Communications of the Association for Information Systems

Volume 42 Article 7

2-2018

Short-term and Long-term Effects of Fear Appeals in Improving Compliance with Password Guidelines

Florence Mwagwabi
Murdoch University, F.Mwagwabi@murdoch.edu.au

Tanya McGill
Murdoch University

Mike Dixon
Murdoch University

Recommended Citation

Mwagwabi, Florence; McGill, Tanya; and Dixon, Mike (2018) "Short-term and Long-term Effects of Fear Appeals in Improving Compliance with Password Guidelines," *Communications of the Association for Information Systems*: Vol. 42 , Article 7.
DOI: 10.17705/1CAIS.04207
Available at: http://aisel.aisnet.org/cais/vol42/iss1/7

Communications of the Association for Information Systems

Research Paper DOI: 10.17705/1CAIS.04207 ISSN: 1529-3181

Short-term and Long-term Effects of Fear Appeals in Improving Compliance with Password Guidelines

Florence Mwagwabi
Murdoch University
Singapore
f.mwagwabi@murdoch.edu.au

Tanya McGill
Murdoch University
School of Engineering and Information Technology
Australia

Mike Dixon
Murdoch University
School of Engineering and Information Technology
Australia

Abstract:

Passwords are the most widely used method of authentication on the Internet, but users find compliance with password guidelines difficult, and we know little about the long-term effects of attempts to improve compliance. In this paper, we extend the work of fear appeals use in the IS security domain to investigate their longer-term effects. We conducted a longitudinal experimental study to examine fear appeals' long- and short-term effects. Using a model based on protection motivation theory (Rogers, 1983), we found that fear of threat, perceived password effectiveness, and password self-efficacy predicted compliance. We also found that neither perceived vulnerability to a security attack nor perceived severity of an attack influenced compliance. Providing persuasive communication improved compliance with password guidelines and resulted in significantly stronger passwords, but the effects on compliance intentions were only short term. This study extends our understanding of the factors that influence compliance with password guidelines and how we can modify them to improve compliance. We raise interesting questions about the role of fear in different IS security contexts. We also highlight the need for more research on the long-term impact of persuasive communication.

Keywords: Fear Appeals, Protection Motivation Theory, Compliance Intentions, Actual Compliance, Password Security, Longitudinal Study.

This manuscript underwent peer review. It was received 02/16/2016 and was with the authors for 18 months for 3 revisions. Idranil Bose served as Associate Editor.

1 Introduction

Information systems (IS) security threats pose a serious ongoing risk to information assets for both organizations and personal users. Recent research has focused on the potential value of fear appeals in improving security practices. A form of persuasive messages, fear appeals are designed to warn users of potential threats and to motivate them to take action to avoid IS security threats. To contribute to better security practices, we extend the work done in recent studies that have explored the value of fear appeals use in the IS security domain (e.g., Jenkins, Grimes, Proudfoot, & Lowry, 2013; Johnston & Warkentin, 2010; Johnston, Warkentin, & Siponen, 2015; Posey, Roberts, & Lowry, 2015; Vance, Eargle, Ouimet, & Straub, 2013). In particular, we examine personal IS security and focus on how one can improve compliance with password guidelines on the Internet via using fear appeals not just in the short term but also in the longer term.

IS security research has primarily focused on fear appeals' immediate effects (e.g., Jenkins et al., 2013; Johnston & Warkentin, 2010; Johnston et al., 2015; Posey et al., 2015; Vance et al., 2013). Recent research suggests that fear appeals that include explicit messages administered repeatedly are more efficacious in improving security behaviors than less explicit messages administered once (Boss, Galletta, Lowry, Moody, & Polak, 2015). Research does not understand the extent to which the effects of fear appeals persist in the long term, which we address in this paper. Given the constraints associated with providing ongoing IS security training and support (Rudis et al., 2016)—indeed, a large proportion of organizations provide security training just once a year (Quagliata, 2011)—we need more research to examine the longevity of fear-appeal campaigns. We address this gap by examining the efficacy of fear appeals in both the short and the long term and when administered once. To do so, we investigate factors that drive Internet users to comply with password guidelines and investigate if fear appeals can engender positive compliance and improve password strength. We explore both the short-term effects of fear appeals and the extent to which the effects of fear appeal messages persist in the long term.

In our study, we focus on a security threat that affects users on a personal level and with large potential consequences to organizations: poor password practices associated with Internet users' lack of motivation to comply with password guidelines. A notable case where someone hacked into a personal email account that belonged to a Twitter employee and gained access to information that enabled the hacker to gain access to a Twitter corporate account (Winkler, 2009) demonstrates the extent to which the impact of poor password practices can extend beyond personal harm. While we focus on compliance with password guidelines on an individual level, our study also has implications for organizations given that organizations are also likely to bear the consequences of security attacks on individual users (Furnell, Bryant, & Phippen, 2007; Jenkins et al., 2013; Winkler, 2009). We make recommendations both about designing training based on fear appeals and on the need for it to be accessible and ongoing.

This paper proceeds as follows. In Section 2, we review relevant literature. In Section 3, we present our research model and hypotheses. In Section 4, we then describe our research methodology. In Section 5, we present our results. In Section 6, we discuss the results and implications for research and practice and our study's limitations. Finally, in Section 7, we conclude the paper.

2 Research Motivation and Literature Review

Historically, IS security research has focused on technological solutions, researchers, and organizations but then began viewing users as the weakest link (Adams & Sasse, 1999), which resulted in a shift from technology to social-behavioral research. Some authors, however, have argued that users are not entirely to blame but that a lack of guidance in the form of support or training contributes to the poor security practices (Adams & Sasse, 1999; Winkler, 2009). We take this position with the premise that guiding users through training can motivate them to engage in recommended security measures.

2.1 User Password Behavior

Despite the challenges associated with their use, usernames and passwords have been widely used to authenticate users for many decades (Bonneau, 2012; Taneski, Heričko, & Brumen, 2014) and are still the preferred method of user authentication due to their low implementation costs (Herley & Van Oorschot, 2012). Users, however, view passwords as inconvenient and mostly difficult to remember (Inglesant & Sasse, 2010; Ur et al., 2012), which leads to their continued use of weak passwords (Florêncio & Herley, 2010; Inglesant & Sasse, 2010).

Notable password leaks (e.g., BBC, 2013; Coursey, 2011) illustrate how widespread weak passwords are across the Internet: the use of weak passwords such as “123456” and “password” is commonplace. Users tend to use weak passwords even when protecting medical files (El Emam, Moreau, & Jonker, 2011) or financial accounts (Florêncio & Herley, 2007). Further, due to the number of passwords users must recall, they resort to reusing passwords across multiple websites, which makes it easier for an attacker to leverage the weakness of one password to access another (Das, Bonneau, Caesar, Borisov, & Wang, 2014). Understanding user compliance on the Internet is particularly important because the economic value of online usernames and passwords surpass stolen credit card information (Ablon, Libicki, & Golay, 2014). Risky security practices on personal online accounts have potentially serious implications for both individuals and to their organizations (Jenkins et al., 2013; Winkler, 2009).

To improve password strength, Taneski et al. (2014) suggest guiding users towards compliance. Yet, as a standalone control measure, password guidelines have little impact on password strength (Florêncio & Herley, 2010; Ur et al., 2012). Even when a visual guide, such as a password strength meter, accompanies them, users’ propensity for choosing weak passwords is still evident (Ur et al., 2012; Vance et al., 2013).

A key problem with extant password guidelines is that they differ from website to website. Users struggle to cope with the variants of password guidelines, which affects their attitude towards passwords and, inevitably, password quality (Bonneau & Preibusch, 2010). Further, users must maintain multiple strong passwords (Bonneau, 2012; Helkala & Svendsen, 2012), which makes recalling passwords one of the most challenging aspects of password usage (NCSA & McAfee, 2011; Zviran & Haga, 1999). This challenge leads to a lack of motivation in users to apply password guidelines (Adams & Sasse, 1999; Bonneau & Preibusch, 2010; Das et al., 2014). Inconsistent password guidelines not only undermine the usability of online services but also force users to resort to risky security behaviors such as writing down their passwords (Das et al., 2014). Studies have linked a lack of protection motivation to how users perceive security threats, such as their assessment of the impact of threats (Liang & Xue, 2010; Woon, Tan, & Low, 2005) and how they perceive the value of implementing security measures (Lee & Larsen, 2009; Zhang & McDowell, 2009).

Studies have shown that one can enhance these perceptions using fear appeals or persuasive messages to improve compliance with security policies (Boss et al., 2015; Johnston & Warkentin, 2010; Johnston et al., 2015; Posey et al., 2015) and to improve password quality (Jenkins et al., 2013; Vance et al., 2013), but we know little about whether this compliance persists over time. In this study, we investigate how altering perceptions about passwords and security threats using fear appeals affects compliance with password guidelines not just in the short term but also in the longer term. Because observing behavioral change is central to our study, we use protection motivation theory (PMT) (Rogers, 1983). Researchers typically use PMT to predict protective behaviors from a threat perspective and also experimentally verify behavioral change (Weinstein, 1993).

2.2 Theoretical Background

Prior to selecting a theoretical framework for this study, we considered three closely related theories: the health belief model (HBM) (Rosenstock, 1974), the theory of reasoned action (TRA) (Fishbein & Ajzen, 1975) and PMT (Rogers, 1975, 1983), all of which researchers have used to explain protective behaviors from a threat perspective. Researchers have used HBM to explain IS security behavior (e.g., Claar, 2011; Ng, Kankanhalli, & Xu, 2009); however, because they have typically used HBM to explain relationships between variables but not to elicit behavioral change (Floyd, Prentice-Dunn, & Rogers, 2000), we did not consider the model ideal for this study. We also considered TRA not suitable for this study since the framework does not adequately describe how to model fear appeals to target specific beliefs (Fishbein & Cappella, 2006). We considered PMT not under the assumption that it is the best protective behavioral theory available but because it is a useful tool for examining behavioral change (Weinstein, 1993) through fear appeals (Rogers, 1975, 1983).

PMT suggests that two independent processes predict protective behavior: threat appraisal and coping appraisal. Threat appraisal refers to an individual’s appraising a threat’s noxiousness and the likelihood it will occur after the individual interacts with a fear appeal. This appraisal leads to perceptions about the threat’s consequences (perceived severity) and the likelihood that it will occur (perceived vulnerability) (Prentice-Dunn & Rogers, 1986). Rogers (1983) proposed that an intervening variable, fear (which he described as an emotional feeling toward threat), further mediates the impact of perceived severity and perceived vulnerability on behavioral intentions. PMT suggests that fear can produce change in behavioral intention (Maddux & Rogers, 1983; Rogers & Prentice-Dunn, 1997).

Coping appraisal refers to an individual's appraising the recommended response's efficacy, the individual's ability to perform the response, and the effort associated with undertaking it. In turn, this appraisal informs people's perceptions about the effectiveness of the recommended measures (response efficacy) and their belief in their ability to perform them (self-efficacy). Self-efficacy is important in the context of IS security behavior because individuals' motivation to perform behaviors and their subsequent actual behaviors are based more on what they believe than on objective external information; hence, self-efficacy beliefs guide behavior (Bandura, 1977). Individuals develop self-efficacy through vicarious experiences such as finding out how others perform the activity and/or by actually performing the activity (Bandura, 1977, 1982). PMT did not originally include self-efficacy; however, consistent with Bandura (1982), Maddux and Rogers (1983) explored the possibility of extending PMT to incorporate self-efficacy. They found self-efficacy had a significant influence on behavioral intentions and suggested using persuasive communications that include instructions on how to execute a recommended action can play a significant role in changing behavior by influencing self-efficacy. Rogers (1983) consequently added self-efficacy to PMT along with additional constructs that relate to perceived rewards and costs associated with the recommended response to produce a more comprehensive model (Rogers, 1983).

While response efficacy and self-efficacy increase behavioral intentions, response cost decreases the likelihood of carrying out the recommended response. Response cost relates to beliefs about the difficulty or effort involved in implementing the recommended response. Rogers (1983) incorporated rewards into PMT as part of coping appraisal to account for beliefs about the benefits of ignoring the recommended behavior, yet fewer studies have explored its role than have investigated other PMT variables. Abraham, Sheeran, Abrams, and Spears (1994) suggested that one could operationalize rewards and response cost as a single variable; for example, that one morph rewards measure into response cost by rewording "increased pleasure" to "reduced benefit" (response cost). Given the possible similarity between the two variables, we did not consider the role of rewards in this study.

Originally intended to explain health-related behavioral changes (e.g., Rippetoe & Rogers, 1987), researchers have increasingly begun to apply fear appeals in IS security research to help understand what motivates users to comply with IS security recommendations (e.g., Boss et al., 2015; Jenkins et al., 2013; Johnston & Warkentin, 2010). PMT also suggests how we can effectively design fear appeals by suggesting what beliefs we can target. Fear appeals can have a positive influence on behavior through altering how individuals perceive threats and altering their perceived recommended behavior. One can also use fear appeals can also influence people's beliefs about their capability to successfully execute a recommended behavior (Bandura, 1982).

2.3 Compliance through Persuasive Communication

In this study, we selected PMT as a model for predicting behavioral change through persuasive communication (Rogers, 1975, 1983; Weinstein, 1993). Early research operationalized fear appeals as a composite construct, which made it difficult to identify which fear appeal component contributed to the observed behavioral change. Consequently, Rogers (1975) developed a comprehensive persuasive communications model and concluded that fear appeals are multidimensional. He identified key independent stimulus variables (magnitude of noxiousness, probability of threat occurrence, and efficacy of available recommended response) that, when distinctively framed in a fear appeals message, help target specific perceptions to effectively engender behavioral change.

PMT suggests that, following a fear appeals intervention, an individual appraises the information about magnitude of noxiousness (severity), probability of occurrence (vulnerability), and response efficacy (effectiveness). A cognitive mediation process follows (Rogers, 1975, 1983) in which individuals develop severity perceptions, vulnerability perceptions, and effectiveness perceptions. When fear appeals incorporate self-efficacy rhetoric, how individuals interpret the fear appeal shapes their self-efficacy perception (Bandura, 1977, 1982). For fear appeals to be effective, one must distinctively frame these four key stimulus variables (i.e., perceived vulnerability, perceived severity, response efficacy, and self-efficacy) in the message (Rogers, 1983).

Applications of fear appeals in IS security research (e.g., Boss et al., 2015; Johnston & Warkentin, 2010; Posey et al., 2015; Posey, Roberts, Lowry, Courtney, & Bennett, 2011) demonstrate how persuasive communication can be mapped into IS security training. For example, Posey et al. (2015) show how PMT-based security education, training, and awareness (SETA) initiatives can help inform users' appraisals of security threats. Security-training efforts can be used to communicate the veracity of threats against information assets (Choi, Kim, Goo, & Whitmore, 2008; Herath & Rao, 2009) and to provide direction for how to appropriately respond to the threats (Puhakainen & Siponen, 2010). For example, knowledge of security technologies can determine whether users pay attention to important security features. Dhamija, Tygar, and Hearst (2006), who analyzed a large dataset on phishing attacks, found that users who lack basic knowledge of browser features are more likely to ignore browser warnings and security indicators, which leads to successful phishing attacks. Empirical evidence also shows that educating users through SETA programs is an effective way to improve their behavior towards organizational information assets (D'Arcy, Hovav, & Galletta, 2009).

IS security studies demonstrate how persuasive messages that target users' beliefs to persuade them to take preventative measures (fear appeals) can motivate them to comply with recommended IS security policies. Studies have shown as much for personal IS security behavior (e.g., Boss et al., 2015; Johnston & Warkentin, 2010; Marett, McNab, & Harris, 2011; Vance et al., 2013) and in organizational settings (Johnston et al., 2015; Posey et al., 2015; Posey et al., 2011). However, IS security training fundamentally differs from other types of training in that it is persuasive in nature (Karjalainen & Siponen, 2011), which introduces additional challenges. For instance, university training is typically descriptive and cognitive: teachers explain concepts without intending to influence learners' behaviors (Karjalainen & Siponen, 2011), while persuasive communication involves influencing an individual's beliefs in an attempt to persuade them to take specific action(s) (Rogers, 1983). Karjalainen and Siponen (2011) argue that, for IS security training to be effective, one needs a sound theory-based understanding of how to design it.

In one of the first applications of fear appeals in IS research, Johnston and Warkentin (2010) examined how fear appeals can influence university students and staff members to implement anti-spyware software. In their study, fear appeals, designed to target key PMT variables, helped enhance security appraisals and, ultimately, influenced intentions to apply anti-spyware controls. Similarly, in examining fear appeals in an organizational environment, Posey et al. (2015) found that, by helping to shape threat and coping appraisals, fear appeals played a significant role in improving employees' motivation to protect their organization's information assets and actual compliance. While these results are promising, the longer-term impact of fear appears on security behavior have more importance, yet we lack longitudinal IS security studies on the topic (Crossler et al., 2013).

In the health domain, we have some evidence that the effects of fear appeal messages can be maintained over time (Floyd et al., 2000; Hodgkins & Orbell, 1998; Wurtele & Maddux, 1987), but, in the IS security domain, we lack longitudinal studies that have investigated the long-term effects of manipulating PMT variables using fear appeals. The few studies that have looked at longer-term impacts of other kinds of IS security interventions suggest that the impacts may not be well sustained. For example, Hagen, Albrechtsen, and Ole Johnsen (2011) investigated the long-term effects of an e-learning tool that focused on improving employees' information security knowledge, awareness, and behavior and found that the effects of use diminished over time. Similarly, Shepherd, Mejias, and Klein (2014), who used persuasive communication but did not manipulate PMT variables, found a long-term effect of providing acceptable use policies to prevent Internet abuse but that it dwindled over time, particularly when the communication used mild messages.

2.4 Applications of PMT in IS Security Research

PMT primarily explains health-related protective behaviors. By drawing similarities between preventative behavior related to health threats and preventative behavior related to computer security threats, IS security researchers have used PMT to investigate a variety of security behaviors in organizational settings (e.g., Crossler, Long, Loraas, & Trinkle, 2014; Herath & Rao, 2009; Ifinedo, 2012; Vance, Siponen, & Pahnila, 2012) and those that relate to personal computer protection (e.g., Anderson & Agarwal, 2010; Crossler, 2010; Johnston & Warkentin, 2010; Liang & Xue, 2010). Table A1 in Appendix A summarizes our review of the applications of PMT in the IS security domain. We summarized IS security-related research; specifically, we indicate which PMT variables we examined and whether these studies applied fear appeals messages. While these studies have contributed greatly to the understanding of what motivates users to protect their personal information assets or those of their organizations, we show that we lack experimental studies and particularly longitudinal designs that examine both the short and long-term effects of fear appeals.

Because the majority of PMT-based IS security studies are correlational studies and do not include fear appeal manipulations, existing research on PMT has failed to capture the theory's core underpinnings (Boss et al., 2015), which focus on behavioral change. While previous studies generally agree that perceived severity, perceived vulnerability, response efficacy, response cost, and self-efficacy play a significant role in security behavior (e.g., Liang & Xue, 2010; Siponen, Mahmood, & Pahnila, 2014; Vance et al., 2012; Woon et al., 2005), we lack consensus on the exact relationship between these factors and behavioral intentions. Additionally, there appear to be two distinct viewpoints. The first considers attitude as a mediating variable (e.g., Anderson & Agarwal, 2010; Herath & Rao, 2009) and suggests that a user's decision to apply security measures depends on their attitude towards the security measure. While Anderson and Agarwal (2010) found support for this proposition, Herath and Rao (2009) did not.

The second and most commonly held viewpoint is that these factors have a direct influence on behavioral intentions. Yet, even with this viewpoint, different studies interpret PMT—particularly the threat appraisal component—differently. For example, Siponen, Pahnila, and Mahmood (2010) model threat appraisal as a single independent variable, Posey et al. (2011) propose that fear is a function of perceived severity and perceived vulnerability, and Zhang and McDowell (2009) suggest that the three variables have independent and direct impacts on intentions. These diverse interpretations of PMT make comparing results across studies a challenging task. As PMT proposes (Rogers, 1983; Rogers & Prentice-Dunn, 1997), in this study, we consider perceived severity and perceived vulnerability as two independent variables.

The exact role of fear in eliciting behavioral change is also unclear. Some early work (e.g., Maddux & Rogers, 1983; Rippetoe & Rogers, 1987) has suggested that fear directly influences behavior. In the IS security domain, research has shown the emotion of fear, operationalized using items relating to security concerns such as fear of being hacked (e.g., Zhang & McDowell, 2009) or fear of losing data from one's computer (Boss et al., 2015), to directly influence users' protection motivation. The findings have, however, been mixed, though they reveal an interesting trend. For example, Zhang and McDowell's (2009) and Boss et al.'s (2015) findings suggest that fear plays a significant role in motivating users to take preventative action. These two studies investigated the impact of fear on personal IS security behavior. However, in organizational settings (e.g., Posey et al., 2015; Posey et al., 2011), fear appears to have no influence on users' motivation to protect their organization's information assets. Note that many PMT applications in IS security research have overlooked the role of fear (Boss et al., 2015; Posey et al., 2015); thus, we do not understand fear's influence as PMT suggests and whether it differs across contexts. In this paper, we examine the role of fear in personal IS security and, thus, contribute to an area with lacking research and to explaining whether fear's role depends on context.

Overall, IS security research have found consistent findings for the role of coping appraisals. However, while some studies have found support for the role of threat appraisal in influencing IS security behavior (e.g., Ifinedo, 2012; Lee & Larsen, 2009; Siponen et al., 2014; Workman, Bommer, & Straub, 2008), others (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 reported inconsistent findings, particularly on the relationship between perceived vulnerability and IS security compliance intentions.

Interestingly, studies that have examined security behavior in the context of personal protection (e.g., Crossler, 2010; Liang & Xue, 2010; Woon et al., 2005; Zhang & McDowell, 2009) have consistently found no support for a direct relationship between perceived vulnerability to threats and intentions. Because we examine compliance in the context of personal protection, our findings should provide more insight into the link between perceived vulnerability and behavioral intentions.

3 Research Model and Hypotheses Development

3.1 Research Model

In this section, we propose a theoretical model that we draw from PMT. Figure 1 presents the model and its associated hypothesized relationships. We also address two additional hypotheses not represented in Figure 1. In our proposed model, we represent the threat appraisal component of PMT as "threat perceptions", which relates to an individual's assessment about the severity of password-related threats (perceived severity), vulnerability to password-related threats (perceived vulnerability), and emotions such as worrying about password-related threats (fear of threat). We represent the coping appraisal component of PMT as "efficacy perceptions", which relates to one's assessment of one's ability to undertake recommended password guidelines (password self-efficacy), one's perceived effectiveness of the password guidelines (perceived password effectiveness), and one's assessment about the difficulty of following the recommended password guidelines (perceived cost).

We define intentions to comply as an individual's willingness to choose a password that follows the guidelines that the system recommends. These guidelines might specify a combination of numbers, letters, and symbols; a password that differs from previously used passwords; or a password that differs from other online passwords.

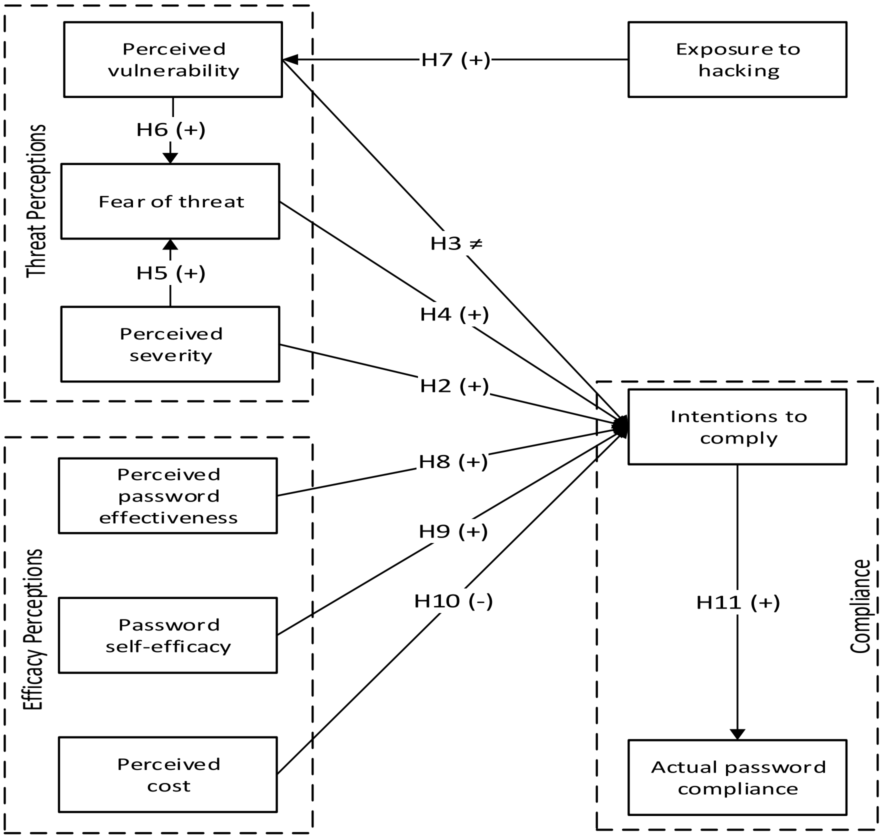


Figure 1. Proposed Research Model

PMT assumes that behavioral intentions predict protective behavior (Rogers & Prentice-Dunn, 1997); thus, its dependent variable is a measure of behavioral intentions. Although the literature in many domains suggests that intentions to perform a task influence actual behaviors, little research has examined the link between intentions and actual compliance with respect to passwords. Therefore, we also include actual password compliance in the research model.

3.2 Fear Appeals

For this study, we define fear appeals as persuasive messages that draw attention to the prevalence and severity of password-related threats and the efficacy of password guidelines in protecting online accounts against threats such as hacking. To improve self-efficacy, one's ability to perform the recommended behavior is crucial; therefore, fear appeals also include instructions on how to execute the recommended course of action (Leventhal, 1970). Thus, in this study, fear appeals include training on how to create strong passwords with a mnemonic strategy for creating memorable passwords.

An antecedent to protection motivation, fear appeals are intended to alter how users perceive threats and change perceptions about the recommended course of action to influence their behavior. Consistent with PMT (Rogers, 1983), after a user encounters information about information security threats (fear appeals), they first appraise the information, and their interpretation of the information then shapes their overall perceptions about the threat. Fear appeals work by increasing threat awareness and the preventative measures available, which, in turn, drives individuals to act.

Earlier IS security research largely overlooked the fear appeal component, which has resulted in mixed findings and the need for a better understanding on how to inspire better security practices (Boss et al., 2015). However, more recently, researchers have successfully used fear appeals to persuade users to adopt a variety of computer security measures (e.g., Boss et al., 2015; Jenkins et al., 2013; Johnston & Warkentin, 2010; Posey et al., 2015; Vance et al., 2013). For example, Jenkins et al. (2013) used fear appeals to inform users about the risks of reusing passwords. In turn, users' threat perceptions (i.e., their appraisal of how vulnerable they are to hacking when reusing passwords across websites) increased significantly, which improved their password choices. Johnston and Warkentin (2010) empirically examined the effectiveness of fear appeals on individuals in a university setting. They observed the effect fear appeals rhetoric had on spyware threats and found that fear appeals significantly improved security perceptions and intentions to apply spyware protection. Other research such as Marett et al. (2011), who examined the effect of fear appeals on social media users, also shows that one can use fear appeals to inspire safer social media security behavior. Fear appeals are also useful in inspiring individuals to protect their organizations' information assets. Posey et al. (2015) show the value of SETA programs as an important tool for disseminating security threat information in the real world. They used fear appeals with employees from various organizations and industries and improved their security behaviors. Thus, we hypothesize:

H1: Fear appeals will increase user compliance with password guidelines.

3.3 Threat Perceptions

We define perceived severity as the extent to which a user believes the consequences of password threats would be detrimental. Research has proposed elevating severity perceptions to increase the likelihood of individuals' complying with recommended measures (Rogers, 1975, 1983), and IS security research has shown perceived severity to contribute to compliance with IS security measures. For example, Woon et al. (2005) found that users were more likely to enable wireless security measures if they believed a breach on their home wireless network would be detrimental, while Lee and Larsen (2009) found perceived severity had a direct impact on executives' intentions to install anti-malware software. This direct link between perceived severity and protection motivation holds true in organizations, where individuals are most likely to comply with security polices if they believe the threats to their organization would be detrimental (Posey et al., 2015; Siponen et al., 2014; Siponen et al., 2010). Thus, it seems likely that users will be more likely to comply with password-security recommendations if they believe that the consequences of being hacked would be severe. Thus, we hypothesize:

H2: Perceived severity of password-related threats is positively related to intentions to comply with password guidelines.

We define perceived vulnerability as the extent to which users believe they are likely to experience password-related threats. PMT suggests a direct association between perceived vulnerability and intentions to carry out recommended precautions. However, in the IS security domain and particularly in the context of personal computer protection, most studies (e.g., Crossler, 2010; Liang & Xue, 2010; Milne, Labrecque, & Cromer, 2009; Woon et al., 2005; Zhang & McDowell, 2009) have failed to provide evidence of a direct link between perceived vulnerability and compliance intentions. For example, Crossler (2010) found that whether users feel vulnerable to losing personal files on their computer had no significant influence on their intentions to back up personal data.

The role of vulnerability perceptions in motivating individuals to take action against threats may in fact be marginal as Milne and Milne (2000) found in their meta-analysis of health-related PMT studies. As for why, Weinstein (1984) notes that, because people inherently believe others are more vulnerable to threats than them, they tend to underestimate their vulnerability to threats. Research has shown as much to be true for individuals' IS security perceptions. For example, in their quest to understand drivers of poor security practices, Sasse, Brostoff, and Weirich (2001) observed that many users misguidedly believe that their information is not important enough to be targeted. As such, it is unsurprising that research has found little evidence of a direct relationship between perceived vulnerability and compliance intentions as it concerns personal IS protection. Thus, it seems likely that, in the context of personal password protection, perceived vulnerability has no direct effect on a user's intentions to comply with password-security guidelines. Thus, we hypothesize:

H3: Perceived vulnerability to password-related threats do not have a direct effect on intentions to comply with password guidelines.

Synonymous with the construct fear (Rogers, 1983), we define fear of threat as the extent to which a user experiences negative arousal, such as concern or worry, about password-related threats. While we lack research on the impact of fear on IS security behaviors (Boss et al., 2015; Johnston et al., 2015), some evidence suggests that increasing vulnerability and severity perceptions would significantly influence users' fear of threats (e.g., Boss et al., 2015; Posey et al., 2015; Posey et al., 2011). Thus, to elevate fear of IS security threats, users must believe that they are vulnerable to threats and that the impact of breaches to information assets would be detrimental. Thus, users' fear of threat level is likely to increase if they believe that they are likely to be hacked and if they believe it would lead to serious consequences. Thus, we hypothesize that:

H4: Perceived vulnerability is positively related to fear of threat.

H5: Perceived severity is positively related to fear of threat.

While we lack research that examines the direct relationship between fear and security behavior, studies such as Zhang and McDowell (2009) have found a positive correlation between fear of password threats and users' intentions to apply password-protection measures. Boss et al. (2015), who used fear appeals manipulations, also found that fear plays a significant role in users' security behavior. This finding suggests that, if users are worried about password-related threats, they are more likely to intend to comply with recommended password guidelines. Note, however, that both these studies examined the role of fear in the context of personal protection. Zhang and McDowell (2009) investigated the role of fear in inspiring users to protect their online password account, while Boss et al. (2015) examined the influence of fear on users' decisions to back up their hard drives. Interestingly, fear does not appear to influence users' decisions to comply with their organizations' security guidelines (Posey et al., 2015; Posey et al., 2011). In this study, we examine the role of fear in users' decisions to comply with password guidelines for their online email accounts. Thus, we hypothesize:

H6: Fear of threat is positively related to intentions to comply with password guidelines.

Because users tend to underestimate their vulnerability to security threats (Sasse et al., 2001; Woon et al., 2005), we need to understand the antecedents of perceived vulnerability. PMT does not explicitly include prior exposure to threat as a predictor of threat perceptions. However, given that PMT-related IS security studies have thus far yielded mixed findings (e.g., Herath & Rao, 2009; Johnston et al., 2015; Lee & Larsen, 2009; Vance et al., 2012), particularly on the relationship between perceived vulnerability and behavioral intentions, we explore other factors that may explain how individuals develop a sense of vulnerability to security threats. In particular, we explore the proposition that, when people or someone they know personally encounters a threat, this exposure to threat informs their vulnerability perceptions (Skogan & Maxfield, 1981; Weinstein, 1984). Consistent with this proposition, in the context of IS security, Boss (2007) found that individuals develop vulnerability perceptions through both personal exposure and knowledge about others' exposure to cybersecurity threats. We define exposure to hacking as prior exposure to a hacking incident that users or someone they know personally experienced and propose that, if users or someone they know personally has their online account hacked, the experience should elevate their perceived vulnerability. Thus, we hypothesize:

H7: Exposure to hacking increases perceived vulnerability.

3.4 Efficacy Perceptions

We define perceived password effectiveness as the extent to which a user believes the recommended password guidelines will prevent password-related threats. PMT proposes that the likelihood of compliance increases when individuals perceive the recommended response as effective (Rogers, 1975, 1983). In the IS security domain, several studies (Boss et al., 2015; Marett et al., 2011; Workman et al., 2008) have found support for the influence of response efficacy on security practices. For example, Workman et al. (2008) found that employees are more likely to comply with IS security policies if they believe the policies are effective, while Johnston and Warkentin (2010) provided empirical evidence of the important role that perceived effectiveness of anti-spyware software plays in users' intentions to implement anti-spyware protection. Marett et al. (2011), who applied PMT to explain social media security behavior, found that individuals who believe that removing sensitive information would help protect them from online threats are more likely to agree not to post sensitive information. It seems likely that, if users believe that recommended password guidelines will prevent password-related threats, they will be more likely to intend to comply with the recommended guidelines. Thus, we hypothesize:

H8: Perceived password effectiveness is positively related to intentions to comply with password guidelines.

We define password self-efficacy as the extent to which users are confident in their ability to create strong passwords. In testing the revised version of PMT, Maddux and Rogers (1983) found self-efficacy to be a key driver of protective behavior. Research has shown self-efficacy to be a predictor of security behaviors in, for example, the context of personal anti-spyware protection (Johnston & Warkentin, 2010), social media use (Marett et al., 2011), and backing up of personal data (Boss et al., 2015). Several empirical studies (e.g., Siponen et al., 2014; Siponen et al., 2010; Workman et al., 2008) also provide evidence of the key role self-efficacy plays in significantly reducing the likelihood of non-compliance. Thus, we believe that users will be more likely to comply with password-security recommendations if they are confident about their ability to create a strong password. Thus, we hypothesize:

H9: Password self-efficacy is positively related to intentions to comply with password guidelines.

PMT (Rogers, 1983) proposes that the likelihood of compliance decreases as the costs associated with the recommended measures increase. Thus, if individuals believe that carrying out the recommended measures would require too much effort, they should be less likely to undertake them. Research has shown perceived cost to have a negative effect on employees' intentions to comply with security policies (Vance et al., 2012), and Woon et al. (2005) found that, when users perceive home wireless security measures as difficult, they are less likely to implement them.

In this study, we define perceived cost as the extent to which a user believes that remembering strong passwords would be difficult. Difficulty in recalling passwords is a key challenge to users and seen as a significant barrier to password security (Inglesant & Sasse, 2010; Ur et al., 2012); therefore, we propose that users will be less likely to comply with password-security measures if they believe it would be difficult to remember strong passwords. Thus, we hypothesize:

H10: Perceived cost is negatively related to intentions to comply with password guidelines.

3.5 Intentions and Actual Compliance with Password Guidelines

We lack password-related research that has examined the link between intentions and actual compliance. Our proposed research model (see Figure 1) extends the PMT model to include a relationship between intentions to comply and actual password compliance in order to reflect the extent to which compliance intentions translate into actual behavior. Studies in other IS security areas provide evidence to support an extension of the PMT to include a link between intentions and actual behavior (e.g., LaRose, Rifon, & Enbody, 2008; Liang & Xue, 2010; Siponen et al., 2014). Thus, we hypothesize:

H11: Intentions to comply is positively related to actual password compliance.

3.6 Effects of Fear Appeals over Time

Applications of PMT-based persuasive communication in IS security research have primarily focused on the immediate effects of fear appeals (e.g., Jenkins et al., 2013; Johnston & Warkentin, 2010; Vance et al., 2013). We lack longitudinal IS security studies even though we need to better understand fear appeals' long-term efficacy (Floyd et al., 2000; Crossler et al., 2013). Shepherd et al. (2014) suggest that persuasive communication can have a long-term effect on security behavior. Although they did not manipulate the PMT variables, their findings draw attention to the importance of longitudinal analysis of the effects of fear appeals in that they demonstrate that providing acceptable use policies to prevent Internet abuse can have a long-term effect but that the effects may dwindle over time.

We could find no published follow-up studies to determine the long-term effects of manipulating all four key PMT variables using fear appeals (see Appendix A). In the IS security domain, Boss et al. (2015) conducted a longitudinal study in which they administered fear appeals three times across several months. While their findings suggest that fear appeals may be effective several months after they are first administered, it is unclear if an overlap in when the researchers administered the fear appeals and measured individuals' security behavior contributed to those findings. It is also unclear whether administering the fear appeals once, which is typically the case in practice (Quagliata, 2011), have a long-term effect. To investigate whether the effects of fear appeals can persist in the long term, we examined the immediate effect of fear appeals administered once and the effects weeks after administration. Further, as the fear appeals Boss et al. (2015) used did not manipulate the coping appraisal component, we examined the short- and long-term effects of manipulating all four key PMT variables. Consistent with the small amount of previous relevant research (Boss et al., 2015; Shepherd et al., 2014), we hypothesize:

> **H12:** Users who receive fear appeals have a higher intention to comply over time than those who do not.

4 Research Methodology

We targeted Internet users with at least one online email account as participants. We used a between-group experimental design in which we exposed one group to fear appeals and another to no such appeals to test the research model and to examine the impact of fear appeals on compliance with password guidelines. We collected data from the two separate groups using two separate questionnaires hosted on SurveyGizmo (version 3.1), one of which contained fear appeal messages. To explore the long-term effects of altering user perceptions, we collected data in two phases separated by six weeks.

4.1 Participants and Data Collection Procedure: Phase I

We sought participants from a wide spectrum of backgrounds including gender, level of education, computer skills, and computer security knowledge. To recruit such participants, we used a third party recruiting company located in the United States (Authentic-Response, 2012) who, using census-balanced random sampling, selected potential participants from the United States. The recruiting company randomly allocated these panel members to either control or treatment group and invited them to participate via email. During this phase, the company sent 3,830 email invitations.

The questionnaire used in phase I had two sections: background information and measures of the constructs in the research model. The treatment group first completed the background section followed by the password-security information and training session. To ensure that they paid attention to the password-security information and to maximize the intervention's impact, they also completed an interactive question-and-answer (Q&A) session. After completing the password-security information and training session, the treatment group completed the second section of the questionnaire. The control group completed both sections of the questionnaire without a break between them. In total, 459 people completed surveys with a valid completion rate of 10.9 percent (control = 209 and treatment = 210).

Because we sought to determine whether the password-security information and training session completed by the treatment group would improve their compliance with password-security guidelines, the survey asked the participants at to create a password they would use to return to the survey-hosting website to complete phase II and to view preliminary results from phase I. We used this password to assess actual password compliance.

4.2 Participants and Data-collection Procedure: Phase II

Six weeks after the participants completed phase I, the recruiting company emailed all control and treatment group participants (419) to invite them to complete a follow-up questionnaire and to view the preliminary results from phase I. Access to the follow-up questionnaire required the passwords created at the end of phase I. In anticipation that some participants would forget their passwords, we also created a generic password and issued it to those who forgot their passwords at the login screen.

The questionnaire included the items we used to measure intentions to comply with password guidelines in phase I. In total, 256 participants completed the follow-up survey of which 194 were valid completions (control = 99 and treatment = 95)—a 46.3 percent valid response rate for the follow-up session.

4.3 Measurement Development

To ensure the measurement items' validity and reliability, we used previously validated items and adapted their wording as necessary to the password domain. Appendix B lists all items, and, below, we describe the derivation of the items for each construct. The constructs in our study are reflective because each captures one dimension of a given construct as opposed to formative constructs that capture more than one dimension and are proposed to cause variance in the construct (Cenfetelli & Bassellier, 2009).

To measure perceived vulnerability and perceived severity, we adapted items from Zhang and McDowell (2009). We used a seven-point Likert scale to measure perceived vulnerability and a seven-point scale from (1) "not at all severe" to (7) "very severe" to measure perceived severity. We measured fear of threat on a seven-point Likert scale using items adapted from Milne, Orbell, and Sheeran (2002). We used items adapted from Boss (2007) to measure exposure to hacking on a scale of (0) if participants answered “no” to being hacked or (1) “low impact” to (7) “high impact”.

We measured perceived password effectiveness on a seven-point Likert scale using items adapted from Zhang and McDowell (2009) to be consistent with password guidelines from the National Institute of Standards and Technology (NIST) (Scarfone & Souppaya, 2009) and the United States Computer Emergency Readiness Team (US-CERT) (McDowell, Rafail, & Hernan, 2009). We adapted the items we used to measure password self-efficacy from the computer self-efficacy items that Compeau and Higgins (1995) developed and measured them on a 10-point scale from (1) “not at all confident” to (10) “totally confident”. We measured perceived cost on a seven-point Likert scale using items adapted from Milne, Orbell, and Sheeran (2002).

We adapted the items for intentions to comply with password guidelines from those that Bulgurcu, Cavusoglu, and Benbasat (2010) developed and measured them on a seven-point scale from (1) “not at all likely” to (7) “very likely”. We used the same items to measure intentions to comply in phases I and II.

The fear appeals we used in this study were in the form of password-security information and training in four approximately equally sized distinct fear appeal narratives. The fear appeal narratives contained information that emphasized the prevalence and potential consequences of password threats, effective ways to prevent password-related threats, and training on how to create strong passwords with a mnemonic strategy for creating memorable passwords. We based the fear appeals on the NIST guide to enterprise password management (Scarfone & Souppaya, 2009), the US-CERT password-security guidelines (McDowell et al., 2009) and the Certified Information Systems Security Professional (CISSP) curriculum (Stewart, Tittel, & Chapple, 2008). The training included an interactive question-and-answer session with questions directly related to the password-security information and an exercise on how to use the mnemonic technique in which one uses the first letter of each word in a sentence or familiar phrase to create a password. Several studies (e.g., Helkala & Svendsen, 2012; Vu et al., 2007; Yan, Blackwell, Anderson, & Grant, 2004) have shown this mnemonic technique to improve individuals’ ability to remember passwords.

In this study, we measured actual password compliance using password strength. Studies that have analyzed password strength have used different approaches such as password-cracking techniques (e.g., Cazier & Medlin, 2006); however, results vary depending on the software used and processor speed. An alternative approach uses a mathematical formula to estimate password unpredictability and character variation—that is, the password’s “entropy”. One advantage of this method is independence from processor speed. Further, as a lack of character variation is a key issue with user-generated passwords (Burr et al., 2013), measuring password strength using a measure of character variation better suited our study.

The password strength guidelines we used build on NIST’s (Burr et al., 2013; Scarfone & Souppaya, 2009) password guidelines. We measured password strength using Shannon’s (2001) formula for calculating entropy as the following example illustrates: a nine-character password selected from a combination of any of the 94 printable standard keyboard characters will have a character width of 94 and entropy of 6.555 bits per character[1]. The total entropy is, therefore, 9*6.555 or 58.995 bits. If one restricts the choice of characters as is the case with repeated characters, the total entropy decreases. The higher the password entropy (bits), the higher the possible values the password could take (2^{bits}) and the longer it would take to guess. To automate the process of calculating password strength, we developed a password analysis-tool coded in Visual Basic.

4.4 Data Analysis Technique

Prior to analyzing the data, we screened it for missing values, outliers, skewness, and kurtosis and performed a normality test. Because less than 2.9 percent of the values were missing and Little’s missing completely at random (MCAR) test yielded a non-significant p-value, we performed data imputation. Skewness and kurtosis were also below the cut-off values. To identify potential multivariate outliers, we used Mahalanobis d-squared values (Byrne, 2010; Hair, Black, Babin, Anderson, & Tatham, 2010)

[1] Entropy per character for a password with a width of 94 = $\mathrm{Log}_2(W) = \mathrm{Log}_2(94) = 6.555$

provided in AMOS version 19. We excluded 13 participants from the analysis as the Mahalanobis d-squared values revealed correlations significantly different from the remaining participants.

We used between-group ANOVA to examine the effects of the fear appeals and two-step structural equation modeling (SEM) using AMOS version 19 to test the model.

To validate the measurement items, we assessed construct validity using two criteria. First, we assessed the discriminant validity of each construct to ensure they were distinct from each other. To show discriminant validity, the square root of the average extracted variance (AVE) for each latent variable should be higher than the correlation between latent variables (Hair et al., 2010). We examined the convergent validity of the measurement items to ensure the factor loadings were high and consistent. To show convergent validity, construct reliability (CR) should be greater 0.7 and also greater than the AVE, and the AVE should be above 0.5 (Hair et al., 2010).

Using the following fit indices and cutoff values, we assessed how well the observed data fit the hypothesized model: χ^2, normed χ^2 (χ^2/df; between 1-2), comparative fit index (CFI) and Tucker-Lewis index (TLI) (>.95), root mean squared error of approximation (RMSEA; < 0.05 or < .08 if CFI is > .95), and standardized root mean residual (SRMR; Minimum <.06 or up to 0.09 if CFI is > .92) (Byrne, 2010; Hair et al., 2010; Hu & Bentler, 1999). We assessed the measurement model for threat appraisal factors, coping appraisal factors, and intentions to comply separately and analyzed the control and treatment data separately. Using regression imputation, we computed a single composite score to measure exposure to hacking.

Because our study includes a multi-group analysis, before testing the structural model, we performed a test for measurement model equivalence to examine whether the measurement model operated equally across the two groups (Hair et al., 2010). We tested model equivalence by comparing the pre-established good fitting model χ^2 (baseline model) with a model in which we constrained all paths to be equal. To show model equivalence, the χ^2 difference should be non-significant (p >.05). We then tested the structural model using the same goodness-of-fit indices we used to assess the measurement model.

5 Data Analysis and Results

5.1 Participant Demographic Characteristics

Of the 419 participants, 57.9 percent were female. Their average age was 43.7, (participants ranged from 18 to 85 years' old). A follow-up chi-squared (χ^2) test of independence showed no significant difference in gender, age, or self-assessed computer security knowledge between the two groups.

5.2 Measurement Validity

For exposure to hacking, we calculated Cronbach's alpha (CA) because we used a single composite score in the structural model testing. The CA value for the treatment group was acceptable at 0.738. The control group value (0.633) was, however, lower than recommended. Since exposure to hacking serves as an exploratory factor in our study, given that PMT does not include it, we considered both values acceptable because they were greater than 0.5, the minimum recommended threshold for exploratory factors. Thus, we considered the construct reliability for exposure to hacking to be satisfactory.

Prior to analyzing the structural model, we tested the measurement models for possible multicollinearity or cross-loading issues and the impact of excluding problematic AVE measurement items. We examined the items for high standardized residuals (SR) values and high correlations between items, which would indicate low item reliability. We also examined the standardized residual covariances to further test for discrepancies between our proposed and observed data. We found no significant discrepancies (greater than 2.58) except for the covariance between items we identify above as problematic. For both the treatment and control models, we dropped items with low reliability as suggested by the high SR and correlations between items. The resulting AVE values indicate the final models had no discriminant or convergent validity issues and that all construct reliability measures were also acceptable.

Further, the square root of the AVE for each variable was higher than the correlations with other variables (see Appendix C), which indicates our model had good discriminant validity. The CR values were all greater than 0.7 and greater than the AVE for each variable. Additionally, all AVE values were greater than 0.5, which suggests our model had no convergent validity issues.

Table 1. Construct Validity and Reliability

Construct reliability measures	Control group			Treatment group		
	CA	CR	AVE	CA	CR	AVE
Exposure to hacking*	0.633	-	-	0.738	-	-
Perceived severity	0.920	0.922	0.745	0.897	0.887	0.667
Perceived vulnerability	0.879	0.882	0.715	0.920	0.922	0.798
Fear of threat	0.976	0.976	0.890	0.961	0.960	0.828
Perceived password effectiveness	0.846	0.846	0.526	0.921	0.918	0.691
Password self-efficacy	0.893	0.885	0.662	0.909	0.910	0.716
Perceived cost	0.876	0.880	0.650	0.886	0.899	0.692
Intentions to comply	0.906	0.900	0.751	0.897	0.879	0.709

* Because we used a composite score to measure exposure to hacking, we did not compute CR and AVE (calculated using standardized factor loadings).

We conducted a model-equivalence test for each component of the measurement model. With a non-significant χ^2 difference (p = 0.568), the control and treatment group's threat-perception components were equivalent. The efficacy perceptions component achieved satisfactory partial equivalence (p = 0.136) when we did not constrain one item (Byrne, 2010). The intentions to comply congeneric model was also partially equivalent across the two groups (p = 0.063).

5.3 Structural Model Analysis

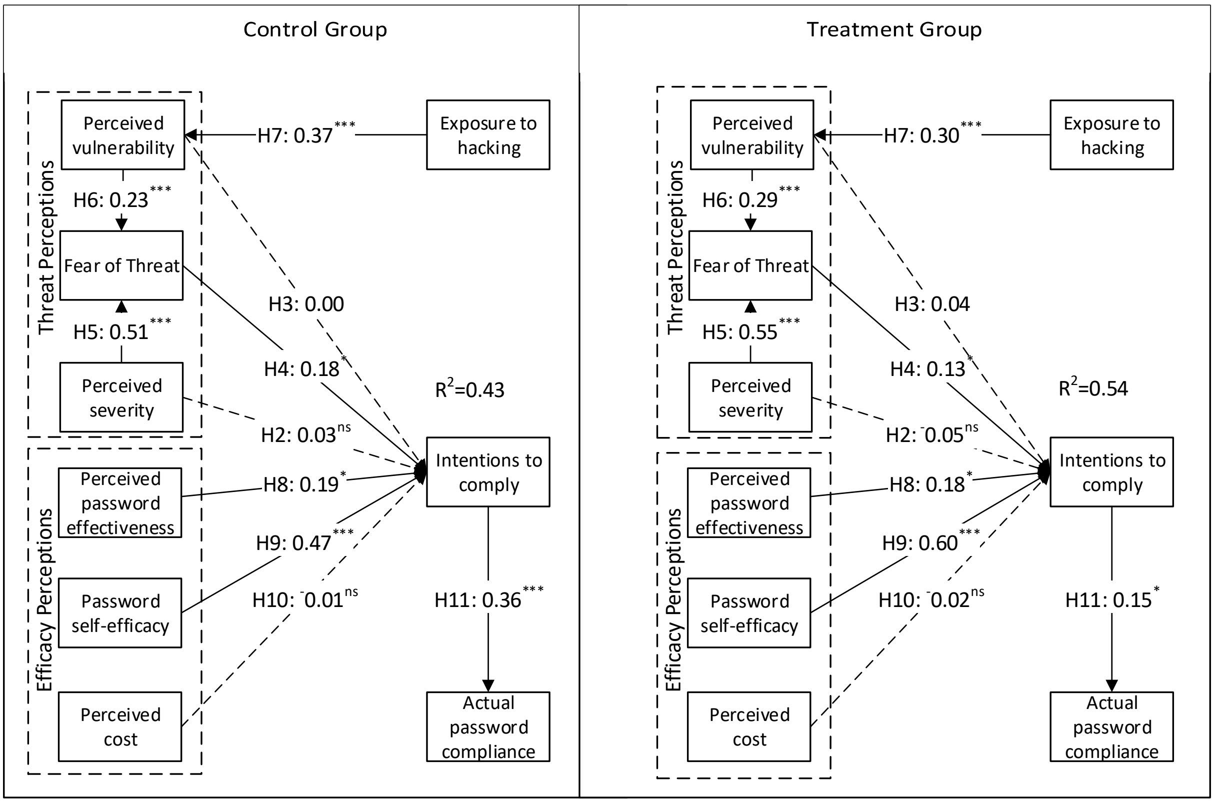
The model fit statistics suggest that the observed data fit the proposed structural model well. Normed χ^2 was acceptable at 1.716, and, because the sample size was greater than 200, a significant χ^2 p-value ($p < 0.001$) was acceptable. For a complex model with 29 observed variables, the CFI (0.947), TLI (0.940) and RMSEA (0.042) indicated good fit (Hair et al., 2010). The SRMR (0.092) was also acceptable since the value was less than 0.1 and the CFI was greater than 0.92 (Hair et al., 2010).

Figure 2 represents the full control and treatment group structural models. The control group model and treatment group model supported the same hypotheses. Similarly, the control group model and treatment group model rejected the same hypotheses, which suggests the models were equal across the two groups (note that Figure 2 does not show the results of H1 and H12; we present them in Section 5.4 and Section 5.5). As Figure 2 shows, the model explains the variance in intentions to comply moderately well (control $R^2 = 0.43$ and treatment $R^2 = 0.54$), and we found support for most hypothesized relationships.

As for threat perceptions, perceived severity had no association with intentions to comply (control path coefficient = 0.03; treatment path coefficient = -0.05), which does not support H2. This finding indicates that perceived severity of threats did not influence intentions to comply. As hypothesized, perceived vulnerability had no influence on intentions to comply (control path coefficient = 0.00; treatment path coefficient = 0.04), which supports H3 and implies that there is no direct link between vulnerability perceptions and intentions to comply with password guidelines. Although perceived vulnerability had no impact on intentions to comply, the results show a significant relationship between perceived vulnerability and fear of threat (control path coefficient = 0.23; treatment path coefficient = 0.29). The path between perceived severity and fear of threat was also significant (control path coefficient = 0.51; treatment path coefficient = 0.55). Further, fear of threat significantly influenced intentions to comply (control path coefficient = 0.18; treatment path coefficient = 0.13). This finding suggests that severity and vulnerability perceptions influence fear of password threats, which, in turn, increases the likelihood of compliance. These results support H4, H5 and H6. Exposure to hacking also significantly influenced perceived vulnerability (control path coefficient = 0.38; treatment path coefficient = 0.30), which supports H7 and implies that previous exposure to hacking has no influence on an individual's vulnerability perceptions.

Of the three efficacy perceptions factors, password self-efficacy (control path coefficient = 0.47; treatment path coefficient = 0.60) and perceived password effectiveness (control path coefficient = 0.19; treatment path coefficient = 0.18) had a significant influence on compliance intentions, which supports H8 and H9**.** This finding implies that whether individuals intend to comply with password guidelines depends on their beliefs about whether recommended guidelines would effectively prevent password threats and on their confidence in their ability to create strong passwords. Contrary to H10, the path between perceived cost and intentions to comply was not significant (control path coefficient = -0.01; treatment path coefficient = -0.02).

The results also show a significant link between intentions and actual password compliance, which supports H11 (control path coefficient = 0.36; treatment path coefficient = 0.15) and suggests that compliance intentions plays a significant role in actual compliance with password guidelines.



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

Figure 2. Model Testing Results for the Control and Treatment Group

5.4 Short-term Effects of Fear Appeals

We computed a composite score for each latent variable using regression imputation in AMOS version 19. As the ANOVA results in Table 2 indicate, the fear appeals significantly raised the levels of perceived severity, perceived vulnerability, fear of threat, perceived password effectiveness, password self-efficacy, intentions to comply, and actual password compliance. The magnitudes of the ANOVA effect sizes (η^2) ranged from 0.011 to a high of 0.217 with perceived password effectiveness as the most influenced by the fear appeals (they explained 21.7% of its variance). Only perceived cost was not significantly higher for the treatment group. The password-security information and training appeared to alter threat and efficacy perceptions and, thus, lead to significantly improved intentions to comply and actual password compliance. Therefore, we found support for H1.

5.5 Effects of Fear Appeals in the Long Term

We performed a one-way between-group ANOVA to test the hypothesis that fear appeals have a long-term effect on intentions to comply. Although those who received the password-security information and training had slightly higher levels of intentions to comply (M = 5.42, SD = 1.08 versus M = 5.33, SD = 1.17), the difference was not significant (F (1,192) = 0.316, p = 0.574). As the difference between in intentions to comply with password guidelines was not significantly different between those who had received fear appeal and those who had not, we did not find support for H12. Thus, although those who had received the fear appeals were more likely to intend to comply with password guidelines immediately after the training, their intentions were no better than those of the control group six weeks later.

As an additional post hoc exploration of the long-term effects of fear appeals, we compared participants' ability to remember the password they created in phase I between the groups. Of the 99 returning participants in the control group, 6.1 percent remembered their previous password, while 11.6 percent of those in the treatment group remembered their passwords. We conducted a χ^2 test of independence to examine if the proportion of those who remembered their passwords was significantly different between the two groups but found no significant difference (χ^2 (1) = 1.85, p = 0.174).

Table 2. Effects of Fear Appeals

Variable	ANOVA			No fear appeal		Fear appeal	
	F	p	η^2	Mean	St.dev	Mean	St.dev
Perceived vulnerability	27.04	0.00	0.063	3.65	1.34	4.36	1.42
Fear of threat	5.91	0.02	0.014	5.24	1.53	5.57	1.22
Perceived severity	4.57	0.03	0.011	4.36	1.56	4.66	1.19
Password self-efficacy	6.58	0.01	0.016	5.22	1.31	5.53	1.08
Perceived password effectiveness	112.05	0.00	0.271	4.74	0.92	5.75	1.01
Perceived cost	1.19	0.28	0.003	4.75	1.50	4.90	1.30
Intentions to comply	71.44	0.00	0.150	5.29	1.06	6.22	1.18
Actual password compliance	5.43	0.02	0.013	37.90	17.16	41.82	16.73

Control n = 202; treatment n = 204; η^2 = partial eta squared (equivalent to R^2).
Mean scores based on a seven-point scale for all variables except self-efficacy (10-point scale) and actual password compliance.

6 Discussion and Implications

6.1 Discussion

In this study, investigate how perceptions about passwords and security threats affect compliance with password guidelines and explore the effect of altering these perceptions both in the short term and longer term. Our results several key findings on the use of fear appeals in the IS security domain. First, fear appeals can elevate user security perceptions and improve users' confidence in the effectiveness of recommended security measures and their ability to comply with security guidelines. Second, providing password-security information can lead to improved short-term compliance in terms of both intentions to comply and actual password behavior. Both these findings are consistent with Johnston and Warkentin (2010) who found that improving threat perceptions and efficacy perceptions improves intentions to apply anti-spyware safeguards and with Vance et al. (2013) who conducted a password-related study and found that fear appeals can lead to significantly stronger passwords. Third, the fear appeals we used had only a short-term effect, which supports H1 but not H12. In our study, six weeks later, we found no difference in intentions to comply with password guidelines between those who had the password-security information and training session and those who did not. Using fear appeals that targeted both threat appraisal and coping appraisal had a positive impact on security behavior but only in the short term. Table 3 summarizes the hypothesized relationships and shows what ones we found support for and what ones we did not.

We included exposure to hacking in the proposed model to help explain how individuals develop vulnerability perceptions given the mixed findings on the role of perceived vulnerability in the IS security domain. We found that, when users or someone they know personally has their online account hacked, they are more likely to feel at risk—likely because, although users tend to underestimate their vulnerability to security threats (Sasse et al., 2001; Woon et al., 2005), this exposure provides acquired information that shapes how people assess their vulnerability to threats (Skogan & Maxfield, 1981; Weinstein, 1984). Both LaRose et al. (2008), who investigated the influence of prior exposure on intentions to adopt virus protection, and Tsai et al. (2016), who investigated its impact on general security intentions, also found similar results.

Table 3. Summary of Hypothesized Relationships and Effects of Fear Appeals

Hypothesized relations: supported
H1: Fear appeals → compliance with password guidelines (short-term effects)
H3: Perceived vulnerability ↛ intentions to comply
H4: Fear of threat → intentions to comply
H5: Perceived vulnerability → fear of threat
H6: Perceived severity → fear of threat
H7: Exposure to hacking → perceived vulnerability
H8: Perceived password effectiveness → intentions to comply
H9: Password self-efficacy → intentions to comply
H11: Intentions to comply → actual password compliance
Hypothesized relations: not supported
H2: Perceived severity → intentions to comply
H10: Perceived cost → intentions to comply
H12: Fear appeals → intentions to comply (long-term effects)

PMT (Rogers, 1975, 1983) proposes that perceived vulnerability has a direct impact on protection motivation; however, our results show no direct relationship between perceived vulnerability and intentions to comply with password guidelines. Believing that their online email account was likely to be hacked failed to motivate users to intend to comply with password guidelines, which supports H3 and corroborates the findings of several other IS security studies (e.g., Lee & Larsen, 2009; Vance et al., 2012; Woon et al., 2005).

We also found that awareness of password threats' potential consequences did not influence users' intention to comply with password guidelines—an interesting finding given it contradicts some other studies in the IS security domain that have found perceived severity to play a role in motivating users to follow security recommendations (Siponen et al., 2014; Vance et al., 2012; Workman et al., 2008). However, the fact that both perceived vulnerability and severity were not good predictors of compliance intentions is consistent with some previous IS security studies (e.g., Crossler et al., 2014; Posey et al., 2011; Siponen et al., 2010; Zhang & McDowell, 2009). Given that even participants who received the fear appeals had relatively low vulnerability and severity perceptions, we might question whether providing information about the likelihood and consequences of threats is enough to improve compliance with security recommendations. Further, Johnston et al. (2015) argue that conventional fear appeals may be inadequate in altering IS security behaviors because the rhetoric focuses on threats to users' information assets, and, thus, the users may not feel personally threatened. It is also possible that the fear appeal we used in our study was not adequately robust. As Boss et al. (2015) show in comparing a high and low fear appeal model, accounting for fear appeal strength may have provided a better understanding of the unexplained variance in our model.

We found that perceived vulnerability and perceived severity influence fear of threat. When users perceive that their online email accounts are vulnerable to password threats, they develop an emotional feeling of concern for password threats. Likewise, users are inclined to feel threatened when they are aware of a breach's potential consequences. This finding concurs with Boss et al. (2015) who found positive relationships between both vulnerability and severity perceptions and fear of IS security threats. Herath and Rao (2009) also found a relationship between employees' awareness of a breach's consequences and their level of concern about security breaches, although perceived vulnerability did not influence level of concern in that study. They also found low average levels of perceived vulnerability.

We found that fear of threat has a significant influence on compliance intentions. Users who express a high level of concern about risks are more likely to intend to adopt necessary preventative measures. This finding supports the results of Zhang and McDowell (2009), who found a positive relationship between fear and intentions to apply online password protection and found fear to be a better predictor of behavioral intentions than perceived vulnerability or perceived severity. This finding is important because many previous applications of PMT to IS security behaviors have overlooked the role of fear.

As in several other IS security studies (e.g., Lee & Larsen, 2009; Posey et al., 2015; Woon et al., 2005), our results show a positive relationship between perceived effectiveness and intentions to comply. Users are more willing to comply with password guidelines when they believe the recommended guidelines will protect their online account from being hacked. While awareness of available security mechanisms is important (Dhamija et al., 2006), it seems that users' decision to apply security measures depends on whether they perceive them as effective. As such, users need to have confidence that the recommended security safeguards will effectively thwart security attacks.

We found that password self-efficacy has a significant influence on intentions to comply with password guidelines. When users are confident in their ability to create and remember strong passwords, they are more likely to comply with guidelines. Other research has also found that self-efficacy plays 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 in an organization.

Surprisingly, our results showed no link between perceived cost and intentions to comply with password guidelines. The effort associated with remembering passwords appears to play no role in users' compliance intentions. This result differs from a previous password-related study (Zhang & McDowell, 2009) and several other IS security studies (e.g., Lee & Larsen, 2009; Vance et al., 2012). One reason for why is that the items we used to measure perceived cost focused on password recall issues, and other password-related cost factors could contribute to poor practices. For example, Tam, Glassmana, and Vandenwauverb (2009) found that, when users have limited time to memorize their email passwords, they tend to create weak passwords, and Grawemeyer and Johnson (2011) found usability issues such as mistype errors can have a negative impact on password quality. Thus, we may have discovered better insights into the relationship had we considered other costs associated with password use.

Our results support our hypothesis that users who have a strong motivation to comply with password guidelines are more likely to comply. This finding supports Fishbein and Ajzen's (1975) proposition that intentions determine behavior and Liang and Xue's (2010) finding that home computer users' avoidance motivation determines their threat-avoidance behavior. However, the relationship between intentions and actual compliance, particularly for the treatment group, was not strong. While PMT assumes that behavioral intentions can adequately predict behavior (Prentice-Dunn & Rogers, 1986; Weinstein, 1993), our results indicate a gap between intentions and actual compliance and suggest that we need more research to determine how well intentions can predict IS security behavior and the possible factors that may contribute to a weak predictability of actual behavior. Lee and Larsen (2009) provide one possible explanation for the difference in relationship strength between the two groups in this study; these authors found similar differences in relationship strength across four different groups of participants categorized as IT knowledgeable or non-IT knowledgeable. While the correlation between intentions and actual behavior was significant for all four groups, the authors found a weaker correlation between intentions and behavior for IS experts and participants from IT-intensive industries compared with non-IS experts and non-IT intensive participants. Similarly, in our study, the association between compliance intentions and actual password compliance proved to be weaker for the group of participants who we provided with password-security information and training compared to the control group. This gap suggests knowledgeable users in IS security might consider other things when deciding whether to implement IS security measures.

While some experimental evidence (e.g., Jenkins et al., 2013; Johnston & Warkentin, 2010; Vance et al., 2013) supports the use of fear appeals in the IS security domain, research has largely overlooked their long-term effects. In this study, although fear appeals had an immediate effect on compliance intentions and password strength, they had no longer-term effects, which we did not expect given that studies in the health domain (e.g., Hampstead et al., 2012) have shown the long-term value of the mnemonic training included with fear appeals. This lack of long-term impact may indicate that a single application of fear appeals is not sufficient to ensure more than a short-term change in intentions and is consistent with the suggestion from Boss et al. (2015) that users need ongoing IS security training to ensure they continue to comply. As the proportion of those who remembered their passwords after six weeks without using it was nearly double for the treatment group, our study draws attention to the need for longitudinal studies in this area.

6.2 Implications for Research

Our findings open new potential avenues for research. For instance, one could make two possible propositions regarding the role of perceived vulnerability and fear on IS security behavior. First, in the context of personal protection, an emotional response to threats could possibly influence users. Second, 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), perceived vulnerability does not likely influence users' IS security behavior in the context of personal protection. These potential context-related differences have important implications for how personal IS users protect themselves and should be investigated further.

The study is also the first to explicitly investigate the long-term effects of fear appeals in personal IS security. The lack of long-term effects highlights the need for further longitudinal studies to explore to examine if, and under what conditions, fear appeals can have longer-term effects on IS security behavior.

6.2.1 Future Research Should Further Explore the Role of Fear in IS Security Behavior

Much IS security research has investigated the direct effects of severity and vulnerability perceptions on IS protection motivation; however, research has largely overlooked fear's influence. Yet, we found that fear of threat was the only threat perceptions factor to have a direct influence on password compliance intentions. Our results and those from other IS security-related studies (e.g., Boss et al., 2015; Zhang & McDowell, 2009) demonstrate that we should consider fear a key variable in future applications of PMT to IS security behaviors. Our study makes an important contribution to our understanding of PMT's application in IS security-related studies and particularly the importance of measuring fear and applying PMT as originally prescribed.

6.2.2 Users May Behave Differently in Different IS Security Contexts

Our results point to two potential differences in how users behave in different IS security contexts. The first relates to how fear influences behavioral intentions in different IS security contexts. We found that, in their decision to comply with security recommendations, users respond emotionally when the security behavior relates to personal protection. The results of other personal computing studies (e.g., Liang & Xue, 2010; Zhang & McDowell, 2009) also suggest that users respond positively to security recommendations if they feel threatened or nervous. Zhang and McDowell (2009) found that fear of password-related threats influenced users' intentions to implement password protection, and Liang and Xue (2010) found that users will avoid security threats when they feel personally threatened.

Posey et al. (2011) also investigated the influence of fear on IS security behavioral intentions. They examined the role of fear in employees' motivation to protect their organization's information assets and found no relationship between fear and IS security behavior. They note that fear may be a predictor of intentions only in the context of personal computer protection. Posey et al. (2015) also found that fear does not drive employees unless they are personally connected or committed to their organizations, which suggests personal relevance is critical in engendering protection motivation in an organizational setting. Collectively, these findings suggest that, in the context of personal protection, users respond emotionally to threats and that this emotional feeling towards security threats influences their willingness to implement security measures. However, we need more research to better understand the impact of fear in different IS security contexts.

The second potential difference relates to how users assess their vulnerability to security threats. In this study, the degree to which a user believed they were likely to experience a password-related threat did not directly influence their compliance intentions. Interestingly, studies in the context of organizational security (e.g., Ifinedo, 2012; Lee & Larsen, 2009; Siponen et al., 2014; Workman et al., 2008) suggest an association between perceived vulnerability and intentions. However, an overwhelming majority of studies in the context of personal protection (e.g., Crossler, 2010; Liang & Xue, 2010; Milne et al., 2009; Woon et al., 2005; Zhang & McDowell, 2009), our study included, have found no such link. Perceived vulnerability and perceived severity are considered cognitive responses to threats (LaTour & Rotfeld, 1997); thus, users may respond cognitively in an organizational setting and emotionally in a personal setting. Future research should explore if users behave differently in different IS security contexts, particularly in their threat-appraisal process, which may provide 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 PMT has different applicability in different IS security contexts raises the question of whether PMT in its entirety is ideal for explaining IS security behaviors. Thus far, research applying PMT in the IS security domain largely proposes perceived severity, perceived vulnerability, response efficacy, response cost, and self-efficacy as key determinants of security behavior. However, no consensus on the exact relationship between these factors and behavioral intentions has emerged. The prevailing view suggests threat appraisal and coping appraisal factors have an independent and direct impact on users' IS security behavioral intentions. However, the interpretation of PMT, particularly that of threat appraisal component, varies greatly from study to study, which makes comparing results across studies challenging, and, as the our findings show, leaves the applicability of PMT open to question. As Johnston et al. (2015) argue, future studies should investigate the applicability of PMT in different IS security domains.

6.2.3 Future Studies Should Undertake Longitudinal Analysis of the Effects of Fear Appeals

Some studies in the IS security domain have examined the effectiveness of fear appeals (e.g., Boss et al., 2015; Jenkins et al., 2013; Johnston & Warkentin, 2010; Vance et al., 2013), and none thus far have considered whether the effects of fear appeals persisted after the intervention. To the best of our knowledge, we are the first to explicitly investigate the long-term effects of fear appeals in personal IS security. The fear appeals we used in this study had only a short-term effect, and, while discouraging, this finding highlights the importance of longitudinal studies and an opportunity for future studies to explore to examine if, and under what conditions, fear appeals can have longer-term effects on IS security behavior.

6.3 Implications for Practice

We demonstrate that providing guidance such as awareness training and the necessary skills to implement the recommended security measures can significantly improve security practices immediately after training. While we examine 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 (Jenkins et al., 2013; Winkler, 2009). Thus, our study has implications for organizations and IS security training practitioners.

Our study also has implications for users and for vendors and websites that require users to use passwords to access their services. Given that the information accessible can include financial and medical information (Goncharov, 2012), personal online accounts such as social networking accounts are high on hackers' target lists (El Emam et al., 2011; Florêncio & Herley, 2007). Yet, despite the widespread use of weak passwords (Florêncio & Herley, 2010; Lorenz, Kikkas, & Klooster, 2013), 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 an organizational setting can be a challenge. Vendor websites typically rely on a set of password guidelines to ensure that 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).

Research has shown training strategies such as communicating the reality of threats to information (Herath & Rao, 2009) and ensuring users realize the appropriate response mechanisms (Puhakainen & Siponen, 2010) to improve compliance with security policies. Persuasive communication that targets individuals' beliefs to persuade them to take preventative measures appears to be an effective method of encouraging users to apply security safeguards in the short term (e.g., Johnston & Warkentin, 2010; Johnston et al., 2015; Vance et al., 2013). We found that users with password-security training had higher threat awareness, which also increased their overall level of concern for security threats and likelihood of complying with password guidelines. Organizations should try to convince users that security attacks are prevalent and emphasize what impact they may have on both parties (i.e., user and organization). In addition, users are more likely to comply if they are convinced that the recommended security mechanisms will prevent threats and, more importantly, if they believe they can implement the available security mechanisms. Organizations should communicate to users what effective responses they can take to prevent a security breach. In addition, we show that, to comply with password guidelines, users must believe that they can create strong, memorable passwords. As self-efficacy perceptions had the strongest impact on intentions to comply, 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.

Our study shows that fear appeals can improve compliance with security policies but that the effect may be short term, which suggests that, ideally, organizations need to engage with users about security on an ongoing basis. The findings of Boss et al. (2015), who used multiple applications of fear appeals, also suggest organizations need to frequently train users. In practice, however, due to limited resources and time constraints for security-training teams (Rudis et al., 2016), the key question our study raises concerns how to increase the longevity of fear appeals. This question is relevant in organizations where limited resources may limit the frequency of security-training efforts and for personal users who have limited access to formal training, which forces them to rely on information sources such as friends, the media, and the Internet (Furnell et al., 2007).

6.4 Limitations

In this study, we explored the long-term effectiveness of fear appeals; however, we found that they had no long-term effect on users' compliance. A potential limitation in this study is that we used a single application of fear appeals, which 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.

Although PMT assumes that behavioral intentions can adequately predict behavior (Prentice-Dunn & Rogers, 1986; Weinstein, 1993), we extend the model to reflect the influence of intentions on compliance. We found a weak relationship between intentions and actual compliance. A limitation of the study is that the measure of intentions related to intention to follow guidelines to protect users' “important email account”, while the measure for actual compliance related to passwords for the “study survey account”, which possibly reduced relationship strength.

Another limitation of our study relates to how we measured perceived cost. We found no association between perceived cost and users' motivation to comply with password guidelines. The measurement items we used focused on password memory issues, which are arguably one of the most important aspects of password use and something that users find difficult. However, research has shown other cost factors such as time to memorize passwords and ease of typing to contribute to poor password quality (e.g., Grawemeyer & Johnson, 2011; Tam et al., 2009), and future password-related research should include it when measuring response cost.

7 Conclusions

We investigated how perceptions about security threats and passwords can affect compliance with guidelines, and, in doing so, explored the effect of altering these perceptions via fear appeals on password compliance both immediately and in the longer term. Except for perceived cost, the fear appeals we used significantly raised participants' levels of threat and efficacy perceptions and both intentions and actual password compliance, which demonstrates that altering perceptions can improve compliance with IS security policies in the short term. However, of the threat perceptions considered, we found that only fear of threat had a direct impact on compliance intentions, which suggests that targeting perceived effectiveness of security measures and self-efficacy is more important in improving IS security compliance. However, Peters, Ruiter, and Kok (2014) found that fear appeal developers underestimate the importance of efficacy-inducing components. Our study highlights the need for fear appeals to emphasize the effectiveness of protection mechanisms and to support the development of self-efficacy.

Our proposed model includes three key modifications to the PMT (Rogers, 1975, 1983), which reflects previous findings in the IS security domain. First, we hypothesize that perceived vulnerability does not directly influence intentions to comply with password guidelines. We found support for this hypothesis, which suggests the need for further research into the role of vulnerability perceptions in IS security behavior.

Second, our model incorporates the impact of prior exposure to hacking on vulnerability perceptions to explain how users' vulnerability perceptions develop. Adding this path provided insights into how users develop vulnerability perceptions but provided no additional insight into the role vulnerability perceptions play in decisions to comply with security recommendations.

Last, we propose a path between compliance intentions and actual password compliance. We found evidence to support an extension to PMT to include a link between intentions and actual behavior. Until Boss et al. (2015), no published work had used fear appeals, examined the role of fear in IS security behaviors, and also measured actual compliance behaviors. Our study also addresses this gap in the literature and further contributes by examining the long-term implications of using fear appeals; we found that their effects declined over time. Future research should examine how we can increase the impact and longevity of fear appeals. In the meantime, this result suggests that users need ongoing training..

References

Ablon, L., Libicki, M. C., & Golay, A. A. (2014). *Markets for cybercrime tools and stolen data: Hackers' bazaar*. Santa Monica, CA: Rand Corporation.

Abraham, C. S., 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.

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

Authentic-Response. (2012). *Market research survey panels*. Retrieved from www.authenticresponse.com [now www.criticalmix.com]

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.

BBC. (2013). Analysis reveals popular Adobe passwords. *BBC.* Retrieved from http://www.bbc.co.uk/news/technology-24821528

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, San Francisco, CA.

Bonneau, J., & Preibusch, S. (2010). *The password thicket: Technical and market failures in human authentication on the web*. Paper presented at the 9th Workshop on the Economics of Information Security, Cambridge, MA.

Boss, S. R. (2007). *Control, perceived risk and information security precautions: External and internal motivations for security behavior* (doctoral thesis). University of Pittsburgh.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837-864.

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, W. E., Dodson, D. F., Newton, E. M., Pelner, R. A., Polk, W. T., Gupta, S., & Nabbus, E. A. (2013). *Electronic authentication guideline* (NIST Special Publication 800-63-2). National Institute for Standards and Technology.

Byrne, B. M. (2010). *Structural equation modeling with AMOS: Basic concepts, applications, and programming* (2nd ed.). New York, NY: Routledge.

Cazier, J. A., & Medlin, B. D. (2006). Password security: An empirical investigation into e-commerce passwords and their crack times. *Information Security Journal, 15*(6), 45-55.

Cenfetelli, R. T., & Bassellier, G. (2009). Interpretation of formative measurement in information systems research. *MIS Quarterly*, *33*(4), 689-707.

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, C. L. (2011). *The adoption of computer security: An analysis of home personal computer user behavior using the health belief model* (doctoral thesis). Utah State University, Utah.

Compeau, D. R., & Higgins, C. A. (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.* Retrieved from http://www.forbes.com/sites/davidcoursey/2011/11/21/25-worst-passwords-of-2011-revealed/

Crossler, R. E. (2010). Protection motivation theory: Understanding determinants to backing up personal data. In *Proceedings of the 43rd Hawaii International Conference on System Sciences*.

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

Crossler, R. E., Long, J. H., Loraas, T. M., & Trinkle, B. S. (2014). Understanding compliance with BYOD policies utilizing protection motivation theory: Bridging the intention-behavior gap. *Journal of Information Systems, 28*(1), 209-226.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information systems research, 20*(1), 79-98.

Das, A., Bonneau, J., Caesar, M., Borisov, N., & Wang, X. (2014). The tangled web of password reuse. In *Proceedings of Symposium on Network and Distributed System Security.*

Dhamija, R., Tygar, J., & Hearst, M. (2006). Why phishing works. In *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), e18.

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

Fishbein, M., & Cappella, J. N. (2006). The role of theory in developing effective health communications. *Journal of Communication, 56*, S1-S17.

Florêncio, D., & Herley, C. (2007). *A large-scale study of web password habits*. Paper presented at 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, 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.

Furnell, S., Bryant, P., & Phippen, A. (2007). Assessing the security perceptions of personal Internet users. *Computers & Security, 26*(5), 410-417.

Goncharov, M. (2012). Russian underground 101. *Trend Micro*. Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

Grawemeyer, B., & Johnson, H. (2011). Using and managing multiple passwords: A week to a view. *Interacting with Computers, 23*(3), 256-267.

Hagen, J., Albrechtsen, E., & Ole Johnsen, S. (2011). The long-term effects of information security e-learning on organizational learning. *Information Management & Computer Security, 19*(3), 140-154.

Hair, J., Black, W., Babin, B., Anderson, R., & Tatham, R. (2010). *Multivariate data analysis* (7th ed.). Upper Saddle River, NJ: Prentice Hall.

Hampstead, B. M., Sathian, K., Phillips, P. A., Amaraneni, A., Delaune, W. R., & Stringer, A. Y. (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), 385-399.

Helkala, K., & Svendsen, N. K. (2012). The security and memorability of passwords generated by using an association element and a personal factor. In P. Laud (Ed.), *Information security technology for applications* (pp. 114-130). Berlin: Springer.

Herath, T., Chen, R., Wang, J., Banjara, K., Wilbur, J., & Rao, H. R. (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, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Herley, C., & Van Oorschot, P. (2012). A research agenda acknowledging the persistence of passwords. *IEEE Security & Privacy, 10*(1), 28-36.

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.

Hu, L., & Bentler, P. M. (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.

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, P. G., & Sasse, M. A. (2010). The true cost of unusable password policies: Password use in the wild. In *Proceedings of the 28th International Conference on Human Factors in Computing Systems.*

Jenkins, J. L., Grimes, M., Proudfoot, J. G., & Lowry, P. B. (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, 20*(2), 196-213.

Johnston, A., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549-566.

Johnston, A. C., Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly, 39*(1), 113-134.

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.

LaRose, R., Rifon, N., Liu, S., & Lee, D. (2005). *Understanding online safety behavior: A multivariate model.* Paper presented at the 55th Annual Conference of the International Communication Association, New York, NY.

LaRose, R., Rifon, N. J., & Enbody, R. (2008). Promoting personal responsibility for Internet safety. *Communications of the ACM, 51*(3), 71-76.

LaTour, M. S., & Rotfeld, H. J. (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., & Larsen, K. R. (2009). Threat or coping appraisal: Determinants of SMB executives decision to adopt anti-malware software. *European Journal of Information Systems, 18*(2), 177-187.

Leventhal, H. (1970). Findings and theory in the study of fear communications. In L. Berkowitz (Ed.), *Advances in experimental social psychology* (vol. 5, pp. 119-186). New York: Academic Press.

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. In L. Marinos & I. Askoxylakis (Eds.), *Human aspects of information security, privacy, and trust* (pp. 276-283). Berlin: Springer.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*(5), 469-479.

Marett, K., McNab, A. L., & Harris, R. B. (2011). Social networking websites and posting personal information: An evaluation of protection motivation theory. *AIS Transactions on Human-Computer Interaction, 3*(3), 170-188.

McDowell, M., Rafail, J., & Hernan, S. (2009). Choosing and protecting passwords. *United States Computer Emergency Readiness Team.* Retrieved from http://www.us-cert.gov/cas/tips/ST04-002.html

Milne, G. R., Labrecque, L. I., & 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.

NCSA & McAfee. (2011). NCSA/McAfee Internet home users survey. *National Cyber Security Alliance Studies*. Retrieved from http://www.staysafeonline.org/stay-safe-online/resources/

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

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Which factors explain employees' adherence to information security policies? An empirical study. In *Proceedings of the Pacific Asia Conference on Information Systems.*

Peters, G. J. Y., Ruiter, R. A., & 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.

Posey, C., Roberts, T., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32*(4), 179-214.

Posey, C., Roberts, T., Lowry, P. B., Courtney, J., & Bennett, B. (2011). Motivating the insider to protect organizational information assets: Evidence from protection motivation theory and rival explanations. In *Proceedings of 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), 757-778.

Quagliata, K. (2011). Impact of security awareness training components on perceived security effectiveness. *ISACA Journal, 4*, 1-6.

Rippetoe, P. A., & Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology, 52*(3), 596-604.

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, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. Gochman (Ed.), *Handbook of health behavior research: Determinants of health behavior* (pp. 113-132). New York, NY. Springer.

Rosenstock, I. M. (1974). Historical origins of the health belief model. *Health Education Monographs, 2*, 1-8.

Rudis, B., Hayden, L., Kretschmer, G., Sasse, A., Becker, I., & Homer, J. (2016). SANS security awareness report—securing the human. *SANS.* Retrieved from https://www.sans.org/security-awareness-training/reports/2016-security-awareness-report

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]. Gaithersburg, MD: NIST.

Shannon, C. E. (2001). A mathematical theory of communication. *SIGMOBILE Mobile Computing and Communications Review, 5*(1), 3-55.

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*. Paper presented at the 47th Hawaii International Conference on System Sciences, Waikoloa, Hawaii.

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

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64-71.

Skogan, W., & Maxfield, M. (1981). *Coping with crime: Individual and neighborhood reactions*. Beverly Hills, CA: Sage.

Stewart, J. M., Tittel, E., & Chapple, M. (2008). *CISSP: Certified information systems security professional study guide* (4th ed.). San Francisco, CA: Sybex.

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.

Taneski, V., Heričko, M., & Brumen, B. (2014). *Password security–no change in 35 years?* Paper presented at the 37th International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija, Croatia.

Tsai, H.-y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security, 59*, 138-150.

Ur, B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M. L., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N., & Cranor, L. F. (2012). *How does your password measure up? The effect of strength meters on password creation*. Paper presented at the 21st USENIX Conference on Security Symposium, Bellevue, WA.

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 46th Hawaii International Conference on System Sciences, Wailea, HI.

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.

Vu, K.-P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B.-L. B., Cook, J., & Schultz, E. E. (2007). Improving password security and memorability to protect personal and organizational information. *International Journal of Human-Computer Studies, 65*(8), 744-757.

Weinstein, N. D. (1984). Why it won't happen to me: Perceptions of risk factors and susceptibility. *Health Psychology, 3*(5), 431-457.

Weinstein, N. D. (1993). Testing four competing theories of health-protective behavior. *Health Psychology, 12*(4), 324.

Winkler, I. (2009). Winkler: The real problems with cloud computing. *CSO.* Retrieved from http://www.csoonline.com/article/2124281/cloud-security/winkler--the-real-problems-with-cloud-computing.html

Woon, I., Tan, G.-W., & Low, R. (2005). *A protection motivation theory approach to home wireless security*. Paper presented at the 26th International Conference on Information Systems, Las Vegas, NV.

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*(6), 2799-2816.

Wurtele, S. K., & Maddux, J. E. (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, L., & McDowell, W. C. (2009). Am I really at risk? Determinants of online users' intentions to use strong passwords. *Journal of Internet Commerce, 8*(3), 180-197.

Zviran, M., & Haga, W. J. (1999). Password security: An empirical study. *Journal of Management Information Systems, 15*(4), 161-185.

Appendix A: Summary of PMT Applications in IS Research

Table A1. Summary of PMT Applications in IS Research

Summary of PMT applications in IS research (in alphabetical order)				
Study	**Behavior context**	**Theory**	**Variables adopted from PMT**	**Fear appeals**
Anderson & Agarwal (2010)	Intentions to adopt security precautions, home computer	PMT TPB	Concern regarding security threats, perceived citizen effectiveness, security behavior self-efficacy	No fear appeal manipulation
Boss et al. (2015)	Intentions and actual data back-up and use anti-malware, personal (study 1) Intentions and actual use of anti-malware, personal (study 2)	PMT	Perceived threat severity, perceived threat vulnerability, fear, response efficacy, self-efficacy, response costs, maladaptive rewards	Study 1: longitudinal; administered three times to examine strength effects. Study 2: short-term; both studies manipulated only threat appraisal and fear.
Crossler (2010)	Actual adoption of data backup measures, personal computer	PMT	Perceived security vulnerability, perceived security severity, security self-efficacy, response efficacy, prevention cost	No fear appeal manipulation
Crossler et al. (2014)	Intentions and actual compliance with BYOD policies, organization	PMT	Perceived threat severity, perceived threat susceptibility, self-efficacy, response efficacy, response cost	No fear appeal manipulation
Herath & Rao (2009)	Intentions to comply with security policies, organizational	PMT DT	Perceived probability of security breach, perceived severity of security breach, security breach concern level, response efficacy, response cost, self-efficacy	
Herath et al. (2014)	Intentions to adopt email authentication service, online email services	PMT TTAT TAM	Email risk perception, email screening self-efficacy	Manipulate non-PMT variables
Ifinedo (2012)	Intentions to comply with security policies, organization	PMT TPB	Perceived vulnerability, perceived severity, response efficacy, response cost, self-efficacy	No fear appeal manipulation
Jenkins et al. (2013)	Create unique passwords, online Web accounts	PMT	Threat severity, threat vulnerability, response efficacy	Short-term effects
Johnston & Warkentin (2010)	Intentions to use anti-spyware software, personal computer	PMT Social Influence	Perceived threat severity, perceived threat susceptibility, response efficacy, self-efficacy	Short-term effects
Johnston et al. (2015)	Intentions to comply with recommended protective strategies, insiders (organization)	PMT DT	Perceived threat severity, prceived threat vulnerability, perceived self-efficacy, perceived response efficacy	Short-term effects
LaRose, Liu, & Lee (2005)	Actual online security behavior: personal online safety	PMT SCT	Perceived threat susceptibility, perceived threat seriousness, coping efficacy, response efficacy, perceived benefits, perceived cost	No fear appeal manipulation
LaRose et al. (2008)	Intentions to adopt security measures, home Internet	PMT ELM SCT	Threat susceptibility, threat severity, self-efficacy, response efficacy	Manipulate SCT variables
Lee & Larsen (2009)	Intentions and actual adoption (purchase) of anti-malware software, organization (SMB)	PMT TAM	Perceived severity, perceived vulnerability, response efficacy, self-efficacy, perceived cost	No fear appeal manipulation

Table A1. Summary of PMT Applications in IS Research

Liang & Xue (2010)	Intention and actual avoidance of spyware/use of anti-spyware software	PMT TTAT	Perceived severity, perceived susceptibility, perceived threat, safeguard effectiveness, safeguard cost, self-efficacy	No fear appeal manipulation
Marett et al. (2011)	Intentions to change risky social media behavior (adaptive response), social network	PMT	Perceived threat severity, fear, self-efficacy, response efficacy, intrinsic rewards, extrinsic rewards, response costs, maladaptive response (avoidance and hopelessness)	Short-term effects
Milne et al. (2009)	Actual adoption and avoidance, actual risky and protective behavior, e-commerce consumers	PMT SCT	Perceived online threats, perceived likelihood of online threat, self-efficacy	No Fear Appeals manipulation
Pahnila, Siponen, & Mahmood (2007)	Intentions and actual compliance with security policy, organization	PMT GDT TRA IS success	Threat appraisal (perceived vulnerability and perceived severity items), self-efficacy, response efficacy	No fear appeal manipulation
Posey et al. (2011)	Intentions and actual protection of organization's information assets, organization	PMT	Intrinsic rewards, extrinsic rewards, threat vulnerability, threat severity, fear, response efficacy, self-efficac , response costs	No fear appeal manipulation
Posey et al. (2015)	Intentions and actual protection of organization's information assets: insiders (organization)	PMT Organizational commitment	Intrinsic rewards, extrinsic rewards, threat vulnerability, threat severity, fear, response efficacy, self-efficacy, response costs	Short-term effects
Siponen et al. (2010)	Intentions and actual compliance with information security policies, organization	PMT TRA GDT IDF	Threat appraisal (threat vulnerability and threat severity items), self-efficacy, response efficacy, rewards	No fear appeal manipulation
Siponen et al. (2014)	Intentions and actual adherence to information security policies, organization	PMT TRA CET	Perceived severity, perceived vulnerability, response efficacy, self-efficacy, rewards	No fear appeal manipulation
Vance et al. (2012)	Intentions to comply with security policies, organization	PMT TH	Perceived vulnerability, perceived severity, rewards, response efficacy, self-efficacy, response cost	No fear appeal manipulation
Vance et al. (2013)	Actual password strength, online Web accounts	PMT	Perceived severity, perceived susceptibility, response efficacy, self-efficacy	Short-term effects
Woon et al. (2005)	Actual adoption of wireless security measures: home network	PMT	Perceived vulnerability, perceived severity, response efficacy, self-efficacy, response cost	No fear appeal manipulation
Workman et al. (2008)	Actual non-compliance with security recommendations, organization	PMT	Perceived severity , perceived vulnerability, self-efficacy, response efficacy	No fear appeal manipulation
Zhang & McDowell (2009)	Intentions to use strong password, variety of online accounts	PMT	Perceived severity, perceived vulnerability, fear, response efficacy, response cost	No fear appeal manipulation

Table A1. Summary of PMT Applications in IS Research

Current study (this paper)	Intentions to comply with password guidelines, actual password compliance	PMT	Perceived severity, perceived vulnerability, fear of threat, perceived password effectiveness, password self-efficacy, perceived cost	Longitudinal: administered once to examine immediate and long-term effects. Manipulated threat and coping appraisal.

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.

Appendix B: Measurement Items

Table B1. Measurement Items

Measurement items
_E_xposure to hacking (no = 0; 1 = low impact; 7 = high impact)
Have you ever had your important email account, online shopping account or online banking account hacked into?
Has someone you know personally ever had their important email account, online shopping account or online banking account hacked into?
Perceived vulnerability (1 = strongly disagree; 7 = strongly agree)
There is a chance that someone could successfully guess at least one of my passwords
There is a chance that someone could successfully crack at least one of my passwords using password cracking software
There is a chance that someone could hack into at least one of my important email accounts
If someone hacked into my important email account, there is a chance that they could guess my other important passwords*
Perceived severity (1 = not at all severe; 7 = very severe)
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 someone:
…successfully guessed any of your important email passwords
…hacked into any of your important email accounts*
…used any of your important email accounts to send messages to your contact list without your knowledge
…obtained your personal information from your important email accounts
…changed the password to your important email accounts without your knowledge
… tole the password to one of your important email accounts*
Fear of threat (1 = strongly disagree; 7 = strongly agree)
The thought of someone guessing the password to any of my important email accounts makes me worried*
The thought of someone hacking into any of my important email accounts makes me worried
The thought of someone using any of my important email accounts without my knowledge makes me worried
The thought of someone using my personal information from any of my important email accounts makes me worried
The thought of someone changing or deleting information obtained from any of my important email accounts makes me worried
The thought of someone using password monitoring software to record my important passwords makes me worried
Perceived password effectiveness (1 = strongly disagree; 7 = strongly agree)
Making sure that my passwords contain a combination of numbers, letters and symbols will prevent my passwords from being guessed*
Making sure that my passwords do not contain any dictionary words will make them more difficult to guess
Making sure that my passwords do not contain personal information such as my date of birth will make them more difficult to guess
I can protect my online accounts better if I use a different password for each of my online accounts
I can protect my online accounts better if I change my passwords regularly
I can protect my online accounts better if I use a long complex password
Password self-efficacy (1 = not at all confident; 10 = totally confident)
I would be able to create a strong password that is difficult to hack:
…if I had instructions on how to create a strong password
…if I had step-by-step instructions on how to memorize a strong password
…if I had a lot of time to create a strong password
…if I had used strong passwords before

Table B1. Measurement Items

Perceived cost (1 = strongly disagree; 7 = strongly agree)
Remembering a password that contains a combination of numbers, letters and symbols would be difficult
Remembering a password that is long and complex would be difficult
Remembering a password that does not contain any dictionary words would be difficult
Remembering a password that does not contain personal information such as date of birth would be difficult*
If I use different passwords for each of my web accounts, it would be difficult for me to remember them all*
If I change my passwords regularly, it would be difficult for me to remember them
Intentions to comply with password guidelines (1 = not at all likely; 7 = very likely)
I would choose a password that follows the password length requirement suggested by the system
I would choose a password with a combination of numbers, letters, and symbols as suggested by the system
I would choose a password that is difficult to guess*
I would choose a password that follows all the guidelines provided by the system
I would choose a password that is different from my old password*
I would choose a password that is different from my other online passwords*
The thought of someone using any of my important email accounts without my knowledge makes me worried
The thought of someone using my personal information from any of my important email accounts makes me worried
The thought of someone changing or deleting information obtained from any of my important email accounts makes me worried
The thought of someone using password monitoring software to record my important passwords makes me worried
Perceived password effectiveness _(1 = strongly disagree; 7 = strongly agree)_
Making sure that my passwords contain a combination of numbers, letters and symbols will prevent my passwords from being guessed*
Making sure that my passwords do not contain any dictionary words will make them more difficult to guess
Making sure that my passwords do not contain personal information such as my date of birth will make them more difficult to guess
I can protect my online accounts better if I use a different password for each of my online accounts
I can protect my online accounts better if I change my passwords regularly
I can protect my online accounts better if I use a long complex password
Password self-efficacy (1 = not at all confident; 10 = totally confident)
I would be able to create a strong password that is difficult to hack:
…if I had instructions on how to create a strong password
…if I had step-by-step instructions on how to memorize a strong password
…if I had a lot of time to create a strong password
…if I had used strong passwords before
Perceived cost (1 = strongly disagree; 7 = strongly agree)
Remembering a password that contains a combination of numbers, letters and symbols would be difficult
Remembering a password that is long and complex would be difficult
Remembering a password that does not contain any dictionary words would be difficult
Remembering a password that does not contain personal information such as date of birth would be difficult*
If I use different passwords for each of my web accounts, it would be difficult for me to remember them all*
If I change my passwords regularly, it would be difficult for me to remember them
Intentions to comply with password guidelines (1 = not at all likely; 7 = very likely)
I would choose a password that follows the password length requirement suggested by the system
I would choose a password with a combination of numbers, letters, and symbols as suggested by the system

Table B1. Measurement Items

I would choose a password that is difficult to guess*
I would choose a password that follows all the guidelines provided by the system
I would choose a password that is different from my old password*
I would choose a password that is different from my other online passwords*

Appendix C: Correlation Matrix

Table C1. Correlation Matrix (Control Group)

Latent variable	1	2	3	4	5	6	7	8	9
1. Exposure to hacking	*								
2. Perceived vulnerability	0.395	**0.715**							
3. Fear of threat	0.171	0.339	**0.890**						
4. Perceived severity	0.237	0.189	0.573	**0.745**					
5. Perceived password effectiveness	0.036	0.123	0.447	0.346	**0.526**				
6. Password self-efficacy	-0.015	0.045	0.303	0.308	0.562	**0.662**			
7. Perceived cost	0.145	0.282	0.264	0.199	0.169	0.136	**0.650**		
8. Intentions to comply	-0.055	0.109	0.426	0.340	0.551	0.665	0.135	**0.751**	
9. Actual password compliance	0.007	0.018	0.106	0.187	0.277	0.246	0.038	0.345	*

Bold values on diagonal represent square root of AVEs
*As we used a composite score to measure exposure to hacking and we used a single score to measure actual password compliance, we did not compute square root of AVE.

Table C2. Correlation Matrix (Treatment Group)

Latent variable	1	2	3	4	5	6	7	8	9
1. Exposure to hacking	-*								
2. Perceived vulnerability	0.308	**0.798**							
3. Fear of threat	0.035	0.436	**0.828**						
4. Perceived severity	0.018	0.289	0.629	**0.667**					
5. Perceived password effectiveness	-0.118	0.193	0.532	0.524	**0.691**				
6. Password self-efficacy	-0.044	0.119	0.442	0.466	0.630	**0.716**			
7. Perceived cost	0.169	0.365	0.256	0.145	0.266	0.209	**0.692**		
8. Intentions to comply	-0.110	0.184	0.471	0.405	0.602	0.769	0.197	**0.709**	
9. Actual password compliance	-0.203	-0.102	0.096	0.170	0.285	0.274	-0.108	0.137	-*

Bold values on diagonal represent square root of AVEs
*As we used a composite score to measure exposure to hacking and we used a single score to measure actual password compliance, we did not compute square root of AVE.

About the Authors

Florence Mwagwabi is a Lecturer in Information Technology at Murdoch University's Singapore campus. She holds a PhD from Murdoch University. Her major research interests include end-user information security, cross-cultural research in information systems security, usability of password authentication systems, user-generated passwords and cyber-psychology.

Tanya McGill is an Associate Professor in Information Technology at Murdoch University in Western Australia. She has a PhD from Murdoch University. Her major research interests include information system security, technology adoption, e-learning and ICT education. Her work has appeared in various journals including *Computers & Education*, *Decision Support Systems*, *Behaviour and Information Technology*, and *Journal of Computer Assisted Learning*.

Mike Dixon is a Senior Lecturer in Information Technology at Murdoch University in Western Australia. He holds a PhD from Murdoch University and an MBA in Telecommunications Management from Golden Gate University. His major research interests include information security, network security and information technology education.