A Protection Motivation Theory Approach to Improving Compliance with Password Guidelines

Florence Mwaka Mwagwabi, BA., Masters. IT

This thesis is presented for the degree of Doctor of Philosophy of Murdoch University

2015

I declare that this thesis is my own account of my research and contains as its main content work which has not previously been submitted for a degree at any tertiary education institution.

.....
(Florence Mwagwabi)

Abstract

Usernames and passwords form the most widely used method of user authentication on the Internet. Yet, users still find compliance with password guidelines difficult. The primary objective of this research was to investigate how compliance with password guidelines and password quality can be improved. This study investigated how user perceptions of passwords and security threats affect compliance with password guidelines and explored if altering these perceptions would improve compliance. This research also examined if compliance with password guidelines can be sustained over time. This study focuses on personal security, particularly factors that influence compliance when using personal online accounts.

The proposed research model is based on the Protection Motivation Theory (PMT) (Rogers, 1975, 1983), a model widely used in information systems security research. As studies have failed to consistently confirm the association between perceived vulnerability and information security practices, the model was extended to include exposure to hacking as a predictor of perceived vulnerability. Experimental research was used to test the model from two groups of Internet users, one of which received PMT based fear appeals in the form of a password security information and training exercise. To examine if password strength was improved by the fear appeals, passwords were collected. A password strength analysis tool was developed using Shannon's (2001) formula for calculating entropy and coded in Visual Basic. Structural equation modeling was used to test the model.

The proposed model explains compliance intentions moderately well, with 54% of the variance explained by the treatment model and 43% explained by the control group model. Overall, the results indicate that efficacy perceptions are a stronger predictor of compliance intentions than threat perceptions. This study identifies three variables that

predict user intentions to comply with password guidelines as particularly important. These are perceived threat, perceived password effectiveness and password self-efficacy. The results show no association between perceived vulnerability to a security attack and a user's decision to comply. The results also showed that those who are provided with password information and training are significantly more likely to comply, and create significantly stronger passwords. However, the fear appeals used in this study had no long-term effects on compliance intentions. The results on the long-term effects of password training on the participants' ability to remember passwords were however promising. The group that received password training with a mnemonic training component was twice as likely to remember their passwords over time.

The results of this research have practical implications for organizations. They highlight the need to raise the levels of concern for information systems security threats through training in order to improve compliance with security guidelines. Communicating to users what security responses are available is important; however, whether they implement them is dependent on how effective they feel the security responses are in preventing an attack. Regarding passwords, the single most important consideration by a user is whether they have the ability to create strong, memorable passwords. At the very least, users should be trained on how to create strong passwords, with emphasis on memorization strategies. This research found mnemonic password training to have some long-term effects on users' ability to remember passwords, which is arguably one of the most vexing challenges associated with passwords. Future research should explore the extent to which the effects of PMT based information systems security communication can be maintained over time.

Table of Contents

List of Figures

List of Tables

Acknowledgements

I would like to express my sincere gratitude to my supervisors Dr. Mike Dixon and Associate Professor Tanya McGill for their expertise, support and excellent guidance for the past several years. As I moved from one idea to another and to a completed thesis, they have been nothing but patient and motivating. I could not have imagined having better supervisors.

My sincere thanks also goes to Peter Cole for making my data collection possible. I cannot thank him enough. I would also like to thank Dr. Allen G. Harbaugh for the enormous amount of help and useful advice he provided me on structural equation modeling. Special thanks goes to Danny Toohey who in the final stretch of my write-up knocked on my door every morning just to make sure I was on track, and of course to pick up some candy.

To the anonymous reviewers at the HICSS-47 Conference who provided instructive feedback, thank you for helping shape my thesis with your insightful comments.

I will forever be thankful to my friends for their patience and encouragement throughout this process. In particular, I would like to thank Dr. Kevin Lee for providing invaluable research and career advice during our many lunches.

Finally, I would like to thank my best friend for giving me the push I needed to get started, and my family for pushing me to the finish line.

1 Introduction

1.1 Background

Usernames and passwords have been a conventional method of authentication for many decades (e.g., Bonneau, 2012; Morris & Thompson, 1979; Taneski, Heričko, & Brumen, 2014). Despite the weaknesses associated with passwords and availability of other innovative authentication technologies such as tokens and biometrics, usernames and passwords are still the preferred method of user authentication (Keith, Shao, & Steinbart, 2007; Komanduri et al., 2011; Shay et al., 2012; Stewart, Tittel, & Chapple, 2008). Organizations view password authentication as a cost effective, easier to implement alternative (Tsai, Lee, & Hwang, 2006), yet users view them as inconvenient and mostly difficult to remember (Inglesant & Sasse, 2010; Ur et al., 2012; Yan, Blackwell, Anderson, & Grant, 2004). This attitude toward passwords has ultimately led to a continued use of weak passwords making users vulnerable to threats such as hacking (Florêncio & Herley, 2010; Inglesant & Sasse, 2010).

Unfortunately, users use weak passwords even when it is in their best interest to use strong passwords, such as when protecting medical files (El Emam, Moreau, & Jonker, 2011) or financial accounts (Florêncio & Herley, 2007). Findings from several large-scale analysis of thousands to millions of passwords leaked on the internet draw attention to how common weak passwords are on the Internet (e.g., BBC, 2013; Calin, 2009; Coursey, 2011). While some of the leaked passwords were collected through social engineering techniques such as phishing, the findings from these studies are indicative of how users still find compliance with password guidelines difficult. Users still use passwords such as ‘123456’ and ‘password’ on the Internet, including security professionals (Lorenz, Kikkas, & Klooster, 2013).

Another poor password practice prevalent amount Internet users is password reuse across several websites or recycling passwords from an old password (Florêncio & Herley, 2007). Florêncio and Herley (2007) observed password practices of over half a million users across websites such as YouTube, PayPal, eBay and Yahoo and found that it was common for users to reuse passwords across these websites. A large scale study by Zhang, Monrose, and Reiter (2010), demonstrates the extent to which password reuse can pose threat to any system. They managed to crack 41% of recycled passwords in as little as three seconds.

A survey of Internet home users conducted by the National Cyber Security Alliance (NCSA) (2011) also highlights the prevalence of poor password practices among Internet users. Of the 2,300 Internet users surveyed, three quarters had not changed their passwords in over six months, with two thirds of them citing difficulty to remember and the hassle of changing passwords as their reasons for not changing passwords. Their study found that most home users are not concerned about someone hacking their non-financial and email accounts. Given the persistent use of weak passwords even on sensitive personal accounts, the key challenge to organizations is to motivate users to use strong passwords.

1.2 Research problem

To improve password strength, users should be guided toward the adoption of recommended password policies (Taneski et al., 2014). The conventional method of encouraging users to create strong passwords is through password guidelines. Password guidelines are a set of password best practices that provide control over the quality of passwords used on a system and also serve as a guide to safe password management practices (Florêncio & Herley, 2010). However, several studies have

found no correlation between provision of password guidelines and the quality of passwords users create (Florêncio & Herley, 2010; Inglesant & Sasse, 2010; Ur et al., 2012; Yan et al., 2004). Furthermore, even when additional tools such as a password strength meter are used, users' propensity for using weak passwords is still evident (Egelman, Sotirakopoulos, Muslukhov, Beznosov, & Herley, 2013; Ur et al., 2012; Vance, Eargle, Ouimet, & Straub, 2013).

An analysis of the password guidelines of 75 online websites conducted by Florêncio and Herley (2010) brings to light why unstandardized password guidelines may be a long term issue. They found websites that rely on advertising have a significantly lower average password requirement compared with websites that do not. This is because advertisement-driven websites have to compete for users in order to generate traffic, thus strict password requirements would potentially discourage users (Florêncio & Herley, 2010). Although Bonneau and Preibusch (2010) recommend more homogenous password guidelines, Florêncio and Herley (2010) argue that variation in password guidelines is likely to be a long term issue for as long as websites are driven by user traffic.

Unfortunately, users find it difficult to cope with this variation in password guidelines (Inglesant & Sasse, 2010), affecting their attitude and consequently the quality of passwords created (Florêncio & Herley, 2010; Komanduri et al., 2011). Whilst approaches such as check-off password system (Warkentin, Davis, & Bekkering, 2004) and passphrases have shown some promise (Keith, Shao, & Steinbart, 2009), negative attitudes among users will continue to affect compliance with password policies. Therefore, other means of encouraging users to create strong passwords must be pursued.

Having a solid information systems (IS) security policy and procedures is key to ensuring security (Peltier, 2005; Tipton & Hernandez, 2009), however many organizations and web services resort to strict password guidelines. When password guidelines are too stringent they inadvertently promote poor password management practices such as writing them down, or passwords reuse across websites (Inglesant & Sasse, 2010; Yan et al., 2004). This is partly because password policies do not always create conditions that promote safer password practices (Florêncio & Herley, 2007; Herley, 2009; Shay et al., 2010; Yan et al., 2004) or assist users in maintaining multiple strong passwords (Helkala & Svendsen, 2012). Instead, users perceive them as counterproductive because they lead to passwords that are difficult to remember (Inglesant & Sasse, 2010; Yan et al., 2004).

The key challenge for users is creating and maintaining multiple strong, long passwords, that contain a series of random characters with no dictionary or common words (Bonneau, 2012; Burr, Dodson, Newton, Pelner, & Polk, 2013; Helkala & Svendsen, 2012; Pham, Syed, & Halgamuge, 2011). Remembering strong passwords is cited as one of the most challenging aspects of password usage (NCSA-McAfee, 2011; Zviran & Haga, 1999). Users' inability to remember random characters (Yan et al., 2004; Zviran & Haga, 1993, 1999), an important characteristic of a strong password is also said to contribute to poor password practices (Adams & Sasse, 1999) and a lack of motivation to comply with password policies (Bonneau & Preibusch, 2010; Florêncio & Herley, 2010; Inglesant & Sasse, 2010). Since the human brain can only memorize a sequence of five to nine random objects (Miller, 1956), it is unsurprising that remembering passwords is difficult for most users.

Studies have linked user motivation to how they perceive security threats, such as their assessment of the consequences of security threats (Liang & Xue, 2010; Woon, Tan, &

Low, 2005; Zhang & McDowell, 2009), and how they perceive security measures such as their assessment of the effectiveness of security measures in preventing threats (Lee & Larsen, 2009; Woon et al., 2005; Zhang & McDowell, 2009). User security perceptions are therefore a key motivator and predictor of security practices.

As passwords remain the most commonly used method of user authentication it is becoming increasingly important to examine ways to promote better password practices. Over the years organizations have invested heavily on IS security technologies to secure their information assets, and according to the Federal Government Cybersecurity Survey (Moyle & Kelley, 2012), lack of information security technologies is no longer seen as a challenge to organizations. Yet, most organizations spend 10% or less of their IS security budget on security awareness and training programs, while users continue to be a threat to information security (Richardson, 2011). Regarding user password security, focusing on users is particularly important.

1.3 Purpose of the research

The study focuses on concepts pertaining to security perceptions, and investigates how user perceptions of passwords and security threats affect compliance with guidelines and if these perceptions can be altered to improve compliance.

Several factors have been identified as influencing IS security practices and compliance with IS security policies. How users assess the severity of threats drives their decision to apply security measures (Siponen, Mahmood, & Pahnila, 2014; Vance, Siponen, & Pahnila, 2012; Woon et al., 2005) or if they believe the threat is imminent (Ifinedo, 2012; Lee & Larsen, 2009; Workman, Bommer, & Straub, 2008). Further, whether a user chooses to apply security measures is dependent upon the

perceived effectiveness of the recommended security measures (Lee & Larsen, 2009; Woon et al., 2005; Zhang & McDowell, 2009), assessment their ability to successfully implement the security measures (Johnston & Warkentin, 2010a; Woon et al., 2005), and a user would also consider the effort it would take to successfully execute the security measures (Lee & Larsen, 2009; Woon et al., 2005; Workman et al., 2008; Zhang & McDowell, 2009). Additionally, studies have shown that these perceptions can be manipulated to improve compliance with security policies (Jenkins, Grimes, Proudfoot, & Lowry, 2013; Johnston & Warkentin, 2010a), and to improve password quality (Vance et al., 2013).

The objective of this research is four-fold. Firstly, this study investigates how perceptions about severity of password threats and vulnerability to password threats affect compliance with password guidelines. Secondly, examines how user perception about the effectiveness of passwords guidelines in preventing password threats and beliefs about one's ability to create strong passwords contributes to compliance with password guidelines. The research also seeks to investigate if fear appeals or persuasive messages can be effectively used to alter these perceptions to improve compliance with password guidelines and ultimately password strength. Finally, this research explores the extent to which the effects of the fear appeals messages persist after a period of time has elapsed.

The ultimate objective of this research is to provide a better understanding of the relationship between user perceptions about passwords and password threats, and the impact of these perceptions upon compliance with password guidelines. The research attempts to show that these perceptions can be altered to motivate users to comply with password guidelines and if compliance can be maintained over time.

To achieve the objectives of this research the following research questions are addressed:

1. How do user perceptions about password threats and password efficacy affect compliance with password guidelines?
2. Can these perceptions be altered?
    2a. If so, can altering these perceptions improve compliance with password security guidelines?
    2b. Can the effects of altering these perceptions be maintained over time?

1.4 Research significance

With a target population of online email account holders, this study aims to provide a better understanding of the factors that affect compliance with online password policies and how compliance with online password guidelines can be improved using fear appeals. Why online email accounts? Online usernames and passwords are becoming even more valuable than stolen credit card information. A recent study by Ablon, Libicki, and Golay (2014) in conjunction with the RAND Research Corporation, found that the economic value of online usernames and passwords is surpassing that of credit card details. This, according to Ablon et al. (2014), is partly because the value of stolen credit cards information is temporal and depreciates with time. However, online passwords including those of social media accounts such as Twitter, command a higher price because such personal accounts can lead to other valuables and revealing information. Therefore, an individual employee's risky security practices, particularly on a personal online accounts have potentially serious implications to an organization (Ives, Walsh, & Schneider, 2004; Jenkins et al., 2013; Winkler, 2009).

While it is important to investigate compliance with password policies within an organization, given that online email and social networking accounts are the most targeted online accounts by hackers (Goncharov, 2012), the aim of this study is to investigate ways to improve online password practices. Therefore, in addition to research implications, the findings in this study should have societal and organizational implications.

Many password security researchers have questioned the effectiveness of password guidelines in preventing password threats (Adams & Sasse, 1999; Florêncio & Herley, 2010; Inglesant & Sasse, 2010; Yan et al., 2004). Existing password guidelines are however challenging and confusing to users and as a result users lack motivation to comply with recommended requirements (Bonneau & Preibusch, 2010; Florêncio & Herley, 2010; Inglesant & Sasse, 2010). Understanding how to motivate users is central to the future success of password based authentication. As studies have linked this lack of motivation to how users perceive security threats (Bonneau & Preibusch, 2010; Woon et al., 2005), it is important to examine the role user perceptions play in compliance with password policies and determine if compliance levels can be increased by altering these perceptions. The research described in this thesis should help organizations to take action to improve password security compliance.

Designed to ensure passwords meet certain security standards, existing password guidelines have failed to prevent password related threats. Further, large websites such as Facebook, Google and Twitter implement the least restrictive password policies (Florêncio & Herley, 2010), despite the sensitive nature of information kept by users. This highlights the need for other strategies for improving compliance with password guidelines and password quality. While feedback techniques such as the use of password strength meters have been used to improve password quality, the available

evidence shows mixed results (Egelman et al., 2013; Ur et al., 2012; Vance et al., 2013) on its effectiveness in persuading users to follow the recommended password guidelines. The focus should instead be on providing users with knowledge of security threats (Adams, Sasse, & Lunt, 1997) therefore enhancing user knowledge about password security threats. It is important to investigate how security threats can be effectively communicated to users, and if this will in turn improve password strength.

Implementing effective security awareness and training programs is key to motivating users to practice security and to promote realistic user security perceptions (Adams & Sasse, 1999; Inglesant & Sasse, 2010). In addition, IS security training programs should include a password security component and instructions on how to create strong passwords (Stewart et al., 2008). Given the ubiquitous nature of passwords more targeted IS security training incorporating a password security component is of increasing importance. The outcomes of this research should also help identify training components with the strongest influence on compliance.

The proposed research model is based on the health-based Protection Motivation Theory (PMT) (Rogers, 1975, 1983) which suggests that how users evaluate health risks may increase or decrease their likelihood of complying with protective measures. One of the reasons PMT was selected for this study is its usefulness in predicting behavioral change using persuasive communication and its extensive application in experimental studies (Weinstein, 1993). IS security researchers have shown interest in the PMT (Herath & Rao, 2009; Johnston & Warkentin, 2010a; Siponen et al., 2014; Vance et al., 2013; Woon et al., 2005; Workman et al., 2008), however only a few published works (e.g., Jenkins et al., 2013; Johnston & Warkentin, 2010a; Vance et al., 2013), are experimental studies. None thus far appear to have examined the long term effects of fear appeals on IS security behavior.

While empirical studies (e.g., Bonneau, 2012; Cazier & Medlin, 2006; Dell'Amico, Michiardi, & Roudier, 2010; Shay et al., 2010; Weber, Guster, Safonov, & Schmidt, 2008; Weir, Aggarwal, Collins, & Stern, 2010; Yan et al., 2004; Zhang, Luo, Akkaladevi, & Ziegelmayer, 2009; Zhang et al., 2010; Zviran & Haga, 1999) have been instrumental to this study in identifying factors affecting password practices, the theory grounded research described in this thesis provides insights into the relationships between these factors and compliance with password guidelines. In particular, the theory based experimental research used in this study provides further insight into how IS security training can be designed effectively, as suggested by the PMT framework (Rogers, 1975, 1983), to target these key factors and ultimately improve security practices. Thus, the findings from this experimental research should also contribute to IS security training development, an area where theory based research is lacking (Puhakainen & Siponen, 2010).

This research also addresses password measurement issues and seeks to examine ways to measure password strength. A key challenge in measuring password strength is the lack of universal metric for measuring password strength (Bonneau, 2012), coupled with the ambiguity of the term password strength (Dell'Amico et al., 2010; Egelman et al., 2013). A password analysis tool was therefore developed to measure password strength. The goal was to develop a user-friendly password analysis tool that can also be used as a research tool or in conjunction with password security training within an organization

1.5 Research approach

To achieve the objectives described in this thesis, a model based on the health-related PMT model (Rogers, 1975, 1983) was proposed. PMT has received considerable

attention among IS security researchers and has been shown to be a helpful model for predicting IS security behavior (e.g. Herath & Rao, 2009; Johnston & Warkentin, 2010a; Posey, Roberts, Lowry, Courtney, & Bennett, 2011; Vance et al., 2012; Woon et al., 2005; Workman et al., 2008; Zhang & McDowell, 2009). As a persuasive communications theory (Rogers, 1975, 1983), PMT has also been shown to be a useful framework for designing IS security persuasive messages (e.g., Jenkins et al., 2013; Johnston & Warkentin, 2010a; Vance et al., 2013).

This research focuses on password practices on the Internet. As such, the target population was Internet users who have at least one Internet email account. Data was collected through an online questionnaire. To ensure the respondents held at least one online email account participants were recruited through email invitations. One of the research questions addressed in this study seeks to explain how perceptions about password threats and password efficacy affect password practices. To address this question the model developed for this study was used to explain password behavior.

Another research question addressed in this study seeks to examine if these perceptions can be changed with the ultimate goal of enhancing the level of compliance with password guidelines. To address this question, PMT was used as a framework for designing persuasive communication and as suggested by Leventhal (1970) an experimental design where one group is exposed to fear appeals and another is not, was conducted. As such, data was collected from two separate groups using two separate survey instruments, where one contained the fear appeal messages.

As a follow-up to the second research question, this study investigates if the effects of altering user perceptions can be sustained over time. To address this question, a follow-up study was conducted where data was collected from the same pool of participants and their level of compliance was subsequently examined.

The model was tested using structural equation modeling (SEM) and to examine behavioral change. Multivariate analysis of variance (MANOVA) and analysis of variance (ANOVA) was conducted.

1.6 Overview of chapters

This thesis is presented in seven key chapters. The first chapter provided an overview of the proposed research, with emphasis on issues pertaining to the use and management of text-based passwords. It also presented the rationale for this study, and the objectives and research questions addressed in this study.

The rest of this thesis is presented as follows. Chapter 2 reviews relevant literature and is organized into three major sections. The first is centered on concepts pertaining to security perceptions. This is followed by a review of competing theories commonly used to explain preventative behaviors, including background, core components, limitations and applicability of the theories to this study. Lastly, it presents a review of literature relating to passwords and key challenges related to their usage.

In Chapter 3 the research questions and supporting literature are presented. The chapter also describes the theoretical framework on which the proposed research model is based. Lastly, the hypotheses developed for this study are presented alongside the proposed research model and definitions of the constructs used.

Chapter 4 is organized as follows. First, a detailed description of the study design is presented. This is followed by a description of the participants, the method by which they were recruited, and a description of the data collection procedure. The study materials, which include fear appeal messages and survey instruments, are then described. The survey instruments used in the follow-up study and data collection procedure for the follow-up study are then described. Finally, a detailed description of

SEM, the primary data analysis techniques elected for this study and the procedure used to validate the measurement model and to test the structural model are presented.

In Chapter 5, the analysis and results of this study are presented in four major sections, as follows. The first is a description of the demographic and computer background data about the participants. The results of the measurement model assessment and validation are then presented, followed by a section presenting results of the structural model testing. The final section presents the results of each hypothesis.

Chapter 6 discusses the results presented in Chapter 5. It discusses the key findings of this study with reference to relevant research and discusses shortcomings of this research requiring further consideration.

Finally, the implications for future research based on the results and limitations of this study are discussed in Chapter 7. Also building on the results of this research, this chapter discusses the practical implications for organizations and IS security training practitioners.

2 Literature Review

2.1 Introduction

This study is centered on concepts pertaining to security perceptions, and investigates how user perceptions of passwords and security threats affect compliance with password guidelines. The question of whether these perceptions can be altered in order to improve compliance is also addressed in this research.

This chapter contains three major sections. Section 2.2 provides background information on user perceptions of IS security, and particularly how these perceptions are formed, which is important to this study for a better understanding of how to alter these perceptions. Section 2.3 presents four competing theories used for predicting preventative behaviors in a variety of research domains and reviews previous research attempting to explain IS security behaviors. Lastly, Section 2.4 provides an overview of user challenges related to text-based password authentication on the Internet.

Historically, IS security research was focused primarily on technology as a solution to security issues (Adams & Sasse, 1999; Hitchings, 1995). It, however, became clear technology alone is insufficient to guarantee security, thus the prevailing view took a turn, and humans were considered key players in security breaches (Hitchings, 1995). Organizations and researchers began to view users as the weakest link (Adams & Sasse, 1999; Sasse, Brostoff, & Weirich, 2001), which led to a shift in focus from technology to social-behavioral research (Anderson & Agarwal, 2010; Woon et al., 2005; Workman et al., 2008). The notion of the weakest link originated partly from how authentication mechanisms, designed to prevent unauthorized access to protected information, are largely dependent on a user's input (Adams & Sasse, 1999). As security technologies are implemented and used by human beings, and thus prone to

human error (Hitchings, 1995), focus on human factors is important. However, some argue that users are only partly to blame and that a lack of guidance such as awareness training and motivation play a significant role in undesirable security practices (Adams & Sasse, 1999; Sasse et al., 2001; Winkler, 2009). The research described in this thesis takes this position, and based on the premise that users can be guided towards engaging in recommended security measures.

2.2 Information security perceptions

Security recommendations ensure users maintain a certain level of security. However, studies show that users lack the motivation to comply, even when the recommended measures are aimed to protect personal financial information (e.g., El Emam et al., 2011; Florêncio & Herley, 2007). This failure to follow security recommendations has led to numerous studies seeking to understand what motivates users to adopt security measures.

The literature generally associates motivation to comply with security recommendations with perceptions about security threats and perceptions of the security mechanisms. These perceptions play a significant role in motivating users to perform security measures in an organizational setting (Ifinedo, 2012; Siponen et al., 2014; Vance et al., 2012) as well as in a personal computing environment (Johnston & Warkentin, 2010a; LaRose, Rifon, & Enbody, 2008; Woon et al., 2005). Further, several studies have shown that users' overall security perception is shaped by their awareness of computer security threats (e.g., Adams et al., 1997; Bulgurcu, Cavusoglu, & Benbasat, 2010; Huang, Patrick Rau, Salvendy, Gao, & Zhou, 2011) and awareness of the available security measures (e.g., Dhamija, Tygar, & Hearst, 2006; Furnell, Bryant, & Phippen, 2007; Woon et al., 2005). A lack of computer security awareness

and a lack of knowledge of how to implement the available security measures can in turn lead to poor security practices. It is therefore important to understand how security perceptions are developed (Goodhue & Straub, 1991) and particularly important in this study which seeks to investigate how these perceptions can be modified to improve password security.

2.2.1 Awareness of security threats

As Goodhue and Straub (1991) suggest, in order to raise the level of concern for security, an appropriate level of awareness must also be reached. Woon et al. (2005) also view awareness issues as key triggers of poor security practices. They argued that if security knowledge is made accessible, users would more likely be motivated to practice security. Awareness of threats and particularly, their severity and prevalence is key to improving compliance with security policies (Siponen, Pahnila, & Mahmood, 2010).

Several studies have demonstrated how lack of awareness (Adams & Sasse, 1999; Bulgurcu et al., 2010; Huang, Rau, & Salvendy, 2008) could lead to poor security practices. For example, Adams and Sasse (1999) found a link between a lack of sufficient security threat awareness and misconceptions about what data should be classified as sensitive or confidential. The participants in their study rated personal files as sensitive while customer and financial data as less sensitive. Without guidance from the organization, users form their own perceptions that led to the users perceiving organizational security threat as low. (Adams & Sasse, 1999).

Results from an exploratory study by Huang et al. (2008) investigating IS security perceptions that different people hold, also suggest a link between awareness and users' overall security perceptions. They found that experienced computer and Internet

users, perceived security threats such as hackers and malware such as worms and viruses as most dangerous, however they rated threats such as spam significantly lower. They found that the level of awareness of the possible impact, severity and likelihood of occurrence of security threats and knowledge of threats significantly influenced the overall security perceptions. Consistent with Adams and Sasse (1999), their study also demonstrates the misconception about what is harmful and what is not. For example, although spam was shown to play a significant role in the spread of malware such as viruses in a study Kanich et al. (2008) conducted around the same period, participants in the study by Huang et al. (2008) rated spam as a significantly lower threat than malware such as viruses (Huang et al., 2008).

As a follow-up to their earlier study, Huang et al. (2011) conducted an experiment to investigate if risk perceptions can be adjusted to improve intentions to adopt security measures. Their experiment involved two groups of participants from a university in China, where one group received security information about e-banking security threats. This group formed different (higher levels) perceptions of threat, and was more likely to adopt e-banking security measures.

Bulgurcu et al. (2010) also has similar findings concerning how risk beliefs are formed. Their study, which was based on the Theory of Planned Behavior (TPB) (Ajzen, 1991), investigated how security awareness impacts on outcome beliefs about consequences of compliance or non-compliance. Based on a sample size of 464 employees from different organizations they found that awareness plays a significant role in shaping beliefs such as perceived vulnerability of threat, harmfulness of threat, and beliefs that compliance would effectively prevent security potential threats. Based on their findings, Bulgurcu et al. (2010) noted that IS security awareness programs should be designed with emphasis on these beliefs.

2.2.2 Awareness of security mechanisms

The findings of the studies discussed in Section 2.2.1 provide qualitative, exploratory, experimental, and theory grounded support for a link between security awareness, security perceptions and users' decisions to carry out security recommendations. Furthermore, the experimental study by Huang et al. (2011) provides additional insight into this relationship and shows how security perceptions can be adjusted to ultimately improve adoption of security measures. Users' decision to adopt security measures is also associated with perceived effectiveness of the security measures (Lee & Larsen, 2009; Woon et al., 2005; Zhang & McDowell, 2009), and whether users believe they can successfully execute the required security features (Johnston & Warkentin, 2010a; Woon et al., 2005). Users are however uninformed about existing security technology (Dhamija et al., 2006; Furnell, 2007; Furnell et al., 2007; Woon et al., 2005). Unfortunately a lack of understanding of the security technologies may sometimes lead to reliance on the only security options the users are familiar with (Chen, Paik, & McCabe, 2014).

Awareness of security technologies is particularly important because it plays a significant role in shaping how users perceived the available security measures (Dhamija et al., 2006; Dinev & Hu, 2007; Woon et al., 2005). Awareness of security technologies can determine whether users pay attention to the existence of important security features. For example, Dhamija et al. (2006), who analyzed large scale dataset on phishing attacks, found that users who lack basic knowledge of browser features are more likely to ignore browser warnings or security indicators such as HTTPS, which, led to successful phishing attacks.

The link between awareness and security behaviors is also shown in theory grounded studies by Woon et al. (2005) and Dinev and Hu (2007). For example, Woon et al.

(2005) who used the PMT model to explain factors that motivate users to apply wireless security features on their home computers, found those with low security knowledge and awareness of available wireless security options showed a low level of confidence in applying security measures and were also less likely to follow security recommendations. Likewise, those who applied wireless security features showed a high level of confidence in their ability to implement security measures. Consistent with Woon et al. (2005), Using a sample size of 332 IS professionals and students to test their model based on the technology acceptance model (TAM) (Davis, 1989) and TPB (Ajzen, 1991), they found awareness to be highly correlated with factors such as perceptions about the usefulness of the security technology and a user's confidence in using the system, referred to as self-efficacy (Bandura, 1982). Thus, their study also demonstrates how awareness informs key perceptions about security technologies and how this leads to improved intentions to adopt security technology.

2.2.3 The role of security awareness training

The studies discussed in Sections 2.2.1 and 2.2.2, associate awareness of security threats and awareness of security technologies, with user IS security perceptions and behavior. Of interest to this study is how to alter these perceptions to improve password security. To improve security practices, awareness of the full range of security measures is important, and one approach is to provide security awareness training to compensate for a lack of adequate security knowledge (Straub & Welke, 1998). Thus, this study considers security awareness training as a strategy for improving compliance with password security recommendations.

Users can be made aware of security threats and security mechanism through a security awareness training approach (Puhakainen & Siponen, 2010) and also by communicating the reality of threats to information is crucial to ensure behavioral

adjustments (Choi, Kim, Goo, & Whitmore, 2008; Herath & Rao, 2009). For example, in their experimental study Yan et al. (2004) found that training improves password recall and password strength Yan et al. (2004). The challenge is, IS security training is fundamentally different from other types of training in that it is persuasive in nature (Karjalainen & Siponen, 2011). For example, university education is typically descriptive and cognitive, where scientific concepts are explained with no intentions of influencing behaviors (Karjalainen & Siponen, 2011), while persuasive communication targets individuals' beliefs in an attempt to persuade them to take a specific course of action (Fishbein, 2008; Fishbein & Cappella, 2006; Rogers, 1983). As such, for IT security training to be effective, a sound theory based understanding of how to design security training is important (Karjalainen & Siponen, 2011).

A study by Johnston and Warkentin (2010a) demonstrated how theory grounded persuasive communication can be mapped into IS security training, and effectively enhance users security perceptions, and in turn improve compliance intentions. Based on PMT (Rogers, 1975, 1983), Johnston and Warkentin (2010a) designed persuasive messages highlighting, among others, the dangers of spyware and potential consequences, and found that user intentions can be influenced by using persuasive messages. Similarly, Jenkins et al. (2013) also used PMT based persuasive messages that warned users against reusing passwords and highlighted the high risk of hacking associated with password reuse. This improved perceptions about the probability of a threat occurrence and their perceptions about the effectiveness of the recommended response, which significantly influenced their password choices. These studies illustrate how IS security perceptions can be shaped using theory grounded persuasive messages, ultimately improving security practices.

Based on works discussed in Section 2.1, the research described in this thesis is centered on security perceptions as a key predictor of security behavior and is based on the premise that these perceptions can be altered using training that incorporates information on existing security threats and preventative measures.

2.3 Theoretical background

This section reviews several competing theories considered prior to selecting a theoretical framework for this study. Examining behavioral change is of importance to this study, therefore an established theory that can enable experimental verification was sought. The following section presents background information, key components, limitations and applicability of theories relevant to this study.

2.3.1 Competing theories

Four widely used and comprehensive protective behavior theories, as reviewed by Prentice-Dunn and Rogers (1986) and Weinstein (1993), were initially considered for this study. The Health Belief Model (HBM) (Janz & Becker, 1984; Rosenstock, 1974), the Subjective Expected Utility (SEU) model (Ronis, 1992), the Theory of Reasoned Action (TRA) (Ajzen & Fishbein, 1980; Fishbein & Ajzen, 1975) and the PMT model (Rogers, 1975, 1983). These models have been used to explain protective behaviors from a perceived threat and threat severity perspective (Weinstein, 1993), although the specific variables considered in the models vary.

2.3.1.1 Health belief model

Developed out of frustration over a lack of participation in a free disease screening program, the HBM (Janz & Becker, 1984; Rosenstock, 1974) was established as a framework for explaining why people lacked motivation to take a free screening test (Janz & Becker, 1984). The original framework (Rosenstock, 1974), suggests that

peoples motivation to take precautions against a disease is dependent upon their perceived susceptibility to an illness and their perception of the severity of the illness. An individual would also weigh whether undertaking the precautions is beneficial, and assess the barriers associated with taking the precautions. At a later stage, HBM was extended to incorporate self-efficacy beliefs (Rosenstock, Strecher, & Becker, 1988), thus accounting for how an individual's belief about the ability to successfully execute the recommended precautions influences their preventative behavior.

Although HBM has been applied in the IS security domain (e.g., Claar, 2011; Ng, Kankanhalli, & Xu, 2009), one drawback is that evidence supporting its usefulness in predicting IS security behavior is lacking. By drawing similarities between preventative behavior related to health threats and preventative behavior related to computer security threats, Ng et al. (2009) proposed a HBM model to investigate factors that motivate employees to take precautions as a preventative measure against email threats. Using 134 part-time working students as a surrogate for employees, they only found perceived susceptibility, perceived benefit, and self-efficacy, to be associated with motivation to take email precautions. Likewise, the thesis by Claar (2011) examining factors that drive home users to implement security software, found support for relationships between perceived susceptibility, self-efficacy, perceived barrier, and user intentions to implement security software.

Another drawback is while HBM is useful for predicting correlational relationships between variables, how these variables could be manipulated to elicit behavioral change is unclear (Floyd, Prentice-Dunn, & Rogers, 2000). Thus, it is limited in its ability to provide experimental verification (Prentice-Dunn & Rogers, 1986). Given that the research described in this thesis seeks to investigate factors that influence users' compliance intentions, and particularly how these factors can be altered to

engender change in compliance with password guidelines, HBM was deemed unsuitable for this study.

2.3.1.2 Subjective expected utility

Another model considered for this study is the SEU model (Ronis, 1992). SEU is an mathematical framework that was originally developed to explain why people would choose to risk a sum of money in a flip coin game with infinite odds (Schoemaker, 1982). SEU holds that when people face a risk related decision they assess the desirability (expected utility) of all available alternate actions, and chose the action with the most desirability. For example, the benefits of taking health precautions, that is reduced chance of an illness, would be considered desirable. As the action with the most desirability would be chosen, perceived benefit would increase the likelihood of taking precautions (Ronis, 1992).

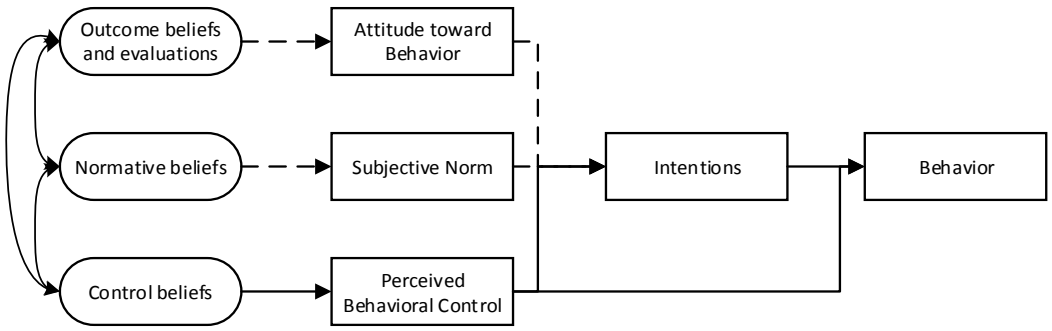
The SEU has two notable drawbacks relevant to this study. One is that SEU does not explicitly describe which beliefs are applicable to a given decision (Weinstein, 1993), and therefore works better as an integrated model (Ronis, 1992). For example, SEU can be integrated with theories such as HBM that are more specific about what risk beliefs are relevant to preventative health behavior (e.g., Ronis, 1992), or as was the case in the IS security study by Peace, Galletta, and Thong (2003) it can be integrated with TRA/TPB and Deterrence Theory. It, therefore, appears that by itself, SEU lacks a strong basis for predicting IS security behavior. Furthermore, as suggested by Mathieson (1991), when a model does not specify the relevant variables, a costly implementation process of identifying relevant variables may be needed, and therefore SEU would potentially be costly for this study.

2.3.1.3 Theory of reasoned action

The development of the TRA model came about as a result of a lack of consensus on the structure and role of attitudes in explaining human behavior (Ajzen, 2012). This was partly due to weak correlations observed in numerous studies between attitudes and behavior, suggesting that perhaps attitudes was not the main driver of behavior. The prevailing viewpoint was that attitude is a multidimensional construct, represented by different aspects of beliefs. However, Fishbein argued that attitude is a unidimensional independent construct that is determined by beliefs. Subsequently, Fishbein and Ajzen (1975) teamed up and developed a framework for explaining human behavior, and a model that also provides a better understanding of the role of attitudes.

They started with the assumption that an individual's intentions determine behavior, making intention the primary predictor of behavior. They identified two independent constructs, attitudes towards behavior and subjective norm, as the key determinants of intentions. TRA, shown in dotted lines in Table 2.1, suggests that outcome beliefs such as evaluations of whether the outcomes of the behavior will be of benefit, is what shapes people's attitudes, this in turn informs their intentions. Likewise, normative beliefs such as social pressure to perform the behavior shapes subjective norm that in turn influences people's intentions.

Figure 2.1: Theory of Reasoned Action/Theory of Planned Behavior (Ajzen, 1991)



One limitation of TRA is it does not account for when people have limited control over a behavior in question, such as lack of resources or skills to perform the behavior. Consequently, TRA was extended to address this limitation by incorporating the concept of self-efficacy, based on Bandura's work on self-efficacy expectancy (Bandura, 1977). In the extended TRA, named the Theory of Planned Behavior (TPB) (Ajzen, 1991) self-efficacy was represented as perceived behavioral control (PBC) and was incorporated in the model as a third independent construct. Control beliefs, such as perceived obstacles, available resources or difficulty in undertaking a given course of action determine an individual's PBC. Ajzen (1991) proposed that in addition to determining behavioral intentions, PBC also plays an active role in influencing human behavior. Thus, PBC is the only belief factor not mediated by attitudes, and is purported to have a direct impact on intentions and behavior as well. In this review, the two models are represented as TRA/TPB (see Table 2.1).

While studies have successfully used TRA/TPB to explain adoption of IT technologies and IS security behaviors, the model carries two notable limitations of interest to this study. The first is partly attributable to its generality, as a model for explaining a wide range of human behaviors (Mathieson, 1991). TRA/TPB was originally developed to explain general behaviors (Weinstein, 1993). In fact, in its inception the model was tested by investigating the association between beliefs and attitudes towards African American people (Ajzen, 2012), and the first application of the complete TRA model (Fishbein & Ajzen, 1981) was used to explain voting behavior. TRA/TPB can, nonetheless, be used to explain health-related preventative behaviors (Fishbein, 2008). However, TRA/TPB omits relevant beliefs, such as perceived effectiveness of the recommended preventative measures (Weinstein, 1993), which play a significant role in IS security practices. Further, emotions and perceptions about risks which are not

explicitly defined, are considered an individual difference variable with indirect effect on behavioral intentions (Ajzen, 1991; Fishbein, 2008).

Nonetheless, TRA/TPB has been successfully used to explain behavior related to IS security, however without the relevant risk and response variables, on its own the model may require a costly implementation process such as the need for a pilot test to identify belief outcomes, relevant normative beliefs or control factors (Mathieson, 1991). Thus, IS security studies (e.g., Anderson & Agarwal, 2010; Ifinedo, 2012; Siponen et al., 2014; Siponen et al., 2010; Zhang, Reithel, & Li, 2009) have had to incorporate risk based theories.

In IS security research (e.g., Dinev & Hu, 2007; Herath et al., 2014; Johnston & Warkentin, 2010b; Lee & Kozar, 2008; Lee & Larsen, 2009), TRA/TPB has also been integrated with technology adoption models such as the TAM (Davis, 1989). Based on TRA, Davis (1989) developed TAM to better understand factors that influence technology adoption. However, as factors considered when contemplating adopting security protective technologies such as anti-spyware differ from those considered in the adoption of technologies such as productivity software, traditional technology adoption theories are inadequate in explaining IS security behaviors (Liang & Xue, 2009). It is of interest to note that, although TAM is said to be a better predictor of technology acceptance than TRA/TPB (Mathieson, 1991), TAM was not considered in this study because it is more useful in explaining technology acceptance (Mathieson, 1991), as opposed to explaining use of protective technology which involves a threat element (Dinev & Hu, 2007).

The second limitation relates to persuasive communication, which can be applied within the TRA/TPB framework as a strategy for behavioral change (Fishbein & Ajzen, 1975). However, the model does not adequately describe how persuasive

messages can be used to target specific beliefs (Fishbein, 2008; Fishbein & Cappella, 2006). Because of this limitation, Fishbein and Cappella (2006) suggested that a theory grounded in communication theory would be more appropriate for designing persuasive communication. Therefore, PMT was chosen for this study. The following sections provide the rationale for selecting PMT and a detailed description of the PMT model and its applicability to this study.

2.3.2 Protection motivation theory

PMT was chosen not under the assumption that it is the best protective behavioral theory available. Rather, PMT was selected as it is a useful tool for examining behavioral change using persuasive communication (Weinstein, 1993), and describing how persuasive communication can be effectively designed (Rogers, 1975, 1983).

PMT was developed as a model for predicting behavioral change through persuasive communication, also referred to as fear appeals (Rogers, 1975, 1983). Early research viewed fear appeals as a composite construct and as a result, the operationalization of fear appeals varied. This made it difficult to compare experimental studies, and to determine what component produced the observed behavioral change. As such, Rogers (1975) established a comprehensive fear appeals framework and identified key stimulus variables that facilitate behavioral change. He concluded that fear appeals are a multidimensional construct consisting of independent stimulus variables that can be distinctively framed within a fear appeals message to target specific perceptions.

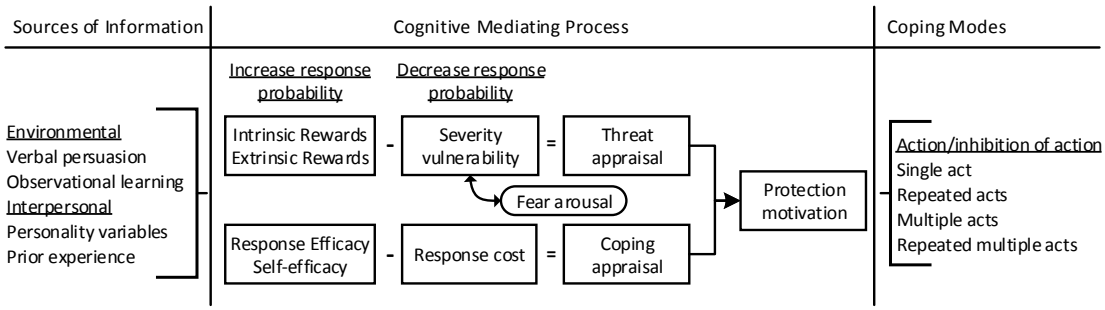
Rogers (1975) identified three independent stimulus variables: magnitude of noxiousness, probability of threat occurrence and efficacy of available recommended response. An individual's perceived severity of threat, perceived susceptibility to threat and perceived efficacy of the recommended response develop from a cognitive

mediational process that involves appraisal of the information about magnitude of noxiousness, probability of occurrence and efficacy of the response. In turn, these perceptions have an impact on protection motivation. In PMT, protection motivation is synonymous with, and measured as, behavioral intentions (Rogers, 1983).

Excluded from the earlier persuasive communications theories (Rogers, 1983) is the concept of self-efficacy, described as the belief that one is capable of carrying out the recommended response. Leventhal (1970) proposed a similar concept, although it was not referred to as self-efficacy at the time. Leventhal proposed that persuasive communication should incorporate instructions on how to execute a behavior in question. Bandura (1977, 1982) suggested that self-efficacy can be developed through vicarious experiences such as finding out how others perform or actually performing the activity. Persuasion such as suggestions aimed to persuade individuals to believe that they are capable of performing a given task can also shape an individual's self-efficacy beliefs. Ultimately, an individual's perceived self-efficacy is influenced by the interpretation of the persuasive information (Bandura, 1977, 1982).

Following Bandura's work on self-efficacy (Bandura, 1977, 1982), Rogers (1983) explored the possibility of extending PMT to incorporate self-efficacy. Rogers teamed up with Maddux (Maddux & Rogers, 1983) to verify the role of self-efficacy by experimentally manipulating self-efficacy using fear appeals and found self-efficacy to have a significant influence on behavioral intentions. They therefore included self-efficacy as a key PMT variable. In addition, the revised PMT was intended to provide a more comprehensive model (Rogers, 1983), including additional variables such as perceived rewards and costs associated with the recommended response. Figure 2.2 is a representation of the PMT framework as presented in the work by Rogers (1983, p. 168).

Figure 2.2: Protection Motivation Theory (Rogers, 1983)



2.3.2.1 Threat appraisal: applicability to this study

Two independent constructs predict protective behavior: threat appraisal and coping appraisal. Threat appraisal refers to an individual's appraisal of the magnitude of noxiousness and probability of threat occurrence, following fear appeals communication, which leads to form beliefs about the consequences of the threat, represented as perceived severity and beliefs about the likelihood of occurrence, represented as perceived vulnerability (Prentice-Dunn & Rogers, 1986).

The impact of perceived severity and perceived vulnerability on behavioral intentions is further mediated by an intervening variable, fear, described as an emotional feeling toward threat (Rogers, 1983). However, fear, often described as fear arousal, is purported to have an indirect impact on intention. Thus, PMT assumes that fear can produce change in attitudes and behavioral intention but only indirectly through perceived severity and perceived vulnerability. Fear was therefore incorporated in the revised PMT model but as an indirect determinant of protection motivation, but as a function of perceived severity and perceived vulnerability. Therefore, this study considers fear as a function of perceived severity and perceived vulnerability that in turn have a direct influence on behavioral intentions.

2.3.2.2 Fear arousal: applicability to this study

In other key persuasion theories, the role of fear as purported varies slightly (Rogers, 1983). For example, the Drive Model (Janis, 1967) suggests that rather than having a direct influence on behavior, fear drives people to reduce emotional feeling towards threat. It is from this reduced emotional state that behavioral change is experienced. However, the key difference between the Drive Model and other persuasion theories (Rogers, 1983), is the hypothesized inverted-U-shaped association with behavior. Janis (1967) suggests that fear arousal has a positive effect up to a certain point: the top of the inverted-U. This is the optimum arousal point where maximum motivation is experienced. Exceeding this point of fear arousal, according to Janis (1967), decreases the effects of fear on behavior. However, there has been little data supporting the inverted-U relationship and thus the model has been widely rejected (Rogers, 1983).

Another opposing view on the role of fear is that proposed by the Parallel Process Model (PPM) (Leventhal, 1970) whereby fear control (emotional response to threat) and threat control (cognitive response to threat) are viewed as completely independent. While PPM suggests that behavior is predicted solely by cognitive response to threat, the revised PMT (Rogers, 1983) assumes that both emotional and cognitive response to threat play a significant role in predicting behavior. However, Roger's (1975) original position supports this viewpoint, and therefore excluded fear as a key variable, until later when it was incorporated into the revised PMT (Witte, 1992).

Motivation through fear arousal has received some support, and while some studies (e.g., Liang & Xue, 2010; Zhang & McDowell, 2009) have found a direct link, results in other studies (e.g., Maddux & Rogers, 1983; Rippetoe & Rogers, 1987; Witte, 1994) reveal an indirect link. Further, Witte (1992) investigated the possibility of redefining the role of fear by incorporating fear in an extended PPM model (Extended PPM).

Following a study conducted to validate the proposed EPPM (Witte, 1994), the findings revealed an indirect relationship between fear and intentions, as well as fear and behavior, as purported in the PMT model. It is of interest to note that, while EPPM borrows, in part, from the original PMT (Maloney, Lapinski, & Witte, 2011), it also incorporates a message rejection component intended to explain how individuals control fear. As message rejection is not the focus of this study, Witte's EPPM (1994) was not considered in this study.

Though limited, some evidence (e.g., Liang & Xue, 2010; Zhang & McDowell, 2009) suggest that fear may also have a direct influence on behavioral intentions, and as recommended by Johnston and Warkentin (2010a) this link should be explored more in IS security studies. Thus, this study also considers the role of fear on compliance with password guidelines.

2.3.2.3 Coping appraisal: applicability to this study

Coping appraisal represents an individual's assessment of the information on the efficacy of the recommended response and appraisal of the ability to perform the recommended response. This in turn develops into perceptions about the effectiveness of the recommended measures, represented as response efficacy and perceptions about an individual's ability to perform the response, referred to as self-efficacy.

While response efficacy and self-efficacy increase behavioral intentions, response cost is purported to decrease the likelihood that an individual will carry out the recommended response. Response cost, which follows an individual's assessment of the costs associated with the available preventative measures, relates to beliefs about the difficultly, inconvenience, unpleasantness, or the amount of effort needed to implement the recommended response (Prentice-Dunn & Rogers, 1986; Rogers, 1983). Coping appraisals factors have been found to be strong predictors of behavioral

intentions (e.g., Floyd et al., 2000; Milne & Milne, 2000). Therefore, this study considers the role of all three coping appraisal factors in predicting compliance with password guidelines.

2.3.2.4 Rewards: applicability to this study

Rewards, was incorporated in the revised PMT model (Rogers, 1983) to account for beliefs about the benefits of ignoring the recommended behavior and is purported to decrease the likelihood of adoption. However only a few health-related studies have exclusively tested rewards (Norman, Boer, & Seydel, 2005; Rogers & Prentice-Dunn, 1997). There have also been only a few IS security studies that have considered rewards (Siponen et al., 2014; e.g., Siponen et al., 2010; Vance et al., 2012), and these have examined the role of rewards in an organizational setting.

This may be attributable to the similarity between the two constructs. Rewards and response cost are two independent constructs where the benefits, that is the pleasure of disregarding a given preventative measure has a negative effect on behavior, while the costs associated with a given preventative response are also said to have detrimental effects on behavior. Abraham, Sheeran, Abrams, and Spears (1994) suggested that the two variables could be operationalized as a single construct. For example, that the measures of the construct rewards be morphed into response cost by rewording from "increased pleasure" to "reduced benefit" (response cost). Given the possible similarity between the two constructs, this study did not consider the role of rewards.

2.3.3 Applications of PMT in health-related research

Originally developed as a model for predicting health-related protective behaviors, PMT is useful in predicting correlational relationships between key variables and behavioral intentions (Weinstein, 1993). As a framework for designing persuasive

communication, PMT is also useful in experimental research (Prentice-Dunn & Rogers, 1986). Correspondingly, PMT studies have taken either an experimental or correlational approach to predicting behaviors (Norman et al., 2005). Experimental studies typically involve the use of fear appeals to manipulate key PMT variables, examining effectiveness in facilitating behavioral change, and also testing correlational relationships using experimental data. Correlational studies involve testing correlational relationships in a proposed PMT model or an extended version of the PMT model using survey data.

In the health domain, PMT has been applied to a variety of health-related conditions in the areas of disease detection and screenings (e.g., de Nooijer, Lechner, Candel, & de Vries, 2004; Hodgkins & Orbell, 1998; Rippetoe & Rogers, 1987) or prevention techniques such as exercising or vaccination (e.g., Abraham et al., 1994; Brewer et al., 2007; Maddux & Rogers, 1983; Milne, Orbell, & Sheeran, 2002; Norman et al., 2005; Plotnikoff & Higginbotham, 2002; Wurtele & Maddux, 1987). Health-related PMT research can also be categorized as experimental (de Nooijer et al., 2004; Maddux & Rogers, 1983; Milne et al., 2002; Norman et al., 2005; Oenema, Tan, & Brug, 2005), or correlational (Abraham et al., 1994; Hodgkins & Orbell, 1998). Although the PMT model does not provide a utility for predicting future behavior (Milne & Milne, 2000), some studies (e.g., de Nooijer et al., 2004; Milne et al., 2002; Norman et al., 2005; Oenema et al., 2005; Wurtele & Maddux, 1987) have managed to successfully predict behavioral intentions and behaviors in longitudinal studies.

2.3.4 Applications of PMT in IS security research

By drawing similarities between preventative behavior related to health threats and preventative behavior related to computer security threats, PMT has been successfully used to explain IS security behaviors in a variety of IS security areas. For example,

within an organizational setting (e.g., Crossler, Long, Loraas, & Trinkle, 2014; Herath & Rao, 2009; Ifinedo, 2012; Lee & Larsen, 2009; Siponen et al., 2014; Siponen et al., 2010; Vance et al., 2012) or in relation to personal IS security such as home computer protection or online password security (e.g., Anderson & Agarwal, 2010; Crossler, 2010; Johnston & Warkentin, 2010a; Liang & Xue, 2010; Milne, Labrecque, & Cromer, 2009; Woon et al., 2005; Zhang & McDowell, 2009). Table 2.1 summarizes the applications of PMT in IS security research.

Table 2.1: Applications of the Protection Motivation Theory in IS security research

Summary of applications of Protection Motivation Theory in IS security research					
Study	**Theoretical Background**	**Target Behavior & Context**	**Dependent Variable**	**Purpose of study and key findings related to PMT variables**	**Sample (valid)**
Experimental studies					
Jenkins et al. (2013)	PMT Fear appeals	Create unique passwords; online web accounts	Actual Behavior (actual unique passwords)	**Purpose:** Investigate ways to discourage password reuse **Strategy:** Used Fear Appeals to manipulate all PMT variables except self-efficacy **Findings:** Their data revealed that 88% of those who received fear appeals created unique passwords, compared with only 4.5% of those who did not	135 university students 2 study groups
Vance et al. (2013)	PMT Fear appeals	Create strong passwords; online web accounts	Actual Behavior (actual password strength)	**Purpose:** Examine if fear appeals can improve password strength and effectiveness of interactive fear appeals **Strategy:** Used Fear Appeals to manipulate perceived severity and vulnerability, self-efficacy, response efficacy **Findings:** Fear appeals have an impact on password strength. Further, those who received interactive fear appeals created significantly stronger passwords	354 web users from 65 countries 3 study groups
Johnston & Warkentin (2010)	PMT Fear appeals	Use anti-spyware software; personal computer environment	Intentions	**Purpose:** Investigate if fear appeals do influence user intentions to comply with recommended security measures **Strategy:** Used Fear Appeals to manipulate perceived severity and vulnerability, self-efficacy, response efficacy **Findings:** Fear appeals successfully elicited change in perceptions that ultimately influenced intentions to apply anti-spyware security measures.	275 university staff and students 3 study groups
Herath et al. (2014)	PMT TTAT	Adopt email authentication	Intentions	**Purpose:** Examines factors that drive users to use an email authentication service, after a 2 month trial period	186 at time1; 134 at time 2 two months;

Summary of applications of Protection Motivation Theory in IS security research					
Study	**Theoretical Background**	**Target Behavior & Context**	**Dependent Variable**	**Purpose of study and key findings related to PMT variables**	**Sample (valid)**
	TAM	service; online email services		**Strategy:** Provided a 2 month training **Findings:** User intention to adopt email authentication service is predicted by email-related risk perceptions, self-efficacy and attitudes towards the email service	Undergraduates from a US university. 1 group
LaRose et al. (2008)	PMT ELM Persuasive messages(SCT)	Adopt security measures such as firewalls, anti-virus, anti-spyware; home Internet use	Intentions	**Purpose:** Investigate ways to motivate internet users to take personal responsibility and take internet safely measures **Strategy:** Used persuasive messages to manipulate personal responsibility **Findings:** Personal responsibility, response efficacy and self-efficacy were found to be the best predictors of online security behavior	206 students 4 study groups
Correlational studies					
Crossler et al. (2014)	PMT	Comply with BYOD policies; organization	Intentions Actual compliance (self-reported coded as 1/0 binary)	**Purpose:** Investigate factors that influence employees' decisions to comply with BYOD policies **Findings:** Only self-efficacy and response efficacy had a significant impact on intentions.	250, accounting and non-accounting college students and white collar employees
Crossler (2010)	PMT	Adopt data backup measures; personal computer	Actual Behavior (self-reported)	**Purpose:** Examine factors that drive users to back up data on their own personal computers **Findings:** response efficacy and self-efficacy increases the frequency of data backups. Interestingly, perceived severity and perceived vulnerability were found to have a negative impact on intentions.	112, small business employees, graduate students and private citizens
Anderson & Agarwal (2010)	PMT TPB	Adopt security precautions; home computer	Intentions, mediated by attitude towards security measures	**Purpose:** To explain factors that motivate users to secure their own computers and the internet at their home. **Findings:** Concern for security threats, response efficacy and self-efficacy influences attitude towards security measures. Favorable attitude towards security measures increase adoption intentions	594 home computer users
Vance et al. (2012)	PMT TH	Comply with security policies	Intentions	**Purpose:** Examine factors that influence IS security compliance and the role of habit in shaping these factors. Habit is based on PMT's assumption	210 participants from one municipal

Summary of applications of Protection Motivation Theory in IS security research					
Study	**Theoretical Background**	**Target Behavior & Context**	**Dependent Variable**	**Purpose of study and key findings related to PMT variables**	**Sample (valid)**
		related to locking PCs, sharing passwords, etc; organizational		that prior experience is an antecedent to threat and coping appraisals **Findings:** Prior habit was found to be influence all threat and coping appraisal factors. All hypothesized relationships were supported with the exception of perceived vulnerability and intentions	in Finland
Siponen et al. (2014)	PMT TRA CET	Adherence to information security policies; organizational	Intentions Actual compliance (self-reported)	**Purpose:** Develop an integrated theory to explain adherence to information security policies **Findings:** Perceived severity, perceive vulnerability and self-efficacy are associated with compliance intentions. The link between intentions and actual compliance was very highly correlated.	669 employees from four different organizations in Finland
Siponen et al. (2010)	PMT TRA GDT IDF	Compliance with security policies; organizational	Intentions Actual compliance (self-reported)	**Purpose:** Proposed an integrated model for explaining factors that drive employee to follow security policies. **Findings:** Threat appraisal, operationalized as a single construct consisting of perceived severity and vulnerability items, intentions to comply. Self-efficacy also plays a significant role	917 employees from several Finnish organizations
Liang & Xue (2010)	PMT TTAT	Motivation to avoid malicious technology; personal computer	Intentions Actual behavior (self-reported)	**Purpose:** To test a previously developed PMT based TTAT model, a framework for testing avoidance of malicious technology. **Findings:** Perceived threat is a function of both perceived severity and perceived vulnerability. Perceived threat has positive impact on motivation. No direct link between perceived severity and perceived vulnerability and motivation, but their effect is mediated by perceived threat. Coping appraisals play a significant role on motivation.	152 business students from a major US university
Woon et al. (2005)	PMT	Adoption of wireless security measures; home network	Actual Behavior (self-reported using yes/no binary measure)	**Purpose:** Use PMT to examine factors that predict adoption of wireless security measures on home computers **Findings:** Their study found support for all hypothesized direct relationships except for the relationship between perceived vulnerability and adaption of recommended behavior.	189 home computer users who own a wireless network at their home, recruited from a large university
Ifinedo (2012)	PMT TPB	Compliance with security policies;	Intentions	**Purpose:** Investigate factors influencing intentions to comply with organizational IS security policies	124 IS professional and business

Summary of applications of Protection Motivation Theory in IS security research					
Study	**Theoretical Background**	**Target Behavior & Context**	**Dependent Variable**	**Purpose of study and key findings related to PMT variables**	**Sample (valid)**
		organizational		**Findings:** All PMT variables with the exception of response cost had a significant impact on intentions. However, perceived severity had a significant but negative impact on intentions. Contrary to numerous other studies, self-efficacy had the weakest effect on intention.	managers
Herath & Rao (2009)	PMT DT	Compliance with security policies; organizational	Intentions, mediated by attitude towards security policy	**Purpose:** Conduct a field study of employee intentions to comply with security policies. Similar to Woon et al. (2005), proposes no direct link between threat severity and threat probability to intentions. Proposes that attitudes mediate the effects of threat concern, self-efficacy, Response efficacy and response cost on intentions **Findings:** Threat concern is a function of threat severity and threat probability. Although threat concern, self-efficacy, response efficacy and response cost all had a significant impact on attitudes towards organizational security policy, attitude has no direct impact on intentions.	312 participants from 78 organizations in the western areas of New York, USA
Lee & Larsen (2009)	PMT TAM	Adoption of anti-malware software; organizational	Intentions Actual adoption (purchase of anti-malware software y/n)	**Purpose:** Investigate factors that influence SMB executives' decision to adopt anti-malware software. Also examines if those in IT intensive industries differ from those in non-IT intensive industry **Findings:** All PMT variables that is threat appraisal and coping appraisal factors play a significant role in SMB executives' decision to adopt anti-malware software. However, effect of perceived vulnerability was weak. IS experts are influenced more by threat appraisal, while non-IS experts are influenced by coping appraisal.	239 U.S SMB executives form various industries including finance, construction, healthcare, government, retail, manufacturing and educational services
Workman et al. (2008)	PMT	Non-compliance with security recommendations such as data backup, password protection, anti-virus updates; organizational	Actual behavior (self-reported) and; (observed computer logs of e.g. password changes etc.)	**Purpose:** Test a proposed, PMT based, Threat Control model. To explain why users, who are familiar with IS security policies, choose to omit security precautions. Proposes a cost/benefit measure of response cost. **Findings:** Higher levels of perceived severity and vulnerability, self-efficacy and response efficacy significantly reduce the likelihood of non-compliance with security recommendations. Those who perceive that the benefits associated with compliance outweigh the cost are also less likely to ignore security recommendations	To recruit those who are familiar with IS security policies, 588 employees from a technology oriented organization

Summary of applications of Protection Motivation Theory in IS security research					
Study	**Theoretical Background**	**Target Behavior & Context**	**Dependent Variable**	**Purpose of study and key findings related to PMT variables**	**Sample (valid)**
Posey et al. (2011)	PMT	Protect organization's information assets using measures such as protecting; sensitive information, computer; organizational	Intentions Actual behavior (self-reported)	**Purpose:** Investigate factors that motivate insiders (employees) to protect their organization's information assets. Also, proposes fear as a predictor of protection motivation in an organizational setting. **Findings:** Intrinsic rewards and coping appraisals significantly influence insiders' protection motivation. Response efficacy is the strongest predictor. Coping appraisal is a better predictor than threat appraisals. Fear is a function of perceived severity and perceived vulnerability, but has no significant influence on employees' decision to protect their organization's information assets.	380 insiders from various organizations and industries in the US
Milne et al. (2009)	PMT SCT	Motivation to practice risky and safe online practices; consumer internet use	Actual risky behavior Actual protective behavior (self-reported)	**Purpose:** Examine factors that drive online consumer to take action that either put them at risk or action that protects their information. In particular, the degree to which threat perceptions and self-efficacy contribute to online consumers' Internet security practices. **Findings:** Risky behavior was not impacted by perception of online threat or perceived likelihood of online threats. Protective behavior was not impacted by perceived likelihood of online threats, though the effect was reported as weak at $p<0.1$. Self-efficacy did decrease the likelihood of risky behavior and also had a positive impact on protective behavior.	449 online shoppers recruited from the US
Zhang & McDowell (2009)	PMT	Intentions to use strong password; variety of online accounts (e.g. email, social networking accounts)	Intentions	**Purpose:** To test a PMT based model adapted to explaining online password security. Self-efficacy was excluded from the model **Findings:** Coping appraisal factors, response efficacy and response cost were found to have a significant impact on intentions. Fear, also has a significant impact on intentions to create strong passwords.	182 students from three universities in southern US
PMT = Protection Motivation Theory; TTAT = Technology Threat Avoidance Theory; TAM = Technology Acceptance Model; SCT = Social Cognitive Theory ; ELM = Elaboration Likelihood Model; TPB = Theory of Planned Behavior; CET = Cognitive Evaluation Theory; GDT = General Deterrence Theory; IDF = Innovation Diffusion Theory; DT = Deterrence Theory; TH = Theory of Habit;					

In several experimental studies (e.g., Jenkins et al., 2013; Johnston & Warkentin, 2010a; Vance et al., 2013), PMT is shown to be useful in designing IS security fear appeals communication. These studies have also shown how persuasive communication can be mapped into a security awareness communication by targeting specific IS threat perceptions and efficacy perceptions, and found fear appeals to be effective in enhancing security practices. However, theory based IS security training research is limited (Puhakainen & Siponen, 2010). Therefore, this research should contribute to a growing but much needed body theory grounded work on the efficacy of fear appeals in IS security research.

The applications of the PMT model in IS security research, can also be categorized as either experimental or correlational, with most studies being of a correlational design (see Table 2.1). The following section is therefore divided into two major sections. Section 2.3.4.1, reviews experimental studies involving a direct manipulation of all or part of the key PMT variables. Section 2.3.4.2, focuses primarily on correlational studies involving part or all of the key variables described in the PMT model.

2.3.4.1 Experimental studies

According to Rogers (1983), for persuasive communication to be effective, all four key components must be addressed in a fear appeals message. While only a few IS security applications of PMT have used an experimental design, only Johnston and Warkentin (2010a), one of the works that has influenced this research, used fear appeals directed at all four key variables. Further, although the research by Herath et al. (2014) and LaRose et al. (2008) are experimental studies (see Table 2.1), they were omitted in this review as they are unrelated to PMT based fear appeals. For example, the study by LaRose et al. (2008) used persuasive messages with emphasis on personal responsibility, as described in the Social Cognitive Theory, while the study by Herath

et al. (2014) did not involve any group treatments or manipulation of the PMT variables. While the literature on fear appeals in IS security is lacking, as evidenced by the PMT studies summarized in Table 2.1, some evidence support their applicability in IS security training and their effectiveness in improving compliance with security recommendation.

Jenkins et al. (2013), for example, examined if fear appeals could be used to improve password security using messages intended to dissuade users from reusing passwords. They asked 135 participants to create an account and a password of their choice on a website designed specifically for their study. The participants were then required to create a new password, with some randomly assigned to a treatment group with fear appeals set to appear on the screen as they typed their new passwords. They designed an algorithm to detect reused password and triggers a fear appeals message, warning the participants against reusing passwords. Targeting perceived severity and vulnerability, the message warned of the high risk of hacking. The message also provided a recommendation to choose a unique password as a way of protecting their account, hence targeting response efficacy. Interestingly, the message excluded self-efficacy statements, such as suggesting how to create multiple passwords that are unique, strong and easy to remember. This was a critical omission as users are typically expected to create passwords for other websites (Helkala & Svendsen, 2012), and as noted by Jenkins et al. (2013) was a limitation in their study.

Nevertheless, their results revealed that 88% of those who received fear appeals created unique passwords, compared with only 4.5% of those who did not. They also examined the effects of fear appeals on perceptions about severity, vulnerability, response efficacy and self-efficacy. Considering that the fear appeals message omitted the self-efficacy component, it is unsurprising that the fear appeals messages had no

impact on the participants' self-efficacy. Jenkins et al. (2013) suggest that adding statements about techniques for creating unique passwords would have possibly influenced self-efficacy. Thus, although they successfully thwarted attempts to reuse passwords by significantly decreasing the potential numbers of reused passwords, it is unclear if this outcome would apply in other websites.

In addition, their study omitted a measure of password strength, which as Jenkins et al. (2013) indicated, was another notable limitation in their study where the effects of fear appeals on password strength are unknown. Conversely, in another experimental study by Vance et al. (2013), which included measures of password strength, fear appeals were shown to have an impact on password strength. In their study, they also investigated whether the effectiveness of fear appeals differed when presented as interactive messages or as static messages. They randomly assigned 354 web users from 65 countries to a control group that received only a password strength meter and two treatment groups, one which received interactive and another which received static fear appeals. While, the group that received interactive fear appeals created significantly stronger passwords, the results showed no difference in password strength between the group that received static fear appeals and the control group. This suggests that the interactive fear appeals were significantly more effective than the static fear appeal messages.

This finding contradicts the position of Jenkins, Durcikova, and Burns (2012) that static IS security training can significantly improve password practices. They conducted a study to compare the effectiveness of media rich training materials containing a narrated video, and the efficacy of static training materials. The static training materials had a significant impact on password practices. One advantage of using static training materials, as Jenkins, Durcikova, and Burns (2012) suggest, is that

they do not cognitively overload the user. As persuasive communication is already initiating a process of cognitive assessment of the information at hand (Rogers, 1983), it would seem more logical to use static training material.

A notable omission in the study by Vance et al. (2013), is they failed to indicate if the fear appeal messages had any impact on the individual PMT variables. Although the study also aimed to manipulate the four key PMT variables using fear appeals, there seems to be no explanation of the effects of the fear appeals on the levels of threat severity, vulnerability, response efficacy and self-efficacy perceptions. This information, as alluded in Roger's (1983) reference to the importance of manipulating all four key components of fear appeals, may have been useful in identifying what component of the static fear appeals was problematic.

Johnston and Warkentin (2010a) provided empirical data from 275 university staff and students supporting the use of fear appeals, in static format. They supplied fear appeals to users who were largely responsible for applying security measures on their university computers, and examined if the fear appeals messages would influence their severity and vulnerability perceptions, response efficacy and self-efficacy perceptions, and explored the effect on security practices. The fear appeals contained information on: the potential consequences of spyware, such as identity theft; statistics alluding to a prevalence of spyware threats; statements supporting the effectiveness of anti-spyware software; and information regarding the effort needed install the software thus pertaining to the efficacy of the participants. They found that fear appeals can elicit change in perceptions and intentions to apply anti-spyware security measures.

Though the evidence is limited, the studies reviewed in this section provide some experimental evidence supporting the use of fear appeals within the IS security domain. However, the drawback is that the available evidence supports only the

immediate effects of the fear appeals, while the long-term effects are unknown. As such, future research should explore the extent to which the effects of fear appeals persist. In fact, as Shepherd, Mejias, and Klein (2014) show the effects of persuasive communication can decline over time, particularly when mild messages are used.

A longitudinal study by Shepherd et al. (2014), where a form of persuasive communication was used in an attempt to reduce Internet abuse by employees, revealed that when mild acceptable use policies (AUP) messages were used, the effects were maintained for a brief period of time. Their study also examined the effectiveness of more severe deterrence theory-based AUP messages that emphasized the severity of sanctions. The severe AUP messages were more effective over a longer period compared with the mild AUP messages. While their study used a different theoretical approach from the research proposed in this thesis, the findings indicate that while persuasive communication can be effective, a follow-up study can provide further insight into the effectiveness of these messages in the long term.

Based on the findings in the studies reviewed in this section, static fear appeals were used in this study and as proposed by Rogers (1983), all four key PMT variable were manipulated. Furthermore, to address the research question relating to whether the effects of fear appeals are long term, a follow-up study was conducted.

2.3.4.2 Correlational studies

This section reviews correlational studies involving either part or all of the key variables described in the PMT model. Overall, the review revealed a consensus that perceived severity, perceived vulnerability, response efficacy, response cost and self-efficacy play a significant role in security behavior. However, the literature suggests no consensus on the exact relationship between these factors and behavioral intentions. Further, two distinct viewpoints were revealed. The first considers attitude as a

mediating role in the relationship between these factors and behavioral intentions. The second and most commonly agreed upon viewpoint is that these factors have a direct influence on behavioral intentions.

According to Anderson and Agarwal (2010) and Herath and Rao (2009), users' decision to apply security measures is dependent upon whether they have a favorable or unfavorable attitude towards the security measure, thus attitudes play a key role. Based on PMT and TPB, the study conducted by Anderson and Agarwal (2010) examined factors that motivate users to secure their home computing environment. Results from 594 home computer users suggest, attitude is the immediate predictor of security behavior. As proposed by TPB, their study also found that users develop their attitudes from their perceptions about security threats, effectiveness of security measures and self-efficacy. However, their proposition differed from PMT's view that these perceptions have a direct influence on behavioral intentions.

Similarly, results from a survey of 312 employees from 78 organizations conducted by Herath and Rao (2009) show a link between attitudes towards organizational security policy, and threat and efficacy perception. Yet, contrary to Anderson and Agarwal (2010), attitude was found to have no direct impact on compliance intentions. Interestingly, self-efficacy also had a direct impact on compliance intentions, suggesting that a direct link may have provided better insights into the role of the PMT variables on intentions. Given the inconsistent findings and the limited evidence supporting this viewpoint, the purported mediational role of attitudes was not considered in this study.

The prevailing view is that threat appraisal and coping appraisal factors have an independent and direct impact on users' IS security behavioral intentions. However, the interpretation of the PMT model, particularly on the structure of the threat

appraisal component, varies greatly from study to study. This makes comparing results across studies a challenging task. For example, Siponen et al. (2010) views threat appraisal factors as a single independent variable, while some (e.g., Liang & Xue, 2010; Posey et al., 2011) propose that fear is a function of perceived severity and perceived vulnerability, although Liang and Xue's (2010) position on the role of perceived severity and vulnerability differs from that of Posey et al. (2011).

Siponen et al. (2010), who based their research model on PMT, General Deterrence Theory, TRA and Innovation Diffusion Theory proposed an integrated model to explain factors that drive users to follow security policies within an organizational setting. They conceptualized threat appraisal as a single construct, measured using items related to both severity (e.g., "security breach would be a serious problem") and vulnerability to threats (e.g., "I could be subjected to a serious security threat"). One limitation with this approach is that an individual may perceive a threat as severe, yet not necessarily feel that the threat is imminent (Liang & Xue, 2010). In fact, following a field survey of 917 employees from several Finnish organizations Siponen et al. (2010) found threat appraisal to have a significant but weak impact on the employees' compliance intentions. Thus, the study proposed in this research considered perceived severity and perceived vulnerability as two independent constructs.

The nature of the association between fear and behavioral change is somewhat unclear. It is of interest to note that some studies represent the variable fear as *perceived threat*. For example Liang and Xue (2010) described their variable as perceived threat, however the items that describe the concept of fear of threat as described in PMT. Therefore, in this review, the term fear is synonymous with perceived threat.

Fear is excluded from the original PMT model as a key construct, however given that the revised PMT (Rogers, 1983) and works such as that of Witte (1992) sought to

redefine the role of fear, suggests that fear should be explored. As proposed in PMT, some available evidence (e.g., Maddux & Rogers, 1983; Rippetoe & Rogers, 1987; Witte, 1994) suggests that fear has an indirect impact on behavior. However results from IS security research, though limited, reveal some inconsistencies. For example, some findings (e.g., Liang & Xue, 2010; Zhang & McDowell, 2009) suggest a direct link between fear and IS security behavior, while results from studies such as that of Posey et al. (2011) show no such link.

To investigate users' motivation to avoid malicious technology, and test their previously proposed PMT based Threat Avoidance Theory (TTAT) (Liang & Xue, 2009), Liang and Xue (2010) hypothesized that of the three threat appraisal factors, only perceived threat, described in their study as the feeling of being threatened, would have a direct impact on behavior. They proposed that the effects of perceived severity and perceived vulnerability on protection motivation are indirect. Using a sample of 152 university business students, they found no direct links found between perceived severity, perceived vulnerability and security behavior. This finding is in contrast to the PMT, which proposes that perceived threat (fear) has an indirect influence on intentions, while perceived severity and perceived vulnerability have a direct impact on intentions. Interestingly, results from a study by Zhang and McDowell (2009) investigating factors that motivate users to apply online password protection, also contradict PMT's position. Their survey of 182 students from a univerity in the United States found no direct link between perceived severity and perceived vulnerability and password practices. Yet, their study found that fear had a direct positive impact on motivation to implement online password protection.

A notable similarity between the two studies, in addition to the direct link found between fear and behavior, is that both studies examined behaviors related to personal

protection. Interestingly, the only other study that explicitly incorporated fear in their model was in an organizational setting, and found no link between fear and security behavior. This was a survey of 380 employees from various organizations and industries in the US in which fear was found to have no significant impact on intentions to protect the organizations' information assets (Posey et al., 2011). Posey et al. (2011) suggested these findings may possibly be an indication that fear is a predictor of intentions, but only in the context of personal protection. While the available evidence is limited, this rationale is consistent with the results in the studies by Zhang and McDowell (2009) and Liang and Xue (2010), and corroborates the findings by Adams and Sasse (1999) whose study revealed that users worry more about their personal information as opposed to others' or an organization's.

Given the limited number of studies explaining fear arousal, it is clear that the role of fear arousal has been largely overlooked in the IS security literature. Johnston and Warkentin (2010a) indicated that discounting the role of fear in their study may have impacted the predictive ability of their proposed model, and thus suggested that more research into how propensity to fear may impact security practices. Therefore, to provide further insight into the role of fear, particularly in the context of personal password security, fear was considered a key variable in this study.

In contrast to the view that perceived severity and perceived vulnerability indirectly affect compliance intentions, most researchers propose a direct link between threat appraisal factors and IS security behavioral intention, and also a direct path between coping appraisal factors and security behavior. While support for the role of coping appraisal has been relatively consistent, the findings concerning the threat appraisal component, particularly on the role of perceived vulnerability are not universal. However, the available results supporting the direct impact of threat appraisal factors

appear to be more consistent in the context of organizational protection than in the context of personal protection.

For example, Lee and Larsen (2009) who investigated factors that influence small and midsize business (SMB) executives' adoption of anti-malware software found support for all hypothesized relationships in their model which was based on PMT and TAM (Davis, 1989). However, their results revealed only a weak relationship between perceived vulnerability and adoption intentions. Similarly, results from Workman et al. (2008) who investigated why users with considerable security knowledge would ignore security recommendations, also found support for all hypothesized relationships. Using a Threat Control model based on PMT and data from a field study of 588 employees from several technology oriented organizations, all key PMT variables (perceived severity of threats and vulnerability, and self-efficacy, response efficacy and response cost) were found to have a significant and direct impact on compliance with security policies.

While support for coping appraisal has mostly been consistent, the results reported by Siponen et al. (2014) are somewhat atypical, where threat appraisal was shown to be a better predictor of behavior than coping appraisal. In their study, an integrated model drawn from PMT, TRA and the Cognitive Evaluation Theory (CET) (Ryan, 1982), was proposed to explain employee adherence to security policies. Data from a field survey of 669 employees from four organizations in Finland support the hypothesized relationships between perceived severity, perceive vulnerability, self-efficacy and compliance intentions. Response efficacy was however unrelated to compliance intentions, while self-efficacy was found to be a weak predictor of intentions to comply with organizational security policies.

Similar to Siponen et al. (2014), Ifinedo (2012) also provides some support for the role of threat appraisal, but mixed support for coping appraisal factors. Using an integrated model based on PMT and TPB to explain compliance with organizational IS security policies, and a sample of 124 IS professionals and business managers, his study found support for the roles of all PMT variables with the exception of perceived severity and response cost. Consistent with the results reported by Siponen et al. (2014), self-efficacy was found to have the weakest influence on intentions. However, this is contrary to numerous other studies (Maddux & Rogers, 1983; Woon et al., 2005) and meta-analytic findings (e.g., Floyd et al., 2000; Milne & Milne, 2000) that suggest that self-efficacy may be the most robust predictor of protection behavior.

Based on the results in these studies (e.g., Ifinedo, 2012; Lee & Larsen, 2009; Siponen et al., 2014; Workman et al., 2008), the role of threat appraisal in influencing IS security behavior has received some support. Yet, other applications of PMT (e.g., Crossler et al., 2014; Posey et al., 2011; Vance et al., 2012) represent a growing number of PMT related IS security studies that have found no direct link between threat appraisal factors and compliance with security policies. For example, Vance et al. (2012) found no association beteen perceived vulnerability and employee intentions to comply with IS security policies. They proposed an integrated PMT model with Habit Theory (Verplanken & Orbell, 2003), describing habit as routine behavior or an action an individual is accustomed to performing. Results from 210 employees of a municipality in Finland, suggest that habit influences all PMT variables including perceived vulnerability. However, the results supported all hypothesized relationships except a direct link between perceived vulnerability and compliance intentions. Although habit influences perceived vulnerability, the employees' perceptions of the organization's vulnerability to a security threat had no impact on their compliance intentions.

Following this trend, Crossler et al. (2014) also reported mixed findings on the relationship between perceived severity, perceived vulnerability and intentions to comply with Bring your own Device (BYOD) policies in an organizational setting. They proposed that compliance with BYOD policy would differ between non-accounting and accounting professionals who handle sensitive information and examined if the model operates different between the two groups of participant. While the results related to coping appraisal factors were consistent for both groups, the results related to threat appraisal factors differed between the two groups. Self-efficacy and response efficacy influenced compliance in both groups. Perceived severity was significant but only for accountants, suggesting that those in industries that deal with sensitive information are likely to be more sensitive to threats against data security hence more likely to comply with BYOD policies (Crossler et al., 2014). However, for either group perceived vulnerability did not influence their decision to comply regardless of whether the individuals are aware of security threats or not.

Overall, the finding on the effects of self-efficacy, response efficacy and response cost on IS security behavior, have been consistent, with fewer studies finding weak or no support compared with support for threat appraisal factors.

In the context of organizational security, perceived vulnerability has received some support. However, in the context of personal protection, the findings appear to be more conclusive, albeit contrary to Roger's (1975, 1983) position that perceived vulnerability has a direct influence on behavioral intentions. All studies reviewed (i.e., Crossler, 2010; Liang & Xue, 2010; Milne et al., 2009; Woon et al., 2005; Zhang & McDowell, 2009), found no support for a direct relationship between threat vulnerability and intentions, in the context of personal protection. Weinstein (1984) has argued that people have an unrealistically low perception about their susceptibility

to threats, and that this intrinsically reduced perceived vulnerability may have a negative effect on preventative behaviors. As users tend to think that a hacker would not target their data (Sasse et al., 2001), it is unsurprising that many studies have failed to show that perceived vulnerability explains personal protection (in Crossler, 2010; Liang & Xue, 2010; Milne et al., 2009; Woon et al., 2005; Zhang & McDowell, 2009).

Interestingly, users do perceive their data as important to them (Adams & Sasse, 1999), just not important enough to others as shown by Sasse et al. (2001). Thus it is expected that in the context of personal protection perceived severity has received more support than perceived vulnerability such as in the study by Woon et al. (2005), who investigated factors that influence users' decision to apply wireless security features on their home computers. In a survey of 189 home computer users who own a wireless network at their home, their study found support for all proposed relationships except the relationship between perceived vulnerability and intentions to implement wireless security measures. Consistent with Weinstein (1984), Woon et al. (2005) also observed that the participants in their study did not believe that they were vulnerable to security threats prompting a suggestion that communicating to users about the severity of a security threat may be more effective than educating them about the probability of experiencing a computer attack.

Another study by Milne et al. (2009) also adds to the mixed findings on the role of threat perceptions in IS security practices. They examined factors that affect adaptive behaviors, where adaptive relates to taking security action, while they also examined factors that lead to maladaptive behavior such as avoiding online shopping altogether. Following a survey of 449 online shoppers from the US, their study found that perceived online threats had no impact on shoppers' security practices, but were more likely to lead users to skip online shopping all together. Their study also found that

perception of online threats and perceived vulnerability had no impact on behaviors, and that users were more likely to perform risky Internet practices such as saving passwords on a browser regardless of perceived threats or their perceived vulnerability.

Adding to the number of studies that have found no support for perceived vulnerability in predicting IS related behavior, is a study by Crossler (2010) who examined factors that motivate users to back up their personal data. With a sample size of 112 participants consisting of employees from small businesses, graduate students and private citizens, the study found self-efficacy and response efficacy to be significant motivating factors in users' decision to back up their personal data. The results found no evidence supporting direct relationships between perceived severity and perceived vulnerability, and users' intentions to back up their information.

Like Crossler (2010), Zhang and McDowell (2009), also found no support for the role of either perceived severity and perceived vulnerability in explaining IS security behavioral intentions. Zhang and McDowell (2009) examined factors that influence user intention to use strong passwords on personal online web accounts. Results from 182 university students from the United States revealed that there was no relationship between either perceived severity or perceived vulnerability and user intention to protect their personal online web account.

Given that the research proposed in this study is in the context of personal protection, and following the overwhelming results pointing to a non-significant relationship between perceived vulnerability and personal protection motivation, finding more insight into the link between perceived vulnerability and IS security behavioral intentions is particularly important in this study.

2.4 Password security literature

With the ubiquity of online services that require password authentication and reliance on emails or social media as a personal and organizational communication, users face several password related challenges. Firstly, the existing online password guidelines vary greatly from website to website (Bonneau & Preibusch, 2010; Florêncio & Herley, 2010), which has made it difficult to determine the ideal minimum password strength (Egelman et al., 2013). Another challenge relates to the number of accounts users manage on a daily basis, which has also been associated with poor security practices such as reusing passwords across different websites (Adams & Sasse, 1999; Grawemeyer & Johnson, 2011; Inglesant & Sasse, 2010). Lastly, and perhaps the most important contributor of poor password practices (Yan et al., 2004; Zviran & Haga, 1999), is that users struggle to remember passwords.

The following section reviews literature pertaining to these challenges and how they relate to this study.

2.4.1 The existing password guidelines problem

Aimed at providing some control over password quality and password behavior (Florêncio & Herley, 2010), password guidelines are typically presented as a set of rules pertaining to password quality such as minimum allowable password length, character composition, or restrictions on behavior such as reusing passwords. Online password guidelines occasionally come with an additional feedback mechanism such as a password strength meter designed to visually guide users to create stronger passwords (Egelman et al., 2013; Ur et al., 2012). However, password guidelines have little impact on password strength (Florêncio & Herley, 2010; Inglesant & Sasse, 2010; Ur et al., 2012; Yan et al., 2004).

The existing password guidelines have two notable problems. Table 2.2 summarizes password guidelines used on the 20 websites in the US as reported by quantcast.com. The table also reveals a wide variation as to what the ideal minimum password length or character composition is, which as Bonneau and Preibusch (2010) suggest, can inadvertently impede security, particularly that of high security websites. Bonneau and Preibusch (2010) also found that websites with less restrictive password requirements lead users to choose weak passwords. Given that users have a tendency to reuse passwords across websites (Ives et al., 2004; Jenkins et al., 2013), this may inadvertently compromise the security of high-security websites.

Secondly, it appears likely that password guidelines alone are ineffective in persuading users to create strong passwords or to comply with the recommended guidelines (Vu et al., 2007; Yan et al., 2004). Straub and Welke (1998) argues that deterrent measures such as information security guidelines do not have an active role in influencing a user to comply. However, strategies such as incorporating techniques for creating strong memorable passwords (Helkala & Svendsen, 2012; Vu et al., 2007; Yan et al., 2004), or persuasive messages (Jenkins et al., 2013), have been shown to be more effective in deterring users from insecure password practices.

Furthermore, the results of studies on the effectiveness of password strength meters have been mixed, with some showing mixed results (Ur et al., 2012), minimal effect (Egelman et al., 2013), or no effect (Vance et al., 2013) on password quality, whereas active strategies such as mnemonic training and persuasive communication have found more consistent support (e.g., Hampstead et al., 2012; Jenkins et al., 2013; Johnston & Warkentin, 2010a; Kuo, Romanosky, & Cranor, 2006; Nelson & Kim-Phuong, 2009; Vance et al., 2013; Yan et al., 2004).

Table 2.2: Existing recommendation on password selection varies as follows

Existing password guidelines for commonly used websites Top 20* Ranked Websites in the US						
Web service	**Min length**	**Min Char type**	**Password†: 23549988**	**Feedback**	**Password†: Communication**	**Feedback**
Google**	8	1	Accepted	Strong	Accepted	Fair
Facebook	6	1	Accepted	Medium	Accepted	Medium
Microsoft**	8	2	Rejected	Must contain all character types	Accepted	NA
Twitter	6	1	Accepted	Could be more secure	Accepted	Password is ok
Yahoo!**	8	3	Rejected	Must contain uppercase	Rejected	Must contain a number
Amazon	6	1	Accepted	NA	Accepted	NA
Yelp	6	1	Accepted	NA	Accepted	NA
eBay	6	2	Rejected	Invalid	Accepted	Weak
Buzzfeed	6	1	Accepted	NA	Accepted	NA
Pinterest	6	1	Accepted	NA	Accepted	NA
LinkedIn	6	1	Accepted	Weak	Accepted	fair
Wikipedia	1	1	Accepted	NA	Accepted	NA
CraigsList	8	2	Rejected	Must contain two character types	Accepted	NA
Playbuzz	1	1	Accepted	NA	Accepted	NA
PayPal	8	3	Rejected	Weak	Rejected	Weak
Adobe***	6	1	Accepted	NA	Accepted	NA
AOL	6	1	Accepted	Weak	Accepted	Strong
Weather	6	1	Accepted	NA	Accepted	NA
ASK***	6	1	Accepted	NA	Accepted	NA
Norton***	6	1	Accepted	Weak	Accepted	Strong

†The passwords were arbitrarily selected for demonstration only;*Ranking as of July-31-2014 as reported by www.quantcast.com;**Also used to access email and other services; ***The password '123456' was also accepted; Min length = minimum allowed number of characters; Min char = minimum number of character type actually enforced;

2.4.2 The password strength problem

As Table 2.2 illustrates, the consensus on what constitutes acceptable minimum password strength remains unclear. For example, Google.com considers the password '23549988' as strong, yet PayPal.com considered the same password as weak. Likewise, Yahoo.com rejected the password 'Communication' while Norton.com considers the same password as strong. Surprisingly, websites such as Amazon.com and Norton accept 123456 as a valid password. Without a clear definition of password strength, improving password security will remain a challenge (Mazurek et al., 2013). The literature (e.g., McDowell, Rafail, & Hernan, 2009; Scarfone & Souppaya, 2009; Tipton & Hernandez, 2009; Weir et al., 2010; Yan et al., 2004) seems to agree that a strong password is lengthy; contains a combination of numbers, upper and lower case letters, and symbols; and is free of dictionary words, common name or personal information. However, the precise definition of password strength is still elusive (Dell'Amico et al., 2010; Egelman et al., 2013).

Further, studies analyzing password strength seem to follow one of two techniques, which may also help clarify what the ideal password strength is. The first technique involves password cracking tools (Cazier & Medlin, 2006; Mazurek et al., 2013; Stone-Gross et al., 2009; Vu et al., 2007; Weber et al., 2008) while the second technique employs an entropy calculation, which estimates password unpredictability usually measured in bits (e.g., Burr, Dodson, & Polk, 2006; Egelman et al., 2013; Florêncio & Herley, 2007; Komanduri et al., 2011). These approaches differ, entropy calculations determines password strength by its length and character variation only (Burr et al., 2013; Egelman et al., 2013), whereas password cracking tools consider the length, character variation and information contained in a password such as dictionary words. While entropy calculations overlook dictionary words, entropy computations

consider character unpredictability a key determinant of the overall guessability of a password. Therefore, in both approaches password strength is a function of length, character variation and unpredictability of a password, which corroborates the general definition of a strong password.

Interestingly, it appears that users are capable of maintaining a higher than minimum required password length (Shay et al., 2010), however they struggle with the use of character variations and the type of information contained within their passwords is generally predictable (Bonneau, 2012; Burr et al., 2013; Pham et al., 2011). For example, as reported by Cazier and Medlin (2006) in their analysis of passwords used on an e-commerce website, the average password length was between 7 and 8 characters long, yet less than 2% of these passwords contained special characters. Using a dictionary attack, they were able to crack 90% of the passwords in less than a minute. Likewise, Calin (2009) who performed a statistical analysis on 10,000 leaked Hotmail passwords, found that even without enforcement, 69% of the passwords were between 6 and 9 characters. Yet, as the results showed, the top 20 most commonly used passwords contained names, sequential numbers and dictionary words, making them vulnerable to dictionary attacks.

2.4.3 The password reuse problem

Concerning password length, users are inclined use relatively long passwords. However, as studies have shown, the real challenge is using strong passwords, which is expected given that on average users manage anywhere between 6 (Grawemeyer & Johnson, 2011) to 7 (Florêncio & Herley, 2007) distinct passwords in a given day. Unfortunately, users are unable to deal with multiple passwords and thus resort to weak passwords (Adams & Sasse, 1999), or reuse passwords across websites (Ives et al., 2004). Password reuse can compromise the security of even the most secure

systems (Jenkins et al., 2013). Hackers could take advantage of low-security websites with less restrictive password requirements, where users are inclined to use weak passwords, to access high-security websites (Ives et al., 2004; Jenkins et al., 2013). A compromised low-security website, such as a personal web account, can perpetuate security threats to individuals and even to organizations (Furnell, 2007; Ives et al., 2004; Winkler, 2009).

Personal web accounts usually contain personal information such as names, contact details, and occasionally more sensitive information such as date of birth, bank or even health-related sensitive information (Beckjord et al., 2007). Thus on the surface, a compromised personal account appears to be harmful to personal information leading to threats such as identity theft (Jenkins et al., 2013). However, organizations are also likely to bear the consequences of an attack on a personal user (Furnell et al., 2007; Ives et al., 2004). A notable case (Winkler, 2009), involving an administration assistant at Twitter Inc. and a hacked personal email account, demonstrates the extent to which the impact of password reuse extends beyond personal harm. The Twitter employee's personal email account which was hacked through a simple reset technique, contained a password that was used on her other sites which subsequently led the hacker to successfully guessing the password to Twitter's corporate Google Apps account (Winkler, 2009). While the personal email account was hacked through a dubious password reset technique, the password reuse facilitated the domino effect that lead to the hacking of the corporate account. While this demonstrates the impact a low-security website can have on high-security systems, it shows what role password reuse can play in compromising security of a seemingly secure system.

Unfortunately, users have to deal with multiple unique passwords (Florêncio & Herley, 2007; Grawemeyer & Johnson, 2011), in order to maintain access to a large number of

websites on a daily basis. This means each unique password is reused, across an average of 4 websites (Florêncio & Herley, 2007). This prevalence of password reuse was also evident in a survey of over 400,000 leaked Yahoo Voices passwords which were compared with previously leaked passwords from a Sony breach (Hunt, 2012). The analysis revealed a whopping 59% of passwords reused between the two websites. That trend is consistent with an empirical study by Grawemeyer and Johnson (2011) who examined diary entries by participants from two organizations over a 7 day period and found that only 40% of the participants used unique passwords, while 50% reused their passwords across four authentication systems.

To deter users from reusing passwords, Ives et al. (2004) proposed incorporating policies that limit reuse of passwords across systems. However, Jenkins et al. (2013) tested a method that limits password reuse on a single website in combination with persuasive communication. Their study involved monitoring keystrokes as a technique for detecting password reuse and persuasive communication as a deterrence strategy. To detect reuse, they used an algorithm for calculating time between pressing a key and releasing a key and then compared the total time value with a second password. While keystrokes analysis detected password reuse with a high accuracy (81%), no empirical validation of this method exist thus far and the extent to which keystrokes analysis is effective in detecting password reuse across several websites is unknown. On the other hand, their deterrence strategy using fear appeals showed more promise, resulting in 88% of those who received fear appeals creating unique passwords, thus providing evidence of the efficacy of fear appeals in preventing unsafe password practices.

2.4.4 The password memorability problem

One of the limitations of the strategy used by Jenkins et al. (2013) to persuade users to create unique passwords is that the users were constrained to one specific password creating strategy, that is, creating unique passwords. The drawback is that the strategy overlooks their ability to actually create and maintain unique passwords beyond the one website. As users are expected to create different passwords for different websites (Helkala & Svendsen, 2012), constraining users to a specific password creating strategy may inadvertently have a negative impact on the overall password quality (Adams & Sasse, 1999; Jenkins et al., 2013). Given that one of the reasons users reuse passwords is because of their inability to manage and remember multiple strong passwords (Adams & Sasse, 1999; Helkala & Svendsen, 2012; Inglesant & Sasse, 2010), it is important to also incorporate a password creating strategy that addresses management of strong passwords that are also easy to remember.

Password memorability, which relates to the degree to which a user can remember a password, has been associated with the number of password users have to remember (Florêncio & Herley, 2007; Vu et al., 2007) coupled with the requirement to use strong passwords. Ability to remember passwords has been cited as a key challenge in text-based password usage (Zviran & Haga, 1999). In particular, users struggle to remember a series of random characters or strong passwords, an important requirement if passwords are to remain unpredictable or uncrackable (Tam, Glassmana, & Vandenwauverb, 2009; Yan et al., 2004).

Users are also faced with another challenge which relates to the type of information a human brain has the natural capacity to hold. It is said that the human brain can only memorize about five to nine random objects in the short-term (Miller, 1956). Miller's proposition seems to hold in the context of password memorization, where password

related studies (e.g., Calin, 2009; Cazier & Medlin, 2006; Weir et al., 2010), show that users are able to create passwords that are on average six to nine characters long, yet they appear to be unable to create random passwords. Miller further suggests that, for the brain to retain information in the long term, the items to be memorized must have some meaning to the individual. Therefore, it is expected that the key challenge for users is selecting passwords that contain random characters and avoid common words (Tam et al., 2009; Yan et al., 2004).

It is also unsurprising that research shows that password memorability can be improved through methods such as mnemonic training where passwords are created using meaningful phrases (Helkala & Svendsen, 2012; Vu et al., 2007; Yan et al., 2004). Furthermore, Yan et al. (2004) suggest that a password can contain some meaningful phrases and still be difficult to guess. In their study involving 288 college students, Yan et al. (2004), found that random passwords were significantly more difficulty to remember which led users to write them down. Passwords containing meaningful phrases were significantly easier to remember yet difficult to guess given that the method also involves substituting letters with special characters, thus resulting in a random string of characters. In addition, only the group that used the meaningful phrase strategy included special characters in their passwords.

Results reported in a smaller scale study by Vu et al. (2007) also provide support for a password creating strategy that incorporates some meaningful information to improve password memorability while generating passwords that are also difficult to crack. Twenty students created password using the first letter of a sentence of their choosing but with at least six words, while another twenty used the same method but also included special characters and numbers between any letters. They found that incorporating special characters and numbers between any letters, results in passwords

that are less susceptible to cracking but also memorable. Thus, Vu et al. (2007) concluded that without some type of memorability technique, password guidelines alone are inadequate.

Concerning passwords, the overall findings suggest that Internet users face numerous challenges related to passwords, from multiple variations of password guidelines and password strength requirements, through to having to memorize multiple strong passwords. In developing the study materials for the research described in this thesis, the user perceptions considered include their perceived effectiveness of password guidelines, their judgment about their ability to create strong passwords and the extent to which remembering strong passwords impacts their compliance with password guidelines.

2.5 Chapter overview

This chapter reviewed the literature related to the research questions addressed in this study with emphasis on concepts pertaining to security perceptions, and how user perceptions of passwords and security threats influence compliance with password guidelines. The literature therefore covered research that provides an understanding of how these perceptions are formed thus forming the basis for addressing the question of whether these perceptions can be altered in order to improve compliance.

The literature also looked at four competing theories, that is, HBM, SEU, TRA/TPB, and PMT, which have been used to explain protective behaviors from a perceived threat perspective. The key components and limitations of these frameworks was described and however PMT's behavioral change component was highlighted as a benefit of the PMT framework in explaining and changing IS security behavior. In particularly its usefulness in experimental research and the ability to map PMT based

fear appeals into IS security awareness communication was noted. Yet this review revealed a lack of experimental research in the applications of PMT in IS security research and that thus far there appears to be no follow-up studies examining if the effects of fear appeals used in IS security have a long term effect on security practices. This review also revealed that while the most commonly agreed upon view is that threat and coping appraisal play a significant role in security behavior, the applications of PMT in IS security research particularly on the structure of threat appraisal factors vary greatly from study to study. This review draws attention to the need for a consensus to improve the predictability of PMT grounded research models and to improve the ability to compare results across studies. This review draws particular attention to the overwhelming lack of confirmation for a direct link between perceived vulnerability and IS behavior and the need for further research into this link.

The literature related to text based password and the challenges associated with their use on online web accounts were described. This review draws attention to the challenges users face as a result of password guidelines that vary greatly across the Internet and how the existing password guidelines have failed to persuade users to create strong passwords. The use of fear appeals in combination with mnemonic training has been shown to be effective in improving compliance with password guidelines and more importantly improve password strength. However, the question of whether the effects of fear appeals can be maintained over time remains unclear.

3 Research Model and Hypotheses

3.1 Introduction

To achieve the objectives described in this thesis, this study considers the role of user perceptions about password threats and password efficacy in motivating users to comply with password guidelines. This research also aims to provide insight into whether these perceptions can be altered to improve compliance with password guidelines and if compliance can be maintained over time. This chapter presents the research questions addressed in this study and describes the theoretical framework from which the research model is based. The hypotheses and proposed research model for this study are then presented.

3.2 Research questions

To achieve the objectives of this study, two core research questions are addressed in the research described in this thesis.

The first research question is:

1. *How do user perceptions about password threats and password efficacy affect compliance with password guidelines?*

Based on Protection Motivation Theory (PMT) (Maddux & Rogers, 1983; Rogers, 1975, 1983), this research question seeks to examine the role of password threat perceptions and efficacy perceptions in compliance with recommended password guidelines. In this study, compliance with password guidelines is examined as behavioral intentions as well as actual behavior.

The second research question is:

2. *Can these perceptions be altered?*

Literature about the effectiveness of fear appeals or persuasive messages in IS security (e.g., Jenkins et al., 2013; Johnston & Warkentin, 2010a; Vance et al., 2013) suggests that threat and efficacy perceptions can be altered using fear appeals, to ultimately improve security practices. This research seeks to investigate if fear appeals, which take the form of password security training in this study, can be effectively used to change threat perceptions and efficacy perceptions.

As a follow-up to the previous question, two subsidiary research questions are asked. The first considers whether changing threat and efficacy perceptions can increase the likelihood that an individual will comply with password guidelines:

2a. If so, can altering these perceptions improve compliance with password security guidelines?

This research question seeks to investigate whether the proposed changes in these perceptions will have a positive impact on intentions to comply with password guidelines and actual compliance. The second subsidiary question explores whether any improved compliance with password guidelines is maintained over time:

2b. Can the effects of altering these perceptions be maintained over time?

Many previous studies have reported on effects achieved immediately after fear appeals have been used (e.g., Jenkins et al., 2013; Johnston & Warkentin, 2010a; Vance et al., 2013). Therefore, this question seeks to examine if the benefits of altering these perceptions extend beyond the fear appeals intervention period.

3.3 Theoretical framework

The research model used in this study is drawn from PMT (Maddux & Rogers, 1983; Rogers, 1975, 1983), which originated as a model for predicting health-related behavior. PMT proposes how an individual assesses threats, referred to as threat appraisal, determines the likelihood of follow recommended preventative measures. PMT also suggests that the likelihood that an individual will comply with recommended measures is dependent upon perceptions about the effectiveness of the preventative measures, ability to perform them, and any perceived difficulties associated with the preventative measures, referred to as coping appraisal. The PMT model (Rogers, 1975) was also originally developed to explain the effects of using persuasive messages or fear appeals to influence threat and coping appraisal processes and ultimately change behavior.

The threat appraisal component of PMT includes the constructs (i) *perceived severity* or an individual's assessment of the severity of a threat, (ii) *perceived vulnerability* or an individual's assessment of vulnerability to threat and (iii) *fear*, which is triggered by an emotional feeling towards a threat, sometimes referred to as fear arousal. In the PMT literature, fear arousal is described and has been measured using adjectives such as frightened, worried or nervous (Maddux & Rogers, 1983; Milne & Milne, 2000; Witte, 1992; Zhang & McDowell, 2009).

The coping appraisal component of PMT includes the constructs (i) *self-efficacy* or an individual's assessment of the ability to perform the recommended preventative measure, (ii) *response efficacy* or assessment about the effectiveness of the proposed preventative measure and (iii) *response cost* or an individual's assessment about how inconvenient or difficult a preventative measure would be to undertake. According to the revised PMT (1983), *self-efficacy* and *response efficacy* are factors that motivate

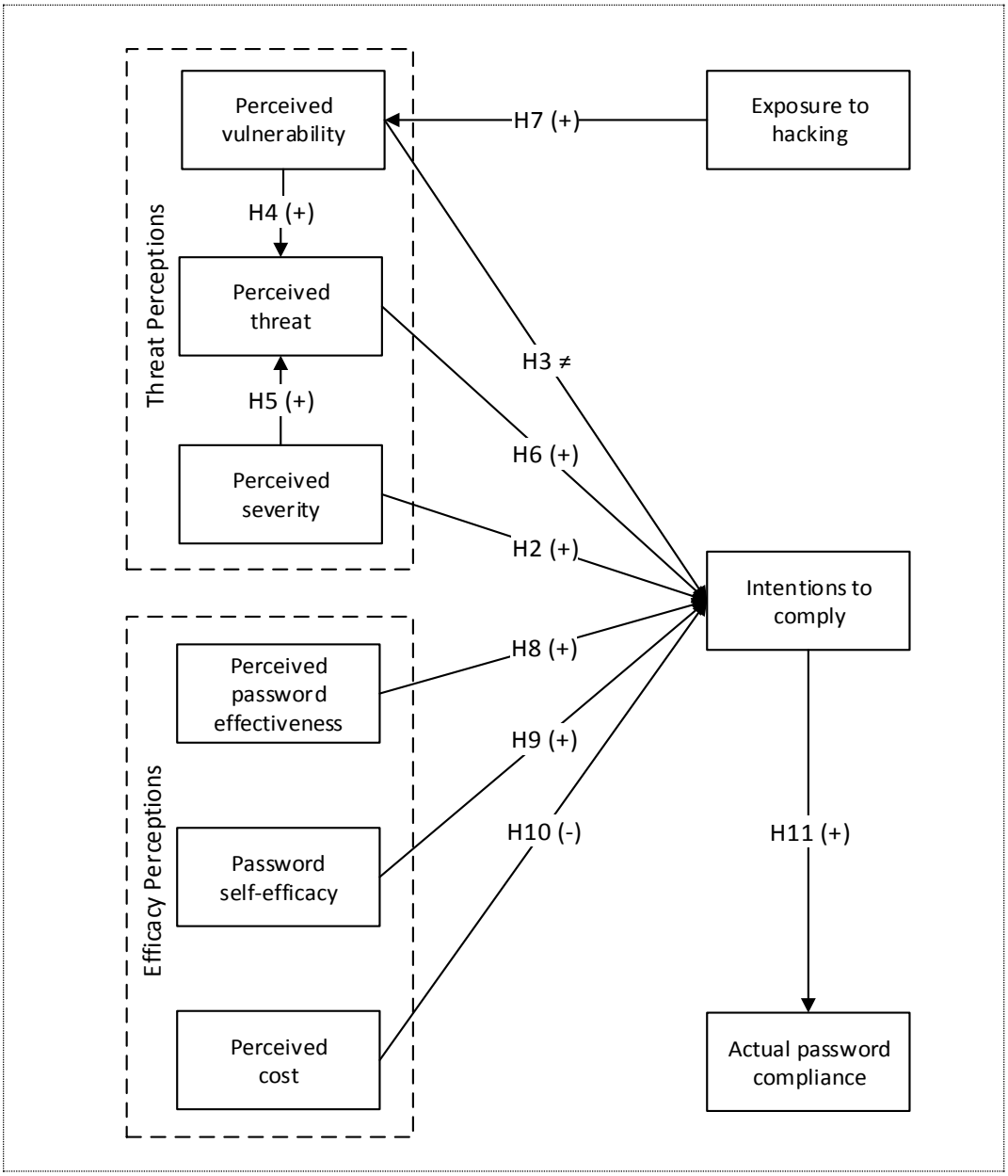
individuals to follow recommended preventative measures, while *response cost* contributes to an individual's decision to ignore preventative measures, thus has a negative effect on behavioral intentions.

Drawn from PMT's threat appraisal component, the *Threat Perception* component of the proposed model in this study, relates to an individual's assessment about the severity of password related threat (*perceived severity*), vulnerability to password related threats (*perceived vulnerability*), and emotions such as worrying about password related threats (*perceived threat*). In this thesis, *perceived threat* is synonymous with fear. The coping appraisal component is represented in this study as *Efficacy Perceptions*, which relates to the assessment about one's ability to undertake recommended password guidelines (*password self-efficacy*), perceived effectiveness of the password guidelines (*perceived password effectiveness*) and assessment about the difficulty of following the recommended password guidelines (*perceived cost*).

Figure 3.1 presents the research model used in this study and the hypothesized relationships. The model shows the proposed relationships between *Threat Perceptions* and *Efficacy Perceptions* and the dependent variable, *intentions to comply* with password guidelines. The dependent variable, which is represented by the construct *protection motivation* in PMT, is typically a measure of behavioral intentions (Floyd et al., 2000; Rogers & Prentice-Dunn, 1997) and in fact PMT asserts that protective behavior is most appropriately predicted by behavioral intentions (Prentice-Dunn & Rogers, 1986; Rogers & Prentice-Dunn, 1997; Weinstein, 1993). However, a meta-analysis (Floyd et al., 2000) conducted on PMT studies that have measured both intentions and actual behaviors, suggests that PMT can be effectively used to predict intentions and actual behavior. Accordingly, the research model used in this study also includes measures of actual behavior, described as *actual password compliance*. The

model used in this research is also extended to include *exposure to hacking*, which relates to prior exposure to a hacking incident (discussed further in Section 3.6).

Figure 3.1: Research model and the hypothesized relationships



The PMT model is useful for explaining how threat and efficacy perceptions influences behavior and therefore suitable for this study. PMT has been successfully used to explain IS security behaviors in a growing number of IS security studies (e.g. Herath & Rao, 2009; Jenkins et al., 2013; Johnston & Warkentin, 2010a; Posey et al., 2011; Siponen et al., 2014; Vance et al., 2012; Woon et al., 2005; Workman et al., 2008). In this study, the relationships implied in the PMT framework form the bases

for the research model. Further, this study examines the direct effects of the variables *perceived severity*, *perceived vulnerability*, *perceived threats*, *perceived password effectiveness*, *password self-efficacy* and *perceived cost* on *intentions to comply* with password guidelines. Table 3.1 shows the definitions of the constructs used in this study.

Table 3.1: Constructs definitions

Construct	Definition
Fear appeals	Persuasive messages containing information that emphasizes the severity of password related threats such as hacking and the likelihood of being exposed to the threats
Perceived severity	The degree to which a user believes that the consequences of password related threats would be severe
Perceived vulnerability	The degree to which a user believes that they are likely to experience password related threats
Perceived threat	The degree to which a user is worried about password related threats
Exposure to hacking	Prior exposure to a hacking incident, experienced by either a user, or someone they know personally
Perceived password effectiveness	The degree to which a user believes that recommended password guidelines will prevent password related threats
Password self-efficacy	The degree to which a user is confident in their ability to create a strong password
Perceived cost	The degree to which a user believes that remembering passwords would be difficult if password guidelines were followed
Intentions to comply	The degree to which a user intends to follow a set of recommended password guidelines
Actual password compliance	The quality of passwords created and is represented as password strength
Password memorability	The degree to which a user can remember a password

With the exception of Siponen et al. (2010) who operationalized perceived severity and perceived vulnerability as a single variable, recent IS security studies have examined the direct effects of the individual threat appraisal and efficacy appraisal variables on IS security practice; for example: perceived vulnerability and perceived severity (Lee & Larsen, 2009; Posey et al., 2011; Vance et al., 2012; Woon et al., 2005; Zhang &

McDowell, 2009), response efficacy and self-efficacy (Johnston & Warkentin, 2010a; Lee & Larsen, 2009; Vance et al., 2012; Woon et al., 2005; Zhang & McDowell, 2009), and response cost (Lee & Larsen, 2009; Siponen et al., 2010; Vance et al., 2012; Woon et al., 2005; Zhang & McDowell, 2009). This practice is also followed in this study.

In this study, *intentions to comply* relates to an individual's willingness to choose a password that follows all the guidelines recommended by the system. These might include: a combination of numbers, letters, and symbols; a password that is different from previously used passwords; or a password that is different from other online passwords. In this study, PMT is used as a basis for explaining intention and behavior in relation to password threats and also to explain the effects of fear appeals on password related behaviors. The following sections describe the fear appeals and variables examined in this study and the hypotheses formulated for this study (see Table 3.2).

Table 3.2: Summary of hypotheses

Hypothesis	Description of hypothesis
H.1	Fear appeals will increase user compliance with password guidelines.
H.2	*Perceived* severity of password related threats is positively related *to intentions to* comply with password guidelines.
H.3	*Perceived vulnerability* to password related threats will not have a direct effect on *intentions to comply* with password guidelines.
H.4	*Perceived vulnerability* is positively related to *perceived threat*.
H.5	*Perceived severity* is positively related to *perceived threat*.
H.6	*Perceived threat* is positively related to *intentions to comply* with password guidelines.
H.7	*Exposure to hacking* is positively related to *perceived vulnerability*
H.8	*Perceived password effectiveness* is positively related to *intentions to comply* with password guidelines
H.9	*Password self-efficacy* is positively related to *intentions to comply* with password guidelines
H.10	*Perceived cost* is negatively related to *intentions to comply* with password guidelines
H.11	*Intentions to comply* is positively related to *actual password compliance*.
H.12	Users who receive fear appeals will have **higher** *intentions to* comply over time than those who do *not*
H.13	Users who receive fear appeals with a **mnemonic** training emphasis will have higher *password* memorability over time than those who do not

3.4 Fear appeals

Fear appeals are persuasive messages aimed at motivating individuals to engage in a recommended behavior (Maddux & Rogers, 1983; Rogers, 1975, 1983). Fear appeals can have a significant impact on behavioral intentions, by altering individuals' perceptions of threats and influencing the way they perceive recommended precautions. Fear appeals can also be used to motivate people to believe that they possess the capabilities to successfully execute the recommended precautions (Bandura, 1982). Fear appeal messages have been used in health-related studies to improve adoption of health preventative measures (e.g., Rippetoe & Rogers, 1987), and also in IS security studies to improve adoption of computer security preventative measures (e.g., Jenkins et al., 2013; Johnston & Warkentin, 2010a).

In a health-related study, Rippetoe and Rogers (1987) examined the effectiveness of fear appeals in promoting breast cancer examination by using persuasive messages to influence self-efficacy, response efficacy and threat perceptions. Their study found that those who received written statements and graphic information about the severity of breast cancer were more likely to go through with a breast cancer examination than those who received non-threatening messages. In an IS security study, Johnston and Warkentin (2010a) used fear appeal messages to influence perceptions about threats posed by computer spyware and perceptions about the effectiveness of anti-spyware software and Jenkins et al. (2013) successfully used fear appeals to deter users from reusing password on an online website. Consistent with Rippetoe and Rogers (1987) these IS security studies show that fear appeals can be effectively used to improve users' intentions to perform recommended IS security measures.

This study defines *fear appeals* as persuasive messages containing information that emphasizes the severity of password related threats such as hacking and the likelihood of being exposed to the threats. In this study, *fear appeals* also include statements emphasizing the effectiveness of recommended password guidelines in preventing password related threats and training on how to create strong passwords that are also easy to remember. The fear appeals also incorporate the use of a mnemonic strategy for creating passwords where a password is created from the first letter of a sentence or a familiar phrase. Studies (e.g., Helkala & Svendsen, 2012; Vu et al., 2007; Yan et al., 2004) show that this mnemonic training improves ability to remember passwords. Using fear appeals as a method of persuading individuals to follow recommendations, the PMT model is aimed at explaining change in threat and efficacy perceptions, and also predicting behavioral change (Rogers, 1975, 1983).

A key focus of this study is behavioral change, or improving compliance with password guidelines using fear appeals and the hypotheses in this study are formulated on the basis that behavioral change is mediated via increased intention to comply with password security recommendations. It is therefore hypothesized that:

H.1 *Fear appeals* will **increase** user *compliance* with password guidelines.

3.5 Effects of threat perceptions on intentions

According to PMT, an individual's assessment of threats, that is, beliefs about the likelihood of exposure to a threat, described as perceived vulnerability, and assessment of how severe the threat is likely to be, described as perceived severity, have a direct impact on behavioral intentions. Perceived vulnerability and perceived severity are also said to trigger an emotional feeling towards threat, also referred to as fear (Liang & Xue, 2010; Maddux & Rogers, 1983; Rogers, 1975, 1983; Witte, 1992), which is

described in this study as *perceived threat*. Thus in this study *perceived threat* is synonymous with fear as described in PMT.

In this study, the *Threat Perception* component of the proposed model includes the variables: *perceived severity*, per*ceived vulnerability* and *perceived threat* which are described in the following sections.

3.5.1 Effects of perceived severity on intentions

In this study, *perceived severity* relates to the degree to which a user believes that the consequences of password related threats would be severe. PMT suggests that higher perceptions of the severity of threats increase the likelihood that an individual will comply with recommended precautions (Maddux & Rogers, 1983; Rogers, 1975, 1983). In IS security research perceived severity has been shown to contribute to compliance with IS security measures. For example, Woon et al. (2005) found that users are more likely to enable wireless security measures if they believe that a breach on their home wireless network would be detrimental.

Several health-related PMT studies (Maddux & Rogers, 1983; Milne & Milne, 2000; Rippetoe & Rogers, 1987), have found a significant direct effect of perceived severity on likelihood of undertaking recommended behavior. Perceived severity has been found to have a direct effect on users' decisions to implement wireless security on their home computers (Woon et al., 2005) and a direct impact on business executives' intentions to install anti-malware software within an organization (Lee & Larsen, 2009). Thus, it seems likely that if users believe the consequences of being hacked into would be detrimental, they are more likely to comply with password security recommendations. This suggests that elevating users' perception of the severity of

password related threats will increase their motivation to comply with recommended password guidelines. It is therefore hypothesized that:

H.2 *Perceived severity* of password related threats **is positively related to** *intentions to comply* with password guidelines.

3.5.2 Effects of perceived vulnerability on intentions

In this study, *perceived vulnerability* relates to the degree to which a user believes that they are likely to experience password related threats. PMT proposes a direct link between perceived vulnerability and behavioral intentions towards recommended precautions. This suggests that if users believe that their password is likely to be hacked they are more likely to comply with recommended password guidelines. The association between perceived vulnerability and intentions to perform recommended measures may not be direct. Some studies in the health-related domain and especially those in the IS security domain (Crossler et al., 2014; Skogan & Maxfield, 1981; Vance et al., 2012; Woon et al., 2005; Zhang & McDowell, 2009) have failed to confirm the impact of *perceived vulnerability* on motivation to perform preventative measures. Further, as meta-analysis (Milne & Milne, 2000) of PMT studies shows, although some studies find a significant relationship between perceived vulnerability and intentions, the strength of the association is typically small.

Weinstein (1984) suggests that people usually have an unrealistically low perception about the likelihood of a threat occurring, and that this intrinsically reduced perceived vulnerability may have a negative effect on preventative behaviors. In fact, Sasse et al. (2001), who examined the link between user behavior and security failures, found that users generally believe that their information is worthless and not important enough to be targeted. It is thus not surprising that support for the link between perceived

vulnerability and compliance intentions has been weak. Further, Liang and Xue (2010) suggest that perceived severity and perceived vulnerability also have an indirect effect on behavioral intentions through perceived threat and that the relationship is mediated by perceived threat. This may further explain the mixed findings in studies that only examined direct effects of perceived vulnerability on behavioral intentions. Thus, it seems likely that perceived vulnerability will have no direct effect on a user's intention to comply with password security guidelines.

It should be noted that the null hypothesis is consistent with the fact that an overwhelming majority of published IS security research in the context of personal IS security has failed to establish perceived vulnerability as a predictor of intentions to comply. This also draws attention to the extent to which PMT is applicable in the IS security domain. It is therefore hypothesized that:

H.3 *Perceived vulnerability* to password related threats will **not have a direct effect** on *intentions to comply* with password guidelines.

3.5.3 Effects of perceived severity and perceived vulnerability on perceived threat

Perceived threat is a function of perceived severity and perceived vulnerability (Herath & Rao, 2009; Liang & Xue, 2010; Plotnikoff & Higginbotham, 2002; Rogers, 1983; Weinstein, 2000; Witte, 1994) and a better predictor of behavioral intentions than perceived severity or perceived vulnerability (Liang & Xue, 2010). Herath and Rao (2009) examined the relationship between the three threat perception variables, and found that perceived severity increases concern for security breaches. Although their study found insignificant correlation between perceived vulnerability and level of concern for security, a study by Liang and Xue (2010) found that both perceived severity and perceived vulnerability affects users' level of concern. Their study found

that perceived severity and vulnerability have an indirect effect on intentions to use anti-spyware software and that the relationship is mediated by perceived threat.

This suggests that threat perception increases if users believe that their online account is likely to be hacked and if they believe that hacking can lead to serious consequences. Thus, it seems likely that elevating a user's *perceived vulnerability* and *perceived severity* would increase *perceived threat*. It is therefore hypothesized that:

H.4 *Perceived vulnerability* **is positively related to** *perceived threat*.

H.5 *Perceived severity* **is positively related to** *perceived threat*.

3.5.4 Effects of perceived threat on intentions

In the model proposed in this thesis *perceived severity* and *perceived vulnerability* are proposed to trigger an emotional feeling towards threat, which is described as *perceived threat*. *Perceived threat* relates to the degree to which a user is worried about password related threats and reflects the emotional aspect of *Threat Perceptions* or concern for threats that result from fear of threats, while *perceived severity* and *perceived vulnerability* represent beliefs about the likelihood of being exposed to threat or the severity of threats (LaTour & Rotfeld, 1997; Maddux & Rogers, 1983; Plotnikoff & Higginbotham, 2002; Rogers, 1975).

Perceived threat is said to increase the likelihood of behavioral intentions to comply with recommended precautions (LaTour & Rotfeld, 1997; Maddux & Rogers, 1983; Rogers, 1983; Skogan & Maxfield, 1981). The role of fear on behavioral intentions has received some support in several studies. While some (Rippetoe & Rogers, 1987; Rogers, 1983; Witte, 1994) suggest that fear has an indirect impact on intentions, via perceived severity and perceived vulnerability, studies such as that of Zhang and McDowell (2009) and Liang and Xue (2010) have found that fear (represented as

perceived threat) has a direct and positive impact on users' intentions to protect their personal information. Therefore, fear, represented as *perceived threat*, is included in this study.

Zhang and McDowell (2009) found that users who are nervous about password hacking are significantly more likely to implement password protection measures. Their study supports a direct effect of perceived threat on intentions to comply with recommended precautionary measures. Findings from a study by Liang and Xue (2010) investigating users' decisions to protect their personal computers, also found that fear, represented in their study as perceived threat, had a direct influence on users' intentions to protect their computer. This suggests that, the more worried users are about password related threats, the more likely they are to comply with password security guidelines. Therefore, it seems likely that, elevating a user's *perceived threat* of password related threats would increase motivation to comply with recommended password guidelines. It is therefore hypothesized that:

H.6 *Perceived threat* **is positively related to** *intentions to comply* with password guidelines.

3.6 Effects of exposure to hacking on perceived vulnerability

Exposure to hacking is defined as prior exposure to a hacking incident, experienced by either a user or someone they know personally. The PMT model does not explicitly include threat experience as a direct predictor of *Threat Perceptions*. However, PMT related studies, including health and IS security related studies, have reported mixed findings and failed to consistently confirm the significance of the construct *perceived vulnerability* in predicting behavioral intentions (Herath & Rao, 2009; Lee & Larsen,

2009; Rippetoe & Rogers, 1987; Vance et al., 2012; Woon et al., 2005; Zhang & McDowell, 2009). These mixed findings warrant a consideration of the role of threat experience on vulnerability perceptions. Therefore, the relationship between password hacking experience and users' perceived vulnerability to password related threats will also be examined.

When a person or someone they know personally is exposed to threats, this experience is viewed as a form of acquired knowledge that could affect an individual's perceived vulnerability (Skogan & Maxfield, 1981; Weinstein, 1989). In an IS related security study by Boss (2007), found that perceived vulnerability is developed through both personal experience and knowledge about others' exposure to cyber security threats. This suggests that if a user or someone they know personally has had their online account hacked into, *perceived vulnerability* should increase. Therefore, it seems likely that *exposure to hacking* will be positively related to *perceived vulnerability*. It is therefore hypothesized that:

H.7 *Exposure to hacking* **is positively related to** *perceived vulnerability*.

3.7 Effects of efficacy perceptions on intentions

PMT (Maddux & Rogers, 1983; Rogers, 1975, 1983) suggests that intentions to adopt recommended preventative measure are maximized if the recommended measure is believed to be an effective means of preventing threats; this is referred to as response efficacy. Further, PMT suggests that behavioral intentions are elevated if an individual is confident in successfully executing the recommended measure; this is referred to as self-efficacy (Maddux & Rogers, 1983; Rogers, 1983). PMT also suggests that behavioral intentions can be negatively impacted if the costs associated with performing the recommended measures are high and this is referred to as response

cost. In PMT, these factors are collectively referred to as coping appraisal. In this study, coping appraisal is represented as *Efficacy Perceptions*, and includes the variables: *perceived password effectiveness*, *password self-efficacy* and *perceived cost*, which are synonymous with PMT's response efficacy, self-efficacy and response cost respectively. The *Efficacy Perceptions* variables investigated in this study are described in the following sections.

3.7.1 Effects of perceived password effectiveness on intentions

Perceived password effectiveness relates to the degree to which a user believes that recommended password guidelines will prevent password related threats. As suggested in PMT (Maddux & Rogers, 1983; Rogers, 1975, 1983) and supported in studies based on PMT (e.g., Ifinedo, 2012; Lee & Larsen, 2009; Posey et al., 2011; Rippetoe & Rogers, 1987; Woon et al., 2005; Zhang & McDowell, 2009), the higher the level of perceived effectiveness the higher the probability of compliance with recommended precautions.

Studies that have examined factors associated with health-related preventative behaviors (e.g., Maddux & Rogers, 1983; Rippetoe & Rogers, 1987) as well as those that have examined IS security related preventative behaviors using the PMT model (e.g., Johnston & Warkentin, 2010a; Lee & Larsen, 2009; Woon et al., 2005; Zhang & McDowell, 2009), have found evidence to support a positive association between perceived effectiveness and motivation to adopt preventative measures. In the health domain, importance of beliefs about the effectiveness of preventative measures was supported in an experiment by Maddux and Rogers (1983) which found that those who believed that quitting cigarette smoking would effectively eliminate the risks of heart and lung disease were more likely to follow through with the preventative measures.

Further, in a study by Rippetoe and Rogers (1987), perceived effectiveness, described in their study as response efficacy towards breast cancer detection, was found to be the strongest predictor of behavioral intentions.

Studies such as those by Woon et al. (2005), Lee and Larsen (2009), and Zhang and McDowell (2009) suggest that users' decision to adopt IS security measures is determined by whether they perceive the security measures as an effective means of preventing security threats. For example, Woon et al. (2005), who investigated factors associated with adoption of wireless security by home computer users, found perceived effectiveness to play a significant role in users' decisions to implement wireless security. In a study by Lee and Larsen (2009), the perception that installing anti-malware software would prevent malware threat, was also found to have a significant positive impact of business executives' decisions to implement anti-malware measures within their small-to-medium (SME) sized organizations.

Consistent with Rippetoe and Rogers (1987), Zhang and McDowell (2009), who used the PMT model to examine factors affecting password protection, found perceived effectiveness to be the strongest predictor of behavioral intentions among university college students. They found that those who believed that implementing password security measures would effectively safeguard their online accounts were more likely to implement password protection. This suggests that if users believe that the recommended password guidelines are an effective means of preventing password related threats such as hacking, they are more likely to comply with the guidelines. Therefore, it seems likely that elevating a user's *perceived password effectiveness* would increase motivation to comply with password guidelines. It is therefore hypothesized that:

H.8 *Perceived password effectiveness* **is positively related to** *intentions to comply* with password guidelines.

3.7.2 Effects of password self-efficacy on intentions

Password self-efficacy relates to the degree to which a user is confident in their ability to create a strong password. The revised version of the PMT model (Maddux & Rogers, 1983; Rogers, 1983), which was revised to incorporate the variable self-efficacy, suggests that in addition to beliefs about the effectiveness of recommended preventative measures, an individual's beliefs about the ability to perform the recommended measures also have a significant impact on behavioral intentions (Maddux & Rogers, 1983; Rippetoe & Rogers, 1987). Following their experimental validation of the role of self-efficacy in protective behavior, Maddux and Rogers (1983) found self-efficacy to be a significant and key component of the PMT model. Furthermore, findings from several studies including meta analytic analyses of PMT studies (e.g., Floyd et al., 2000; Maddux & Rogers, 1983; Milne & Milne, 2000; Woon et al., 2005) suggest that self-efficacy may possibly be the strongest predictor of behavioral intentions to adopt preventative measures.

In IS security related research, self-efficacy has been shown to play a significant role in determining a user's intentions to use spyware software (Johnston & Warkentin, 2010a) and also in motivating SME business executives to install anti-malware software (Lee & Larsen, 2009). Woon et al. (2005) also found that users who are confident that they can use wireless security measures are more likely to implement recommended wireless security measures and Siponen et al. (2014) also found that self-efficacy plays a significant role in motivating employees to comply with organizational IS security policies. This suggests that if users are confident about their

ability to create a strong password they are more likely to comply with password security recommendations. Therefore, it seems likely that elevating *password self-efficacy* would increase the likelihood of compliance with recommended password guidelines. It is therefore hypothesized that:

H.9 *Password self-efficacy* **is positively related to** *intentions to comply* with password guidelines.

3.7.3 Effects of perceived cost on intentions

Perceived cost relates to the degree to which a user believes that remembering passwords would be difficult if password guidelines were followed. PMT suggests that response cost, referred in this study as *perceived cost* decreases the likelihood that an individual will comply with recommended measures (Maddux & Rogers, 1983; Rogers, 1983) and that the motivation process is stronger when perceived costs are low (Prentice-Dunn & Rogers, 1986). In accordance with PMT, if an individual believes that carrying out recommended measures would be difficult, complex, costly, unpleasant or require too much effort, they are less likely to undertake the recommended measures (Prentice-Dunn & Rogers, 1986). Difficulty in remembering passwords has been identified as a challenge to users and a significant barrier to safe password practices (Gaw & Felten, 2006; Inglesant & Sasse, 2010; Ur et al., 2012; Yan et al., 2004; Zviran & Haga, 1999).

Several key characteristics define a strong password; however these characteristics also make them difficult to remember (Yan et al., 2004). These include the number of characters, the uniqueness of characters, inclusion of special characters, and exclusion of familiar words such as dictionary words. They should also be changed frequently and be different from those used for other web accounts. These characteristics are a

standard requirement of most password guidelines. The problem is, the human memory is designed to remember short series of items that are familiar or memorable to the individual (Miller, 1956), and as studies have shown, this requirement has inadvertently let to inability to remember strong passwords (Yan et al., 2004; Zviran & Haga, 1999). This inability to remember strong passwords decreases the likelihood of compliance with password requirements (Yan et al., 2004). Further, the number of passwords users are required to memorize makes it even more difficult for them (Zhang, Luo, et al., 2009) and including special characters and numbers makes passwords less meaningful (Warkentin et al., 2004). In this study, *perceived cost* represents an individual's belief that remembering strong passwords would be difficult.

Perceived cost has been found to have a negative effect on behavioral intentions in a variety of IS security domains. For example, perceived cost was found to have a negative impact on: intentions to adopt anti-malware software by SME business executives (Lee & Larsen, 2009); intentions to comply with security policies relating to encrypting portable media, locking employee computers or sharing passwords (Vance et al., 2012); intentions to update and create strong unique passwords (Zhang & McDowell, 2009), and also influences actual implementation of wireless security measures by home computer users (Woon et al., 2005). This suggests that if users believe that a password that is created according to suggested password guidelines would be difficult to remember, they are less likely to comply with password security measures. It seems likely that decreasing a user's *perceived cost* of conforming to password guidelines will increase likelihood to comply with the password guidelines. It is therefore hypothesized that:

H.10 *Perceived cost* **is negatively related to** *intentions to comply* with password guidelines.

3.8 Compliance with password guidelines

PMT is a behavioral intentions model that explains how sources of information about threats can affect an individual's intentions to perform preventative measures (Maddux & Rogers, 1983; Rogers, 1975, 1983). In its original form, the PMT model does not explicitly predict actual behavior, but rather assumes that protective behavior is most appropriately predicted by behavioral intentions (Prentice-Dunn & Rogers, 1986; Weinstein, 1993). However, several studies have provided evidence to support incorporating actual behavior in the PMT model (Floyd et al., 2000; Milne & Milne, 2000). The model described in this study (see Figure 3.1) explicitly includes both intentions and actual behavior. The following sections describe the dependent variables *intentions to comply* with password guidelines and *actual password compliance*.

Based on the PMT construct protection motivation (Maddux & Rogers, 1983; Rogers, 1975, 1983), *intentions to comply* refers to the degree to which a user intends to follow a set of recommended password guidelines. PMT assumes that behavioral intentions adequately predict behavior and therefore the dependent variable is usually operationalized as a measure of intentions (Prentice-Dunn & Rogers, 1986). As such, in this research, the dependent variable *intentions to comply* captures the degree to which an individual is willing or planning to follow a set of recommended password guidelines.

Many studies have used PMT in its original form, where behavioral intentions is assumed to sufficiently represent actual behavior and thus no measure of actual behavior is included. For example, measures of intentions have been used in the health-related domain to examine intentions to undertake breast cancer self-examination (Rippetoe & Rogers, 1987) and to quit smoking (Maddux & Rogers, 1983). PMT based IS security studies, have also used measures of intentions such as

intentions to use anti-spyware programs (Johnston & Warkentin, 2010a), intentions to use anti-malware software (Lee & Larsen, 2009), intentions to comply with security policies relating to implementing encryption on portable media, locking computers and sharing passwords within an organization (Vance et al., 2012), and intentions to create strong unique passwords for online accounts (Zhang & McDowell, 2009).

Although the literature suggests that an individual's intentions to perform a particular task influences actual behaviors in many domains, there has been little research with respect to passwords examining the link between intentions and actual compliance. Therefore, the relationship between *intentions to comply* and *actual password compliance*, operationalized as password strength is explored in this study. Thus, this study investigates if behavioral change in users' *intentions to comply* with a set of recommended password guidelines leads them to actually create stronger passwords.

Studies (e.g., LaRose et al., 2008; Liang & Xue, 2010; Plotnikoff & Higginbotham, 2002) that have incorporated actual behavior in a model based on PMT, have provided evidence to support an extension of the PMT to include a link between intentions and actual behavior. Using the PMT, Plotnikoff and Higginbotham (2002) examined factors that motivate individuals to exercise. Their study found a strong significant relationship between intentions to get adequate exercise and actual exercise behavior. In the IS security domain, Liang and Xue (2010) also found a significant positive relationship between users' intentions to avoid the dangers of spyware and actually installing anti-spyware software. However, their model explained a larger variance in user intentions than actual behavior.

It is assumed that measures of intentions can predict behavior to some extent (Ajzen, 1991; Rogers, 1975, 1983). However, some studies suggest that the effects of manipulating the PMT variables are generally stronger on behavioral intentions than

on actual behavior (Floyd et al., 2000; Webb, 2006); for example, a medium sized change in behavioral intentions may not lead to a medium sized change in actual behavior, but rather a medium to small association (Webb, 2006). Further, findings from meta-analytical studies by Floyd et al. (2000) and Milne and Milne (2000) show that while the effect sizes for intentions tend to be large, the effect sizes for actual behaviors are typically smaller. As such, it is important to also examine the extent to which *intentions to comply* in this study can predict *actual password compliance*.

It is assumed that users' *intentions to comply* with password guidelines can predict users' *actual password compliance* or password strength, but the variance explained in *actual password compliance* could be low. However, it seems plausible that elevating a user's *intentions to comply* with password guidelines will increase likelihood of actually creating strong passwords. It is therefore hypothesized that:

H.11 *Intentions to comply* **is positively related to** *actual password compliance*.

3.9 Effects of fear appeals over time

Applications of persuasive communication, as described in the PMT framework, have typically considered the immediate effectiveness of fear appeals on motivating individuals to follow recommendations (Floyd et al., 2000; Milne & Milne, 2000). Similarly, applications of PMT defined fear appeals in IS security research have primarily examined the immediate effects of fear appeals on intentions (e.g., Johnston & Warkentin, 2010a) or actual behavior (Jenkins et al., 2013; Vance et al., 2013).

Longitudinal studies that have examined the long-term effectiveness of fear appeals provide evidence to suggest that the effects of fear appeal messages can be maintained over time (Floyd et al., 2000). However, there has been little research with respect to the long-term effects of fear appeals on compliance with password policies. Therefore

this study investigates if change in an individual's *intentions to comply* with a set of recommended password guidelines can be maintained over time. This study also explores if the ability to remember passwords, referred to as *password memorability* in this study, can be sustained over time following fear appeal communication. The following subsections describe the two dependent variables, *intentions to comply* and *password memorability*, examined for long-term effects.

3.9.1 Effects of fear appeals on intentions to comply over time

This study explores whether fear appeals will affect *intentions to comply* over time, following the fear appeals intervention. As the fear appeals used in this study are a form of security information and training intended to change behavioral intentions, this study aims to investigate if individuals are still motivated to comply with password guidelines once time has elapsed after the training. The information and training (fear appeal) used in this study corresponds with the four stimulus variables, magnitude of noxiousness, probability of threat occurrence and efficacy of available recommended response and self-efficacy, as described in PMT (Rogers, 1975, 1983). A key strength of the PMT is that it is a model for establishing experimental interventions (fear appeals) aimed at changing behavior, yet only few studies have explored the long-term effectiveness of fear appeals on behavioral change.

One such study is that of Wurtele and Maddux (1987), who examined the immediate and long-term effects of fear appeals on intentions to engage in regular exercise. To examine the long-term effects of the fear appeals, they conducted a follow-up study to determine if the change in behavioral intentions led to behavioral change two weeks following the intervention. The follow-up study examined behavioral change using measures of self-reported behavior by asking whether the participants' level of

exercise was the same, decreased or increased two weeks later. A study by Hodgkins and Orbell (1998) also suggests that changed behavioral intentions can also be maintained over an extended period of time. In their follow-up study, the participants were asked if they had intended to perform breast cancer examination in the past month. Although their study did not use fear appeals communication to manipulate the PMT variable, their findings suggest that intentions can be sustained over time. However, thus far no published IS security behavioral studies appear to have conducted a follow-up study to determine if fear appeals have a long term effect on compliance intentions.

Based on these findings, it is suggested that for users who receive fear appeals, changes in *intentions to comply* should be maintained over time. It is therefore hypothesized that:

H.12 Users who receive *fear appeals* will have **higher** *intentions to comply* over time than those who do not.

3.9.2 Effects of fear appeals on password memorability over time

Password memorability relates to the degree to which a user can remember a password. This study also explores whether fear appeal communication will have a long-term effect on *password memorability*. *Password memorability* is a key barrier to secure password practices (Inglesant & Sasse, 2010; Ur et al., 2012; Yan et al., 2004).

Users have difficulty remembering lengthy random characters (Yan et al., 2004; Zviran & Haga, 1993), in combination with the need to remember multiple unique passwords (Florêncio & Herley, 2007; Grawemeyer & Johnson, 2011; Helkala & Svendsen, 2012), they inevitably choose weak passwords. Training users how to create strong

passwords using a mnemonic technique where a password is created using the first letter of a sentence or phrase, improves password memorability (Helkala & Svendsen, 2012; Yan et al., 2004), Further, the use of a mnemonic technique has been shown to be an effective way of improving memory, both short-term and long-term (Hampstead et al., 2012).

Evidence suggest that mnemonic training can improve password recall (e.g., Vu et al., 2007; Yan et al., 2004). Further, although Yan et al. (2004) did not explicitly examine the long-term effects of the mnemonic technique, their results suggest that the mnemonic strategies may have had a long term effect password recall. In their study, the group that created mnemonic based passwords reported them to be significantly easier to remember, and of the three experimental groups, this group kept written copies of their passwords for the least amount of time. This suggests that the mnemonic technique improved ability to remember passwords long after the mnemonic passwords were created.

It therefore seems likely that users who receive fear appeal communications with a mnemonic training emphasis will have a more sustained ability to remember passwords over time. It is therefore hypothesized that:

H.13 Users who receive *fear appeals* with a mnemonic training emphasis will have **higher** *password memorability* over time than those who do not.

3.10 Chapter Overview

This chapter presented the research questions and hypotheses formulated for this study. With emphasis on the role of security perceptions and password efficacy perceptions, the objective the study described in this thesis is to provide insights into what motivates users to comply with password guidelines. The question of whether these

perceptions can be altered to improve compliance with password guidelines is also addressed in this study. A key component of this study is the use of fear appeals in eliciting change in IS password security behavior. This study seeks to investigate whether the effects of fear appeals can be sustained over time through a longitudinal study, which thus far has been overlooked in fear appeals based IS security research.

The theoretical framework proposed in this chapter is based on PMT (Rogers, 1975, 1983). PMT has received some support in IS security research (e.g. Herath & Rao, 2009; Johnston & Warkentin, 2010a; Vance et al., 2012; Woon et al., 2005; Workman et al., 2008) although studies (e.g., Crossler, 2010; Liang & Xue, 2010; Milne et al., 2009; Posey et al., 2011; Vance et al., 2012; Woon et al., 2005; Zhang & McDowell, 2009) have failed to consistently confirm the role of perceived vulnerability in explaining IS security behaviors. Therefore, the research model proposed in this study was a modified version of the PMT framework proposing a null relationship between perceived vulnerability and IS security behavior. The proposed model was extended to explore the role of prior exposure to hacking incident and the possibility of providing better insights into the role of perceived vulnerability in IS security behavior.

4 Research Methodology

4.1 Introduction

This chapter describes the methodology, participants and the procedure for data collection used in this study. This Chapter also presents the study materials used in this study including those used for a follow-up. Lastly, this chapter describes SEM, the primary data analysis techniques applied in this study, which includes a description of procedure for assessing the measurement and structural model.

4.2 Research design

This study takes a quantitative and experimental design approach. This study uses a between-group experimental design to examine the impact of fear appeals on compliance with password security guidelines. As suggested by Leventhal (1970) a design where one group is exposed to fear appeals and another is not was chosen for this study. Thus, the study was designed so that a treatment group was exposed to fear appeal messages about the prevalence and potential consequences of password related threats, the effectiveness password guidelines, a password training session, and a questionnaire used to assess the influence of the fear appeals upon threat and efficacy perceptions, and compliance with password guidelines. The control group was unexposed to the fear appeal messages.

This study used two kinds of study materials: i) password security information and training materials, representing fear appeals, and (ii) a survey instrument measuring the participants' background information and the variables related to the research model described in this thesis. The control group completed the survey only; while the treatment group was exposed to the password security information and training

material and completed the survey. To assess the impact of fear appeals on actual compliance (password strength), passwords were collected from both study groups.

Data was collected in two phases. Phase I is where the participants' background information and initial levels of study variables were measured and also when the treatment group undertook the password security information and training session. Phase II was a post-training follow-up session undertaken to determine whether the effects of fear appeals are maintained over time. The second phase was conducted six weeks after completion of phase I.

4.3 Participants

As the target population for this study was Internet users who hold at least one online email account, data collected through an online questionnaire was not only appropriate but also ensured that the respondents held an online email account. Only participants who were 18 years of age or over were recruited, making the background variable *age* the only exclusion criteria for this study. Participants were sought from a wide spectrum of backgrounds including gender, level of education, computer skills and computer security knowledge. Having a group of participants from a wide range of backgrounds is of importance to the generalizability of the research findings.

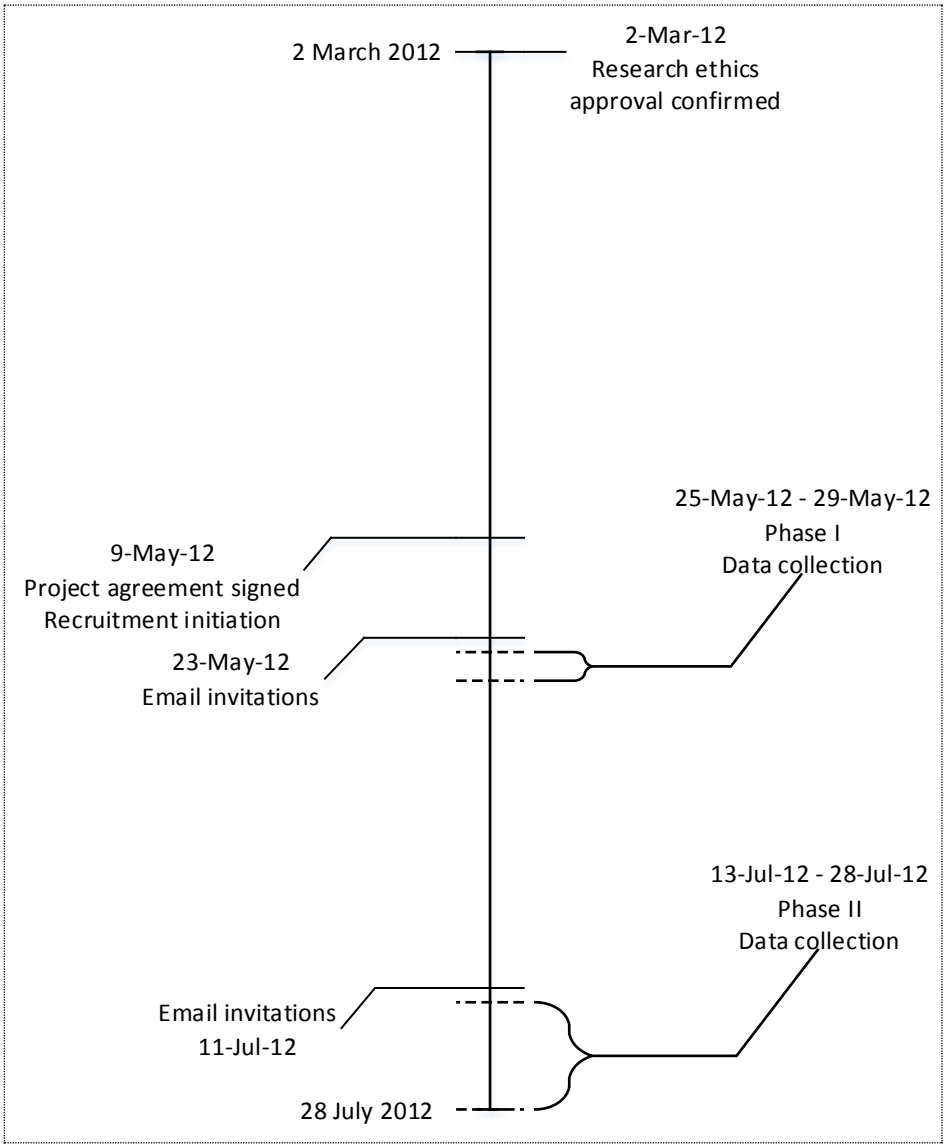
A sample size of ≥ 200 per study group was sought for this study. Details of how the sample size was estimated are described in Section 4.8.1.1. To ensure that the participants met the required sample size of ≥ 200, and fit the target population for this study, a third party recruiting company located in the United Stated (Authentic-Response, 2012), was used. Using the recruiting company ensured that the participants were recruited from a wide cross-section of Internet users and that the required sample

size was achieved. A similar recruitment method was used by Bulgurcu et al. (2010) in their study investigating employee IS security compliance.

4.4 Phase I data collection procedure

This section describes the procedure for Phase I data collection. Figure 4.1 is an overview of the timeline of the recruitment and data collection process and shows an overview of Phase II.

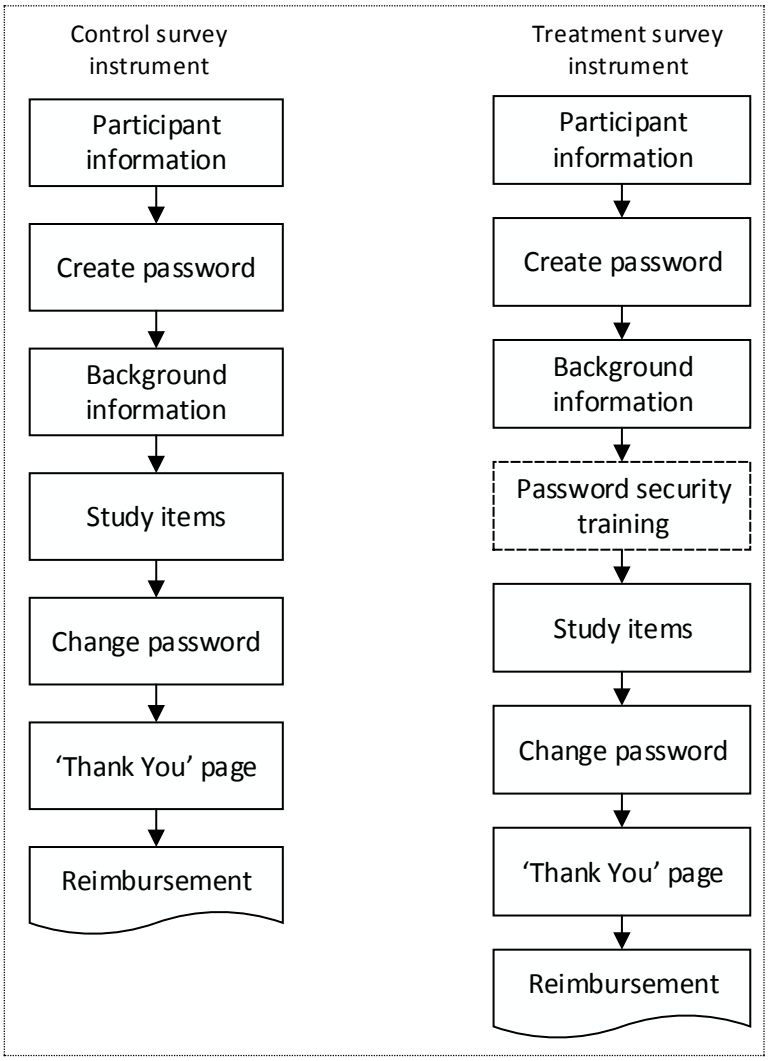
Figure 4.1: Timeline of the recruitment and data collection process



Prior to data collection ethics approval was sought from the Murdoch University Human Research Ethics Committee (HREC) under Permit No. 2010/218 (see Appendix A, for a copy of the HREC approval). Authentic Response Inc. was contacted to prepare a project agreement, after which the email invitation was prepared. The participants were then contacted directly and invited by Authentic Response Inc. to participate in this study through an online survey. Using census balanced random sampling, a form of stratified random sampling, 3830 email invitations were distributed to the panel members who were randomly allocated to either the control or treatment group. The email invitations (see Appendix B) contained information on reimbursement for participating and a direct link to the version of the online survey the potential participant was to use. The reimbursement was points-equivalent to approximately $1.50 - $2.00 US dollars each, where the points could be used to claim a reward.

Figure 4.2 shows an overview of the order in which data was collected for the control and treatment group respectively, for Phase I of the study. On the first page of the survey, labeled "Participant Information", potential participants were presented with background information about the study and the expected duration of the study. The participants were also informed of their right to privacy and provided with the opportunity to consent to participate by clicking on a check box. Here they were also informed that they would be rewarded for participating.

Figure 4.2: Overview of the data collection procedure for Phase I



As depicted in Figure 4.2 two separate survey instruments were prepared for the two study groups, and administered online using SurveyGizmo version 3.1 (2012). As, one of the objectives of this research was to determine if the password security information and training session completed by the treatment group would improve compliance with password security guidelines as well as improve password strength, two sets of passwords were collected.

To obtain passwords the participants were required to create a password at the start of the survey, right after the Participant Information page, and also at the end they were asked to change their passwords. To collect the first set of passwords, participants were

instructed to create passwords that they would use to return to the survey hosting website to complete the follow-up study (Phase II) and to view the preliminary results from Phase I. This was done to ensure that the passwords created were realistic and representative of actual passwords used on the Internet.

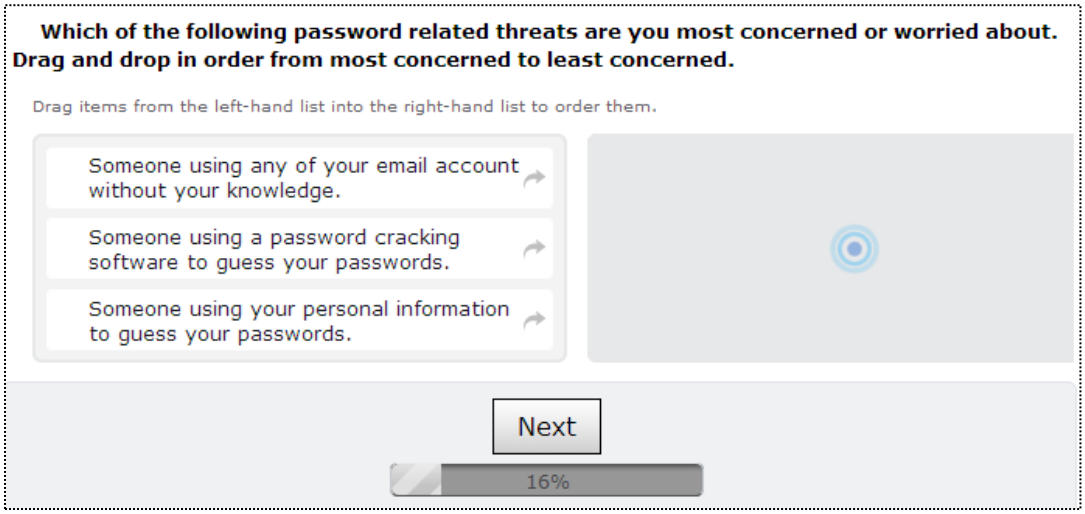
After creating the first password, the control group completed two sections containing 56 items; these included background information (including self-reported knowledge of computer security) and measures of the constructs in the proposed research model: *exposure to hacking*; *perceived severity*; *perceived vulnerability*; *perceived threat*; *perceived password effectiveness*; *perceived cost*, *password self-efficacy*; *intentions to comply* with password guidelines; and *actual password compliance*. This was completed in approximately 15 minutes.

The treatment group first completed the background information section, followed by the password security information and training session. The treatment group then completed the section to measure the model constructs. As the intention was to influence participants' perceptions, the password security information and training session was completed after the collection of background information, but prior to collection of data relating to the model. To ensure that the treatment group paid attention to the password security information, they also completed an interactive question and answer session.

See Figure 4.3 for a sample of the interactive questions and answers used in this study. The questions were directly related to the password security information presented. A similar approach was used by Maddux and Rogers (1983) to ensure that respondents paid close attention to the treatment materials used in their study, and to maximize the effects of the intervention material. After the password security information session, the treatment group completed the second section which consisted of the measures of

the variables in the proposed model. Their session took approximately 25 minutes in total.

Figure 4.3: A sample interactive questions and answer



Prior to completing the survey session, on the second to last page of the survey, the second set of passwords was collected. As mentioned earlier, the two sets of passwords were collected to examine if password strength was improved. To examine if there were any group differences in password strength, a second password was collected from the control group as well. The participants were asked to change their previously selected password and to ensure that their new password was strong but easy to remember. This was to ensure that both groups were given equal opportunity to create passwords that they perceived as strong and easy to remember.

On the final page of the survey, labeled “Thank You”, the participants were informed that after completing the study, they would automatically be re-directed back to the Authentic Response Inc. website to receive reimbursement. The Thank You page also reminded the participants to keep their passwords safe as they would need them to return to the website. The participants were then automatically redirected to Authentic Response website.

4.5 Password security information and training materials

The password security information and training materials represented the four components of fear appeals discussed in Section 3.4. The materials consisted of four information segments: i) *vulnerability information*; (ii) *severity information*; (iii) *password effectiveness information;* and (iv) a *password training* exercise. To ensure that the amount of information in each segment was balanced, each segment contained roughly the same word count, ranging from 327 to 375. A similar approach was used by Maddux and Rogers (1983) and also Rippetoe and Rogers (1987) to administer the fear appeal messages in their study. Copies of the password security information and training materials discussed below are located in Appendix C.

4.5.1 Vulnerability information

The first segment of the password security information contained statements that emphasized the likelihood of being exposed to password related threats, and information about existing password threats and countermeasures. The information was based on the NIST Guide to Enterprise Password Management (Scarfone & Souppaya, 2009), the United States Computer Emergency Readiness Team's (US-CERT) guidelines on choosing and protecting passwords (McDowell et al., 2009) and the Certified Information Systems Security Professional (CISSP) (Stewart et al., 2008).

4.5.2 Severity information

The second segment of the password security information contained statements that emphasized the consequences and severity of password related threats. The information was also based on the NIST (Scarfone & Souppaya, 2009) password guidelines, US-CERT (McDowell et al., 2009) and CISSP (Stewart et al., 2008). This

segment was a follow on from the vulnerability information segment and described possible consequences of password related threats such as hacking.

4.5.3 Password effectiveness information

The password effectiveness segment of the password security information material focused on countermeasures described in the NIST (Scarfone & Souppaya, 2009) password guidelines and US-CERT (McDowell et al., 2009), with emphasis on their effectiveness. This segment consisted of a list of six preventative measures such as avoiding dictionary words or using a combination of upper and lowercase letters, numbers and special characters and described how these measures can make passwords difficult to crack.

4.5.4 Password technique information

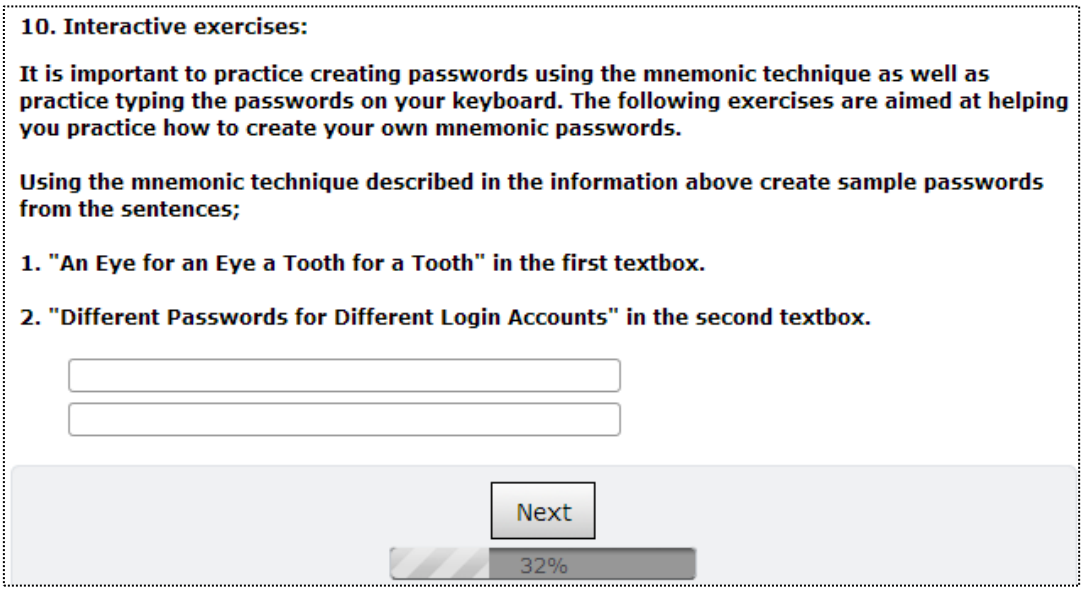
Lastly, participants were presented with training on how to create strong memorable passwords using the mnemonic password selection technique. A mnemonic password selection technique is a method of creating passwords using letters from a sentence or a familiar phrase. The information presented in this study was based on a password instructional sheet used in an experimental password study by Yan et al. (2004).

In addition to being presented with several examples of how to apply the technique, participants were also given an opportunity to practice creating passwords using the mnemonic technique via interactive exercises included as part of the training segment, as shown in Figure 4.4.

The interactive exercises involved creating mnemonic passwords using two different English phrases; “An Eye for an Eye a Tooth for a Tooth” and “Different Passwords for Different Login Accounts”. Vance et al. (2013) found that adding interactivity in password training improves the efficacy of the training (Vance et al., 2013).

Furthermore, while static fear appeals have been shown to elicit changes in perceptions, perceived self-efficacy alone is no substitute for a lack of ability (Bandura, 1977, 1982), thus as a reinforcement, the interactive practice session was proposed.

Figure 4.4: Interactive exercises



4.6 Phase I survey instrument

As mentioned in Section 4.4, the survey instrument used in Phase I was split into two major sections. The first section contained items to measure background and demographic variables. The second section consisted of items measuring the constructs in the research model as follows: *exposure to hacking*, *perceived severity*, *perceived vulnerability*, *perceived threat*, *perceived password effectiveness*, *perceived cost*, *password self-efficacy*, *intentions to comply* with password guidelines, and *actual password compliance*. The development of the instrument involved a review of many existing survey instruments. To ensure validity and reliability of the measures used, previously validated items were adopted where possible. See Appendix D for the complete survey instrument.

4.6.1 Exposure to hacking

The construct *exposure to hacking* relates to whether a user or someone they know personally has ever had their online account hacked into and the degree to which the experience affected them. Two items, shown in Table 4.1 were used to measure the construct. The items relate to negative impact experienced personally and through others who have been impacted by hacking. The items used to measure this construct were adapted from the items used in a study by Boss (2007), to measure how participants have been impacted by computer security threats such as virus infection. In his study, Boss reported a Cronbach alpha of 0.80.

Only some participants or people they know personally are likely to have fallen victim to hacking. Therefore, the items used in this study were measured on a score of zero (0) if participants answered 'no' to being hacked or a 7-point scale indicating the degree of impact with a score of (1) for 'low impact' and (7) for 'high impact'.

Table 4.1: Items used to measure the construct *exposure to hacking*

Many web users have email accounts set up for receiving important information such as email messages from friends and family members, online banking notifications and online shopping confirmation. **For the purpose of this study, we classify such email accounts as 'important' email accounts.**	
HACKED01	Have you ever had your important email account, online shopping account or online banking account hacked into? If yes, please indicate the degree to which that experience affected you (in terms of lost data, lost time, monetary losses, identity theft etc.) If no, please select 'no'.
HACKED02	Has someone you know personally ever had their important email account, online shopping account or online banking account hacked into? If yes, please indicate the degree to which that experience affected them (in terms of lost data, lost time, monetary losses, identity theft etc.) If no, please select 'no'.

4.6.2 Perceived vulnerability

The construct *perceived vulnerability* refers to the degree to which a user believes that they are likely to experience password related threats. The items developed for this

study were adapted from those used by Zhang and McDowell (2009). Their study used three items to measure users' perceived vulnerability to password guessing and password cracking. Their items were used as a starting point in developing the items for this study.

The four items shown in Table 4.2 were used in this study and measure *perceived vulnerability* on a 7-point scale ranging from (1) labeled 'strongly disagree' and (7) labeled 'strongly agree'.

Table 4.2: Items used to measure *perceived vulnerability*

Consider the passwords you use to log into your important email accounts and where you keep the password, for example on a piece of paper or saved on your computer etc. **To what extent do you agree or disagree with the following statements?**	
PVUL01	There is a chance that someone could successfully guess at least one of my passwords
PVUL02	There is a chance that someone could successfully crack at least one of my passwords using password cracking software
PVUL03	There is a chance that someone could hack into at least one of my important email accounts
PVUL04	If someone hacked into my important email account, there is a chance that they could guess my other important passwords

4.6.3 Perceived severity

The construct *perceived severity* relates to the degree to which a user believes that if they were exposed to password related threats the impact would be detrimental. The items used by Zhang and McDowell (2009) to measure users' perceived severity of password threats and were used as a starting point in developing the items for this study.

In this study, the six items shown on Table 4.3 were used to measure *perceived severity.* They were measured on a 7-point scale where (1) indicated 'not at all severe' and (7) indicated 'very severe'.

Table 4.3: Items used to measure *perceived severity*

Consider the type of information you have saved in your important email accounts and the type of passwords you use for logging into your important email accounts. **How severe do you think the consequences would be if:**	
PSEV01	Someone successfully guessed any of your important email passwords
PSEV02	Someone hacked into any of your important email accounts
PSEV03	Someone used any of your important email accounts to send messages to your contact list without your knowledge
PSEV04	Someone obtained your personal information from your important email accounts
PSEV05	Someone changed the password to your important email accounts without your knowledge
PSEV06	Someone stole the password to one of your important email accounts

4.6.4 Perceived threat

The construct *perceived threat* relates to the degree to which users are worried about password related threats. In PMT literature, this is referred to as fear arousal and described using mood adjectives such as frightened, anxious, nervous or worried. The items developed for this study were adapted from those developed by Milne et al. (2002) to investigate the degree to which respondents felt frightened, scared or worried. The items (see Table 4.4) were modified to reflect concern for password related threats.

Table 4.4: Items used to measure *perceived threat*

Please indicate the extent to which you agree or disagree with the following statements.	
PTHR01	The thought of someone guessing the password to any of my important email accounts makes me worried
PTHR02	The thought of someone hacking into any of my important email accounts makes me worried
PTHR03	The thought of someone using any of my important email accounts without my knowledge makes me worried
PTHR04	The thought of someone using my personal information from any of my important email accounts makes me worried
PTHR05	The thought of someone changing or deleting information obtained from any of my important email accounts makes me worried
PTHR06	The thought of someone using password monitoring software to record my important passwords makes me worried

The six items shown in Table 4.4 were used to measure the construct *perceived threat* on a 7-point Likert scale where (1) indicated 'strongly disagree' and (7) indicated 'strongly agree'.

4.6.5 Perceived password effectiveness

The construct *perceived password effectiveness* refers to the degree to which a user believes the recommended password guidelines will prevent password related threats. The items developed for this study are adapted from those used by Zhang and McDowell (2009).

Based on the PMT construct response efficacy (Maddux & Rogers, 1983; Rippetoe & Rogers, 1987), the items developed in the study by Zhang and McDowell measure the degree to which participants believe that password rules such as using strong passwords would protect their online accounts. Their items had a Cronbach alpha of 0.96. In this study, the items were also based on the recommended password guidelines described in the NIST (Scarfone & Souppaya, 2009) password guidelines and US-CERT (McDowell et al., 2009). The degree to which a user believes that these guidelines are effective was assessed.

The construct *perceived password effectiveness* was measured using the six items shown in Table 4.5 and is measured on a 7-point scale where (1) is labeled 'strongly disagree' and (7) is labeled 'strongly agree'.

Table 4.5: Items used to measure *perceived password effectiveness*

Please indicate the extent to which you agree or disagree with the following statements.	
PEFF01	Making sure that my passwords contain a combination of numbers, letters and symbols will prevent my passwords from being guessed
PEFF02	Making sure that my passwords do not contain any dictionary words will make them more difficult to guess
PEFF03	Making sure that my passwords do not contain personal information such as my date of birth will make them more difficult to guess
PEFF04	I can protect my online accounts better if I use a different password for each of my online accounts
PEFF05	I can protect my online accounts better if I change my passwords regularly
PEFF06	I can protect my online accounts better if I use a long complex password

4.6.6 Password self-efficacy

The construct *password self-efficacy* refers to the degree to which a user believes they are capable of creating strong passwords. The items used in this study were adapted from the computer self-efficacy items developed by Compeau and Higgins (1995) to measure respondents' confidence in their software skills. Their measure of computer self-efficacy relates to a user's confidence in performing unfamiliar computing tasks given a range of circumstances. For example, participants in their study indicated whether they were confident in using unfamiliar computer software if they had step-by-step instructions or written manuals. Their instrument consisted of 10 items measured on a 10-point scale from (1) 'not at all confident' to (10) 'totally confident' with a reported Cronbach alpha of 0.95.

In this study, the four items shown in Table 4.6 were developed to measure password self-efficacy. The items are similar to those used by Compeau and Higgins (1995) with slight modifications aimed to reflect a typical password login environment. The four items used in this study also relate to a range of circumstances that users face when creating passwords such as availability of time or instructions. Such circumstances are said to have a significant effect on an individual's confidence in performing unfamiliar

tasks (Bandura, 1991; Compeau & Higgins, 1995). The construct password self-efficacy was measured using a 7-point scale where (1) indicated 'not at all confident' and (7) indicated 'totally confident'.

Table 4.6: Items used to measure *password self-efficacy*

Consider the following scenario. Due to an increase in password hacking incidents, the password requirements for your email account have been changed. You have been asked to change your password immediately and to make sure that your new password follows strict password guidelines provided by the system. **Please indicate how confident you are that you would be able to create a password that is strong enough to protect your email account from being hacked into.** **I would be able to create a strong password that is difficult to hack...**	
PSEF01	If I had instructions on how to create a strong password
PSEF02	If I had step-by-step instructions on how to memorize a strong password
PSEF03	If I had a lot of time to create a strong password
PSEF04	If I had used strong passwords before

4.6.7 Perceived cost

The construct *perceived cost* relates to the degree to which a user believes that remembering passwords would be difficult if password guidelines were followed. *Perceived cost* corresponds to the response cost construct described in PMT (Rippetoe & Rogers, 1987). The items in this study were adapted from the measurement instrument used by Milne et al. (2002) to operationalize the PMT construct, response cost. Milne et al. (2002) used a 4-item scale to measure participants' beliefs about the cost of exercising at three different times yielding an average Cronbach alpha of 0.75.

In this study, the objective was to create items that measure beliefs about difficulty in remembering passwords when specific guidelines are followed. The items used by Milne et al. (2002) were adjusted to match the password guidelines recommended by the US-CERT (McDowell et al., 2009). The six items shown in Table 4.7 were developed for this study and measured using a 7-point scale where (1) was labeled 'strongly disagree' and (7) was labeled 'strongly agree'.

Table 4.7: Items used to measure *perceived cost*

Please indicate the extent to which you agree or disagree with the following statements.	
COST01	Remembering a password that contains a combination of numbers, letters and symbols would be difficult
COST 02	Remembering a password that is long and complex would be difficult
COST 03	Remembering a password that does not contain any dictionary words would be difficult
COST 04	Remembering a password that does not contain personal information such as date of birth would be difficult
COST05	If I use different passwords for each of my web accounts, it would be difficult for me to remember them all
COST06	If I change my passwords regularly, it would be difficult for me to remember them

4.6.8 Intentions to comply

Based on the PMT construct *protection motivation* (Maddux & Rogers, 1983), in this study *intentions to comply* represents the degree to which a user intends to follow a set of recommended password guidelines. This study investigates users' willingness or intentions to comply with a set of password guidelines on their important online email accounts. This study described an important email account as an email account set up for receiving important information such as email messages from friends and family members, online banking notifications and online shopping confirmations. The items used to measure *intentions to comply* were adapted from items developed by Bulgurcu et al. (2010) based on Ajzen's TPB (Ajzen, 1991). Bulgurcu et al. (2010) reported a Cronbach alpha of 0.977.

Table 4.8 shows the six items used to measure the construct *intentions to comply* with password guidelines. The items measure participants' *intentions to comply* with password guidelines as described in the NIST (Scarfone & Souppaya, 2009) password guidelines and the US-CERT's recommendations for choosing and protecting passwords (McDowell et al., 2009). The items were measured on a 7-point scale where (1) was labeled 'not at all likely' and (7) was labeled 'very likely'.

Table 4.8: Items used to measure *intentions to comply* with password guidelines

If you were required to change the password for one of your important email accounts, to what extent would you agree or disagree with the following statements.	
INTC01	I would choose a password that follows the password length requirement suggested by the system
INTC02	I would choose a password with a combination of numbers, letters, and symbols as suggested by the system
INTC03	I would choose a password that is difficult to guess
INTC04	I would choose a password that follows all the guidelines provided by the system
INTC05	I would choose a password that is different from my old password
INTC06	I would choose a password that is different from my other online passwords

4.6.9 Actual password compliance

In this study, the construct *actual password compliance* represents password strength. Password strength was calculated for the two passwords collected using the survey instrument for Phase I. Different studies have measured password strength in a variety of ways. For example, studies have used password cracking tools to estimate how long it would take to crack a password (Cazier & Medlin, 2006; Mazurek et al., 2013; Vu et al., 2007; Weber et al., 2008; Zhang et al., 2010). However, this method of measuring password strength has some limitations. First, numerous password cracking tools exist today, most of which use different cracking algorithms making some more efficient than others (Cazier & Medlin, 2006). In addition, the amount of time it takes to crack a password using cracking software can vary depending on a computer's processor speed. Should a password cracking tool be used, the processor speed should at least be reported as did Zhang et al. (2010) whose study also used the password cracking method.

Another method of measuring password strength is to determine the degree of character variation in a given password, also known as *entropy* or unpredictability of a password (Shay et al., 2010). Entropy is a "measure of uncertainty" (Shannon, 2001 p. 21) and can be applied in different areas of communication (Burr et al., 2013; Burr et

al., 2006). In relation to passwords, entropy, generally measured in bits, is a measure of unpredictability of passwords, or how difficult a password is to guess (Burr et al., 2013; Burr et al., 2006; Komanduri et al., 2011). This method has an advantage because it uses a mathematical formula to calculate password strength, and thus independent of a computer's processor speed. Additionally, lack of character variation is a key problem with user created passwords (Burr et al., 2013; Burr et al., 2006; Jermyn, Mayer, Monrose, Reiter, & Rubin, 1999). Therefore measuring password strength using a measure of character variation (entropy) seemed appropriate for this study.

In this study, password strength was measured using Shannon's (2001) formula for calculating entropy (see Table 4.9). Password strength guidelines included in the password strength measurement are based on the NIST (Burr et al., 2013; Burr et al., 2006; Scarfone & Souppaya, 2009) password guidelines.

Table 4.9: Character combinations and corresponding entropy used in this study

Group	Group combination	Total possible characters	Entropy per character (bits)
1	SC	32	5.000
2	N	10	3.322
3	SL	26	4.700
4	CL	26	4.700
5	SC, N	42	5.392
6	SC, SL	58	5.858
7	SC, CL	58	5.858
8	N, SL	36	5.170
9	N, CL	36	5.170
10	SL, CL	52	5.700
11	SC, N, SL	68	6.087
12	SC, N, CL	68	6.087
13	SC, SL, CL	84	6.392
14	N, SL, CL	62	5.954
15	SL, N, SL, CL	94	6.555
SC = Special Character; N = Number; SL = Small Letter; CL = Capital Letter			

To calculate password entropy using Shannon's formula two key units of information must be determined from a given password. First, the number of possible characters based on the 94 printable standard keyboard character-set (labeled character width) is determined. Then the actual number of characters in a password is totaled. Using these two values, the number of attempts an attacker would need to try out all possible combinations in a password cracking attack can be calculated. The resulting value is measured in bits; a high bit value indicates a strong password.

The following two examples illustrate how password entropy was calculated in this study. The first example is a 9-digit pin code selected from a combination of any of the 10 digits found on a standard keyboard. The character width or the number of possible characters is 10 as each digit has 10 possible choices. The pin code has an entropy of 3.322 bits per character[1] and a total entropy of (9*3.322) = 29.898 bits. In other words, each character adds 3.322 bits of entropy to the password or $2^{3.322}$ possible combinations.

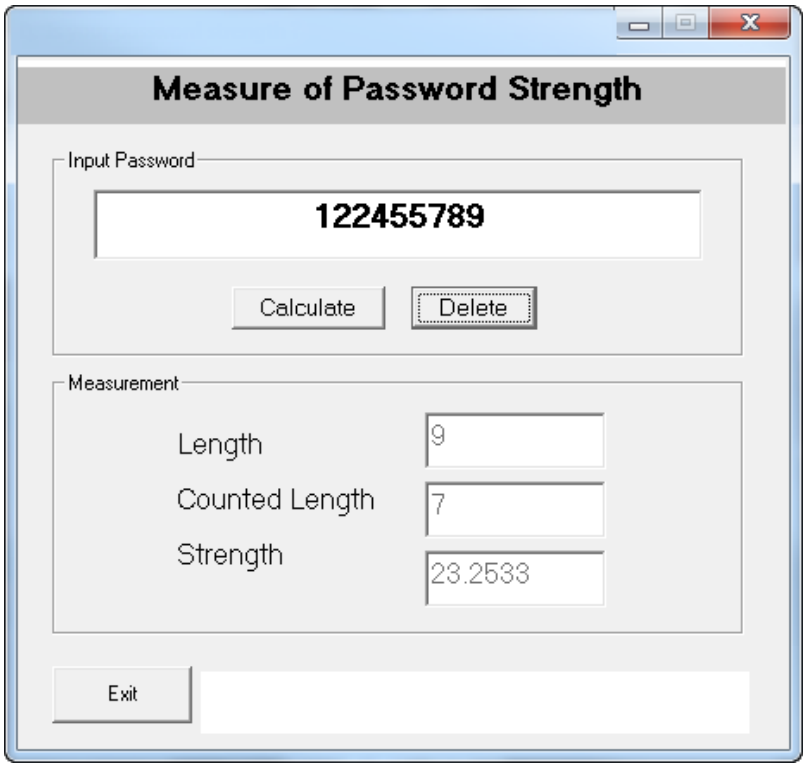
The second example is of a 9 character password selected from a combination of any of the 94 printable standard keyboard characters. The password can have a combination of numbers, upper and lowercase letters, and symbols, giving it a character width of 94, an entropy of 6.555 bits per character[2] and a total entropy of (9*6.555) = 58.995 bits. However, if any of the characters are repeated, the total entropy is reduced. For example, the total password entropy of the 9 digit pin "122455789" is reduced to (7*3.322) = 23.25 bits. The higher the password entropy (in

[1] Entropy per character for a PIN number with a width of 10 = $Log_2(W) = Log_2(10) = 3.322$
[2] Entropy per character for a password with a width of 94 = $Log_2(W) = Log_2(94) = 6.555$

bits) the greater the number of possible values (2^{bits}) which would take an attacker a longer time to guess (Burr et al., 2006).

To automate the process of calculating password strength, a password analysis tool was developed and coded in Visual Basic. Figure 4.5 shows how the password strength of the 9 digit pin "122455789" was calculated using the password strength analysis tool.

Figure 4.5: Password strength analysis tool used in this study



Once the password strength was calculated a repeated measures ANOVA was conducted to determine if there was a significant increase in password strength after the training. To examine if there was an improvement in password strength, password strength was also examined within each group comparing the passwords created at the beginning of the study (time 1) and the passwords created at the conclusion of the study (time 2). Then a within-group ANOVA was conducted to determine if the improvement was a result of the training.

4.7 Phase II data collection

This section describes the data collection procedure and survey instruments used in the follow-up session designed to address the research question of whether the effects of fear appeals can be maintained over time. Data was collected from the participants who completed Phase I and who were invited back to complete Phase II. However, as the participants were to remain anonymous there were no unique values attached to the participants to identify them across the two phases.

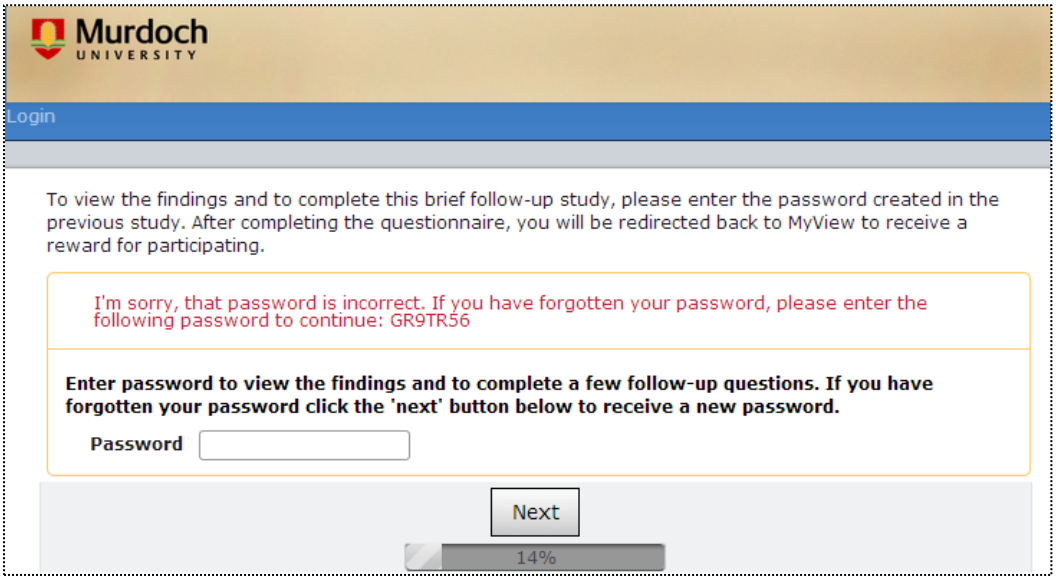
One survey instrument was prepared. The survey instrument was organized into three sections: i) a login section where participants entered the password created in Phase I, ii) items measuring *password memorability*, and (iii) a final section measuring *intentions to comply* at follow-up. Both groups completed the same survey questionnaire. However, data was collected from the control and treatment groups separately. Therefore, two separate online surveys were used for the follow-up data collection and administered using SurveyGizmo version 3.1 (2012).

4.7.1 Phase II data collection procedure

Data collection for Phase II followed six weeks later from Phase I, and was conducted (see Figure 4.1). Both control and treatment group participants were invited back via an email from Authentic Response Inc. to complete a follow-up questionnaire and to view the preliminary results from Phase I. A copy of the email invitation is located in Appendix E. Access to the follow-up questionnaire required the participants to enter the passwords created at the end of Phase I. In anticipation that some participants would forget their passwords, a generic password, as shown in Figure 4.6, was created and issued to those who forgot their passwords at the login screen. The generic

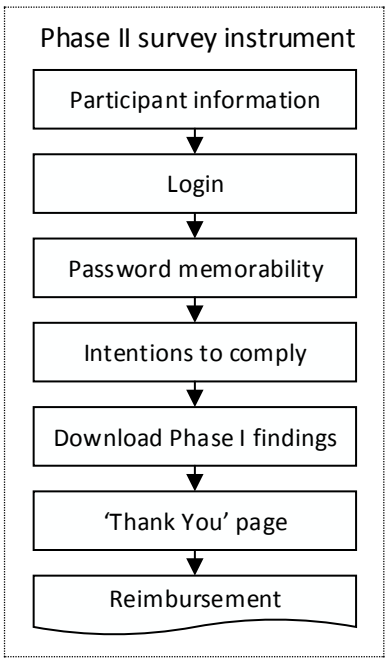
password was also used during analysis to determine the proportion of the participants who forgot their previously created passwords.

Figure 4.6: Phase II login screen



On the first page of Phase II survey, the returning respondents were presented with information about this Phase of the data collection and the approximate duration of the study (see Figure 4.7 for an overview of the survey instrument).

Figure 4.7: Overview of the data collection procedure for Phase II



The participants were also informed of their right to privacy and provided with the opportunity to consent to participate by clicking on a check box. Here they were also informed that they will be reimbursement. Lastly, to assess if there were any changes to compliance intentions, the participants completed the same items described in Section 4.6.8, measuring the construct *intentions to comply*. For both groups, Phase II survey was completed in approximately 5 minutes.

4.7.2 Phase II survey instrument

The survey instrument was used to collect three types of information (see Appendix F for the complete follow-up survey instrument). It was first used to collect actual passwords created in Phase I. Password information was collected at the login section where participants entered their previously created password or generic password. The next two sections of the follow-up survey consisted of items to measure *password memorability* and *intentions to comply* respectively. The items used to measure *intentions to comply* are identical to the ones used in Phase I (see Section 4.6.8).

The construct *password memorability* relates to the degree to which a user can remember a password. The construct *password memorability* is operationalized using two constructs: *actual password memorability*, which refers to whether they can actually remember their password, and *perceived password memorability*, which refers to whether they perceive their password as easy to remember. The measure of *actual password memorability* was to gauge whether the participants used the generic password or the original password.

The measure of *perceived password memorability* consisted of one item, "It was easy for me to remember the password I created for this study". The item was based on a measure of perceived ease of use in a study of usability of passphrases by Keith et al.

(2007). In this study, the item was modified to measure perceived ease of password recall using a 7-point scale where (1) indicated 'strongly disagree' and (7) indicated 'strongly'.

4.8 Data analysis techniques

Data management was performed using SPSS version 19. However, the primary data analysis methods elected for this study was Structural Equation Modeling (SEM) using AMOS version 19 (Arbuckle, 2010a), while multivariate analysis of variance (MANOVA) and analysis of variance (ANOVA) were used to examine group differences.

A one-way MANOVA was conducted to examine the overall effect of the fear appeals (the password security information and training) on the participants' password threat perceptions and efficacy perceptions. One-way ANOVA was also conducted on individual variables to test the hypothesis that the participants who were presented with the training materials will have a higher *perceived severity, perceived vulnerability, perceived threat, perceived password effectiveness, password self-efficacy, perceived cost* and *intentions to comply* with password guidelines than those who were not. A composite score was computed for each latent variable using regression imputation in AMOS version 19. A split-plot ANOVA with repeated measures and a between group analysis was conducted to examine if the participants who were presented with the training materials will have a higher password strength. The computed composite score is based on the factors scores of the measurement items.

SEM is one of many multivariate analysis techniques available today. Other examples of multivariate analysis techniques include multiple regression, factor analysis and

MANOVA (Hair, Black, Babin, Anderson, & Tatham, 2010). What separates SEM from other multivariate analysis techniques is SEM's ability to combine different aspects of multivariate analysis techniques (factor analysis and multiple regression) and simultaneously estimate relationships between numerous latent variables while examining relationships among observed variables.

In addition to performing simultaneous parameter estimation, the SEM method separates estimation of errors associated with the measurement model to account for any unexplained phenomenon. Ultimately the measurement models and structural models are examined, and in the process errors associated with each measurement item are accounted for as well. SEM allows for simultaneous examination of multiple observed variables and their latent constructs and relationships amongst the latent constructs. This also means that multiple relationships can be explored at the same time.

In SEM, the concept of latent construct or latent variable is used to describe a variable that cannot be measured directly (Byrne, 2010). Because a latent construct represents a phenomenon that is not directly quantifiable, an indirect measure of the latent construct is used to operationalize the latent variable. For example, in this study the latent construct *perceived vulnerability* cannot be measured directly. Therefore, a set of measurement items, also known as observed variables, were used to measure the latent construct *perceived vulnerability*. The terms latent construct, unobserved variable or latent variable are synonymous.

SEM has two distinct types of model, structural model and measurement model, which relate to the multiple regression analysis and factors analysis upon which SEM is based. The structural model comprises a set of dependent relationships between latent variables. A single-headed arrow is typically used to represent the relationships. The

measurement model is a set of observed variables and their underlying latent constructs. The measurement component, models relationships of the measurement items to the underlying latent variable and enable the ability to assess the underlying construct.

Although SEM allows for a one-step approach to testing models, that is, a simultaneous estimation of relationships amongst multiple observed variables and their underlying latent variables combined with path analysis, a two-step approach is recommended instead (Anderson & Gerbing, 1988; Hair et al., 2010). A two-step approach involves assessing the measurement model first then testing the structural model for relationships. The first step is the assessment of the measurement model, which involves establishing model fit and validity of the observed and latent variables before testing the structural model. Whereas the second step is when the path model is tested and significance of hypothesized relationships amongst the latent variables is assessed. The two-step approach to SEM ensures that any issues with the measurement model are dealt with and eliminated where necessary before proceeding with path analysis. As such, a two-step approach was used in this study to first identify and assess the measurement model before testing the structural model. The following sections describe the two-step SEM process undertaken in this study.

4.8.1 Measurement Model

The goal of measurement model assessment is to firstly find measurement items that best represent the underlying latent construct, then to assess the items for validity and finally to evaluate how well the observed data fit the hypothesized model (Anderson & Gerbing, 1988; Hair et al., 2010). As it is rare to find one measurement item that perfectly measures a latent construct, multiple observed variables are used. Observed variables are a major part of the data collection process. For example, observed

variables in this study are the responses collected from the online questionnaire described in Section 4.6. A set of these responses (observed data) represent an underlying construct, the latent variable. As it is expected that the observed items do not entirely measure the latent constructs, the measurement model must also account for this expected inaccuracy. This measurement inaccuracy is known as measurement error in SEM. Therefore, during the first step of the two-step SEM process, observed variables and their associated errors are specified.

Once data is collected the observed variables must be assessed for construct validity. Construct validity estimates how well the observed variables measure the latent construct they are designed to represent (Hair et al., 2010). Since structural model analysis involves examining relationships between latent constructs, construct validity was assessed prior to analysis of the structural model. Although, the measurement items used in this study are from previously validated items, evidence of construct validity is of importance and was sought for this study. Construct validity is implies that the hypothesized latent constructs are distinct from each other, represented as discriminant validity, and that the observed variables have high factor loadings on the construct they represent, represented as convergent validity. The indicators of discriminant validity and convergent validity are described next.

Discriminant validity is a measure used to demonstrate that latent constructs are truly different from each other. Each set of observed variables is unidimensional and represent only one underlying latent construct. To show that a set of items are unidimensional and that the latent constructs are distinct, there should be no cross loadings between latent constructs and no cross loadings between correlated error terms (Anderson & Gerbing, 1988; Hair et al., 2010). This means that a set of latent constructs that cross load is indicative of discriminant validity problems. This can be

determined by examining the Modification Indices (M.I.) in AMOS where large values between items indicate cross loadings.

In addition to assessing the uniqueness of each latent construct, in this study a more rigorous measure of discriminant validity based on Average Extracted Variance (AVE) values (Fornell & Larcker, 1981; Hair et al., 2010) was also used. AVE is the average percentage of variance explained by the observed variables for a latent construct or the amount of variance observed variables have in common (Hair et al., 2010), as shown in the formula below. The AVE values of two latent constructs should be greater than the square of the correlation between them as a larger AVE value indicates that a construct has more variance in common with its own measurement items (Hair et al., 2010).

$$\text{Average Extracted Variance (AVE)} = \frac{\sum Std.\,factor\ loadings^2}{n}$$

To examine convergent validity two measures, Construct Reliability (CR) and AVE, are looked at. CR is only one of several measures of reliability. CR is used in SEM while another measure of reliability, Cronbach's Alpha, is commonly used in traditional statistical analysis techniques. CR is derived from summation of squared factor loadings, which is the loading of the items on the latent variables (Hair et al., 2010), as shown in the formula below. To demonstrate convergent validity, CR should be greater 0.7 and also greater than AVE, and AVE should be larger than 0.5 (Hair et al., 2010).

$$\text{Construct Reliability (CR)} = \frac{(\sum Std.\,factor\ loadings)^2}{(\sum Std.\,factor\ loadings)^2 + (\sum error\ variance\ terms)}$$

The weight of the factor loading is an important aspect of convergent validity because in SEM models both CR and AVE are calculated using standardized factor loading estimates. As a rule of thumb, factor loadings greater than 0.5 are considered acceptable and 0.7 are recommended (Hair et al., 2010) and reflect that a set of observed variables that do not correlate well with each other is indicative of convergent validity issues.

4.8.1.1 Sample size consideration

When using SEM careful consideration of the sample size is required because SEM applications use parameter estimation algorithms that produce unreliable results when small sample sizes are used (Hair et al., 2010). Guidelines about sample size cutoff values vary in the SEM literature, with recommended values ranging from 50 to 500 depending on the SEM estimation technique applied (Curran, West, & Finch, 1996; Hair et al., 2010). The sample size required is also dependent on the following: the number of measurement items per latent variable and data characteristics such as multivariate non-normality and missing data (Boomsma & Hoogland, 2001; Curran et al., 1996; Hair et al., 2010; Marsh & Hau, 1999).

An estimation technique is a mathematical calculation of estimates of the parameters identified in a given model. A Monte Carlo simulation study conducted by Curran et al. (1996) showed that when using the asymptotically distribution free (ADF) estimation technique, a sample size of less than 500 yields unreliable results. The study further showed that the maximum likelihood (ML) estimation technique yields stable results even at a sample size of 200.

This study follows two strategies for determining appropriate sample size. Regarding the link between sample size and estimation techniques, one strategy was to take into consideration the SEM software used in this study and the estimation techniques

provided by the software. In this study AMOS version 19 (Arbuckle, 2010a) was used. The AMOS software provides ADF and ML among other estimation methods (Arbuckle, 2010b). ML produces more accurate parameter estimates under multivariate-normality conditions and is therefore the most frequently used estimation technique in SEM (Hair et al., 2010). While the ADF technique requires a large sample size, typically greater than 500 (Boomsma, 2000), ML can produce reliable results even with a sample size of 200. Therefore, a minimum sample size of 200 per unit of analysis was deemed appropriate and sought for this study.

Another strategy was to ensure that there were enough measurement items per latent variable. When a model has a small number of items per latent variable, a large sample size is needed for any SEM estimation method to yield reliable results (Boomsma & Hoogland, 2001; Marsh & Hau, 1999). Likewise, increasing the number of items per latent variable can make up for a small sample size. In their simulation study, Marsh and Hau (1999) showed that when only two items per latent variable were measured a sample size greater than 400 was needed. Their results also indicated that a smaller sample size of 200 can yield reliable results when three to four measurement items per latent variable are used. Further, in an extreme case of six to twelve items per latent variable a sample size as small as 50 is sufficient (Boomsma & Hoogland, 2001). Given the high number of items per latent variable in this study, a sample size of at least 200 per study group was deemed appropriate for this study. Therefore, a sample size of ≥ 200 per study group was sought.

4.8.1.2 Data screening process

The observed data was screened for missing values, univariate normality, specifically skewness and kurtosis, and multivariate outliers. Performing tests for normality is essential and should be conducted before using any multivariate analysis methods such

as SEM (Arbuckle, 2010b; Byrne, 2010). Screening for missing values, outliers, skewness and kurtosis was conducted using SPSS version 19 (SPSS, 2010) and screening for multivariate outliers was conducted in AMOS.

The test for missing values was conducted using Little's Missing Completely at Random (MCAR) test which is used to examine if any existing missing values follow a specific pattern or if the values are missing completely at random (Hair et al., 2010). In this study the MCAR test was conducted to firstly examine if the participants had left any survey questions unanswered and if so, what proportion of the questions were unanswered. Secondly, the MCAR test's p-value was examined to determine if the unanswered questions were completely random. If less than 10% of the values are missing and the MCAR test yields a non-significant p-value then any method of data imputation can be applied to remedy any potential missing data issues (Hair et al., 2010; Schafer & Graham, 2002). In this study, data imputation was conducted using Expectation Maximization (EM) in SPSS version 19 prior to conducting SEM analysis.

In this study, a test for univariate normality was conducted to investigate whether the data distributions for individual (univariate) variables are weighted heavily towards the left or right (skewness) or if the distribution is excessively flat or peaked (kurtosis). It is important to test for skewness and kurtosis for several reasons: skewness will affect mean estimates while kurtosis will impact variances and covariance tests (DeCarlo, 1997). As analysis of covariance is the basis for SEM as used in this study, severely kurtotic data would be of concern to the study. Likewise, as mean differences between control and treatment groups are also a focus of the study, severely skewed data would be problematic. With univariate skewness and kurtosis the impact decreases as sample size approaches 200 (Hair et al., 2010). Given that the sample size for both the control group and the treatment group was greater than 200, attention was paid only to extreme

cases of univariate skewness and kurtosis. Univariate kurtosis greater than ± 7 and skewness greater than ± 3 are considered problematic (Curran et al., 1996) and therefore of concern to this study.

As SEM is a form of multivariate data analysis the multivariate outlier test conducted in this study aimed to examine if there were participants who had extreme values on multiple variables. Mahalanobis d-squared values (Byrne, 2010; Hair et al., 2010; Kline, 2011) provided in AMOS (Arbuckle, 2010a) were used to identify potential multivariate outliers. As suggested by Hair et al. (2010) and Kline (2011) a conservative p-value ($p<0.001$) was used to identify possible influential outliers. This prevents discarding cases that are representative of the population, a mistake that could limit the ability to generalize the study results.

4.8.1.3 Goodness-of-fit Indices and thresholds for this study

The fundamental goal of the measurement model assessment is to establish validity and reliability of the observed items and the underlying constructs they represent. How well the observed data fit the hypothesized model, referred to model fit, is then assessed. A measurement model is of good fit if the difference between the observed data and the hypothesized model is small (Byrne, 2010; Hair et al., 2010; Hu & Bentler, 1999). To evaluate model fit several fit statistics are used, and over the years, different cut-off values have been suggested. With no consensus on the exact cut-off values, the SEM literature recommends reporting more than one fit statistic.

Many of the fit indices are sensitive to factors such as sample size, number of observed variables or sample distribution such as skewness or kurtosis (Hair et al., 2010; Sharma, Mukherjee, Kumar, & Dillon, 2005). For example, chi-square (χ^2) can fluctuate when sample sizes exceeds 200, and while a non-significant χ^2 is sought, when a large sample size is used a significant χ^2 p-value is expected (Byrne, 2010;

Hair et al., 2010; Hu & Bentler, 1999). Historically, the χ^2 statistic was the primary measure of model fit in SEM, however due to its volatility, indices that are less sensitive to sample size, have been developed as alternates (Hair et al., 2010). These alternates are however sensitive to a variety of other factors. For example, while Goodness-of-fit Index (GFI) was developed to minimize the effects of sample size, it is sensitive to sample distribution (Bollen, 1990; Hu & Bentler, 1998). Further, the formula for estimating Standardized Root Mean Residual (SRMR) includes χ^2 therefore, sample size indirectly affects SRMR (Marsh, Hau, & Wen, 2004; Tanaka, 1993).

Cutoff values for the fit indices must also be determined. As with fit indices, setting cutoff values is also a vexing challenge. For example, when an absolute cutoff value is used, models with numerous observed variables would likely be rejected than models with few observed variables (Sharma et al., 2005). As such, the SEM literature recommends multiple fit indices and provides various guidelines for cutoff values. Table 4.10 summarizes the goodness-of-fit indices and cutoff values used in this study.

Table 4.10: Goodness-of-fit indices and cutoff values used in this study

Goodness-of-Fit Indices	Cutoff Values or Rules
Chi-square (χ^2)	The smaller the value the better
Chi-square significance (χ^2 *p-value*)	>.05 or <.05 if sample size is ≥ 200
Normed Chi-square (χ^2/df)	Between 1 and 2
Comparative Fit Index (CFI)	>.95 (Hair et al., 2010; Hu & Bentler, 1999)
Root Mean Squared Error of Approximation (RMSEA)	< .50 or < .08 if CFI is > .95 (Hair et al., 2010; Hu & Bentler, 1999; Sharma et al., 2005)
Tucker-Lewis Index (TLI)	>.95 (Hair et al., 2010; Hu & Bentler, 1999)
Standardized Root Mean Residual (SRMR)	Minimum <.06, < .80 – 0.9 if CFI is > .92 (Hair et al., 2010; Hu & Bentler, 1999),
Parsimony Normed Fit Index (PNFI)	No set threshold, model with a higher PNFI value is more supported
Chi-square Difference ($\Delta\chi^2$)	Significant if p <.05 (Byrne, 2010)

The numerous fit indices developed to date can be distinguished by their functions and categorized as either *absolute, incremental* or *parsimony* fit indices (Hair et al., 2010; Hu & Bentler, 1998). Given their different functions and sensitivity to such factors as sample size, reporting at least one fit index from each category is recommended (Hair et al., 2010).

Absolute indices directly measure how well the observed data fit the hypothesized model. Chi-square (χ^2), Normed Chi-square (χ^2 / *df* or χ^2: *df*), Standardized Root Mean Residual (SRMR) and Root Mean Squared Error of Approximation (RMSEA) are used in this study. Given its volatility, the χ^2 statistic is reported in conjunction with Normed Chi-square. Normed Chi-square is the degrees of freedom (*df*) associated with the χ^2 and is calculated as a ratio of χ^2: *df*. As discussed earlier, a non-significant χ^2 can be expected with sample sizes larger than 200 (Byrne, 2010; Hair et al., 2010; Hu & Bentler, 1999). As a sample size of greater than 200 was used for each group in this study, a significant χ^2 can be expected. Therefore, normed chi-square is reported as a supplement to χ^2. While a ratio (normed chi-square) between 2 and 5 is acceptable, a ratio of between 1 and 2 is indicative of a good fitting model (Hair et al., 2010).

As mentioned earlier, with large samples models tend to be rejected due to a significant χ^2 p-value. RMSEA was developed to remedy this problem, and as shown in a Monte Carlo study by Sharma et al. (2005), RMSEA is not affected by sample size larger than 200. As an absolute fit index, RMSEA assesses how well the observed data fits the hypothesized model. As an added benefit, RMSEA also measures how well the hypothesized model fits the population (Hair et al., 2010). Another absolute index used in this study is the SRMR, which assesses the discrepancy between observed data and hypothesized model. SRMR is sensitive to misspecified latent variable covariances

(Hu & Bentler, 1998) and is therefore a good method of identifying misspecified models.

Coincidentally, both SRMR and RMSEA are measures of badness-of-fit in that larger values indicate bad fit. Including both SRMR and RMSEA we satisfy the guideline that at least one badness-of-fit index be evaluated. The cutoff values used in this study for these indices are < .50 as recommended for RMSEA and < 0.60 for SRMR the cutoff values is < .60 (Hair, et al., 2010; Hu & Bentler, 1999; Sharma, et al., 2005)

Incremental indices, sometimes called *comparative* indices compare χ^2 for a baseline model with χ^2 for the posited model. A baseline model, also referred to as a null or independence model, is a model that assumes that the observed variables are uncorrelated. As such, a baseline model will yield large χ^2 values and thus be of poor fit. Hence an incremental index compares the hypothesized model with a model of poor fit. Comparative Fit Index (CFI) and Tucker-Lewis Index (TLI) are the incremental indices used in this study. TLI is used to compare the normed chi-square of a hypothesized model with that of the baseline model and is favored as it is generally not affected by sample size (Hu & Bentler, 1998). Before CFI was developed, Normed Fit Index (NFI) was one of the primary incremental indices used. However, complex models with many parameters inflate the NFI values. In contrast, CFI accounts for model complexity and for that reason is preferred to NFI (Hair et al., 2010). While CFI compares the χ^2 of the hypothesized model and the baseline model, TLI compares the normed chi-square values of the two models. Therefore, this study reports both the CFI and TLI values. A cutoff value of >.95 (Hair, et al., 2010; Hu & Bentler, 1999) for both CFI and TLI is used in this study.

When evaluating the χ^2, generally a small value indicates good fit. A problem is that χ^2 can be manipulated by adding parameters to the model which in turn deflates the χ^2 value (Mulaik et al., 1989). Manipulating the χ^2 fit index in this manner can result in meaningless parameters that are only specific to the sample data and therefore ungeneralizable. When generalizing the results the model should ideally be parsimonious, with fewer parameters. Parsimony fit indices are adjustments of absolute and incremental indices that favor models with more parameters. Parsimony fit indices such as Parsimony Normed Fit Index (PNFI) are intended to ensure that model complexity (number of estimated parameters) is accounted for and models with more parameters are penalized. The advantage of PNFI is that it combines elements of parsimony and elements of goodness-of-fit together (Mulaik et al., 1989), and being the most commonly used parsimony index (Hair et al., 2010), PNFI was applied in this study. Although values approaching one and zero indicate parsimony and lack of parsimony respectively, PNFI has no absolute cutoff point (Hair et al., 2010; Hooper, Coughlan, & Mullen, 2008).

PNFI is generally used to compare models where a model with a higher value is more parsimonious and is therefore preferred (Hair et al., 2010). Also to compare models, chi-square difference ($\Delta\chi^2$) between two models can be calculated. The $\Delta\chi^2$ is also regarded as a goodness-of-fit index and is used to compare multi group models such as the ones used in this study. A significant $\Delta\chi^2$ p-value (<.05) indicates that the multi group models are significantly different. Analysis of the multi group measurement model is discussed in the following section.

4.8.1.4 Baseline model specification and re-specification

Once goodness-of-fit and validity of the measurement model is assessed, the structural model can then be tested. However, in the case of a multi group study such as this

study, it is important to first assess whether the measurement model operates the same way across groups. When comparing data across more than one group, it is the assumption that the observed variables measure the same underlying latent construct and that they behave the same way across groups. This assumption is statistically tested using SEM analysis tools at the measurement model stage (Byrne, 2008).

As this study includes a multi-group analysis, before performing a test of the structural model the goal was to test whether the measurement model behaves the same way across the two groups. Testing for multi-group equivalence on a measurement model, as described by Byrne (2008), involves determining a good-fitting baseline model also known as a *configural model*. The model is established separately for each group. This is the proposed measurement model and is tested separately for each group.

In practice, it may be difficult to find a fully identical measurement model across groups. In such situations one group may have error covariance specified on a set of observed variables, while other groups may have none or they may have error covariance specified on different observed variables (Arbuckle, 2010b; Byrne, 2008; Hair et al., 2010). This was the case in findings presented by Byrne et al. (1989). If a fully equivalent measurement model cannot be achieved, structural analysis can still proceed if certain conditions are met. In addition to a priori theoretical knowledge of existing group differences (Byrne, 1989, 2008), partial equivalence is acceptable if at least two observed variables per latent variable are equal (Hair et al., 2010).

During the process of determining a good fitting baseline model, goodness-of-fit statistics were used to establish model fit. Covariance M.I. which are calculated for all unspecified parameters, were used to identify misspecified parameters. Although an M.I. value greater than 4.0 suggests some degree of misspecification they should only be used as a guide to identifying potential problematic items (Hair et al., 2010). Only

excessively high M.I. values were used to identify problematic measurement items and allow error terms to covary.

Finally, this study used standardized residuals estimates to examine the degree of discrepancy (residuals) between the hypothesized measurement model and the observed sample data. Smaller residuals indicate better fit (Hair et al., 2010). Standardized residuals between 2.5 and 4 are large but not necessarily a problem. However, they should be examined for other problems associated with specific items (Hair et al., 2010).

A baseline model is final when all items have been examined for reliability issues. Following the measurement model analysis, factor loadings for each latent variable were examined for item reliability for each item. This is different from Convergent Validity as described in Section 4.8.1, which determines reliability of the latent variable. In this study, factor loadings greater than 0.7 (Hair et al., 2010), with Critical Ratio greater than ±1.96 indicating that the factor loading is significantly different from zero when $p<0.05$, were considered acceptable. Also, provided in AMOS, the Squared Multiple Correlations (SMC) estimates were used to examine individual item reliability. In this study a SMC value greater than 0.5, which suggests that at least 50% of the variance in an item is accounted for by a latent variable (Hair et al., 2010), is considered acceptable while item reliability (SMC) between 0.3 and 0.5 are considered weak but adequate (Hair et al., 2010).

In summary, to determine a good fitting baseline model for each group, the proposed model was examined for model fit (baseline model) and the baseline model was re-specified as needed and tested for discriminant and convergent validity issues. Each latent variable was then tested for item reliability issues and finally a test for model equivalence (described in Section 4.8.1.5) was conducted on the baseline model to

ensure that the model operates the same way across the two groups. The analysis was conducted separately for the two study groups and items dropped accordingly. This process was conducted separately for the *Threat Perceptions* model, described in Section 3.5, and the *Efficacy Perceptions* model described in Section 3.7, while the latent variable *intentions to comply* described in Section 3.8 was analyzed as a congeneric model. A final analysis was conducted on the full measurement model and goodness-of-fit statistics and reliability measures examined. This was to rule out any possible multicollinearity issues (high correlation between two or more latent variables) or cross loadings (high correlation between measurement items and unrelated latent variables).

4.8.1.5 Test for multi-group measurement model equivalence

Once a good-fitting baseline model is established for both groups individually, the data files are combined in order to test for multi-group model equivalence. This process tests whether the two baseline models are equivalent. The two baseline measurement models, which may have covariances specified on different items, are run simultaneously and with no equality constraints. If the goodness-of-fit statistics for the baseline model are reasonable, then testing for measurement model equivalence can be initiated.

When testing for measurement model equivalence, factor loadings for the first group are estimated then equal constraints are imposed on the second group. As it is possible to have error covariance specified on one set of observed variables for one group, while another group may have none or they may have error covariance specified on a different set of observed variables (Arbuckle, 2010b; Byrne, 2008; Hair et al., 2010), in this study error covariances were only constrained equal if they were specified on both group models. This is because imposing equality constraints on error variances is

not a common practice and may be considered overly rigid (Byrne, 2010). If error covariances are specified on both models, equal constraints must be imposed on the error covariances.

To test for equivalence AMOS calculates the difference between the baseline model and the constraint model. If the chi-square-square difference ($\Delta\chi^2$) is significant, then the two models are not equivalent. To claim model equality, a non-significant $\Delta\chi^2$ is desired. A test for multi-group equivalence was performed separately for each latent variable and for each group. To determine if the measurements are equal across groups a non-significant *p-value* is sought (Byrne, 2010; Hair et al., 2010).

4.8.2 Structural model

The second step in the two-step approach is the evaluation of the structural model. This process involves structural model specification and assessment of structural model validity. Model specification involves assessing model fit as a nested model by combining the control and treatment group models and calculating goodness-of-fit. M.I. and standardized residuals are also examined to identify significant discrepancies (residuals) between the hypothesized structural model and the observed sample data.

Similar to assessment of the measurement model, Chi-square (χ^2) is also used to assess structural model fit. However the χ^2 of the structural model must not be lower than that of the measurement model because the structural model must include the same relationships between latent constructs as specified in the measurement model (Hair et al., 2010). To assess structural model fit, the same seven goodness-of-fit indices used to assess measurement model fit were used. These are, Chi-square χ^2, normed chi-square (χ^2 /df), SRMR, RMSEA, CFI and TLI and PNFI. Table 4.10 summarizes describes the above goodness-of-fit indices and their cutoff values.

Following the specification of the structural model, validity of the structural model was examined. For each group model, validity of the structural model, including the direction of the relationships path significance and size of the path estimates. In addition, the extent to which the structural model explains the variance in the latent dependent variable was examined. Similar to the assessment of measurement model validity, explained variance was used to determine the validity of the structural model. This approach is analogous to the use of R^2 applied in multiple regression analysis. In AMOS this is reported as SMC associated with dependent latent variables which measures the percentage of variance explained. Finally, analysis of the research hypotheses was conducted.

4.8.3 Summary statistical analysis techniques

Table 4.11 summarizes the hypotheses and the statistical analysis techniques used to test the hypotheses.

Table 4.11: Summary statistical analysis techniques

Overview of constructs hypothesis and statistical analysis	
Hypothesis	**Statistical analysis**
H 1 *Fear appeals* will **increase** user compliance with password guidelines.	Between subjects MANOVA to determine group differences on multiple variables Password strength tool to measure pre and post password strength Repeated measures ANOVA with Split Plot to determine if password strength was improved A between subjects ANOVA to determine if improved password was due to fear appeals
H2 Perceived severity of *password* related threats is positively related to intentions *to comply* with password guidelines.	SEM
H 3 *Perceived vulnerability* to password related threats will **not have a direct effect** on *intentions to comply* with password guidelines.	SEM
H 4 Perceived threat is *positively related* to **intentions** *to comply with* password guidelines.	SEM
H 5 Perceived vulnerability is *positively related* to **perceived** threat.	SEM
H 6 Perceived severity is *positively related* to **perceived** threat.	SEM
H 7 *Exposure to hacking* is **positively** *related to* perceived vulnerability	SEM
H 8 Perceived *password effectiveness is* positively **related** *to intentions to* comply with password guidelines	SEM
H 9 Password *self-efficacy is* positively **related** *to intentions to* comply with password guidelines	SEM
H 10 Perceived *cost is* negatively **related** *to intentions to* comply with password guidelines	SEM
H 11 Intentions *to comply is* positively **related** to actual password compliance.	SEM
H 12 Users who receive *fear appeals* will have **higher** *intentions to comply* over time than those who do not	One-way between-group ANOVA
H 13 Users who receive *fear appeals* with a mnemonic training emphasis will have **higher** *password memorability* over time than those who do not	One-way between-group ANOVA

4.9 Phase II data analysis techniques

The data collected in Phase II is aimed to determine if the fear appeals used in this study had a long-term effect on *password memorability* and *intentions to comply* with password guidelines.

To determine the long-term effects of the fear appeals on the participants' ability to remember passwords, a generic password supplied during login was used during analysis to determine the proportion of the participants who forgot the passwords they created in Phase I. A χ^2 test of independence was conducted to examine if there were group differences. Further, a one-way between-group ANOVA was performed to determine in fear appeals had a long-term effect on the participants' perceived *password memorability*. Finally, a one-way between-group ANOVA was performed to examine if the fear appeals had a long-term effect on *intentions to comply*.

4.10 Chapter overview

This chapter described the research design and analysis techniques used in Phase I and Phase II of this study. The study was a between-group experimental design where one group completed a password information and training, and another was not. The training included information about the pervasiveness and consequences of password related threats, the effectiveness password guidelines and a password training session. The participants were Internet users who held at least one online email account. Through a third party recruiting company the participants were from a wide spectrum of backgrounds including gender, level of education, computer skills and computer security knowledge.

This chapter provided a detailed description of the primary data analysis technique used in this study, SEM and the two-step approach to SEM used in this study. Chapter 5 reports the results of the data analysis techniques described in this chapter.

5 Data Analysis and Results

5.1 Introduction

This chapter reports the findings from the analysis of the data collected to test the research hypotheses. The chapter is divided into four major sections. The first section reports the demographic and computer background data about the participants. This study uses a two-step SEM approach where analysis of the measurement model and the structural model was conducted separately. Thus, the results of the measurement model assessment and validation method, and the results of the structural model testing are presented in two separate sections. The final section presents the results of each hypothesis.

5.2 Participants' demographic characteristics

This section presents the background information about the participants. This section also reports the number of online email accounts, password management practices, level of education and self-reported computer and computer security knowledge.

5.2.1 Phase I participants

In total, 459 surveys were completed in Phase I. Of these 209 were participants in the control group and 210 in the treatment group. The total number of valid completions was 419, a valid response rate of 10.9% as 3830 email invitations were distributed. Generally, web based surveys have lower response rates, with an average of 34% and as low as 7% (Shih & Fan, 2008). Considering the data in Phase I of this study was collected over three days, the valid response rate for this study is acceptable. The results in this section are based on the 419 valid survey responses. For each background variable, a follow-up chi-squared (χ^2) test of independence was conducted

to examine if there were any group differences. As can be seen in Table 5.1, for both study groups, the majority of participants were female, 56.8% and 58.9% for the control and treatment groups respectively. In total, there were 42.1% males and 57.9% females. A χ^2 test of independence showed no significant difference in gender ($\chi^2(1) = 0.194$, p=0.659) between the two groups.

Table 5.1: Gender of the participants in control and treatment groups

	Male Frequency	Female Frequency	Male %	Female %
Control Group	89	117	43.2	56.8
Treatment Group	85	122	41.1	58.9
Combined Total	174	239	42.1	57.9

As shown in Table 5.2, the participants' ages ranged from 18 to 84 for the control group and 18 to 85 for the treatment group. The average ages were 43.78 and 43.61 for the control and the treatment group respectively, with a combined average age of 43.70. There was no significant difference in age ($\chi^2(62) = 57.36$, p=0.643) between the two groups.

Table 5.2: Age of the participants in control and treatment groups

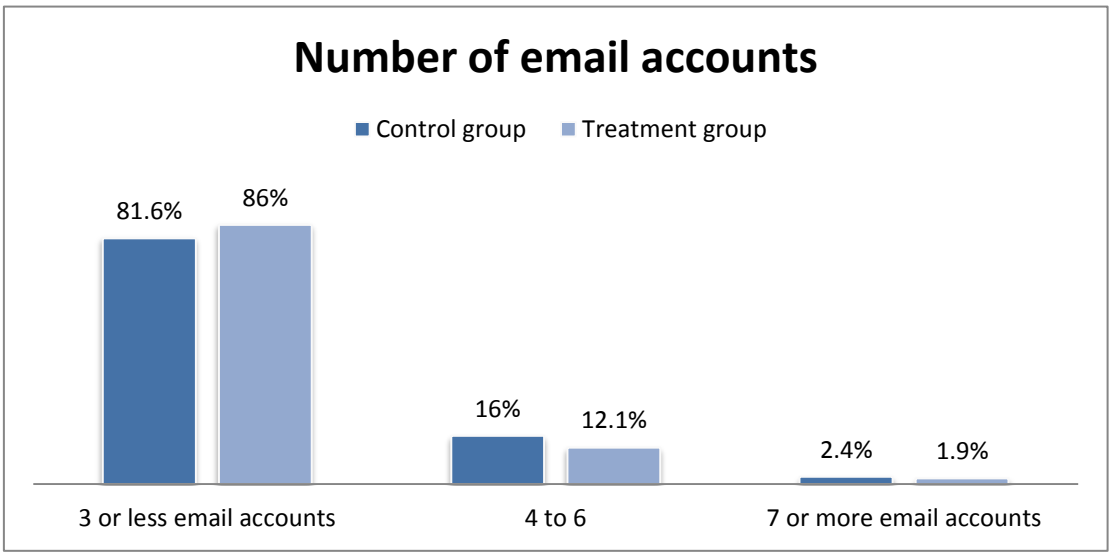
	Average	Median	Minimum	Maximum	SD
Control Group	43.8	44	18	84	15.3
Treatment Group	43.6	44	18	85	15.3
Combined	43.7	44	18	85	15.3

5.2.2 Number of online email accounts

Figure 5.1 shows the two groups share a similar pattern of distribution about the number of email accounts they hold. Most participants, 81.4% of the control group and 86% of the treatment group, indicated that they have three or less online email addresses. A χ^2 test comparing the two groups showed no significant difference in the

number of email accounts (χ^2 (15) = 18.79, p=0.223) held by participants in the control and treatment groups.

Figure 5.1: Participants' number of online email accounts



5.2.3 Password management practices

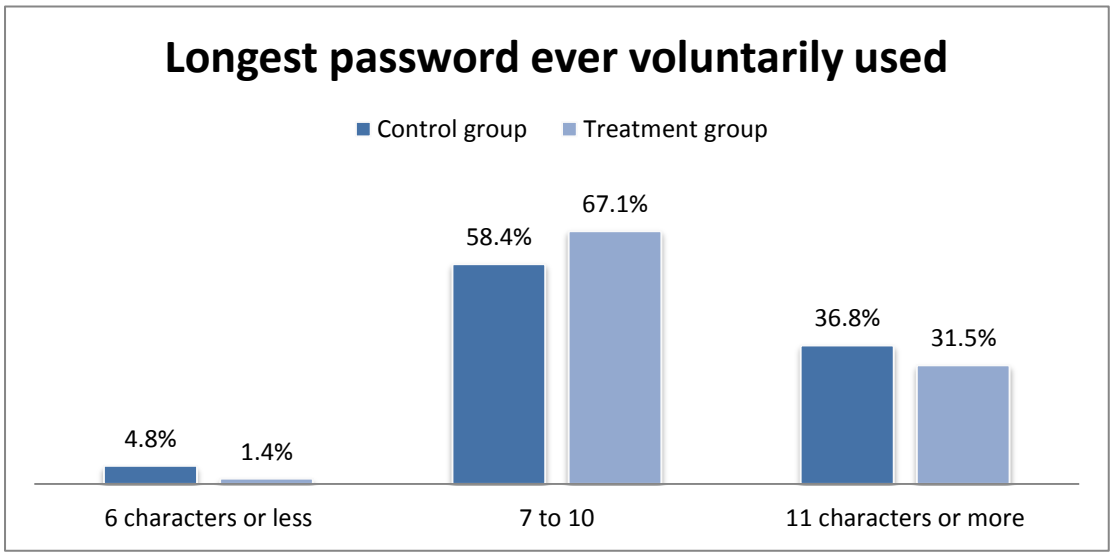
Data on participants' password management practices, including password length, changing passwords and password sharing were also collected. As shown in Figure 5.2, most participants indicated that the longest password they had voluntarily created was between 7 and 10 characters long. The data shows a noticeably different pattern of distribution between the two groups, with 58.4% of the control group and a much higher proportion (67.1%) of the treatment group indicating that they had used a password of 7 to 10 characters long without being prompted. A χ^2 test comparing the two groups on password length showed that there was a significant difference in the self-reported password length (χ^2 (6) = 13.98, p=0.030), thus indicating that the reported maximum password length was different between the two groups.

The maximum password length reported by the participants in this study is consistent with those reported in studies such as that of Calin's (2009), who analyzed 10,000

leaked Hotmail passwords and found that most (69%) of the passwords were between 6 to 9 characters long. Also, Cazier & Medlin's (2006) empirical investigation of an e-commerce website with no password restrictions observed that the average password length was 7 to 8 characters. This phenomenon is supported by Miller's (1956) claim that the human brain can only memorize between 5 to 9 non-arbitrary objects.

Interestingly, this result reveals a very different trend compared with that shown in Zviran and Haga (1999) approximately 15 years back. In their study, a majority (71.9%) of participants indicated that their password was six or less characters long. The current trend toward password length appears to have increased.

Figure 5.2: Participants' longest password ever voluntarily used



Further, as shown in Table 5.3, when asked if they had ever changed their passwords voluntarily, a majority of participants in each group indicated that they had changed passwords even when password change was not enforced: 68.4% and 71.2% for the control and treatment group respectively. There was also no significant group difference in password management practices related to changing passwords voluntarily ($\chi^2(1) = 0.375$, p=0.540).

Table 5.3: Proportion of participants who have changed passwords voluntarily

	Yes (n)	No (n)	Yes (%)	No (%)
Control Group	141	65	68.4	31.6
Treatment Group	146	59	71.2	28.8

As shown in Table 5.4, only 15.7% and 20.1% of the control and treatment group respectively indicated that they had shared passwords before and there was no significant difference between the two groups ($\chi^2(1) = 1.37$, p=0.243).

Table 5.4: Proportion of participants who have shared passwords

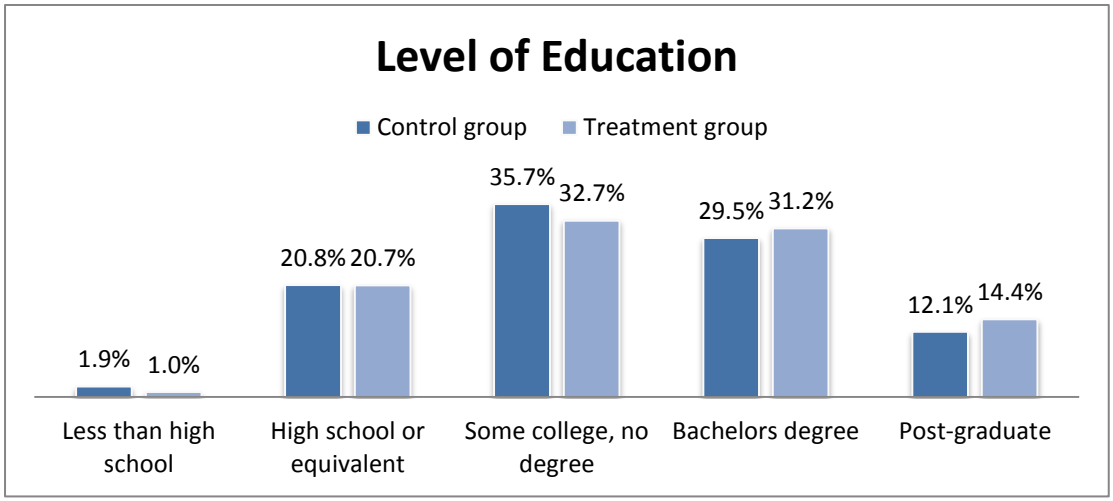
	Yes (n)	No (n)	Yes (%)	No (%)
Control Group	32	172	15.7	84.3
Treatment Group	42	167	20.1	79.9

With regards password management practices, both groups appear to have no difficultly creating long passwords, as indicated by the results in Figure 5.2, or changing passwords voluntarily, and a large proportion of the participants do not share passwords.

5.2.4 Education and ICT background

Figure 5.3 shows the distribution of the participants' levels of education. Only a small proportion of the control group (1.9%) indicated that they had less than a high school diploma, while 20.8% had a high school diploma or equivalent, 35.7% had some college but with no degree, 29.5% held a bachelor's degree and 12.1% held a post-graduate degree. With a similar distribution, a small proportion of the treatment group (1%) had less than a high school diploma, 20.7% had a high school diploma or equivalent, 32.7% had some college but with no degree, 31.2% held a bachelor's degree and 14.4% held a post-graduate degree. No significant differences were found in level of education ($\chi^2(4) = 1.499$, p=0.827) across the two study groups.

Figure 5.3: Participants' level of education



Both groups had a similar pattern of distribution in their reported computer skills and computer security knowledge. Both groups perceived themselves as having mostly average or above average computer skills and knowledge of computer security. Only 8.6% of the control group rated their computer skills as below average and a low 6.2% of the treatment group rated their computer skills as below average. Slightly more participants from both groups indicated that they had a below average knowledge of computer security compared to computer skills. Still, a low 15.3% of the control group rated themselves as below average and a low 12.4% of the treatment group rated their computer security knowledge as below average. No significant group differences were found in self-reported computer skills (χ^2 (6) = 3.941, p=0.685) or computer security knowledge (χ^2 (6) = 2.890, p=0.822). The complete demographic computer and computer security background of respondents can be located in Appendix G.

5.3 Analysis of measurement model

This section reports the results of the measurement model analysis. First, the results for the data cleaning process are presented. This section also reports the results of the measurement model analysis for the construct *exposure to hacking*, and the *Threat*

Perceptions and *Efficacy Perceptions* models. The latent variable *intentions to comply* with password guidelines, was analyzed as a congeneric model. With the exception of *exposure to hacking* and *actual password compliance*, tests for multi-group model equivalence were carried out and the results are presented separately for the *Threat Perceptions* and *Efficacy Perceptions* models and the *intentions to comply* congeneric model. This section also presents the results of final full measurement model analysis.

5.3.1 Data cleaning results

Prior to the measurement model analysis using SEM, the data was examined for missing values, potential outliers and tested for normality, with emphasis on skewness and kurtosis issues. The following sub-sections present the outcomes of the data screening process.

5.3.1.1 Missing data analysis

The MCAR test, described in Section 4.8.1.2, was conducted separately for the observed data for the *Threat Perceptions* model, the *Efficacy Perceptions* model, *perceived cost* and *intentions to comply*. *Exposure to hacking* and *actual password compliance* were required fields therefore there were no missing values. Observed data for *perceived cost* was examined separately as it is the only construct hypothesized to have a negative impact on *intentions to comply* with password guidelines. Table 5.5 and Table 5.6 summarize the results obtained from the MCAR tests. As can be seen from the MCAR statistics in Table 5.5, the test produced non-significant p-values ($p = >0.5$) across all variables for the control group suggesting that the values were missing completely at random. Given that the highest proportion of missing values on any given set of variables was 2.9%, data imputation was conducted using EM in SPSS version 19 (SPSS, 2010).

Table 5.5: Control group MCAR test statistics

Variable Set	Max. % of missing values	Max. no. of missing values	Little's MCAR test Sig.
Threat Perceptions	2.9%	6	p = .931
Efficacy Perceptions	1.9%	4	p = .967
Perceived Cost	1.4%	3	p = .928
Intentions to Comply	2.9%	6	p = .808

In Table 5.6 is a summary of the results of the MCAR test carried out on the treatment group dataset. The results were non-significant across all variables indicating that the missing data pattern occurred completely at random. Therefore, imputation of the missing values was also conducted using the EM method prior to SEM analysis.

Table 5.6: Treatment group MCAR test statistics

Variable Set	Max. % of missing values	Max. no. of missing values	Little's MCAR test Sig.
Threat Perceptions	2.4%	5	p = .987
Efficacy Perceptions	2.4%	5	p = .968
Perceived Cost	1.4%	3	p = .128
Intentions to Comply	2.4%	5	p = .969

5.3.1.2 Test for univariate normality assumption

The data in Table 5.7 show the extent to which the distribution for each observed variable deviates from normality. A normal distribution would have a kurtosis and skewness of zero, while kurtosis and skewness greater than ± 1.96 is generally considered non-normal (Cramer & Howitt, 2004) and values up to ± 7 and ± 3 respectively would be considered extreme (Curran et al., 1996). Therefore, in this study values up to ± 7 and ± 3 were considered problematic. As can be seen in Table 5.7, the kurtosis and skewness values are below the cutoff values and meet the univariate non-normality assumption for this study.

Table 5.7: Parameters of Univariate Skewness and Kurtosis

Variables	Min. Skewness	Max. Skewness	Min. Kurtosis	Max. Kurtosis
Control group				
Exposure to Hacking	0.844	1.373	-0.839	0.392
Perceived Vulnerability	-0.546	0.084	-0.998	-0.175
Perceived Severity	-0.807	0.005	-1.118	-0.566
Perceived Threat	-1.207	-0.637	-0.251	0.728
Perceived Effectiveness	-1.171	-0.366	-0.482	1.488
Perceived Cost	-0.832	0.105	-1.054	-0.005
Perceived Self-efficacy	-0.923	-0.517	0.481	-0.457
Intentions to Comply	-1.032	-0.725	-0.177	0.816
Treatment group				
Exposure to hacking	0.551	0.962	-1.221	-0.647
Perceived Vulnerability	-0.472	-0.211	-0.772	-0.304
Perceived Severity	-1.144	-0.415	-0.569	0.953
Perceived Threat	-1.000	-0.542	-0.181	0.421
Perceived Effectiveness	-1.283	-0.941	0.347	1.769
Perceived Cost	-0.969	-0.088	-1.011	0.274
Perceived Self-efficacy	-0.945	-0.593	-0.333	0.825
Intentions to Comply	-1.068	-0.801	-0.032	0.917
Min-Max = range				

5.3.1.3 Test for multivariate Outliers

To test for multivariate outliers a conservative Mahalanobis d-squared p-value of <0.001 (Hair et al., 2010) was used as a cutoff value. Additionally, following a closer examination of the actual data, seven control group cases and six treatment group cases were identified as extreme or potential influential multivariate outliers. The Mahalanobis d-squared p-value suggests that the correlations between variables for 13 participants were significantly different from the rest of the respondents. Including these cases would potentially distort the multivariate SEM analysis results (Hair et al., 2010; Kline, 2011), therefore the cases were deleted.

A total of 202 control and 204 treatment group cases were used in the subsequent analysis of the measurement model and the structural model analysis.

5.3.2 Exposure to hacking measurement

The exploratory variable *exposure to hacking* was measured using two measurement items where the participants indicated whether they or someone they know personally had ever been a victim of hacking. A single composite score was computed using regression imputation in AMOS version 19 (Arbuckle, 2010a), and construct reliability examined.

The Cronbach's Alpha value for the treatment group was acceptable with a construct reliability value of 0.738, while the control group value (0.633) was slightly lower than the recommended construct reliability value of > 0.7. However, as discussed in Chapter 3, the construct *exposure to hacking* is not part of the PMT (Maddux & Rogers, 1983), and therefore considered exploratory for this study. Construct reliability of 0.633 is acceptable as it is greater than > 0.5, the minimum recommended threshold for exploratory factors. Therefore, the construct reliability for *exposure to hacking* was considered satisfactory.

5.3.3 Threat perceptions measurement model

The *Threat Perceptions*, *Efficacy Perceptions* and the *intentions to comply* congeneric models were analyzed and the results are reported separately in Sections 5.3.3 - 5.3.5. Each section reports the model specification, including the goodness-of-fit statistics for the initial model described in Chapter 3, construct validity (discriminant and convergent validity), individual latent variables, individual item reliability, and finally a multi-group model equivalence test. The outcome of each section is a good fitting measurement model that operates the same way across the two groups. Section 5.3.7 reports the results for the full measurement model assessed to rule out any possible multicollinearity issues.

This section presents the results of analysis of the *Threat Perceptions* measurement model. The model includes the latent constructs, *perceived vulnerability*, *perceived severity* and *perceived threat.* The analysis was conducted for the control and treatment group separately.

5.3.3.1 Baseline model specification and re-specification

The initial analysis of the hypothesized model yielded goodness-of-fit statistics higher than the recommended cutoff values proposed for this study (see Table 4.10), thus indicating poor fit. As discussed in Section 4.8.1.4, only items with relatively high M.I. values were allowed to covary, and only items with high correlations, standardized residual values, and low reliability (SMC) values were examined to determine if they should be excluded from the measurement model. Appendix H, Section H.1 presents the complete M.I. values, standardized residuals and SMC values associated with the *Threat Perceptions* model.

The correlation between PSEV01 and PSEV02 (0.66) and PTHR01 and PTHR02 (0.60) for the control group was particularly high, suggesting that each set of items had a high level of shared variance or that the items were possibly measuring the same thing. The correlation between PSEV01 and PSEV02 was also excessively high for the treatment group at 0.72. The standardized residuals for the treatment group were greater than 2.0 between PVUL04 and items PSEV01, PSEV0 2 and PSEV03. Further, for both groups, PVUL04 had the lowest item reliability (SMC) values. Therefore, with the high M.I. and standardized residuals values, and a high correlation between PSEV01- PSEV02 and PTHR01 - PTHR02, PSEV01 and PTHR01 were dropped due to lower than recommended item reliability. PVUL04 was also dropped due to high standardized residuals and low item reliability.

5.3.3.2 Assessment of construct validity

After determining a good-fitting baseline *Threat Perceptions* model, four *perceived severity* items were retained, three items were retained for *perceived vulnerability* and five measurement items were retained for *perceived threat*. Discriminant and convergent validity and construct reliability for the three latent variables were then examined.

Table 5.8 summarizes the goodness-of-fit statistics and reliability measures for the control group. With the exception of the χ^2 p-value (significant at p= 0.007) which is expected when the sample size is greater than 200 (Hair et al., 2010), all goodness-of-fit statistics were acceptable indicating that the control group sample data represents the proposed baseline model well. Reliability measures were also acceptable with composite reliability ranging from .884 to a high reliability value of .976 while Cronbach's alpha ranged from .879 to .976. AVE values were also acceptable indicating no discriminant or convergent validity issues.

Table 5.8: Reliability and goodness-of-fit statistics, Threat Perceptions model

Chi-square (X^2)	**Control**			**Treatment**		
Chi-square (χ^2)	78.2			89.1		
Degrees of freedom (df)	50			49		
Normed chi-square (χ^2/df)	1.56			1.82		
Chi-square (χ^2) p-value	0.007			0.000		
Goodness-of-fit indices						
Comparative fit index (CFI)	0.989			0.983		
Tucker-Lewis index (TLI)	0.985			0.977		
Standardized root mean residual (SRMR)	0.028			0.045		
Root mean square error of approximation (RMSEA)	0.053			0.063		
Construct reliability measures	**CA**	**CR**	**AVE**	**CA**	**CR**	**AVE**
Perceived severity	0.920	0.922	0.746	0.897	0.887	0.667
Perceived vulnerability	0.879	0.882	0.714	0.920	0.922	0.797
Perceived threat	0.976	0.976	0.889	0.961	0.960	0.827
CA= Cronbach's alpha; CR= composite reliability; AVE= average extracted variance						

The goodness-of-fit statistics for the treatment group also suggested the observed data fits the treatment group *Threat Perceptions* measurement model well. Reliability measures were also adequate with CR values ranging from .887 to .960 and acceptable Cronbach's alpha values ranging from .897 to .961. The AVE values suggested no discriminant or convergent validity issues.

The following subsections describe the parameter estimates for each latent variable in the *Threat Perceptions* model including item reliability measures for each retained item. Factor loadings are provided as both unstandardized estimates as shown in the *Estimates* column, and standardized estimates, in the *Standardized Estimates* column, in Table 5.9. In AMOS (Arbuckle, 2010a), path coefficients and factor loadings are labeled as regression weights. In this study, path coefficients represent structural path correlations and factor loadings refer to correlations between measurement items and their underlying factors.

5.3.3.3 Perceived severity

As shown in Table 5.9 all factor loadings and CR values are acceptable. Item reliability values, represented as SMC, are also acceptable with the exception of the SMC value of 0.425 for the item PSEV03 (treatment group) which is slightly low but considered adequate. Therefore, all retained measurement items were considered a good measure of *perceived severity*.

Table 5.9: Parameter estimates for perceived severity

Item		Latent Variable	Estimate	S.E.	Critical Ratio	*p*	SMC	Std. Estimate
Control group								
PSEV01	<---	PERCEIVED_SEVERITY	1				0.665	0.816
PSEV03	<---	PERCEIVED_SEVERITY	1.040	0.072	14.530	***	0.739	0.860
PSEV04	<---	PERCEIVED_SEVERITY	1.136	0.071	16.070	***	0.854	0.924
PSEV05	<---	PERCEIVED_SEVERITY	1.089	0.076	14.332	***	0.725	0.852
Treatment group								
PSEV01	<---	PERCEIVED_SEVERITY	1				0.552	0.743
PSEV03	<---	PERCEIVED_SEVERITY	0.911	0.069	13.127	***	0.425	0.652
PSEV04	<---	PERCEIVED_SEVERITY	1.226	0.090	13.616	***	0.908	0.953
PSEV05	<---	PERCEIVED_SEVERITY	1.126	0.086	13.074	***	0.783	0.885
Std. Estimate=factor loadings; *=p<0.05; **=p<0.01; ***=p<0.001								

5.3.3.4 Perceived threat

As can be seen from the parameter estimates in Table 5.10, all factor loadings for perceived threat are significant and acceptable. In addition, item reliability measures (SMC) for all five measurement items are acceptable suggesting that all measurement items are a good measure of *perceived threat*.

Table 5.10: Parameter estimates for perceived threat

Item		Latent Variable	Estimate	S.E.	Critical Ratio	*p*	SMC	Std. Estimate
Control group								
PTHR02	<---	PERCEIVED_THREAT	1				0.866	0.931
PTHR03	<---	PERCEIVED_THREAT	1.044	0.036	23.364	***	0.935	0.967
PTHR04	<---	PERCEIVED_THREAT	1.029	0.037	28.175	***	0.918	0.958
PTHR05	<---	PERCEIVED_THREAT	1.003	0.040	25.104	***	0.867	0.931
PTHR06	<---	PERCEIVED_THREAT	0.979	0.040	24.708	***	0.859	0.927
Treatment group								
PTHR02	<---	PERCEIVED_THREAT	1				0.832	0.912
PTHR03	<---	PERCEIVED_THREAT	1.041	0.043	24.182	***	0.893	0.945
PTHR04	<---	PERCEIVED_THREAT	0.965	0.042	22.944	***	0.863	0.929
PTHR05	<---	PERCEIVED_THREAT	0.955	0.048	20.010	***	0.784	0.886
PTHR06	<---	PERCEIVED_THREAT	0.944	0.049	19.354	***	0.764	0.874
Std. Estimate=factor loadings; *=p<0.05; **=p<0.01; ***=p<0.001								

5.3.3.5 Perceived vulnerability

Table 5.11 summarizes factor loadings and reliability measures for the items measuring *perceived vulnerability*. As suggested by the Critical Ratio values, all factor loadings are acceptable and the three measurement items significantly correlate to the underlying latent variable. In addition, the SMC for all measurement items are greater than 0.5, signifying acceptable item reliability and that the items are a good measure of *perceived vulnerability*.

Table 5.11: Parameter estimates for perceived vulnerability

Item		Latent Variable	Estimate	S.E.	Critical Ratio	*p*	SMC	Std. Estimate
Control group								
PVUL01	<---	PERCEIVED_VULNERABILITY	1				0.611	0.781
PVUL02	<---	PERCEIVED_VULNERABILITY	1.008	0.079	12.696	***	0.732	0.856
PVUL03	<---	PERCEIVED_VULNERABILITY	1.098	0.085	12.964	***	0.800	0.894
Treatment group								
PVUL01	<---	PERCEIVED_VULNERABILITY	1				0.747	0.864
PVUL02	<---	PERCEIVED_VULNERABILITY	0.907	0.056	16.259	***	0.734	0.857
PVUL03	<---	PERCEIVED_VULNERABILITY	1.509	0.057	18.706	***	0.911	0.954
Std. Estimate=factor loadings; *=p<0.05; **=p<0.01; ***=p<0.001								

5.3.3.6 Multi-group analysis of model equivalence

Once the baseline model was determined for both groups a multi-group analysis was conducted to investigate if the measurement models were equivalent across the two groups. Multi-group analysis accounts for both groups therefore one set of goodness-of-fit statistics was computed and is presented in this section.

The two baseline models were first analyzed with no equality constraints imposed. Equality constraints were sequentially added to the factor loadings (Model A), error covariances (Model B) and factor covariances (Model C). To examine if the two baseline models were equivalent, the two models were analyzed simultaneously and goodness-of-fit statistics for the three models (A, B and C) were compared as shown in Table 5.12.

Table 5.12: Threat Perceptions model equivalence test results

Model Chi-square	Baseline	Model A	Model B	Model C
Chi-square χ^2	167.30	174.78	174.81	179.93
Degrees of freedom (df)	99	108	109	112
Normed chi-square χ^2/df	1.69	1.62	1.60	1.61
χ^2 p-value	0.000	0.000	0.000	0.000
Goodness-of-fit indices				
CFI	0.986	0.986	0.987	0.986
TLI	0.981	0.983	0.984	0.984
SRMR	0.028	0.027	0.027	0.490
RMSEA	0.041	0.039	0.490	0.390
Test of model equivalence				
$\Delta\chi^2$	-	7.67	7.99	13.34
Δdf	-	9	10	13
$\Delta\chi^2$ p-value	-	0.568	0.629	0.422

Baseline model=no constraints
A=Factor Loadings constrained equal
B=Factor Loadings + Error Covariance constrained equal
C=Factor Loadings + Error Covariance + Factor Covariance constrained equal
$\Delta\chi^2$, Δdf, $\Delta\chi^2$ p-value compared with Baseline model with no equal constraints

Analysis of the unconstrained baseline model yielded a χ^2 value of 167.30 with 99 degrees of freedom. All the goodness-of-fit statistics were acceptable, confirming that the constrained model fits the sample data as well as the unconstrained model. As can be seen from the $\Delta\chi^2$ p-values in Table 5.12, the results of the multi-group analysis reveal that when all factor loadings, error covariances and factor covariances are constrained equal, the $\Delta\chi^2$ between the constrained models and the baseline model are not statistically different. This indicates that the *Threat Perceptions* measurement model is a good fitting model and operates the same across both control and treatment groups, suggesting that the two measurement models are equivalent.

5.3.4 Efficacy perceptions measurement model

This section reports the results of analysis of the *Efficacy Perceptions* measurement model. The latent variables included in this model are *perceived password*

effectiveness, *password self-efficacy* and *perceived cost*. The analysis was conducted for the control and treatment group separately.

5.3.4.1 Baseline model specification and re-specification

The goodness-of-fit statistics for the two initial group models suggested poor fit. Items with relatively high M.I. values were allowed to covary, while items with high correlations, high standardized residuals values and low item reliability (SMC) values were dropped. Appendix H, Section H.2 shows the complete M.I. values, standardized residuals and SMC values associated with the *Efficacy Perceptions* model.

The correlation between the error terms associated with COST05 and COST06 for the control group was particularly high at 0.71 suggesting that the two items are possibly measuring the same thing. Also for the control group, the M.I. and standardized residuals associated with COST05 and COST06 were high, thus the two items were allowed to covary. This resulted in a relatively low item reliability for PEFF01 (0.37) and COST04 (0.31) suggesting that these items are problematic and may be candidates for deletion. Similarly, the treatment group model yielded high standardized residuals and M.I. values for COST05 and COST06, and PEFF01 and COST04 also had low item reliability compared to the rest of the items. As the correlation between COST05 and COST06 was high for both groups suggesting that the two items are measuring the same thing, only COST05 was deleted. Therefore, items PEFF01, COST04 and COST05 were excluded from the model.

5.3.4.2 Assessment of construct validity

After a good-fitting baseline model was determined, five *perceived password effectiveness* measurement items were retained, all four *password self-efficacy* items were retained and four *perceived cost* items were retained. Discriminant and

convergent validity and construct reliability for the three latent variables were then examined.

As shown in Table 5.13, the goodness-of-fit statistics were all acceptable, suggesting that the observed data fits the control group baseline model well. Reliability measures were also acceptable with CR ranging from .846 to .883 and Cronbach's Alpha ranging from .846 to .893. The AVE values were also acceptable indicating that the model has no discriminant or convergent validity issues.

Table 5.13: Reliability and goodness-of-fit statistics, Efficacy Perceptions model

Chi-square (χ^2)	**Control**			**Treatment**		
Chi-square (χ^2)	100.4			106.7		
Degrees of freedom (df)	59			60		
Normed chi-square (χ^2/df)	1.70			1.78		
Chi-square (χ^2) p-value	0.001			0.000		
Goodness-of-fit indices						
Comparative fit index (CFI)	0.971			0.976		
Tucker-Lewis index (TLI)	0.962			0.968		
Standardized root mean residual (SRMR)	0.048			0.041		
Root mean square error of approximation (RMSEA)	0.059			0.062		
Construct reliability measures	**CA**	**CR**	**AVE**	**CA**	**CR**	**AVE**
Perceived password effectiveness	0.846	0.846	0.526	0.921	0.918	0.691
Password self-efficacy	0.893	0.883	0.656	0.909	0.910	0.717
Perceived cost	0.876	0.879	0.649	0.886	0.898	0.690
CA=Cronbach's alpha; CR=composite reliability; AVE=average extracted variance						

The goodness-of-fit statistics and reliability measures for the treatment group baseline model were also all acceptable suggesting that the observed data fits the model well. The three latent variables had no reliability issues as indicated by the CR values that range from .898 to .918 and the Cronbach's Alpha values which range from .886 to .921. No discriminant or convergent validity issues were observed as suggested by the AVE values.

The following subsections summarizes the parameter estimates for each latent variable in the *Efficacy Perceptions* measurement model, including item reliability measures for

each retained item. Table 5.14 to Table 5.16 show the item reliability measures for the individual items, as suggested by the SMC values and factors loadings (Standardized Estimates) for the 3 latent variables.

5.3.4.3 Perceived password effectiveness

All factor loadings for *perceived password effectiveness* are within the acceptable range as shown in Table 5.14 and the SMC values are adequate for this study. The goodness-of-fit statistics and construct validity measures suggest that all items are a good measure of *perceived password effectiveness*.

Table 5.14: Parameter estimates for perceived password effectiveness

Item		Latent Variable	Estimate	S.E.	Critical Ratio	*p*	SMC	Std. Estimate
Control group								
PEFF02	<---	PERCEIVED_EFFECTIVENESS	0.859	0.103	8.311	***	0.433	0.658
PEFF03	<---	PERCEIVED_EFFECTIVENESS	0.820	0.094	8.726	***	0.396	0.629
PEFF04	<---	PERCEIVED_EFFECTIVENESS	1				0.672	0.820
PEFF05	<---	PERCEIVED_EFFECTIVENESS	0.890	0.083	10.738	***	0.572	0.757
PEFF06	<---	PERCEIVED_EFFECTIVENESS	0.836	0.079	10.574	***	0.555	0.745
Treatment group								
PEFF02	<---	PERCEIVED_EFFECTIVENESS	0.962	0.066	14.51	***	0.635	0.797
PEFF03	<---	PERCEIVED_EFFECTIVENESS	1				0.802	0.896
PEFF04	<---	PERCEIVED_EFFECTIVENESS	0.906	0.059	15.397	***	0.683	0.827
PEFF05	<---	PERCEIVED_EFFECTIVENESS	0.876	0.061	14.413	***	0.636	0.798
PEFF06	<---	PERCEIVED_EFFECTIVENESS	0.903	0.057	15.741	***	0.696	0.834

Std. Estimate=factor loadings; PERCEIVED_EFFECTIVENESS=perceived password effectiveness
*=p<0.05; **=p<0.01; ***=p<0.001

5.3.4.4 Password self-efficacy

Table 5.15 shows the factors loadings and reliability measures for the four items measuring *password self-efficacy*. All factor loadings are significant (Critical Ratios >1.96, p<0.001) and acceptable. The SMC values are acceptable suggesting that the four items are an adequate measure of *password self-efficacy*.

Table 5.15: Parameter estimates for password self-efficacy

Item		Latent Variable	Estimate	S.E.	Critical Ratio	*p*	SMC	Std. Estimate
Control group								
PSEF01	<--	PASSWORD_SELF-EFFICACY	1				0.738	0.859
PSEF02	<--	PASSWORD_SELF-EFFICACY	1.085	0.067	16.162	***	0.880	0.938
PSEF03	<--	PASSWORD_SELF-EFFICACY	0.882	0.072	12.255	***	0.545	0.739
PSEF04	<--	PASSWORD_SELF-EFFICACY	0.716	0.066	10.847	***	0.461	0.679
Treatment group								
PSEF01	<--	PASSWORD_SELF-EFFICACY	1				0.715	0.845
PSEF02	<--	PASSWORD_SELF-EFFICACY	1.058	0.071	14.888	***	0.724	0.851
PSEF03	<--	PASSWORD_SELF-EFFICACY	1.078	0.069	15.613	***	0.772	0.879
PSEF04	<--	PASSWORD_SELF-EFFICACY	0.901	0.065	13.809	***	0.656	0.810
Std. Estimate=factor loadings *=p<0.05; **=p<0.01; ***=p<0.001								

5.3.4.5 Perceived cost

Table 5.16 summarizes the factors loadings and reliability measures for the four items measuring *perceived cost*. As shown in the table, all Critical Ratios are greater than 1.96, indicating that all factor loadings are significant. Although COST06 (control group) has the lowest factor loading (0.6550 and a low item reliability of 0.429, all estimates are within acceptable range. All four items are therefore adequate measures of *perceived cost*.

Table 5.16: Parameter estimates for perceived cost

Item		Latent Variable	Estimate	S.E.	Critical Ratio	*p*	SMC	Std. Estimate
Control group								
COST01	<--	PERCEIVED_COST	1				0.750	0.866
COST02	<--	PERCEIVED_COST	1.038	0.063	16.571	***	0.863	0.929
COST03	<--	PERCEIVED_COST	0.857	0.069	12.417	***	0.551	0.743
COST06	<--	PERCEIVED_COST	0.704	0.068	10.373	***	0.429	0.655
Treatment group								
COST01	<--	PERCEIVED_COST	1				0.757	0.870
COST02	<--	PERCEIVED_COST	1.078	0.066	16.364	***	0.843	0.918
COST03	<--	PERCEIVED_COST	0.997	0.078	12.786	***	0.576	0.759
COST06	<--	PERCEIVED_COST	0.938	0.084	11.112	***	0.584	0.764
Std. Estimate=factor loadings; *=p<0.05; **=p<0.01; ***=p<0.001								

5.3.4.6 Multi-group analysis of model equivalence

Having determined a baseline model for both study groups, measurement model equivalence was examined for the *Efficacy Perceptions* measurement model. Table 5.17 summarizes the goodness-of-fit statistics and the results for the chi-square difference ($\Delta\chi^2$) test.

Table 5.17: Efficacy Perceptions model equivalence test results

Model Chi-square	Baseline	Model A	Model B	Model C	Model D
Ch-square χ^2	207.02	226.53	226.99	224.40	222.02
Degrees of freedom (df)	119	129	132	131	130
Normed chi-square χ^2/df	1.74	1.76	1.72	1.71	1.71
χ^2 p-value	0.000	0.000	0.000	0.000	0.000
Goodness-of-fit indices					
CFI	0.974	0.971	0.972	0.972	0.972
TLI	0.965	0.965	0.966	0.967	0.967
SRMR	0.048	0.048	0.050	0.049	0.049
RMSEA	0.043	0.043	0.042	0.420	0.042
Test of model equivalence					
$\Delta\chi^2$	-	19.51	19.97	17.38	14.998
Δdf	-	10	13	12	11
$\Delta\chi^2$ p-value	-	0.034	0.096	0.136	0.183

Baseline model=no constraints
A=Factor Loadings constrained equal
B=Factor Loadings + Factor Covariance constrained equal
C=Factor Loadings + Error Covariance constrained equal + no constrain on PEFF03
D=Factor Loadings + Error Covariance constrained equal + no constrain on PEFF03 and PSEF03
$\Delta\chi^2$, Δdf, $\Delta\chi^2$ p-value compared with Baseline model with no equal constraints

The goodness-of-fit statistics for the multi-group baseline model are acceptable, as shown in Table 5.17, with a χ^2 of 207.02 with 119 degrees of freedom suggesting that the proposed baseline model is a good fitting model across both groups. The $\Delta\chi^2$ between the baseline model and the fully constrained Model A was significant ($\Delta\chi^2$ p = 0.034). This means that the two models are significantly different and that one or more factor loadings are not equivalent across the two groups.

As the treatment group had relatively higher factor loadings on items PEFF03 and PSEF03, the two items were unconstrained in Model C and D respectively both

yielding a non-significant $\Delta\chi^2$, Model C ($\Delta\chi^2$ p = 0.136) and D ($\Delta\chi^2$ p = 0.183). This suggests that when the two items are unconstrained the model fit was not significantly different from the baseline model.

Although a fully equivalent measurement model was not achieved, structural analysis was conducted since the results show that at least two of the observed variables are equal (Hair et al., 2010). The *Efficacy Perceptions* measurement model was therefore considered a good fitting model and, though only partially equivalent, the model is considered to be sufficiently equal across the two study groups.

5.3.5 Intentions to comply congeneric model

This section presents the results for the analysis of the *intentions to comply* congeneric model. The analysis was conducted for the control and treatment group separately.

5.3.5.1 Baseline model specification and re-specification

The goodness-of-fit statistics for the initial model suggest that the sample data did not fit the proposed model well. As discussed in Section 4.8.1.4, only items with high M.I. values were allowed to covary, and items with high correlations, high standardized residuals and low item reliability (SMC) values were dropped. Appendix H, Section H.3 presents the complete M.I. values, standardized residuals and SMC values associated with the *intentions to comply* congeneric model.

The M.I. values and standardized residuals associated with INT05 and INT06 were high, particularly for the control group model. When the items were allowed to covary the correlation between the error terms associated with the two items (0.66) was approaching the extreme threshold of 0.7. This suggested that the two items have a high shared variance and that one of the items may be a candidate for deletion. Of the

two items, INT06 had lower item reliability and was therefore excluded from the model.

Reliability issues was also observed on one other item, INT03, which had considerably low item reliability (0.387) compared to the remaining five items and was therefore dropped. Ultimately, four measurement items were retained.

5.3.5.2 Assessment of construct validity

Table 5.18 summarizes the goodness-of-fit statistics for the four-item *intentions to comply* congeneric model. Although the normed chi-square (χ^2/df), TLI and RMSEA (0.159) for both groups suggested poor fit, the CFI and SRMR indicated good fit. Construct reliability measures, CR and Cronbach's Alpha, were also acceptable suggesting that the four items are an acceptable measure of *intentions to comply* latent variable.

Table 5.18: Reliability and goodness-of-fit statistics, intentions to comply

Chi-square (χ^2)	**Control**		**Treatment**	
Chi-square (χ^2)	12.15		8.25	
Degrees of freedom (df)	2		1	
Normed chi-square (χ^2/df)	6.07		8.25	
Chi-square (χ^2) p-value	0.002		0.004	
Goodness-of-fit indices				
Comparative fit index (CFI)	0.979		0.984	
Tucker-Lewis index (TLI)	0.937		0.906	
Standardized root mean residual (SRMR)	0.029		0.018	
Root mean square error of approximation (RMSEA)	0.159		0.159	
Construct reliability measures	**CA**	**CR**	**CA**	**CR**
Intentions to comply	0.876	0.89	0.881	0.872
CA=Cronbach's alpha; CR=composite reliability; Note, AVE is not available for congeneric models				

5.3.5.3 Intention to comply

Table 5.19 summarizes the item reliability measures, shown as SMC, and factor loadings (Std. Estimates) for the four items measuring *intentions to comply*. All factor loadings were acceptable. However, SMC for INT05 for the control group (0.441) and

particularly treatment group (0.395) was low compared to the other measurement items. While item reliability between 0.3 and 0.5 is still considered adequate, item INT05 was a possible candidate for deletion. Section 5.3.7 below reports the results of the analysis of the full measurement model where the implications of deleting the item were assessed.

Table 5.19: Parameter estimates for intentions to comply

Item		Latent Variable	Estimate	S.E.	Critical Ratio	*p*	SMC	Std. Estimate
Control group								
INT01	<--	INTENTIONS_TO_COMPLY	1				0.681	0.825
INT02	<--	INTENTIONS_TO_COMPLY	1.040	0.072	14.51	***	0.750	0.866
INT04	<--	INTENTIONS_TO_COMPLY	1.077	0.071	15.16	***	0.815	0.903
INT05	<--	INTENTIONS_TO_COMPLY	0.796	0.079	10.14	***	0.441	0.664
Treatment group								
INT01	<--	INTENTIONS_TO_COMPLY	1				0.841	0.917
INT02	<--	INTENTIONS_TO_COMPLY	0.749	0.061	12.32	***	0.554	0.745
INT04	<--	INTENTIONS_TO_COMPLY	0.857	0.059	14.57	***	0.729	0.854
INT05	<--	INTENTIONS_TO_COMPLY	0.581	0.060	9.697	***	0.395	0.628
Std. Estimate=factor loadings; *=p<0.05; **=p<0.01; ***=p<0.001								

5.3.5.4 Multi-group analysis of model equivalence

Multi-group analysis was conducted to test if the measurement items for the *intentions to comply* congeneric model operate equally for both groups. Table 5.20 summarizes the goodness-of-fit statistics and chi-square difference ($\Delta\chi^2$) test results.

With the exception of the normed chi-square, TLI and RMSEA, all goodness-of-fit statistics were acceptable. The values of the normed chi-square (χ^2/df = 6.8), TLI (0.926), and RMSEA (0.12) suggest that the baseline model is a poor representation of the sample data. Further, the $\Delta\chi^2$ values in Table 5.20 show that the baseline congeneric model and the constrained Model A were significantly different ($\Delta\chi^2$ p = 0.009) suggesting that one or more items were not operating equally across the two groups. To find out which item was different across groups, each item was unconstrained separately. As can be seen from the $\Delta\chi^2$ values, all three models, Model

B ($\Delta\chi^2$ p = 0.004), Model C ($\Delta\chi^2$ p = 0.009) and Model D ($\Delta\chi^2$ p = 0.025), were significantly different from the baseline model.

Table 5.20: Intentions to comply congeneric model equivalence test results

Model Chi-square	Baseline	Model A	Model B	Model C	Model D	Model E
Ch-square χ^2	20.40	31.91	31.64	31.91	27.76	51.23
Degrees of freedom (df)	3	6	5	6	5	6
Normed chi-square χ^2/df	6.80	5.32	6.33	5.32	5.55	7.32
χ^2 p-value	0.000	0.000	0.000	0.000	0.000	0.000
Goodness-of-fit indices						
CFI	0.982	0.973	0.972	0.973	0.976	0.953
TLI	0.826	0.945	0.932	0.945	0.942	0.920
SRMR	0.029	0.340	0.034	0.034	0.034	0.033
RMSEA	0.120	0.103	0.115	0.103	0.106	0.125
Test of model equivalence						
$\Delta\chi^2$	-	11.51	11.24	11.51	7.36	7.29
Δdf	-	3	2	3	2	3
$\Delta\chi^2$ p-value	-	0.009	0.004	0.009	0.025	0.063

Baseline model=no constraints
A=Factor Loadings constrained equal
B=Factor Loadings constrained equal + no constrain on INT05
C=Factor Loadings constrained equal + no constrain on INT04
D=Factor Loadings constrained equal + no constrain on INT02
E=Factor Loadings constrained equal + INT02 to 0
$\Delta\chi^2$, Δdf, $\Delta\chi^2$ p-value compared with Baseline model with no equal constraints

To further investigate model equality issues, item INT05, which as discussed in Section 5.3.5.3 was a candidate for deletion, had error covariance specified between INT02 and INT05 specified for the treatment group model. The error covariance associated with INT02 and INT05 was constrained to zero (see Model E in Table 5.20) and item INT02 was unconstrained given the relatively high chi-square difference p-value as seen in Model D ($\Delta\chi^2$ p = 0.025). The results of the $\Delta\chi^2$ test for the *intention to comply* congeneric model E ($\Delta\chi^2$ p = 0.063), suggest partial equivalence, which is adequate (Hair et al., 2010).

5.3.6 Actual password compliance measurement

Actual password compliance was measured as a single item. It was obtained from the password strength of the passwords collected in Phase I of this study. Password strength was computed using the password analysis tool developed for this study (see Section 4.6.9).

5.3.7 Analysis of the full measurement model

To rule out any possible multicollinearity issues or cross-loadings, the re-specified measurement models described in Sections 5.3.3 to 5.3.5 were combined, then analyzed as a full measurement model and goodness-of-fit statistics and reliability measures examined.

Table 5.21 summarizes the goodness-of-fit statistics and reliability measures for the full control and treatment measurement models. The table shows the data with and without INT05. As shown, excluding INT05 resulted in a better fitting control group model and a significant change in χ^2 ($\Delta\chi^2 = 59.517$, $\Delta df = 27$, $p<0.001$). Excluding INT05 also resulted in a better fitting treatment group model and a significant change in χ^2 ($\Delta\chi^2 = 55.693$, $\Delta df = 26$, $p<0.001$). The AVE values indicate that the final control and treatment models had no discriminant or convergent validity issues while all construct reliability measures were also acceptable. There was also no indication of multicollinearity issues, or cross-loading issues for either model. Therefore, the proposed final measurement model is a good representation of the sample data in this study, thus suitable for SEM structural model analysis.

Table 5.21: Reliability and goodness-of-fit statistics, full measurement model

Chi-square (χ^2) without INT05	Control		Treatment	
Chi-square (χ^2)	516.24		531.67	
Degrees of freedom (df)	325		325	
Normed chi-square (χ^2/df)	1.59		1.64	
Chi-square (χ^2) p-value	0.000		0.000	
Goodness-of-fit indices				
Comparative fit index (CFI)	0.959		0.958	
Tucker-Lewis index (TLI)	0.952		0.951	
Standardized root mean residual (SRMR)	0.051		0.044	
Root mean square error of approximation (RMSEA)	0.054		0.056	
Construct reliability measures	**CR**	**AVE**	**CR**	**AVE**
PERCEIVED_SEVERITY	0.921	0.745	0.887	0.667
PERCEIVED_THREAT	0.976	0.890	0.960	0.828
PERCEIVED_VULNERABILITY	0.882	0.715	0.922	0.798
PERCEIVED_SELF-EFFICACY	0.885	0.662	0.910	0.716
PERCEIVED_COST	0.880	0.650	0.899	0.692
PERCEIVED__PASSWORD_EFFECTIVENESS	0.846	0.526	0.918	0.691
INTENTIONS_TO_COMPLY	0.900	0.751	0.879	0.709
CR=composite reliability; AVE=average extracted variance				

5.4 Analysis of structural model validity

This section presents the results of the structural model testing. The final structural model was first examined for specification issues by considering the goodness-of-fit statistics of the nested structural model. The validity of the structural model, including the direction of the relationships, path significance, size of the path estimates, and the SMC values which are comparable to the use of R^2 in multiple regression were examined.

5.4.1 Structural model specification

This section presents the analysis of the validity of the structural model and the path coefficient results. The goodness-of-fit statistics for the nested model were acceptable. Model χ^2 was 1220.024 with 711 degrees of freedom resulting in an acceptable normed chi-square (χ^2/df) of 1.716. The χ^2 p-value was significant (p = 0.000) which

was expected for a sample size greater than 200 (Hair et al., 2010). Although the SRMR was 0.094, suggesting poor fit, the CFI (0.947), TLI (0.940) and RMSEA (0.042) indicated good fit for a complex model with 29 observed variables (Hair et al., 2010). Given a complex model like this one, the SRMR statistic of 0.094 is acceptable since the value is less than 0.1 indicating that it is not a bad fit, and the CFI is greater than 0.92 (Hair et al., 2010). Thus, the goodness-of-fit statistics for the nested structural model suggest that the control and treatment group baseline structural models fit the data well.

Only a few residuals (particularly for the treatment group) were high, and the M.I. values were not high enough to warrant additional paths or suggest cross-loadings. As it is normal for two groups to behave differently (Byrne, 2008), and a non-normal distribution can be expected in a treatment group (Hair et al., 2010), the differences in residuals observed in this study are considered acceptable. As the fit of the structural model was good, no further modifications were made.

5.4.2 Structural model validity

To assess the validity of the structural model the correlations between latent variables, the path coefficients (path correlations), standard errors, and goodness-of-fit statistics were considered. Table 5.22 shows the goodness-of-fit statistics and path estimates for the control and treatment group structural models.

The correlations between latent variables were all below the recommended 0.9 threshold (Hair et al., 2010). Complete correlation matrices for the control and treatment group structural model can be located in Appendix I, Table I.11 and Table I.12. The goodness-of-fit statistics for both models were all acceptable except SRMR. However, for a complex model like the one tested in this study, SRMR of 0.092

(control and treatment, separately) is acceptable as the CFI for each study group was greater than 0.92 (Hair et al., 2010). Thus, the goodness-of-fit statistics suggest that even when tested separately the observed data fits the each group's final structural model well.

The final structural models consist of five exogenous variables, *exposure to hacking*, *perceived severity*, *password self-efficacy*, *perceived password effectiveness* and *perceived cost*, and four endogenous variables, *perceived vulnerability*, *perceived threat*, *intentions to comply* with password guidelines and *actual password compliance*. As shown in Table 5.22, seven hypothesized paths were significant while three were not.

Table 5.22: Path coefficients, standard errors and goodness-of-fit statistics for the structural model

Hypothesized path			Path coefficient	S.E.	p-value	Path coefficient	S.E.	p-value
			Control			Treatment		
Exposure to hacking	→	Perceived vulnerability	0.38	0.097	<0.001	0.30	0.053	<0.001
Perceived severity	→	Perceived threat	0.51	0.065	<0.001	0.55	0.072	<0.001
Perceived vulnerability	→	Perceived threat	0.23	0.071	<0.001	0.29	0.052	<0.001
Perceived vulnerability	≠	Intentions to comply	0.00	0.053	0.500	0.04	0.054	0.284
Perceived threat	→	Intentions to comply	0.18	0.058	0.013	0.13	0.078	0.047
Perceived severity	→	Intentions to comply	0.03	0.052	0.340	-0.05	0.077	0.267
Password self-efficacy	→	Intentions to comply	0.47	0.065	<0.001	0.60	0.085	<0.001
Perceived password effectiveness	→	Intentions to comply	0.19	0.095	0.015	0.18	0.094	0.016
Perceived cost	→	Intentions to comply	-0.01	0.046	0.421	-0.02	0.056	0.404
Intentions to comply	→	Actual compliance	0.36	1.105	<0.001	0.15	1.016	0.024
Goodness of fit statistics								
Chi-square (X^2)			629.62			695.77		
Degrees of freedom (df)			383			383		
Normed chi-square (X^2/df)			1.64			1.64		
Chi-square (X^2) p-value			0.000			0.000		
Comparative fit index (CFI)			0.948			0.948		
Tucker-Lewis index (TLI)			0.940			0.940		
Standardized root mean residual (SRMR)			0.092			0.092		
Root mean square error of approximation (RMSEA)			0.057			0.057		
Path coefficient are represented as Standardized Regression Weights in AMOS								

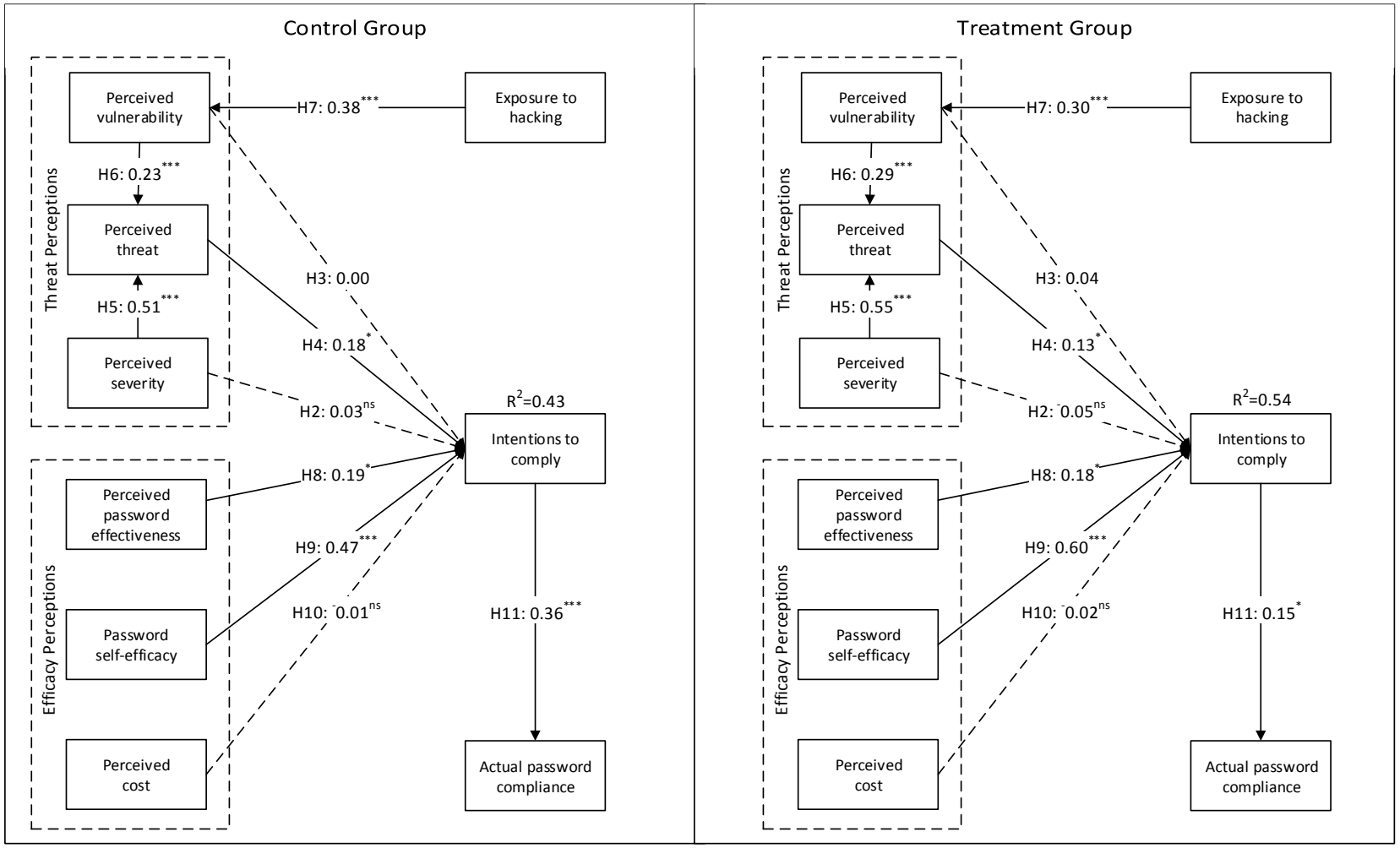
Finally, as an additional goodness-of-fit measure, the SMC associated with the dependent variable, *intentions to comply*, was also considered. In SEM analysis, the SMC values associated with an endogenous variable represent the proportion of variance explained by the structural model. The SMC is thus analogous to R^2 in a traditional regression analysis. The SMC values (control 0.43 and treatment 0.54) indicate that the control group model explained 43% of the variance in *intention to comply* and the treatment group model explained 54% of variance in *intention to comply*. Therefore, both models explained *intention to comply* moderately well.

5.5 Analysis of the research hypotheses

Figure 5.4 is a representation of the full control and treatment group structural model. The hypotheses that were supported in the control group model were also supported in the treatment group model. Similarly, the hypothesized relationships that were rejected in the control group model were also rejected in the treatment group model, thus suggesting that the models are equal across the two groups.

The paths between the two *Threat Perceptions* factors, *perceived severity* and *perceived vulnerability*, and *intentions to comply* with password guidelines were not significant. Also not significant, was the path between *perceived cost* and *intentions to comply* with password guidelines. The strongest predictor of *intentions to comply* with password guidelines was *password self-efficacy* for the both the control group (path coefficient=0.47) and the treatment group (path coefficient=0.60). Whether the participants intended to comply with the password guidelines was largely based on their confidence in their ability to create strong passwords.

Figure 5.4: Structural model for the control and treatment group



*p<0.05; **p<0.01; ***p<0.001; ns=not supported; ⟶ = significant path; - - → = non-significant path;

The path between *perceived severity* and *perceived threat* were significant, and the path between *perceived vulnerability* and *perceived threat* was also significant. This suggests that *perceived threat* is influenced by *perceived severity* and *perceived vulnerability*. While the path between *perceived vulnerability* and *intentions to comply* was not significant, nor the one between *perceived severity* and *intentions to comply*, the path between *perceived threat* and *intentions to comply* was significant. According to Baron and Kenny (1986) these results suggest that the effect of *perceived vulnerability* and *perceived severity* on *intentions to comply* with password guidelines may be mediated by *perceived threat*. An analysis of total effects was thus conducted to explore if there were any significant indirect effects, particularly for the *Threat Perceptions* component of the model.

The standardized total effects summarized in Table 5.23 indicate that for both groups *exposure to hacking* had a significant indirect effect on *perceived threat* however the effect was weak at <0.2 (Hair et al., 2010). *Exposure to hacking* had no significant indirect impact on *intentions to comply* with password guidelines. The results also suggest that for the control group, *perceived severity* and *perceived vulnerability* had a significant indirect effect on *intentions to comply* with password guidelines through *perceived threat*. Also for the control group, the results indicate that *perceived threat* has a significant indirect effect on *actual password compliance*. The control group's *password self-efficacy* also had a significant indirect effect on *actual password compliance*.

The standardized total effects were however different for the treatment group. *Perceived severity* and *perceived vulnerability* did not have a significant indirect impact on *intentions to comply* with password guidelines and *perceived threat* had no significant indirect effect on the treatment group's *actual password compliance*.

Therefore, the effects of *perceived vulnerability* and *perceived severity* on compliance intentions differ between the two groups. The effect of *password self-efficacy* on *actual password compliance* was also different between the two groups. Unlike the control group, the treatment group's *password self-efficacy* also had no significant indirect effect on *actual password compliance.*

Table 5.23: Standardized total effects on the dependent variables

	Exposure to hacking	Perceived severity	Perceived vulnerability	Perceived threat	Perceived password effectiveness	Password self-efficacy	Perceived cost	Intentions to comply
Control group								
Perceived vulnerability	0.375**							
Perceived threat	**0.087****	0.514**	0.233**					
Intentions to comply	0.016	**0.125***	**0.042***	0.181*	0.186*	0.472**	-0.013	
Actual password compliance	0.006	0.044	0.015	**0.064***	0.066	**0.168***	-0.005	0.356**
Treatment group								
Perceived vulnerability	0.299**							
Perceived threat	**0.085****	0.546**	0.285**					
Intentions to comply	0.023	0.022	0.076	0.131*	0.179*	0.597**	-0.015	
Actual password compliance	0.003	0.003	0.011	0.019	0.026	0.086	-0.002	0.144*

Two-tailed significance at 95% Confidence Interval: * $p < 0.05$; ** $p < 0.01$
Table shows total effects (direct effect + indirect effect) of each latent variable listed across the top of the table as column headings and all the dependent variable listed as side row headings.
Significant indirect effects are shown in bold text

The following sections are organized as follows. Sections 5.5.1 to 5.5.4 present the results of testing the hypothesized paths as depicted in Figure 5.4. Section 5.5.5 presents the results relating to the effects of fear appeals on *Threat Perceptions*, *Efficacy Perceptions*, and compliance with password guidelines. Lastly, Section 5.5.6 reports the results of the long-term effects of the fear appeals used in this study.

5.5.1 Exposure to hacking and perceived vulnerability

As hypothesized, *exposure to hacking* was shown to have a significant influence on *perceived vulnerability* for the control (path coefficient=0.38) and treatment group (path coefficient=0.30). This suggests that when individuals or people they know personally are exposed to a hacking incident, they are more inclined to feel vulnerable to password threats. Therefore, **H7**, *exposure to hacking* is **positively related to** *perceived vulnerability* **was supported**.

5.5.2 Threat perceptions and intentions to comply

Contrary to what was hypothesized, *perceived severity* had no association with *intentions to comply* for the control (path coefficient=0.03) and the treatment group (path coefficient=-0.05). This finding suggests that the degree to which a user believes that the consequences of password threat would be detrimental has no impact on *intention to comply* with recommended password guidelines. Therefore, **H2**, a user's *perceived severity* of password related threats is **positively related to** *intentions to comply* with password guidelines, **was not supported**.

As hypothesized, the results of this study also provide no evidence of an association between *perceived vulnerability* and *intentions to comply* with password guidelines. The paths associated with this relationship were not significant for both the control (path coefficient=0.00) and treatment group (path coefficient=0.04). This suggests that

the degree to which users believe they are likely to experience a password related threat does not influence their compliance intentions. This finding is consistent with numerous other PMT studies in the IS security domain, particularly those related to personal computer protection, which found no support for a direct relationship between threat vulnerability and intentions (e.g., Crossler, 2010; Liang & Xue, 2010; Milne et al., 2009; Woon et al., 2005; Zhang & McDowell, 2009). Therefore, **H3**, *perceived vulnerability* to password related threats **will not have a direct effect** on intentions to comply with password guidelines, **was supported**.

Although in this study *perceived vulnerability* had no impact on *intentions to comply* with password guidelines, the results show a significant relationship between *perceived vulnerability* and *perceived threat* for both the control (path coefficient=0.23) and the treatment group (path coefficient=0.29). This indicates that the degree to which users believe that they are likely to experience password related threats contributes to their emotional feeling of concern towards password related threats. Therefore, **H4**, a user's *perceived vulnerability* is **positively related to** *perceived threat,* **was supported**.

The results of this study suggest that *perceived threat* is also influenced by perceptions about the severity of password threats. The path between *perceived severity* and *perceived threat* was significant for both the control (path coefficient=0.51) and the treatment group (path coefficient=0.55). This suggests that users' *perceived severity* significantly affects their level of concern for password related threats. Therefore, **H5**, a user's *perceived severity* is **positively related to** *perceived threat,* **was supported**.

Of the three *Threat Perceptions* latent variables, *perceived threat* was the only one shown to directly predict the participants' compliance intentions. The path between *perceived threat* and *intentions to comply* with password guidelines was significant for both the control (path coefficient=0.18) and treatment group (path coefficient=0.13).

This suggests that when users worry about password threats, they are more likely to form *intentions to comply* with the recommended guidelines. Therefore, **H6**, a user's *perceived threat* is **positively related to** *intentions to comply* with password guidelines, **was supported.**

In summary, the results suggest that the *Threat Perceptions* component of the research model is a weak predictor of *intentions to comply* with password guidelines. This is, however, consistent with findings in the PMT literature (e.g., Aytes & Connolly, 2004; Maddux & Rogers, 1983; Milne & Milne, 2000). The results of this study thus suggest that the threat appraisal component of PMT has only a relatively small impact on IS security behaviors.

5.5.3 Efficacy perceptions and intentions to comply

The results of this study suggest that *perceived password effectiveness* affects compliance intentions. The path between *perceived password effectiveness* and *intentions to comply* with password recommendations was significant for the control (path coefficient=0.19) as well as for the treatment group (path coefficient=0.18). This suggests that users are more likely to intend to comply with password guidelines when they believe that doing so will protect their online account from being hacked. Therefore, **H8**, a user's *perceived password effectiveness* is **positively related to** *intentions to comply* with password guidelines, **was supported**.

As hypothesized, the results of this study show that self-efficacy perceptions play a significant role in promoting compliance intentions. The path between *password self-efficacy* and *intention to comply* was significant for both the control (path coefficient=0.47) and the treatment group (path coefficient=0.60). This implies that the users confidence in their ability to create strong passwords that are also easy to

remember determines whether they intend to comply with recommended measures. Therefore, **H9**, a user's *password self-efficacy* is **positively related to** *intentions to comply* with password guidelines, **was supported**.

Contrary to what was hypothesized, the path between *perceived cost* and *intentions to comply* was not significant for either the control (path coefficient=-0.01) or the treatment group (path coefficient=-0.02). This indicates that the participants' perceived difficulty in remembering strong passwords did not affect their intentions to follow the recommended password guidelines. Therefore, **H10**, a user's *perceived cost* is **negatively related to** *intentions to comply* with password guidelines, **was not supported**.

In summary, the *Efficacy Perceptions* component of the research model proposed in this study is a better predictor of *intentions to comply* than the *Threat Perceptions* component. Of the three *Efficacy Perceptions* factors, *password self-efficacy* and *perceived password effectiveness* have a significant influence on compliance intentions. This is consistent with findings from several PMT studies (e.g., Aytes & Connolly, 2004; Floyd et al., 2000; Maddux & Rogers, 1983; Milne & Milne, 2000) which suggest that coping appraisal may be a better predictor of preventative behavior than threat appraisal. Like these studies, the results of this study also suggest that self-efficacy perceptions have a strong influence on compliance intentions.

5.5.4 Intentions to comply and actual password compliance

As hypothesized, *intentions to comply* with password guidelines predict *actual password compliance*. The paths between *intentions to comply* with password guidelines and *actual password compliance* were significant for both the control (path coefficient=0.36) and treatment group (path coefficient=0.15). This suggests that

whether a user intends to comply predicts actual compliance. However, the correlation between compliance intentions and *actual password compliance* was stronger for the control group. Overall, the results provide evidence of a significant link between intentions and actual behavior. Therefore, **H11**, intentions to comply is **positively related to** *actual password compliance,* **was supported**.

5.5.5 Effects of fear appeals on perceptions and compliance

This study proposes that providing fear appeals will increase user compliance with password guidelines. In this study, compliance with password guidelines is examined as compliance intentions and actual compliance. Thus, this section reports the results on whether the fear appeals (password security information and training) used in this study increased threat and efficacy perceptions, and whether the effects led to improved compliance intentions and password strength.

This section first presents the results of the one-way MANOVA conducted to examine the overall effect of the password security information and training. This is followed by the results of the one-way ANOVA conducted on the variables from the model (*perceived severity*, *perceived vulnerability*, *perceived threat*, *perceived password effectiveness*, *password self-efficacy*, *perceived cost* and *intentions to comply* with password guidelines), to examine if the means were higher for participants who interacted with the training materials. As the variable *actual password compliance* was measured on a different scale from the other variables, the ANOVA was conducted separately and is discussed later in this section.

The test of MANOVA effect was statistically significant with Pillai's Trace value of 0.345 ($F(7, 398) = 29.99$, $p = 0.000$), therefore the null hypothesis that the group means are equal across the tested variables could be rejected. This suggests that

Internet users' password *Threat Perceptions*, *Efficacy Perceptions* and *intentions to comply* with password guidelines depend on whether they receive training or not. The estimated effect size represented by the Partial Eta Squared value (partial η^2) was 0.345 indicating that 34.5% of the variance in *Threat Perceptions*, *Efficacy Perceptions* and *intentions to comply* with password guidelines was accounted for by the fear appeals.

Prior to examining the individual dependent variables using ANOVA, the assumption of homogeneity of variance was examined. Of the seven dependent variables, three (*perceived threat* p = 0.014; *perceived severity*, p = 0.000; and *password self-efficacy*, p=0.005) did not satisfy the homogeneity of variance assumption of equality of variance. However, none of the variances were greater than four times the size of the standard deviations (SD) and corresponding variances (see Table 5.24). As such, given that the sample sizes of the two groups were virtually equal (n=202 and n=204), the ANOVA results would still be applicable (Howell, 2012).

Table 5.24: Between group mean difference

	ANOVA			Control group			Treatment group		
Dependent variable	F	p-value	η^2	Mean	SD	Variance	Mean	SD	Variance
Perceived vulnerability	27.04	0.000	0.063	3.645	1.337	1.787	4.359	1.424	2.028
Perceived threat	5.91	0.015	0.014	5.235	1.531	2.343	5.569	1.219	1.486
Perceived severity	4.57	0.033	0.011	4.361	1.555	2.417	4.655	1.190	1.417
Password self-efficacy	6.58	0.011	0.016	5.220	1.305	1.704	5.525	1.083	1.172
Perceived password effectiveness	112.05	0.000	0.271	4.736	0.915	0.838	5.750	1.012	1.024
Perceived cost	1.19	0.275	0.003	4.746	1.497	2.240	4.897	1.296	1.680
Intentions to comply	71.44	0.000	0.150	5.286	1.055	1.113	6.224	1.178	1.387

Control n=202; Treatment n=204; η^2 = partial eta squared (equivalent to R^2)
Mean scores based on a 7-point scale

As indicated by the p-values in Table 5.24, all dependent variables except *perceived cost* were significantly different between the two groups. Thus, fear appeals appear to significantly raise the level of *perceived severity*, *perceived vulnerability*, *perceived threat*, *perceived password effectiveness*, *password self-efficacy*, and *intentions to*

comply with password guidelines. For both groups the average levels of *perceived vulnerability* and *perceived severity* were low compared to the rest. The participants' vulnerability perceptions were however the lowest implying that on average users have a low perceived vulnerability to security threats.

The magnitude of the ANOVA effect size (η^2) ranged from 0.011 to a high of 0.217 for the six statistically significant dependent variables with *perceived password effectiveness* shown to be the most influenced by the fear appeals, with the highest variance explained (21.7%) by the fear appeals. The ANOVA effect results suggest that virtually no variance (0.003%) in *perceived cost* was explained by the fear appeals. Except for *perceived cost*, the password security information and training (fear appeals) therefore appear to alter perceptions and lead to higher *intentions to comply* with password guidelines as hypothesized.

The rest of the section presents the results for the effects of the fear appeals on *actual password compliance*. First repeated measures ANOVA results are reported to determine if the password strength for the treatment group was significantly improved compared with the control group. Then a within-group ANOVA is reported to determine if the improvement is a result of the fear appeals.

A repeated measures ANOVA was first conducted to determine if the post-test password strength (the passwords created at the conclusion of Phase I, Time 2) was significantly improved compared with the pre-test password strength (the passwords created at the beginning of Phase I, Time 1). At Time 2, both groups were instructed to create a password that is strong and easy to remember, while the treatment group was also exposed to fears appeals. As hypothesized, the treatment group had a larger improvement compared with the control group; however, the control group also had a significant increase in password strength.

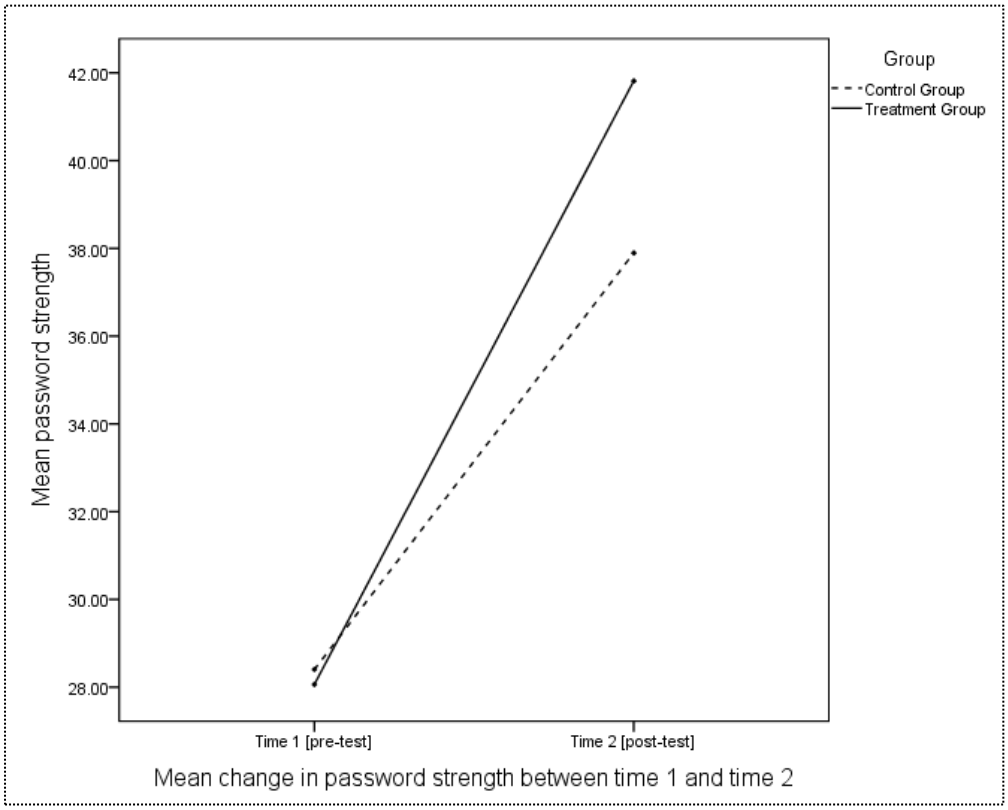
As the means and p-values in Table 5.25 show, there was a significant increase in password strength for both groups ($p<0.001$). The control group had a mean password strength of 28.405 bits at Time 1 and showed a significant ($p<0.001$) increase in password strength (mean = 37.896 bits) at Time 2. The treatment group had a mean password strength of 28.064 bits at Time 1 and a significant ($p<0.001$) increase in password strength at Time 2 (mean = 41.816 bits).

Table 5.25: Descriptive statistics and password strength means

	Mean in bits	Std. deviation	Mean diff.	Std. Error	Sig.
Control Group					
Password strength at Time 1 (pre-test)	28.405	13.534	9.491	1.106	p<0.001
Password strength at Time 2 (post-test)	37.896	17.161			
Treatment Group					
Password strength at Time 1 (pre-test)	28.064	11.029	13.752	1.149	p<0.001
Password strength at Time 2 (post-test)	41.816	16.727			
Mean password strength=password entropy in bits					

Figure 5.5 provides a visual illustration of the mean pre-test and post-test password strength for each group. The lines for both groups suggest that the two groups had a substantial increase in password strength from Time 1 to Time 2. However, the treatment group had a greater increase in password strength.

Figure 5.5: Profile plot showing the mean change in password strength between time 1 and time 2



Given that both groups showed a significant increase in password strength, a between-group ANOVA was performed to examine if the password security information and exercise session had an effect (interaction) on the password strength of the treatment group. The analysis incorporates both a repeated measure effect where password strengths before and after the exercise session are analyzed as well as a between groups effect. The analysis was a 2 x 2 ANOVA with two levels in a repeated measure (pre-test password strength and post-test password strength) and the between groups effects has two groups (control group and treatment group). The results of the within-subjects effects suggest that the treatment group increased significantly more than the control group. The results also show that the group interaction was significant ($F(1,404) = 7.136$, $p = 0.008$), indicating that the treatment group increased significantly more than the control group.

To determine if the increase in password strength was a result of the fear appeals the results of a follow-up within-subject ANOVA (see Table 5.26) were examined. The partial eta squared (η^2) values indicate that compared with the control group, the treatment group had a higher variance explained by the fear appeals. The partial η^2 values suggest that for the control group, only 26.8% of the variance in password strength was accounted for by the time variable, yet for the treatment group 41.4% of the variance in password strength was predicted by the time variable. This suggests that the fear appeals presented to the treatment group led to significantly stronger password strength.

Table 5.26: Within-subjects ANOVA

Test of within subjects effects	df	Mean Square	F	Sig.	Partial Eta^2
Control Group					
Pre-post	1	9098.356	73.684	0.000	.268
Pre-post(Error)	201	123.478			
Treatment Group					
Pre-post	1	19290.545	143.206	0.000	.414
Pre-post(Error)	203	134.705			

In summary, the password security information and training appear to alter threat and efficacy perceptions and lead to significantly improved intentions to comply and improved password strength. Therefore, **H1,** fear appeals will **increase** user compliance with password guidelines, **was supported**.

5.5.6 Effects of fear appeals in the long-term

This section presents the results of the analysis of the data collected in Phase II, six weeks after Phase I. The data includes the passwords used to access the Phase II survey, and the variables related to perceived *password memorability* and *intentions to comply* with password guidelines. The data was examined to determine whether the effects of the fear appeals used this this study were maintained over time.

5.5.6.1 Phase II Participants

A total of 256 follow-up surveys were completed with a total of 194 valid completions. Of these, 99 surveys were completed by participants in the control group and 95 by participants in treatment group. As email invitations were distributed to all the 419 participants who completed Phase I, the valid response rate for the follow-up session was 46.3%.

5.5.6.2 Intentions to comply, six weeks later

Table 5.27 shows the descriptive statistics associated with *intentions to comply* across the two groups. The control group had a slightly lower mean level (M =5.33, SD=1.17) than the treatment group (M=5.42, SD=1.08). To test the hypothesis that password training had a long-term effect on *intentions to comply*, a one-way between-group ANOVA was performed. The assumption of homogeneity of variances was first tested and based on Levene's F test, $F(1,192) = 2.399$, $p = 0.123$ this assumption was satisfied.

Table 5.27: Intentions to comply six weeks later

	n	M	SD	Skew	Kurtosis
Control Group	99	5.33	1.17	-.767	-.328
Treatment Group	95	5.42	1.08	-1.284	-2.049

The between-group ANOVA yielded a statistically non-significant effect F (1,192) = 0.316, p = 0.574, η=.002. Thus, the hypothesis that the means are different was not supported. This indicates that after six weeks, the two groups are equally likely to intend to comply with password guidelines. In comparison, immediately after taking the password security training (six weeks prior), the treatment group's *intentions to comply* with password guidelines were significantly higher (M =6.22, SD=1.18) than those of the control group (M =5.28, SD=1.05). The treatment group was more likely

than the control group to intend to comply with password guidelines immediately after the training. However, six weeks later their intentions were virtually the same as those of the control group. Therefore, **H12,** users who receive fear appeals will have **higher** *intentions to comply* over time than those who do not, **was not supported.**

5.5.6.3 Password memorability

Table 5.28 shows the descriptive statistics associated with actual *password memorability* for the two study groups. Of the 99 returning participants in the control group, only 6.1% (n=6) remembered their previous passwords. While 11.6% of the 95 returning participants in the treatment group remembered their passwords. Those who did not remember their password used a generic password to access the Phase II survey.

Table 5.28: Actual password memorability six week later

	Forgot (used generic passwords)	Remembered (used previous passwords)
Control n=99		
n	93	6
%	93.9	6.1
Treatment n=95		
n	84	11
%	88.4	11.6

A follow-up χ^2 test of independence was conducted to examine if the proportion of those who remembered their passwords was significantly different between the two groups. The χ^2 test statistics suggests no significant difference in actual *password memorability* ($\chi^2(1) = 1.85$, p=0.174) between the two groups. This indicates that the proportion of those who remembered their previous passwords did not vary significantly between the two groups. Although the proportion of those who remembered their passwords was relatively small for both groups, given that the

number of those in the treatment who remembered their passwords was nearly double, this should be explored further in future research.

Table 5.29 shows the descriptive statistics associated with perceived *password memorability* across the two groups. The control group was associated with the smallest mean level of perceived *password memorability* (*M*=2.45, *SD*=1.83) while the treatment group had a higher mean score (*M* =2.81, *SD*=1.94). However, given that the scores were on a 7-point scale, both groups had a relatively low level of perceived *password memorability*. Both groups indicated that it was difficult to remember their password. To determine if the password training had an effect on perceived *password memorability*, a one-way between-group ANOVA was performed. The assumption of homogeneity of variances was first tested. From Levene's F test, $F(1,192) = .68$, $p = 0.410$, the assumption that the variances are equal across the two groups was satisfied.

Table 5.29: Perceived password memorability six weeks later

	n	M	SD	Skew	Kurtosis
Control Group	99	2.45	1.83	1.22	.539
Treatment Group	95	2.81	1.94	.89	-.312

The between-group ANOVA yielded a statistically non-significant effect $F(1,192) = 1.74$, $p = 0.189$, with a squared eta (η^2) value of .009. Thus, the hypothesis that the means are different was rejected, indicating that the two groups showed the same level of perceived *password memorability*. Therefore, **H13,** users who receive fear appeals with a mnemonic training emphasis will have **higher** *password memorability* over time than those who do not, was **not supported.**

5.6 Chapter overview

This chapter reported the results of the data analysis and findings for the research hypotheses for Phase I and II. The results of the measurement model analysis suggest that the final measurement model was a good representation of the sample data in this study. The test of model equivalence also suggests that the measurement model was adequately equivalent across the two groups, and thus suitable for SEM structural model analysis. The structural model was also examined for specification and validity issues. The goodness-of-fit statistics for the nested structural model suggested that the control and treatment group structural models fit the sample data well, thus no modifications were made.

The results of the path analysis show that of the three *Threat Perceptions* latent variables, *perceived threat* has a significant influence on compliance intentions. The *Efficacy Perceptions* component of the research model proposed in this study is a better predictor of *intentions to comply* than the *Threat Perceptions* component, with *password self-efficacy* and *perceived password effectiveness* shown to have a significant influence on compliance intentions. The fear appeals used in this study appear to significantly raise the level of threat and efficacy perceptions, which also lead to significantly improved intentions to comply and password strength. The fear appeals were however shown to have no long-term effects on compliance intentions.

The model explained 43% of the variance in *intentions to comply* for the control group and 54% of variance for the treatment group. Therefore, both models explained *intention to comply* moderately well. Of the ten structural paths tested using SEM, only three were non-significant. As the path between *perceived vulnerability* and *intentions to comply* with password guidelines was hypothesized to be non-significant, eight of

the hypothesized paths were supported by the data. The following chapter discusses in detail the results presented in this chapter.

6 Discussion

6.1 Introduction

This chapter discusses the results and explains the key findings of this study with reference to relevant research. The chapter first presents a discussion of the effects of the fear appeals used in this study on threat and efficacy perceptions and on compliance with password guidelines. This chapter then discusses the results of each hypothesis with explanation of the findings. The contribution of the research model is also discussed in this chapter. Finally, the chapter summarizes key findings and contribution of this research in answering the research questions raised in this study.

6.2 Effects of password security information and training on perceptions and compliance

The fear appeals used in this study, which were in the form of a password security information and training session, were used as a stimuli to alter threat perceptions and efficacy perceptions. This study reveals two key findings concerning the use of fear appeals in the IS security domain.

First, the results suggest that providing password security information and training can alter threat and efficacy perceptions. The participants who received password security information and training had significantly higher mean levels of all threat and efficacy perceptions except *perceived cost*, demonstrating that fear appeals can elevate perceptions about threat and efficacy of password security recommendations. The higher threat and efficacy perceptions among the users who received the fear appeals suggest that fear appeals can be used to elevate user security perceptions and improve

users' confidence in the effectiveness of recommended security measures and their ability to comply with security guidelines.

Contrary to expectations, the fear appeals, which included password training with a mnemonic technique for creating complex passwords, did not significantly decrease the levels of *perceived cost*. On average, both groups indicated that they slightly agree that remembering passwords would be difficult if they followed password guidelines. A potential reason why the two groups had the same average level of *perceived cost* is that most participants already used passwords with 7 or more characters. Further, as indicated by the background statistics described in Section 5.2.3, many of the participants in this study also changed their passwords voluntarily. This may be an indication that the scenarios used in the measurement items for *perceived cost* may have been trivial for this group of participants and therefore the training had no impact on their *perceived cost.*

The second key finding related to fear appeals suggests that providing password security information could lead to improved compliance. In this study, compliance with password guidelines was examined as compliance intentions and actual compliance. The results of this study show that those with high threat perceptions and efficacy perceptions also had significantly higher motivation to comply with password guidelines. This implies that changing how users perceive security threats, their self-efficacy and their confidence in the effectiveness of the security measures, causes significant changes in their compliance intentions. This finding is consistent with PMT (Rogers, 1975, 1983) which suggests that elevating threat and efficacy perceptions increases protection motivation. This finding is also consistent with Johnston and Warkentin's (2010a) experimental study in the IS security domain, where improving

threat perceptions and efficacy perceptions was found to improve users intentions to apply anti-spyware safeguards.

As described in Section 4.6.9, passwords were collected at the beginning of the study (time 1) and at the end of the study (time 2) to determine if there was a significant increase in password strength after the training. The results confirm that providing password security information could improve password strength. The fear appeals used in this study contributed to a significant increase in password strength for the treatment group after the training session. The group of participants who received password security information and training created significantly stronger passwords than those who did not. This is consistent with findings from other password related studies, which found that fear appeals (Vance et al., 2013) or provision of password security training (Charoen, Raman, & Olfman, 2008; Jenkins et al., 2012; McCrohan, Engel, & Harvey, 2010) can significantly improve password strength.

It is of interest to note that the control group also created significantly stronger passwords after completing the survey. There are two possible reasons for this. First, just answering the survey questions may have sensitized the respondents' awareness thus leading to stronger passwords. Secondly, both groups were instructed to create strong memorable passwords at this point. This instruction was to ensure that both groups had an equal opportunity to create passwords that they perceived as strong and easy to remember, thus emulating a typical password login environment. Both groups were therefore expected to have stronger passwords than they created initially when they were only asked to create a password with no additional instruction. However, the password security training led to a weak but significant increase in password strength for the treatment group.

Another interesting finding is that the participants who received the password security information highlighting the likelihood and consequences of password related threats the raised levels of *perceived vulnerability* and *perceived severity* did not lead to increased compliance intentions.

A possible explanation for this finding is that the concept of fear appeals was originally applied to health-related risks such as to promote use of breast cancer preventative measures (Rippetoe & Rogers, 1987). Thus, it is likely that the magnitude of the feeling of susceptibility and severity of an illness such as cancer may not be comparable to the feeling of susceptibility and severity of password related threats (Crossler et al., 2013). This rationale points to a possible limitation in this study and raises the question of whether a more severe message pertaining to vulnerability and severity of password threats would have resulted in higher perceptions of vulnerability and severity. Future research should be undertaken to compare the effectiveness of using different fear appeals messages such as low-threat and high-threat messages.

6.3 Discussion of hypotheses

This section discusses the results of the hypotheses testing relating to the research model proposed in this study. Table 6.1 summarizes the hypothesized relationships, indicating which were supported and which were not. Reasons for this are then explored.

Table 6.1: Summary of hypothesized relationships and effects of fear appeals

Hypothesized relations [supported]
Exposure to hacking → perceived vulnerability
Perceived vulnerability ≠ intentions to comply
Perceived severity → perceived threat ← perceived vulnerability
Perceived threat → intentions to comply
Perceived password effectiveness → intentions
Password self-efficacy → intentions to comply
Intentions to comply → actual password compliance
Fear appeals effects → compliance with password guidelines
Hypothesized relations [not supported]
Perceived severity → intentions to comply
Perceived cost → intentions to comply
Long-term effects of fear appeals → intentions to comply
Long-term effects of fear appeals → password memorability

6.3.1 Exposure to hacking affects perceived vulnerability

Users have a tendency to underestimate their vulnerability to security threats (Sasse et al., 2001; Woon et al., 2005). It is therefore important to understand what it takes to make users believe they are vulnerable to IS security threats. The results of this study suggest that prior *exposure to hacking* contributes to users' belief that they are vulnerable to security threats. When a user or someone they know personally has their online account hacked into they are more likely to feel at risk. This experience is a form of acquired information that shapes how people assess their vulnerability to threats (Skogan & Maxfield, 1981; Weinstein, 1984). By adding a path between *exposure to hacking* and *perceived vulnerability* this study provides some explanation how vulnerability perceptions are developed. A discussion of how *perceived vulnerability* is developed is important given the mixed findings on the role of *perceived vulnerability* in the IS security domain.

6.3.2 Perceived vulnerability does not affect intentions

According to PMT (Rogers, 1975, 1983), a person's perceived vulnerability has a direct impact on their protection motivation. However, the results of this study show no direct association between *perceived vulnerability* and *intentions to comply* with password guidelines. Believing that their online email account was likely to be hacked did not motivate users to comply with password guidelines. This finding supports the hypothesis of this study that *perceived vulnerability* and *intentions to comply* with password guidelines are not significantly related. The results of this study also corroborate the findings of several other IS security studies (e.g. Lee & Larsen, 2009; Vance et al., 2012; Woon et al., 2005; Zhang & McDowell, 2009).

A possible explanation why *perceived vulnerability* is not a significant predictor of compliance intentions in this study is that there might be differences in how users behave in their decision to protect their personal computer environment versus in an organizational setting. This study examined how *perceived vulnerability* relates to users' intentions to comply with the recommended password guidelines on their personal online email accounts.

Like this study, an overwhelming majority of the studies that have examined the relationship between *perceived vulnerability* and IS security behavioral intentions in the context of personal computer protection (i.e., Crossler, 2010; Liang & Xue, 2010; Milne et al., 2009; Woon et al., 2005; Zhang & McDowell, 2009), have found no evidence to support this association. On the contrary, the role of perceived vulnerability has received some support in organizational settings. For example, Lee and Larsen (2009) reported the significant impact perceived vulnerability has on executives' adoption of anti-malware software for their organization. While other studies (e.g., Ifinedo, 2012; Workman et al., 2008) found that perceived vulnerability

influences employees' intentions to comply with security policies within an organizational setting.

The view that users behave differently in different IS security context corroborates Fishbein and Ajzen's (1975) proposition that, given different situations, different beliefs guide an individual's intentions to carry out a specific behavior. A possible implication of this is that it potentially opens new research directions in the applications of PMT to IS security behaviors. For example, future research could be undertaken to compare user security behavior in personal and organizational settings.

6.3.3 Perceived severity does not affect intentions

It was hypothesized that users who view password related threats as a serious issue would be more willing to comply with password guidelines. The results of this study did not support this hypothesis. Whether or not the Internet users were aware of the potential consequences of a threat targeted at their online email account did not influence their compliance intentions. This is an interesting finding given that it contradicts numerous other studies in the IS security domain (e.g., Herath & Rao, 2009; Lee & Larsen, 2009; Siponen et al., 2014; Vance et al., 2012; Woon et al., 2005; Workman et al., 2008) that have found perceived severity to play a significant role in motivating users to follow security recommendations.

The fact that *perceived severity* and, as discussed above, *perceived vulnerability* had no significant influence on *intentions to comply* with password guidelines in this study might be indicative of the limitations of the threat appraisal component in explaining IS security behavior. The fact that perceived vulnerability and severity were weak predictors of compliance intentions is consistent with previous IS security studies (e.g., Aytes & Connolly, 2004; Crossler et al., 2014; Posey et al., 2011; Siponen et al., 2010;

Zhang & McDowell, 2009). Given that even the group of participants who received the fear appeals in this study also had relatively low vulnerability and severity perceptions, this study also raises the question of whether providing information about the likelihood and consequences of threats is enough to improve compliance with security recommendations. The results of this study on the relationship between *perceived vulnerability* and intentions, and *perceived severity* and intentions, also draw attention to the possibility that the underlying assumptions of PMT may not be applicable in the IS security domain.

6.3.4 Perceived severity and perceived vulnerability affect perceived threat

It was hypothesized that when users believe that their email account could be hacked into and that the consequences would be severe, they would be more inclined to worry about threats. Also referred to as fear arousal (LaTour & Rotfeld, 1997; Maddux & Rogers, 1983), *perceived threat* is an emotional response to threat where people feel threatened or worried. As hypothesized, *perceived vulnerability* and *perceived severity* had a significant influence on *perceived threat*. When users perceive their online email accounts as vulnerable to password threats, they develop an emotional feeling towards password related threats.

Likewise, users are inclined to feel threatened when they are aware of the potential consequences of a breach on their email account. This is consistent with the results of Liang and Xue (2010) who found a significant relationship between threat perception and vulnerability and severity perceptions. Herath and Rao (2009) also found a significant relationship between employees' level of concern about security breaches and their awareness of the consequences of a breach, however perceived vulnerability

did not influence their level of concern in that study. Their results also revealed that on average the participants had low perceived vulnerability.

Interestingly, the results of this study revealed a stronger relationship between *perceived severity* and *perceived threat*, than between *perceived vulnerability* and *perceived threat*, for both groups. The results imply perceived severity is a better predictor of *perceived threat* than perceived vulnerability. Although Woon et al. (2005) suggested that communicating to users about severity of a security threat may be more effective than educating them about the probability of experiencing a computer attack, given that users generally have a low perceived vulnerability, perhaps more effort should be made to effectively communicate the prevalence of IS security threats.

6.3.5 Perceived threat affects intentions

As hypothesized, the results of this study show that *perceived threat* had a significant influence on compliance intentions. Users who express a high level of concern about IS security risks are more likely to adopt the necessary preventative measures. This finding supports the previous results of Zhang and McDowell (2009), who found a positive relationship between perceived threat (represented as fear in their study) and intentions to apply online password protection. Liang and Xue (2010) also found a significant association between threat perception and motivation to avoid security risks. Also consistent with this study is the fact that Zhang and McDowell (2009) found perceived threat to be a better predictor of behvaioral intentions than *perceived vulnerability* or *perceived severity*. This is an important finding because many previous applications of PMT to IS security behaviors have overlooked the role of fear.

Conversely, the results of this study contradict the PMT (Rogers, 1983) and other health-related literature (e.g., Maddux & Rogers, 1983; Rippetoe & Rogers, 1987; Witte, 1994) which suggest that fear has an indirect relationship with behavioral intentions through perceived vulnerability and severity. An important implication of this finding is that it highlights the possibility that the role and influence of fear could be different in the IS security domain. Although few IS studies have tested the ability of fear to predict IS security behavioral intentions, the results of this study and that of Liang and Xue (2010) and Zhang and McDowell (2009) suggest that fear has a direct influence on IS related protective behavior. More research will however need to be undertaken before the role and influence of fear in the IS security domain can be clearly understood.

Another important finding is that based on the results of this study, and that of Liang and Xue (2010) and Zhang and McDowell (2009), it appears that emotions play a significant role in motivating users to safeguard their personal information assets. Thus, users feel threatened when they think about the security threats to their personal information assets, which in turn motivates them to apply safeguards. However, in Posey et al. (2011), fear was shown to have no significant influence on employees' intention to protect their organization's information assets.

In fact, the participants in their study had low levels of fear suggesting that employees do not feel threatened when they think about the security threats to their organization. Thus, as Posey et al. (2011) noted it appears that in the context of organizational protection emotions do not influence employees' compliance considerations. The results in this study, and the results of Liang and Xue (2010) and Zhang and McDowell (2009), point to the possibility that there might be a difference between domains, though the evidence is limited.

6.3.6 Perceived password effectiveness affects intentions

As hypothesized, the results of this study show a positive relationship between *perceived password effectiveness* and *intentions to comply* with password guidelines. Users intend to comply with password guidelines with greater consistency when they believe that password guidelines will protect their online account from being hacked. This is consistent with several IS security studies (e.g., Lee & Larsen, 2009; Woon et al., 2005; Zhang & McDowell, 2009) that found perceptions about effectiveness of password guidelines to play a significant role in users' implementation of security measures.

While it is important that users are aware of the available security mechanisms (Dhamija et al., 2006; Dinev & Hu, 2007; Woon et al., 2005), the results of this study show that their decision to apply security measures is dependent on whether they perceive them as effective. It is therefore important that users have confidence that the recommended security safeguards will effectively thwart security attacks.

6.3.7 Password self-efficacy affects intentions

As hypothesized, *password self-efficacy* had a significant influence on *intentions to comply* with password guidelines. This finding suggests that when users are confident in their ability to create and remember strong passwords they are more likely to comply with password guidelines. Self-efficacy has also been found to play a significant role in improving compliance with organizational IS security policies. For example, Vance et al. (2012) and Siponen et al. (2014) demonstrate the importance of strengthening users' beliefs about their ability to apply recommended IS security measures within an organization. Also consistent with this study are findings from

other studies (e.g., Crossler, 2010; Woon et al., 2005) that self-efficacy beliefs have a significant effect on IS security behavior in the context of personal protection.

6.3.8 Perceived cost does not affect intentions

Surprisingly, the hypothesis that *perceived cost* would have a negative influence on *intentions to comply* with password guidelines was not supported. Perceived effort in remembering passwords when the recommended guidelines are followed does not appear to be a factor in users' intentions to comply. This result differs from a previous password related study by Zhang and McDowell (2009), who found that perceived cost has a significant negative influence on users intentions to follow password guidelines. Several other studies have also found perceived cost to have a negative effect on motivation to apply security safeguards (e.g., Lee & Larsen, 2009; Vance et al., 2012).

A possible factor that may have contributed to the non-significant finding is that the items used to measure *perceived cost* all focused on password recall issues. While the struggle to remember and maintain multiple strong password has been a longstanding issue (Bonneau, 2012; Inglesant & Sasse, 2010; NCSA-McAfee, 2011; Yan et al., 2004; Zviran & Haga, 1999), other password related cost factors have also been shown to contribute to poor password practices. For example, Tam et al. (2009) found that when users have a limited time to memorize their email passwords, they tend to create weak passwords. While Grawemeyer and Johnson (2011) found that usability issues such as mistype errors can have a negative impact on password quality. Thus, a consideration of other costs associated with password use such as time (e.g., Tam et al., 2009) and mistype issues (e.g., Grawemeyer & Johnson, 2011) could provide better insights into the relationship.

6.3.9 Compliance intentions leads to actual compliance

It was hypothesized that *intentions to comply* with password guidelines would predict *actual password compliance*. This hypothesis was supported. Users who have a strong motivation to comply with password guidelines are more likely to comply. This finding supports Fishbein and Ajzen's (1980; 1975) proposition that behavior is determined by intentions. The results of this study are also consistent with Liang and Xue's (2010) study in the IS security domain, where home computer users' threat avoidance behavior was found to be determined by avoidance motivation.

Although the hypothesis in this study was supported, the relationship between intentions and actual compliance, particularly for the treatment group, was not strong. This finding has important implications in the application of PMT in IS security research where measures of intentions have been used to predict a variety of security behaviors such as, adoption of specific anti-malware software (Johnston & Warkentin, 2010a; Lee & Larsen, 2009), compliance with a range of security policies (Vance et al., 2012), and adoption of online passwords measures (Zhang & McDowell, 2009).

While PMT assumes that behavior can be adequately predicted by behavioral intentions (Prentice-Dunn & Rogers, 1986; Weinstein, 1993), the results of this study indicate a gap between intentions and actual compliance. Thus it is important to determine how well intentions can predict IS security behavior and the possible factors that may contribute to a weak predictability of actual behavior.

The weak relationship in this study may be attributable to the fact that the participants were asked to indicate their *intentions to comply* with password guidelines for "their important email account" (see Appendix D), but the actual passwords were for a different context, that is, survey passwords. The limitation in this is that when users

perceive their web account as unimportant, they are more likely to ignore safe password practices and use weak or recycled passwords (Adams et al., 1997; Taiabul Haque, Wright, & Scielzo, 2014; Zviran & Haga, 1999). It is therefore possible that the users perceived the survey account as unimportant which may have influence the quality of passwords (*actual password compliance*).

6.3.10 Fear appeals do not have a long-term effect on compliance intentions and password memorability

While some experimental evidence (e.g., Jenkins et al., 2013; Johnston & Warkentin, 2010a; Vance et al., 2013) supports the use of fear appeals within the IS security domain, the long term effects have been largely overlooked. As such, this study contributes to a growing body of fear appeals based IS security research, draws attention to the need of more longitudinal studies in this area. The fear appeals used in this study led to an immediate positive effect on compliance intentions and password strength. However, contrary to the hypothesis in this study, the fear appeals had no long-term effects on *intentions to comply* with password guidelines. This finding suggests that there may be a need for an ongoing IS security training to ensure that users continue to comply.

Fear appeals also had no significant impact on *password memorability* over time. The lack of evidence of a long-term effect of the fear appeals used in this study may be attributable to the fact that the participants were not actually using the passwords for a period of six weeks. The less frequently a password is used, the more difficult it is to remember. While this study provides a point of reference on how difficult it is to memorize passwords, this was a critical limitation, as it does not model a typical operational setting.

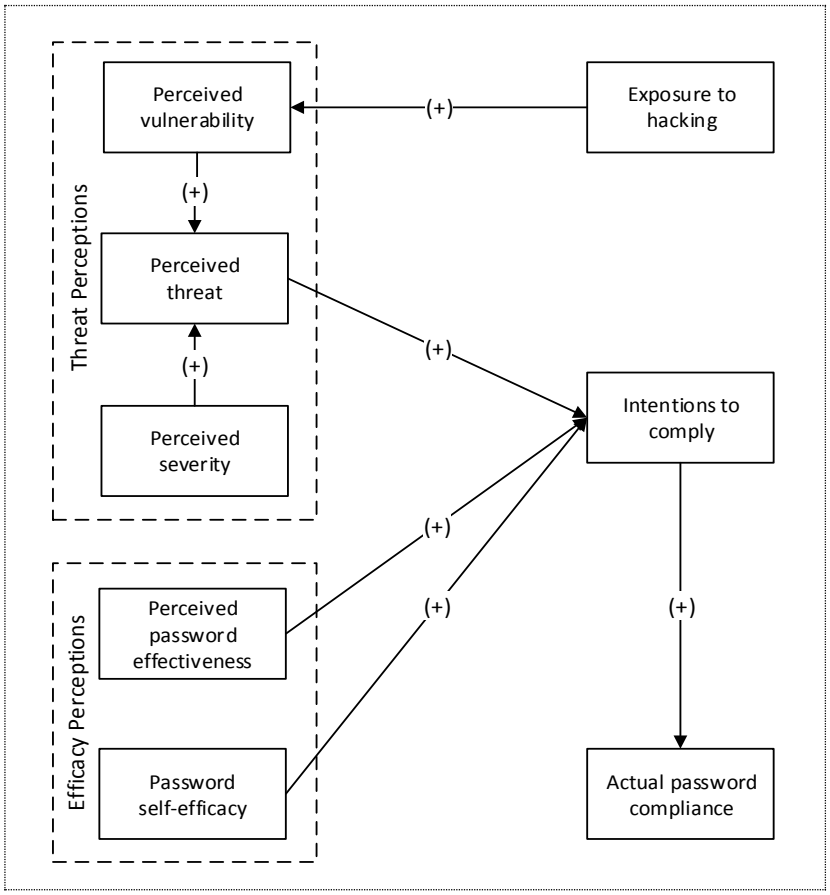
However, as the proportion of those who remembered their passwords after six weeks without using it was nearly double for the group that received mnemonic password training , and the long-term impact of mnemonic training has been demonstrated in studies such as that of Hampstead et al. (2012), further research is warranted. Given that improving a user's ability to memorize passwords promotes safe password practices, the findings in this study, though not conclusive, demonstrates how a key challenge associated with insecure password practices, can be improved and potentially be sustained over time.

6.4 Support for the model proposed in this study

Figure 6.1 illustrates the revised model based on the results. Overall, the proposed research model appears to explain the hypothesized relationships and compliance with password policies relatively well.

The results of this study show that the observed data fit the proposed model well and a large proportion of the variance in *intentions to comply* for both the control and treatment groups. Given that the relationship between *perceived vulnerability* and *intentions to comply* with password guidelines was hypothesized as a non-significant relation, only two hypothesized relationships were not supported. This model therefore provides a substantial contribution to applications of PMT to IS security behaviors.

Figure 6.1: Revised model based on the results



The results suggest that users who have had their online accounts breached are more inclined to feel vulnerable to password related threats, but their vulnerability perceptions have no direct impact on their compliance intentions. Likewise, awareness of the potential consequences of a breach has no direct influence on users' motivation to comply with recommended password guidelines. Although awareness of the likelihood and consequences of a security breach have no direct impacts on compliance intentions, they play a significant role in increasing the level of concern for security threats. When users are concerned about security threats, they are more inclined to be motivated to follow the recommended measures. Internet users who recognize that compliance will protect their online account from being hacked are more motivated to comply. In particular, users' confidence in their ability to create

strong passwords that they can easily recall has a strong influence on their compliance considerations.

6.5 Research questions

This section discusses the contribution of this study toward answering the research questions raised in this study.

The first research question addressed in this study is:

1. *How do user perceptions about password threats and password efficacy affect compliance with password guidelines?*

The results of this study indicate that the threat perceptions have an impact on users' password guidelines compliance intentions but these are not entirely as proposed. *Perceived threat* has a direct impact on compliance intentions, however this study shows that *perceived severity* and *perceived vulnerability* have no direct influence on *intentions to comply* with password guidelines. Interestingly, for those who did not receive the password security information and training compliance intentions appeared to be indirectly influenced by *perceived vulnerability* and *perceived severity* via *perceived threat*. The indirect impact was however weak. These findings highlight the complex nature of the relationship between threat perceptions and IS security behaviors, and raises the question of the potential difference between organizational and personal domains.

The results suggest that efficacy perceptions, *perceived password effectiveness* and *password self-efficacy* have a direct influence on users' intentions to comply with recommended password guidelines, while *perceived cost* has no effect on their compliance intentions. Efficacy perceptions appear to be better predictors of

compliance intentions than threat perceptions, and the relationships were consistent for those who received the training and those who did not.

The second research question addressed in this study is:

2. *Can these perceptions be altered?*

With the exception of *perceived cost*, the results of this study indicate that fear appeals can effectively alter threat perceptions and efficacy perceptions. Overall, the results of this study provide evidence that threat and efficacy perceptions can be altered using fear appeals.

As a follow-up to the previous question, this study also explored whether altering these perceptions can have a positive impact on intentions to comply with password guidelines and actual compliance:

2a. If so, can altering these perceptions improve compliance with password security guidelines?

The results showed that fear appeals significantly increase *intentions to comply* among those who were exposed to the fear appeals. Additionally, those exposed to fear appeals create significantly stronger passwords. Therefore, the results demonstrate that threat and efficacy perceptions can be altered using fear appeals and ultimately improve compliance.

A second follow-up question explores whether any improved compliance with password guidelines is maintained over time:

2b. Can the effects of altering these perceptions be maintained over time?

While the immediate effects of fear appeals were positive, the benefits of altering these perceptions on compliance intentions did not extend very long after the fear appeals intervention period. The results revealed no evidence of a long-term effect. The results show that immediately after providing the password security training, the treatment group's *intentions to comply* with password guidelines was significantly higher than the control group. However, six weeks later their intentions were not significantly different to those of the control group.

It is, however, of interest that nearly double the proportion of those who received training remembered their password over time, suggesting that password recall could potentially be maintained over time if training programs included password memory strategies. However, as *password memorability* was not significantly different between groups, further research, particularly longitudinal studies should be undertaken.

6.6 Chapter overview

This chapter discussed the results of this study and provided possible explanation for the key findings. This study provides insight into how compliance with password guidelines can be improved.

This study demonstrates that fear appeals can elevate perceptions about password threats and about the efficacy of password security recommendations. More importantly, this study shows that elevating users' threat perceptions and efficacy perceptions increases their compliance intentions and significantly improve password quality. Of the three threat perception factors examined in this study, only perceived threat was found to have a significant influence users motivation to comply. Another important finding is that that fear plays a significant role in motivating users to

safeguard their personal information assets therefore highlighting the importance of investigating the influence of fear in future IS security research.

This study contributes to a growing body of fear appeals based research in the IS security domain. In particular, this appears to be the first reported study to examine the long-term effects of fear appeals on IS security behavior. While this study found no evidence of long-term effects on *intentions to comply* with password guidelines, it highlights the need for continuing IS security training to ensure that users continue to comply and more importantly, it draws attention to the importance of conducting longitudinal studies in this area. The following chapter discusses the implications of this research for future research and for practice.

7 Conclusions

7.1 Introduction

This chapter summarizes the contribution of this study to research and practice. The chapter first discusses the key findings of this study and the future research directions associated with the findings. This chapter then discusses the practical contribution of this study. Finally, the key limitations of this study are noted.

7.2 Summary of research contribution

The study described in this thesis addresses three key research questions. The first relates to the impact of perceived password threats and password efficacy perceptions on compliance with password guidelines. While threat perceptions contribute to compliance with password guidelines, only perceived threat was found to have a direct impact on compliance intentions. The results about the role of efficacy perceptions suggest that perceived effectiveness of security measures and self-efficacy perceptions are better predictors of IS security compliance intentions than threat perceptions. This is an interesting finding. Unfortunately, as found in a study by Peters, Ruiter, and Kok (2014) on the effectiveness of fear appeals communication, fear appeals developers underestimate the importance of efficacy-inducing components. Further, perceived cost did not have an effect on compliance intentions.

The second research question relates to whether fear appeals can alter threat and efficacy perceptions, and if in turn, this would improve compliance with password guidelines. The fear appeals used in this study significantly raised the levels of *perceived vulnerability*, *perceived severity*, *perceived threat*, *perceived password effectiveness*, and *password self-efficacy*; only *perceived cost* was not affected.

Furthermore, those who received the fear appeals were more motivated to comply and created stronger passwords. Thus this study shows that fear appeals can be used to alter users' security perceptions and improve compliance with IS security policies.

Finally, this research explores the extent to which the effects of fear appeals are maintained over time. Currently, little is known about the long-term effects of fear appeals on compliance with IS policies. While the fear appeals in this study had no long-term effects on users' compliance intentions, this study makes a substantial contribution by highlighting the need for more longitudinal studies in the IS security domain.

The research model proposed in this study included three key modifications to the PMT (Rogers, 1975, 1983), made to reflect previous research in the IS security domain. Firstly, this study hypothesized that the path between *perceived vulnerability* and *intentions to comply* with password guidelines would be a non-significant relationship. The results of this study support this hypothesis and open up opportunities for future research questions on the role *perceived vulnerability* plays IS security behavior.

Secondly, the model incorporates the impact of prior exposure to a hacking incident (*exposure to hacking*) on *perceived vulnerability*. PMT related studies have reported mixed findings on the role of *perceived vulnerability* and its influence on IS behavioral intentions (Herath & Rao, 2009; Lee & Larsen, 2009; Rippetoe & Rogers, 1987; Vance et al., 2012; Woon et al., 2005; Zhang & McDowell, 2009). *Exposure to hacking* was originally added to the model to help provide a better understanding of the role of *perceived vulnerability* and how vulnerability perceptions are formed. Adding this path provided insights into how users develop vulnerability perceptions but provided no additional insight into the role vulnerability perceptions play in their

decisions to comply with security recommendations. Future research could explore other possible relationships between exposure to hacking, and threat perception and efficacy perception variables.

Lastly, the research model in this study incorporated a path between *intentions to comply* with password guidelines and *actual password compliance*. Like several other studies (e.g., LaRose et al., 2008; Liang & Xue, 2010; Siponen et al., 2014), this study also provides evidence to support an extension of the PMT to include a link between intentions and actual behavior, which only few studies (see Table 2.1), particularly with respect to passwords, have explored.

The research model explained the influences of password compliance relatively well, with eight of the ten hypothesized relationships supported. Further, the model explained 43% of the variance in intentions for the control group and 54% of variance for the group that received the fear appeals. Therefore, the model proposed in this research made a useful contribution to the existing literature.

7.3 Implications for research

This research has provided a better understanding of factors that affect compliance with password guidelines and the effects of fear appeals on IS security compliance. Based on the key findings in this study, a range of areas for future research are discussed in this section.

Future research should further explore the role of fear in IS security behavior: Fear, represented in this study as *perceived threat*, was the only *Threat Perceptions* factor found to have a significant direct impact on password compliance intentions. This is an interesting finding given that the PMT framework (Rogers, 1983) assumes that fear has an influence on protective behavior but only through perceived severity

and perceived vulnerability. Further, this study found that *perceived severity* and *perceived vulnerability* have no direct impact on IS security behavior. This finding also contradicts PMT, and other health-related research (e.g., Maddux & Rogers, 1983; Rippetoe & Rogers, 1987; Rogers, 1983; Witte, 1994) that suggests that severity perceptions and vulnerability perceptions have a direct influence on preventative behavior.

The prevailing viewpoint in IS security research is that severity and vulnerability perceptions have a direct influence on IS protection motivation (e.g., Crossler, 2010; Crossler et al., 2014; Ifinedo, 2012; Lee & Larsen, 2009; Siponen et al., 2014; Vance et al., 2012; Woon et al., 2005; Workman et al., 2008), while the influence of fear has been largely overlooked. The results of this study and findings from studies such as that of Zhang and McDowell (2009) and Liang and Xue (2010), demonstrate that fear should be considered a key variable in future applications of PMT to IS security behaviors.

Users may behave differently in different IS security contexts: The results of this study point to two potential differences in how users behave in different IS security contexts. First, the results open up some interesting questions about how fear influences behavioral intentions, given different IS security contexts. This study suggests that in their decision to comply with security recommendations, users respond emotionally when the security behavior relates to personal protection as opposed to in a work environment. The results of studies such as that of Zhang and McDowell (2009) and Liang and Xue (2010), also suggest that users respond positively to security recommendations if they feel threatened or nervous. In the study by Zhang and McDowell (2009) fear of password related threats was found to influence users' intentions to implement online password protection. While Liang and Xue (2010)

found that users will avoid security threats when they feel personally threatened. A key similarity between these studies and the current study is that they all examined the role of fear in the context of personal computer protection.

One other study that investigated the influence of fear on IS security behavioral intentions was that of Posey et al. (2011). Their study examined the role of fear in employees' motivation to protect their organization's information assets. Posey et al. (2011) found no significant relationship between fear and IS security behavior. They noted that fear may only be a predictor of intentions in the context of personal computer protection. Collectively, these findings suggest that in the context of personal protection, users respond emotionally to threat; this emotional feeling towards security threats influences their willingness to implement security measures. More research should however be undertaken to better understand the impact of fear in different IS security contexts.

The second potential difference in users' protection motivation behavior in different IS security contexts relates to how they assess their vulnerability to security threats. The results of this study show that, in the context of personal protection, the degree to which users believe they are likely to experience a password related threat does not influence their compliance intentions. Interestingly, studies in organizational settings (e.g., Ifinedo, 2012; Lee & Larsen, 2009; Siponen et al., 2014; Workman et al., 2008) have found evidence of a relationship between perceived vulnerability and intentions. While an overwhelming majority of studies in the context of personal protection (i.e., Crossler, 2010; Johnston & Warkentin, 2010a; Liang & Xue, 2010; Milne et al., 2009; Woon et al., 2005; Zhang & McDowell, 2009), including this study, have found no such link. The findings in these studies corroborate the proposition that users generally perceive others as more vulnerable to threats (Sasse et al., 2001; Weinstein, 1984;

Woon et al., 2005). Thus, users' tendencies to perceive others as more vulnerable than them could explain why, in a personal setting, perceived vulnerability has no direct influence on compliance intentions as the results of this study show.

The findings in this study open up a new set of interesting research questions and potential avenues for future research. Based on the results of this study two possible propositions could be made regarding the role of perceived vulnerabity and fear on IS security behavior. First, it is possible that in the context of personal protection, users are influenced by an emotional response to threat. Secondly, given that people appear to have an unrealistically low perception about their vulnerability to threats (Sasse et al., 2001; Weinstein, 1984; Woon et al., 2005), it is likely that in the context of personal protection users' IS security behavior is not influenced by perceived vulnerability. Perceived vulnerability and perceived severity are considered a cognitive response to threat (LaTour & Rotfeld, 1997). Thus, users may respond cognitively in an organizational setting and emotionally in a personal setting. More research should be undertaken to explore if users behave differently, particularly in their threat appraisal process, given different IS security contexts. This would also provide more insight into why the threat appraisal component of PMT has received weak support in the IS security domain.

While these findings suggest an interesting phenomenon, the possibility that the PMT model operates differently in different IS security contexts raises the question of whether PMT in its entirety is applicable in explaining IS security behaviors. Thus, future studies should investigate the applicability of PMT in different IS security domain.

Thus far, research applying the PMT model in the IS security domain largely proposes perceived severity, perceived vulnerability, response efficacy, response cost and self-

efficacy as a key determinant of security behavior. There is, however, no consensus on the exact relationship between these factors and behavioral intentions. The prevailing view is that threat appraisal and coping appraisal factors have an independent and direct impact on users' IS security behavioral intentions. However, the interpretation of the PMT model, particularly on the structure of the threat appraisal component, varies greatly from study to study. This not only makes comparing results across studies challenging, but also, as the findings in this study show, the applicability of PMT in the IS domain is open to question and should be addressed in future studies.

Future studies should consider longitudinal analysis of the effects of fear appeals to determine the long-term effects of fear appeals: The results of this study show that those provided with fear appeals are significantly more likely to comply with password guidelines, and create significantly stronger passwords immediately after experiencing the fear appeals. However, the fear appeals used in this study only had short-term effects. While the results of this aspect of the study are discouraging, they nevertheless suggest a need for future research.

An interesting direction would be to examine whether individual differences play a role in the long-term effects of fear appeals. For example, Hu, West, Smarandescu, and Yaple (2014), found that individuals with low self-control have a tendency to ignore long-term security implications and therefore make risky decisions that are beneficial in the short-term. Using electroencephalography (EEG) and event related potentials (ERPs), the findings in their study, which examined brain neural processes of high and low self-control subjects, suggest that the effectiveness of SETA (security education, training, and awareness) programs may depend on whether an employee has high or low-self-control. Neuro IS security examinations should therefore play a part in future IS security research.

Only a few published applications of the PMT model have examined the effectiveness of fear appeals in IS security research (e.g., Jenkins et al., 2013; Johnston & Warkentin, 2010a; Vance et al., 2013), and none thus far appear to have considered if the effects of fear appeals were maintained after the intervention. As the results of this study show, fear appeals do not always have a long-term effect on security behavior. This study highlights the importance of longitudinal studies; these should be conducted to examine if, and under what conditions, fear appeals can have longer-term effects on IS security behavior.

No significant long-term effect of password training on participants' ability to remember passwords was found. However, although the proportion of those who remembered their passwords after six weeks was not statistically different between the two groups, given that the number of those in the treatment who remembered their passwords was nearly double, future research should consider the long-term effects of different training strategies.

7.4 Implications for practice

This section discusses the practical implications of the findings from this study. This study demonstrates that providing guidance such as awareness training and the necessary skills to implement the recommended security measures can significantly improve security practices. While this study examines compliance with password guidelines on personal email accounts, risky security practices by employees, particularly on their personal online accounts can have serious implications for an organization (Ives et al., 2004; Jenkins et al., 2013; Winkler, 2009). Therefore, in addition to the implications for personal users, this study has implications for organizations as well as IS security training practitioners.

Personal online accounts such as social networking accounts are high on hackers' target lists (Goncharov, 2012). This is because personal online accounts contain sensitive information, including financial and medical information (El Emam et al., 2011; Florêncio & Herley, 2007). Yet, despite the widespread use of weak passwords on the Internet (Florêncio & Herley, 2010; Inglesant & Sasse, 2010; Lorenz et al., 2013), only a small proportion of Internet users are concerned about someone hacking their non-financial or email accounts (NCSA-McAfee, 2011). While this study demonstrates that providing guidance and support to users is important, making such support accessible to users outside of an organizational setting can be a challenge. Vendors and websites typically rely on a set of password guidelines to ensure that the users maintain a certain level of password quality and security, however password guidelines alone have proved to have little impact (Florêncio & Herley, 2007; Vu et al., 2007; Yan et al., 2004). The findings in this study also have implications for vendors and websites that require users to use passwords to access their services.

The importance of raising security awareness through training: Security awareness training has been proposed as an effective strategy for improving compliance with security policies. Training strategies can include communicating the reality of threats to information (Choi et al., 2008; Herath & Rao, 2009) and ensuring users are aware of the appropriate response mechanisms (Puhakainen & Siponen, 2010). Persuasive communication which targets an individual's beliefs in an attempt to persuade into taking preventative measures (Fishbein, 2008; Fishbein & Cappella, 2006; Rogers, 1983) has also been shown to be a valuable means to encourage users to apply security safeguards (Johnston & Warkentin, 2010a; Vance et al., 2013).

This study has shown that users with password security training have higher levels threat awareness, which also increases their overall level of concern for security threats

and the likelihood of compliance with security policies. Organizations should aim to convince users that security attacks are prevalent and emphasize the magnitude of severity this sort of attack could have on their organization or on themselves. Concerning passwords, one of the challenges with the existing password guidelines is that they are ineffective in convincing users to comply with the recommended guidelines (Vu et al., 2007; Yan et al., 2004). Such websites should play a more active role by providing additional information about the likelihood of being hacked and the possible consequences if weak passwords are used.

In addition, users are also more likely to comply if they are convinced that the recommended security mechanisms will prevent threats, and more importantly, if they believe they are able to implement the available security mechanisms. Organizations should also communicate to users what recommended responses are available to prevent a security breach. As this study shows, whether they adopt the recommended security response is dependent upon how effective they feel the recommended response would be in preventing attacks. Therefore, the information should also communicate to users how the recommended security response would prevent attacks. In addition, this study shows that to comply with password guidelines, users must believe that they are capable of creating strong, memorable passwords. As self-efficacy perceptions had the strongest impact on intentions to comply in this study, improving users' self-efficacy should be a training priority. Therefore, at the very least, security training should include how-to instructions, such as how to create strong passwords that are also easy to remember.

There may be need for ongoing IS security training: This study shows that fear appeals can improve compliance with security policies, but only in the short-term. Immediately after the training provided in this study, the group that received the

password information and training were significantly more motivated to comply than the group that received no training. However, six weeks after the training, the two groups were equally likely to intend to comply, suggesting that the effects of the fear appeals diminished over time. The follow-up conducted in this study suggests that organizations may need to communicate security policies to users, including the reason for needing them, available security measures and how to respond using the available security measures, on an ongoing basis.

7.5 Limitations

This research set out to examine factors that contribute to Internet users' motivation to comply with password security recommendations, and to determine if these factors can be manipulated to improve compliance. One of the strengths of this study is that it looked at online password behavior, not in general, but specific to high-value personal email accounts. This is important as, for instance, a user's perception of severity may vary between a personal email account and a blog account, leading to different password behaviors across different websites (Zhang & McDowell, 2009). Thus, the results of this study can be generalized to password behaviors on high-value online accounts.

There are however several limitations of this study that need to be considered. First, the data was obtained from one country, the USA. Future studies may consider potential differences in the effect of fear appeals across different cultures. A study by Hovav and D'Arcy (2012) in the IS security area, found significant cultural differences in the effect of some IS misuse deterrence mechanisms. Their results suggest that for users in the USA, severity of punishments is effective as a deterrent against IS misuse, while users from Korea are motivated by the likelihood of being caught. Although

their study examined compliance within an organizational setting, cultural differences may also apply in the context of personal protection. Nonetheless, the data used in this study represent a wide cross-section of demographics, age, gender and level of education (see Section 5.2), and the sample used was relatively large.

Another limitation in this study relates to the measurement of *perceived cost*. In this study, *perceived cost* had no influence on users' motivation to comply with password guidelines. This may be attributable to the fact that the measurement items focused on password memory issues, which are arguably one of the most important aspects of password use, and something that users find difficult. However, other cost factors that have been shown to contribute to poor password quality (e.g., Grawemeyer & Johnson, 2011; Tam et al., 2009) could be considered in future studies. One aspect of *perceived cost* that could be considered is whether users believe that they have enough time to memorize passwords. When users have a short amount of time to memorize a password they tend to choose weak passwords that are easier to remember (Tam et al., 2009). Usability is another aspect of perceived cost that future studies could consider. Authentication errors resulting from mistyped passwords, which Grawemeyer and Johnson (2011) found to affect password quality, should also be considered in future studies.

This research explored the extent to which the effects of fear appeals are maintained over time. While this is a substantial contribution in the IS security domain where little is known about the long-term effects of fear appeals, the fear appeals in this study had no long-term effects on users' compliance intentions. A potential limitation in this study is that a single application of fear appeals was used; this may not have been adequate to test the long-term implications of fear appeal exposure. Future longitudinal research could incorporate follow-up fear appeal rhetoric as reinforcement.

It is of interest to note that there was a significant increase in password strength for both the treatment group and the control groups. While the treatment group created significantly stronger passwords than the control group, the difference in password strength was small. This suggests that other factors may have led to the increase in password strength, a potentially critical limitation in this study. For example, just answering the survey questions may have sensitized the respondents' awareness thus leading to stronger passwords. Additionally, both groups were instructed to create strong memorable passwords, which was expected to lead to both groups creating stronger passwords than they created initially when they were only asked to create a password with no additional instruction.

Lastly, although PMT assumes that behavioral intentions can adequately predict behavior (Prentice-Dunn & Rogers, 1986; Weinstein, 1993), the model in this study was extended to determine how well intentions predict compliance in IS security policies. As the results of this study show, the relationship between intentions and compliance, particularly for the treatment group, was not strong. A potentially critical limitation of this part of the study is the fact that the measures of intentions related to intention to follow guidelines to protect my "important email account", while the measure for actual compliance related to a different behavioral context, the passwords for the "study survey account". Measures of intentions should be compatible with the measures of actual behavior (Ajzen, 1991; Ajzen & Fishbein, 1977), such as examining intentions to comply with organizational password policies, and actual passwords for the organization.

While this limitation may have affected the predictability of actual compliance, this study makes a significant contribution to the applications of PMT to IS security behaviors, as only a few studies (e.g., LaRose et al., 2008; Liang & Xue, 2010;

Siponen et al., 2014) have examined the link between intentions and actual behavior. This study draws attention to the need for more studies to be undertaken to determine how well intentions predict actual security behaviors.

Appendices

Appendix A HREC permit approval

Murdoch UNIVERSITY

www.murdoch.edu.au

Research Ethics Office
Division of Research and Development

Chancellery Building
South Street
MURDOCH WA 6150
Telephone: 9360 6677
Facsimile: 9360 6686
human.ethics@murdoch.edu.au
www.research.murdoch.edu.au/ethics

Friday, 02 March 2012

Dr Mike Dixon
School of Information Technology
Murdoch University

Dear Mike,

Project No. 2010/218
Project Title Risk Communication and Password Security

AMENDMENT: **Change to the recruitment process**
Change to the reimbursement process

Your application for an amendment to the above project, received on 29 February 2012 was reviewed by the Murdoch University Research Ethics Office and was;

APPROVED

Approval is granted on the understanding that research will be conducted according the standards of the *National Statement on Ethical Conduct in Human Research* (2007), the *Australian Code for the Responsible Conduct of Research* (2007) and Murdoch University policies at all times. You must also abide by the Human Research Ethics Committee's standard conditions of approval (see attached). **All reporting forms are available on the Research Ethics web-site.**

I wish you every success for your research.

Please quote your ethics permit number in all correspondence.

Kind Regards,

Dr. Erich von Dietze
Manager of Research Ethics

cc: Dr Tanya McGill; Florence Mwagwabi

HREC Outright Approval Letter 16012012

CRICOS Provider Code: 00125J
ABN: 61 616 369 313

Appendix B Phase I email invitation

[INSERT NAME], We Have A New Survey For You!

We have a new survey for you. This survey will only take a few minutes and we would appreciate a few minutes of your time to share your opinions. If you qualify and complete this additional survey, we will reward you with 1250 MVPs.

You will need to login to start this survey.
AS A REMINDER, YOUR USERNAME IS: [INSERT USERNAME]

Click Here to Start Your Survey

Please let me know if I can help you in any way. My contact information is below, and I'm always available for your questions.

Sincerely,

Jordan Miller
MyView Community Service Manager
Need Help? I'm Here! Just click to reach me in Customer Care.

MyView • 304 Park Avenue South • 7th Floor • New York, NY 10010

Appendix C Password security information and training materials

Vulnerability Information

The following information illustrates common risks associated with the use of passwords and the likelihood of being hacked into if weak passwords are used. Please read the following text carefully and answer the questions below.

Passwords are the most commonly used methods for logging into online accounts. Passwords are also considered the weakest login methods. This is because techniques for guessing or cracking passwords have become easier than in the past and software for hacking into online accounts is also freely available on the internet. Password guessing is even easier when passwords that are easy to guess are used. For example if your password contains any of the following characteristics your chances of being hacked into are high;

Consecutive numbers such as 12345 – easily cracked using freely available software tools.

Consecutive letters such as ABCD – easily cracked using freely available software tools.

Consecutive keyboard letters such as QWERTY – easily cracked using freely available software tools.

A word or words straight out of a dictionary - easily cracked using freely available password cracking software which searches through a database of dictionary words.

Personal information such as names of your family members, birthdates, geographical location - through a quick internet search, a hacker can easily guess a password containing any personal information.

Reports show that incidents of password hacking are on the rise as internet users continue to use passwords that are easy to guess. In addition, computers are becoming more powerful making it easier and faster to guess passwords. Therefore, if you continue to use weak passwords, it is highly likely that sooner or later your passwords will be cracked and online accounts will be hacked into.

Severity Information

The following information illustrates the consequences and severity of being exposed to password related threats such as hacking.

If any of your passwords are cracked or any of your online accounts are hacked into, any information saved in your account including your personal information may be used by a hacker or exposed to the public. Depending on the information saved on your online account the consequences of hacking can be extremely severe, such as in the case of identity theft, where someone uses your personal information to obtain financial resources such as bank loans or to commit crime. Also, with a cracked password, a hacker can hack into your email account to send spam to your trusted friends. Although this may seem like a mere annoyance, it may also carry severe consequences, in particular, if the spam contains web links or attachments with computer viruses or other malicious software. This may also prompt your email provider to suspend your web account.

The result of one hacked account can lead to additional undesirable consequences. Once one of your online accounts is hacked, a hacker can use information saved in the account to find clues to guessing your other passwords. Information, such as email communications from banks and online shopping stores, may also contain information such as account numbers that attackers may use to crack passwords and attempt to access such accounts.

If any of your online accounts containing personal information such as date of birth, pet’s name, mother’s maiden name, employee number, driver’s license number, government ID number, passport number, credit/debit card number or insurance policy number was hacked into the consequences could be detrimental.

Password Effectiveness Information

The following information describes how password related threats such as hacking can be prevented.

Password related threats can be easily and effectively prevented. The following preventative measures have been shown to effectively prevent password related threats.

Avoiding dictionary words: Password guessing tools work by searching through a list of dictionary words and other commonly used words in any language. Therefore, avoiding dictionary words would prevent your password from being guessed using such tools.

Avoiding personal information in passwords: Passwords should not contain personal information such as date of birth or names of family members. Eliminating personal information from your password would prevent your password from being guessed by people you know or an attacker who may have access to your personal information.

Use of complex passwords: Avoiding dictionary words alone is not enough to prevent successful password guessing attacks, passwords must also be complex. A complex password is long and contains a combination of upper and lowercase letters, numbers and symbols. A complex password is difficult to crack and therefore an effective way to discourage an attacker and make them move on to a less complex password.

Changing passwords regularly and using different passwords for different login accounts is an effective way to prevent an attacker from attempting to access your other web accounts. Changing your password is only effective if the new password is different and not a variation of your other passwords or a compromised password.

Password Training and Exercise

The following information demonstrates how to create a strong password that is also easy to remember. Please read carefully then complete the interactive exercises below.

The use of long complex passwords is a must to prevent password cracking or guessing. However, complex passwords are also difficult to remember. In fact, studies show that users' inability to memorize long series of random characters often forces them to use weak passwords. Studies have also shown that human beings have a better ability to remember more meaningful items such as phrases or songs.

The use of a mnemonic technique will not only help you create strong complex passwords but, most importantly, will help you create passwords you can easily remember. A mnemonic password is created from a sentence or familiar phrase using some letters of each word in the phrase. For example, the phrase, "Pat and I are going to Australia" can be used to create the password; "P&Irg2A".

Keep in mind that the longer the password the harder it is to guess. Although the password "P&Irg2A" is more secure than a password that contains dictionary words or a variation of dictionary words, it does not meet the minimum recommended password length of 8 characters. Furthermore, although a minimum of 8 characters is recommended on many web accounts, a password of 12 characters or more is advised. This is because password guessing software and computer hardware are becoming more powerful making short passwords very easy to crack.

When you use a mnemonic technique, you can create a long, complex password with a combination of random characters and special characters such as "@"without difficulty. For example, using the same sentence "Pat and I are going to Australia", a 12-character password such as "P@&!rg2Aust." can be easily created.

The sentence was transformed into a secure password through the following meaningful patterns, "Pat" was changed to "P@" because of similar sound, "and" to "&", "I" to the symbol "!", "are" to "r", "going" to "g", "to" was changed to the number "2" and "Australia" to "Oz" and finally the password has a period, ".", at the end. Using this method you can create passwords that are difficult for an attacker to guess yet easy for you to remember**.**

Interactive exercises:

It is important to practice creating passwords using the mnemonic technique as well as practice typing the passwords on your keyboard. The following exercises are aimed at helping you practice how to create your own mnemonic passwords.

Using the mnemonic technique described in the information above create sample passwords from the sentences;

1. "An Eye for an Eye a Tooth for a Tooth" in the first textbox.

2. "Different Passwords for Different Login Accounts" in the second textbox.*

Appendix D Phase I survey instrument

Participant Information

We invite you to participate in a research study looking at factors that influence password security practices on the internet. This study is part of my Doctor of Philosophy in Information Technology, supervised by Dr. Mike Dixon and Associate Professor Dr. Tanya McGill at Murdoch University.

Passwords remain the most commonly used method of authentication and are also regarded as the weakest form of authentication. Both technical and non-technical security measures have been developed to prevent password related threats such as hacking. However, researchers and information security practitioners have questioned the effectiveness of such methods in safeguarding users' web accounts. The goal of this study is to investigate ways to develop more effective password guidelines and standards. The outcomes of this study should help us to develop more effective password guidelines and standards.

It is estimated that the questionnaire and activities will take approximately 15/25 minutes to complete. Completion is entirely voluntary and you can decide not to participate at any time simply by closing the browser window. While we would be pleased to have you participate, we respect your right to decline. **We do not ask you to provide your name, email address or other identifying data, so it will not be possible to identify you from your responses.** Please note, you must be 18 years or older to participate in this study.

Please, do not forget to bookmark this website. Once we have analyzed the information, we will be posting a summary of our findings on this website from **June 17 2012** to **July 15 2012**. Also, after completing the questionnaire and activities, you will be redirected back to MyView to receive a reward for participating.

We would like to thank you in advance for your assistance with this research project.

Research contact information

If you have any questions, comments or concerns about this research project, please feel free to contact either myself, Florence Mwagwabi (F.Mwagwabi@murdoch.edu.au), or my research supervisors, Dr Mike Dixon (M.Dixon@murdoch.edu.au) and Associate Professor Dr. Tanya McGill (T.McGill@murdoch.edu.au).

This study has been approved by the Murdoch University Human Research Ethics Committee (Approval No. 2010/218). If you have any reservation or complaint about the ethical conduct of this research, and wish to talk with an independent person, you may contact Murdoch University's Research Ethics Office (Tel. +61 8 9360 6677 or e-mail ethics@murdoch.edu.au). Any issues you raise will be treated in confidence and investigated fully, and you will be informed of the outcome.

Participation is entirely voluntary and you can decide not to participate at any time simply by closing the browser window.

Please confirm you are 18 years or older.*

( ) I am 18 years or older.

If you would like to participate in the survey, please select the box below.

( ) Yes, I agree to participate in this study.
( ) No, I do not want to participate in this study.

*****Page Break Here**

Create password

Once the information collected from this study is analyzed the findings will be posted on this website. You will need a password to return to the website to view the findings and to complete a brief follow-up study and receive another reward from MyView.

Create your password in the textbox below.

Please note: It is advised that you do choose a password that is different from your other passwords. Create a password similar to the kind you would normally use.

Type your password here:_____

*****Page Break Here**

Password and background information

1. What is the longest password you have ever voluntarily used?

( ) 6 characters or less
( ) 7 characters
( ) 8 characters
( ) 9 characters
( ) 10 characters
( ) 11 character
( ) Longer than 12 characters

2) How many email accounts do you currently have? _____

3) Have you ever voluntarily changed any of your email passwords?

( ) Yes
( ) No

4) Have you ever shared any of your email passwords?

( ) Yes
( ) No

	Poor						Excellent
5) How would you rate your computer skills?	1	2	3	4	5	6	7
6) How would you rate your computer security knowledge?	1	2	3	4	5	6	7

*****Page Break Here**

Exposure to hacking

Many web users have email accounts set up for receiving important information such as email messages from friends and family members, online banking notifications and online shopping confirmation. For the purpose of this study, we classify such email accounts as 'important' email accounts.

7. Have you ever had your important email account, online shopping account or online banking account hacked into? If yes, please indicate the degree to which that experience affected you (in terms of lost data, lost time, monetary losses, identity theft etc.) If no, please select 'no'.

(0) No (1) Low impact (2) (3) (4) (5) (6) (7) High impact

8) Has someone you know personally ever had their important email account, online shopping account or online banking account hacked into? If yes, please indicate the degree to which that experience affected them (in terms of lost data, lost time, monetary losses, identity theft etc.) If no, please select 'no'.

(0) No (1) Low impact (2) (3) (4) (5) (6) (7) High impact

*****Page Break Here**

Perceived vulnerability

Consider the passwords you use to log into your important email accounts and where you keep the password, for example on a piece of paper or saved on your computer etc.

To what extent do you agree or disagree with the following statements?

	Strongly disagree						Strongly agree
9) There is a chance that someone could successfully guess at least one of my passwords	1	2	3	4	5	6	7
10) There is a chance that someone could successfully crack at least one of my passwords using password cracking software	1	2	3	4	5	6	7
11) There is a chance that someone could hack into at least one of my important email accounts	1	2	3	4	5	6	7
12) If someone hacked into my important email account, there is a chance that they could guess my other important passwords	1	2	3	4	5	6	7

*****Page Break Here**

Perceived severity

Consider the type of information you have saved in your important email accounts and the type of passwords you use for logging into your important email accounts. How severe do you think the consequences would be if:

	Not at all severe						Very severe
13) Someone successfully guessed any of your important email passwords	1	2	3	4	5	6	7
14) Someone hacked into any of your important email accounts	1	2	3	4	5	6	7
15) Someone used any of your important email accounts to send messages to your contact list without your knowledge	1	2	3	4	5	6	7
16) Someone obtained your personal information from your important email accounts	1	2	3	4	5	6	7
17) Someone changed the password to your important email accounts without your knowledge	1	2	3	4	5	6	7
18) Someone stole the password to one of your important email accounts	1	2	3	4	5	6	7

*****Page Break Here**

Perceived threat

Please indicate the extent to which you agree or disagree with the following statements.

	Strongly disagree						Strongly agree
19) The thought of someone guessing the password to any of my important email accounts makes me worried	1	2	3	4	5	6	7
20) The thought of someone hacking into any of my important email accounts makes me worried	1	2	3	4	5	6	7
21) The thought of someone using any of my important email accounts without my knowledge makes me worried	1	2	3	4	5	6	7
22) The thought of someone using my personal information from any of my important email accounts makes me worried	1	2	3	4	5	6	7
23) The thought of someone changing or deleting information obtained from any of my important email accounts makes me worried	1	2	3	4	5	6	7
24) The thought of someone using password monitoring software to record my important passwords makes me worried	1	2	3	4	5	6	7

*****Page Break Here**

Perceived Password Effectiveness

Please indicate the extent to which you agree or disagree with the following statements.

	Strongly disagree						Strongly agree
25) Making sure that my passwords contain a combination of numbers, letters and symbols will prevent my passwords from being guessed	1	2	3	4	5	6	7
26) Making sure that my passwords do not contain any dictionary words will make them more difficult to guess	1	2	3	4	5	6	7
27) Making sure that my passwords do not contain personal information such as my date of birth will make them more difficult to guess	1	2	3	4	5	6	7
28) I can protect my online accounts better if I use a different password for each of my online accounts	1	2	3	4	5	6	7
29) I can protect my online accounts better if I change my passwords regularly	1	2	3	4	5	6	7
30) I can protect my online accounts better if I use a long complex password	1	2	3	4	5	6	7

***Page Break Here**

Perceived Cost

Please indicate the extent to which you agree or disagree with the following statements.

	Strongly disagree						Strongly agree
31) Remembering a password that contains a combination of numbers, letters and symbols would be difficult	1	2	3	4	5	6	7
32) Remembering a password that is long and complex would be difficult	1	2	3	4	5	6	7
33) Remembering a password that does not contain any dictionary words would be difficult	1	2	3	4	5	6	7
34) Remembering a password that does not contain personal information such as date of birth would be difficult	1	2	3	4	5	6	7
35) If I use different passwords for each of my web accounts, it would be difficult for me to remember them all	1	2	3	4	5	6	7
36) If I change my passwords regularly, it would be difficult for me to remember them	1	2	3	4	5	6	7

***Page Break Here**

Password Self-efficacy

Consider the following scenario. Due to an increase in password hacking incidents, the password requirements for your email account have been changed. You have been asked to change your password immediately and to make sure that your new password follows strict password guidelines provided by the system. Please indicate how confident you are that you would be able to create a password that is strong enough to protect your email account from being hacked into.

I would be able to create a strong password that is difficult to hack...

	Not at all confident						Totally confident
37) If I had instructions on how to create a strong password	1	2	3	4	5	6	7
38) If I had step-by-step instructions on how to memorize a strong password	1	2	3	4	5	6	7
39) If I had a lot of time to create a strong password	1	2	3	4	5	6	7
40) If I had used strong passwords before	1	2	3	4	5	6	7

***Page Break Here**

Intentions to comply with password guidelines

If you were required to change the password for one of your important email accounts, to what extent would you agree or disagree with the following statements.

	Not at all Likely						Very likely
41) I would choose a password that follows the password length requirement suggested by the system	1	2	3	4	5	6	7
42) I would choose a password with a combination of numbers, letters, and symbols as suggested by the system	1	2	3	4	5	6	7
43) I would choose a password that is difficult to guess	1	2	3	4	5	6	7
44) I would choose a password that follows all the guidelines provided by the system	1	2	3	4	5	6	7
45) I would choose a password that is different from my old password	1	2	3	4	5	6	7
46) I would choose a password that is different from my other online passwords	1	2	3	4	5	6	7

*****Page Break Here**

Demographics

47) Please select your gender.

( ) Male
( ) Female

48) How old are you? _____

49) What is the highest level of education you have completed?

( ) Less than high school
( ) Graduated high school or equivalent
( ) Some college, no degree
( ) Bachelor's degree
( ) Post-graduate

50) Comments/Questions: _____

*****Page Break Here**

Change your Password

Please change your previously selected password. Make sure your new password is strong and easy to remember.

Please note: It is advised that you do choose a password that is different from your other passwords.

Don't forget you will use the password to return to this website to access the study results. You will also need the password to return to the website and answer a few brief follow-up questions and receive another reward from MyView.

You old password is: _____

Please create a new password as required: _____

*****Page Break Here**

Thank You!

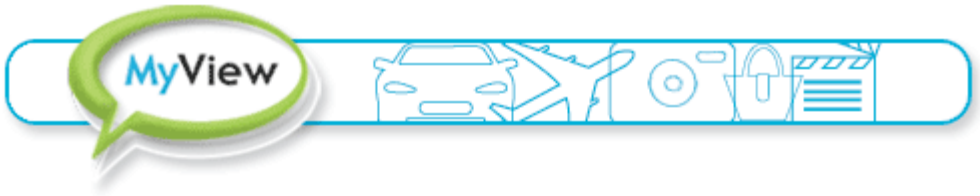
Thank you for taking our survey. Your response is very important to us.

Please, do not forget to bookmark this website. Remember to keep your password safe so that you can use it to return to this website to access the study results. You will also need the password to return to the website and complete a brief follow-up study and receive another reward from MyView.

You will be redirected to MyView in a few seconds.

If you have any questions, comments or concerns about this questionnaire or our research, please feel free to contact either myself, Florence Mwagwabi (F.Mwagwabi@murdoch.edu.au) or my research supervisors, Dr Mike Dixon (M.Dixon@murdoch.edu.au) and Associate Professor Dr. Tanya McGill (T.McGill@murdoch.edu.au).

Appendix E Phase II email invitation



[INSERT NAME], We Need Just A Few More Minutes!

You recently participated in a survey and we have a few more questions for you. This survey will only take a few minutes and we would appreciate a few minutes of your time to share your opinions. If you qualify and complete this additional survey, we will reward you with 1250 MVPs.

You will need to login to start this survey.
AS A REMINDER, YOUR USERNAME IS: [INSERT USERNAME]

Click Here to Start Your Survey

Please let me know if I can help you in any way. My contact information is below, and I'm always available for your questions.

Sincerely,

Jordan Miller
MyView Community Service Manager
Need Help? I'm Here! Just click to reach me in Customer Care.

MyView • 304 Park Avenue South • 7th Floor • New York, NY 10010

Appendix F Phase II survey instrument

Participant Information

Thank you for your previous participation and for returning to view the results and to answer a few further questions. This research study seeks to investigate factors that influence password security practices on the internet and is part of my Doctor of Philosophy in Information Technology, supervised by Dr. Mike Dixon and Associate Professor Dr. Tanya McGill at Murdoch University. The outcomes of this study should help us to develop more effective password guidelines and standards.

It is estimated that the questionnaire will take approximately 5 minutes to complete. Completion is entirely voluntary and you can decide not to participate at any time simply by closing the browser window. While we would be pleased to have you participate, we respect your right to decline. **We do not ask you to provide your name, email address or other identifying data**, so it will not be possible to identify you from your responses.

After completing the questionnaire, you will be redirected back to MyView to receive a reward for participating.

We would like to thank you once again for your assistance with this research project.

Research contact information

If you have any questions, comments or concerns about this research project, please feel free to contact either myself, Florence Mwagwabi (F.Mwagwabi@murdoch.edu.au), or my research supervisors, Dr. Mike Dixon (M.Dixon@murdoch.edu.au) and Associate Professor Dr. Tanya McGill (T.McGill@murdoch.edu.au).

This study has been approved by the Murdoch University Human Research Ethics Committee (Approval No. 2010/218). If you have any reservation or complaint about the ethical conduct of this research, and wish to talk with an independent person, you may contact Murdoch University's Research Ethics Office Tel. (+61 8 9360 6677 or e-mail ethics@murdoch.edu.au). Any issues you raise will be treated in confidence and investigated fully, and you will be informed of the outcome.

Participation is entirely voluntary and you can decide not to participate at any time simply by closing the browser window.

If you would like to participate in the follow-up survey, please select the box below.

If you would like to participate in the survey, please select the box below.*

( ) Yes, I agree to participate in this study.

( ) No, I do not want to participate in this study.

*****Page Break Here**

Login

To view the findings and to complete this brief follow-up study, please enter the password created in the previous study. After completing the questionnaire, you will be redirected back to MyView to receive a reward for participating.

Enter password to view the findings and to complete a few follow-up questions. If you have forgotten your password click the 'next' button below to receive a new password.

Password :_____

*****Page Break Here**

Perceived password memorability

Please indicate the extent to which you agree or disagree with the following statements.

1. It was easy for me to remember the password I created for this study.

(1) Strongly disagree (2) (3) (4) (5) (6) (7) Strongly agree

*****Page Break Here**

Intentions to comply with password guidelines (time 2)

If you were required to change the password for one of your important email accounts, to what extent would you agree or disagree with the following statements.

	Not at all Likely						Very likely
2) I would choose a password that follows the password length requirement suggested by the system	1	2	3	4	5	6	7
3) I would choose a password with a combination of numbers, letters, and symbols as suggested by the system	1	2	3	4	5	6	7
4) I would choose a password that is difficult to guess	1	2	3	4	5	6	7
5) I would choose a password that follows all the guidelines provided by the system	1	2	3	4	5	6	7
6) I would choose a password that is different from my old password	1	2	3	4	5	6	7
7) I would choose a password that is different from my other online passwords	1	2	3	4	5	6	7

*****Page Break Here**

Summary of Findings (Download)

Please click here to download the summary of the previous study's findings.

Click the next button below to be redirected back to MyView.

*****Page Break Here**

Thank You!

Thank you once again for participating in this follow-up study. Your response is very important to us.

You will be redirected to MyView in a few seconds.

If you have any questions, comments or concerns about this questionnaire or our research, please feel free to contact either myself, Florence Mwagwabi (F.Mwagwabi@murdoch.edu.au) or my research supervisors, Dr Mike Dixon (M.Dixon@murdoch.edu.au) and Associate Professor Dr. Tanya McGill (T.McGill@murdoch.edu.au).

Appendix G Summary of demographic and computer background of respondents

Table G.1: Summary of demographic and computer background of respondents

	Control group		Treatment group	
	n	*%*	*n*	*%*
Gender				
Male	89	43.2%	85	41.1%
Female	117	56.8%	122	58.9%
Age				
18 - 24	27	13.0%	29	13.9%
25 - 34	41	19.6%	39	18.7%
35 - 44	37	17.7%	40	19.1%
45 - 54	48	23.0%	46	22.0%
55 - 64	35	16.7%	36	17.2%
65 and over	21	10.0%	19	9.1%
Number of online email accounts				
3 or less	168	81.6%	178	86.0%
4 to 6	33	16.0%	25	12.1%
4 or more	5	2.4%	4	1.9%
Password management practices				
Longest password ever voluntarily used				
6 characters or less	10	4.8%	3	1.4%
7 to 10 characters	122	58.4%	141	67.1%
11 characters or more	77	36.8%	66	31.5%
Have change passwords voluntarily	141	68.4%	146	71.2%
Have shared passwords	32	15.7%	42	20.1%
Self-reported computer skills				
Below average	18	8.6%	13	6.2%
Average	51	24.4%	44	21.0%
Above average	140	67.0%	153	72.8%
Self-reported computer security knowledge				
Below average	32	15.3%	26	12.4%
Average	69	33.0%	76	36.2%
Above average	108	51.7%	108	51.4%
Level of education				
Less than high school	4	1.9%	2	1.0%
High school or equivalent	43	20.8%	43	20.7%
Some college, no degree	74	35.7%	68	32.7%
Bachelor's degree	61	29.5%	65	31.2%
Post-graduate	25	12.1%	30	14.4%

Appendix H Analysis of measurement model

This section is organized around each measurement model, as follows:

1. Modification Indices (covariances)
2. Standardized Residuals (covariances)
3. Squared Multiple Correlations
4. Measurement model for each group, showing items that were allowed to covary and the corresponding correlations.

H.1 Threat perceptions model

Table H.2: Threat perceptions model – Modification indices

Modification Indices			Control
ePSEV1	<>	ePSEV6	12.176
ePSEV1	<>	ePSEV5	8.461
ePSEV1	<>	ePTHR2	6.828
ePSEV2	<>	**ePSEV1**	**93.892**
ePSEV2	<>	ePSEV5	36.287
ePSEV2	<>	ePTHR2	17.891
ePSEV2	<>	ePTHR5	5.830
ePSEV2	<>	ePTHR1	5.736
ePSEV4	<>	ePTHR1	10.470
ePSEV4	<>	ePTHR2	7.634
ePSEV4	<>	ePTHR4	7.202
ePSEV4	<>	ePSEV3	7.019
ePSEV4	<>	ePTHR5	5.157
ePSEV4	<>	ePSEV1	4.332
ePSEV5	<>	ePSEV6	30.471
ePSEV5	<>	ePTHR1	11.104
ePSEV5	<>	ePTHR6	7.415
ePTHR2	<>	**ePTHR1**	**70.282**
ePTHR2	<>	ePTHR5	9.953
ePTHR2	<>	ePTHR6	7.885
ePTHR4	<>	ePTHR1	7.337
ePTHR5	<>	ePTHR6	16.397
ePVUL1	<>	ePSEV2	5.155
ePVUL1	<>	ePTHR1	4.524
ePVUL2	<>	ePSEV2	8.684
ePVUL2	<>	ePSEV4	4.977
ePVUL3	<>	ePSEV4	9.271
ePVUL4	<>	ePSEV5	10.151
ePVUL4	<>	ePTHR6	7.508
ePVUL4	<>	ePTHR1	5.962

Modification Indices			Treatment
ePSEV1	<>	ePSEV5	20.100
ePSEV1	<>	ePSEV6	13.055
ePSEV1	<>	ePTHR1	5.330
ePSEV2	<>	**ePSEV1**	**97.987**
ePSEV2	<>	ePSEV5	24.132
ePSEV2	<>	ePSEV6	10.071
ePSEV3	<>	ePSEV2	38.729
ePSEV3	<>	ePSEV1	25.642
ePSEV3	<>	ePSEV5	24.364
ePSEV3	<>	ePTHR4	6.559
ePSEV4	<>	ePSEV5	19.756
ePSEV4	<>	ePSEV3	11.231
ePSEV4	<>	ePSEV2	10.045
ePSEV4	<>	ePTHR4	9.081
ePSEV4	<>	ePSEV1	6.159
ePSEV4	<>	ePTHR6	4.337
ePSEV5	<>	ePSEV6	25.739
ePSEV5	<>	ePTHR4	6.052
ePTHR1	<>	ePTHR6	12.064
ePTHR1	<>	ePTHR5	4.514
ePTHR2	<>	**ePTHR1**	**41.229**
ePTHR2	<>	ePTHR5	14.282
ePTHR2	<>	ePTHR6	5.745
ePTHR4	<>	ePTHR1	6.228
ePTHR5	<>	ePTHR6	20.288
ePVUL2	<>	ePSEV6	5.629
ePVUL3	<>	ePSEV5	8.157
ePVUL4	<>	ePSEV4	7.548
ePVUL4	<>	ePTHR6	6.726
ePVUL4	<>	ePTHR2	5.085

Table H.3: Threat perceptions model – Standardized residuals

	PTHR06	PTHR05	PTHR01	PTHR02	PTHR03	PTHR04	PSEV06	PSEV05	PSEV01	PSEV02	PSEV03	PSEV04	PVUL01	PVUL02	PVUL03	PVUL04
Control																
PTHR06	0.000															
PTHR05	0.331	0.000														
PTHR01	-0.208	-0.207	0.000													
PTHR02	-0.226	-0.246	0.994	0.000												
PTHR03	0.021	-0.083	-0.131	0.042	0.000											
PTHR04	-0.037	0.092	-0.271	-0.043	0.071	0.000										
PSEV06	0.228	0.558	-0.124	-0.047	-0.221	-0.173	0.000									
PSEV05	0.149	0.396	-1.295	-0.596	-0.444	-0.540	0.624	0.000								
PSEV01	0.164	0.625	0.277	0.681	0.133	0.209	-0.386	-0.548	0.000							
PSEV02	0.067	0.548	0.463	0.843	0.154	0.206	-0.114	-0.978	1.539	0.000						
PSEV03	-0.299	0.317	-0.499	-0.553	-0.369	-0.789	0.007	0.032	-0.229	-0.252	0.000					
PSEV04	-0.075	0.674	-0.956	-0.417	-0.264	0.027	-0.050	0.269	-0.321	-0.130	0.436	0.000				
PVUL01	0.002	0.126	0.790	0.375	-0.187	-0.149	-0.256	-0.585	0.318	0.694	-0.475	-0.387	0.000			
PVUL02	0.061	-0.371	-0.444	-0.355	-0.244	-0.336	0.111	0.278	-0.340	-0.356	-0.742	0.020	-0.078	0.000		
PVUL03	-0.058	-0.176	-0.180	-0.220	-0.313	-0.281	-0.042	0.185	-0.084	0.124	-1.016	-0.971	-0.008	0.090	0.000	
PVUL04	0.547	1.131	1.899	1.243	0.941	1.222	1.176	0.056	1.550	1.685	0.599	1.103	0.182	-0.086	-0.124	0.000
Treatment																
PTHR06	0.000															
PTHR05	0.722	0.000														
PTHR01	-0.527	-0.300	0.000													
PTHR02	-0.296	-0.435	0.700	0.000												
PTHR03	-0.113	-0.012	0.038	0.050	0.000											
PTHR04	0.321	0.259	-0.288	-0.113	-0.001	0.000										
PSEV06	0.149	0.431	-0.480	-0.527	-0.368	-0.244	0.000									
PSEV05	0.533	0.838	-1.059	-0.319	-0.212	0.270	0.580	0.000								
PSEV01	0.462	0.365	0.093	-0.018	-0.098	-0.706	-0.511	-0.853	0.000							
PSEV02	0.049	0.278	-0.262	0.023	0.023	-0.257	-0.441	-0.919	2.307	0.000						
PSEV03	0.697	0.438	0.507	0.372	0.566	-0.167	-0.184	-1.152	1.473	1.779	0.000					
PSEV04	1.038	0.579	-0.366	0.051	0.056	0.611	0.162	0.602	-0.418	-0.524	-0.692	0.000				
PVUL01	-0.216	-0.288	0.155	-0.034	0.038	-0.307	-0.476	-0.256	0.818	1.050	1.337	0.146	0.000			
PVUL02	0.594	-0.730	-0.411	-0.336	-0.509	-0.498	-1.871	-1.412	0.099	0.020	0.962	-0.720	-0.144	0.000		
PVUL03	0.497	-0.446	0.863	0.029	0.243	-0.300	-0.718	-0.924	0.828	1.010	1.731	0.179	0.022	0.057	0.000	
PVUL04	-0.199	-0.119	0.815	0.830	0.488	-0.231	0.827	1.234	**2.176**	**2.352**	**2.042**	0.593	0.214	0.209	-0.220	0.000

Table H.4: Threat perceptions model – Squared multiple correlations

Squared Multiple Correlations	Control	Treatment
PTHR06	0.872	0.761
PTHR05	0.878	0.787
PTHR01	0.755	0.805
PTHR02	0.881	0.859
PTHR03	0.926	0.894
PTHR04	0.909	0.846
PSEV06	0.880	0.852
PSEV05	0.733	0.773
PSEV01	0.743	0.682
PSEV02	0.796	0.690
PSEV03	0.715	0.565
PSEV04	0.805	0.811
PVUL01	0.622	0.764
PVUL02	0.731	0.748
PVUL03	0.786	0.884
PVUL04	0.532	0.542

Figure H.1: Threat perceptions measurement model (control)

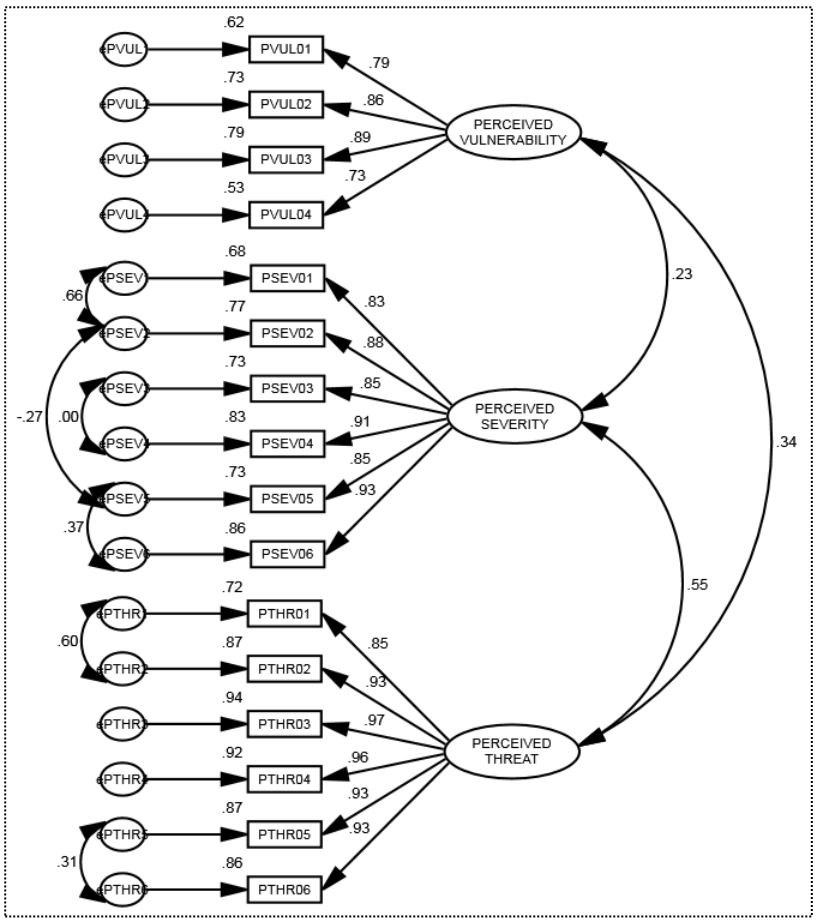
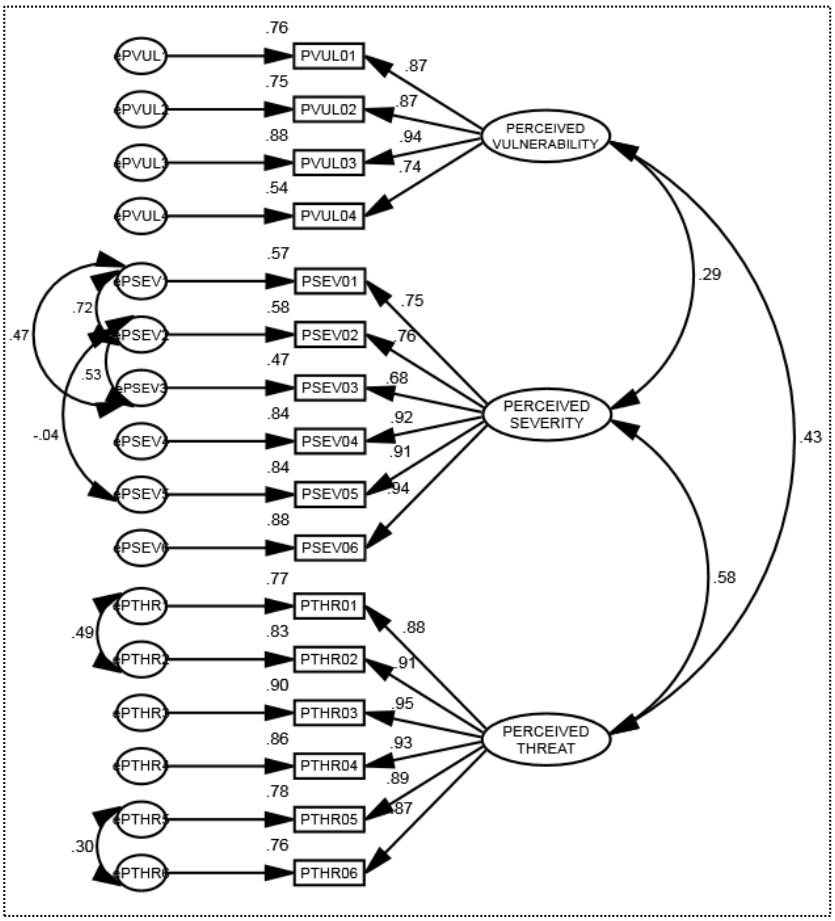


Figure H.2: Threat perceptions measurement model (treatment)



H.2 Efficacy perceptions model

Table H.5: Efficacy perceptions model – Modification indices

Modification Indices			Control
eCOST5	**<>**	**eCOST6**	**95.351**
eCOST1	<>	eCOST5	10.423
eCOST2	<>	eCOST6	20.108
eCOST2	<>	eCOST5	5.757
eCOST2	<>	eCOST1	27.338
eCOST4	<>	eCOST3	21.471
ePEFF5	<>	eCOST6	4.078
ePEFF5	<>	eCOST2	4.382
ePEFF1	<>	ePEFF6	7.971
ePEFF1	<>	ePEFF5	11.234
ePEFF2	<>	ePEFF1	26.326
ePEFF3	<>	ePEFF1	4.917
ePEFF3	<>	ePEFF2	4.827
ePEFF4	<>	ePEFF6	16.893
ePEFF4	<>	ePEFF5	7.525
ePEFF4	<>	ePEFF2	17.355
ePSEF1	<>	eCOST5	6.993
ePSEF2	<>	ePEFF2	5.172
ePSEF2	<>	ePSEF1	8.230
ePSEF3	<>	eCOST4	6.739
ePSEF3	<>	ePEFF6	12.746
ePSEF3	<>	ePEFF5	4.198
ePSEF3	<>	ePEFF1	5.663
ePSEF3	<>	ePSEF1	5.457
ePSEF4	<>	eCOST1	4.294
ePSEF4	<>	eCOST4	5.508
ePSEF4	<>	ePSEF2	7.500
ePSEF4	<>	ePSEF3	28.964

Modification Indices			Treatment
eCOST5	**<>**	**eCOST6**	**114.082**
eCOST1	<>	eCOST6	33.799
eCOST1	<>	eCOST5	10.291
eCOST2	<>	eCOST6	9.231
eCOST2	<>	eCOST5	11.455
eCOST2	**<>**	**eCOST1**	**55.434**
eCOST3	<>	eCOST5	12.613
eCOST4	<>	eCOST5	4.550
eCOST4	<>	eCOST3	33.360
ePEFF6	<>	eCOST6	4.485
ePEFF6	<>	eCOST5	4.735
ePEFF6	<>	eCOST4	5.578
ePEFF1	<>	eCOST1	4.419
ePEFF1	<>	eCOST4	6.811
ePEFF2	<>	ePEFF5	6.226
ePEFF2	<>	ePEFF1	6.749
ePEFF3	<>	eCOST3	14.484
ePEFF3	<>	ePEFF1	4.600
ePEFF3	<>	ePEFF2	4.795
ePEFF4	<>	eCOST3	7.613
ePEFF4	<>	ePEFF5	36.963
ePEFF4	<>	ePEFF1	19.212
ePSEF2	<>	eCOST6	4.537
ePSEF2	<>	ePEFF2	6.316
ePSEF3	<>	eCOST6	4.949
ePSEF3	<>	eCOST1	7.802
ePSEF3	<>	eCOST2	6.588
ePSEF4	<>	ePEFF6	5.882

Table H.6: Efficacy perceptions model – Standardized residual

	COST06	COST05	COST01	COST02	COST03	COST04	PEFF06	PEFF05	PEFF01	PEFF02	PEFF03	PEFF04	PSEF01	PSEF02	PSEF03	PSEF04
Control																
COST06	0.000															
COST05	**2.913**	0.000														
COST01	-0.484	-0.765	0.000													
COST02	-0.940	-0.447	0.878	0.000												
COST03	-0.422	-0.531	-0.282	0.207	0.000											
COST04	-0.487	-0.061	-0.585	-0.256	1.947	0.000										
PEFF06	1.599	1.175	1.114	1.350	1.780	0.887	0.000									
PEFF05	-0.595	0.583	-0.025	1.555	0.888	-0.220	0.505	0.000								
PEFF01	-0.953	-1.016	-0.803	-0.319	-0.806	0.296	-1.135	-1.297	0.000							
PEFF02	-0.790	-0.430	-0.441	0.458	0.343	0.542	-0.530	-0.452	1.875	0.000						
PEFF03	-0.764	-0.776	-0.637	0.529	-0.296	0.058	-0.462	-0.465	0.841	0.768	0.000					
PEFF04	-0.386	-1.507	-0.982	-0.384	-0.816	-1.441	1.526	0.980	-0.460	-1.406	-0.344	0.000				
PSEF01	0.374	0.570	0.265	0.381	-0.207	-0.845	-1.236	0.832	-0.305	-0.953	-1.085	-0.035	0.000			
PSEF02	-0.121	-0.465	0.235	0.055	-0.282	-0.955	-0.674	1.313	-0.147	0.302	-0.795	-0.026	0.360	0.000		
PSEF03	0.199	-0.282	0.615	0.877	0.683	1.227	1.159	1.956	-0.945	-0.119	-1.194	-0.019	-0.526	-0.210	0.000	
PSEF04	-0.763	-1.510	-1.217	-0.580	0.478	0.416	0.623	1.834	0.784	0.071	0.117	1.208	-0.421	-0.484	1.768	0.000
Treatment																
COST06	0.000															
COST05	**2.385**	0.000														
COST01	-1.429	-0.869	0.000													
COST02	-0.535	-0.655	1.585	0.000												
COST03	-0.200	-0.932	0.047	0.155	0.000											
COST04	-0.448	-0.765	0.072	-0.393	2.208	0.000										
PEFF06	1.356	1.639	1.959	1.029	0.081	-1.095	0.000									
PEFF05	-0.498	-0.347	0.750	0.590	-0.531	-0.241	-0.038	0.000								
PEFF01	-0.711	-0.652	1.196	-0.043	-1.411	0.012	0.053	-0.294	0.000							
PEFF02	-1.273	-0.710	0.130	-0.260	-1.352	-1.180	-0.478	-0.611	0.730	0.000						
PEFF03	-0.379	-0.008	0.494	0.226	-2.059	-1.881	0.034	-0.304	0.411	0.411	0.000					
PEFF04	0.308	0.435	0.872	0.740	0.348	-0.957	0.032	1.272	-1.052	-0.175	-0.201	0.000				
PSEF01	-0.039	0.124	0.639	0.234	0.514	-0.802	0.763	-0.224	0.767	0.487	-0.047	-0.064	0.000			
PSEF02	-0.619	-0.214	0.609	0.191	-0.201	-0.413	0.549	-0.232	0.834	0.997	-0.560	-0.158	-0.072	0.000		
PSEF03	0.066	0.148	-0.695	-0.780	0.091	-0.968	0.353	-1.153	0.091	-0.236	-1.110	-0.837	-0.013	0.160	0.000	
PSEF04	0.482	0.612	0.646	0.470	0.275	-0.473	1.768	-0.059	0.675	0.214	0.365	0.384	0.034	-0.212	0.018	0.000

Table H.7: Efficacy perceptions model – Squared multiple correlations

Squared Multiple Correlations	Control	Treatment
COST06	0.568	0.702
COST05	0.638	0.657
COST01	0.690	0.605
COST02	0.778	0.756
COST03	0.590	0.624
COST04	0.375	0.409
PEFF06	0.489	0.688
PEFF05	0.515	0.694
PEFF01	0.499	0.625
PEFF02	0.552	0.636
PEFF03	0.528	0.792
PEFF04	0.551	0.712
PSEF01	0.730	0.715
PSEF02	0.828	0.725
PSEF03	0.610	0.772
PSEF04	0.537	0.655

Figure H.3: Efficacy perceptions measurement model (control)

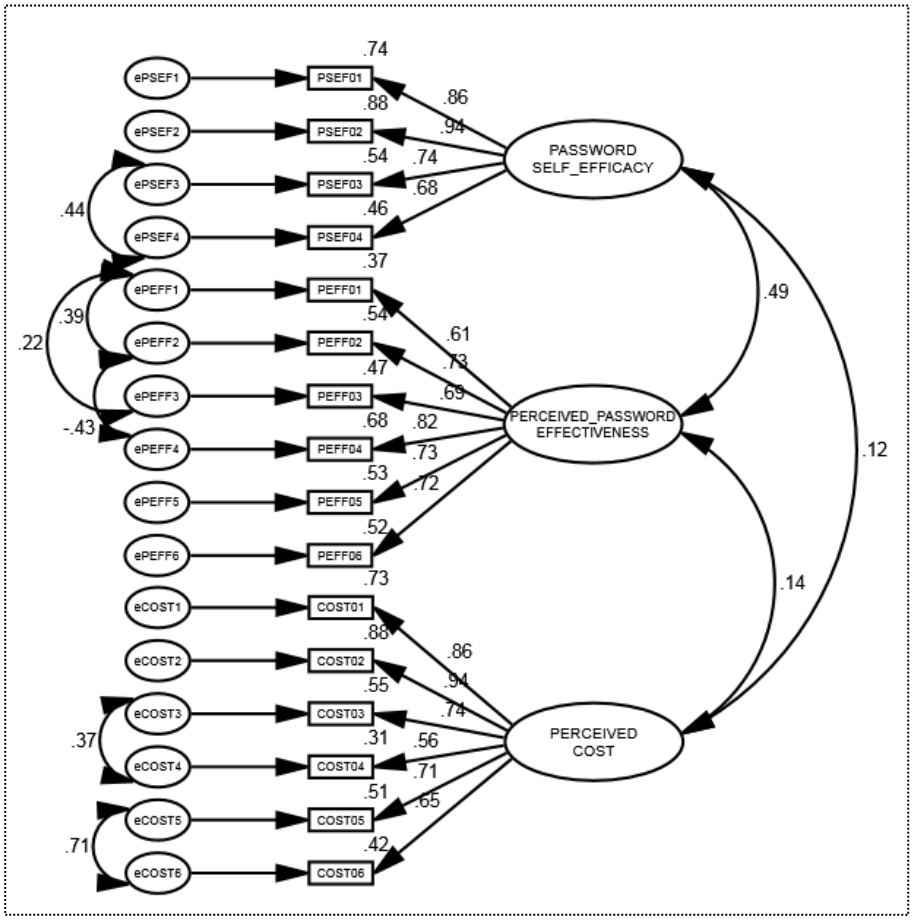
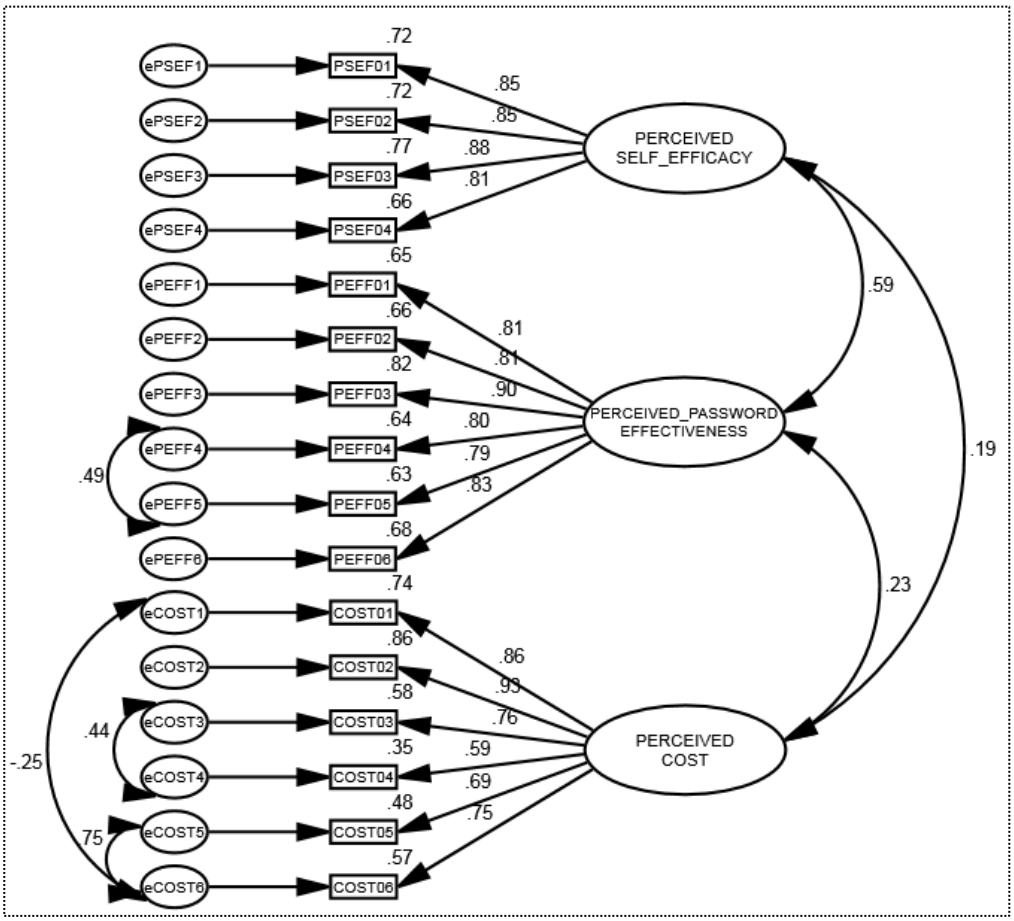


Figure H.4: Efficacy perceptions measurement model (treatment)



H.3 Intention to comply congeneric model

Table H.8: Intentions to comply congeneric model – Modification indices

Covariances: Modification Indices			Control	Treatment
eINT5	**<-->**	**eINT6**	**86.019**	**33.329**
eINT4	<-->	eINT6	7.453	4.661
eINT4	<-->	eINT5	5.127	7.796
eINT3	<-->	eINT5	14.881	4.050
eINT2	<-->	eINT6	4.977	6.269
eINT2	<-->	eINT5	5.477	5.072
eINT1	<-->	eINT6	12.751	10.930
eINT1	<-->	eINT5	21.685	18.362
eINT1	<-->	eINT4	14.123	49.625
eINT1	<-->	eINT3	5.798	9.626
eINT1	<-->	eINT2	11.276	6.851

Table H.9: Intentions to comply congeneric model – Standardized residual

	INTC06	INTC05	INTC04	INTC03	INTC02	INTC01
Control						
INTC06	0					
INTC05	**3.810**	0				
INTC04	-0.703	-0.477	0			
INTC03	0.498	1.136	-0.151	0		
INTC02	-0.664	-0.569	0.139	-0.173	0	
INTC01	-1.379	-1.472	0.744	-0.665	0.767	0
Treatment						
INTC06	0					
INTC05	**1.766**	0				
INTC04	-0.706	-0.704	0			
INTC03	0.781	0.750	-0.410	0		
INTC02	-0.699	0.071	-0.294	0.021	0	
INTC01	-1.091	-1.091	1.915	-1.002	0.675	0

Table H.10: Intentions to comply congeneric model – Squared multiple correlations

Squared Multiple Correlations	Control	Treatment
INTC06	**0.426**	0.509
INTC05	0.570	0.660
INTC04	0.779	0.627
INTC03	0.647	0.523
INTC02	0.731	0.654
INTC01	0.608	0.622

Figure H.5: Intentions to comply congeneric model (control)

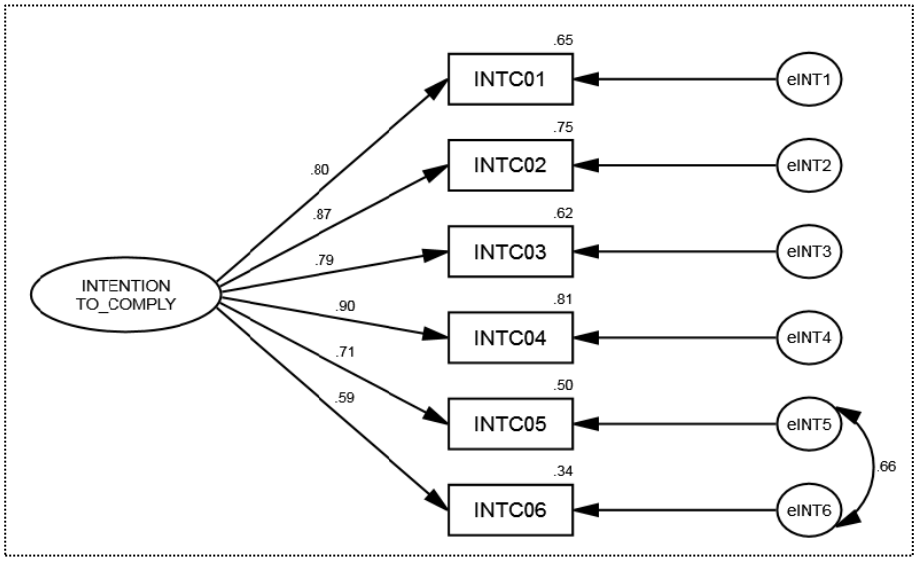
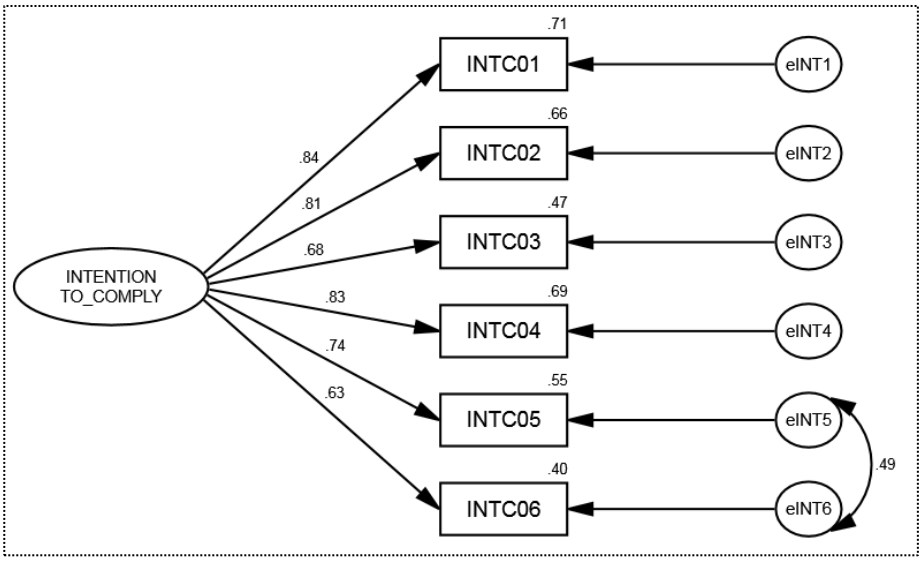


Figure H.6: Intentions to comply congeneric model (treatment)



Appendix I Analysis of structural model

Table I.11: Structural model – Correlations between latent variables (control group)

Latent variable	1	2	3	4	5	6	7	8	9
1. Exposure to hacking	**1.000**								
2. Perceived vulnerability	0.395	**1.000**							
3. Perceived threat	0.171	0.339	**1.000**						
4. Perceived severity	0.237	0.189	0.573	**1.000**					
5. Perceived password effectiveness	0.036	0.123	0.447	0.346	**1.000**				
6. Password self-efficacy	-0.015	0.045	0.303	0.308	0.562	**1.000**			
7. Perceived cost	0.145	0.282	0.264	0.199	0.169	0.136	**1.000**		
8. Intentions to comply	-0.055	0.109	0.426	0.340	0.551	0.665	0.135	**1.000**	
9. Actual password compliance	0.007	0.018	0.106	0.187	0.277	0.246	0.038	0.345	**1.000**

Table I.12: Structural model – Correlations between latent variables (treatment group)

Latent variable	1	2	3	4	5	6	7	8	9
1. Exposure to hacking	**1.000**								
2. Perceived vulnerability	0.308	**1.000**							
3. Perceived threat	0.035	0.436	**1.000**						
4. Perceived severity	0.018	0.289	0.629	**1.000**					
5. Perceived password effectiveness	-0.118	0.193	0.532	0.524	**1.000**				
6. Password self-efficacy	-0.044	0.119	0.442	0.466	0.630	**1.000**			
7. Perceived cost	0.169	0.365	0.256	0.145	0.266	0.209	**1.000**		
8. Intentions to comply	-0.110	0.184	0.471	0.405	0.602	0.769	0.197	**1.000**	
9. Actual password compliance	-0.203	-0.102	0.096	0.170	0.285	0.274	-0.108	0.137	**1.000**

References

Ablon, L, Libicki, MC, & Golay, A. (2014). Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar.

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

Adams, A, & Sasse, M. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40-46.

Adams, A, Sasse, M, & Lunt, P. (1997). Making passwords secure and usable. *People and Computers*, 1-20.

Ajzen, I. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179-211.

Ajzen, I. (2012). Martin Fishbein's Legacy The Reasoned Action Approach. *The Annals of the American Academy of Political and Social Science, 640*(1), 11-27.

Ajzen, I, & Fishbein, M. (1977). Attitude-behavior relations: A theoretical analysis and review of empirical research. *Psychological Bulletin, 84*(5), 888-918.

Ajzen, I, & Fishbein, M. (1980). Understanding attitudes and predicting social behaviour.

Anderson, CL, & Agarwal, R. (2010). Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions. *Mis Quarterly, 34*(3), 613-643.

Anderson, JC, & Gerbing, DW. (1988). Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin, 103*(3), 411-423.

Arbuckle, J. (2010a). AMOS [computer software] (Version 19.0.0). PA, USA: Amos Development Corporation.

Arbuckle, J. (2010b). *IBM SPSS Amos 19 User's Guide*. Chicago: Amos Development Corporation.

Authentic-Response. (2012). Market research survey panels. (December 2012). www.authenticresponse.com

Aytes, K, & Connolly, T. (2004). Computer Security and Risky Computing Practices A Rational Choice Perspective. *Journal of organizational and end user computing, 16*(3), 22-40. doi: 10.4018/joeuc.2004070102

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. *Psychological Review, 84*(2), 191-215.

Bandura, A. (1982). Self-efficacy mechanism in human agency. *American Psychologist, 37*(2), 122-147.

Bandura, A. (1991). Social cognitive theory of self-regulation. *Organizational Behavior and Human Decision Processes, 50*(2), 248-287.

Baron, RM, & Kenny, DA. (1986). The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of personality and social psychology, 51*(6), 1173.

BBC. (2013). Analysis reveals popular Adobe passwords. *BBC New Technology*, (November 5, 2013). http://www.bbc.co.uk/news/technology-24821528

Beckjord, EB, Rutten, LJF, Squiers, L, Arora, NK, Volckmann, L, Moser, RP, & Hesse, BW. (2007). Use of the internet to communicate with health care providers in the United States: estimates from the 2003 and 2005 Health Information National Trends Surveys (HINTS). *Journal of Medical Internet Research, 9*(3).

Bollen, KA. (1990). Overall fit in covariance structure models: Two types of sample size effects. *Psychological Bulletin, 107*(2), 256.

Bonneau, J. (2012). *The science of guessing: Analyzing an anonymized corpus of 70 million passwords*. Paper presented at the IEEE Symposium on Security and Privacy (SP).

Bonneau, J, & Preibusch, S. (2010). *The password thicket: Technical and market failures in human authentication on the web.* Paper presented at the Proceedings of the Ninth Workshop on the Economics of Information Security, Harvard University, USA.

Boomsma, A. (2000). Reporting analyses of covariance structures. *Structural Equation Modeling: A Multidisciplinary Journal, 7*(3), 461-483.

Boomsma, A, & Hoogland, JJ. (2001). The robustness of LISREL modeling revisited. In R. Cudeck, S. du Toit & D. Sörbom (Eds.), *Structural Equation Modeling: Present and Future* (pp. 139-168). Chicago: Scientific Software International.

Boss, SR. (2007). *Control, perceived risk and information security precautions: External and internal motivations for security behavior.* (PhD Thesis), University of Pittsburgh.

Brewer, NT, Chapman, GB, Gibbons, FX, Gerrard, M, McCaul, KD, & Weinstein, ND. (2007). Meta-analysis of the relationship between risk perception and health behavior: the example of vaccination. *Health Psychology, 26*(2), 136.

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

Burr, WE, Dodson, DF, Newton, EM, Pelner, RA, & Polk, WT. (2013). Electronic Authentication Guideline: NIST Special Publication 800-63-2: NIST Special Report 800-63-3.

Burr, WE, Dodson, DF, & Polk, WT. (2006). Electronic Authentication Guideline: NIST Special Publication 800-63: NIST Special Report 800-63.

Byrne, BM. (1989). Testing for the equivalence of factor covariance and mean structures: The issue of partial measurement invariance. *Psychological Bulletin, 105*(3), 456-466.

Byrne, BM. (2008). Testing for multigroup equivalence of a measuring instrument: A walk through the process. *Psicothema, 20*(4), 872-882.

Byrne, BM. (2010). *Structural equation modeling with AMOS: Basic concepts, applications, and programming* (2 ed.): Routledge Academic, NY.

Calin, B. (2009). Statistics from 10,000 leaked Hotmail passwords. http://www.acunetix.com/blog/news/statistics-from-10000-leaked-hotmail-passwords/

Cazier, JA, & Medlin, BD. (2006). Password security: An empirical investigation into e-commerce passwords and their crack times. *Information Security Journal, 15*(6), 45-55.

Charoen, D, Raman, M, & Olfman, L. (2008). Improving end user behaviour in password utilization: An action research initiative. *Systemic Practice and Action Research, 21*(1), 55-72.

Chen, J, Paik, M, & McCabe, K. (2014). *Exploring Internet Security Perceptions and Practices in Urban Ghana.* Paper presented at the Symposium on Usable Privacy and Security (SOUPS).

Choi, N, Kim, D, Goo, J, & Whitmore, A. (2008). Knowing is doing: An empirical validation of the relationship between managerial information security awareness and action. *Information Management & Computer Security, 16*(5), 484-501.

Claar, CL. (2011). *The adoption of computer security: an analysis of home personal computer user behavior using the health belief model.* Utah State University.

Compeau, DR, & Higgins, CA. (1995). Computer self-efficacy: Development of a measure and initial test. *MIS Quarterly, 19*(2), 189-211.

Coursey, D. (2011). 25 "Worst Passwords" of 2011 revealed. *Forbes.com,* (November 21st, 2011). http://www.forbes.com/sites/davidcoursey/2011/11/21/25-worst-passwords-of-2011-revealed/

Cramer, D, & Howitt, D. (2004). *The Sage dictionary of statistics: A practical resource for students in the social sciences*. London: Sage Publications.

Crossler, RE. (2010). *Protection motivation theory: Understanding determinants to backing up personal data.* Paper presented at the System Sciences (HICSS), 2010 43rd Hawaii International Conference on.

Crossler, RE, Johnston, AC, Lowry, PB, Hu, Q, Warkentin, M, & Baskerville, R. (2013). Future directions for behavioral information security research. *computers & security, 32*, 90-101.

Crossler, RE, Long, JH, Loraas, TM, & Trinkle, BS. (2014). Understanding Compliance with BYOD (Bring Your Own Device) Policies Utilizing Protection Motivation Theory: Bridging the Intention-Behavior Gap. *Journal of Information Systems*.

Curran, PJ, West, SG, & Finch, JF. (1996). The robustness of test statistics to nonnormality and specification error in confirmatory factor analysis. *Psychological methods, 1*(1), 16-29.

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

de Nooijer, J, Lechner, L, Candel, M, & de Vries, H. (2004). Short-and long-term effects of tailored information versus general information on determinants and intentions related to early detection of cancer. *Preventive medicine, 38*(6), 694-703.

DeCarlo, LT. (1997). On the meaning and use of kurtosis. *Psychological Methods, 2*(3), 292-307.

Dell'Amico, M, Michiardi, P, & Roudier, Y. (2010). *Password strength: An empirical analysis.* Paper presented at the INFOCOM, 2010 Proceedings IEEE.

Dhamija, R, Tygar, J, & Hearst, M. (2006). *Why phishing works*. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Montréal, Québec, Canada.

Dinev, T, & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. *Journal of the Association for Information Systems, 8*(7), 23.

Egelman, S, Sotirakopoulos, A, Muslukhov, I, Beznosov, K, & Herley, C. (2013). *Does my password go up to eleven? The impact of password meters on password selection.* Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

El Emam, K, Moreau, K, & Jonker, E. (2011). How strong are passwords used to protect personal health information in clinical trials? *Journal of medical Internet research, 13*(1).

Fishbein, M. (2008). A reasoned action approach to health promotion. *Medical Decision Making, 28*(6), 834-844.

Fishbein, M, & Ajzen, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*.

Fishbein, M, & Ajzen, I. (1981). Attitudes and voting behavior: An application of the theory of reasoned action. *Progress in applied social psychology, 1*, 253-313.

Fishbein, M, & Cappella, JN. (2006). The role of theory in developing effective health communications. *Journal of Communication, 56*(s1), S1-S17.

Florêncio, D, & Herley, C. (2007, May 8–12,). *A large-scale study of web password habits.* Paper presented at the Proceedings of the 16th International Conference on World Wide Web, Banff, Alberta, Canada.

Florêncio, D, & Herley, C. (2010). *Where do security policies come from?* Paper presented at the Symposium on Usable Privacy and Security (SOUPS), Microsoft in Redmond, WA.

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

Fornell, C, & Larcker, DF. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of marketing research, 18*(1), 39-50.

Furnell, S. (2007). An assessment of website password practices. *Computers & Security, 26*(7-8), 445-451.

Furnell, S, Bryant, P, & Phippen, A. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security, 26*(5), 410-417.

Gaw, S, & Felten, E. (2006, July 12-14). *Password management strategies for online accounts.* Paper presented at the Proceedings of The Second Symposium On Usable Privacy And Security, Pittsburgh, PA, USA.

Goncharov, M. (2012). Russian Underground 101. *Trend Micro Incorporated.* http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

Goodhue, DL, & Straub, DW. (1991). Security concerns of system users: a study of perceptions of the adequacy of security. *Information & Management, 20*(1), 13-27.

Grawemeyer, B, & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers, 23*(3), 256-267. doi: http://dx.doi.org/10.1016/j.intcom.2011.03.007

Hair, J, Black, W, Babin, B, Anderson, R, & Tatham, R. (2010). *Multivariate data analysis* (7 ed.). Upper Saddle River, NJ: Prentice Hall.

Hampstead, BM, Sathian, K, Phillips, PA, Amaraneni, A, Delaune, WR, & Stringer, AY. (2012). Mnemonic strategy training improves memory for object location associations in both healthy elderly and patients with amnestic mild cognitive impairment: A randomized, single-blind study. *Neuropsychology, 26*(3), 385.

Helkala, K, & Svendsen, NK. (2012). The security and memorability of passwords generated by using an association element and a personal factor *Information Security Technology for Applications* (pp. 114-130): Springer.

Herath, T, Chen, R, Wang, J, Banjara, K, Wilbur, J, & Rao, HR. (2014). Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service. *Information Systems Journal, 24*(1), 61-84.

Herath, T, & Rao, HR. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Herley, C. (2009). *So long, and no thanks for the externalities: The rational rejection of security advice by users.* Paper presented at the Proceedings of the New Security Paradigms Workshop Oxford, United Kingdom.

Hitchings, J. (1995). Deficiencies of the traditional approach to information security and the requirements for a new methodology. *Computers & Security, 14*(5), 377-383.

Hodgkins, S, & Orbell, S. (1998). Can protection motivation theory predict behaviour? A longitudinal test exploring the role of previous behaviour. *Psychology and Health, 13*(2), 237-250.

Hooper, D, Coughlan, J, & Mullen, M. (2008). Structural equation modelling: Guidelines for determining model fit. *Electronic Journal of Business Research Methods, 6*(1), 53-60.

Hovav, A, & D'Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management, 49*(2), 99-110.

Howell, DC. (2012). *Statistical methods for psychology*. Belmont, CA: Wadsworth Publishing Company.

Hu, L, & Bentler, PM. (1998). Fit indices in covariance structure modeling: Sensitivity to underparameterized model misspecification. *Psychological methods, 3*(4), 424.

Hu, L, & Bentler, PM. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal, 6*(1), 1-55.

Hu, Q, West, R, Smarandescu, L, & Yaple, Z. (2014, 6-9 Jan. 2014). *Why Individuals Commit Information Security Violations: Neural Correlates of Decision Processes and Self-Control.* Paper presented at the System Sciences (HICSS), 2014 47th Hawaii International Conference on.

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

Huang, D, Rau, P, & Salvendy, G. (2008). Perception of information security. *Behaviour & Information Technology, 27*(1), 1-12.

Hunt, T. (2012). What do Sony and Yahoo! have in common? Passwords! http://www.troyhunt.com/2012/07/what-do-sony-and-yahoo-have-in-common.html

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83-95.

Inglesant, PG, & Sasse, MA. (2010). *The true cost of unusable password policies: Password use in the wild.* Paper presented at the Proceedings of the 28th International Conference on Human Factors in Computing Systems.

Ives, B, Walsh, K, & Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM, 47*(4), 75-78.

Janis, IL. (1967). Effects of fear arousal on attitude change: Recent developments in theory and experimental research. *Advances in experimental social psychology, 3*, 166-224.

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

Jenkins, JL, Durcikova, A, & Burns, MB. (2012). *Forget the Fluff: Examining How Media Richness Influences the Impact of Information Security Training on Secure Behavior.* Paper presented at the System Science (HICSS), 2012 45th Hawaii International Conference on.

Jenkins, JL, Grimes, M, Proudfoot, JG, & Lowry, PB. (2013). Improving Password Cybersecurity Through Inexpensive and Minimally Invasive Means: Detecting and Deterring Password Reuse Through Keystroke-Dynamics Monitoring and Just-in-Time Fear Appeals. *Information Technology for Development*(ahead-of-print), 1-18.

Jermyn, I, Mayer, A, Monrose, F, Reiter, MK, & Rubin, AD. (1999). *The design and analysis of graphical passwords.* Paper presented at the Proceedings of the 8th USENIX Security Symposium, Washington DC.

Johnston, A, & Warkentin, M. (2010a). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549-566.

Johnston, AC, & Warkentin, M. (2010b). The influence of perceived source credibility on end user attitudes and intentions to comply with recommended IT actions. *Journal of Organizational and End User Computing (JOEUC), 22*(3), 1-21.

Kanich, C, Kreibich, C, Levchenko, K, Enright, B, Voelker, GM, Paxson, V, & Savage, S. (2008). *Spamalytics: An empirical analysis of spam marketing conversion.* Paper presented at the Proceedings of the 15th ACM conference on Computer and communications security.

Karjalainen, M, & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems, 12*(8), 518-555.

Keith, M, Shao, B, & Steinbart, P. (2007). The usability of passphrases for authentication: An empirical field study. *International Journal of Human-Computer Studies, 65*(1), 17-28.

Keith, M, Shao, B, & Steinbart, P. (2009). A Behavioral Analysis of Passphrase Design and Effectiveness. *Journal of the Association for Information Systems, 10*(2), 63-89.

Kline, RB. (2011). *Principles and practice of structural equation modeling* (3 ed.). New York, NY: Guilford press.

Komanduri, S, Shay, R, Kelley, PG, Mazurek, ML, Bauer, L, Christin, N, . . . Egelman, S. (2011). *Of passwords and people: Measuring the effect of password-composition policies*. Paper presented at the Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Vancouver, BC, Canada.

Kuo, C, Romanosky, S, & Cranor, L. (2006). *Human selection of mnemonic phrase-based passwords.* Paper presented at the Symposium on Usable Privacy and Security (SOUPS), Pittsburgh, PA.

LaRose, R, Rifon, NJ, & Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM, 51*(3), 71-76.

LaTour, MS, & Rotfeld, HJ. (1997). There are threats and (maybe) fear-caused arousal: Theory and confusions of appeals to fear and fear arousal itself. *Journal of Advertising, 26*(3), 45-59.

Lee, Y, & Kozar, KA. (2008). An empirical investigation of anti-spyware software adoption: A multitheoretical perspective. *Information & Management, 45*(2), 109-119.

Lee, Y, & Larsen, KR. (2009). Threat or coping appraisal: Determinants of SMB executives decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177-187.

Leventhal, H. (1970). Findings and Theory in the Study of Fear Communications. *Advances in experimental social psychology, 5*, 119-186.

Liang, H, & Xue, Y. (2009). Avoidance of information technology threats: a theoretical perspective. *Management Information Systems Quarterly, 33*(1), 6.

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.

Lorenz, B, Kikkas, K, & Klooster, A. (2013). "The Four Most-Used Passwords Are Love, Sex, Secret, and God": Password Security and Training in Different User Groups *Human Aspects of Information Security, Privacy, and Trust* (pp. 276-283): Springer.

Maddux, JE, & Rogers, RW. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469-479.

Maloney, EK, Lapinski, MK, & Witte, K. (2011). Fear appeals and persuasion: A review and update of the extended parallel process model. *Social and Personality Psychology Compass, 5*(4), 206-219.

Marsh, HW, & Hau, KT. (1999). Confirmatory factor analysis: Strategies for small sample sizes. In R. H. Hoyle (Ed.), *Statistical strategies for small sample size* (pp. 251-306). Thousand Oaks, CA: Sage.

Marsh, HW, Hau, KT, & Wen, Z. (2004). In search of golden rules: Comment on hypothesis-testing approaches to setting cutoff values for fit indexes and dangers in overgeneralizing Hu and Bentler's (1999) findings. *Structural Equation Modeling: A Multidisciplinary Journal, 11*(3), 320-341.

Mathieson, K. (1991). Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. *Information systems research, 2*(3), 173-191.

Mazurek, ML, Komanduri, S, Vidas, T, Bauer, L, Christin, N, Cranor, LF, . . . Ur, B. (2013). *Measuring password guessability for an entire university.* Paper presented at the Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security.

McCrohan, KF, Engel, K, & Harvey, JW. (2010). Influence of Awareness and Training on Cyber Security. *Journal of Internet Commerce, 9*(1), 23-41. doi: 10.1080/15332861.2010.487415

McDowell, M, Rafail, J, & Hernan, S. (2009). Choosing and protecting passwords. *US-CERT Cyber Security Tip ST04-002*. Retrieved from United States Computer Emergency Readiness Team (US-CERT) website: http://www.us-cert.gov/cas/tips/ST04-002.html

Miller, G. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *Psychological Review, 63*(2), 81-97.

Milne, GR, Labrecque, LI, & Cromer, C. (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs, 43*(3), 449-473.

Milne, S, & Milne. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology, 30*(1), 106.

Milne, S, Orbell, S, & Sheeran, P. (2002). Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology, 7*(2), 163-184.

Morris, R, & Thompson, K. (1979). Password security: A case history. *Communications of the ACM, 22*(11), 594-597.

Moyle, E, & Kelley, D. (2012). Federal government cybersecurity survey 2012. *Information Week Reports*, 1-26.

Mulaik, SA, James, LR, Van Alstine, J, Bennett, N, Lind, S, & Stilwell, CD. (1989). Evaluation of goodness-of-fit indices for structural equation models. *Psychological Bulletin, 105*(3), 430.

NCSA-McAfee. (2011). NCSA/McAfee internet home users survey. *National Cyber Security Alliance Studies*, 1-16. http://www.staysafeonline.org/stay-safe-online/resources/

Nelson, DL, & Kim-Phuong, LV. (2009). *Effects of a mnemonic technique on subsequent recall of assigned and self-generated passwords*. Paper presented at the HCI International Symposium on Human Interface, San Diego, CA.

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

Norman, P, Boer, H, & Seydel, ER. (2005). Protection motivation theory.

Oenema, A, Tan, F, & Brug, J. (2005). Short-term efficacy of a web-based computer-tailored nutrition intervention: main effects and mediators. *Annals of Behavioral Medicine, 29*(1), 54-63.

Peace, AG, Galletta, DF, & Thong, JY. (2003). Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems, 20*(1), 153-178.

Peltier, T. (2005). Implementing an information security awareness program. *Information Systems Security, 14*(2), 37-49.

Peters, GJY, Ruiter, RA, & Kok, G. (2014). Threatening communication: A qualitative study of fear appeal effectiveness beliefs among intervention developers, policymakers, politicians, scientists, and advertising professionals. *International Journal of Psychology, 49*(2), 71-79.

Pham, DV, Syed, A, & Halgamuge, MN. (2011). Universal serial bus based software attacks and protection solutions. *Digital Investigation, 7*(3), 172-184.

Plotnikoff, R, & Higginbotham, N. (2002). Protection motivation theory and exercise behaviour change for the prevention of heart disease in a high-risk, Australian representative community sample of adults. *Psychology, health & medicine, 7*(1), 87-98.

Posey, C, Roberts, T, Lowry, PB, Courtney, J, & Bennett, B. (2011). *Motivating the insider to protect organizational information assets: evidence from protection motivation theory and rival explanations.* Paper presented at the The Dewald Roode Workshop in Information Systems Security.

Prentice-Dunn, S, & Rogers, R. (1986). Protection motivation theory and preventive health: Beyond the health belief model. *Health Education Research, 1*(3), 153 - 161.

Puhakainen, P, & Siponen, M. (2010). Improving Employees'compliance Through Information Systems Security Training: An Action Research Study. *Mis Quarterly, 34*(4).

Richardson, R. (2011). CSI computer crime and security survey 2010/2011. *Computer Security Institute, 15*, 1-32.

Rippetoe, PA, & Rogers, RW. (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.

Rogers, R. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91*(1), 93-114.

Rogers, R. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. T. Cacioppo & R. E. Petty (Eds.), *Social Psychophysiology* (pp. 153-176). New York: Guilford Press.

Rogers, RW, & Prentice-Dunn, S. (1997). Protection Motivation Theory. In D. Gochman (Ed.), *Handbook of health behavior research: Determinants of Health Behavior* (Vol. 1, pp. 113 - 132). New York, NY: Springer.

Ronis, DL. (1992). Conditional health threats: Health beliefs, decisions, and behaviors among adults. *Health Psychology, 11*(2), 127.

Rosenstock, IM. (1974). Historical origins of the health belief model. *Health Education Monographs, 2*, 1-8.

Rosenstock, IM, Strecher, VJ, & Becker, MH. (1988). Social learning theory and the health belief model. *Health Education & Behavior, 15*(2), 175-183.

Ryan, RM. (1982). Control and information in the intrapersonal sphere: An extension of cognitive evaluation theory. *Journal of personality and social psychology, 43*(3), 450.

Sasse, M, 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.

Scarfone, K, & Souppaya, M. (2009). Guide to enterprise password management (Draft) *Recommendations of the National Institute of Standards and Technology (NIST)*. Gaithersburg, MD: NIST Special Publication 800-118.

Schafer, JL, & Graham, JW. (2002). Missing data: our view of the state of the art. *Psychological methods, 7*(2), 147.

Schoemaker, PJ. (1982). The expected utility model: Its variants, purposes, evidence and limitations. *Journal of economic literature*, 529-563.

Shannon, CE. (2001). A mathematical theory of communication. *SIGMOBILE Mobile Computing and Communications Review, 5*(1), 3-55.

Sharma, S, Mukherjee, S, Kumar, A, & Dillon, WR. (2005). A simulation study to investigate the use of cutoff values for assessing model fit in covariance structure models. *Journal of Business Research, 58*(7), 935-943.

Shay, R, Kelley, PG, Komanduri, S, Mazurek, ML, Ur, B, Vidas, T, . . . Cranor, LF. (2012). *Correct horse battery staple: Exploring the usability of system-assigned passphrases.* Paper presented at the Proceedings of the Eighth Symposium on Usable Privacy and Security.

Shay, R, Komanduri, S, Kelley, P, Leon, P, Mazurek, ML, Bauer, L, . . . Cranor, LF. (2010). *Encountering stronger password requirements: User attitudes and behaviors.* Paper presented at the Symposium on Usable Privacy and Security (SOUPS), Redmond, WA USA.

Shepherd, M, Mejias, R, & Klein, G. (2014). A Longitudinal Study to Determine Non-technical Deterrence Effects of Severity and Communication of Internet Use Policy for Reducing Employee Internet Abuse (pp. 3159-3168).

Shih, T-H, & Fan, X. (2008). Comparing response rates from web and mail surveys: A meta-analysis. *Field methods, 20*(3), 249-271.

Siponen, M, Mahmood, MA, & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224. doi: http://dx.doi.org/10.1016/j.im.2013.08.006

Siponen, M, Pahnila, S, & Mahmood, MA. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer, 43*(2), 64-71. doi: 10.1109/MC.2010.35

Skogan, W, & Maxfield, M. (1981). *Coping with crime: Individual and neighborhood reactions*. Beverly Hills, CA: Sage Publications.

SPSS. (2010). SPSS Statistics [computer software] (Version 19.0.0): SPSS - IBM.

Stewart, JM, Tittel, E, & Chapple, M. (2008). *CISSP: Certified Information Systems Security Professional Study Guide* (4th ed.). San Francisco, CA: Sybex.

Stone-Gross, B, Cova, M, Cavallaro, L, Gilbert, B, Szydlowski, M, Kemmerer, R, . . . Vigna, G. (2009). *Your botnet is my botnet: analysis of a botnet takeover.* Paper presented at the Proceedings of the 16th ACM conference on Computer and communications security.

Straub, D, & Welke, R. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

SurveyGizmo.com. (2012). SurveyGizmo [Web-based Survey Software] (Version 3.1). Boulder, CO USA Widgix Software, LLC. Retrieved from http://www.surveygizmo.com

Taiabul Haque, SM, Wright, M, & Scielzo, S. (2014). Hierarchy of users′ web passwords: Perceptions, practices and susceptibilities. *International Journal of Human-Computer Studies, 72*(12), 860-874. doi: http://dx.doi.org/10.1016/j.ijhcs.2014.07.007

Tam, L, Glassmana, M, & Vandenwauverb, M. (2009). The psychology of password management: A tradeoff between security and convenience. *Behaviour & Information Technology, 29*(3), 233-244.

Tanaka, JS. (1993). Multifaceted conceptions of fit in structural equation models. In K. A. Bollen & J. S. Long (Eds.), (pp. 10-39). Newbury Park, CA: Sage.

Taneski, V, Heričko, M, & Brumen, B. (2014). Password security–no change in 35 years?

Tipton, HF, & Hernandez, S. (2009). *Official (ISC) 2 Guide to the CISSP CBK*: Auerbach Publications.

Tsai, CS, Lee, CC, & Hwang, MS. (2006). Password authentication schemes: Current status and key issues. *International Journal of Network Security, 3*(2), 101-115.

Ur, B, Kelley, PG, Komanduri, S, Lee, J, Maass, M, Mazurek, M, . . . Bauer, L. (2012). *How does your password measure up? The effect of strength meters on password creation.* Paper presented at the Proceedings of the 21st USENIX Conference on Security Symposium.

Vance, A, Eargle, E, Ouimet, K, & Straub, D. (2013). *Enhancing Password Security through Interactive Fear Appeals: A Web-Based Field Experiment.* Paper presented at the 2013 46th Hawaii International Conference on System Sciences (HICSS), Hawaii.

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.

Verplanken, B, & Orbell, S. (2003). Reflections on Past Behavior: A Self-Report Index of Habit Strength1. *Journal of Applied Social Psychology, 33*(6), 1313-1330.

Vu, K, Proctor, R, Bhargav-Spantzel, A, Tai, B, Cook, J, & Eugene Schultz, E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies, 65*(8), 744-757.

Warkentin, M, Davis, K, & Bekkering, E. (2004). Introducing the Check-off password system (COPS): An advancement in user authentication methods and information security. *Journal of Organizational and End User Computing, 16*(3), 41-58.

Webb, TL. (2006). Does Changing Behavioral Intentions Engender Behavior Change? A Meta-Analysis of the Experimental Evidence. *Psychological bulletin, 132*(2), 249-268. doi: 10.1037/0033-2909.132.2.249

Weber, JE, Guster, D, Safonov, P, & Schmidt, MB. (2008). Weak password security: An empirical study. *Information Security Journal, 17*(1), 45-54.

Weinstein, N. (1984). Why it won't happen to me: Perceptions of risk factors and susceptibility. *Health Psychology, 3*(5), 431 - 457.

Weinstein, N. (1989). Effects of personal experience on self-protective behavior. *Psychological Bulletin, 105*(1), 31-50.

Weinstein, N. (2000). Perceived probability, perceived severity, and health-protective behavior. *Health Psychology, 19*(1), 65-74.

Weinstein, ND. (1993). Testing four competing theories of health-protective behavior. *Health psychology, 12*(4), 324.

Weir, M, Aggarwal, S, Collins, M, & Stern, H. (2010). *Testing metrics for password creation policies by attacking large sets of revealed passwords.* Paper presented at the Proceedings of the 17th ACM conference on Computer and communications security.

Winkler, I. (2009). Winkler: The Real Problems With Cloud Computing. *csoonline.com*. http://www.csoonline.com/article/2124281/cloud-security/winkler--the-real-problems-with-cloud-computing.html

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs, 59*(4), 329-349.

Witte, K. (1994). Fear control and danger control: A test of the extended parallel process model (EPPM). *Communications Monographs, 61*(2), 113-134.

Woon, I, Tan, G, & Low, R. (2005). *A protection motivation theory approach to home wireless security.* Paper presented at the Proceedings of the Twenty-Sixth International Conference on Information Systems, Las Vegas.

Workman, M, Bommer, WH, & 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.

Wurtele, SK, & Maddux, JE. (1987). Relative contributions of protection motivation theory components in predicting exercise intentions and behavior. *Health Psychology, 6*(5), 453.

Yan, J, Blackwell, A, Anderson, R, & Grant, A. (2004). Password memorability and security: Empirical results. *IEEE Security & Privacy, 2*(5), 25-31.

Zhang, J, Luo, X, Akkaladevi, S, & Ziegelmayer, J. (2009). Improving multiple-password recall: an empirical study. *European Journal of Information Systems, 18*(2), 165-176.

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

Zhang, L, & McDowell, WC. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce, 8*(3), 180-197.

Zhang, Y, Monrose, F, & Reiter, MK. (2010). *The security of modern password expiration: An algorithmic framework and empirical analysis.* Paper presented at the Proceedings of the 17th ACM conference on Computer and communications security.

Zviran, M, & Haga, W. (1993). A comparison of password techniques for multilevel authentication mechanisms. *The Computer Journal, 36*(3), 227 - 237.

Zviran, M, & Haga, W. (1999). Password security: An empirical study. *Journal of Management Information Systems, 15*(4), 161 - 185.