20_2 I fear that computer security issues are beyond the control of individuals Q20_3 I am concerned about the rapid changes in computer security issues Q20_4 Current online security issues make me feel afraid Q20_5 When I think of computer security issues, I get very anxious about what might happen
Domain Knowledge	
	Q25 What does the “https://” at the beginning of a URL denote, as opposed to http:// (without the “s”)? Q26 Which of the following is an example of a “phishing” attack? Q27 A group of computers that is networked together and used by hackers to steal information is called a…. Q28 Some websites and online services use a security process called two-step authentication. Which of the following images is an example of two-step authentication? Q29 Which of the following four passwords is the most secure? Q30 Criminals access someone’s computer and encrypt the user’s personal files and data. The user is unable to access this data unless they pay the criminals to decrypt the files. This practice is called…. Q31 “Private Browsing” is a feature in many internet browsers that lets users access web pages without any information (like browsing history) being stored by the browser. Can internet service providers see the online activities of their subscribers when those subscribers are using private browsing?

	Q32Turning off the GPS function of your smartphone prevents any tracking of your phone's location. Q33 All email is encrypted by default Q34 By law, how many free credit reports can Americans obtain in a calendar year from each of the three major credit bureaus?
	Q35 If a public Wi-Fi network (such as in an airport or cafe') requires a password to access is it generally safe to use that network for sensitive activities such as online banking? Q36 What kind of cybersecurity risks can be minimized by using a Virtual Private Network (VPN)? Q37 Older Internet browsers have security weaknesses and might compromise my security as I look at web pages. Q38 Internet browsers automatically update themselves so users never need to check them
Learning Items Post	
	Q45 Older Internet browsers have security weaknesses and might compromise my security as I look at web pages Q46 Internet browsers automatically update themselves so users never need to check them.
Protection Motivation	
	Q47_1 I will upgrade my security measures to protect myself better online Q47_2 I will check to see if my browser is up to date Q47_3 I will change my passwords more often Q47_4 I will learn how to be more secure online Q47_5 I will only download software from firms that I trust Q47_6 I will update my protective software regularly
Specific Protection Motivation	
	Q48_1 I feel more confident that I can take actions to protect myself Q48_2 I will check my browser to see if it is up to date Q48_3 I will continue to check my browser occasionally to make sure it is updating correctly
Post Fear	

	Q48_4 The trends in online security are worrisome to me
	Q48_5 I fear that computer security issues are beyond the control of individuals
	Q48_6 I am worried about the rapid changes in computer security issues
	Q48_7 Current online security issues make me feel afraid
	Q48_8 When I think of computer security issues, I get very scared about what might happen
Post Response Efficacy	
	Q49_1 Protective software would be useful for detecting and removing malware or viruses
	Q49_2 Having hard to guess passwords that are different for my different accounts will help improve my security protections
	Q49_3 Keeping my operating systems updated will help improve my security protections
	Q49_4 Keeping my Internet browser updated will help improve my security protections
	Q49_5 Keeping my software programs updated will help improve my security protections

Appendix 4.2: Hayes moderation analysis output

Run MATRIX procedure:

**** PROCESS Procedure for SPSS Version 3.00 ****

Written by Andrew F. Hayes, Ph.D. www.afhayes.com
Documentation available in Hayes (2018). www.guilford.com/p/hayes3

****

Model : 2
Y : Protection Motivation
X : Self-Efficacy
W : Domain Knowledge
Z : Training

Sample
Size: 52

****

OUTCOME VARIABLE:
Protection Motivation

Model Summary

R	R-sq	MSE	F	df1	df2	p
.6069	.3684	.6726	5.3652	5.0000	46.0000	.0006

Model

	coeff	se	t	p	LLCI	ULCI
constant	5.2187	1.8736	2.7854	.0077	1.4473	8.9901
SelfEffi	.0083	.3851	.0216	.9829	-.7668	.7834
DomainK_	.5179	.1942	2.6667	.0105	.1270	.9088
Int_1	-.0885	.0404	-2.1893	.0337	-.1698	-.0071
Training	-2.2075	.9492	-2.3255	.0245	-4.1182	-.2967
Int_2	.4450	.1991	2.2353	.0303	.0443	.8457

Product terms key:
Int_1 : Self-Efficacy x Domain Knowledge
Int_2 : Self-Efficacy x Training

Test(s) of highest order unconditional interaction(s):

	R2-chng	F	df1	df2	p
X*W	.0658	4.7932	1.0000	46.0000	.0337
X*Z	.0686	4.9965	1.0000	46.0000	.0303

Focal predict: SelfEffi (X)
Mod var: DomainK_ (W)
Mod var: Training (Z)

Conditional effects of the focal predictor at values of the moderator(s):

DomainK_	Training	Effect	se	t	p	LLCI	ULCI
2.3568	1.0000	.2447	.1781	1.3740	.1761	-.1138	.6033
2.3568	2.0000	.6897	.1613	4.2764	.0001	.3651	1.0143
5.2308	1.0000	-.0095	.1459	-.0653	.9482	-.3032	.2842
5.2308	2.0000	.4354	.1381	3.1519	.0029	.1574	.7135
8.1047	1.0000	-.2638	.1945	-1.3563	.1816	-.6553	.1277
8.1047	2.0000	.1812	.1978	.9158	.3645	-.2170	.5794

Data for visualizing the conditional effect of the focal predictor:
Paste text below into a SPSS syntax window and execute to produce plot.

```
DATA LIST FREE/
  SelfEffi  DomainK_  Training  Protection Motivation  .
BEGIN DATA.
   3.4596   2.3568   1.0000   5.0785
   4.6490   2.3568   1.0000   5.3696
   5.8385   2.3568   1.0000   5.6607
   3.4596   2.3568   2.0000   4.4104
   4.6490   2.3568   2.0000   5.2308
   5.8385   2.3568   2.0000   6.0511
   3.4596   5.2308   1.0000   5.6871
   4.6490   5.2308   1.0000   5.6758
   5.8385   5.2308   1.0000   5.6645
   3.4596   5.2308   2.0000   5.0190
   4.6490   5.2308   2.0000   5.5370
   5.8385   5.2308   2.0000   6.0549
   3.4596   8.1047   1.0000   6.2958
   4.6490   8.1047   1.0000   5.9820
   5.8385   8.1047   1.0000   5.6683
   3.4596   8.1047   2.0000   5.6277
   4.6490   8.1047   2.0000   5.8432
   5.8385   8.1047   2.0000   6.0587
END DATA.
GRAPH/SCATTERPLOT=
 SelfEffi WITH     Protecti BY       DomainK_ /PANEL   ROWVAR=  Training .
```

********** ANALYSIS NOTES AND ERRORS **********

Level of confidence for all confidence intervals in output:
  95.0000

W values in conditional tables are the mean and +/- SD from the mean.

NOTE: Variables names longer than eight characters can produce incorrect output.
      Shorter variable names are recommended.

------ END MATRIX -----

Appendix 4.3: Fornell-Larker results

Table 4.4: Fornell-Larker table

	Comm. Exp.	Dom. Kn.	Fatalism	Fear	Fear POST	Prot. Actions	Prot. Habits	Prot. Motivation	Resp. Cost	Resp. Eff.	Resp. Eff. POST	Self Efficacy	Ser. Exp.	Target Prot. Mot.	Threat Severity	Threat Vul.	Time
Common Experience with Threat																	
Domain Knowledge	0.063	1															
Fatalism	0.352	-0.056	0.568														
Fear	-0.45	0.162	-0.147	0.685													
Fear POST	-0.186	0.127	-0.018	0.563	0.767												
Protection Actions	-0.357	0.437	-0.492	0.466	0.139												
Protection Habits	-0.141	-0.047	-0.008	0.011	0.186	-0.318	0.933										
Protection Motivation	-0.637	0.102	-0.391	0.619	0.449	0.459	0.274										
Response Cost	0.06	-0.085	0.357	-0.185	-0.12	-0.445	0.193	-0.153	0.646								
Response Efficacy	-0.525	0.177	-0.129	0.668	0.535	0.327	0.384	0.693	-0.165	0.892							
Response Efficacy POST	-0.685	0.166	-0.303	0.563	0.257	0.504	-0.036	0.825	-0.196	0.518	0.927						
Self Efficacy	-0.536	0.079	-0.321	0.263	-0.084	0.525	0.031	0.504	-0.419	0.318	0.608	0.878					
Serious Experience with Threat	0.79	-0.012	0.438	-0.342	-0.287	-0.22	-0.286	-0.639	0.143	-0.436	-0.526	-0.335					
Target Protection Motivation	-0.588	0.142	-0.314	0.427	0.275	0.348	0.243	0.844	-0.327	0.54	0.784	0.565	-0.654				
Threat Severity	-0.427	-0.209	-0.109	0.145	0.089	0.011	0.172	0.283	-0.14	0.18	0.329	0.394	-0.27	0.247	0.935		
Threat Vulnerability	-0.13	-0.285	-0.012	0.204	0.106	-0.188	0.505	0.196	-0.229	0.214	0.092	0.383	-0.121	0.21	0.413	0.759	
Time Online	0.165	0.101	0.147	-0.108	0.198	-0.185	-0.302	-0.123	-0.067	-0.148	-0.139	-0.182	0.018	-0.114	0.013	-0.219	1

Appendix 4.4: Script for message

SCRIPT OF VIDEO FOR ALL CONDITIONS

Your browser it the tool that you use to access the Internet. You use it to get your email, surf websites such as Facebook, Twitter, Instagram, YouTube, news sites, banking, shopping, or anything else you do on the Internet with your computer.

You probably have a favorite browser. You can personalize it, add bookmarks, and you feel comfortable with it. You are probably very familiar with how web sites look when you use your favorite browser. Some people get so complacent that they don't want it to change at all. They may even turn off updates because they fear change. They might not realize that updates are extremely important. Their comfortable familiarity is full of security risks. Having an out-of-date browser can endanger **your privacy and security.** Browser updates not only help improve speed and functionality, they also help protect **you** from many **serious** threats.

Updates are very important. They are usually issued because a weakness is discovered in the code that runs the browser. This weakness usually will impact your safety and security when using that browser. Criminals and hackers know about these weaknesses and are often trying to make malware or viruses as soon as these weaknesses are found.

You may think that you don't go to websites that are sketchy or dangerous. Actually, very familiar web sites often harbor malware. Some types of malware can be downloaded on your computer simply by visiting a web page, even if you don't click on anything. Sometimes the advertisements running on websites, even sites by familiar news organizations, are hijacked and download code onto your computer as you are innocently reading a news article.

Out of date browsers might also not be correctly verifying secure sites, you may think a site is secure for shopping when it isn't.

An up-to-date browser is one of the key tools to protect you from these kinds of attacks. Many of the newer browsers often notify you if you are going to a web site that has indicators it is a site harboring known threats.

Most browsers automatically update themselves when new versions are available. However, quite often browsers don't update themselves for many reasons. Security researchers have found that about 25 to 30 percent of people's browsers are not up-to-date and most of these individuals are totally unaware that they are at risk.

You can check your browser and make sure it is up to date and protecting you from many known threats. Not only will an up-to-date browser protect you better, it will improve performance and speed in your browsing experience.

END SCRIPT FOR CONTROL PARTICIPANTS

FOR FIREFOX USERS- HIGH EFFICACY CONDITION

Making sure Firefox is running the latest version is very easy, once you see how to do it, you can check it whenever you want. Just open up Firefox, click on "Firefox" at the very top and a drop down menu will appear.

Select "About Firefox" and a little dialog screen pops up while Firefox checks if you have the latest version. Sometimes you will need to close Firefox and restart it to have the updates take effect. That is all there is to it! It will keep all of your bookmarks and settings and your browser will be fixed of known weaknesses.

FOR CHROME USERS- HIGH EFFICACY CONDITION

Making sure Google Chrome is running the latest version is very easy, once you see how to do it, you can check it whenever you want. Just open up Chrome, click on “Chrome” at the very top and a drop down menu will appear.

Select “About Chrome” and a little dialog screen pops up while Chrome checks if you have the latest version. Sometimes you will need to close Chrome and restart it to have the updates take effect. That is all there is to it! It will keep all of your bookmarks and settings and your browser will be fixed of known weaknesses.

FOR MICROSOFT INTERNET EXPLORER HIGH EFFICACY CONDITION

If you have any version of Internet Explorer before version 11, please do not use it anymore. You can export any you have to bookmarks to version 11. Microsoft is no longer offering updates to older versions of Internet Explorer and these are very unsafe to use. Since these older browsers were widely used at one time, there are criminal forces exploiting weaknesses in these browsers. Either use Internet Explorer 11, Microsoft Edge, or another company’s browser, but don’t use these compromised versions. To check if you Windows Explorer 11 is up to date, click on the about tab on top of the window. A window will open and it will search to see if you are running the latest version. It will updated itself and tell you if you need to restart your browser for the changes to take effect. That is all there is to it! It will keep all of your bookmarks and settings and your browser will be fixed of known weaknesses

Appendix 4.5: IRB approval for pilot study

MICHIGAN STATE UNIVERSITY

Initial IRB Application Determination *Exempt*

October 17, 2017

To: Wietske Van Osch
404 Wilson Road
427 Comm Arts Building

Re: IRB# x17-1374e Category: Exempt 2
Approval Date: October 11, 2017

Title: Mind the Gap: Perceived self-efficacy, domain knowledge and their effects on responses to a cybersecurity compliance message

The Institutional Review Board has completed their review of your project. I am pleased to advise you that your project has been deemed as exempt in accordance with federal regulations.

The IRB has found that your research project meets the criteria for exempt status and the criteria for the protection of human subjects in exempt research. Under our exempt policy the Principal Investigator assumes the responsibilities for the protection of human subjects in this project as outlined in the assurance letter and exempt educational material. The IRB office has received your signed assurance for exempt research. A copy of this signed agreement is appended for your information and records.

Renewals: Exempt protocols do not need to be renewed. If the project is completed, please submit an *Application for Permanent Closure*.

Revisions: Exempt protocols do not require revisions. However, if changes are made to a protocol that may no longer meet the exempt criteria, a new initial application will be required. If the project is modified to add additional sites for the research, please note that you may not begin your research at those sites until you receive the appropriate approvals/permissions from the sites.

Problems: If issues should arise during the conduct of the research, such as unanticipated problems, adverse events, or any problem that may increase the risk to the human subjects and change the category of review, notify the IRB office promptly. Any complaints from participants regarding the risk and benefits of the project must be reported to the IRB.

Follow-up: If your exempt project is not completed and closed after three years, the IRB office will contact you regarding the status of the project and to verify that no changes have occurred that may affect exempt status.

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

If we can be of further assistance, please contact us at 517-355-2180 or via email at IRB@msu.edu. Thank you for your cooperation.

c: Ruth Shillair

Office of Regulatory Affairs
Human Research Protection Programs

Biomedical & Health Institutional Review Board (BIRB)

Community Research Institutional Review Board (CRIRB)

Social Science Behavioral/Education Institutional Review Board (SIRB)

4000 Collins Road
Suite 136
Lansing, MI, 48910
(517) 355-2180
Fax: (517) 432-4503
Email: irb@msu.edu
www.hrpp.msu.edu

WORKS CITED

WORKS CITED

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

Bandura, A. (1971). Social Learning Theory. Social Learning Theory. http://doi.org/10.1111/j.1460-2466.1978.tb01621.x

Bandura, A. (1977). Self-efficacy: Toward a Unifying Theory of Behavioral Change. Pyschological Review, 84(2), 191–215. http://doi.org/http://dx.doi.org/10.1037/0033-295X.84.2.191

Diamantopoulos, A., Riefler, P., & Roth, K. P. (2008). Advancing Formative Measurement Models. Journal of Business Research, 61(12), 1203–1218. http://doi.org/10.1016/j.jbusres.2008.01.009

Dutton, W. H., & Shepherd, A. (2006). Trust in the Internet as an Experience Technology. Information, Communication & Society, 9(4), 433–451. http://doi.org/10.1080/13691180600858606

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. American Marketing Association, 18(1), 39–50.

Gioia, D. A., & Manz, C. C. (1985). A Script of Cognition Processing Vicarious Behavior: Interpretation Learning. Academy of Management, 10(3), 527–539.

Hanus, B., & Wu, Y. “Andy.” (2015). Impact of Users’ Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. Information Systems Management, 10580530.2015.1117842. http://doi.org/10.1080/10580530.2015.1117842

Hasan, B. (2003). The Influence of Specific Computer Experiences on Computer Self-efficacy Beliefs. Computers in Human Behavior, 19(4), 443–450. http://doi.org/10.1016/S0747-5632(02)00079-1

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our Network Safe: A Model of Online

Protection Behaviour. Behaviour & Information Technology, 27(5), 445–454. http://doi.org/10.1080/01449290600879344

Liang, H., & Xue, Y. (2009). Avoidance of Information Technology Threats: A Theoretical Perspective. MIS Quarterly, 33(1), 71–90. http://doi.org/Article

Liang, H., & Xue, Y. (2010). Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective. Journal of the Association for Information Systems, 11(7), 394–413.

Maddux, J. E., & Rogers, R. W. (1983). Protection Motivation and Self-efficacy: A Revised Theory of Fear Appeals and Attitude Change. Journal of Experimental Social Psychology, 19(5), 469–479. http://doi.org/10.1016/0022-1031(83)90023-9

Meulman, J. J., Anita., V. D. J., & Heiser, W. J. (2004). Principal Components Analysis with Nonlinear Optimal Scaling Transformations for Ordinal and Nominal Data. In D. Kaplan (Ed.), The Sage Handbook of Quantitative Methodology for the Social Sciences (pp. 49–70). Thousand Oaks CA: Sage.

Microsoft. (2016). Microsoft Security Intelligence Report, 21, 7–8. Retrieved from https://www.microsoft.com/security/sir/story/default.aspx#!10year_timeline

O'Brien, R. M. (2007). A Caution Regarding Rules of Thumb for Variance Inflation Factors. Quality & Quantity, 41(5), 673–690. http://doi.org/10.1007/s11135-006-9018-6

Olmstead, K., & Smith, A. (2017). What the Public Knows about Cybersecurity. Washington, D.C. Retrieved from http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/

Rhodes, N., Roskos-Ewoldsen, D. R., Edison, A., & Bradford, M. B. (2008). Attitude and Norm Accessibility Affect Processing of Anti-smoking Messages. Health Psychology, 27(3S), S224–S232. http://doi.org/10.1037/0278-6133.27.3(Suppl.).S224

Ringle, C. M., Wende, S., & Becker, J.-M. (2015). SmartPLS 3.0. Retrieved from http://www.smartpls.com

Rippetoe, P. a., & 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), 596–604. http://doi.org/10.1037//0022-3514.52.3.596

Roskos-Ewoldsen, D. R., Yu, H. J., & Rhodes, N. (2004). Fear Appeal Messages Affect Accessibility of Attitudes Toward the Threat and Adaptive Behaviors. Communication Monographs, 71(1), 49–69. http://doi.org/10.1080/0363452042000228559

Shillair, R. (2015). Experiencing Online Safety: Previous Experiences and Their Impact on Attitudes and Digital Hygiene. Michigan State University CAS Research Presentations. East Lansing, MI.

Shillair, R. (2016). Talking About Online Safety: A Qualitative Study Exploring the Cybersecurity Learning Process of Online Labor Market Workers. In SIGDOC 2016 - 34th ACM International Conference on the Design of Communication. http://doi.org/10.1145/2987592.2987605

Shillair, R., LaRose, R., Jiang, M., Rifon, N. J., & Cotten, S. R. (2017). The Role of Habits and Prior Experience in Motivating User Cybersecurity Behavior. In International Communication Association (p. 30). San Diego, California.

Shillair, R., LaRose, R., & VanOsch, W. (2015). Experiencing Online Safety: Previous Experiences and Their Impact on Attitudes and Digital Hygiene. In Michigan State University CAS Research Presentations. East Lansing, MI.

Vaniea, K., Rader, E., & Wash, R. (2014). Betrayed By Updates : How Negative Experiences Affect Future Security. In CHI 2014, One of a CHInd (pp. 2671–2674).

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer Acceptance and Use of Information Technology: Extending the Unified Theory of Acceptance and Use of Technology. MIS Quarterly, 36(1), 157–178.

Wash, R., Rader, E., & Fennell, C. (2017). Can People Self-Report Security Accurately ? Agreement Between Self-Report and Behavioral Measures. In CHI 2017 (pp. 2228–2232). Denver.

Witte, K. (1994). Fear Control and Danger Control: A Test of the Extended Parallel Process Model (EPPM). Communication Monographs. http://doi.org/10.1080/03637759409376328

Witte, K., & Allen, M. (2000). A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns. Health Education & Behavior, 27(5), 591–615. http://doi.org/10.1177/109019810002700506

Chapter 5
Main experimental study

5.1 Introduction

Only through experimental testing of a theoretically based model can we demonstrate if there is a gap between users' self-efficacy and their actual domain knowledge and if that game makes a difference in their attitudes and actions in being cyber secure. This will give insights into why individuals respond in certain ways to cybersecurity compliance messages and give insights into more effective solutions.

The pilot study tested the model and a message. As previously discussed, the results indicated the need for further study using a larger, more diverse sample. The path analysis rejected the null hypothesis and demonstrated the impact of self-efficacy in cyber protections, previous experiences, domain knowledge, and the type of message they received. Individuals' intentions to protect themselves were specifically impacted by: previous experiences; their appraisal of threats; their appraisal of the efficacy and usability (e.g., cost) of these solutions; their domain knowledge; and their self-efficacy in carrying out protections. The pilot study also demonstrated that there were interactions happening between the participant's domain knowledge and self-efficacy in their response to a cybersecurity compliance message. These interactions were not linear but resembled a normal distribution with those with higher levels of domain knowledge showing lower intention to comply.

These findings were limited by the size of the sample and the overall low levels of domain knowledge. One might presume that college students from a competitive university would have a fairly robust understanding about online threats since they interact with the latest technologies on their campus; however, our sample's domain knowledge was low with a mean of 5 correct answers out of 12 items. A population sample

that includes individuals who have been in the workforce for some time, or those who have had to manage their own computer maintenance for years might have a broader range of domain knowledge and respond quite differently to a compliance message.

In other domains, such as health communications, a fairly linear relationship tends to exist between increased health literacy and protective actions (Miller, 2016). As aforementioned, the pilot study indicated that the impact of increased domain knowledge did not necessarily lead to better compliance intentions. The pilot study suggests that cybersecurity might display a more complex interaction between domain knowledge and compliance than other domains. This might be because of the constantly changing nature of online threats (Shillair & Dutton, 2016), or it might be because of demographic conditions that make learning about new technologies difficult (Tsai, Shillair, Cotten, Winstead, & Yost, 2015). It also might be because prior experiences with cybersecurity failures discourage individuals from putting effort into protecting themselves by inducing a fatalistic mindset (Shillair, LaRose, Jiang, Rifon, & Cotten, 2017). For those who go online frequently for work, their workplace may provide training, increasing their domain knowledge and awareness of threats (Li et al., 2014). A larger sample that includes a wider demographic should provide deeper insights into the impacts of domain knowledge in the threat appraisal and coping appraisal process. However, before moving forward to testing the research instrument on a new audience, I took the insights learned from the pilot study to improve the research instrument, thus increasing the internal and external validity.

5.1.1 Changes made to the research instrument

The new constructs used in the pilot study seemed to perform well in the sample and both internal and external validity were acceptable as discussed in the previous chapter. Based on previous literature, I expected stronger performance of some of the constructs. This was especially true of self-efficacy, which was a strong determinant of cybersecurity compliance in other studies (Hasan, 2003; Vance, Siponen, & Pahnila, 2012; Yi & Im, 2004), yet it was only a minor determinant to protection motivation (b= -0.024) in the pilot study. Since self-efficacy is seen as foundational both theoretically and empirically to taking any action for self-improvement (Ajzen., 2002; Yeo & Neal, 2006), finding only minimal evidence of its importance might indicate that the operational measures used did not accurately capture the construct of self-efficacy in the context of cybersecurity.

The pilot study operational measures for perceived self-efficacy in cybersecurity were: “I feel comfortable taking measures to secure my primary home computer; taking the necessary security measures is entirely under my control; I have the resources and the knowledge to take necessary security measures; and taking necessary security measures is easy.” These were taken from Anderson and Agarwal's (2010) work on cybersecurity compliance. After a review of several of the focus group discussions, and a review of Bandura's (2006) guide to constructing self-efficacy scales, these measures were revised. The phrase “entirely under my control” and “easy” were problematic. As is frequently discussed, selecting best cybersecurity measures is anything but easy, even for professionals (Furnell, 2005; Mannan & Van Oorschot, 2007; Reeder, Ion, & Consolvo, 2017). Also, for those who have had their personal information compromised

because of poor security practices of businesses that hold our information (e.g., a data breech of a password manager program), “entirely under my control” is also inaccurate. Furthermore, reviewing the focus groups, several claimed to know there was more they could do to enact higher security measures, but they chose not to put in the effort to do more. The implication was that they felt efficacious, thus they felt confident, but they did not feel the current threat level to them personally warranted the extra effort to enact further protections. Thus, the modified self-efficacy measures are: “I feel comfortable taking measures to secure my primary home computer”; “I am able to take measures to protect myself online”; “I have the resources and the knowledge to take necessary security measures; taking necessary security measures is very doable”; and, “if I want to, I can take measures to protect myself online”. These modifications keep the bulk of the operationalizations the same, yet they more accurately capture the construct of self-efficacy in the current threat environment.

The pilot study compliance video was carefully examined with the help of an expert on messaging strategies. The goal was to improve clarity of the content of the video and avoid any unintended messaging confounds. As a result, we revised the script and we determined that the recordings should be redone at a slower pace. The experimental condition, that included vicarious learning would also need to be redone so that the demonstration of checking browser version was repeated for improved learning and comprehension (Li, 2016). Additionally, updates were made in the video to capture the latest versions of each type of browser demonstration (i.e., Google Chrome, Mozilla Firefox, Microsoft Edge, and Apple Safari). To add validity to the findings I wanted to verify that participants watched the entire video message, thus, extra measures were also

adopted. One of the measures adopted was to notify participants that at the somewhere in the video was a number that they would write in to confirm that they watched the video. The participants would enter this number in a box at the end of the video. Also, post-exposure to the message, questions were added about a point discussed on all versions of the video as an attention check. These measures helped improve assurances that the participants were indeed watching the video.

During the revisions of the survey instrument, the institutional review board changed their standard consent form and review process, subsequently, the consent statements were also revised. The revised consent form, survey instrument, script for the video in all conditions, data protection plans, privacy protections, and a link to the sample video were all submitted to MSU's Institutional Review Board and approved as exempt (STUDY 00000328).

5.1.2 The modifications to the experimental instrument

After the study was approved, the video script was recorded by a voice actor at the slower pace, and the various versions were rebuilt including the repetition of the vicarious learning element. The survey flow was constructed so that half of the overall participants would be in the control condition and half would be in the training condition, regardless of their preferred browser type, since it was unknown a priori what browsers our participants would use. Once the entire experiment was loaded into Qualtrics, the survey flow and presentation was checked for accuracy. The full items for each construct and the script of the various versions of the cybersecurity compliance message are in Appendix 5.1.

Before the presentation of the video the participant would select which one of the following browsers that they used the most: Chrome, Firefox, Internet Explorer, or Safari.

All of the participants watched the same security compliance message. This message told participants of the benefit of having a browser that is up-to-date, the dangers of out-of-date browsers and how most of them update automatically but for various reasons many don't, thus they were told it is important to periodically check if their browser is up-to-date. The visuals were built using public domain clip art and browser screen shots. The overall tone of the message was similar to one approved by a major credit union for use with their members. It is factual, builds awareness of the threat, yet encourages belief in the efficacy of self-protective actions and ends with a positive note. This message was identical in all conditions of the study. For those in the experimental condition, the video additionally gave a demonstration of how to check one's browser for updates (which was presented contextually in the version that they had selected), so participants could learn vicariously. The demonstration was repeated to increase confidence and increase learning retention (Li, 2016; Tsai, Shillair, & Cotten, 2017). The demonstration ended with encouragement and a positive tone to help increase perceived self-efficacy. This contextual presentation meant that there was a total of five videos that were produced (e.g., one control condition and the four different experimental/ training conditions - one for each browser type). The videos were posted in a private YouTube channel and the entire study, including the new measures, was uploaded into Qualtrics.

As mentioned in the pilot study, it is helpful to see if the message impacts overall protection motivation or only the specific task that is mentioned in the videos. Thus, there are two direct variables: general protection motivation and target protection motivation. Target protection motivation deals specifically with the issues discussed in the message(s). General protection motivation is overall "best practices" type actions.

5.2 Methods

For this research I wanted computer users who would have at least some awareness of potential cybersecurity threats, and that might be motivated to protect themselves. Thus, individuals who used their computers frequently for work, yet in an environment where they were responsible for their own protection (e.g., self-employed or gig workers, rather than exclusively workers from companies that have internal IT support). I chose Amazon MTurk workers to get my population sample as they meet both of these requirements. The MTurk service allows individuals to sign up for small tasks online, these include helping train artificial intelligence (AI), flagging pictures for content, or taking surveys. Despite concerns of validity in using MTurk workers for research, numerous studies found them to be suitable for many types of research (Buhrmester, Kwang, & Gosling, 2011; Casler, Bickel, & Hackett, 2013; Chandler & Kapelner, 2013). Berinsky, Huber, & Lenz, (2012) found them to be more representative of the general population than convenience or snowball samples. A recent study by Redmiles, Kross, Pradhan, and Mazurek (2017) found MTurk workers had responses that were very comparative to panels solicited through web services and face-to-face recruitment. To improve quality of responses qualifications for participants included only US IP addresses and that the worker had completed over 100 tasks successfully.

A solicitation was posted in Amazon's MTurk web service for people to participate in "an online study about how individuals can improve their cyber security". They were told there was a short video about four minutes and a survey before and after the video. They were told the entire participation time was an average of 20 minutes (which was the time our pre-testing indicated) and they were offered $1.25 as an incentive. The

solicitation was posted in several waves to allow error checking between sets of data collection. First, a small set of 20 participants were solicited. Once, the data were checked for an accurate distribution and that the video viewing counts on YouTube were appropriate, then four waves of 200 participants were solicited. After each solicitation wave was completed and checked, all the participant identification numbers were put into a filter so that the Mturk workers who already participated would not see any additional posting. The entire data collection took a little over a week for a total of 820 participants. All participants were paid even if they did not pass the quality screening process.

Once the data was collected, to assure the quality of the data, the results were checked for: time of participation (e.g., too short to complete survey accurately), attention check questions, correctly entering the number in the video, and correctly answering the manipulation check question about software browser vulnerabilities. The process reduced the number of from 820 to 794 that passed all the quality controls.

Once the participants were checked for quality, the data itself went through several rounds of cleaning to verify that the data collection software correctly imputed data. The Qualtrics results needed several rounds of cleaning. The randomized matrix items were occasionally yielding incorrect items (e.g., instead of values of 1-7 corresponding to the Likert scales it was 15-21 or 18-24) these were corrected using the “recode into new item” command in SPSS.

Using the cleaned data (n=794), all the constructs were tested using multiple tools to test validity and to use the most appropriate tools to best understand how the data confirms or challenges the proposed model. This mixed method approach of analysis is to achieve deeper understanding of how domain knowledge, self-efficacy, and the PMT

process work together to impact individuals' intentions to protect themselves from cyber threats.

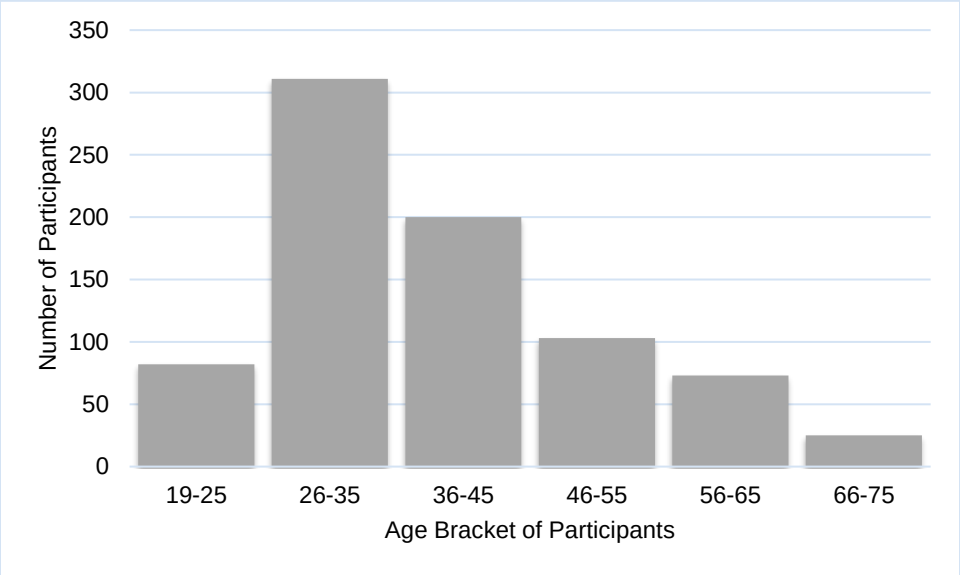
The first wave of analysis included descriptive analysis and confirmatory factor analysis using SPSS v.25. Since the next step was to test my theoretical model, structural equation modeling (SEM) is the most rigorous method to achieve this goal. SEM allows testing "specific theory-based causal connections between variables and between those latents and relevant indicator variables" (Hayduk, Cummings, Boadu, Pazderka-Robinson, & Boulianne, 2007, p. 843). I used SmartPLS as this does not require the assumption of normally distributed data, is appropriate for models that have a mix of formative and reflective constructs, and is resilient for complex models with a high number of latent variables (Dijkstra & Henseler, 2015). This is preferred by some researchers over covariance-based SEM, which is likely to produce non-convergent results (Dijkstra & Henseler, 2015).

5.3 Results

5.3.1 Demographics

For the 794 participants in the cleaned data, 420 (52.9%) were female, 367 (46.2%) were male, 2 (.3%) were other and 5 (.6%) preferred not to answer. The age range was from 19-75. Table 5.1 shows the age distribution of the participants. Most of the participants were in the 26-35 age bracket. There were quite a few participants over 55 years old with the oldest participant being 75.

Table 5.1: Age of participants



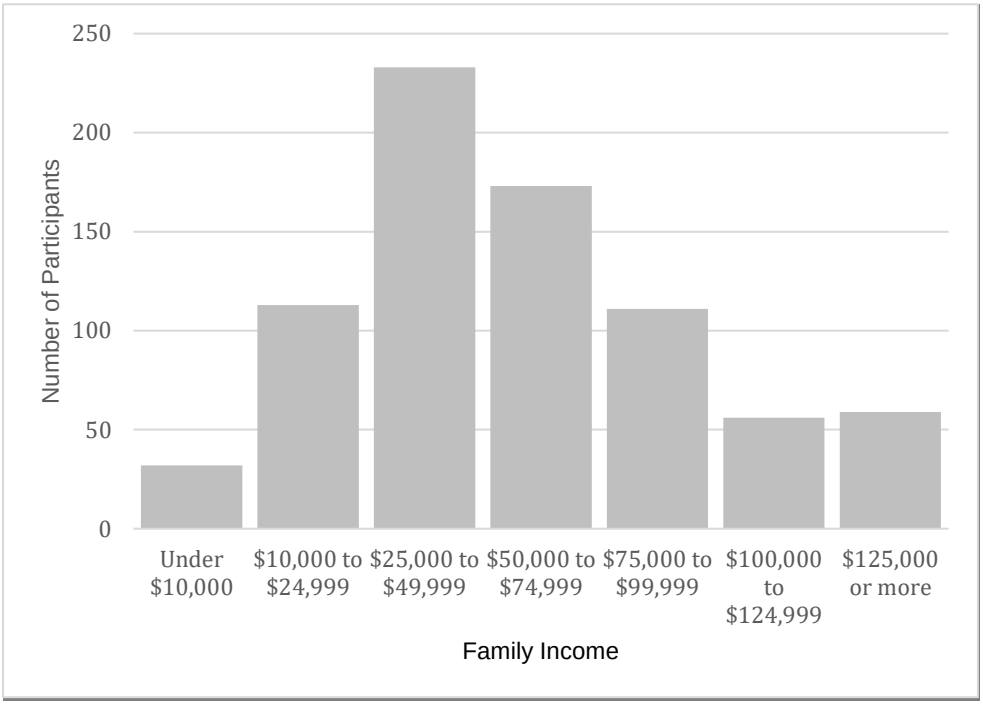
Participants shared their racial/ ethnic background with 11.0% (87) black/ African American, 80.6% (640) white, 7.7% (61) Asian, and 2.6% (21) Native American or Native Alaskan. 10.1% (80) also indicated that they were of Spanish/ Hispanic/ or Latino background.

Participants indicated the highest level of education completed. Educational backgrounds varied widely with .6% (5) completing middle school, 18.8% (148) finishing high school or a GED, 20.9% (166) finishing a Community College or Jr. College, 41.7% (331) completing a bachelor's, 11.5% (91) having a master's, 2.9% (23) having a Ph.D. or M.D., and 3.8% (30) having a specialized certification. Employment status is shown in Table 5.2, over half of the participants worked full time, an additional 16.1% worked part time.

Table 5.2: Employment status	Percent (n)
Employed full time	63.0 (500)
Employed part time	16.1 (128)
Homemaker not employed outside the home	5.5 (44)
Unemployed	5.16 (41)
Retired	2.9 (23)
Student and working at least part time	2.9 (23)
Disabled not working outside home	2.3 (18)
Student not working for wages	2.1 (17)

Reported family income ranged widely from under $10,000 (USD) annually to over $125,000. Only 2.1% (n=17) chose not to share their income. Table 5.3 shows the distribution of income for the participants.

Table 5.3: Family Income



5.3.2 Results of confirmatory factor analysis

The various constructs that work together in the PMT model (e.g., threat severity, response efficacy, threat vulnerability, etc.) are normally measured using reflective operationalizations. This works very well in areas like health communications where trying to access an individual's attitude towards a possible health threat would include several questions that probe different dimensions of their sense of threat severity or threat vulnerability. However, given that cybersecurity threats can come from very diverse sources, asking about attitudes that may capture an attitude from a specific threat, might not capture the individual's overall attitude. For example, the concept of threat vulnerability, threats could come from malware on computers, phishing emails on smart phones, or stalkers gaining information from social media accounts. Thus, the construct is operationalized for this research as formative. Other constructs, such as self-efficacy are theoretically the same as traditional measures so they are reflective. The PMT variables of threat vulnerability, threat severity, protective actions, domain knowledge, and protection motivation are measured using formative measures. The results of the reflective measurement assessment are in Table 5.4. The full questions and possible answers are in the Appendix 5.1.

Table 5.4: Results of the reflective constructs validity assessments

		Convergent Validity		Internal Consistency		
Construct	Items	Loadings	t- statistics	AVE	Cronbach's α	Composite Reliability t-statistics
Self-Efficacy				0.745	0.936	176.521
	SE 14-1	0.808	30.331			
	SE 14-2	0.876	37.875			
	SE 14-3	0.870	46.100			
	SE 14-4	0.878	43.559			
	SE 14-5	0.881	44.878			

Table 5.4: (cont'd)

		Convergent Validity		Internal Consistency		
Construct	Items	Loadings	t- statistics	AVE	Cronbach's α	Composite Reliability t-statistics
Response Cost				0.561	0.897	190.387
	RC 15-1	0.573	15.987			
	RC 15-2	0.642	19.247			
	RC 15-3	0.726	26.212			
	RC 15-4	0.896	31.503			
	RC 15-5	0.661	20.118			
	RC 15-6	0.826	37.793			
	RC 15-7	0.859	43.511			
	RC 15-8	0.573	15.987			
Response Efficacy				0.700	0.872	103.521
	RE 16-1	0.614	12.917			
	RE 16-2	0.662	14.563			
	RE 16-3	0.816	26.030			
	RE 16-4	0.811	27.514			
	RE 16-5	0.793	25.696			
	RE 16-6	0.711	18.494			
Fear				0.634	0.896	127.363
	FR 21-1	0.706	25.988			
	FR 21-2	0.774	30.946			
	FR 21-3	0.754	29.223			
	FR 21-4	0.865	43.626			
	FR 21-5	0.868	46.627			
Protection Habit Strength				0.808	0.926	125.557
	HS 26-1	0.941	41.731			
	HS 26-2	0.914	42.853			
	HS 26-4	0.840	27.216			
Post Self-Efficacy				0.813	0.956	228.416
	PSE 49-1	0.917	60.298			
	PSE 49-2	0.879	44.558			
	PSE 49-3	0.901	43.810			
	PSE 49-4	0.911	52.536			
	PSE 49-5	0.899	52.284			
Post Fear				0.703	0.923	176.722
	PFR 50-1	0.820	36.736			
	PFR 50-2	0.739	27.352			
	PFR 50-3	0.879	47.549			
	PFR 50-4	0.893	62.462			
	PFR 50-5	0.868	60.714			

Table 5.4: (cont'd)

		Convergent Validity		Internal Consistency		
Construct	Items	Loadings	t- statistics	AVE	Cronbach's a	Composite Reliability t-statistics
Post Fatalism				0.579	0.806	49.464
	PFT 53-1	0.697	21.238			
	PFT 53-2	0.823	27.474			
	PFT 53-3	0.758	28.419			
Post Response Cost				0.674	0.923	190.387
	PRC 51-2	0.754	23.260			
	PRC 51-3	0.805	29.257			
	PRC 51-4	0.684	19.465			
	PRC 51-5	0.867	37.284			
	PRC 51-6	0.902	50.052			
	PRC 51-7	0.891	53.452			
Post Response Efficacy				0.700	0.920	109.929
	PRE 52-1	0.834	28.084			
	PRE 52-2	0.766	22.607			
	PRE 52-3	0.843	35.593			
	PRE 52-5	0.872	38.783			
	PRE 52-6	0.864	44.069			

The variables of threat vulnerability, threat severity, protective actions, domain knowledge, and protection motivation are measured using formative measures. Formative measures were all tested for variance inflation factor (VIF) and the constructs themselves were also tested for VIF. Items higher than 5 were removed from all constructs. Through iterative analysis and cleaning the resulting items with their loading weights, standard deviation, t-value, p-value and VIF factors are in Table 5.5 (Liao & Valliant, 2012; O'Brien, 2007; Pahnila, Siponen, & Mahmood, 2007).

Table 5.5: Discriminant validity for formative constructs

Construct	Item	Weight	Std. Error	T-Stat	p-value	VIF
Common Threat Experiences						
	CTE 10_1	0.103	0.065	1.581	0.114	2.199
	CTE 10_2	-0.027	0.051	0.544	0.586	1.904
	CTE 10_3	0.235	0.061	3.862	0.000	2.016
	CTE 10_4	0.467	0.070	6.701	0.000	2.206

Table 5.5: (cont'd)

Construct	Item	Weight	Std. Error	T-Stat	p-value	VIF
Serious Threat Experiences						
	STE Q11_1	0.022	0.023	0.360	0.719	1.505
	STE Q11_2	0.220	0.218	3.059	0.002	2.314
	STE Q11_3	0.069	0.066	1.007	0.314	1.505
	STE Q11_4	0.326	0.332	4.601	0.000	1.807
	STE Q11_5	0.188	0.183	1.897	0.058	2.576
	STE Q11_6	0.380	0.376	3.560	0.000	2.770
Threat Severity						
	TSV 12_1	0.048	0.119	0.406	0.685	1.860
	TSV 12_2	0.325	0.154	2.106	0.035	2.377
	TSV 12_3	0.465	0.157	2.955	0.003	2.675
	TSV 12_4	0.350	0.162	2.167	0.030	3.108
	TSV 12_5	-0.292	0.100	2.929	0.003	1.610
	TSV 12_6	0.134	0.145	0.926	0.354	2.601
	TSV 12_7	-0.320	0.128	2.495	0.013	1.558
	TSV 12_8	-0.211	0.110	1.913	0.056	1.660
Fatalism						
	FTL 20_1	0.318	0.053	5.965	0.000	1.657
	FTL 20_2	0.534	0.045	11.805	0.000	1.260
	FTL 20_3	0.432	0.053	8.114	0.000	1.675
	FTL 20_4	-0.087	0.047	1.848	0.065	1.214
	FTL 20_5	-0.003	0.026	0.102	0.919	1.007
Protective Actions						
	PRA 25_1	-0.060	0.060	0.060	0.311	1.451
	PRA 25_10	0.089	0.065	0.065	0.169	1.514
	PRA 25_11	0.124	0.061	0.061	0.044	1.291
	PRA 25_12	0.276	0.065	0.065	0.000	1.307
	PRA 25_13	0.283	0.128	0.128	0.028	3.578
	PRA 25_2	0.258	0.068	0.068	0.000	1.436
	PRA 25_3	-0.093	0.061	0.061	0.125	1.456
	PRA 25_4	-0.088	0.130	0.130	0.497	3.701
	PRA 25_5	-0.176	0.061	0.061	0.004	1.506
	PRA 25_6	0.036	0.074	0.074	0.625	1.839
	PRA 25_7	0.228	0.074	0.074	0.002	1.583
	PRA 25_8	0.203	0.064	0.064	0.002	1.445
	PRA 25_9	0.296	0.062	0.062	0.000	1.375

Table 5.5: (cont'd)

Construct	Item	Weight	Std. Error	T-Stat	p-value	VIF
General Protection Motivation						
	GPM 48_1	0.160	0.062	2.582	0.010	3.168
	GPM 48_16	0.173	0.058	2.968	0.003	2.554
	GPM 48_4	0.166	0.058	2.843	0.005	2.764
	GPM 48_5	0.315	0.058	5.408	0.000	1.560
	GPM 48_6	0.422	0.060	7.047	0.000	1.957
Target Protection Motivation						
	TPM 48_2	0.358	0.073	4.903	0.000	2.764
	TPM 48_8	0.354	0.053	6.650	0.000	1.467
	TPM 48_9	0.443	0.067	6.574	0.000	2.679

Domain knowledge was a single item scale that was the sum of correct items from the scale developed by Pew Research for the cybersecurity knowledge project with the addition of two items specifically about browser security (Olmstead & Smith, 2017). The Pew study of 1, 055 adults on a panel had an average total correct of 5.5 for their 13-item scale. My MTurk sample had an average of 8.28 correct answers for the 15-item scale.

The data was tested for other forms of discriminant validity as well. The Fornell-Larker criterium was run with results given in Appendix 5.8. Although the Fornell-Larker criterium is widely accepted as a method for demonstrating discriminant validity, there were concerns that these did not always reliably detect issues with discriminant validity (Henseler, Ringle, & Sarstedt, 2015). Thus, using a multitrait-multimethod matrix the heterotrait-monotrait ratio of correlations (HTMT) was developed and growing in use, it asserts that if the HTMT value is below 0.900, that discriminant validity is achieved (Henseler et al., 2015). The HTMT are below in Table 5.6

Table 5.6: HTMT values

Construct Comparisons	Value and p-Value	t Statistics
Fear -> Domain Knowledge	-0.095**	2.606
POST Fatalism -> Domain Knowledge	-0.301***	7.933
POST Fatalism -> Fear	0.291***	6.803
POST Fear -> Domain Knowledge	-0.166***	4.570
POST Fear -> Fear	0.867***	46.525
POST Fear -> POST Fatalism	0.358***	8.529
POST Response Cost -> Domain Knowledge	-0.117**	3.070
POST Response Cost -> Fear	0.400***	10.280
POST Response Cost -> POST Fatalism	0.603***	16.886
POST Response Cost -> POST Fear	0.452***	12.296
POST Response Efficacy -> Domain Knowledge	0.181***	4.936
POST Response Efficacy -> Fear	-0.013	0.358
POST Response Efficacy -> POST Fatalism	-0.426***	9.339
POST Response Efficacy -> POST Fear	-0.062	1.735
POST Response Efficacy -> POST Response Cost	-0.333***	7.726
POST Self-efficacy -> Domain Knowledge	0.216***	6.117
POST Self-efficacy -> Fear	-0.159***	4.033
POST Self-efficacy -> POST Fatalism	-0.353***	8.403
POST Self-efficacy -> POST Fear	-0.169***	4.491
POST Self-efficacy -> POST Response Cost	-0.332***	8.285
POST Self-efficacy -> POST Response Efficacy	0.681***	19.207
Protection Habit Strength -> Domain Knowledge	0.275***	8.471
Protection Habit Strength -> Fear	-0.164***	4.063
Protection Habit Strength -> POST Fatalism	-0.256***	6.219
Protection Habit Strength -> POST Fear	-0.148***	3.817
Protection Habit Strength -> POST Response Cost	-0.304***	8.030
Protection Habit Strength -> POST Response Efficacy	0.279***	7.957
Protection Habit Strength -> POST Self-efficacy	0.518***	18.257
Response Cost -> Domain Knowledge	-0.153***	4.270
Response Cost -> Fear	0.436***	11.602
Response Cost -> POST Fatalism	0.440***	11.459
Response Cost -> POST Fear	0.429***	11.339
Response Cost -> POST Response Cost	0.749***	28.658
Response Cost -> POST Response Efficacy	-0.238***	7.222
Response Cost -> POST Self-Efficacy	-0.315***	9.439
Response Cost -> Protection Habit Strength	-0.339***	9.032
Response Efficacy -> Domain Knowledge	0.240***	6.210
Response Efficacy -> Fear	-0.056	1.403
Response Efficacy -> POST Fatalism	-0.420***	10.708
Response Efficacy -> POST Fear	-0.093*	2.366
Response Efficacy -> POST Response Cost	-0.356***	9.715
Response Efficacy -> POST Response Efficacy	0.718***	25.968
Response Efficacy -> POST Self-efficacy	0.572***	17.369
Response Efficacy -> Protection Habit Strength	0.326***	8.701
Response Efficacy -> Response Cost	-0.297***	8.533
Self-efficacy -> Domain Knowledge	0.293***	8.533

Table 5.6: (cont'd)

Construct Comparisons	Value and p-Value	t-Statistics
Self-efficacy -> Fear	-0.270***	6.868
Self-efficacy -> POST Fatalism	-0.333***	8.604
Self-efficacy -> POST Fear	-0.253***	6.481
Self-efficacy -> POST Response Cost	-0.349***	9.354
Self-efficacy -> POST Response Efficacy	0.457***	11.794
Self-efficacy -> POST Self-Efficacy	0.643***	20.142
Self-efficacy -> Protection Habit Strength	0.574***	20.080
Self-efficacy -> Response Cost	-0.427***	13.139
Self-efficacy -> Response Efficacy	0.549***	13.814
Threat Vulnerability -> Domain Knowledge	-0.262***	7.562
Threat Vulnerability -> Fear	0.370***	10.189
Threat Vulnerability -> POST Fatalism	0.286***	6.850
Threat Vulnerability -> POST Fear	0.397***	11.741
Threat Vulnerability -> POST Response Cost	0.355***	9.101
Threat Vulnerability -> POST Response Efficacy	-0.131***	3.676
Threat Vulnerability -> POST Self-efficacy	-0.243***	6.739
Threat Vulnerability -> Protection Habit Strength	-0.210***	5.360
Threat Vulnerability -> Response Cost	0.468***	14.150
Threat Vulnerability -> Response Efficacy	-0.210***	5.177
Threat Vulnerability -> Self-efficacy	-0.321***	7.884

*p<.05, **p<.01, ***p<.001

5.3.3 Correlations of constructs

The basic constructs showed strong correlations with each other as shown in Table 5.6. The path model also showed support of the smaller pilot study in many ways, there were some major differences which supported the importance of exploring the potential impacts of domain knowledge and self-efficacy on how individuals process a cybersecurity compliance message. The Pearson's correlations of constructs (2-tailed) showed many strong and statistically significant relationships. A few of these warrant a careful look as they reveal some interesting relationships between domain knowledge, self-efficacy, and willingness to enact protections (i.e., protection motivation).

Domain knowledge was significantly correlated with all items except target protection motivation and general protection motivation. Domain learning was three

specific questions dealt with in the tutorials for all conditions. The lack of significance would indicate that the material was presented in a way that previous domain knowledge was not correlated with the ability to learn and remember the material. Domain knowledge was positively correlated with many constructs that are associated with better cybersecurity protections, such as being positively correlated with self-efficacy $r(792)= .26$, $p<.01$, response efficacy $r(792)= .22$, $p<.01$, protective actions $r(792)= .27$, $p<.01$, and protective habit strength $r(792)= .28$, $p<.01$. It was also negatively correlated with constructs that are usually associated with poor security choices such as fatalism $r(792)= -.29$, $p<.01$, and fear $r(792)= -.09$, $p<.01$. Higher domain knowledge was also negatively correlated with both common $r(792)= -.16$, $p<.01$ and serious $r(792)= -.17$, $p<.01$ threat experiences. It was correlated with a higher sense of threat severity $r(792)= .12$, $p<.01$ but lower sense of threat vulnerability $r(792)= -.25$, $p<.01$. The surprising finding was that this construct was not directly correlated with protection motivation, which would be the stated intentions to improve security protections.

Self-efficacy, as seen in countless studies, was positively correlated with taking actions that were protective in nature. These include general protection motivation $r(785)= .37$, $p<.01$, protection habit strength $r(785)= .56$, $p<.01$, response efficacy $r(785)= .48$, $p<.01$, and threat severity $r(785)= .19$, $p<.01$. At the same time self-efficacy was negatively correlated with fatalism $r(785)= -.32$, $p<.01$, fear $r(785)= -.27$, $p<.01$, response cost $r(785)= -.41$, $p<.01$, threat vulnerability $r(785)= -.31$, $p<.01$, and both common $r(785)= -.20$, $p<.01$ and serious $r(785)= -.22$, $p<.01$ threats. The construct of “Time Difference Online” is the differential of how much time participants reported using computers of all types for all activities, and separate question of how much leisure time they spent on

computing devices. A larger number would indicate that the participant is doing more work-related activities. This value of time on computers for work was positively correlated with lower experiences with both common $r(792)= -.13$, $p<.01$ and serious $r(792)= -.12$, $p<.01$ threat experiences. The higher work time online was positively correlated with domain knowledge $r(792)= .15$, $p<.01$, self-efficacy $r(792)= .09$, $p<.01$, protection actions $r(792)= .07$, $p<.01$, and protective habit strength $r(792)= .10$, $p<.01$

Table 5.7: Pearson's correlations of constructs

	Time Difference Online	Prev. Exp. Common	Prev. Exp. Serious	Threat Severity	Threat Vulnerability	Fatalism	Fear	Response Cost	Response Efficacy
Time Difference Online	1								
Prev. Exp. Common	-.13**	1							
Prev. Exp. Serious	-.12**	.50**	1						
Threat Severity	.07	-.03	-.14**	1					
Threat Vulnerability	-.13**	.41**	.28**	.14**	1				
Fatalism	-.10**	.21**	.18**	-.12**	.29**	1			
Fear	-.09*	.17**	.14**	.12**	.33**	.28**	1		
Response Cost	-.09**	.42**	.24**	.01	.43**	.36**	.40**	1	
Response Efficacy	.09*	-.17**	-.29**	.31**	-.18**	-.30**	-.05	-.26**	1
Self-efficacy	.09*	-.20**	-.22**	.20**	-.31**	-.32**	-.27**	-.41**	.48**
Protection Habit Strength	.10**	-.11**	-.06	.07*	-.21**	-.32**	-.16**	-.32**	.30**
Protection Actions	.07*	-.08*	-.07	.13**	-.13**	-.24**	-.04	-.19**	.29**
Domain Knowledge	.15**	-.16**	-.17**	.12**	-.25**	-.29**	-.09*	-.15**	.22**
Post Fear	-.07*	.20**	.15**	.10**	.36**	.28**	.79**	.39**	-.09*
Post Fatalism	-.06	.21**	.23**	-.18**	.26**	.71**	.29**	.38**	-.32**
Post Self-efficacy	.08*	-.17**	-.23**	.21**	-.23**	-.28**	-.15**	-.30**	.52**
Post Response Efficacy	.05	-.14**	-.27**	.33**	-.11**	-.24**	.00	-.22**	.64**
Post Response Cost	-.08*	.32**	.25**	-.10**	.33**	.35**	.37**	.72**	-.32**
General Protection Motivation	.06	-.11**	-.24**	.27**	-.08*	-.18**	.01	-.22**	.51**
Target Protection Motivation	.03	-.03	-.12*	.23**	-.01	-.14**	.08*	-.13**	.44**

Table 5.7: (cont'd)

	Self-efficacy	Protection Habit Strength	Protection Actions	Domain Knowledge	Post Fear	Post Fatalism	Post Self-efficacy	Post Response Efficacy	Post Response Cost	Target Prot. Mot.
Time Difference Online										
Prev. Exp. Common										
Prev. Exp. Serious										
Threat Severity										
Threat Vulnerability										
Fatalism										
Fear										
Response Cost										
Response Efficacy										
Self-efficacy	1									
Protection Habit Strength	.56**	1								
Protection Actions	.36**	.62**	1							
Domain Knowledge	.26**	.28**	.27**	1						
Post Fear	-.25**	-.15**	-.04	-.17**	1					
Post Fatalism	-.26**	-.23**	-.17**	-.23**	.35**	1				
Post Self-efficacy	.61**	.51**	.38**	.20**	-.16**	-.29**	1			
Post Response Efficacy	.40**	.27**	.28**	.16**	-.05	-.32**	.64**	1		
Post Response Cost	-.33**	-.30**	-.23**	-.12**	.42**	.52**	-.31**	-.30**	1	
General Protection Motivation	.37**	.34**	.38**	.06	-.00	-.29**	.60**	.62**	-.34**	1
Target Protection Motivation	.30**	.34**	.46**	.01	.08*	-.22**	.55**	.56**	-.26**	.74**

At the same time, time online was inversely correlated with threat vulnerability r(792)= -.13, p<.01, fatalism r(792)= -.10, p<.01, fear r(792)= -.09, p<.01, and response cost r(792)= -.09, p<.01. To summarize, the greater the time for work on computers was correlated with many of the constructs seen as leading to protective actions, yet it was not significantly correlated with protection motivation directly.

5.3.4 Correlations of constructs for pre/ post measures by group

The pre/ post measures were analyzed by group to look for changes in the correlations according to condition of the participant. Differences in the correlations would indicate that there was a difference in the impact(s) of the message. A very high correlation (e.g., approaching 1.0) would indicate the message had no impact. The lower the correlation would indicate a greater impact by the message. If there is a difference between the condition, then there would be differences in the correlations between pre and post measures. Using SPSS, I first selected those that were in the control condition and ran the correlations for the pre/post measures; the results are in Table 5.7. Then, I selected the training (e.g., experimental) condition and ran the same analysis; these results are in Table 5.8. The results are presented in a Table side-by-side for ease of comparison in Appendix 5.3.

Some of the constructs showed little change by condition in the correlation analysis. Fear to post fear r(397)=.80, p<.01 in the control group, was little different from fear to post fear r(394)= .78, p<.01 for the training group. Response cost to post response cost was r(392)=.74 for the control group and r(392)=.71 for the training group. Response efficacy showed quite a bit more change by group with r(392)=.67, p<.01 for the control group and r(389)=.60, p<.01 for the training group. Also, fatalism changed by group as it

was r(397)=.75, p<.01 for the control group and r(392)=.66, p<.01 for the training group. The largest change was self-efficacy in that it was r(394)=.70, p<.01 for the control group and r(392)=.54, p<.01 for the training group.

Correlations with our direct variables, general protection motivation did vary by condition. Self- efficacy (control group: r(397)=.55, p<.01; training group r(392)=.56, p<.01) was strongly correlated to general protection motivation, there was less correlation to the target protection motivation in the training group (control group: r(397)=.64, p<.01; training group r(392)=.59, p<.01). Response efficacy was almost identical by group for general protection motivation (control group: r(396)=.56, p<.01; training group r(391)=.55), but for the target issues it was lower for the training group (control group: r(396)=.64, p<.01; training group r(391)=.59, p<.01). Fear was a significant factor for those in the control condition (control group: r(394)=.15, p<.01) but not for the training group r(391)=.00, ns). Fear was also not significantly correlated with the target behaviors in either condition (control group: r(394)=.03, ns; training group r(391)=.00, ns).

Overall, the statistically significant relationships between the constructs in the model indicate that further analysis would be appropriate. Structural equation modeling would best allow a deeper understanding of the relationships and how these constructs work towards motivating individuals towards cyber secure practices.

Table 5.8: Pre/ Post correlations for the control condition

	Fear	Fatalism	Self-Efficacy	Response Efficacy	Response Cost	Post Fear	Post Fatalism	Post Self-Efficacy	Post Response Efficacy	Post Response Cost	General Protection Motivation	Target Protection Motivation
Fear	1											
Fatalism	.27**	1										
Self-Efficacy	-.22**	-.34**	1									
Response Efficacy	-.02	-.34**	.54**	1								
Response Cost	.39**	.43**	-.38**	-.25**	1							
Post Fear	.80**	.26**	-.18**	-.034	.36**	1						
Post Fatalism	.30**	.75**	-.27**	-.36**	.39**	.32**	1					
Post Self-Efficacy	-.14**	-.32**	.70*	.57**	-.32**	-.12*	-.30**	1				
Post Response Efficacy	.019	-.25**	.46**	.67**	-.25**	.01	-.35**	.63**	1			
Post Response Cost	.40**	.40**	-.36**	-.30**	.74**	.40**	.51**	-.28**	-.31**	1		
General Protection Motivation	.11*	-.15**	.38**	.46**	-.12*	.15**	-.21**	.55**	.56**	-.20**	1	
Target Protection Motivation	-002	-.23**	.45**	.52**	-.26**	.03	-.29**	.61**	.64**	-.35**	.75**	1

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

*. Correlation is significant at the 0.05 level (2-tailed).

Table 5.9: Pre/ Post correlations for the training condition

	Fear	Fatalism	Self-Efficacy	Response Efficacy	Response Cost	Post Fear	Post Fatalism	Post Self-Efficacy	Post Response Efficacy	Post Response Cost	General Protection Motivation	Target Protection Motivation
Fear	1											
Fatalism	.30**	1										
Self-Efficacy	-.31**	-.30**	1									
Response Efficacy	-.09	-.26**	.43**	1								
Response Cost	.40**	.29**	-.43**	-.28**	1							
Post Fear	.78**	.30**	-.31**	-.14**	.43**	1						
Post Fatalism	.30**	.66**	-.26**	-.27**	.38**	.39**	1					
Post Self-Efficacy	-.16**	-.24**	.54**	.48**	-.29**	-.19**	-.28**	1				
Post Response Efficacy	-.05	-.23**	.35**	.60**	-.18**	-.12*	-.28**	.65**	1			
Post Response Cost	.35**	.31**	-.30**	-.35**	.70**	.49**	.54**	-.33**	-.28**	1		
General Protection Motivation	.05	-.15**	.24**	.40**	-.15**	.00	-.24**	.56**	.55**	-.31**	1	
Target Protection Motivation	.03	-.15**	.30**	.48**	-.17**	-.04	-.29**	.60**	.59**	-.33**	.73**	1

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

*. Correlation is significant at the 0.05 level (2-tailed).

5.3.5 Results of path analysis

Structural equation modeling (SEM) is growing in use in many fields, such as information systems, since it is able to test more complex models and help improve understanding of processes that are influenced by multiple factors (Fornell & Larcker, 1981). The first step, verifying construct and discriminant validity (Henseler et al., 2015), helps improve validity of the overall model and ultimate findings. As already discussed, the individual constructs indicated strong validity both from external sources (e.g., being developed based on previous research and modified based on focus group research) as well as testing the data using multiple statistical methods.

The data was tested using SmartPLS software using several different methods. SmartPLS was chosen as the tool for analysis, as it does not make the assumption of normal distributions and it is able to analyze models that include both formative and reflective constructs (Ringle, Wende, & Becker, 2015). There are several options in the SmartPLS software for processing the data and each has special strengths that can give insight to the data. Using the software, I generated two groups based on exposure to the control message or the experimental (training) message. Initial data runs were using the PLS Algorithm to look for overall fit. Henseler et al., (2015) suggest using standardized root mean square residual (SRMR) to avoid model misspecification. Less than 0.10 is seen as acceptable fit (Cangur & Ercan, 2015). The composite factor mode of the SRMR for all participants is 0.061, suggesting acceptable model fit. The initial wave of analysis also produced the R square values for all the constructs and the path coefficients. This method produces unstandardized b-values for the coefficients, thus the b value does represent the change expected in the dependent variables by one unit, for one unit of

change in the independent variables, keeping all other independent variables constant (Hayes, Glynn, & Huge, 2012). The initial run, using the PLS consistent algorithm produces values for the entire data set (i.e., “Complete”) as well as all values for each condition showing R square values for each construct, overall model fit, and other discriminant validity variables. The R square values of the combined constructs are shown in Figure 5.1. However, this round of analysis does not test for statistical significance between the groups for each construct and path. Thus, a subsequent run using bootstrapping, with parameters set for 1000 samples for each item and pairwise deletion of missing values was run to produce the significance levels of each path, such as confidence intervals, t-values, p-values. The path values that showed statistical significance are in figure 5.2. The table of path values for the combined participants is in Table 5.9. A third round of analysis was done using multi-group analysis settings. This method is able to test for parametric differences, this would indicate statistical significance between the conditions. Table 5.9 shows the hypotheses and the results of the SEM analysis, this includes the path name, the hypothesized relationship, the path coefficients and statistical significance, the t-values, and if the hypothesis was supported.

The new constructs to the PMT brought some interesting insights. Domain knowledge was significantly influential in many positive dimensions in looking at the combined groups. It led to higher self-efficacy (beta=0.207, p<.001), and higher protection habit strength (beta=0.146, p<.001). Domain knowledge is also negatively related to fatalism (beta= -0.225, p<.001) and threat vulnerability (beta=-0.123. Which would mean as domain knowledge increased fatalism and threat vulnerability decreased. Surprisingly, it was not significantly tied to fear. Self-efficacy led to higher beliefs in response efficacy

(beta=0.472, p<.001) threat severity (beta=0.151, p<.01). Self-efficacy had a negative relationship with response cost (beta=0.341, p<.001), fear (beta=0.176, p<.001) and threat vulnerability (beta=0.199, p<.001).

Experiences with common threats did increase a sense of vulnerability (beta=0.293, p<.001) and were strongly tied to experiencing serious threats (beta=0.724, p<.001). They led to lower self-efficacy (beta= -0.203, p<.001), lower beliefs in response efficacy (beta=0.137, p<.001), and lower perceptions of threat severity (beta= -0.298, p<.001). It also led to higher response cost (beta= 0.375, p<.001). Contrary to what was predicted, the experiences with common threats did not lead to individuals improving their domain knowledge, but there was a negative relationship (beta= -0.304, p<.001).

Figure 5.1: Adjusted R^2 values of model constructs for all participants

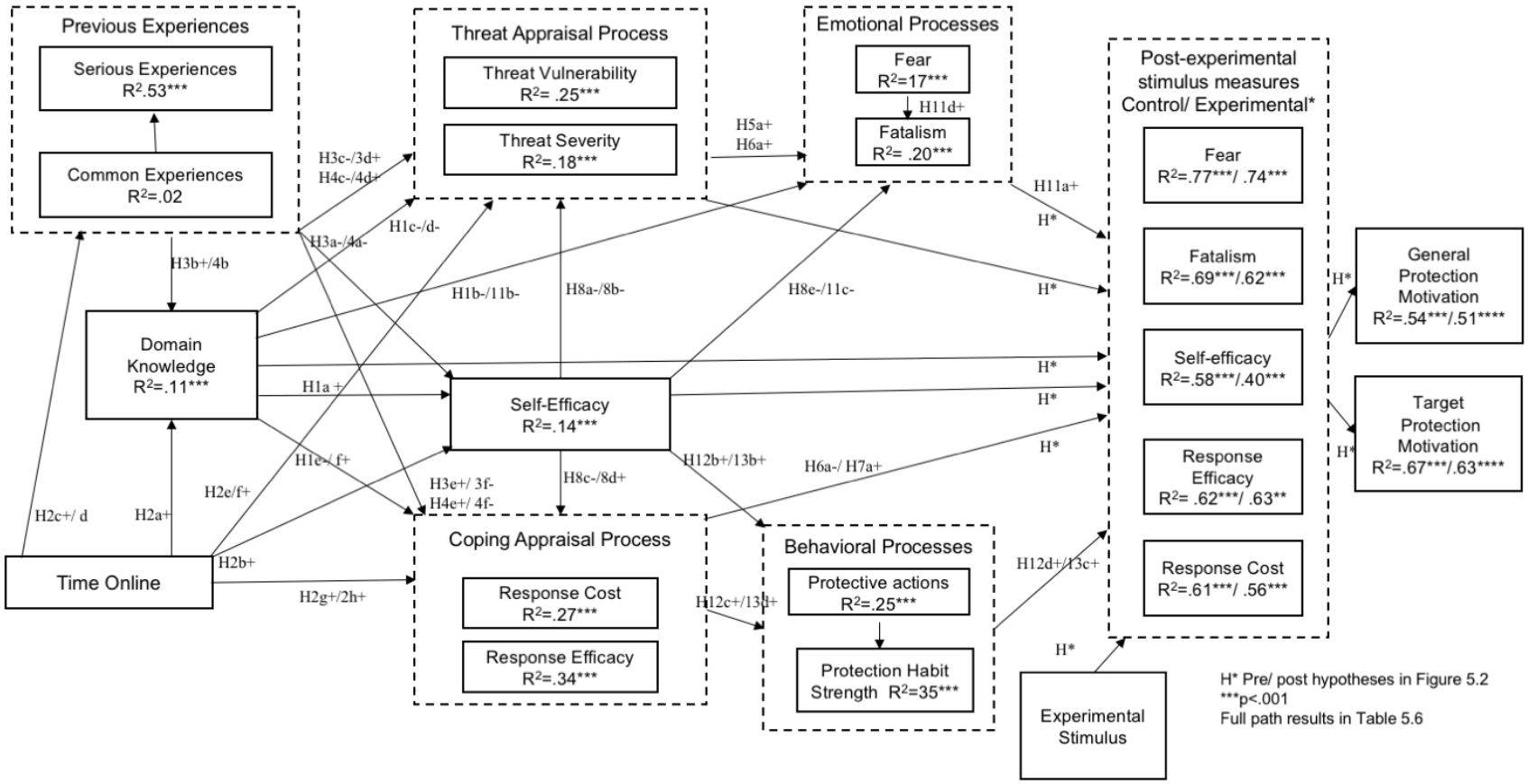


Table 5.10: Pre-experimental hypotheses and path coefficient results

	Path Name	Relationship	Path Coefficient	t-statistic	Hypothesis Supported?
Domain Knowledge					
H1a	Domain knowledge → self-efficacy	positive	0.207***	5.674	yes
H1b	Domain knowledge → fear	negative	0.047	1.323	no, ns
H1c	Domain knowledge → threat severity	positive	0.096*	2.210	yes
H1d	Domain knowledge → threat vulnerability	negative	-0.123**	3.490	yes
Time Online					
H2a	Time online → domain knowledge	positive	0.115**	3.359	yes
H2b	Time online → self-efficacy	positive	0.043	1.184	yes, ns
H2c	Time online → exp. with common threats	negative	-0.148**	3.199	yes
H2d	Time online → threat severity	positive	0.044	1.196	yes, ns
H2e	Time online → threat vulnerability	positive	-0.075*	2.130	yes
Experiences with common threats					
H3a	Exp. common threats → self-efficacy	negative	-0.203**	2.522	yes
H3b	Exp. common threats → domain knowledge	positive	-0.304***	8.114	no
H3c	Exp. common threats → threat severity	negative	-0.298***	4.151	yes
H3d	Exp. common threats → threat vulnerability	positive	0.293***	4.313	yes
H3e	Exp. common threats → response cost	positive	0.375***	6.545	yes
H3f	Exp. common threats → response efficacy	negative	-0.137*	2.205	yes
H3g	Exp. common threats → exp. with serious threats	positive	0.724***	17.118	yes
Experiences with serious threats					
H4a	Exp. serious threats → self-efficacy	negative	-0.053	0.710	yes, ns
H4b	Exp. serious threats → domain knowledge	negative	-0.026	0.448	yes, ns
H4c	Exp. serious threats → threat severity	negative	0.007	0.128	yes, ns
H4d	Exp. serious threats → threat vulnerability	negative	0.029	0.449	no, ns
H4e	Exp. serious threats → response cost	negative	-0.117*	2.196	yes
H4f	Exp. serious threats → response efficacy	negative	-0.111	1.755	yes, ns

Table 5.10: (cont'd)

Path Name		Relationship	Path Coefficient	t-statistic	Hypothesis Supported?
Threat severity & threat vulnerability					
H5a	Threat severity → fear	positive	0.019	0.371	yes, ns
H6a	Threat vulnerability → fear	positive	0.330***	8.875	yes
Self-efficacy					
H8a	Self-efficacy → threat severity	negative	-0.161**	3.236	yes
H8b	Self-efficacy → threat vulnerability	negative	-0.199***	4.265	yes
H8c	Self-efficacy → response cost	negative	-0.341***	9.263	yes
H8d	Self-efficacy → response efficacy	positive	0.472***	11.128	yes
H8e	Self-efficacy → fear	negative	-0.176***	4.334	yes
Fatalism					
H14a	Domain knowledge → fatalism	negative	-0.176***	4.334	yes
H14b	Self-efficacy → fatalism	negative	-0.197***	4.455	yes
H14c	Fear → fatalism	positive	0.173***	3.679	yes
Protective Actions					
H15a	Self-efficacy → protective actions	positive	0.263***	5.443	yes
H15b	Exp. common threats → protective actions	negative	-0.088*	1.974	yes
H15c	Response efficacy → protective actions	positive	0.229***	4.937	yes
Protection Habit Strength					
H16a	Exp. common threats → protection habit strength	positive	0.148***	4.154	yes
H16b	Self-efficacy → protection habit strength	positive	0.548***	13.859	yes
H16c	Domain knowledge → protection habit strength	positive	0.146***	4.289	yes
H16d	Response efficacy → protection habit strength	positive	0.045	0.972	yes, ns
H16e	protection habit strength → general protection motivation	positive	0.037	0.982	yes, ns

* p <.05, ** p <.01, ***p<.001, ns= not significant

The bootstrapping analysis demonstrated the differences between conditions and the intentions to protect after watching the message. Pre-post measures showed little change for fear (beta=0.880, p<.001, control condition and beta=0.844, p<.001, training condition) and fatalism (beta=0.790, p<.001, control condition and beta=0.761, p<.001, training condition). The message seemed to have little impact on these dimensions. Response cost showed some impact as those in the training condition had more of a change and it was no longer a significant detractor from enacting security protections. In other words, those in the control group, without training, still saw response cost as an issue (beta=-0.185, p<.01) to enacting the target protections. Response efficacy showed change in both conditions for the pre-post measures (beta=0.512, p<.001, control condition and beta=0.378, p<.001, training condition). Those in the training condition had lower intentions to enact the specific protections addressed (beta=0.362, p<.001, control condition and beta=0.208, p<.001, training condition), yet they had a higher overall intention to protect.

The construct with the largest change by condition was self-efficacy. All of the participants had an impact in their self-efficacy as even the control condition showed a change compared to the other construct (e.g., fear). The training condition showed the most dramatic change as participants were able to actually see how to perform a security task their self-efficacy plummeted even though it was clearly demonstrated (beta=0.600, p<.001, control condition and beta=0.392, p<.001, training condition). Those in the control condition showed higher intention for the target behavior than those in the training condition (beta=0.362, p<.001, control condition and beta=0.206, p<.001, training condition). Figure 5.3 illustrates the results and Table 5.11 gives full details.

Figure 5.2: Hypotheses results in the composite analysis

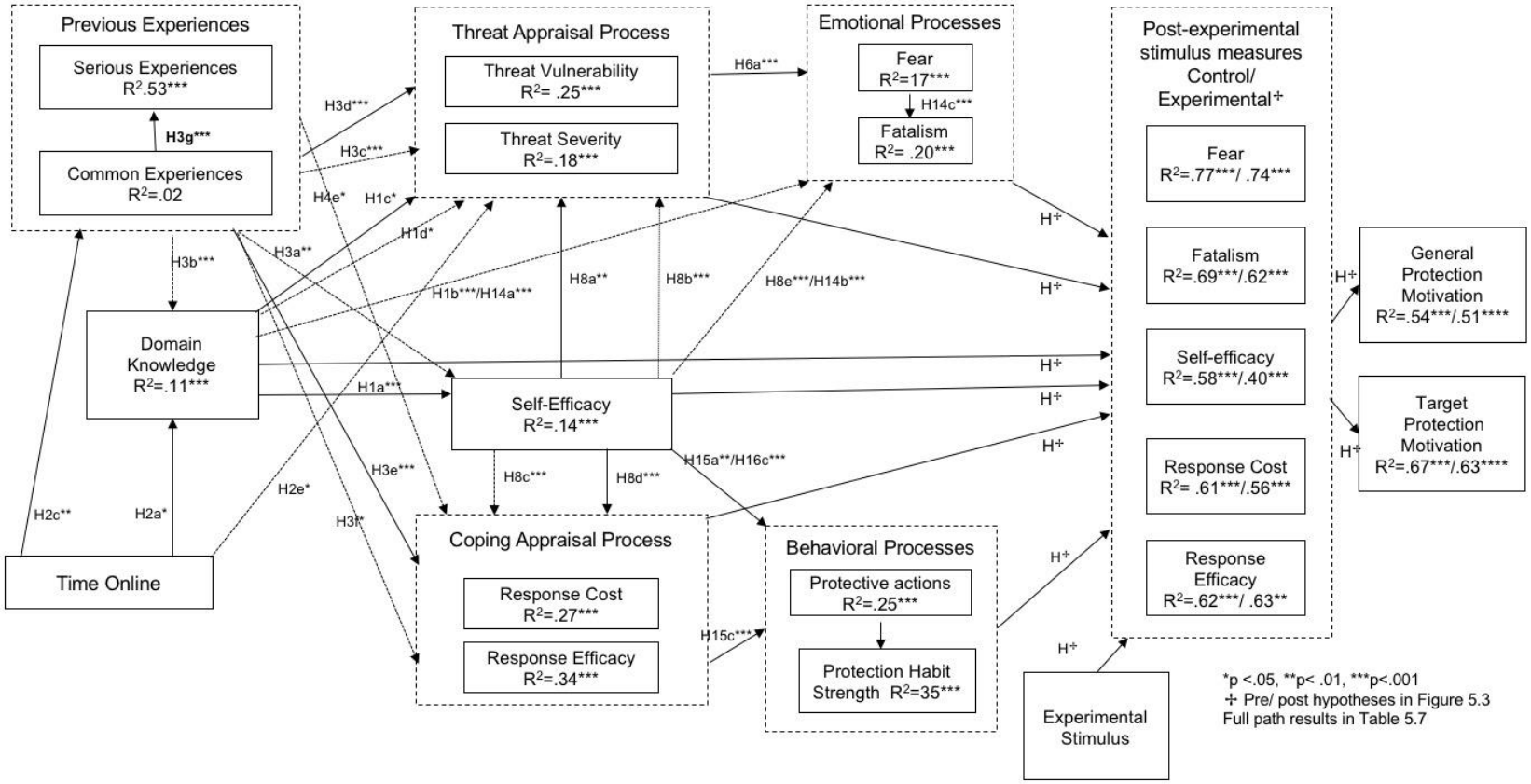


Figure 5.3: Post-exposure constructs and path coefficients by experimental group

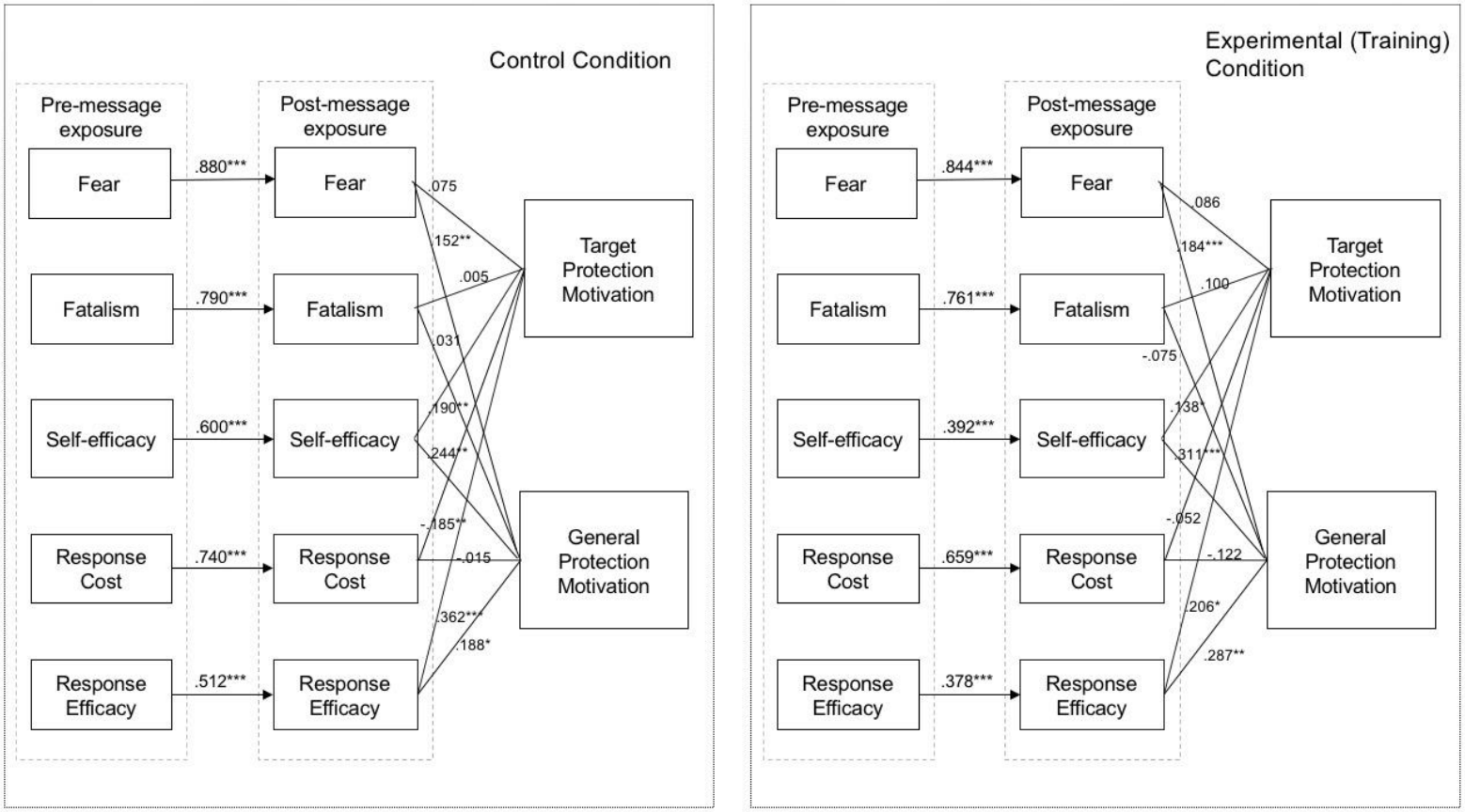


Table 5.11: Comparison of coefficients by experimental condition

H #	Path	Relationship	Coefficient	t-statistic	Hypothesis supported?
Fear- control condition					
H 9a	Fear → post fear	strong	0.880***	37.146	yes
H 9b	Post fear → general protection motivation	negative	0.152**	2.928	no
H 9c	Post fear→ target protection motivation	negative	0.075	1.655	no, ns
Fear- experimental (training) condition					
H9d	Fear → post fear	weaker †	0.844***	27.822	yes
H9e	Post fear → general protection motivation	negative	0.152***	2.928	no
H9f	Post fear → target protection motivation	negative	0.075	1.655	no, ns
Self-efficacy- control condition					
H10a	Self-efficacy→ post self-efficacy	positive	0.600***	10.476	yes
H10b	Post self-efficacy → general protection motivation	positive	0.244**	3.255	yes
H10c	Post self-efficacy → target protection motivation	positive	0.190**	2.589	yes
Self-efficacy experimental (training) condition					
H10d	Self-efficacy → post self-efficacy	weaker †	0.392***	5.181	yes
H10e	Post self-efficacy→ general protection motivation	positive	0.311***	4.633	yes
H10f	Post self-efficacy→ target protection motivation	positive	0.138*	2.350	yes
Response cost- control condition					
H11a	Response cost → post response cost	strong	0.740***	17.525	yes
H11b	Post response cost → general protection motivation	negative	-0.015	0.256	yes, ns
H11c	Post response cost → target protection motivation	negative	-0.185**	3.302	yes
Response cost - experimental (training) condition					
H11d	Response cost → post response cost	weaker †	0.659***	14.456	yes
H11e	Post response cost → general protection motivation	negative	-0.122	1.837	yes, ns
H11f	Post response cost → target protection motivation	negative	-0.052	1.143	yes, ns

Table 5.11: (cont'd)

H#	Path	Relationship	Coefficient	t-statistic	Hypothesis supported?
Response efficacy- control condition					
H12a	Response efficacy → post response efficacy	strong	0.512***	7.692	yes
H12b	Post response efficacy → general protection motivation	positive	0.362***	4.882	yes
H12c	Post response efficacy → target protection motivation	positive	0.188*	2.020	yes
Response efficacy- experimental (training) condition					
H12d	Response efficacy → post response efficacy	stronger †	0.378***	6.483	yes
H12e	Post response efficacy → general protection motivation	positive	0.287**	3.489	yes
H12f	Post response efficacy→ target protection motivation	positive	0.206*	2.524	yes
Response efficacy- control condition					
H13a	Fatalism → post fatalism	strong	0.790***	22.708	no
H13b	Post fatalism → general protection motivation	negative	-0.031	0.487	yes, ns
H13c	Post fatalism → target protection motivation	negative	-0.005	0.059	yes, ns
Response efficacy- experimental (training) condition					
H13d	Fatalism → post fatalism	weaker †	0.761***	19.826	yes
H13e	Post fatalism → general protection motivation	negative	-0.075	1.002	no, ns
H13f	Post Fatalism → target protection motivation	negative	-0.100	1.695	no, ns

*p<.05, **p<.01, ***P<.001 †= comparison to control group

The findings are quite interesting, but there is a threat to validity if the original groups have statistically significant differences. Any differences before the experiment need to be checked to assure that they are not a threat to findings. To test if differences between groups and paths were statistically different I took several steps. First, I ran a multi-group analysis (PLS-MGA) as it allows for testing non-parametric significance and builds on bootstrapping method using the Welch-Satterthwait test for differences between groups. It is appropriate for groups with non-normative distributions and those with large degrees of freedom (Asyraf Afthanorhan, Nazim, & Ahmad, 2014; Huang, 2016) . The Welch-Satterthwait results, showing there were no significant differences between constructs is in Table 5.12.

Table 5.12: Welch-Satterthwait test of reflective construct differences

	Composite Reliability-differential (Condition 1 vs Condition 2)	t-Value (Condition 1 vs Condition 2)
Domain Knowledge	0.000	1.666
Fear	0.000	0.035
POST Fatalism	0.017	1.056
POST Fear	0.008	1.108
POST Response Cost	0.001	0.134
POST Response Efficacy	0.000	0.033
POST Self-Efficacy	0.006	0.939
Protection Habit Strength	0.001	0.076
Response Cost	0.006	0.741
Response Efficacy	0.002	0.144
Self-efficacy	0.001	0.191
Threat Vulnerability	0.002	0.174

* none of the construct differences were significant.

The multi-group analysis also produces an analysis of each path by condition and the results showed the differences between group paths to look for potential pre-message differences that might bias the results by group. The MGA parametric test analyzes the

significance of the path differences. The paths that had significant differences are in Table 5.13. The full results of the parametric MGA analysis is in Appendix 5.4. This analysis was followed with an independent t-test using SPSS to test if the means of the constructs were different by group. The independent t-test was able to test the formative construct group differences which the Welch-Satterthwait test does not include. The most significant difference was between initial self-efficacy measures and post exposure measures (beta=1.91, p<.01), this would indicate the impact of the training portion of the video had a decrease in their self-efficacy after seeing exactly how to perform a security task. This might indicate that their self-efficacy was inflated from their true skill levels.

Table 5.13: Parametric test: paths with significant differences by condition

	Path Coefficients Differential (Control-Training)	t-Value of Path Differential
Self-efficacy → post Self-efficacy	0.191**	2.293
Experience with common threats → Response cost	0.215*	2.023
Self-efficacy → Threat Severity	0.211*	1.710

*p<.05, **p<.01

Other paths with significant differences were between experiences with common threats to response cost, in this case the perceptions of response cost were higher for the control group. In the post-message measures of response cost, this has gone down considerably for general protections, making it an insignificant barrier to enacting protections where before it was. The path for self-efficacy is also significantly higher for the path of self-efficacy to threat severity for those in the control condition. This would indicate that participants in considering their ability to protect themselves were seeing threat severity as a stronger factor. Given that after the message the self-efficacy was higher than those in the training condition, as well as the intentions to enact both general

and the target protections, it indicates the impact of the message was potentially higher than it appears just looking at the path coefficient figures. To further test for any potential validity issues, independent samples t-tests were run on the constructs that showed the path differentials and there was no significant differences in the means for self-efficacy in the control condition (M=5.6, SD=1.2) and the experimental (M=5.7, SD=1.2) conditions; t (785)= 0.676, p=.499. There was also no significant differences in the means for threat severity in the control condition (M=5.7, SD=1.2) and the experimental (M=5.7, SD=1.2) conditions; t (783)= -0.845, p=.398. Nor were there no significant differences in the means for response cost in the control condition (M=3.4, SD=1.3) and the experimental (M=3.4, SD=1.4) conditions; t (785)= -0.635 , p=.526. Finally, there were there no significant differences in the means for experiences with common threats in the control condition (M=2.8, SD=0.8) and the experimental (M=2.7, SD=0.8) conditions; t (782)= 0.817 , p=.414.

5.4 Discussion

Self-efficacy is core to individuals' intentions to protect themselves and be cyber secure. It not only was tied to general protection motivation, it also increased the motivation for performing the target behaviors. Probably the most profound finding of this research is that clearly showing a contextual demonstration of how to perform a cybersecurity task actually lowered self-efficacy. This would indicate that for many individuals, the anticipation of being efficacious in computer safety is not based on actual skills, but rather a perception of efficacy. This might be induced by the usability of other computer functions. Interface designs can give a sense of control and ease of use. There is usually high usability in everyday computer functions, especially those that are revenue

producing (e.g., making a purchase using a credit card). At the same time, privacy and security settings are often buried under layers of interfaces that require persistence to navigate. The responses after the control message would indicate there is an overall desire to protect oneself. However, after seeing exactly how to do it (in the experimental group), self-efficacy plummeted as well as the intentions to protect. The overall practices that lead to better personal cybersecurity seem to be embraced, but when shown the specifics and exactly what needs to be done, intentions suddenly go down. This could easily be due to the issue of enacting protections is harder than anticipated. Even when participants were shown clearly how to enact a protection, and the narration encouraged that the process is simple and quick, there still was lower motivation to perform these specific actions.

Domain knowledge was tied to both increasing the target protection motivation as well as general protection motivation. It also appears to be the dimension that is “working in the trenches” to improve almost all the key PMT constructs that lead to increased motivation to cyber security. It was reducing the attitude of fatalism, that would give individuals a feeling of hopelessness, or “why even try” attitudes. It also increased protection habit strength and general protection motivation. It was key to strengthening self-efficacy, which, and just discussed, it key to overall cyber secure behaviors. It also reduced fear, the emotional response that is seen as problematic in other domains as it often triggers maladaptive behaviors (Fazio & Towles-Schwen, 1999; K. Witte & Allen, 2000; Kim Witte, 1994), as discussed in Chapter Two. A deeper analysis on how different levels of domain knowledge may be interacting with self-efficacy will be in the next chapter.

Previous experiences with both common and serious threats were not a good "teacher." Understandably, experiences with common threats led to a lowered sense of self-efficacy and response efficacy. It also was tied to increased sense of response cost and strongly tied to the likelihood of experiencing a serious threat. Surprisingly, these experiences did not lead to increased domain knowledge, but they did lead to a lowered sense of threat severity. This almost seems like a recipe for disaster if individuals feel it is too much effort (i.e. response cost) to enact protections, they do not feel they are effective (i.e., response efficacy) and the threats are not that serious anyway (i.e., threat severity). Experiences with serious threat were also surprising, the results show no significant correlations with most constructs except that response cost went down. For those who have spent days or weeks trying to straighten out a compromised credit card, bank account, or convincing a vendor that they didn't purchase an item, having strong protections in place is comparatively easy. The mixed results in other measures after a serious threat experience indicate a sense of personal violation may be profound and complex. This should be studied in the future as the ranks of those experiencing the consequences of serious threats grow daily.

The analysis of the data indicated that the message did make an impact on the participants. The strength of the difference between those who were in the training condition and the control condition was surprising and in the opposite direction that was expected. In both conditions, even though attitudes towards general protections increased, intentions to follow through on the issues addressed by the message were not as strong. It would be expected that as a specific security issue is discussed, participants would be freshly aware of that issue and would have higher intention to comply. Those

who received the additional training, that gave even more details had significantly (b=.177, p<.05) lower levels of self-efficacy. It would be expected that an instructional tutorial that clearly showed how to perform a task and encouraged self-efficacy would increase self-efficacy. However, this finding gives us a substantial clue to the process that might be going in in the participants' processing of the message. Overall, people, in the focus groups, pilot study and this major study, care about cybersecurity, conceptually they agree security is a good thing. Yet when it gets down to performing a specific task, even after hearing about a new vulnerability, something happens and there is a lowering of motivation. This may be from the issues of constantly having to improve security protections and learn new routines (Shillair & Dutton, 2016). Or, this lower intention to protect might be indicators of difficulty with the usability of security tasks. Regardless of the difficulty of a task, knowing how to actually do it is a first step. Those who state they intend to do something will be more likely to follow through if they actually know how (see Ewoldsen, Rhodes, & Fazio, 2015; Nabi, Roskos-Ewoldsen, & Carpentier, 2008). This is especially true in the technological realm, things are often more complicated than it appears at first, especially when dealing with enacting security measures.

The often over-looked construct of response efficacy constantly showed itself to be an important component in cybersecurity motivation. Response efficacy was significantly connected with protection motivation both generally and for the target behavior. Individuals are often cognitive and energy misers (Zipf, 1949). They don't perform a task, especially a complicated or time-consuming task unless they feel it will bring some benefit. Given the constant stream of news reports of security breaches it is

important that individuals feel that security solutions work if they are going to bother to enact them.

The surprisingly limited impacts of fear are also profound. The basis of fear messages, increasing fear to improve compliance, has been used by many stakeholders for decades with mixed results. For example, anti-smoking campaigns that featured warnings about the dangers of smoking and increased likelihood of cancer. As these had mixed results in the health domain (Witte & Allen, 2000), this research helps bring insight into why they are even less effective in the cybersecurity domain. Most PMT research in the cybersecurity and information security domain doesn't explore the impact(s) of fear (Boss, Galletta, Lowry, Moody, & Polak, 2015) even though cybersecurity campaigns trigger fear by heightening a sense of risk. This research shows how even though fear can be a factor in enacting protections, this sense of fear doesn't seem to widely impact the desire to continue to use protective solutions.

Overall, this research shows that domain knowledge and self-efficacy go hand-in-hand to lower fatalism, as well as lowering domain cost and increasing motivation for cyber secure practices. For stakeholders, this information is crucial. Governments, companies, educational institutions and special interest groups who want to run initiatives to improve cybersecurity practices need to be careful to tailor the message to focus on increasing domain knowledge, self-efficacy and response efficacy. Heightening fear alone is not enough to increase willingness to improve protections, only when it is accompanied by understandable (e.g., increasing domain knowledge) and actionable (e.g., increasing response efficacy) steps that they can reasonably follow (e.g., increasing self-efficacy) will we see improvements in cyber secure behaviors. This analysis has

several findings that are breakthroughs in understanding how individuals respond to cybersecurity compliance communications. Persistent chasms between users self-reporting intentions and actual behaviors have been problematic for decades (Wash, Rader, & Fennell, 2017). The gap, and the impacts of the gap, between self-efficacy and actual knowledge (i.e., domain knowledge) of how to protect oneself becomes apparent as we look closely at the data.

5.5 Limitations and Further Research

There are many limitations to this phase of the research. As with any online survey, results are limited by the integrity and attentiveness of the participants and that they are honestly expressing their opinions and beliefs. Also, this survey only addresses intentions to protect and doesn't monitor participants' computers to see If they actually follow through on these intentions. More details about the limitations of this study and suggestions for future research will be in Chapter 7.

In the next chapter we explore potential interactions between different levels of domain knowledge and self-efficacy. This will help us understand how various levels of domain knowledge impact protection motivation. Also, we will look at how the different experimental conditions interact with a closer analysis of domain knowledge and its impact on self-efficacy.

APPENDICES

Appendix 5.1 Survey questions included in path analysis and factor loadings

Table 5.14: Variables for measured constructs

If the construct is formative the variance inflation factors are listed (VIF) and if the construct is reflective the Cronbach's alpha (α) and the item factor loadings from the structural equation modeling (SEM) are listed. All loadings and VIF factors are of the complete sample.

Construct/ Source	Variable	Loading/VIF
Time Online Differential		
The time online differential was a 1 item construct taken by subtracting Q7-Q6		VIF
	Q6 On a typical day how much time do you spend on all computing devices?	1.721
	Q7 On a typical day how much time do you spend on the Internet doing non-work activities (e.g., shopping, watching videos, reading news, Facebook, Instagram, etc.)	
Experience with common threats		
7-point scale: Never/ Once/ A couple times/ Several times/ Many times/ Frequently/ Always		VIF
	CT8_1 An unexpected pop up message or pop up ad	1.571
	CT8_2 Emails trying to get me to enter personal information or passwords (phishing)	1.297
	CT8_3 A message popped up offering a free computer security scan	2.005
	CT8_4 Browser warning that a site is compromised or not safe	1.630
	CT8_5 My computer slows down or is not running as fast as it used to	1.854
	CT9_1 Fan is running and computer seems to be working hard even when I am not running many programs	1.623
	CT9_2 New icons or programs appear out of nowhere	2.012
	CT9_3 Computer freezes up	1.726
	CT9_4 My security software won't update or run like it is supposed to	2.066

Table 5.14: (cont'd)

CT10_1 My computer has sent out messages I didn't send (either emails, Twitter, or Facebook messages)	2.201
CT10_2 My email or social media (e.g., Facebook, Instagram) account was compromised and I had to reset my password	1.905
CT10_3 I was locked out of my computer	2.020
CT10_4 My files or my computer was encrypted and held hostage (ransomware)	2.213
Experience with serious threats 7-point scale: Never/ Once/ A couple times/ Several times/ Many times/ Frequently/ Always	VIF
ST11_1 Had my social security number or credit card number stolen	1.506
ST11_2 I was the victim of an online scam and lost money	2.325
ST11_3 Had to have my computer hard drive wiped and reinstall my programs	1.506
ST11_4 Had to buy a new computer because of virus or malware problems	1.813
ST11_5 Had someone take control of my camera and record me	2.589
ST11_6 Been threatened with information gained from someone monitoring my computer activities.	2.639
Threat Vulnerability: Given YOUR current cyber security protections (e.g., using strong passwords, having virus protection software, etc.) and the current threats online, HOW LIKELY do you think the following issues MIGHT to happen to you (7-point scale from very unlikely to very likely	VIF
TV13_1 Have an unexpected pop up message or pop up ad	1.885
TV13_2 Get emails trying to get me to enter personal information or passwords (phishing)	1.616
TV13_3 The computer will slow down or is not run as fast as it used to	2.084
TV13_4 New icons or programs will appear out of nowhere	2.659

Table 5.14: (cont'd)

TV13_5 My email or social media (e.g., Facebook, Instagram) account will be compromised	2.178
TV13_6 My files or my computer will be encrypted and held hostage (ransomware)	3.918
TV13_7 Eventually have to have my computer hard drive wiped and reinstall my programs	3.048
TV13_8 Be threatened with information gained from someone monitoring my computer activities	3.433
Threat Severity: Please rate how harmful they would be IF they happened to you. 7-point Likert scale from not very harmful/ very harmful	VIF
TS12_1 If I had an unexpected pop up message or pop up ad	1.865
TS12_2 If I encounter phishing emails trying to get me to enter personal information	2.390
TS12_3 If my email account was hacked and I had to reset passwords	2.691
TS12_4 If malware was on my computer and other could use my computer for criminal purposes	3.116
TS12_5 If spyware was on my computer and watching what I typed	1.612
TS12_6 If my computer files got locked up and I couldn't access them	2.611
TS12_7 If someone could access my personal photographs	1.561
TS12_8 If I had to have my computer hard drive wiped and re-install my programs	1.662
Self-efficacy: Please tell us how much you agree or disagree with each statement. 7-Point Likert scale agree/disagree. α= .936	Loadings
SE14_1 I feel comfortable taking measures to secure my primary home computer	0.852
SE14_2 I am able to take measures to protect myself online	0.909
SE14_3 I have the resources and the knowledge to take necessary security measures	0.901

Table 5.14: (cont'd)

SE14_4 Taking necessary security measures is very doable	0.894
SE14_5 If I want to, I can take measures to protect myself online	0.905
Response Cost: Please tell us how much you agree or disagree with each statement 7-point Likert scale agree/ disagree. α= .918	Loadings
RC15_1 It always seems like I have to do security updates at the most inconvenient time	0.658
RC15_2 I often feel time pressure when I am trying to log in to my accounts	0.726
RC15_3 Taking security measures can slow down what I need to do	0.898
RC15_4 Following some security measures (e.g., updating software) may cause some of my programs not to work correctly	0.797
RC15_5 It is too much trouble to follow security measures	0.810
RC15_6 Security measures are a lot of hassle	0.707
RC15_7 Keeping security measures straight if bothersome	0.891
RC15_8 It is often inconvenient to take security measures	0.882
Response Efficacy Tell us how much you agree or disagree with each statement 7-point Likert scale Agree/Disagree, α= .920	Loadings
RE16_1 Protective software would be useful for detecting and removing malware or viruses.	0.625
RE16_2 Having hard to guess passwords that are different for my different accounts will help improve my security protections.	0.717
RE16_3 Keeping my operating systems updated will help improve my security protections	0.883
RE16_4 Keeping my Internet browser software updated will help improve my security protections.	0.886

Table 5.14: (cont'd)

RE16_5 Keeping my software programs updated will help improve my security protections	0.882
RE16_6 Avoiding dangerous web sites will keep me safe online	0.684

Fatalism

Tell us how much you agree or disagree with each statement.
7-point Likert scale Agree/Disagree, α= 715.

	Loadings
FT20_1 It doesn't matter what I do, it is random chance that people get hacked.	0.817
FT20_2 I don't worry about online safety because I don't have that much to protect	0.748
FT20_3 Most protective actions are a waste of time, if someone wants to hack you, you are going to get hacked.	0.829

Fear:

Tell us how much you agree or disagree with each statement.
7-point Likert scale Agree/Disagree, α= .896.

	Loadings
FR21_1 The trends in online security are worrisome to me	0.822
FR21_2 I fear that computer security issues are beyond the control of individuals	0.783
FR21_3 I am concerned about the rapid changes in computer security issues	0.856
FR21_4 Current online security issues make me feel afraid	0.880
FR21_5 When I think of computer security issues, I get very anxious about what might happen	0.861

Protective Actions:

Have you ever done any of the following things?
7-point Likert scale- Never/All the Time dots ranging in the middle

	VIF
PA25_1 Set your browser to disable or turn off cookies	1.455
PA25_2 Cleared cookies and browser history	1.439
PA25_3 Use private browser windows	1.459
PA25_4Checked to see if your browser is up to date	3.741
PA25_5 Encrypted your communications (email or text)	1.509

Table 5.14: (cont'd)

PA25_6 Changed the security settings on your Internet browser	1.843
PA25_7 Changed to a stronger password	1.587
PA25_8 Have different passwords for different accounts	1.447
PA25_9 Use a spam filter to block unwanted email	1.377
PA5_10 Check web site URL for "https"	1.291
PA25_11 Check the email address of sender before opening an email	1.291
PA25_12 Not gone to a web site because of a security warning from the browser	1.307
PA25_13 Checked to see if your browser is up to date	3.623

Protection Habit Strength:
Tell us how much you agree or disagree with each statement.
7-point Likert scale Strongly Agree/Strongly Disagree, α= .963

	Loadings
HS26_1 The use of security protections has become a habit for me	0.929
HS26_2 Using security protections has become natural to me	0.944
HS26_3 Online security is something I do automatically	0.955
HS26_4 Online protection is something I do without thinking	0.896
HS26_5 Online safety protection is part of my regular routine	0.944

Domain Knowledge
This is a single item score that is a sum of the correct answers to the following 15 questions (n= 794, M=7.7 (Std. Dev. 2.5)

	VIF
DK25 What does the "https://" at the beginning of a URL denote, as opposed to http:// (without the "s")?	1.000
DK26 Which of the following is an example of a "phishing" attack?	
DK27 A group of computers that is networked together and used by hackers to steal information is called a….	

Table 5.14: (cont'd)

DK28 Some websites and online services use a security process called two-step authentication. Which of the following images is an example of two-step authentication?	
DK29 Which of the following four passwords is the most secure?	
DK31 "Private Browsing" is a feature in many internet browsers that lets users access web pages without any information (like browsing history) being stored by the browser. Can internet service providers see the online activities of their subscribers when those subscribers are using private browsing?	
DK32Turning off the GPS function of your smartphone prevents any tracking of your phone's location.	
DK33 All email is encrypted by default	
DK34 By law, how many free credit reports can Americans obtain in a calendar year from each of the three major credit bureaus?	
DK35 If a public Wi-Fi network (such as in an airport or cafe') requires a password to access is it generally safe to use that network for sensitive activities such as online banking?	
DK36 What kind of cybersecurity risks can be minimized by using a Virtual Private Network (VPN)?	
DK37 Older Internet browsers have security weaknesses and might compromise my security as I look at web pages.	
DK38 Internet browsers automatically update themselves, so users never need to check them	
POST Self-Efficacy	
After watching the video-how much you agree or disagree with each statement.	
7-point Likert scale agree/ disagree. α= .956	Loadings
PSE49_1 I feel comfortable taking measures to secure my primary home computer	0.936

Table 5.14: (cont'd)

PSE49_2 I am able to take measure to protect myself online	0.926
PSE49_3 I have the resources and the knowledge to take necessary security measures	0.911
PSE49_4 Taking necessary security measures is very doable	0.922
PSE49_5 If I want to, I can take measures to protect myself online	0.919

POST Fear

After hearing about how important it is to update your browser, tell us how much you agree or disagree with the following statements. 7-point scale strongly disagree/ strongly agree. α= .923

	Loadings
PFR50_1 The trends in online security are worrisome to me	0.848
PFR50_2 I fear that computer security issues are beyond the control of individuals	0.818
PFR50_3 I am worried about the rapid changes in computer security issues	0.900
PFR50_4 Current online security issues make me feel afraid	0.914
PFR50_5 When I think of computer security issues, I get very scared about what might happen	0.894

POST Response Cost

After hearing about how important it is to update your browser, tell us how much you agree or disagree with the following statements. 7- point scale strongly disagree/ strongly agree, α= .923

	Loadings
PRC51_2 It is often inconvenient to take security measures	0.829
PRC51_3 Taking security measures can slow down what I need to do	0.849
PRC51_4 It is too much trouble to follow security measures	0.723
PRC51_5 Following some security measures (e.g., updating software) may cause some of my programs not to work correctly.	0.861

Table 5.14: (cont'd)

PRC51_6 It always seems like I have to do security updates at the most inconvenient time	0.917
PRC51_7 Security measures are a lot of hassle	0.917

POST Response Efficacy

After hearing about how important it is to update your browser, how do you feel about these issues?

7- point Likert scale Agree/Disagree, α= .920

	Loadings
PRE52_1 Having hard to guess passwords that are different for my different accounts will help improve my security protections	0.823
PRE52_2 Keeping my operating systems updated will help improve my security protections	0.805
PRE52_3 Keeping my Internet browser updated will help improve my security protections	0.912
PRE52_5 Keeping my software programs updated will help improve my security protections	0.907
PRE52_6 Having hard to guess passwords that are different for my different accounts will help improve my security protections	0.907

POST Fatalism

After hearing about how important it is to update your browser, how do you feel about these issues?

7-point Likert scale Agree/Disagree, α= .806

	Loadings
PFT53_1 It doesn't matter what I do, it is random chance that people get hacked.	0.844
PFT53_2 I don't worry about online safety because I don't have that much to protect	0.821
PFT53_3 Most protective actions are a waste of time, if someone wants to hack you, you are going to get hacked.	0.882

POST General Protection Motivation

Thinking of your future actions, indicate the degree to which you agree or disagree with the following statements about protecting yourself on the home computer or other device you would feel safe to use for online financial transactions.

7-point Likert scale Disagree/ Agree

Table 5.14: (cont'd)

	VIF
PPM48_1q I will upgrade my security measures to protect myself better online	3.180
PPM48_4q I will learn how to be more secure online	2.785
PPM48_5q I will only download software from firms that I trust	1.561
PPM48_6q I will update my protective software regularly	1.957
PPM48_16q I will change my weak passwords to stronger ones	2.571

POST Target Protection Motivation

Thinking of your future actions, indicate the degree to which you agree or disagree with the following statements about protecting yourself on the home computer or other device you would feel safe to use for online financial transactions.

7-point Likert scale Disagree/ Agree

	VIF
PSM48_2q I will check my browser to see if it is up to date	2.759
PSM48_8q I feel more confident that I can take a specific action to protect myself online	1.468
PSM48_9q I will continue to check my browser occasionally to make sure it is updating correctly	2.690

Appendix 5.2 Path Coefficients

Table 5:15: Path coefficients by group

	Control Condition		Experimental (Training) Condition	
	Coefficient	t-statistic	Coefficient	t-statistic
Domain Knowledge				
Domain Knowledge -> Fatalism	-0.158**	3.262	-0.273***	5.847
Domain Knowledge -> Fear	0.057	1.035	0.031	0.607
Domain Knowledge -> POST Fatalism	-0.121**	2.976	-0.046	0.977
Domain Knowledge -> POST Fear	-0.139***	3.582	-0.013**	0.327
Domain Knowledge -> POST Protection Motivation	-0.158***	4.403	-0.111**	2.850
Domain Knowledge -> POST Response Cost	-0.001	0.031	0.079*	2.044
Domain Knowledge -> POST Response Efficacy	-0.070*	2.096	-0.023	0.562
Domain Knowledge -> POST Self-efficacy	-0.044	1.165	0.014	0.345
Domain Knowledge -> Protection Habit Strength	0.140**	3.043	0.158**	3.486
Domain Knowledge -> Self-efficacy	0.178**	3.375	0.232**	4.437
Domain Knowledge -> Specific Protection Motivation	0.005	0.124	-0.080*	2.460
Domain Knowledge -> Threat Severity	0.115	1.642	0.086	1.124
Domain Knowledge -> Threat Vulnerability	-0.124*	2.334	-0.112*	2.120
Experiences with Common Threats				
Exp. With Common Threats -> Domain Knowledge	-0.313***	5.517	-0.299***	5.470
Exp. With Common Threats -> Exp. With Serious Threats	0.756	15.714	0.671***	9.249
Exp. With Common Threats -> Protection Habit Strength	0.182**	3.120	0.125*	2.589
Exp. With Common Threats -> Protective Actions	-0.016	0.255	-0.157*	2.099
Exp. With Common Threats -> Response Cost	0.499***	6.581	0.270**	3.259
Exp. With Common Threats -> Response Efficacy	-0.111	1.646	-0.181*	1.844
Exp. With Common Threats -> Self-efficacy	-0.167	1.685	-0.241*	2.199
Exp. With Common Threats -> Threat Severity	-0.241*	1.663	-0.329*	2.025
Exp. With Common Threats -> Threat Vulnerability	0.423	5.075	0.204*	1.980
Exp. With Serious Threats -> Response Cost	-0.169*	2.248	-0.010	1.184
Exp. With Serious Threats -> Response Efficacy	-0.097	1.436	-0.127	1.249
Exp. With Serious Threats -> Self-efficacy	-0.104	0.987	-0.038	0.396

Table 5:15: (cont'd)

	Control condition		Experimental (training condition	
	Coefficient	t-statistic	Coefficient	t-statistic
Exp. With Serious Threats -> Threat Severity	0.019	0.203	-0.030	0.349
Exp. With Serious Threats -> Threat Vulnerability	-0.063	0.812	0.087	0.896
Fatalism				
Fatalism -> POST Fatalism	0.790***	22.708	0.761***	19.826
Fatalism -> POST Response Cost	0.062	1.112	0.121*	2.454
Fatalism -> POST Response Efficacy	-0.003	0.051	-0.046	1.099
Fear				
Fear -> POST Fear	0.880***	37.146	0.844***	27.622
Fear -> Protective Actions	0.088	1.589	0.059	0.818
Post Message Paths				
POST Fatalism -> POST Protection Motivation	-0.031	0.487	-0.075	1.002
POST Fatalism -> Specific Protection Motivation	-0.004	0.059	-0.010	1.695
POST Fear -> POST Protection Motivation	0.152**	2.928	0.184***	3.965
POST Fear -> Specific Protection Motivation	0.075*	1.655	0.086*	2.338
POST Protection Motivation -> Specific Protection Motivation	0.493***	6.752	0.499	8.317
POST Response Cost -> POST Protection Motivation	-0.015	0.256	-0.122	1.837
POST Response Cost -> Specific Protection Motivation	-0.185***	3.302	-0.053	1.143
POST Response Efficacy -> POST Protection Motivation	0.362***	4.882	0.287**	3.489
POST Response Efficacy -> Specific Protection Motivation	0.188*	2.020	0.206**	2.524
POST Self-efficacy -> POST Fear	-0.000	0.001	-0.050	1.218
POST Self-efficacy -> POST Protection Motivation	0.245**	3.255	0.311***	4.633
POST Self-efficacy -> POST Response Cost	-0.035	0.780	-0.138***	2.295
POST Self-efficacy -> POST Response Efficacy	0.333***	5.169	0.412***	5.418
POST Self-efficacy -> Specific Protection Motivation	0.196*	2.589	0.139	1.726
Protection Habit Strength				
Protection Habit Strength -> POST Fear	0.074	1.899	-0.024	0.550
Protection Habit Strength -> POST Protection Motivation	0.079	1.490	0.0302	0.607
Protection Habit Strength -> POST Self-efficacy	0.136*	2.199	0.150*	2.250
Protection Habit Strength -> Specific Protection Motivation	-0.008	0.173	0.052	1.239

Table 5:15: (cont'd)

	Control condition		Experimental (training condition	
	Coefficient	t-statistic	Coefficient	t-statistic
Protective Actions				
Protective Actions -> Fatalism	-0.272***	4.988	-0.247***	4.835
Protective Actions -> POST Protection Motivation	0.214***	4.102	0.181**	2.972
Protective Actions -> POST Response Efficacy	0.074	1.529	0.165**	2.965
Protective Actions -> POST Self-efficacy	0.135**	2.966	0.231***	3.494
Protective Actions -> Specific Protection Motivation	-0.052	1.179	-0.044	0.876
Response Cost				
Response Cost -> POST Response Cost	0.740***	17.525	0.659***	14.456
Response Cost -> Protective Actions	-0.070	1.055	-0.091	1.368
Response Efficacy				
Response Efficacy -> POST Response Efficacy	0.512***	7.692	0.378***	6.483
Response Efficacy -> Protection Habit Strength	0.114	1.605	-0.015	0.247
Response Efficacy -> Protective Actions	0.292***	4.020	0.198**	2.921
Self-Efficacy				
Self-efficacy -> Fear	-0.124*	2.156	-0.214***	3.648
Self-efficacy -> POST Self-Efficacy	0.608***	10.476	0.392***	5.181
Self-efficacy -> Protection Habit Strength	0.535***	8.735	0.556***	11.226
Self-efficacy -> Protective Actions	0.285***	3.818	0.197**	2.992
Self-efficacy -> Response Cost	-0.297***	5.641	-0.379***	7.181
Self-efficacy -> Response Efficacy	0.539***	10.607	0.401***	6.563
Self-efficacy -> Threat Severity	0.275***	3.808	0.055	0.774
Self-efficacy -> Threat Vulnerability	-0.188**	3.380	-0.207**	2.836
Threat Severity				
Threat Severity -> Protective Actions	-0.003	0.033	0.122	1.392
Threat Vulnerability				
Threat Vulnerability -> Fear	0.332***	5.820	0.338***	6.266
Threat Vulnerability -> Protective Actions	-0.020	0.350	0.096	1.518
Time Online				
Time Online -> Domain Knowledge	0.0912	1.788	0.128*	2.507
Time Online -> Exp. With Common Threats	-0.231***	3.539	-0.065	1.044
Time Online -> Protection Habit Strength	0.041	0.948	0.020	0.362

Table 5:15: (cont'd)

	Control condition		Experimental (training condition	
	Coefficient	t-statistic	Coefficient	t-statistic
Time Online -> Self-efficacy	0.084	1.642	0.019	0.293
Time Online -> Threat Vulnerability	-0.098*	2.096	-0.059	0.989

*p< .05, **p<.01, ***p<.001

Appendix 5.3 Pre/ post correlations

Table 5:16: Pre/ post correlations compared by condition

	Fear (Control)	Fear (Training)	Fatalism (Control)	Fatalism (Training)	Self-Efficacy	Self-Efficacy (Training)	Response Efficacy	Response Efficacy (Training)	Response Cost (Control)	Response Cost (Training)	Post Fear (Control)	Post Fear (Training)
Fear	1	1										
Fatalism	.267**	.298**	1	1								
Self-Efficacy	-.215**	-.309**	-.339**	-.295**	1	1						
Response Efficacy	-0.019	-0.092	-.337**	-.256**	.541**	.429**	1	1				
Response Cost	.390**	.402**	.433**	.294**	-.384**	-.428**	-.250**	-.276**	1	1		
Post Fear	.801**	.777**	.260**	.295**	-.177**	-.310**	-0.034	-.135**	.358**	.427**	1	1
Post Fatalism	.299**	.289**	.754**	.662**	-.270**	-.256**	-.358**	-.272**	.386**	.383**	.315**	.394**
Post Self-Efficacy	-.144**	-.159**	-.315**	-.241**	.695**	.535**	.574**	.476**	-.315**	-.285**	-.116*	-.193**
Post Response Efficacy	0.019	-0.046	-.251**	-.227**	.463**	.353**	.671**	.603**	-.253**	-.179**	0.006	-.121*
Post Response Cost	.401**	.350**	.398**	.314**	-.357**	-.301**	-.301**	-.345**	.743**	.707**	.396**	.448**
General Protection Motivation	.106*	0.052	-.147**	-.145**	.375**	.238**	.461**	.403**	-.122*	-.149**	.147**	0.004
Target Protection Motivation	-0.016	0.025	-.226**	-.148**	.449**	.299**	.523**	.480**	-.263**	-.172**	0.028	-0.035

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

*. Correlation is significant at the 0.05 level (2-tailed).

Table 5:16: (cont'd)

	Post Fatalism (Control)	Post Fatalism (Training)	Post Self-Efficacy (Control)	Post Self-Efficacy (Training)	Post Response Efficacy (Control)	Post Response Efficacy (Training)	Post Response Cost (Control)	Post Response Cost (Training)	General Protection Motivation (Control)	General Protection Motivation (Training)	Target Protection Motivation Control	Target Protection Motivation Training
Fear												
Fatalism												
Self-Efficacy												
Response Efficacy												
Response Cost												
Post Fear												
Post Fatalism	1	1										
Post Self-Efficacy	-.297**	-.277**	1	1								
Post Response Efficacy	-.348**	-.277**	.630**	.651**	1	1						
Post Response Cost	.507**	.542**	-.277**	-.331**	-.308**	-.280**	1	1				
General Protection Motivation	-.205**	-.236**	.550**	.563**	.564**	.545**	-.204**	-.310**	1	1		
Target Protection Motivation	-.293**	-.285**	.613**	.598**	.643**	.594**	-.351**	-.330**	.753**	.733**	1	1

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

*. Correlation is significant at the 0.05 level (2-tailed).

Appendix 5.4: Multi-group analysis

Table 5.17: Parametric multi-group analysis for significant path differentials

	Path Coefficients-diff (Condition 1 -Condition 2.0)	t-Value diff (Condition 1 vs Condition 2.0)	p-Value diff (Condition 1 vs Condition 2.0)
Domain Knowledge -> Fatalism	0.110	1.585	0.113
Domain Knowledge -> Fear	0.029	0.422	0.673
Domain Knowledge -> Gen Protection Motivation	0.052	1.026	0.305
Domain Knowledge -> POST Fatalism	0.071	1.245	0.213
Domain Knowledge -> POST Response Cost	0.077	1.435	0.152
Domain Knowledge -> POST Response Efficacy	0.051	1.065	0.287
Domain Knowledge -> POST Self-Efficacy	0.058	1.067	0.286
Domain Knowledge -> Protection Habit Strength	0.020	0.320	0.749
Domain Knowledge -> Self-efficacy	0.052	0.720	0.472
Domain Knowledge -> Target Protection Motivation	0.075	1.608	0.108
Domain Knowledge -> Threat Severity	0.032	0.297	0.766
Domain Knowledge -> Threat Vulnerability	0.010	0.150	0.881
Exp. With Common Threats -> Domain Knowledge	0.014	0.191	0.849
Exp. With Common Threats -> Exp. With Serious Threats	0.085	1.002	0.316
Exp. With Common Threats -> Protection Habit Strength	0.052	0.707	0.480
Exp. With Common Threats -> Protective Actions	0.139	1.472	0.141
Exp. With Common Threats -> Response Cost	0.215	2.023	0.043
Exp. With Common Threats -> Response Efficacy	0.065	0.556	0.579
Exp. With Common Threats -> Self-efficacy	0.073	0.526	0.599
Exp. With Common Threats -> Threat Severity	0.085	0.380	0.704
Exp. With Common Threats -> Threat Vulnerability	0.212	1.621	0.105
Exp. With Serious Threats -> Response Cost	0.068	0.646	0.518
Exp. With Serious Threats -> Response Efficacy	0.026	0.221	0.825
Exp. With Serious Threats -> Self-efficacy	0.064	0.491	0.623
Exp. With Serious Threats -> Threat Severity	0.047	0.367	0.714
Exp. With Serious Threats -> Threat Vulnerability	0.144	1.148	0.251
Fatalism -> POST Fatalism	0.032	0.639	0.523
Fatalism -> POST Response Cost	0.031	0.445	0.657
Fear -> Fatalism	0.014	0.163	0.871
Fear -> POST Fear	0.037	1.031	0.303
Fear -> Protective Actions	0.029	0.366	0.714
Gen Protection Motivation -> Target Protection Motivation	0.007	0.083	0.934
POST Fatalism -> Gen Protection Motivation	0.028	0.378	0.705
POST Fatalism -> Target Protection Motivation	0.063	0.885	0.376
POST Fear -> Gen Protection Motivation	0.015	0.248	0.804
POST Fear -> Target Protection Motivation	0.008	0.154	0.877
POST Response Cost -> Gen Protection Motivation	0.100	1.370	0.171
POST Response Cost -> Target Protection Motivation	0.111	1.940	0.053
POST Response Efficacy -> Gen Protection Motivation	0.063	0.724	0.470

Table 5:17 (cont'd)

	Path Coefficients-diff (Condition 1 -Condition 2.0)	t-Value diff (Condition 1 vs Condition 2.0)	p-Value diff (Condition 1 vs Condition 2.0)
POST Response Efficacy -> Target Protection Motivation	0.012	0.123	0.902
POST Self-efficacy -> Gen Protection Motivation	0.057	0.663	0.507
POST Self-efficacy -> POST Fatalism	0.012	0.187	0.852
POST Self-efficacy -> POST Fear	0.075	1.588	0.113
POST Self-efficacy -> POST Response Cost	0.098	1.451	0.147
POST Self-efficacy -> POST Response Efficacy	0.061	0.694	0.488
POST Self-efficacy -> Target Protection Motivation	0.046	0.471	0.638
Protection Habit Strength -> Gen Protection Motivation	0.044	0.671	0.502
Protection Habit Strength -> POST Self-efficacy	0.003	0.037	0.970
Protection Habit Strength -> Target Protection Motivation	0.048	0.854	0.393
Protective Actions -> Fatalism	0.044	0.528	0.598
Protective Actions -> Gen Protection Motivation	0.032	0.419	0.675
Protective Actions -> POST Response Efficacy	0.083	1.196	0.232
Protective Actions -> POST Self-efficacy	0.086	1.113	0.266
Protective Actions -> Target Protection Motivation	0.014	0.214	0.831
Response Cost -> POST Response Cost	0.057	1.035	0.301
Response Cost -> Protective Actions	0.018	0.208	0.835
Response Efficacy -> POST Response Efficacy	0.093	1.256	0.209
Response Efficacy -> Protection Habit Strength	0.118	1.588	0.113
Response Efficacy -> Protective Actions	0.086	1.037	0.300
Self-efficacy -> Fatalism	0.142	1.764	0.078
Self-efficacy -> Fear	0.081	1.082	0.279
Self-efficacy -> POST Self-efficacy	0.191	2.293	0.022
Self-efficacy -> Protection Habit Strength	0.014	0.207	0.836
Self-efficacy -> Protective Actions	0.092	1.028	0.304
Self-efficacy -> Response Cost	0.077	1.130	0.259
Self-efficacy -> Response Efficacy	0.123	1.710	0.088
Self-efficacy -> Threat Severity	0.211	2.126	0.034
Self-efficacy -> Threat Vulnerability	0.017	0.209	0.834
Threat Severity -> Protective Actions	0.115	0.995	0.320
Threat Vulnerability -> Fear	0.006	0.084	0.933
Threat Vulnerability -> Protective Actions	0.109	1.317	0.188
Time Online -> Domain Knowledge	0.037	0.494	0.622
Time Online -> Exp. With Common Threats	0.166	1.879	0.061
Time Online -> Protection Habit Strength	0.024	0.363	0.717
Time Online -> Self-efficacy	0.063	0.783	0.434
Time Online -> Threat Severity	0.113	1.308	0.191
Time Online -> Threat Vulnerability	0.039	0.523	0.601

Appendix 5.5: Revised script for all conditions

SCRIPT FOR EXPERIMENT ALL CONDITIONS

Your browser is the tool that you use to access the Internet. You use it to get your email, surf websites such as Facebook, Twitter, Instagram, YouTube, news sites, banking, shopping, or anything else you do on the Internet with your computer. Your browser is your first level of protection when you go online. Your browser has built in safety features that help protect you as you read articles, watch videos, make postings, share pictures, shop, or do bank transactions.

We often have a favorite browser. We can personalize it, add bookmarks, and we feel comfortable with it. We get familiar with how web sites look when we use our favorite browser. It can be upsetting if updates change how things look, or where to find certain settings.

However, these updates are extremely important. Having an out-of-date browser is full of security risks. It can endanger **our privacy and security.** Browser updates not only help improve speed and how things work, these updates also help protect **us** from many **serious** threats.

Updates are very important. They are usually issued because a new weakness is discovered in the code that runs the browser. This weakness will impact your safety and security when using that browser. Criminals and hackers know about these weaknesses; and are often finding ways to take advantage of these weaknesses as soon as they are found.

You may think that you don't go to websites that are sketchy or dangerous. Actually, very familiar web sites often harbor malware. Some types of malware can be downloaded on your computer simply by visiting a web page, even if you don't click on anything. Sometimes the advertisements running on websites, even sites by familiar news organizations, are hijacked and download code onto your computer as you are innocently reading a news article. If a browser is out of date, it can't protect you from these threats.

Out of date browsers also might not be correctly verifying secure sites. Many browsers notify you if you are going to a web site that is a known phishing site, or even if it has indicators it is a site harboring known threats. If a browser is out of date, you probably won't receive correct messages.

Most browsers automatically update themselves when new versions are available. However, quite often browsers don't update themselves for many reasons. Security researchers have found that about 25 to 30 percent of people's browsers are not up-to-date and most of these individuals are totally unaware that they are at risk.

Be sure to check your browser and make sure it is up to date and protecting you from many known threats. Not only will an up-to-date browser protect you better, it will help you to have a better browsing experience.

END SCRIPT FOR CONTROL PARTICIPANTS

FOR FIREFOX USERS- HIGH EFFICACY CONDITION

Making sure Firefox is running the latest version is very easy, once you see how to do it, you can check it whenever you want. With Firefox on a Mac Operating System, Just open up Firefox, click on “Firefox” at the very top and a drop down menu will appear. Click on “About Firefox” and a dialog box will open. It will then check to see if your version is up-to-date.

If you have Windows, you will go to the layered bars on the right hand side and a drop down menu will appear. Click on the “help” button. Then click on “About Firefox”. The dialog box opens to check if your version is up-to-date, or if it needs to be updated.

Sometimes you will need to close Firefox and restart it to have the updates take effect.

That is all there is to it! It will keep all of your bookmarks and settings and your browser will be fixed of known weaknesses.

Just to review on how easy it is to make sure you have the latest protections, Let’s do it again.

On a Mac- go up to the upper left-hand corner and click on “Firefox” and a menu will drop down and click on “about Firefox”. The window opens up and it checks for the latest version. On the PC go to the right hand side, click on the options box, go down to “help” and then click on “about Firefox.”

Well done. Now you can easily check to see if your browser is protecting you from known threats. Your browser is your first line of defense as you use the Internet. Making sure your browser is up to date is something that **you** can **easily** do to protect yourself and enjoy better performance when you go online.

FOR CHROME USERS- HIGH EFFICACY CONDITION

Making sure Google Chrome is running the latest version is very easy, once you see how to do it, you can check it whenever you want. On either a Mac operating system or a PC, Just open up Chrome, click on the three dots at the right hand corner of the screen, at the very top, and a drop down menu will appear. Move down the drop down menu to “Help” and a sub menu will pop up.

Select “About Chrome” and a little dialog screen pops up while Chrome checks if you have the latest version. Sometimes you will need to close Chrome and restart it to have

the updates take effect. That is all there is to it! It will keep all of your bookmarks and settings and your browser will be fixed of known weaknesses.

Just to review on how easy it is to make sure you have the latest protections, Let's do it again.

On either a Mac operating system or a PC, Just open up Chrome, click on the three dots at the right hand corner of the screen, at the very top, and a drop down menu will appear. Move down the drop down menu to "Help" and a sub menu will pop up. Select "About Chrome" and a little dialog screen pops up while Chrome checks if you have the latest version.

Well done. Now you can easily check to see if your browser is protecting you from known threats. Your browser is your first line of defense as you use the Internet. Making sure your browser is up to date is something that **you** can **easily** do to protect yourself and enjoy better performance when you go online.

FOR MICROSOFT INTERNET EXPLORER HIGH EFFICACY CONDITION

Making sure Windows Explorer is running the latest version is very easy, once you see how to do it, you can check it whenever you want. If you have any version of Internet Explorer before version 11, please do not use it anymore. Microsoft is no longer issuing security updates and there are **many** known weaknesses that are widely being used by criminals and hackers. Either use Internet Explorer 11 or Microsoft Edge.

Microsoft Edge updates are incorporated with Microsoft Operating System updates. To see if your system is up to date, click on the bottom Windows icon in the lower left hand corner. This will open up a menu bar. Click on "settings" then another window will open up. In this window click on "updates and security." Then a page will appear that will let you know about available updates, and if you need to reboot your device to complete the updates.

That is all there is to it! It will keep all of your bookmarks and settings and your browser will be fixed of known weaknesses.

Just to review on how easy it is to make sure you have the latest protections, Let's do it again.

Click on the bottom Windows icon in the lower left hand corner. This will open up a menu bar. Click on "settings" then another window will open up. In this window click on "updates and security." Then a page will appear that will let you know about available updates, and if you need to reboot your device to complete the updates.

Well done. Now you can easily check to see if your browser is protecting you from known threats. Your browser is your first line of defense as you use the Internet. Making

sure your browser is up to date is something that **you** can **easily** do to protect yourself and enjoy better performance when you go online.

FOR SAFARI HIGH EFFICACY CONDITION

Making sure Safari is running the latest version is very easy, once you see how to do it, you can check it whenever you want. Apple sends out updates periodically whenever security or performance upgrades are issued. On the Mac operating system click on the apple icon in the upper left corner of your screen. A menu will drop down. Click on "About this Mac" and a screen will pop up. Click on the button titled "Software Update" and it will open up the window to the Apple app store. If it doesn't automatically open to "updates," click on the "updates" button on the top. Then you will see a list of possible software updates for your computer. If there is one available for Safari, it will appear here.

That is all there is to it! It will keep all of your bookmarks and settings and your browser will be fixed of known weaknesses.

Just to review on how easy it is to make sure you have the latest protections, Let's do it again.

Click on the apple icon in the upper left corner of your screen. A menu will drop down. Click on "About this Mac" and a screen will pop up. Click on the button titled "Software Update" and it will open up the window to the Apple app store. If it doesn't automatically open to "updates," click on the "updates" button on the top. Then you will see a list of possible software updates for your computer. If there is one available for Safari, it will appear here.

Well done! Now you can easily check to see if your browser is protecting you from known threats. Your browser is your first line of defense as you use the Internet. Making sure your browser is up to date is something that **you** can **easily** do to protect yourself and enjoy better performance when you go online.

Appendix 5.6: IRB approval for research study

MICHIGAN STATE
UNIVERSITY

EXEMPT DETERMINATION

***Flexibility Initiative* - See Special Exclusions Below**

February 20, 2018

To: Wietske Van Osch

Re: **MSU Study ID:** STUDY00000328
Principal Investigator: Wietske Van Osch
Category: Exempt 98
Exempt Determination Date: 2/20/2018

Title: Mind the Gap: Perceived self-efficacy, domain knowledge and their effects on responses to a cybersecurity compliance message (Phase 2)

This project has been determined to be exempt under the Michigan State University (MSU) Flexibility Initiative Exemption Category 98.

Exemption Category: This project has qualified for the Flexibility Initiative Exemption Category 98: Research involving benign interventions in conjunction with the collection of data from an adult subject through verbal or written responses (including data entry) or video recording if the subject prospectively agrees to the intervention and data collection and at least one of the following criteria is met:

(A) The information obtained is recorded in such a manner that human subjects cannot be identified directly or through identifiers linked to the subjects; or

(B) Any disclosure of the human subjects' responses outside the research would not reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, educational advancement, or reputation.

See Human Research Protection Program (HRPP) Manual 8-8-B, Exemption Category 98, for the full text of Exemption Category 98.

Exclusions: To continue to qualify for Exemption Category 98, the project must not include:

- ☐ Federal funding or federal training grants
- ☐ FDA regulated
- ☐ Sponsor or other contractual restrictions
- ☐ Clinical interventions (including clinical behavioral interventions)
- ☐ Prisoners as subjects
- ☐ Receipt of an NIH issued certificate of confidentiality to protect identifiable research data
- ☐ Be a project for which MSU serves as the Institutional Review Board (IRB) of record

Office of Regulatory Affairs
Human Research Protection Program

4000 Collins Road
Suite 136
Lansing, MI 48910

517-355-2180
Fax: 517-432-4503
Email: irb@msu.edu
www.hrpp.msu.edu

- Children as research subjects

If any of the above criteria become applicable to a project determined exempt under this flexibility initiative, the IRB office must be promptly notified prior to implementation of the criteria and the project must be reviewed and approved in accordance with the appropriate review level (e.g. expedited, full board).

Principal Investigator Responsibilities: The Principal Investigator assumes the responsibilities for the protection of human subjects in this project as outlined in HRPP Manual Section 8-1, Exemptions.

Continuing Review: Exempt projects do not need to be renewed.

Modifications: In general, investigators are not required to submit changes to the IRB once a research study is designated as exempt as long as those changes do not affect the exempt category or criteria for exempt determination (changing from exempt status to expedited or full review, changing exempt category) or that may substantially change the focus of the research study such as a change in hypothesis or study design. See HRPP Manual Section 8-1, Exemptions, for examples. If the project is modified to add additional sites for the research, please note that you may not begin the research at those sites until you receive the appropriate approvals/permissions from the sites.

Change in Funding: If new external funding is obtained for an active human research project that had been determined exempt, a new initial IRB submission will be required, with limited exceptions. Please see exclusions as funding changes may disqualify this project from this flexibility initiative.

Reportable Events: If issues should arise during the conduct of the research, such as unanticipated problems that may involve risks to subjects or others, or any problem that may increase the risk to the human subjects and change the category of review, notify the IRB office promptly. Any complaints from participants that may change the level of review from exempt to expedited or full review must be reported to the IRB. Please report new information through the project's workspace and contact the IRB office with any urgent events. Please visit the Human Research Protection Program (HRPP) website to obtain more information, including reporting timelines.

Personnel Changes: After determination of the exempt status, the PI is responsible for maintaining records of personnel changes and appropriate training. The PI is not required to notify the IRB of personnel changes on exempt research. However, he or she may wish to submit personnel changes to the IRB for recordkeeping purposes (e.g. communication with the Graduate School) and may submit such requests by submitting a Modification request. If there is a change in PI, the new PI must confirm acceptance of the PI Assurance form and the previous PI must submit the Supplemental Form to Change the Principal Investigator with the Modification request (http://hrpp.msu.edu/forms).

Closure: Investigators are not required to notify the IRB when the research study is complete. However, the PI can choose to notify the IRB when the project is complete and is especially recommended when the PI leaves the university.

For More Information: See HRPP Manual, including Sections 8-1, Exemptions and 8-8-B, Exemption Category 98 (available at https://hrpp.msu.edu/msu-hrpp-manual-table-contents-expanded).

Contact Information: If we can be of further assistance or if you have questions, please contact us at 517-355-2180 or via email at IRB@ora.msu.edu. Please visit hrpp.msu.edu to access the HRPP Manual, templates, etc.

Appendix 5.7: Fornell-Larker results

Table 5:18: Fornell-Larker criterion for discriminant validity

	Domain Knowledge	Exp. With Common Threats	Exp. With Serious Threats	Fatalism	Fear	Gen Protection Motivation	POST Fatalism	POST Fear	POST Response Cost	POST Response Efficacy
Domain Knowledge	1.000									
Exp. With Common Threats	-0.321									
Exp. With Serious Threats	-0.240	0.724								
Fatalism	-0.278	0.290	0.224							
Fear	-0.103	0.178	0.139	0.250	0.795					
Gen Protection Motivation	0.043	-0.180	-0.175	-0.231	0.061					
POST Fatalism	-0.302	0.346	0.276	0.796	0.291	-0.305	0.762			
POST Fear	-0.166	0.239	0.161	0.253	0.867	0.059	0.347	0.842		
POST Response Cost	-0.121	0.353	0.244	0.382	0.399	-0.286	0.602	0.446	0.821	
POST Response Efficacy	0.180	-0.369	-0.314	-0.318	-0.019	0.638	-0.425	-0.059	-0.333	0.837
POST Self-efficacy	0.216	-0.291	-0.253	-0.323	-0.164	0.603	-0.354	-0.166	-0.334	0.680
Protection Habit Strength	0.276	-0.095	-0.056	-0.319	-0.166	0.358	-0.257	-0.146	-0.307	0.278
Protective Actions	0.255	-0.269	-0.177	-0.286	-0.039	0.497	-0.321	-0.067	-0.309	0.470
Response Cost	-0.157	0.398	0.243	0.395	0.429	-0.166	0.441	0.420	0.751	-0.241
Response Efficacy	0.241	-0.367	-0.332	-0.375	-0.064	0.518	-0.415	-0.091	-0.355	0.709
Self-efficacy	0.293	-0.318	-0.259	-0.358	-0.277	0.364	-0.332	-0.252	-0.351	0.457
Target Protection Motivation	0.071	-0.261	-0.257	-0.254	0.009	0.753	-0.366	0.002	-0.368	0.654
Threat Severity	0.244	-0.381	-0.279	-0.252	-0.059	0.158	-0.342	-0.086	-0.189	0.381
Threat Vulnerability	-0.295	0.428	0.331	0.305	0.378	-0.039	0.316	0.407	0.358	-0.177
Time Online	0.160	-0.148	-0.117	-0.098	-0.095	0.041	-0.059	-0.075	-0.071	0.042

Table 5.18: (cont'd)

	POST Self-efficacy	Protection Habit Strength	Protective Actions	Response Cost	Response Efficacy	Self-efficacy	Target Protection Motivation	Threat Severity	Threat Vulnerability
Domain Knowledge									
Exp. With Common Threats									
Exp. With Serious Threats									
Fatalism									
Fear									
Gen Protection Motivation									
POST Fatalism									
POST Fear									
POST Response Cost									
POST Response Efficacy									
POST Self-efficacy	0.902								
Protection Habit Strength	0.518	0.899							
Protective Actions	0.448	0.538							
Response Cost	-0.321	-0.347	-0.247	0.749					
Response Efficacy	0.570	0.328	0.429	-0.301	0.739				
Self-efficacy	0.644	0.572	0.424	-0.430	0.545	0.863			
Target Protection Motivation	0.610	0.338	0.415	-0.234	0.542	0.387			
Threat Severity	0.212	0.036	0.242	-0.154	0.368	0.287	0.186		
Threat Vulnerability	-0.264	-0.205	-0.144	0.457	-0.249	-0.344	-0.109	-0.182	0.726
Time Online	0.087	0.100	0.074	-0.093	0.098	0.113	0.056	0.121	-0.164

WORKS CITED

WORKS CITED

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

Asyraf Afthanorhan, Nazim, A., & Ahmad, S. (2014). A Parametric Approach To Partial Least Square Structural Equation Modeling of Multigroup Analysis (PLS-MGA). International Journal of Economics, Commerce and Management United Kingdom, II(10), 1–15. http://doi.org/10.9734/BJAST/2015/14380

Bandura, A. (2006). Guide for Constucting Self-efficacy Scales. Self-efficacy Beliefs of Adolescents (pp. 307–337). Information Age Publishig.

Berinsky, A. J., Huber, G. A., & Lenz, G. S. (2012). Evaluating Online Labor Markets for Experimental Research: Amazon.com's Mechanical Turk. Political Analysis, 20(3), 351–368. http://doi.org/10.1093/pan/mpr057

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do Systems Users Have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors. MIS Quarterly, 39(4), 837–864.

Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk: A New Source of Inexpensive, Yet High-Quality, Data? Perspectives on Psychological Science, 6(1), 3–5. http://doi.org/10.1177/1745691610393980

Cangur, S., & Ercan, I. (2015). Comparison of Model Fit Indices Used in Structural Equation Modeling Under Multivariate Normality. Journal of Modern Applied Statistical Methods, 14(1), 152–167. http://doi.org/10.22237/jmasm/1430453580

Casler, K., Bickel, L., & Hackett, E. (2013). Separate But Equal? A Comparison of Participants and Data Gathered Via Amazon's MTurk, Social Media, and Face-to-Face Behavioral Testing. Computers in Human Behavior, 29(6), 2156–2160. http://doi.org/10.1016/j.chb.2013.05.009

Chandler, D., & Kapelner, A. (2013). Breaking Monotony with Meaning: Motivation in Crowdsourcing Markets. Journal of Economic Behavior & Organization, 90, 123–

133. http://doi.org/10.1016/j.jebo.2013.03.003

Dijkstra, T. K., & Henseler, J. (2015). Consistent Partial Least Squares Path Modeling. MIS Quarterly, 39(2), 297–316. Retrieved from http://heim.ifi.uio.no/~petterog/Kurs/INF5220/NatureofTheoryMISQ.pdf

Ewoldsen, D. R., Rhodes, N., & Fazio, R. H. (2015). The MODE Model and Its Implications for Studying the Media. Media Psychology, 18(3), 312–337. http://doi.org/10.1080/15213269.2014.937440

Fazio, R. H., & Towles-Schwen, T. (1999). The MODE Model of Attitude-Behavior Processes. In S. Chaiken & Trope (Eds.), Dual-Process Theories in Social Psychology (pp. 97–115). Guilford Press.

Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. American Marketing Association, 18(1), 39–50.

Furnell, S. (2005). Why Users Cannot Use Security. Computers & Security, 24(4), 274–279. http://doi.org/10.1016/j.cose.2005.04.003

Hasan, B. (2003). The Influence of Specific Computer Experiences on Computer Self-efficacy Beliefs. Computers in Human Behavior, 19(4), 443–450. http://doi.org/10.1016/S0747-5632(02)00079-1

Hayduk, L., Cummings, G., Boadu, K., Pazderka-Robinson, H., & Boulianne, S. (2007). Testing! testing! One, Two, Three – Testing the Theory in Structural Equation Models! Personality and Individual Differences, 42(5), 841–850. http://doi.org/10.1016/j.paid.2006.10.001

Hayes, A. F., Glynn, C. J., & Huge, M. E. (2012). Cautions Regarding the Interpretation of Regression Coefficients and Hypothesis Tests in Linear Models with Interactions. Communication Methods and Measures, 6(1), 1–11. http://doi.org/10.1080/19312458.2012.651415

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling. Journal of the Academy of Marketing Science, 43(1), 115–135. http://doi.org/10.1007/s11747-014-0403-8

Huang, H. (2016). On the Welch-Satterthwaite Formula for Uncertainty Estimation: A Paradox and its Resolution. Cal Lab the International Journal of Metrology, 23(4), 20–28.

Icek Ajzen. (2002). Perceived Behavioral Control, Self-efficacy, Locus of Control, and the Theory of Planned Behavior. Journal of Applied Social Psychology, 80(6), 2918–2940. http://doi.org/10.1111/j.1559-1816.2002.tb00236.x

Li, L., He, W., Xu, L., Ivan, A., Anwar, M., & Yuan, X. (2014). Does Explicit Information Security Policy Affect Employees' Cyber Security Behavior? A Pilot Study. 2014 Enterprise Systems Conference, 169–173. http://doi.org/10.1109/ES.2014.66

Li, Y. W. (2016a). Transforming Conventional Teaching Classroom to Learner-Centred Teaching Classroom Using Multimedia-Mediated Learning Module. International Journal of Information and Education Technology, 6(2), 105–112. http://doi.org/10.7763/IJIET.2016.V6.667

Li, Y. W. (2016b). Transforming Conventional Teaching Classroom to Learner-Centred Teaching Classroom Using Multimedia-Mediated Learning Module. International Journal of Information and Education Technology, 6(2), 105–112. http://doi.org/10.7763/IJIET.2016.V6.667

Liao, D., & Valliant, R. (2012). Variance Inflation Factors in the Analysis of Complex Survey Data. Survey Methodology, 38(1), 53–62.

Mannan, M., & Van Oorschot, P. C. (2007). Security and Usability: The Gap in Real-World Online Banking. IEEE Technology and Society Magazine, 26, 1–14. http://doi.org/10.1109/MTAS.2007.335568

Miller, T. A. (2016). Health Literacy and Adherence to Medical Treatment in Chronic and Acute Illness: A Meta-Analysis. Patient Education and Counseling, 99(7), 1079–1086. http://doi.org/10.1016/j.pec.2016.01.020

Nabi, R. L., Roskos-Ewoldsen, D., & Carpentier, F. D. (2008). Subjective Knowledge and Fear Appeal Effectiveness: Implications for Message Design. Health Communication, 23, 191–201. http://doi.org/10.1080/10410230701808327

O'Brien, R. M. (2007). A Caution Regarding Rules of Thumb for Variance Inflation Factors. Quality & Quantity, 41(5), 673–690. http://doi.org/10.1007/s11135-006-9018-6

Olmstead, K., & Smith, A. (2017). What the Public Knows about Cybersecurity. Washington, D.C. Retrieved from http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' Behavior Towards IS Security Policy Compliance. Proceedings of the Annual Hawaii International Conference on System Sciences, 1–10. http://doi.org/10.1109/HICSS.2007.206

Redmiles, E. M., Kross, S., Pradhan, A., & Mazurek, M. L. (2017). How Well Do My Results Generalize ? Comparing Security and Privacy Survey Results from MTurk and Web Panels to the U . S . Retrieved from https://drum.lib.umd.edu/bitstream/handle/1903/19164/CS-TR-5054.pdf

Reeder, R., Ion, I., & Consolvo, S. (2017). 152 Simple Steps to Stay Safe Online: Security Advice for Non-tech-savvy Users. IEEE Security & Privacy, (99), 1–15. http://doi.org/10.1109/MSP.2017.265093101

Ringle, C. M., Wende, S., & Becker, J.M. (2015). SmartPLS 3.0. Retrieved from http://www.smartpls.com

Shillair, R., & Dutton, W. H. (2016). Instilling a Security Mindset: Getting Into the Cat and Mouse Game. SSRN Electronic Journal. http://doi.org/10.2139/ssrn.2756736

Shillair, R., LaRose, R., Jiang, M., Rifon, N. J., & Cotten, S. R. (2017). The Role of Habits and Prior Experience in Motivating User Cybersecurity Behavior. In International Communication Association (p. 30). San Diego, California.

Tsai, H.-Y. S., Shillair, R., & Cotten, S. R. (2017). Social Support and Playing Around: An Examination of How Older Adults Acquire Digital Literacy with Tablet Computers. Journal of Applied Gerontology, 36(1). http://doi.org/10.1177/0733464815609440

Tsai, H.-Y. S., Shillair, R., Cotten, S. R., Winstead, V., & Yost, E. (2015). Getting Grandma Online: Are Tablets the Answer for Increasing Digital Inclusion for Older Adults in the U.S.? Educational Gerontology, 41(10). http://doi.org/10.1080/03601277.2015.1048165

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49(3–4), 190–198. http://doi.org/10.1016/j.im.2012.04.002

Wash, R., Rader, E., & Fennell, C. (2017). Can People Self-Report Security Accurately? Agreement Between Self-Report and Behavioral Measures. In CHI 2017 (pp. 2228–2232). Denver.

Witte, K. (1994). Fear Control and Danger Control: A Test of the Extended Parallel Process Model (EPPM). Communication Monographs. http://doi.org/10.1080/03637759409376328

Witte, K., & Allen, M. (2000). A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns. Health Education & Behavior, 27(5), 591–615. http://doi.org/10.1177/109019810002700506

Yeo, G. B., & Neal, A. (2006). An Examination of the Dynamic Relationship Between Self-efficacy and Performance Across Levels of Analysis and Levels of Specificity. Journal of Applied Psychology, 91(5), 1088–1101. http://doi.org/10.1037/0021-9010.91.5.1088

Yi, M. Y., & Im, K. S. (2004). Predicting Computer Task Performance. Journal of Organizational and End User Computing, 16(2), 20–37. http://doi.org/10.4018/joeuc.2004040102

Zipf, G. K. (1949). Human Behavior and the Principle of Least Effort. Addison-Wesley Press.

Chapter 6
Examining the impact of domain knowledge

6.1 Introduction

The impacts of secure or insecure computer systems are felt by all of us every time we pick up a cell phone, go online, make a transaction, or use a smart device. If our computers are compromised, we may experience a range of complications, even to the point of having our data stolen by criminal networks. Despite the salience of cybersecurity issues, only a small percentage of the population can claim to have fairly deep understanding of cyber threats and protections. Complicating the issue is the fact that the cybersecurity domain is very complex by nature and is changing rapidly. Thus, to expect non-professional users to have a robust knowledge of cyber issues is unreasonable. However, there are many basic things that non-expert individuals can do to protect themselves, sometimes referred to as digital hygiene issues (Gelbstein, 2014; Shillair & Meng, 2017). These include issues such as having strong and unique passwords, keeping protective software enabled and updated, and avoiding obvious phishing links. Thus, many stakeholders have tried promoting cybersecurity awareness campaigns with mixed results (Albrechtsen, 2007; Bada & Sasse, 2014). Depending on one's educational background or technological training, these digital hygiene issues may be challenging or extremely simple.

Up to now, little was known how domain knowledge might impact how individuals respond to a cybersecurity message. There has been a great deal of research into how individuals respond to messages in other domains such as health (K. Witte & Allen, 2000), and politics (Donsbach, 1991; Margetts, John, Escher, & Reissfelder, 2011), but not the cybersecurity domain. Given the widespread adoption of many technologies, it is important to have a better understanding of how individuals, with their diverse set of

backgrounds and training, would respond to a cybersecurity compliance message. As discussed in Chapter 2, those with lower levels of domain knowledge might not understand terminology and a message may only serve to trigger fear, leading to a maladaptive response, such as ignoring the message (Witte, 1994). On the other hand, those with in-depth knowledge about the extent and power of advanced persistent threats (such as those run by state level actors), may find the same message overly simplistic and feel that typical protections are futile (Singer & Friedman, 2014). Thus, in this chapter we perform a deeper level of analysis on domain knowledge and how it may impact fear, fatalism, self-efficacy, response cost, response efficacy and protection motivation.

To examine the data and look for evidence of these impacts we will first review some of the results from the PLS analysis of the full model, including the influence of domain knowledge on the participants in both the control and the experimental (training) condition. Then I will use conditional PROCESS analysis to examine the impact(s) of different levels of a construct. Since domain knowledge may not have a linear impact (e.g., the higher x is, the higher y is) on protection motivation, it would explain why linear regression-based methods, such as PLS, might not show as robust an impact as expected.

6.1.1 Data indicates the need to look deeper at domain knowledge

As part of the SmartPLS run reported in the previous chapter, I analyzed paths from domain knowledge to the post-exposure constructs of fatalism, fear, self-efficacy and their path values to the target protection motivation and general protection motivation. The results are in Table 5.1.

Table 6.1: Impact of domain knowledge on post message constructs

Hypothesis	Condition	Path Name	Coefficient	t-statistic	Predicted relationship	Hypothesis supported?
H1e	Control	Domain Knowledge -> POST Fear	-0.139***	3.582	negative	yes
	Training		-0.013	0.327		yes, ns
H1f	Control	Domain Knowledge -> POST Self-efficacy	-0.044	1.165	negative	yes, ns
	Training		0.014	0.345		no, ns
H1g	Control	Domain Knowledge -> POST Response Cost	-0.001	0.031	negative	yes, ns
	Training		0.079*	2.044		no
H1h	Control	Domain Knowledge -> POST Response Efficacy	-0.070*	2.096	positive	no
	Training		-0.023	0.562		no, ns
H1i	Control	Domain Knowledge -> General Protection Motivation	-0.158***	4.403	positive	no
	Training		-0.111**	2.850		no
H1j	Control	Domain Knowledge -> POST Fatalism	-0.121**	2.976	negative	yes
	Training		-0.047	0.977		yes, ns
H1k	Control	Domain Knowledge -> Target Protection Motivation	0.005	0.124	positive	yes, ns
	Training		-0.080*	2.460		no

*p<.05, **p<.01, ***p<.001

The results of the analysis supported only some of the hypotheses. Domain knowledge did act in reducing fear after the message in control condition (beta -0.139, p<.001) and reducing fatalism (beta= -0.121, p<.001). This would indicate that as hypothesized, based on literature primarily in the health domain, increased knowledge also decreased fear and fatalism. This balance paved the way for more cognitive-based choices to protect oneself (Nabi, Roskos-Ewoldsen, & Carpentier, 2008; Witte, 1994).

However, many of the domain knowledge impacts didn't fit the results found in other domains. In the training condition, where it was thought that the training would trigger an increase in the impact of domain knowledge, it actually was not significant for both fear (beta= -0.013, ns) and fatalism (beta= -0.047, ns). Also, those with higher domain knowledge also felt response cost was higher in the training condition (beta= 0.079, p<.05). This might indicate, for example, that the training video reminded those with higher domain knowledge that it was hard to implement cyber safety procedures. Also, higher domain knowledge led to lower response efficacy in the control condition (beta-0.070, p<.05). Most concerning, increased domain knowledge led to lower general protection motivation in both the control condition (beta= -0.158, p<.001) and the training condition (beta= -0.111, p<.001). If we were looking at only the dimension of domain knowledge, it might lead to the false conclusion that learning more about cybersecurity will not motivate individuals towards protecting themselves.

However, looking at the larger PMT model it becomes apparent that domain knowledge is crucial for important issues such as self-efficacy (beta= 0.207, p<.001) for all participants. Domain knowledge also can support true self-efficacy as discussed in Chapter 5 which would lead to the ability to enact protections. Thus, to understand the

impact of domain knowledge in cybersecurity, looking for potential interactions, indirect effects and conditional impacts is in order.

As many of the hypotheses concerning domain knowledge failed, and as these are based on current literature, this shows that domain knowledge in cybersecurity is theoretically underdeveloped. Looking more deeply at the data in ways that help visualize the impact of domain knowledge at different levels may give clues to what is happening as people are exposed to a cybersecurity safety message.

In order to test and find and gain a deeper understanding of the data I will use a method called PROCESS that allows examination for moderation and conditional impacts (Hayes, 2018). Conditional impacts are visualized where a construct, in this case domain knowledge, has a differing impact at different levels. At lower levels the lack of domain knowledge may increase fear and fatalism (leading to lower protection motivation) and as domain knowledge increases, fear and fatalism decrease. However, it is possible that as domain knowledge reaches a higher point, individuals become aware that all basic protections have weaknesses. Thus, other factors come in to play and protection motivation goes down. Conditional moderation analysis will allow for better exploration of the data to help answer the overall research questions.

6.2 Method

To do the conditional analysis I used the data set described in Chapter 5 and SPSS v25 with the Hayes PROCESS v.3 plug in. Settings were for a confidence interval of 95% and 10,000 bootstraps. I ran several regressions to demonstrate how this research model builds on previous assumptions and increases our understanding of the impact(s) of self-

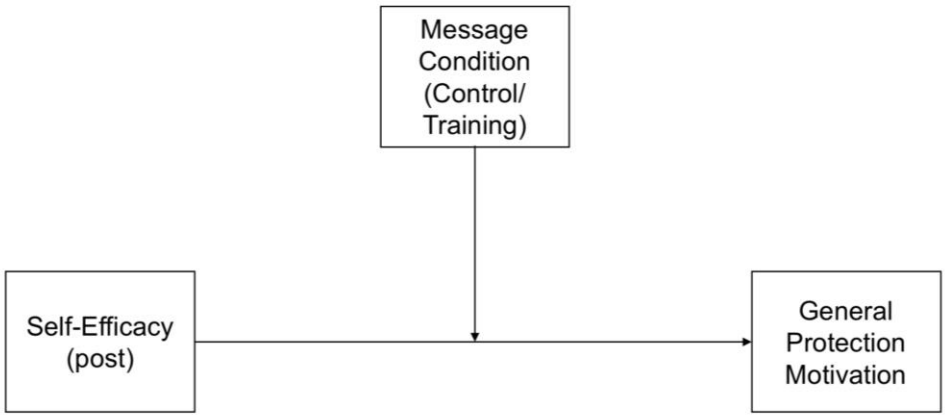
efficacy and domain knowledge, and how the message helped trigger a possible awareness of the gap between them, impacting protection motivation.

6.3 Results

6.3.1 Self-efficacy, message condition and general protection motivation

Starting with a simple analysis of just looking at the impact of self-efficacy on general protection motivation, with the message condition as a modifier (see Figure 6.1) brings results that are echoed in other domains such as health communications research (e.g., Schwarzer & Renner, 2000).

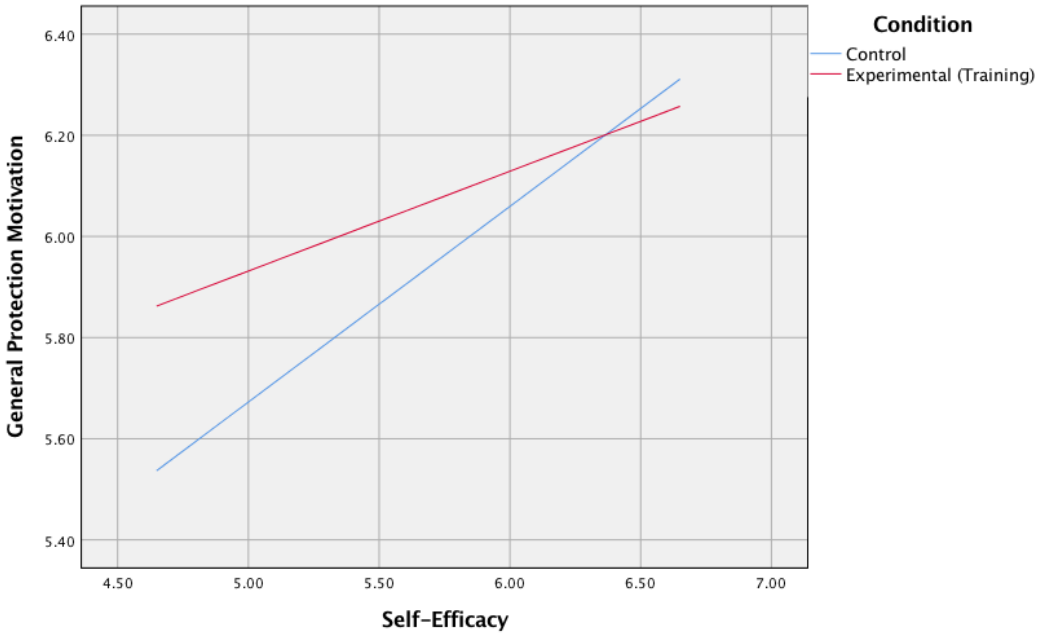
Figure 6.1: The message as a modifier



The effect of the message condition on general protection motivation was significant (B= 1.207, SE=.32, p<.001), indicating that the those in the training condition were more motivated to enact security protections. Self-efficacy also had a significant impact (B= 0.507, SE= .091, p<.001), indicating that as self-efficacy increased, protection motivation intentions also increased. There was a small but significant negative interaction between self-efficacy and the message condition (B= -0.190, SE=.06, t= -3.374, p<.001) indicating that as the levels of self-efficacy increased the impact of the experimental message decreased (see Figure 6.2). This analysis

explained over 13% of the variance (R^2= .13, F (3, 775) 39.69, p<.001) for general protection motivation. These findings are echoed in numerous fields (e.g., health, risk, learning) and show the importance of self-efficacy and how motivation can be increased by clear instruction.

Figure 6.2: Analysis of self-efficacy and message condition



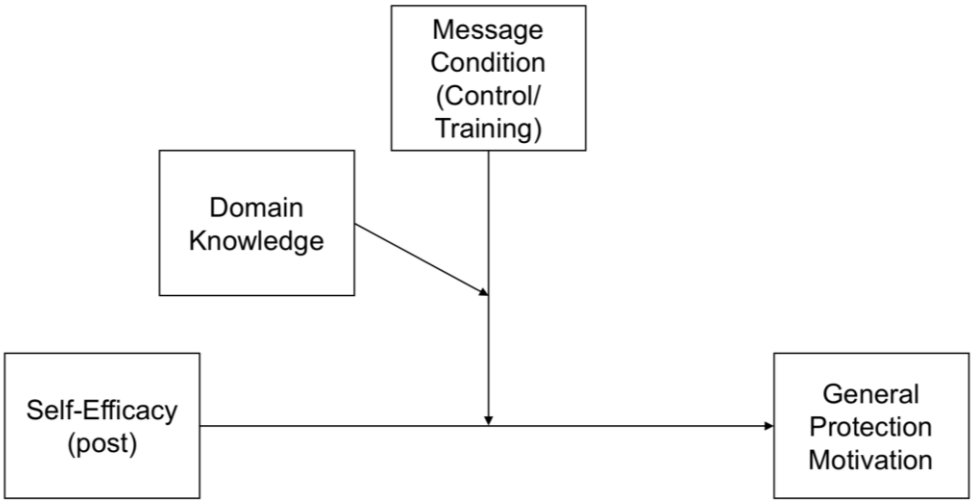
However, as we saw in the path analysis in Chapter 5, other dimensions are negatively impacting protection motivation, which makes understanding response to a message more complex.

6.3.2 Self-efficacy, domain efficacy, message condition and general protection motivation

When we add the dimension of domain knowledge the explanatory factor of the model increases to 36.7% (R^2 = .37, F(7, 774) 63.97, p<.001) for general protection motivation. The message has an increased impact in this model (B = 3.084, SE= .98, p<.001), and self-efficacy (post) is also strong in determining general protection

motivation (B = 1.299, SE= .98, p<.001). Domain knowledge by itself is not a significant factor (B = .330, SE= .21, ns). There are three significant interactions, self-efficacy (post) and the message condition (B = -.515, SE= .02, p<.05), message condition and domain knowledge (B = -.273, SE= .13, p<.05), and self-efficacy (post), message condition and domain knowledge (B = .0477, SE =.02, p<.05). This shows that domain knowledge does interact with self-efficacy as individuals were shown the message, rather than working together to increase protection motivation, they actually interact in a way that at some points decreases motivation, as explained below. An illustration of the analysis is in Figure 6.3

Figure 6.3: The message and domain knowledge as a modifier for general protection motivation



An examination of the interaction at different levels of domain knowledge helps give more insight. The impact of the interaction between the message condition and domain knowledge weakens as domain knowledge increases. At one standard deviation below the mean (5.19) the lack of knowledge has a negative impact (B= -.267, F(1,714) 14.1344, p<.001). For those with an average level of domain knowledge (7.69), it still has a fairly negative impact (B = -.148, F (1, 774) 6.6979) and at the highest levels of

domain knowledge (10.18) there was no longer a significant negative impact (B = -.029, F(1,774), ns). The conditional effects of the moderators working together (domain knowledge and message condition) are shown in Table 6.2.

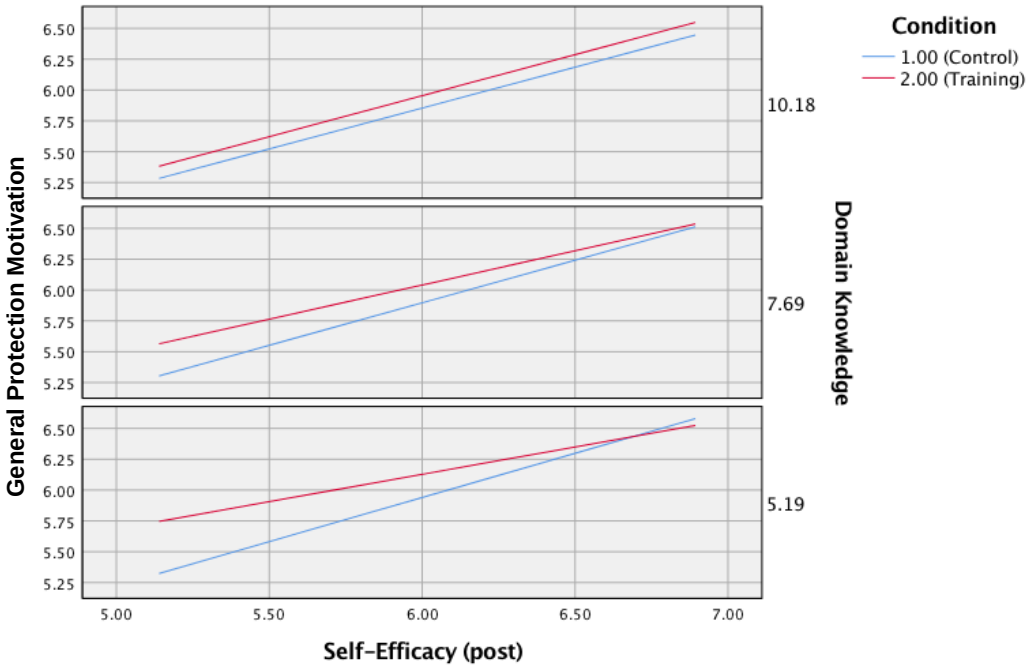
Table 6.2: Conditional effects on general protection motivation by the moderators

Condition	Domain Knowledge	Effect	SE	t-statistic
Control	5.19 (1 SD low)	.6991***	.05	13.936
Control	7.69 (mean)	.6582***	.04	15.481
Control	10.18 (1 SD high)	.6172***	.06	9.861
Training	5.19 (1 SD low)	.4323***	.05	8.615
Training	7.69 (mean)	.5104***	.04	13.402
Training	10.18 (1 SD high)	.5886***	.06	10.386

***p<.001

It is expected that a training condition would raise protection motivation by showing individuals what to do. Indeed, this is what happened for individuals with higher levels of domain knowledge to begin with. However, this was not true across all levels of domain knowledge. For lower levels of domain knowledge and lower levels of self-efficacy the training message had a positive impact, but as self-efficacy was higher (even though actual domain knowledge was low) the training condition had a negative impact. This might be pointing towards the SEM finding in chapter 5 that individuals have an inflated sense of self-efficacy in security practices. The conditional analysis helps us to see the negative impact of lower domain knowledge is even more pronounced at lower levels. Figure 6.4 illustrates the analysis.

Figure 6.4: Analysis of self-efficacy, domain knowledge and general protection motivation by domain knowledge level

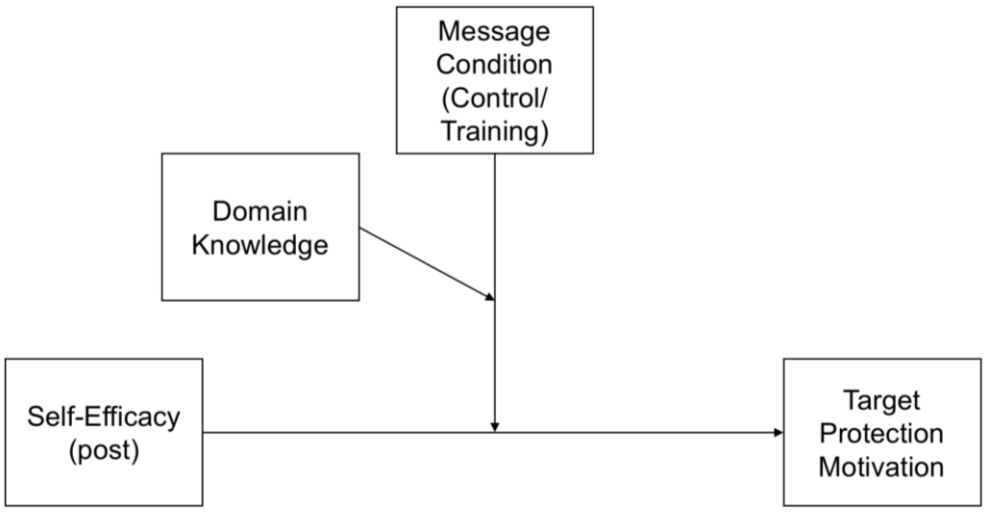


6.3.3 Self-efficacy, domain efficacy, message condition and target protection motivation

Examining the domain knowledge interaction with the target protection actions as our direct variable also gives insight into the path analysis of Chapter 5. This is illustrated in Figure 6.5. The conditional analysis looking at target protection motivation explains 38.6% of the variance (R^2= .39, F (7, 778) 69.97, p <.001) for the target protection motivation. The message condition in this analysis was even more influential on the outcome (B = 3.635, SE= 1.00, p<.001). Self-efficacy was also important (B = 1.333, SE .26, p<.001). Domain knowledge is still not significant by itself (B= .395, SE= .21, p=.06). but it is slightly stronger when looking at target protection motivation items (B= .395, t=1.881, p=.06) than when looking at general protection motivation (B=.330, t=1.608, p=.10).

Looking at the interactions in this analysis, again there are three significant interactions: self-efficacy (post) and the message condition (B = -.559, SE= .17, p<.001); message condition and domain knowledge (B = -.348, SE= .13, p<.01); and self-efficacy (post), message condition and domain knowledge (B = .055, SE =.02, p<.05). The interaction between the message condition (1= control, 2=training) is fairly strong and in an opposite direction. This means that the training condition, which has a higher numerical value) interacted with self-efficacy by lowering it, which is what was shown in the path analysis. Also, as self-efficacy increased there was an increase in target protection motivation.

Figure 6.5: The message and domain knowledge as a modifier for target protection motivation



When looking at the conditional interactions between self-efficacy and message condition at different levels of domain knowledge, the interaction weakens as domain knowledge increases. At one standard deviation below the mean (5.19), low domain knowledge and low self-efficacy has a negative impact (B= -.273, F(1,778) 14.217, p<.001) on the target protection motivation. For those with an average level of domain

knowledge (7.69), the combination of low self-efficacy still has a fairly negative impact (B = -.135, F (1, 778) 5.394, p< .05). The training condition helped negate the impact of low domain knowledge, but not as strongly as those with lower domain knowledge. For those with the highest levels of domain knowledge there was no longer a significant negative impact on self-efficacy (B = -.002, F(1,778), ns). This would indicate that the training condition presentation to those with higher domain knowledge didn't change their motivation. There were other conditional impacts that are shown in Table 6.2.

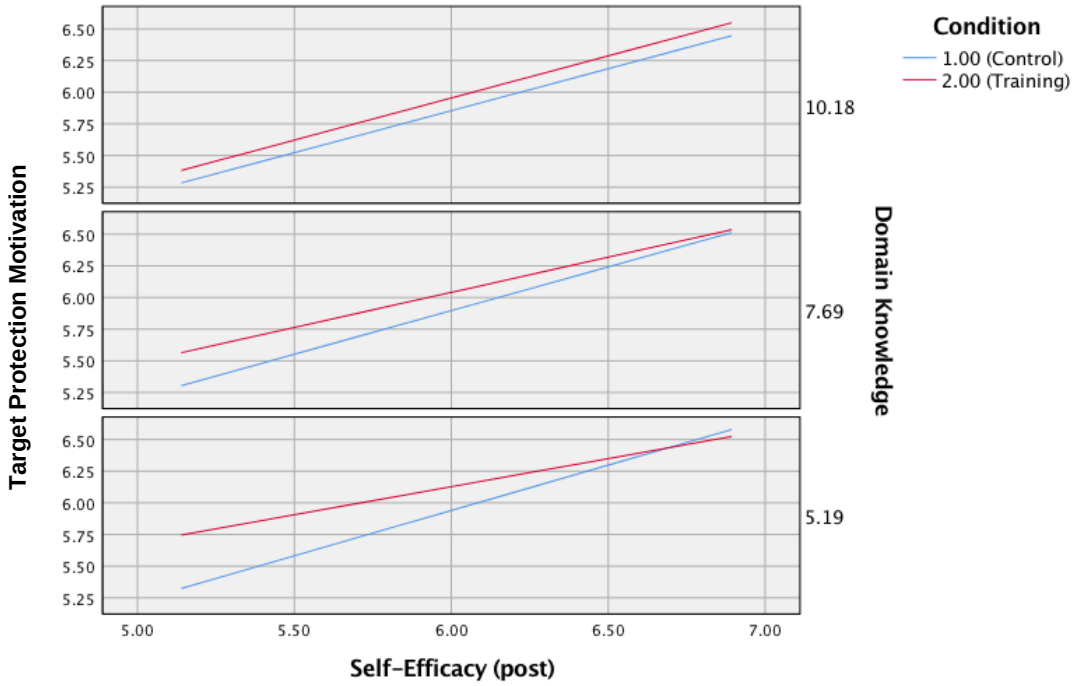
Table 6.3: Conditional effects on target protection motivation by the moderators

Condition	Domain Knowledge	Effect	SE	t-statistic
Control	5.19 (1 SD low)	.7162***	.05	13.909
Control	7.69 (mean)	.6897***	.04	15.843
Control	10.18 (1 SD high)	.6631***	.06	10.362
Training	5.19 (1 SD low)	.4433***	.05	8.711
Training	7.69 (mean)	.5543***	.04	14.285
Training	10.18 (1 SD high)	.6652***	.06	11.479

***p<.001

The training message has a significant impact on increasing target protection motivation for those with lower self-efficacy, but this impact weakens as self-efficacy increases. There is a point for those with very high self-efficacy and low domain knowledge that the training actually has an impact of lowering protection motivation. but it has little impact on those with high self-efficacy. For those with the average level of domain knowledge there was no lowering of target protection motivation. The training condition helped improve motivation and there was no interaction. For those with the highest level of domain knowledge, the impact of the message was uniform across self-efficacy levels. It was slightly higher than in the control condition and there was now interaction. This is illustrated in Figure 6.6.

Figure 6.6: Analysis of self-efficacy, domain knowledge and target protection motivation by domain knowledge level



6.4 Discussion

The conditional analysis helped bring insight into how domain knowledge interacted with the message condition and moderated self-efficacy's impact on protection motivation. By looking at the different levels of domain knowledge we were able to see that the impact of knowing or not knowing the basics of how threats and protections work had a profound impact on individuals' reaction to a cybersecurity message. Those who had the lowest levels of domain knowledge as well as the lowest levels of self-efficacy had the lowest levels of protection motivation. These individuals are probably at the highest risk of being attacked online as they don't know how to protect themselves, yet at the same time they indicate lower levels of planning to learn more or take basic protective actions (e.g., have stronger passwords). However, this research shows there is hope in using a clear and actionable message to reach this population, as the training condition

had the most impact in helping individuals with these characteristics and improved their protection motivation. The message helped move their motivation to be equivalent with those who higher levels of domain knowledge. This research also helps bring insight into the frequent resistance to cybersecurity compliance efforts. Individuals with high self-efficacy and low domain knowledge (those who were very confident of themselves, but really didn't know a lot) had lower protection intentions in the training condition than in the control condition. This would indicate that the message didn't inspire these individuals towards better security practices. It might be, that the message makes them aware of their lack of knowledge. They may reject the message or be frustrated as they try to enact protections and find these are difficult to carry out. The rejection of the message is an attempt to simply continue to participate online. This is similar to how some individuals react to the news of a serious disease, such as cancer. Some people, when hearing a diagnosis of cancer will seek to learn more, cooperate fully with their health care providers and aggressively deal with the issue. Others, in seeking to normalize their lives, ignore a diagnosis and do as little as possible (Germeni & Schulz, 2014). This desire to participate online fully, without making major changes in behaviors, may be at the root of the resistance to improving digital hygiene.

The control message, that alerted individuals to a danger without showing them what to do, resulted in lower motivation than the training message. The control message was fairly typical of what an individual might see at work or at school. It alerted them to the issue and told them clearly what to do- but did not demonstrate how to do it. Only those with higher self-efficacy and higher domain knowledge were more motivated to follow through.

The gap between what people know (i.e., domain knowledge) and what people think they know (i.e., self-efficacy) appears to be a serious issue and why cyber security compliance efforts are so challenging. We use computers for many functions throughout the day and the familiarity builds a sense of self-efficacy and security. At the same time, many individuals do not know how to enact basic protections (e.g., using two-factor identification) or how threats work (e.g., why a free public wifi spot might be dangerous). Examining the interactions of domain knowledge, self-efficacy, message condition and protection motivation showed that cybersecurity has some unique dimensions that are not seen in other domains. The combination of ubiquity and usability may be giving users a false sense of security as domain knowledge is not requited to use most technology. In the next chapter we will discuss what the findings of this research indicates could be done to help improve end user response to messages. In the next chapter I will discuss further the findings and implications of this research.

WORKS CITED

WORKS CITED

Albrechtsen, E. (2007). A Qualitative Study of Users' View on Information Security. Computers and Security, 26(4), 276–289. http://doi.org/10.1016/j.cose.2006.11.004

Bada, M., & Sasse, A. (2014). Cyber Security Awareness Campaigns Why Do They Fail to Change Behaviour? Global Cyber Security Capacity Centre, (July). Retrieved from https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Awareness CampaignsDraftWorkingPaper.pdf

Donsbach, W. (1991). Exposure to Political Content in Newspapers: The Impact of Cognitive Dissonance on Readers' Selectivity. European Journal of Communication, 6(2), 155–186. http://doi.org/10.1177/0267323191006002003

Gelbstein, E. (2014). Imperfect Technologies and Digital Hygiene Staying Secure in Cyberspace. ISACAJournal, 5. Retrieved from https://www.isaca.org/Journal/archives/2014/Volume-5/Documents/Imperfect-Technologies-and-Digital-Hygiene_joa_Eng_0914.pdf

Germeni, E., & Schulz, P. J. (2014). Information Seeking and Avoidance Throughout the Cancer Patient Journey: Two Sides of the Same Coin? A Synthesis of Qualitative Studies. Psycho-Oncology, 23(12), 1373–1381. http://doi.org/10.1002/pon.3575

Hayes, A. F. (2018). Introduction to Mediation, Moderation, and Conditional Analysis (2nd ed.). New York, New York, USA: Guilford Press.

Margetts, H., John, P., Escher, T., & Reissfelder, S. (2011). Social Information and Political Participation on the Internet: an Experiment. European Political Science Review, 3(03), 321–344. http://doi.org/10.1017/S1755773911000129

Nabi, R. L., Roskos-Ewoldsen, D., & Carpentier, F. D. (2008). Subjective Knowledge and Fear Appeal Effectiveness: Implications for Message Design. Health Communication, 23, 191–201. http://doi.org/10.1080/10410230701808327

Schwarzer, R., & Renner, B. (2000). Social-Cognitive Predictors of Health Behavior: Action Self-efficacy and Coping Self-efficacy. Health Psychology, 19(5), 487.

Shillair, R., & Meng, J. (2017). Multiple Sources for Security : The Influence of Source Networks on Coping Self- Efficacy and Protection Behavior Habits in Online Safety. In Information Security and Privacy: Proceedings of the 50th Annual Hawaii International Conference (p. 10).

Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What everyone Needs to Know. New York, New York, USA: Oxford University Press. http://doi.org/10.1016/S1353-4858(14)70039-X

Witte, K. (1994). Fear Control and Danger Control: A Test of the Extended Parallel Process Model (EPPM). Communication Monographs. http://doi.org/10.1080/03637759409376328

Witte, K., & Allen, M. (2000). A Meta-Analysis of Fear Appeals: Implications for Effective Public Health Campaigns. Health Education & Behavior, 27(5), 591–615. http://doi.org/10.1177/109019810002700506

Chapter 7
Discussion

7.1 Introduction

This research has both theoretical and practical value. First of all, it validates the use of PMT for understanding human behavior in cybersecurity. It also adds specificity and improves understanding of human beliefs and attitudes in this domain. Secondly, it offers practical insights into the development and use of cybersecurity compliance initiatives. Additionally, the multi-method approach demonstrates both qualitatively and empirically the results of the gap between self-efficacy and domain knowledge and how it results in a loss of motivation when faced with enacting protections. This gap also points to the issue of usability in cybersecurity actions—when we have individuals who are eager and willing to protect themselves–losing initiative when seeing the steps they have to perform.

This research took many different steps as we probed for a richer understanding of the threat and coping appraisal process that individuals face when deciding how to deal with cyber threats. There were gaps between perceived self-efficacy and actual domain knowledge and these appear to deeply impact overall attitudes and intentions to protect. When exposed to a cybersecurity compliance message, self-efficacy was deeply impacted, especially when presented with a clear and actionable security task. This would indicate the importance for stakeholders to “mind the gap” when trying to improve user practices. The gap can be substantial and can have dangerous outcomes. In this chapter we will briefly review what this research found and what it means to stakeholders.

7.1.1 Review of previous research

In Chapter 2 I discussed the results of my literature review. I found the study of response to cybersecurity communications is fairly undeveloped; especially when

compared with other domains of risk communications such as health communications. Thus, many cybersecurity researchers have borrowed theoretical frameworks from the health domain such as protection motivation theory (PMT) to understand responses to threats (Crossler & Belanger, 2014; Hanus & Wu, 2015; Shillair et al., 2015; Vance, Siponen, & Pahnila, 2012; Woon, Tan, & Low, 2005). PMT posits that individuals go through a threat evaluation process when facing a threat and also a coping evaluation process (Maddux & Rogers, 1983). Another key determiner for carrying out a protective action is self-efficacy (Bandura, 1989; Ajzen, 2002). Witte (1994), enriched our understanding of PMT by looking at how certain emotions, such as fear, might bypass the cognitive evaluation of a threat and cause an emotional reaction resulting in a maladaptive response. Her model, the extended parallel processing model (EPPM), helped explain why individuals often make seemingly irrational choices when faced with a threat. Fazio's (1990) MODE model explored how attitudes impacted behavior, especially when faced with time pressures to evaluate a threat. Previous experiences with a threat also impacted future responses in the health domain, extending PMT with the ordered protection motivation model (OPM; Eppright, Tanner, & Hunt, 1994). Nabi, Roskos-Ewoldsen and Carpentier (2008) found that subjective knowledge (e.g., domain knowledge) was the crucial factor in if individuals actually carried out protective actions after hearing a message in the health domain. Thus, using the framework of protection motivation theory, incorporating the insights provided by other researchers, through adding the dimension of domain knowledge and self-efficacy, I sought to test the response to a cybersecurity message.

7.1.2 Review of focus group materials

To improve validity of the choice of theoretical framework, it was important to test these choices with data that would: 1) verify if PMT is the correct framework to analyze how individuals respond to a cybersecurity message, 2) look for any other constructs that should be explored as part of the PMT model in cybersecurity, and 3) look for ways to improve validity of the PMT constructs given new emergent threats and new protective solutions. Thus, the core of the research instrument is based on these pioneering studies.

In Chapter 3 I described the review of the transcripts from 18 focus groups. The groups had an average of about 10 participants per group and each session lasted about an hour and a half. The participants were grouped by age and use/ non-use of online banking. The focus groups were facilitated using a protocol that guided discussion about their experiences with online threats and how they dealt with those threats. The data was iteratively reviewed and coded using NVivo software to digitally track my findings. As participants shared their experiences, it was clear that they routinely evaluated threats and potential coping responses to those threats. This showed support for using PMT as a framework for understanding response to a cybersecurity message. The comments from participants in the focus groups highlighted the need to explore fatalism, current protective actions and protection habits as an expansion of the PMT framework. New items for previous dimensions were also developed as participants discussed their experiences with emerging threats. The script for the message also emerged from listening to the expressed concerns of the participants and their expressed desires to learn more about how to protect themselves.

7.1.3 Pilot study using a student sample

In Chapter 4 I described the development and testing of the research instrument. The research instrument included a pre-message survey, exposure to a message that had a control and training condition and a post-message survey to measured changes in key attitudes and protective motivation. I used a student sample of 70 participants to test the research instrument and look for ways to refine it. All items were checked for validity, both internal and external. The message was revised and rebuilt. Self-efficacy items were revised and some of the constructs were changed from reflective to formative as new items had changed the nature of a few of the constructs. The results of the pilot study indicated that the research instrument would find significant insights into individuals' response to cybersecurity communications.

7.1.4 Main study and data analysis

In Chapter 5 I discussed the administration of the research instrument to 820 Amazon MTurk workers. After checking the submissions for quality, there were 794 responses that passed the quality checks and were analyzed further. The data was analyzed using SPSS v.25 for confirmatory factor analysis and using SmartPLS 3.0 for path analysis. Both items and constructs were checked with multiple methods for reliability and validity. The constructs had high validity and many of the paths were significant. The new constructs did add explanatory value to the PMT model. The results of the path analysis for key constructs follows.

7.1.5.1 Domain knowledge

Domain knowledge led to higher self-efficacy, higher sense of threat severity, but a lower sense of threat vulnerability. This would indicate those with higher domain

knowledge were aware of online threats, but felt they knew how to protect themselves. Domain knowledge reduced the impact of fear, with its influence lowering fear even post-message in the control condition. However, domain knowledge alone was surprising in that it led to significant reduction of intentions to use generally accepted security practices (e.g., strong and unique passwords, up-to-date security software, clearing cookies). Future research could look more deeply into how those with higher domain knowledge may be more selective about their security practices. Chapter 6 looked more carefully at how domain knowledge interacted with self-efficacy.

7.1.5.2 Time and purpose online

Being online primarily for work purposes was tied with higher levels of domain knowledge and fewer experiences with common threats. This would indicate that those who are online for work purposes are learning how to protect themselves effectively. This could be a result of training at the workplace. Future studies should explore this dimension more thoroughly.

7.1.5.3 Previous experiences with threats

Previous experiences with threats had a tremendous impact on my participants' attitudes, beliefs and practices. Sadly, learning from experience did not lead to knowing more about sources of threat and security solutions. Even minor experiences with threats led to attitudes that would be expected to lead to worse, rather than better, security practices. However, those who had experienced common threats were more likely to be using routine protections. Surprisingly, experiences with serious threats led to responses that made most of these attitudes (e.g., threat vulnerability, response efficacy) no longer significant. This might indicate an ambivalence towards threats which should be studied

in the future. The ray of hope is that those with serious experiences saw response cost as being significantly lower.

7.1.5.4 Self-efficacy

Self-efficacy was truly the powerhouse of the threat and coping appraisal process. It led to lower perceptions of threat and higher beliefs in response efficacy, more protective actions and a stronger protection habit strength. However, this confidence quickly fell apart for many people as they were reminded of a specific threat and especially when they were shown what to do to protect themselves (e.g., in the training condition). Even though the task was very specific (checking to see if one's browser is up to date), being confronted with an actionable task was enough to send self-efficacy plummeting. The cybersecurity message was very positive and supportive, even though it made the user aware of a potential threat. This finding supported empirically what was expressed in the qualitative focus group data- individuals use technology constantly, they are aware of online risks, and want to protect themselves; yet, when confronted with a specific task, it is suddenly overwhelming. This sudden change in attitudes would indicate that the usability of security is a major factor in non-compliance.

Other security professionals and researchers have frequently expressed concerns about the hurdles that individuals face when trying to protect themselves (Cranor & Buchler, 2014; Furnell, 2005; Mannan & Van Oorschot, 2007). The change in self-efficacy illustrated the serious gap between what individuals think they can do and what they are actually able to do. When we have a selection of individuals who appear to care about protecting themselves, are willing to try to do it and find themselves overwhelmed by the

task, there is something seriously wrong with the design of the interface that enhances personal security.

7.1.6 Conditional interaction analysis

The conditional analysis allowed a closer look at the impacts of domain knowledge, self-efficacy and the message condition. The path analysis showed the overall impact of the constructs on the mass of people involved. Looking at the path analysis alone might lead to the incorrect assumption that increased domain knowledge decreased protection motivation and that the training condition had lowered protection motivation overall. Using conditional analysis, we are able to see what the impact of these constructs had on each person.

Domain knowledge had a significant interaction with self-efficacy and the message condition. Those with the lowest domain knowledge and self-efficacy levels were positively impacted by the message and motivated to enact protections. However, those with high self-efficacy and low domain knowledge were negatively impacted by the message- the knowing/doing gap lowered their protection motivation. Since the overall results of the path analysis indicated a negative impact, this would indicate there were enough people in the category of high self-efficacy and low domain knowledge that it pushed the overall results to look like higher domain knowledge and being instructed on how to perform a task (i.e., training condition of the message) led to lower protection motivation. Thus, the conditional analysis allowed us to focus in on the interaction effect of the message, domain knowledge and self-efficacy.

7.2 Answering the research questions

7.2.1 Does domain knowledge impact self-efficacy in the cybersecurity domain?

Domain knowledge had an impact on self-efficacy. However, the impact of domain knowledge was not uniformly positive. This was unexpected given the literature in other domains such as learning (Multon, Brown, & Lent, 1991; Yeo & Neal, 2006) or health practices (Bandura, 1977; Schwarzer & Renner, 2000). In some domains, high self-efficacy without domain knowledge can lead to over confidence and risky behaviors (Krueger & Dickson, 1994; Silvia, 2003). This appears to be true in cybersecurity as well. This data indicates that even a minimal understanding of how threat vectors and basic protections work can help reduce fear and fatalism, bring self-efficacy to more realistic levels, and be better equipped to make choices in protecting themselves.

7.2.2 Does domain knowledge impact the threat appraisal and/or coping appraisal process in the cybersecurity domain?

Domain knowledge lowered the perceptions of threat vulnerability. Even though the paths to response efficacy was positive, it was not significant. Thus, domain knowledge alone did not help move participants towards protection motivation unless the domain knowledge was accompanied by self-efficacy.

7.2.3 Does domain knowledge impact how users respond to a cybersecurity message?

There was the interaction between self-efficacy, domain knowledge and protection motivation discussed in Chapter 6. Domain knowledge had some unexpected impacts in protection motivation indicating that domain knowledge in cybersecurity is undertheorized. Since cybersecurity is a complex, dynamic environment, cybersecurity

messages need to be issued to alert individuals of emerging threats. Having a deeper understanding of how individuals respond to these messages can help improve response. A clear message that included a demonstration of how to carry out a protection was most beneficial for those with lower domain knowledge and lower self-efficacy.

7.2.4 Does domain knowledge reduce fear in the cybersecurity domain?

Domain knowledge not only reduced fear, it also reduced fatalism. This helps reduce the likelihood of an emotional response to a threat and increases the ability of individuals to respond cognitively (Floyd, Prentice-Dunn, & Rogers, 2000; Sommestad, Karlzén, & Hallberg, 2015).

7.2.5 Does the gap between domain knowledge (what individuals actually know) and self-efficacy (what individuals feel confident in) help explain lack of response to cybersecurity initiatives?

In many domains there is a knowing-doing gap (Cox, 2012). Individuals know what to do and yet they don't do it. This research indicates that cybersecurity has a knowing-confidence gap. Participants have high confidence in performing online tasks, and even claim to be performing protective actions, but their actual knowledge is much less than they realize, thus their protective actions may be ineffective. The general lack of domain knowledge can help account for the frequent discrepancies between self-reported security and actual practices (Wash, Rader, & Fennell, 2017). This research showed participants in all phases of the research had concerns about their cybersecurity and willingness to do more, but there was a problem. The gap between what the participants actually knew about cyber threats and protections (i.e., domain knowledge) and the confidence they felt in carrying out (i.e., self-efficacy) protections was huge. There were gaps both ways. Some had low self-efficacy but had high domain knowledge. Others had

high self-efficacy but low domain knowledge. Either way, the gap led to less than optimum protections.

7.3 Implications of findings

These findings indicate that domain knowledge is under-theorized in cybersecurity. Cybersecurity's technical nature and technology's ubiquitous presence make the human dimension of cybersecurity a complex issue. These findings also bring up serious issues about usability in security and the need to prioritize both cybersecurity education and mandate usable security. Throughout this research, individuals expressed that they care about cybersecurity, yet often they don't know what to do to protect themselves. This research also demonstrated that for many people, cybersecurity is hard to do. Self-efficacy took a significant hit when individuals were given a basic safety task to perform. Even though checking for a browser update was a basic task, for some browsers it took several clicks through different levels of menus to find if the browser was up-to-date. It was not easy. Also, during the course of this research and the development of the tutorials, the method to check a browser went through three major changes and required reproducing the demonstration videos. Each browser and each version had unique methods to check status, so learning how to perform the safety task on one browser did not necessarily mean it was easy to do the same task on another browser. The lack of uniform standards increases the difficulty for individuals to go from browser to browser and be sure they are working with a safe version. This problem is multiplied exponentially when we think of the myriad of hardware and software choices we expect novice users to make to protect themselves the they systems they use.

This is troubling, because the systems that should be supporting and protecting individuals is not working. Tremendous effort and resources globally have been spent to help encourage technology adoption and encourage people from all walks of life to be part of today's digital society. Only a fraction of those resources has been devoted to ensuring that these individuals, networks and systems are protected. Increased resources are now being directed towards helping improve this situation; hopefully, this research can help illustrate the need to support end users and equip them with the tools they need to become a part of the cybersecurity solution. The findings offer insights for some of the following stakeholders-

7.3.1 Policy makers

Cybersecurity issues threaten the future of society (Arquilla & Guzdial, 2017; Nicholas, 2015). Even though most research agrees the end-user is often the cause of a security failure (Daugherty, 2016), a growing consensus of stakeholders agree that we need to stop blaming the end-user (Clark, Berson, & Lin, 2014; Furnell, 2008; Sasse, Brostoff, & Weirich, 2001; World Economic Forum, 2017). There is little agreement among stakeholders about what this entails. This research shows individuals do care about cybersecurity and want to improve their protections. However, there is a two-fold problem. Not only is the factual knowledge about threat vectors and protective solutions lacking, the usability of security is atrocious. Prioritizing educational initiatives that improve basic knowledge across all levels of society will build a population that is more savvy and able to become defenders of cybersecurity rather than weak links. But this is not a call to simply "educate the user," but rather to mandate that security is more usable and intuitive (Schneier, 2016). Unlike other technological dimensions where market forces will bring

solutions, security holes are not frequently seen or understood by purchasers or users of the technology, thus there are not the natural incentives to improve security standards. If we want to narrow the security gap in cybersecurity we need to invest widely in helping end users to become informed consumers and mandating cybersecurity standards that increase usability.

7.3.2 Software and hardware designers

Making security usable and intuitive should be a top priority for software and hardware designers. This research shows that individuals care about cybersecurity but that often doesn't translate to action because of lack of usability. Collaborative work across brands to make routine security activities easier and more consistent would be a first step in improving everyone's security. Seeing cybersecurity as a basic dimension of hardware, software, and networks, rather than something added in the last step, will help improve utilization of security in systems. Also, by having verifiable security standards, cybersecurity can become a competitive advantage in the marketplace.

7.3.3 Educators

This data shows support for educational efforts that help end users understand the dynamic nature of threats and how to take adaptive stances to protect ourselves. A well-educated populace can help advocate for improved systems. Also, in addition the critical need for cybersecurity workers (Dychtwald, Erickson, & Morison, 2013), we need individuals at all levels in all professions to see that cybersecurity is a part of whatever task they perform using technology. This research shows the importance of encouraging realistic self-efficacy and problem solving to students. If self-efficacy is inflated above actual skills, it is easy to become overwhelmed when faced with the need to perform a

task. Also, cybersecurity initiatives should clearly show how to perform a task to increase motivation and behavioral change.

7.3.1 Researchers

This research not only verifies the use of PMT in cybersecurity research, it adds insights to understanding the complex processes that individuals face every time they make a security choice. Even though the PMT model is rather complex, with many constructs working within its framework, this research shows its flexibility and ability to provide insight into human behavior. Even though Rippetoe and Rogers (1987) suggested that prior experiences and personal variables may impact how individuals process a threat, this research is the first to explore it using this method in cybersecurity. Testing a cybersecurity message in an experimental format allowed insights into how self-efficacy is impacted when individuals face enacting security protections. These insights give empirical support to what many experts having been saying about the issues of usability in cybersecurity (e.g., Schneier, 2016) and that we cannot blame the user. This research also shows the potential impact of better cybersecurity educational initiatives. By improving knowledge about basic threats and protections, individuals can cognitively evaluate emerging threats and make better protection decisions.

7.4 Limitations and future research

The participants of the online experiment were online workers; thus, they use their computers for financial purposes, they are skilled at using applications on the Internet, and they are digitally literate enough to know how to sign up for and use the Amazon labor pool. They probably have higher domain knowledge about cybersecurity than the typical technology user. They also are highly motivated to protect themselves online as

they want to protect their online earnings and reputation. Other individuals who are not as active online may have lower protection motivation and lower domain knowledge. This research should be replicated with individuals who are not online workers to test if the findings are similar or even more pronounced.

This research uses the expanded PMT framework in one small dimension of cybersecurity, but there are many dimensions of PMT that should be further refined and explored in future research. The concept of measuring protection motivation also needs refinement as cybersecurity is a complex domain where informed cognitive choices are based on weighing costs and benefits that change in each situation. Individuals with higher domain knowledge may be more selective about what protections they bother to enable; thus protection motivation may be high even if the individual doesn't embrace a set of activities. For example, cleaning cookies or rejecting cookies on pages may be seen as increasing privacy and security. We might say that someone is highly motivated to protect himself if he routinely clears cookies. However, cookies allow better customization of experience and are often required for shopping and social networking sites to function. Thus, the decision to clear cookies may be influenced by weighing the increased risk that cookies bring against the inconvenience of clearing all cookies and not having sites function correctly. The person who allows cookies may be making other security choices to act as protections against the risk that cookies could theoretically bring. Further research should help develop more robust and mature insights into the human factors of cybersecurity.

This research is just a tiny voice in the noisy realm of end user behavior in cybersecurity, but hopefully it is a voice that encourages stakeholders to help end users

by increasing the usability of security as well as supporting educational initiatives that enable users to be an informed part of the cybersecurity team. There is a gap between domain knowledge and self-efficacy, lets mind the gap by reducing it so individuals can safely go on their way.

WORKS CITED

WORKS CITED

Arquilla, J., & Guzdial, M. (2017). Crafting a National Cyberdefense, and Preparing to Support Computational Literacy. Communications of the ACM, 60(4), 10–11. http://doi.org/10.1145/3048379

Bandura, A. (1977). Self-efficacy: Toward a Unifying Theory of Behavioral Change. Pyschological Review, 84(2), 191–215. http://doi.org/http://dx.doi.org/10.1037/0033-295X.84.2.191

Bandura, A. (1989). Regulation of Cognitive Processes Through Perceived Self-efficacy. Developmental Psychology, 25(5), 729–735. Retrieved from http://psycnet.apa.org/journals/dev/25/5/729/

Clark, D., Berson, T., & Lin, H. S. (eds). (2014). At the Nexus of Cybersecurity and Public Policy:Some Basic Concepts and Issues. Washington, D.C.: National Academies Press. http://doi.org/10.17226/18749

Cox, J. (2012). Information Systems User Security: A Structured Model of the Knowing–Doing Gap. Computers in Human Behavior, 28(5), 1849–1858. http://doi.org/10.1016/j.chb.2012.05.003

Cranor, L. F., & Buchler, N. (2014). Better Together: Usability and Security Go Hand in Hand. IEEE Security & Privacy, 12(6), 89–93. http://doi.org/10.1109/MSP.2014.109

Crossler, R., & Belanger, F. (2014). An Extended Perspective on Individual Security Behaviors : Protection Motivation Theory and a Unified Security Practices (USP) Instrument. The Database for Advances in Information Systems, 45(4). http://doi.org/10.1145/2691517.2691521

Daugherty, W. R. (2016). Human Error is to Blame for Most Breaches. Retrieved June 17, 2017, from http://www.cybersecuritytrend.com/topics/cyber-security/articles/421821-human-error-to-blame-most-breaches.htm

Dychtwald, K., Erickson, T. J., & Morison, R. (2013). Workforce Crisis: How to Beat the Coming Shortage of Skills And Talent. Harvard Business Press. Retrieved from http://books.google.com/books/about/Workforce_Crisis.html?id=YOiqKakrS2oC&pgis=1

Eppright, D. R., Tanner, J. F., & Hunt, J. B. (1994). Knowledge and the Ordered Protection Motivation Model : Tools for Preventing AIDS. Journal of Business Research, (30), 13–24.

Fazio, R. H. (1990). Multiple Processes by Which Attitudes Guide Behavior : The MODE Model as an Integrative Framework. Advances in Experimental Psychology (Vol. 23), 23(July 1990), 75–109. http://doi.org/10.1016/S0065-2601(08)60318-4

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A Meta-analysis of Research on Protection Motivation Theory. Journal of Applied Social Psychology, 2000, 30, 2, Pp. 407-429., 30,(2,), 407–429. http://doi.org/10.1111/j.1559-1816.2000.tb02323.x

Furnell, S. (2005). Why Users Cannot Use Security. Computers & Security, 24(4), 274–279. http://doi.org/10.1016/j.cose.2005.04.003

Furnell, S. (2008). End-User Security Culture: A Lesson that will Never be Learnt? Computer Fraud and Security, 2008(4), 6–9. http://doi.org/10.1016/S1361-3723(08)70064-2

Hanus, B., & Wu, Y. “Andy.” (2015). Impact of Users’ Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. Information Systems Management, 10580530.2015.1117842. http://doi.org/10.1080/10580530.2015.1117842

Icek Ajzen. (2002). Perceived Behavioral Control, Self-efficacy, Locus of Control, and the Theory of Planned Behavior. Journal of Applied Social Psychology, 80(6), 2918–2940. http://doi.org/10.1111/j.1559-1816.2002.tb00236.x

Krueger, N. F. J., & Dickson, P. R. (1994). “How Believing in Ourselves Increases Risk Taking: Perceived Self-efficacy and Opportunity Recognition.” Decision Sciences, 25(3), 385–400. http://doi.org/10.1111/j.1540-5915.1994.tb00810.x

Maddux, J. E., & Rogers, R. W. (1983). Protection Motivation and Self-efficacy: A Revised Theory of Fear Appeals and Attitude Change. Journal of Experimental Social Psychology, 19(5), 469–479. http://doi.org/10.1016/0022-1031(83)90023-9

Mannan, M., & Van Oorschot, P. C. (2007). Security and Usability: The Gap in Real-World Online Banking. IEEE Technology and Society Magazine, 26, 1–14. http://doi.org/10.1109/MTAS.2007.335568

Multon, K. D., Brown, S. D., & Lent, R. W. (1991). Relation of Self-efficacy Beliefs to Academic Outcomes: A Meta-analytic Investigation. Journal of Counseling Psychology, 38(1), 30–38. http://doi.org/10.1037/0022-0167.38.1.30

Nabi, R. L., Roskos-Ewoldsen, D., & Carpentier, F. D. (2008). Subjective Knowledge and Fear Appeal Effectiveness: Implications for Message Design. Health Communication, 23, 191–201. http://doi.org/10.1080/10410230701808327

Nicholas, J. (2015). Cybercrime Costs the World $US465 Billion Annually. Retrieved September 29, 2015, from http://www.businessinsider.com.au/report-cybercrime-costs-the-world-us465-billion-annually-2015-9

Rippetoe, P. A., & 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), 596–604. http://doi.org/10.1037//0022-3514.52.3.596

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security. BT Technology Journal, 19(3), 122–131. http://doi.org/10.1023/A:1011902718709

Schneier, B. (2016). Stop Trying to Fix the User. IEEE Security and Privacy, 14(5), 96. http://doi.org/10.1109/MSP.2016.101

Schwarzer, R., & Renner, B. (2000). Social-cognitive Predictors of Health Behavior: Action Self-efficacy and Coping Self-efficacy. Health Psychology, 19(5), 487.

Shillair, R., Cotten, S. R., Tsai, H.-Y. S., Alhabash, S., Larose, R., & Rifon, N. J. (2015). Online Safety Begins with You and mMe: Convincing Internet Users to Protect Themselves. Computers in Human Behavior, 48. http://doi.org/10.1016/j.chb.2015.01.046

Silvia, P. J. (2003). Self-efficacy and Interest: Experimental Studies of Optimal Incompetence. Journal of Vocational Behavior, 62(2), 237–249. http://doi.org/10.1016/S0001-8791(02)00013-1

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. International Journal of Information Security and Privacy, 9(1), 26–46. http://doi.org/10.4018/IJISP.2015010102

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory. Information & Management, 49(3–4), 190–198. http://doi.org/10.1016/j.im.2012.04.002

Wash, R., Rader, E., & Fennell, C. (2017). Can People Self-Report Security Accurately ? Agreement Between Self-Report and Behavioral Measures. In CHI 2017 (pp. 2228–2232). Denver.

Witte, K. (1994). Fear control and Danger Control: A Test of the Extended Parallel Process Model (EPPM). Communication Monographs. http://doi.org/10.1080/03637759409376328

Woon, I. M. Y., Tan, G. W., & Low, R. T. (2005). A Protection Motivation Theory Approach to Home Wireless Security. Proceedings of the Twenty-, 367–380. Retrieved from http://dmlab.mis.ttu.edu.tw/conference/2005-ICIS_2005/SA03.pdf

World Economic Forum. (2017). Advancing Cyber Resilience Principles and Tools for Boards. Future of Digital Economy and Society Systems Initiative.

Yeo, G. B., & Neal, A. (2006). An Examination of the Dynamic Relationship Between Self-efficacy and Performance Across Levels of Analysis and Levels of Specificity. Journal of Applied Psychology, 91(5), 1088–1101. http://doi.org/10.1037/0021-9010.91.5.1088