Transactions on Replication Research

Conceptual Replication DOI: 10.17705/1atrr.00035 ISSN 2473-3458

Evaluating the Core and Full Protection Motivation Theory Nomologies for the Voluntary Adoption of Password Manager Applications

Salvatore Aurigemma
Computer Information Systems Department, University of Tulsa, USA
sal-aurigemma@utulsa.edu

Thomas Mattson
Robbins School of Business, University of Richmond, USA
tmattson@richmond.edu

Lori N. K. Leonard
Computer Information Systems Department, University of Tulsa, USA
lori-leonard@utulsa.edu

Abstract:

The protection motivation theory (PMT) is widely used in behavioral information security research, with multiple instantiations of the theoretical model applied in the literature. The purpose of this study is to perform a theoretical (conceptual) replication of both the core and full (PMT) nomologies in the context of voluntary password manager application use for individual home end-users. In our study, the full PMT model explained more variance than the core PMT model, but the relationships between multiple behavioral antecedents differed between the core and full PMT models, possibly due to differences in model complexity. Our findings suggest that researchers should justify the version of the PMT that they choose to use based on their research objectives with the understanding that the same variables may be significant in one version of the PMT but not significant in another version of the PMT.

Keywords: Conceptual Replication, Protection Motivation Theory, Behavioral Security, Password Manager, Voluntary Security Behavior, CBSEM

The manuscript was received 11/16/2016 and was with the authors 14 months for two revisions.

1 Introduction

There are numerous theoretical models used in the behavioral information security literature, but one of the most common is protection motivation theory (PMT) (Aurigemma, 2013). The PMT focuses on the cognitive processes by which individuals assess a threat and how they feel they can cope with that threat as leading indicators of their intent to perform a behavior (Rogers, 1975, 1983). The appraisal of the threat and coping responses results in the intention to perform (or not perform) a particular information security action (Workman, Bommer, & Straub, 2008). The PMT is attractive to information security researchers because it focuses on both a threat and a prevailing countermeasure to mitigate that threat (Crossler & Belanger, 2014; Floyd, Prentice-Dunn, & Rogers, 2000). Given the logical fit between security related behaviors and the PMT, information security researchers have suggested that the PMT has wide generalizability across many different types of behavioral information security issues (Boss, Galletta, Lowry, Moody, & Polak, 2015; Posey, Roberts, & Lowry, 2015, Warkentin, Johnston, Walden, & Straub, 2016). However, the level of generalizability associated with the PMT constructs remains an open theoretical and empirical question partially due to the many different variations of the PMT that have been used in the prior literature.

The purpose of this paper is to provide a replication of the core PMT models as used by Warkentin, Johnston, Shropshire, and Barnett (2016) and Siponen, Mahmood, and Pahnila (2014) along with the full PMT nomology as used by Boss et al. (2015) and Posey et al. (2015). This paper replicates these two different instantiations of the PMT using the voluntary adoption of password manager applications (i.e., applications used to manage a user's passwords across multiple websites and devices) for home end-users. Password managers and home end-users are interesting contexts to replicate the PMT because the adoption of password managers is completely voluntary for home end-users with minimal organizational variables to potentially confound the results. In our study, the full PMT model explained more variance than the core PMT model, but the relationships between multiple behavioral antecedents differed between the core and full PMT models due to differences in model complexity. Our findings suggest that researchers must justify theoretically the version of the PMT that they choose to use based on their research objective because the same variables (i.e., self-efficacy and response efficacy) may be significant in one version of the PMT but not significant in another version of the PMT.

2 Protection Motivation Theory

The PMT relies upon the use of fear appeals to engender threats in order to motivate protective security behaviors. Fear appeals are "a persuasive communication that attempts to arouse fear in order to promote a precautionary motivation and self-protective action" (Ruiter, Kessels, Peters, & Kok, 2014, p. 65). The PMT suggests that fear appeals motivate two cognitive processes: 1) threat appraisal and 2) coping responses. The threat appraisal is an assessment of the threat severity and personal susceptibility to that threat, whereas coping responses are assessments of the effectiveness of the potential responses and one's ability to undertake the responses. Both of these cognitive processes results in high or low protection motivations to perform (or not perform) a particular information security action (Boss et al., 2015; Workman et al., 2008).

It is important to note that a fear appeal is more than just a threatening message; Witte, Meyer, and Martell (2001) argue that successful[1] fear appeals must include both a threat appraisal and a coping response. Having the threat appraisal without the coping response in a fear appeal message typically results in an unsuccessful fear appeal (Boss et al., 2015; Witte et al., 2001). A successful threat appraisal articulates the magnitude of the threat along with the real possibility that the danger associated with the threat can occur to the participant (on a personal level). A successful coping response communicates how the prescriptive solution works, demonstrates that it is within the capability of the recipient of the message, and addresses common barriers from performing the designated response. Prior research has demonstrated that fear appeals containing these two components can activate protection motivation even with small levels of fear in the fear appeal message (Gore et al., 2015; Ruiter et al., 2014). However, high scare tactics without coupling those scare tactics with proper coping responses may not motivate protective actions (Gore et al., 2015; Witte et al., 2001).

[1] Per Ruiter et al. (2014), fear appeal messages are more appropriately classified as successful or unsuccessful rather than high versus low fear appeal messages as tested by Boss et al. (2015). Gore and Bracken (2005) show that only a marginal amount of threat is necessary in a fear appeal to motivate protective actions.

In the "core" PMT, coping responses consist of an individual's self-efficacy (belief in one's ability) to perform a security action, the perceived response efficacy (perceived effectiveness) of the required action, whereas threat appraisals capture the perception of one's vulnerability (perceived likelihood that the threat will occur) from the related security threat and the perceived severity (perceived impact of the threat) of the security threat being studied (Siponen et al., 2014; Warkentin et al., 2016). Figure 1 displays the core PMT model. In general (with a few reported exceptions), higher self-efficacy, higher response efficacy, greater perceived vulnerabilities, and greater perceived severities have been shown to lead to increased protection motivations regarding a wide variety of behavioral information security issues (Crossler, Long, Loraas, & Trinkle, 2014; Herath & Rao, 2009b; Johnston & Warkentin, 2010; Johnston, Warkentin, & Siponen, 2015; Putri & Hovav, 2014; Wall, Palvia, & Lowry, 2013; Warkentin et al., 2016; Workman et al., 2008).

While there is wide agreement in the related literature regarding the behavioral elements identified in the core PMT, researchers are not in agreement about the wide variety of theoretical extensions to the PMT that have been proposed in the prior literature. For example, Chen and Zahedi (2016) used the core PMT constructs in Figure 1 but added a higher-order construct (perceived threat) to capture threat appraisals, which are influenced by both perceived threat susceptibility and severity. Doing so, however, creates a formative versus reflective construct definition issue along with measurement issues that are still open for debate. Additionally, both Johnston and Warkentin (2010) and Johnston et al. (2015) utilize the core PMT constructs albeit with different theorized relationships. Johnston and Warkentin (2010) propose a PMT model where the threat appraisal constructs are antecedents to the coping constructs. The Johnston et al. (2015) PMT model builds off the Johnston and Warkentin (2010) model by adding both a direct effect of the threat appraisal constructs on protection motivations as well as an indirect effect through coping appraisals. Both of their models propose interesting instantiations of the PMT but are also significant deviations from the PMT's historical roots. Despite these variations, the core PMT model identified in Figure 1 presents the simplest interpretation, which has been widely used in recent behavioral information security studies such as Warkentin et al. (2016) and Siponen et al. (2014). Therefore, this paper replicates the core model of the PMT that is displayed in Figure 1.

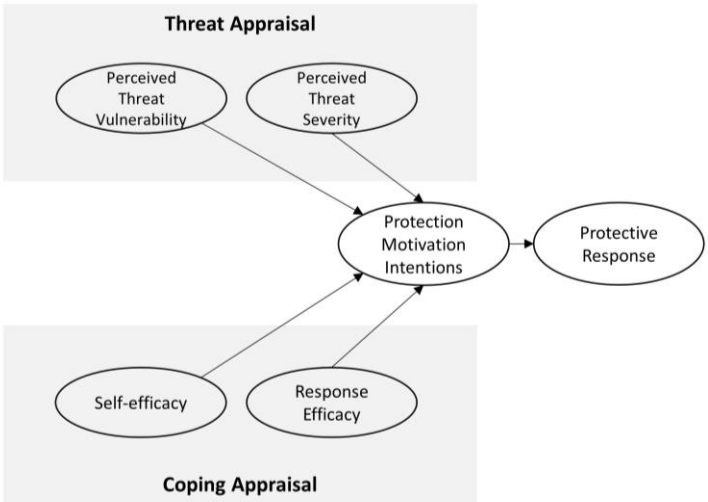

Figure 1. Core PMT Model

Recently, both Posey et al. (2015) and Boss et al. (2015) have proposed the use of a "full" PMT nomology to explain behavioral information security problems. Figure 2 displays the full PMT nomology. Both Posey et al. (2015) and Boss et al. (2015) present the full PMT nomology as a full conceptual implementation of the theory based upon their interpretation of the theoretical roots of the PMT (Rogers & Prentice-Dunn, 1997). Their full PMT nomology includes the following three factors: 1) response cost (the perceived cost

in terms of money, time, and cognitive resources) as an important addition to coping appraisal[2], 2) maladaptive rewards (any kind of reward for not partaking in the prescribed protective action) as an additional component of one's threat appraisal mechanism and 3) perceived fear resulting from a specific fear-appeal impetus. Maladaptive rewards addresses the impact of perceived benefits (implicit or explicit) of continuing risky behaviors (Floyd et al., 2000). Adding maladaptive rewards to the PMT allows a conditional proposition that would otherwise not be considered – if no threat is perceived or the reward for not taking the protective action is greater than the perceived threat, the person subject to the fear appeal may not activate their coping appraisal mechanisms and protection motivation (Boss et al., 2015).

Fear, while an inherent component of every PMT-related study that utilizes a fear appeal, has not traditionally been measured as a separate construct that directly (or indirectly) impacts protection motivation or influences other behavioral antecedents (Boss et al., 2015; Posey et al., 2015). In their full PMT nomology, Boss et al. (2015) and Posey et al. (2015) argue that perceived fear from an information security threat not only directly impacts protection motivation but also partially mediates the effects of perceived threat severity and vulnerability. Measuring fear in this manner not only provides a direct measurement of the effectiveness of the fear appeal message used for the information security threat of interest but it also allows the examination of the impact of that fear on both threat perceptions and protection motivation (Boss et al., 2015).

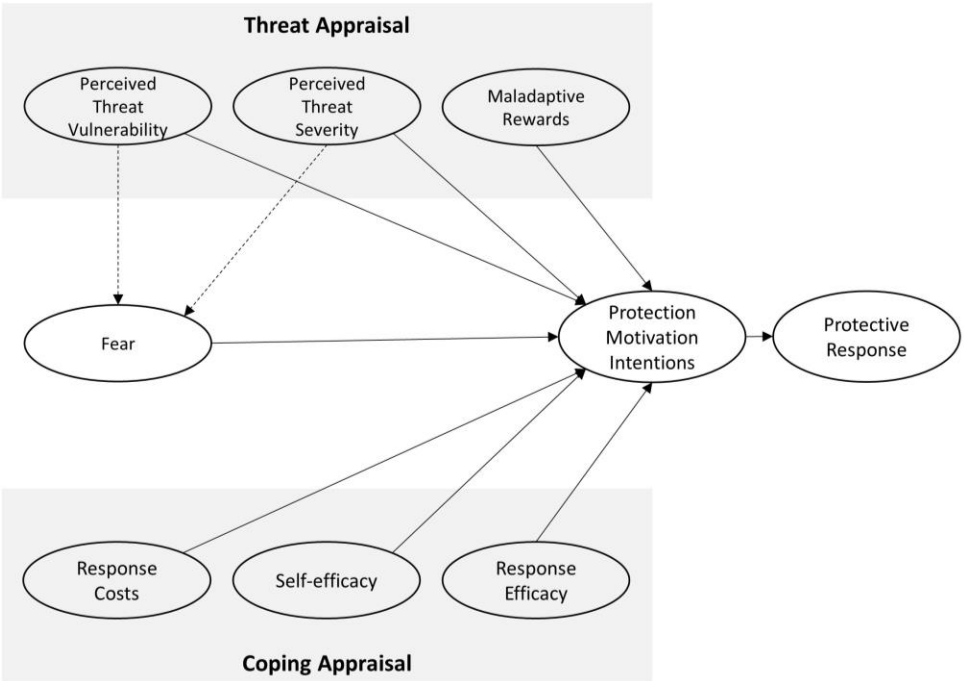

Figure 2. Full PMT Model

The full PMT nomology is a more articulated representation of the theoretical roots of the PMT, which contributes a deeper understanding of the behavioral antecedents affecting protection motivations. In doing so, however, the full PMT becomes a less parsimonious behavioral model, which leads to potential data collection issues (more and varied data need to be collected) as well as complicates future exploration of other behavioral factors that, in conjunction with PMT variables, improve understanding of protection motivation. Therefore, it is important to compare the core PMT model with the full PMT model to determine if the cost of being less parsimonious has more explanatory power in the context of the specific behavioral information security problem being investigated.

[2] Boss et al. (2015) include response costs in their declaration of the core PMT nomology. However, we agree with Posey et al. (2015) that response costs are less prevalent in the behavioral information security PMT literature and, thus, we include the response cost construct in the full nomology only.

3 Research Design and Methods

To empirically test the core and full PMT nomologies in the context of password managers, we employed a sequential two-part study of the adoption (or non-adoption) of a password manager application.[3] Part 1 consisted of presenting a poor password management fear appeal message immediately followed by a survey to capture self-reported perceptions of the factors that affect home end-user security behavior intentions. Part 2, which occurred one week after the completion of Part 1 of the study, captured actual security behavior of the participant. This process is consistent with Boss et al. (2015) and Warkentin et al. (2016) who captured both actual security behaviors and behavioral intentions.

3.1 Participants

We sampled undergraduate college students from a private university in the Midwest portion of the United States. While academics often criticize the use of college students as the sample population in research, much of that criticism comes from trying to generalize the results of student derived data to other organizational contexts (Peterson, 2001). When investigating home end-user information security practices, college students are an excellent population to study due to their extensive use of technology, familiarity with online applications, and lack of conscientiousness with their information privacy and security practices (Drennan, Sullivan, & Previte, 2006).

3.2 Constructs and Measures

We adapted pre-validated (reflective) scales from previous behavioral information security research (as documented in Boss et al. (2015)) to measure all of our latent constructs. We measured all items reflectively using 7-point Likert scales ranging from (1) strongly disagree to (7) strongly agree. Appendix A provides the items, means, standard deviations, and factor loadings. As mentioned earlier, the fear appeal is an essential part of any PMT study. In this study, we built our fear appeal based on the guidelines presented by Witte et al. (2001) and Ruiter et al. (2014). We formatted the fear appeal in a video (see Appendix B for the video link and the transcript). We developed the contents and video format of the message through a series of three pilot studies conducted with 16 Management Information Systems (MIS) students in an introductory information security course. After each pilot, we made small modifications to the video in order to ensure that the video was eliciting a successful fear appeal. The participants in the pilot studies included a mix of 50% American and 50% International students of which only three had prior working knowledge of password managers.

3.3 Primary Data Collection

A total of 372 undergraduate students were provided the opportunity to participate in this study in return for a small amount of extra credit in their course (between 1 and 2% depending on the instructor). The first part of the study provided the participants with a link to an online video that included a fear appeal message related to poor password management and an online survey to measure all of the behavioral constructs including their intent to install and use a password manager within the following week. The second part of the study was conducted one week later to ascertain whether the participants followed through with the security behavior. In part two of the study, we asked the participants whether they took the action to download and use the recommended password manager application or some other password manager. If participants indicated that they adopted a password manager, we asked several questions that could be answered only by using the "Security Challenge" tool in the password manager, which included the relative strength of their master password, total security score for all their accounts, and total number of accounts in their password manager application after initial use.

Individual survey participation was voluntary and responses were de-identified prior to data analysis. We collected a total of 286 responses for the first part of the study, which represents a 77% response rate. Three participants dropped out before part 2, which left us with 283 usable data points. We used covariance-based structural equation modeling (CBSEM) with version 23 of AMOS to evaluate construct relationships and model fit. CBSEM is an appropriate analysis method when testing proposed relationships between latent constructs of a theoretically derived, *a priori* model (Lowry & Gaskin, 2014; Raykov, 2006), which is

[3] Boss et al. (2015) compared a high and a low fear appeal message in their study. We are not attempting to compare different fear appeals in this theoretical replication. Instead, we are testing the core and full PMT nomology given a specific fear appeal that did quantifiably generate a level of fear coupled with a coping response.

the case for our study. Prior to conducting CBSEM analyses, we successfully screened the data for issues that may jeopardize the results, such as outliers, multicollinearity, non-normality, and missing data (Byrne, 2001; Kline, 2011).

3.4 Instrument Validity and Structural Path Analysis

CBSEM consists of two parts: (1) a confirmatory factor analysis (CFA) stage and (2) the structural model analysis (also known as path analysis) stage (Heck, 1998). The CFA stage assesses the quality and validity of the construct measures and is performed on the entire set of measurement items for all latent constructs simultaneously with each observed variable restricted to load on its a priori factor. We examined the average variance extracted (AVE) to ensure individual item reliability and convergent validity. Table 1 displays the measurement item loadings on their respective constructs in the factor loading column. All factor loadings were in the range of 0.666 – 0.991. While the recommended threshold for item loadings is 0.7, individual item loadings between .40 and .70 are acceptable for inclusion as long as composite reliabilities are above .70 (which they were for all constructs) (Chin, 1998). The AVE values were greater than the minimum recommended value of 0.50 in our data, which indicates that the items satisfied the convergent validity requirements.

Table 1. Confirmatory factor analysis results

Construct	CR	AVE	MSV	ASV	Fear	PMI	TSEV	PVUL	REFF	SEFF	COST	MAL
Fear	.848	.650	.236	.109	.806							
PMI	.966	.904	.187	.113	.374	.951						
TSEV	.840	.639	.236	.115	.486	.271	.800					
PVUL	.793	.563	.195	.087	.442	.139	.359	.751				
REFF	.868	.688	.355	.146	.285	.361	.457	.440	.830			
SEFF	.860	.672	.355	.170	.325	.427	.361	.263	.596	.820		
COST	.820	.604	.436	.125	-.057	-.432	-.127	.066	-.161	-.451	.777	
MAL	.908	.715	.436	.097	-.005	-.237	-.099	-.012	-.170	-.383	.660	.845

Legend: CR = Composite Reliability, AVE = Average Variance Explained, MSV = Maximum Shared Squared Variance, ASV = Average Shared Squared Variance, PMI = Protection Motivation Intention, TSEV = Perceived Threat Severity, PVUL = Perceived Threat Vulnerability, MAL = Maladaptive Rewards, REFF = Response Efficacy, SEFF = Self Efficacy, COST = Response Costs

Due to the nature of our data collection instrument, common method variance attributed to measurement method instead of the constructs of interest may bias our results (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). We took several steps to mitigate and assess the potential of common method bias per the guidance in Gefen et al. (2011) and Podsakoff et al. (2003). First, we used the security challenge to objectively determine actual use, which mitigates this problem for actual usage but not for behavioral intentions. Second, we used survey best practices to minimize the possible impact of common method bias (Dillman, Smyth, & Christian, 2014). For instance, study participation was completely voluntary, respondents were assured anonymity prior to data analysis (i.e., we removed email address identifiers to match participants with both parts of the study after data aggregation and prior to analyzing any data), and the survey instructions stated that there were no right or wrong answers so respondents could answer honestly. Third, we conducted the unmeasured latent methods construct (ULMC) approach in accordance with Richardson, Simmering, and Sturman (2009). This method compares the standardized loadings of the items on their respective constructs between CFAs with and without the ULMC marker construct. For our sample, the average difference across all items' standardized loadings was less than 0.01 with a maximum difference of 0.070. Additionally, none of the measured construct items loaded significantly on the marker construct. While the results of the ULMC analysis and the above mitigations do not completely negate the possibility of common method variance, it does suggest that it is not a major concern in our data.

To ensure the discriminant validity of the latent constructs in the research model, we examined the AVE, maximum shared squared variance (MSV), and average shared squared variance (ASV). Table 1 displays all of these values. In our data, the MSV and ASV were both less than the AVE, which is evidence of discriminant validity because the construct items load more on their respective latent variables than on other

constructs (Hair, Black, Babin, & Anderson, 2010). Based upon the criteria set forth in Jarvis et al. (2003) and Petter et al. (2007), all of the construct measures met the requirements to be considered reflective indicators of their respective latent constructs. Finally, the model fit for the CFA analysis (which includes all latent constructs) was satisfactory ($\chi2 = 419.32$, df = 247, $\chi2/df = 1.698$; CFI = 0.963; SRMR = .0424).

Following establishment of the measurement model in the CFA stage, we fit the data to the *a priori* research models as shown in Figures 1 and 2. We assessed initial model fit using multiple criteria such as chi-square, degrees of freedom, and normed chi-square ($\chi2/df$) (Heck, 1998; Kline, 2011; Raykov, 2006). To further account for the potential impact of even mild deviations from perfectly normal data distributions on the $\chi2$ calculations, we conducted Bollen-Stine (1992) bootstrapping to calculate model fit p-values, which were all above the common 0.05 threshold. However, reliance upon $\chi2$ measurements alone for model fit determination is cautioned. As such, we used one goodness-of-fit and one badness-of-fit metric to further assess overall model fit (Heck, 1998).

We used the comparative fit index (CFI) as our goodness-of-fit metric. The CFI measures model fit relative to a null model and non-centrality index. In our data, the CFI values for the core and full PMT CBSEM model evaluation were above the 0.90 (Marsh, Hau, & Wen, 2004) or the 0.95 (Hu & Bentler, 1999) recommended thresholds. We used the standardized root mean square residual (SRMR), which compares the residuals (unexplained variance) to what would be reasonably expected from a well-fitting model, as our badness-of-fit metric. In all of our models, the SRMR were below the common threshold of 0.08, which indicates good model fit (Hu & Bentler, 1999).

4 Results

4.1 Part 1: Modelling Protection Motivation

Table 2 displays the results of the CBSEM structural path analyses for the first part of this study. Model fit was satisfactory for both the core PMT ($\chi2$ / df = 1.552, CFI = 0.984, AIC = 204.156, and SRMR = .0374) and the full PMT ($\chi2$ / df = 1.649, CFI = 0.960, AIC = 561.831, and SRMR = .0442) models. Based on model fit statistics alone, the core PMT model was superior to the full PMT model with a higher CFI and a lower $\chi2$ / df, AIC, and SRMR. However, the core PMT model (SMC = 0.208) explained almost 15.1% less variance in protection motivation intentions than the full PMT model (SMC = 0.359). The increased variance explained by the full PMT model was partially due to the fact that the full PMT model has three additional variables contributing to protection motivation; two of which (fear and response efficacy) are highly significant contributors that were not contained in the core PMT model. However, since the fit statistics were still satisfactory, the full PMT model's increased variance explained and fuller antecedent explanatory value indicate a better overall model in our data. Figures 3 and 4 graphically display the results of structural path analyses.

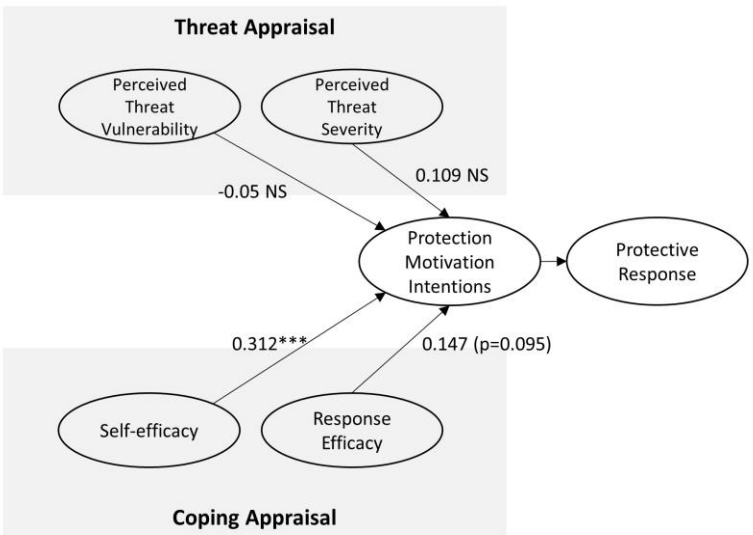

Figure 1. Core PMT Model Results

Based on the construct descriptive statistics (see Appendix A) and SEM path analysis (see Table 2), we see a few notable differences between our core and full PMT models. Our respondents reported a strong belief in the ability of a password manager to counter the poor password management threat (response efficacy mean = 5.75, standard deviation = 0.916). Yet, in our core PMT model response efficacy was a relatively weak contributor to protection motivation ($\beta = 0.147$, $p = 0.095$) while it was a stronger and more significant contributor ($\beta = 0.147$, $p < 0.05$) in our full PMT model. Additionally, while self-efficacy was the strongest antecedent of protection motivation intentions in our core model ($\beta = 0.312$, $p < 0.001$), it fell out of significance with the addition of fear and response cost, which are two behavioral antecedents with defined negative connotations. The threat appraisal constructs in our core and full PMT models were not directly significant contributors to protection motivation intentions. As shown in Table 2 and Figures 3 & 4, coping appraisals contributed most strongly to our core PMT model's relatively low explanatory power (20.8% of the variance of protection motivation intention) compared to our full PMT model.

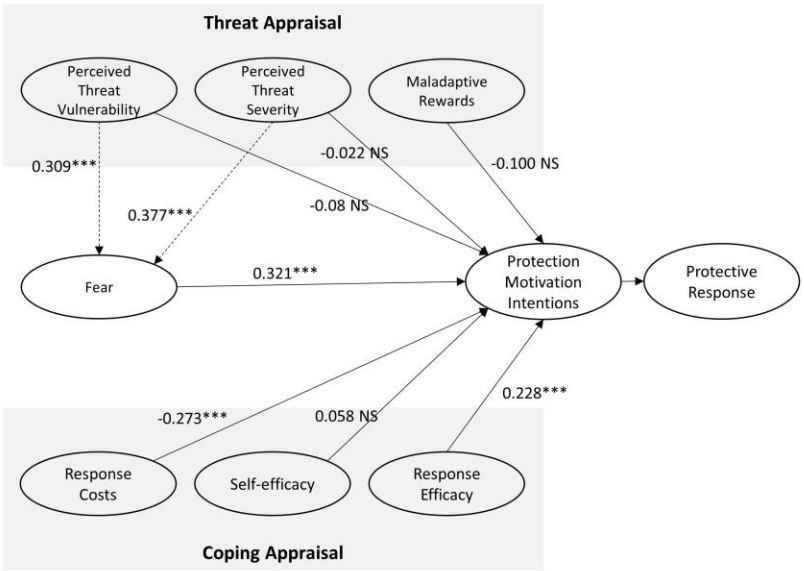

Figure 4. Full PMT Model Results

Interestingly, our full PMT model results do not match the Boss et al. (2015) high fear appeal conditions, their low fear appeal conditions, or the Posey et al. (2015) full model. Our fear path results most closely match the Boss et al. (2015) high conditions in both of their studies, but our main effects do not match either the high or the low fear appeal conditions reported by Boss et al. (2015). Unfortunately, Posey et al.'s (2015) data did not permit them to report their full PMT nomological model, so it is difficult to conclude definitively how our full model is similar to or different from their reported results.

Table 3 summarizes the path coefficients and SMC (R^2) for our study, the Warkentin et al. (2016) PLS-SEM results and the Siponen et al. (2014) model. As shown in Table 3, Warkentin et al.'s (2016) and Siponen et al.'s (2014) core PMT models yielded very different results from our study. They both found a significant positive relationship for perceived threat vulnerability and severity, whereas we found no statistically significant relationship in our core PMT model. Warkentin et al. (2016) found that both threat appraisal constructs and self-efficacy were strong and significant direct contributors that explained 82% of the variance of continued protective behavior intention. Siponen et al. (2014) also reported significant paths for the threat appraisal constructs and self-efficacy similar to Warkentin et al. (2016) but their SMC was much lower (51%). It is important to note that Siponen et al.'s (2014) model included the core PMT plus three additional constructs, which likely contributed to a larger SMC (relative to our core model) and could have impacted (positively or negatively) the coefficient sizes (and significance levels) for their reported core PMT constructs.

Table 2. SEM Model Analysis Results

SEM Model Fit Statistics	Our Core PMT	Our Full PMT	Boss Study 1 High Fear	Boss Study 1 Low Fear	Boss Study 2 High Fear	Boss Study 2 Low Fear	Posey[b]
χ2 / df	1.552	1.649	2.02	2.017	2.702	2.911	1.794
χ2	124.156	413.831	898.45	893.32	5729.01	6175.93	787.688
df	80	251	444	443	2120	2121	439
CFI	0.984	0.96	0.941	0.954	0.94	0.949	0.929
SRMR	0.0374	0.0442	0.046[a]	0.035[a]	0.062[a]	0.062[a]	0.046[c]
PMI SMC	0.208	0.359	0.881	0.419	0.777	0.672	0.351
SEM Path Analyses							
TSEV→ Fear		0.377***	0.406**	0.086 NS	0.320***	0.174*	0.290***
PVUL→ Fear		0.309***	0.507***	0.185*	0.555***	0.638***	Note d
Fear → PMI		0.321***	0.211***	0.178 NS	0.467***	(-0.353)***	0.086 NS
TSEV→ PMI	0.109 NS	(-0.022)NS	0.313***	0.015 NS	0.194*	0.084 NS	0.062 NS
PVUL→ PMI	(-0.05)NS	(-0.08)NS	0.170***	(-0.213)***	0.286*	0.028 NS	Not tested
MAL → PMI		(-0.100)NS	Not Tested	Not Tested	(-0.274)***	(-0.126)*	(-0.128) NS[e]
REFF→ PMI	0.147 (*p*=.095)	0.228**	0.170*	0.060 NS	0.237***	0.310***	0.236***
SEFF→ PMI	0.312***	0.058 NS	0.09*	0.090 NS	0.291***	(-0.202)***	Note f
COST→ PMI		(-0.273)*	(-0.294)***	(-0.491)***	(-0.387)***	(-0.090)***	(-0.190)*

*p<0.05, **p<0.01, ***p<0.001, NS: Not Significant

Legend: CFI = Comparative Fit Index, SRMR = Standardized Root Mean Residual, PMI = Protection Motivation Intention, SMC = Squared Multiple Correlation, TSEV = Perceived Threat Severity, PVUL = Perceived Threat Vulnerability, MAL = Maladaptive Rewards, REFF = Response Efficacy, SEFF = Self Efficacy, COST = Response Costs, Boss = Boss et al. (2015), Posey = Posey et al. (2015)

Notes:

a: Their reported RMSEA is a comparable badness-of-fit test; RMSEA < 0.08 is considered satisfactory.

b: Posey et al. (2015) included SETA frequency and organizational commitment, which are not included in the full PMT nomology.

c: Reported RMSEA a comparable badness-of-fit test; RMSEA < 0.08 is considered satisfactory.

d: Posey et al. (2015) dropped this path because it was highly correlated with the perceived threat severity path.

e: The Posey et al. (2015) operationalization of maladaptive rewards is very different from the Boss et al. (2015) study and our study; our items for this construct were taken from Boss et al. (2015). Therefore, these coefficients cannot be directly compared.

f: Posey et al. (2015) dropped this path because it was highly correlated with the response efficacy path.

Table 3. Core PMT SEM Model Analysis Results

Measurement	Our Core PMT	Warkentin et al. (2016)[b]	Siponen et al. (2014)
Protection Motivation Intention (PMI) Squared Multiple Correlation (SMC) or R^2	0.208	0.82	0.51[a]
Perceived Threat Severity → PMI	0.109 NS	0.414*	0.069*
Perceived Threat Vulnerability → PMI	(-0.05)NS	0.172**	0.062*
Response Efficacy → PMI	0.147 (p=.095)	0.039 NS	0.013 NS
Self-Efficacy → PMI	0.312***	0.285**	0.087**

*p<0.05, **p<*0.01,* ***p<0.001, *NS*: Not Significant

Notes:
a: Siponen et al. (2014)'s model included the core PMT and three additional constructs, including two strongly-significant contributors that likely had a sizable impact on SMC and the strength of construct coefficients. The results as shown do allow an examination of the path significance compared to the present and Warkentin et al. (2106) study.
b: The Warkentin et al. (2016) study used PLS-SEM and not CBSEM.

In our full PMT model, the most significant contributor to the participants' protection motivations was fear. Our respondents reported a mild sense of fear about the password threat (mean = 4.71, standard deviation = 1.22), which provides empirical support to the Ruiter et al. (2014) finding that protection motivation can be activated by employing even small amounts of fear in a fear appeal. None of the threat appraisal constructs (perceived threat severity, vulnerability, maladaptive rewards) in our full PMT nomology showed strong, significant effects on protection motivation intentions, which is consistent with our results from the core PMT model. However, the findings for the coping appraisal constructs is quite different between our core and full PMT models. Whereas in our core PMT model self-efficacy had a strong positive effect and response efficacy did not, these results were flipped in the full PMT model. In the full PMT model, the effect of self-efficacy was suppressed by the inclusion of the two negative-valence constructs (response costs and fear). Additionally, while self-efficacy diminished in explaining intentions, respondent's belief in the efficacy of password managers emerged as the strongest of the positive-valence coping mechanisms.

Although neither perceived threat severity nor vulnerability were significant direct contributors to protection motivations, the full PMT nomology posits that these two variables are at least partially mediated by fear. In order to test for mediation in the full PMT model, we used the bootstrapping method described in Hayes (2009) and illustrated in Vance, Lowry, and Eggett (2015). Table 4 shows the results of the bootstrapping analysis using 5000 resamples. These results indicate that fear does partially mediate the impact of both perceived threat severity and vulnerability on protection motivation intentions.

Table 4. Bootstrapped CI Tests for Full and Partial Mediation in the Full PMT Model

	Mediation Test (ab)			**Full/Partial Mediation Test (c')**			
Variable	**2.5% lower bound**	**97.5% upper bound**	**Zero included?**	**2.5% lower bound**	**97.5% upper bound**	**Zero included?**	**Type of Mediation**
Perceived Threat Severity	0.106	0.368	No	-0.177	0.126	Yes	Partial
Perceived Threat Vulnerability	0.062	0.3	No	-0.253	0.054	Yes	Partial

4.2 Part 2: Actual Behaviors and Inhibiting and Enabling Factors

The evaluation of the structural model in part 1 of the study helped clarify the relationships between the behavioral antecedents of the core and full PMT nomology based on self-reported behavioral intentions from the sample population. Part 2 of our study provided a measure of how many participants actually followed-through and used a password manager, which is consistent with Boss et al.'s (2015) measure of actual usage. However, from our reading of Boss et al. (2015) it is unclear how they estimated beta coefficients from the intention construct to the actual use construct given their small sample sizes, particularly in their high fear appeal groups. Our sample size of 283 coupled with the binary outcome variable that we used for actual use made using CBSEM problematic for this path. As such, we analyzed these data more descriptively.

Of the 283 participants in our study, 38 (13.4%) installed and used the recommended password manager (LastPass). The almost unanimous reason given for deciding to install and use the password manager was because the tool is effective at improving poor password management practices. Participants in Part 2 of the study were also asked about their intentions to use password managers in the future. A comparison of the behavioral intentions scores for Part 1 (mean = 5.43, n = 38, standard deviation = 1.32) and Part 2 (mean = 5.40, n = 38, standard deviation = 1.58) for this group show no statistical differences (t = 0.181, df = 37, p = 0.858). However, it is notable that the Part 1 behavioral intentions scores for those that did not install a password manager (mean = 4.05, n = 245, standard deviation = 1.43) is significantly lower than those that did (mean = 5.43, n = 38, standard deviation = 1.32).

We then analyzed the behavioral intentions scores for the group of participants that chose not to use a password manager provides. The Part 1 behavioral intentions scores (mean = 4.05, n = 245, standard deviation = 1.43) showed effectively neutral intentions to install and use a password manager, which played out in only a small percentage of participants actually performing the recommended security behavior. However, comparing the results of the Part 1 behavioral intentions scores with the Part 2 scores (mean = 4.66, n = 245, standard deviation = 1.48) showed a statistically significant increase in the same population's intention to use a password manager in the future (t = -7.02, df = 244, $p < 0.001$), which may potentially result in additional protective behavior adoption in the future.

5 Discussion and Conclusion

Although the PMT started out as a single theory when it was first formulated (Rogers, 1975, 1983), behavioral information security researchers have applied different variations of the PMT to explain a variety of behavioral information security problems (Aurigemma, 2013; Crossler & Belanger, 2014; Herath & Rao, 2009b; Johnston & Warkentin, 2010; Lee, Larose, & Rifon, 2008; Liang & Xue, 2010). While the core PMT model is still frequently used, the full PMT model presented by Boss et al. (2015) and Posey et al. (2015) offers an extended, arguably more theoretically comprehensive nomological net with the incorporation of response costs, fear, and maladaptive rewards.[4] In our study, we applied the core and full PMT nomologies to the longstanding security problem of poor password management in order to uncover factors that influence home end-user intentions and actual adoption of a password manager application.

Even though the difference in variance explained between our core and full PMT models may suggest that future research should always build off the full PMT nomology, we do not make that recommendation. Which version of the PMT is theoretically justified depends partially on the research objective. For example, one goal of the Boss et al. (2015) paper was to explore the research opportunities and gains afforded by measuring the impact of different fear-appeal manipulations on users' behaviors. In this case, the manipulation and measurement of fear is a centerpiece of the research goal and justifies, if not requires, the use of the full PMT. In comparison, the goal of the Siponen et al. (2014) paper was to present and test a multi-theory model of employee Information Security Policy (ISP) compliance across a range of security threats and actions included in the respondents' security policies. In the case of Siponen et al. (2014), they captured cross-sectional behavioral data from four real organizations to test their integrated model. Siponen et al. (2014) did not directly manipulate or capture fear in their study. Instead, they relied upon the

[4] While the importance of the fear appeal in the PMT-related literature is widely accepted, there is some research that questions the importance of fear (one of the components of a fear appeal) as a behavioral motivator. Warkentin, Johnston, Walden, and Straub (2016) recently conducted a study that examined the impact of fear appeals on participants using fMRI data. They found that while fear appeals activated threat and threat response assessments, they found no evidence of an actual fear response. This finding is in contrast with Boss et al. (2015), Posey et al. (2016), and our study (albeit using significantly different research methods).

documented activities of the employees' organizations security awareness and training education programs to provide organization-specific fear appeals. Although Siponen et al. (2014) did not directly manipulate or measure fear in their study, they were still able to incorporate and evaluate the core PMT constructs in their integrated model based upon the specific goals of their research, which were different from the goals of Boss et al.'s (2015) paper. Therefore, it would be ill-advised to claim that Siponen et al.'s (2014) PMT model is an inferior model simply because they did not use the nomology proposed by Boss et al. (2015) and Posey et al. (2015).

In our study, both the core and full PMT models performed rather poorly in explaining the variance in participant protection motivation intentions relative to the previously published research. One possible reason for this disparity is that the security threats and actions were significantly different in our study from the comparison studies. In the Warkentin et al. (2016) study, for instance, participant data was captured over time for initial installation and continued use of a simulated anti-malware program. In their study, participants voluntarily installed a security program that reminded them to use the software at least weekly. The level of effort required by the participants was highest in the beginning of their study when voluntarily visiting the software download page and installing the software. Continued use of the software required the students to approve the "scanning" of their computer with the software when prompted. The malware threat and associated security actions in their study are very different from those experienced by participants in our study. Our study directly recommended but did not provide a prompt to actually install and use a password manager.

Furthermore, home-end users may be more aware of a threat of a virus relative to the threat associated with reusing a password or employing a relatively weak password (Huth, Orlando, & Pesante, 2013; Zeltser, 2015). Additionally, we suggest that using a password manager is a sufficiently different security action from anti-malware applications in the sense that there is a potentially steep initial learning curve and a fairly high setup cost associated with adopting password managers before the applications become easy to use and useful. This threat context is quite different from the anti-malware (Boss et al., 2015, Warkentin et al., 2016) and data backup contexts (Boss et al., 2015), because there typically is not a high learning curve or an initially high set up cost associated with installing and using those types of applications over time.

The Boss et al.'s (2015) variance explained in both of their fear appeal groups across their two studies was significantly higher than the reported variance explained in our full PMT nomology. One possible explanation for this difference is that the Boss et al. (2015) studies involved repeated measures with repeated security fear appeal messages being presented to participants during use of their computing devices. In the context of anti-malware and data backups, the repeated fear appeal message approach is reasonable. Our study, however, is more reflective of a health-related public service advisory (PSA) type of fear appeal where our threat message does not occur on a regularly recurring basis. Our message introduces the fear appeal to participants, which for many of our participants may have been their first exposure to the threat and the coping mechanism. Additionally, our fear appeal was relatively short and non-recurring which, coupled with our different security related action, may explain the difference in variance explained and path coefficient differences from the comparison studies.

Interestingly, Boss et al. (2015) manipulated fear appeals in their quasi-experimental study whereas Posey et al. (2015) and our study did not manipulate fear appeals. This controlled manipulation allowed Boss et al. (2015) to test the impact of the PMT constructs using different fear appeals, which they categorized as high and low. However, the Boss et al. (2015) study did not have a control group in their quasi-experiment so it is difficult to determine how their low and high fear appeal groups differed from a control group. Both groups in their two studies were manipulated. Nevertheless, different constructs may become more important or less important depending on the threat message or the coping response contained in different fear appeals. Therefore, it is possible that the differences in the full PMT nomology reported by Posey et al. (2015) and our paper may be attributable to characteristics of the fear appeal in addition to (or instead of) the differences in the security action that was investigated.

Irrespective of our explanation for why our results vary from the results reported for other studies using the core and full PMT models, our different results do suggest that researchers should be cautious about universally applying either instantiation of the PMT to all behavioral information security threats and actions. It may very well be that both the core and full PMT models are more capable of explaining the variance with the types of security behaviors examined in the Warkentin et al. (2016) and Boss et al. (2015) papers and less capable for security actions like using password managers. Password managers are not as familiar to users, have higher initial setup costs, and/or do not provide repeated fear appeal messages and prompts. Given these differences, our results suggest further replication of these models is needed using different

types of security actions, different types of research designs, and different types of fear appeals. It is not possible to conclude that our theoretical replication study is better or worse than the previously published papers because each has its own strengths and weaknesses. However, the different path coefficients and variance explained does suggest that there is a scientific need to further replicate both the core and full PMT nomologies.

There are several limitations with our replication study. Our study only considered a pre-set time interval between the two surveys, which may have not been enough time for some of our research participants to act on the fear appeal. An interesting future study may investigate greater time spacing between when intentions are measured and when actual behaviors are determined. Ideally, a longer longitudinal study with more realistic organizational manipulations would be useful in measuring behavioral intentions, actual adoptions, and continued usage over a much longer time period would help reveal further insights into the core and full PMT models. Additionally, our study examines the performance of both PMT models (core and full) using a single fear appeal message. Therefore, our reported differences between Boss et al. (2015) may be a function of the fear appeal. Future research may offer an empirical replication of the Boss et al. (2015) instead of our theoretical replication. Those two studies can then be interpreted in tandem to further contextualize our reported results. Finally, we measured maladaptive rewards using the construct definition and items from Boss et al. (2015), which are very different from the conceptualization and construct measurement items from Posey et al. (2015). Posey et al.'s (2015) operationalization of maladaptive rewards measures intrinsic and extrinsic rewards, which may modify the relative size and magnitude of the effect of maladaptive rewards on protection motivation. Future assessments should seek to gain more comprehensive understanding of maladaptive rewards for use in PMT-related studies.

References

Aurigemma, S. (2013). A Composite framework for behavioral compliance with information security policies. *Journal of Organizational and End User Computing*, 25(3), 32-51.

Bollen, K. A., & Stine, R. A. (1992). Bootstrapping goodness-of-fit measures in structural equation models. *Sociological Methods & Research*, 21(2), 205-229.

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

Byrne, B. M. (2001). Structural equation modeling with AMOS, EQS, and LISREL: comparative approaches to testing for the factorial validity of a measuring instrument. *International Journal of Testing*, 1(1), 55-86.

Chen, Y., & Zahedi, F. M. (2016). Individuals' internet security perceptions and behaviors- polycontextual contrasts between the United States and China *MIS Quarterly*, 40(1), 205-222.

Chin, W. W. (1998). Commentary: Issues and opinion on structural equation modeling. *MIS Quarterly*, 22(1), vii-xvi.

Crossler, R., & Belanger, F. (2014). An extended perspective on individual security behaviors: protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database*, 45(4), 51-71.

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

Dillman, D. A., Smyth, J. D., & Christian, L. M. (2014). *Internet, phone, mail, and mixed-mode surveys: The tailored design method*. Hoboken. New Jersey: John Wiley & Sons, Inc.

Drennan, J., Sullivan, G. M., & Previte, J. (2006). Privacy, risk perception, and expert online behavior: an exploratory study of household end users. *Journal of Organizational and End User Computing*, 18(1), 1-22.

Floyd, D. L., Prentice-Dunn, S., & Rogers, R. W. (2000). A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology*, 30(2), 407-429.

Gefen, D., Straub, D. W., & Rigdon, E. E. (2011). An update and extension to SEM guidelines for admnistrative and social science research. *MIS Quarterly*, 35(2), iii-xiv.

Gore, T. D., & Bracken, C. C. (2005). Testing the theoretical design of a health risk message: reexamining the major tenets of the extended parallel process model. *Health Education & Behavior*, 32(1), 27-41.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate data analysis: A global perspective*. Upper Saddle River, NJ: Pearson.

Hayes, A. F. (2009). Beyond Baron and Kenny: statistical mediation analysis in the new millennium. *Communication Monographs*, 76(4), 408-420.

Heck, R. H. (1998). Factor analysis: exploratory and confirmatory approaches. In G. Marcoulides (Ed.), *Modern Methods for Business Research* (pp. 177-215). Mahwah, NJ: Erlbaum.

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

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

Hu, L., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling*, 6(1), 1-55.

Huth, A., Orlando, M., & Pesante, L. (2013). Password Security, Protection, and Management. Retrieved from https://www.us-cert.gov/security-publications/password-security-protection-and-management.

Jarvis, C. B., Mackenzie, S. B., & Podsakoff, P. M. (2003). A critical review of construct indicators and measurement model misspecification in marketing and consumer research. *Journal of Consumer Research*, 30(2), 199-218.

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

Johnston, A., Warkentin, M., McBride, M., & Carter, L. (2016). Dispositional and situational factors: Influences on information security policy violations. *European Journal of Information Systems*, 25(3), 231-251.

Johnston, A., 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.

Kline, R. B. (2011). *Principles and practice of structural equation modeling*. New York, NY: Guilford Press.

Lee, D., Larose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Behavior & Information Technology*, 27(5), 445-454.

Leventhal, H. (1970). Findings and theory in the study of fear communications. In L. Berkowitz (Ed.), *Advances in Experimental Social Psychology* (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.

Lowry, P. B., & Gaskin, J. (2014). Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Transactions on Professional Communication*, 57(2), 123-146.

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.

Marsh, H. W., Hau, K.-T., & Wen, Z. (2004). In search of golden rules: Comment on hypothesis-testing approaches to setting cutoff values for fit indexes and dangers in overgeneralizing Hu and Bentler's (1999) findings. *Structural Equation Modeling*, 11(3), 320-341.

McIntosh, D. N., Zajonc, R. B., Vig, P. S., & Emerick, S. W. (1997). Facial movement, breathing, temperature, and affect: Implications of the vascular theory of emotional efference. *Cognition & Emotion*, 11(2), 171-195.

Milne, S., Sheeran, P., & Orebell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, 30(1), 106-143.

Osman, A., Barrios, F. X., Osman, J. R., Schneekloth, R., & Troutman, J. A. (1994). The pain anxiety symptoms scale: Psychometric properties in a community sample. *Journal of Behavioral Medicine*, 17(5), 511-522.

Peterson, R. A. (2001). On the use of college students in social science research: Insights from a second-order meta-analysis. *Journal of Consumer Research*, 28(3), 450-461.

Petter, S., Straub, D., & Rai, A. (2007). Specifying formative constructs in information systems research. *MIS Quarterly*, 31(4), 623-656.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879-903.

Posey, C., Roberts, T. L., & 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.

Putri, F. F., & Hovav, A. (2014). Employees compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory. Paper presented at the Proceedings of the European Conference on Information Systems 2014, Tel Aviv, Israel.

Raykov, T., & Marcoulides, G.A. (2006). *A first course in structural equation modeling*. Lawrence Erlbaum.

Richardson, H. A., Simmering, M. J., & Sturman, M. C. (2009). A tale of three perspectives: Examining post hoc statistical techniques for detection and correction of common method variance. *Organizational Research Methods*, 12(4), 762-800.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, 91(1), 93-114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In B.L. Cacioppo & L.L. Petty (Eds.), *Social Psychophysiology: A Sourcebook* (pp. 153-176), London: Guilford.

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. In D. S. Gochman (Ed.), *Handbook of Health Behavior Research* (pp. 113-132). New York, NY: Plenum Press.

Ruiter, R. A. C., Kessels, L. T. E., Peters, G.-J. Y., & Kok, G. (2014). Sixty years of fear appeal research: Current state of the evidence. *International Journal of Psychology*, 49(2), 63-70.

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

Vance, A. O., Lowry, P. B., & Eggett, D. (2015). Increasing accountability through user-interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Quarterly*, 39(2), 345-366.

Wall, J. D., Palvia, P., & Lowry, P. B. (2013). Control-related motivations and information security policy compliance: The role of autonomy and efficacy. *Journal of Information Privacy & Security*, 9(4), 52-79.

Warkentin, M., Johnston, A., Shropshire, J., & Barnett, W. D. (2016). Continuance of protective security behavior: A longitudinal study. *Decision Support Systems*, 92, 25-35.

Warkentin, M., Johnston, A. C., Walden, E., & Straub, D. W. (2016). Neural correlates of protection motivation for secure IT behaviors: An fMRI examination. *Journal of the Association for Information Systems*, 17(3), 194-215.

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communication Monographs*, 59(4), 329-349.

Witte, K. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication*, 1(4), 317-342.

Witte, K. (1998). Fear as motivator, fear as inhibitor: Using the extended parallel process model to explain fear appeal successes and failures. In P. A. Anderson & L. K. Guerrero (Eds.), *Handbook of Communication and Emotion: Research, Theory, Application, and Contexts* (pp. 423-450). San Diego, CA: Academic Press.

Witte, K., Meyer, G., & Martell, D. (2001). *Effective health risk messages: A step-by-step guide.* Sage Publications.

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.

Zeltser, L. (2015). Password Managers. Retrieved from https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201310_en.pdf .

Appendix A. Construct Definitions and Measurement Items

Construct	Definition from Boss et al. (2015)	Survey Question/Measurement Item	Item	Factor Load	Mean	Std Dev
Protection Motivation Intention	Self-reported intention to perform the security behavior.	I intend to use a password manager in the next week.	BINT1	0.95	4.24	1.52
		I predict I will use a password manager in the next week.	BINT2	0.98	4.23	1.54
		I plan to use a password manager in the next week.	BINT3	0.93	4.25	1.57
Fear	A negatively valenced emotion representing a response that arises from recognizing danger. This response may include any combination of apprehension, fright, arousal, concern, worry, discomfort, or a general negative mood, and it manifests itself emotionally, cognitively, and physically (Leventhal, 1970; McIntosh, Zajonc, Vig, & Emerick, 1997; Osman, Barrios, Osman, Schneekloth, & Troutman, 1994; Witte, 1992, 1996, 1998)	I am worried about the prospect of having my online account passwords stolen and abused by cybercriminals.	FEAR1	0.78	4.95	1.31
		I am frightened about the prospect of having my online account passwords stolen and abused by cybercriminals.	FEAR2	0.85	4.82	1.37
		I am anxious about the prospect of having my online account passwords stolen and abused by cybercriminals.	FEAR3	0.79	4.42	1.48
Self-efficacy	"The perceived ability of the person to actually carry out the adaptive [coping] response" (Floyd et al., 2000, p. 411; Maddux & Rogers, 1983)	Password manager software is easy to use.	SE1	0.82	5.27	1.11
		Password manager software is convenient to use.	SE2	0.83	5.15	1.18
		I am able to use password software without much effort.	SE3	0.81	5.14	1.17
Maladaptive Rewards	The general rewards (intrinsic and extrinsic) of not protecting oneself, contrary to the fear appeal (Floyd et al., 2000; Rogers & Prentice-Dunn, 1997)	Using a password manager would slow down the speed of my access to the Internet.	MAL1	0.67	3.52	1.51
		Using a password manager would slow down my computer.	MAL2	0.88	3.01	1.35
		Using a password manager would interfere with other programs on my computer.	MAL3	0.93	3.05	1.38
		Using a password manager would limit the functionality of computer.	MAL4	0.88	2.94	1.31
Response Costs	"Any costs (e.g., monetary, personal, time, effort) associated with taking the adaptive coping response" (Floyd et al., 2000, p. 411)	There is too much work associated with trying to increase the security of my online account. passwords through the use of a password manager application	COST1	0.84	5.77	1.01
		Using a password manager application on my computer would require considerable investment of effort other than time.	COST2	0.88	5.75	0.97
		Using a password manager application would be time consuming.	COST3	0.76	5.73	1.11

Construct	Definition from Boss et al. (2015)	Survey Question/Measurement Item	Item	Factor Load	Mean	Std Dev
Perceived Threat Vulnerability	"How personally susceptible an individual feels to the communicated threat" (Milne, Sheeran, & Orebell, 2000, p. 108)	My online account passwords are at risk of being stolen and abused by cyber-criminals	PVUL1	0.85	4.93	1.33
		It is likely that my online account passwords will be stolen and abused by cyber-criminals.	PVUL2	0.70	4.10	1.36
		It is possible that my online account passwords will be stolen and abused by cyber-criminals.	PVUL3	0.69	5.17	1.36
Perceived Threat Severity	"How serious the individual believes that the threat would be" to him- or herself (Milne et al., 2000, p. 108)	If my online account passwords were stolen and abused by cyber-criminals, it would be severe.	TSEV1	0.71	5.81	1.18
		If my online account passwords were stolen and abused by cyber-criminals, it would be serious.	TSEV2	0.92	6.07	1.02
		If my online account passwords were stolen and abused by cyber-criminals, it would be significant.	TSEV3	0.76	5.94	1.20
Response Efficacy	"The belief that the adaptive [coping] response will work, that taking the protective action will be effective in protecting the self or others" (Floyd et al., 2000, p. 411; Maddux & Rogers, 1983)	Password manager applications work to protect my online account passwords from being stolen and abused by cyber-criminals.	REFF1	0.82	5.77	1.01
		Password manager applications are an effective solution to protect my online account passwords from being stolen and abused by cyber-criminals.	REFF2	0.71	5.75	0.97
		When using a password manager application, online passwords are more likely to be protected from being stolen and abused by cyber-criminals.	REFF3	0.80	5.73	1.11

Appendix B. Video Script

Welcome to this video on password manager applications, why you should use one, and how to get started quickly and for free. Following is a short, 2-minute animation that does a great job at discussing the problems we all face with passwords and what we can do about it.

[The following script is from the EFF's video about using password managers found at https://ssd.eff.org/en/module/animated-overview-using-password-managers-stay-safe-online]

You get a lot done on the internet that means you probably have a lot of accounts with tons of websites right? But do you use the same password on all of them? Or do you almost use the same password and change it a little bit for each site? Well, that's a problem.

If you use the same password on every website and just one of these websites gets broken into by cybercriminals and there is always one site you use that is not secure then those thieves could get the passwords of everyone on that site. Then they can use them to break into all those other accounts.

These kinds of break-ins happen far more often than you think. Sometimes they even happen without the hacked website knowing. So don't reuse your passwords!

But wait! If you have lots of website accounts and each of them now needs a unique password how can you possibly remember them all? Aren't we supposed to keep our passwords in our heads and never write them down? Writing them down is actually not that bad of an idea. If you use lots of passwords write them down and keep them somewhere safe like your wallet then you will at least know if your passwords go missing or get stolen, that's more than you might know if you use just one password everywhere and then a website you use is silently hacked and even a safer plan though is to use a password manager.

Password Managers are programs you can download for your phone or computer, it will create, store and even automatically fill in unique passwords on websites and other online services. It can keep all of your account details safe and synchronize them between all of your devices. So, you never have to remember all those passwords again. You can search for password managers reviews so you can find out what the most secure net users out there prefer. Use password managers to resist the temptation to use one password on all your sites. Remember it's a trap.

There is one catch with password managers though, password managers do need a password for themselves. One that you use to type into the password manager to access all of your other passwords. You will want that password to be extra secure but easy to remember because it is the one password you won't be able to store in your password manager. But that one password will keep you a lot safer in a sometimes dangerous net. [End EFF video script]

That's an interesting video… but maybe it doesn't apply to you? Perhaps you don't have many passwords to worry about. Let's think about it – what are some of your accounts that need passwords? Maybe you have some social media accounts? Did you find a great idea on Pinterest about taking Vine videos of the latest Starbucks drink, then taking a picture of the cup and posting it on Snapchat, Tumblr, Facebook and Twitter while simultaneously telling their 5 different friend groups on GroupMe, Kik, and WhatsAp to please like their Instagram photo of this once-in-a-lifetime event.

Maybe you do some online shopping? Holiday shopping on Amazon or Etsy, Target, ebay, or maybe Walmart for the cheap stuff. And don't forget you have to pay for all of those purchases by putting in your credit card.

And when you are hard at work, you might need a break with some of your many online entertainment options (feel like binge watching Game of Thrones, anyone?). And don't forget your multiple home and work email accounts that you have to constantly check all day long.

Come to think of it… when you start counting all the applications that you use that require passwords, knowing that each one is supposed to have a strong unique password you probably have A LOT more passwords to deal with than originally thought.

So, OK, maybe there is a password management problem we all have to deal with. But are password managers a safe solution? The answer is generally yes. While there will always be some level of risk associated with locking all of your passwords up in one file, even if it is highly encrypted, the benefits of using a password manager are considered much greater than the alternative of using, and reusing, weak or predictable passwords.

The US Department of Homeland Defense's Computer Emergency Readiness Team and the internationally recognized information security training and awareness organization, the SANS institute, both strongly recommend the use of password managers. As well as just about every major technology, news, and consumer advocacy group.

Fortunately, there are many password manager applications to choose from with prices starting as low as FREE. For example, three popular password managers are LastPass, 1Password, and Dashlane.

All good password managers provide similar functionality, such as:

- Importing existing passwords from your web browsers. Many of us use more than one web browser sometimes on different computers, which can be very unsafe.
- Password managers also not only help you easily create strong and unique passwords for each site, but automatically capture login credentials when logging into a site for the first time.
- Another important feature in a good password manager is the ability to check the security level of all of your current passwords. For example, LastPass and 1Password both allow you to check all your passwords to identify all the weak, old, reused and yes, even known COMPROMISED accounts.

For example, if you had a LinkedIn, Yahoo, or Snapchat account any time in the past several years, there is a real possibility that hackers stole your account credentials. Having a password manager that keeps track of major account hacks, so that you don't have to, is a great benefit.

Password managers sound useful, so what's the next step? First, you are strongly recommended to start using a password manager as soon as possible. We recommend LastPass because it is well established and offers great password management functionality and its FREE. Just got to www.lastpass.com to download a version for your Mac, PC, or even Linux. After you install the desktop version of LastPass, you should be prompted to import your current web browser account passwords. You should definitely do this because it not only automatically populates some of your passwords, but makes you safer by getting rid of these passwords in the much-less-secure browser password storage. After you have LastPass populated with some passwords, run the Security Challenge; this will test the strength of your Master Password and all your individual passwords. The security challenge will identify all your compromised, weak, reused or old passwords and then even help you with the process of changing them to strong, secure passwords.

In summary, we all have many account passwords that we need to protect. The simple truth is that it's too hard for most of us to create and remember a lot of passwords, even bad passwords. All of our passwords should be strong and unique, which makes memorizing our passwords even harder! Strong passwords should be 12 characters or longer with mixed letters, numbers, and special characters.

Password managers allow us to create and remember one strong, unique password, our Master Password, which unlocks all our other account passwords. Security experts recommend using password managers because they are safe and effective. Whether you use a free password manager like LastPass or a paid version like 1Password, the investment is well worth it!

[Note: the video for this script is posted at https://youtu.be/ru3JXo7YoVc]

About the Authors

Salvatore Aurigemma. Salvatore (Sal) Aurigemma is an Assistant Professor of Computer Information Systems in the Collins College of Business at the University of Tulsa. His research explores employee information security policy compliance, improving end-user and small business information security practices, and end-user computing focusing on business spreadsheet error detection.

Thomas Mattson. Thomas Mattson is an Assistant Professor of Management at the University of Richmond. His research focuses on social interactions in electronic networks of practice, virtual communities of practice, and other electronic social structures along with assorted issues to information security. Prior to joining academia, he worked as a technology and management consultant designing and building databases and applications for firms in the consumer packaged goods, accounting, and financial industries.

Lori Leonard. Lori Leonard is a Collins Endowed Professor and Professor of Computer Information Systems at the University of Tulsa. She received her Ph.D. from the University of Arkansas and is a member of the Association for Information Systems and the Decision Sciences Institute. Her research interests include electronic commerce, ethics in computing, C2C commerce, online trust, and information security. Her publications have appeared in *Journal of the Association for Information Systems*, *Journal of Computer Information Systems*, *Industrial Management & Data Systems*, *Journal of End User Computing*, *Information & Management*, *Electronic Markets*, *Journal of Organizational Computing and Electronic Commerce*, *Journal of Electronic Commerce in Organizations*, *Journal of Business Ethics*, as well as in other journals, and *Proceedings* of various Conferences.