Association for Information Systems
AIS Electronic Library (AISeL)

PACIS 2018 Proceedings

Pacific Asia Conference on Information Systems (PACIS)

6-26-2018

Understanding Users' Information Security Awareness and Intentions: A full Nomology of Protection Motivation Theory

Farkhondeh Hassandoust
ICL Graduate Business School, ferryhassandoust@icl.ac.nz

Angsana Techatassanasoontorn
Auckland University of Technology, angsana@aut.ac.nz

Understanding Users' Information Security Awareness and Intentions: A full Nomology of Protection Motivation Theory

Research-in-Progress

Farkhondeh Hassandoust
ICL Graduate Business School
Auckland, New Zealand
ferryhassandoust@icl.ac.nz

Angsana A. Techatassanasoontorn
Auckland University of Technology
Auckland, New Zealand
angsana@aut.ac.nz

Abstract

Information security (InfoSec) violations have negative organisational and personal impacts. Studies that examine key factors to motivate individuals to change their security related behaviours are important to promote safe computing. This paper presents a full nomology of the protection motivation theory (PMT) to study the impact of users' InfoSec awareness on their security protection intention. It contributes to a better understanding of users' InfoSec awareness through an examination of the impact of security education, training and awareness (SETA) programme on InfoSec threat and countermeasures awareness and the role of InfoSec awareness as an antecedent to the cognitive processes associated with coping and threat appraisals. In addition, this research contributes to extend PMT by investigating the role of fear and maladaptive rewards in explaining InfoSec behaviours.

Keywords: Information security awareness, fear-appeal, protection motivation theory, security protection intention

Introduction

Due to the pervasive usage of the Internet worldwide and the presence of information security (InfoSec) violations on the Internet, users' InfoSec awareness is a critical first step to achieve the safe and secured environment globally. Recent research has attempted to identify effective approaches to motivate users to protect their information assets with a particular emphasis on InfoSec behaviours of individuals within an organisational context (Boss et al., 2017; Johnston & Warkentin, 2010). Despite the importance of appropriate InfoSec behaviours in organisations, users' personal InfoSec practice still remains a significant concern and the current literature on InfoSec does not pay enough attention to how users deal with InfoSec threats in their personal lives.

According to Hanus and Wu (2016), more than 40% of computer users globally were victims to cybercrimes such as virus, phishing, social engineering, worm or malware attacks and it is estimated that more than half of these users were not completely sure whether their computers were free of any kind of viruses. In addition, almost one third of users do not recognise the potential risks associated with not properly protecting themselves and their information on the Internet. This evidence suggests that, regardless of all technological developments in the InfoSec domain, providing InfoSec training to improve users' awareness and their security protection regarding potential threats remains a priority to achieve safe and secured environments. Although previous research examined the role of security education, training and awareness (SETA) (D'Arcy et al., 2009), the focus was on deterring individuals from fear of organisational sanctions rather than motivating them to engage in security behaviours based on their own calculations of consequences of security threats. Drawing on Protection Motivation Theory (PMT), this study aims to extend the current body of knowledge by investigating the role of SETA programmes on users' awareness and subsequent coping and threat appraisals. This study offers an explanation that links InfoSec awareness with intentions to practice InfoSec behaviours.

In recent years, InfoSec literature has shifted from relying on general deterrence theories to having a stronger emphasis on PMT. General deterrence theories emphasise the concept of command and control, whilst PMT mostly focuses on using persuasive messages to warn people of a threat and explain countervailing measures and protective behaviours. PMT is applicable to InfoSec contexts, where users require additional motivation in order to protect their information assets (Boss et al., 2017; Floyd, Prentice-Dunn, & Rogers, 2000). Several InfoSec studies (e.g., Dang-Pham & Pittayachawan, 2015; Dinev & Hu, 2007; Hanus & Wu, 2016; Ifinedo, 2012) have adopted PMT in their investigations, but they have not fully leveraged PMT. In particular, they do not offer an explanation on how fear-appeal and maladaptive rewards shape InfoSec behaviours (Boss et al., 2017). In addition, although PMT has been widely used to examine different aspects of InfoSec, researchers have mostly paid attention to InfoSec issues in organisations. Previous studies that applied PMT to investigate individuals' InfoSec protective behaviours reported conflicting results on the significance of the users' protection motivation mechanism (e.g., Hanus & Wu, 2016; Liang & Xue, 2010). The review of InfoSec literature reported a gap in an investigation of antecedents of users' threat and coping appraisals (Hanus & Wu, 2016; Milne et al., 2000). Therefore, this study aims to apply all PMT core constructs by investigating security awareness as an antecedent of threat and coping appraisals and subsequent InfoSec protection intention among computer and Internet users.

SETA programmes provide users with the knowledge on InfoSec threats and solutions to avoid or mitigate the impact of security attacks. This study classifies awareness into threat awareness and countermeasure awareness to precisely examine how different types of awareness shape users' InfoSec protection intention. According to previous InfoSec research, providing effective InfoSec awareness is considered the most cost effective solution to encourage users to adopt a more protective and proactive approach rather than a reactive approach (Hanus & Wu, 2016). Although the need for research on security awareness among users has been suggested, most of previous studies focused on organisational security policies to deter InfoSec threats. Even though the literature on PMT presents the importance of the sources of information that users apply to assess the importance of threats and their abilities to address such threats (Milne et al., 2000), the antecedents of threat and coping appraisals are frequently neglected in the literature. The present study aims to fill this gap and answer the question of 'what is the influence of SETA and user's coping and threat appraisals on their InfoSec behaviours?'

The rest of this research is organised as follows. First, the relevant literature on InfoSec and a full nomology of PMT are presented. Then, the research model and hypotheses are proposed, followed by the discussion of research methodology and measurement scales. Finally, the results from a pilot study are reported, along with the discussion of the expected theoretical and practical contributions and possible limitations of this study.

Literature Review

InfoSec protection is recognised as a systematic effort to protect users from negative effects of cybercrimes. Previous research questioned the investigation of InfoSec education and awareness programme in relation to protection and prevention strategies (Dinev & Hu, 2007). SETA includes a series of programmes to promote InfoSec awareness by providing users with general InfoSec knowledge about threats along with skills to perform necessary InfoSec protection procedures. SETA programmes apply ongoing attempts (e.g., workshops, posters) that emphasise acceptable usage guidelines and highlight the potential consequences of InfoSec threats and vulnerabilities (D'Arcy et al., 2009). SETA programmes such as training would help users to improve their awareness of computer and InfoSec issues and educate users about the consequences of potential InfoSec risks and how to protect their information and computer from them. Although previous security studies have looked at the benefits of SETA programmes and their positive influence on users' security protective intentions (D'Arcy et al., 2009), there is a lack of empirical studies that explain the underlying cognitive processes connecting the relationship between SETA programmes and InfoSec protection intentions.

InfoSec awareness is about promoting users' knowledge of specific security risks or threats and the potential countermeasures against those risks to protect their information and computers. Researchers proposed including users' InfoSec awareness in InfoSec models in order to better evaluate their InfoSec awareness intentions within their personal lives and in workplaces (Hanus & Wu, 2016). In addition, users are vulnerable to security threats and the lack of awareness is considered as the main issue to cause such vulnerability. Hence, InfoSec awareness should be seen as a necessity for users.

Recently, InfoSec researchers have relied on PMT to investigate users' InfoSec related processes. Originally, PMT is developed based on the anticipation of a negative outcome in individuals' health and their willingness to minimise it in order to protect themselves. By extending this logic to InfoSec protection behaviours, one can argue that a user is motivated to practice InfoSec protection in order to avoid consequences of security threats. In particular, PMT focuses on the concept of protection motivation to predict users' protective intention after receiving fear arousing recommendations known as fear- appeals (Floyd et al., 2000). Fear-appeals are persuasive messages developed to cause fear by explaining harmful consequences that will happen to them if individuals do not follow the recommendations in the messages. Findings from previous studies showed that fear-appeals explain a user's protective intentions (Boss et al., 2015; Johnston & Warkentin, 2010).

PMT explains the relationship between fear-appeals and protective intentions through two mechanisms – threat appraisal and coping appraisal. A fear-appeal increases threat as well as efficacy by providing users with a recommendation to address the threat (Boss et al., 2015). Threat appraisal refers to the procedure of noticing the severity and vulnerability to a threat against the maladaptive rewards and maladaptive intentions/responses. Threat severity presents users' belief on how serious a threat would be to themselves. Threat vulnerability refers to how susceptible users feel in relation to a potential threat (Milne et al., 2000). Maladaptive rewards refer to the intrinsic and extrinsic rewards of not protecting oneself against the fear-appeal, such as saving time, money and pleasure of being sabotaged (Rogers & Prentice-Dunn, 1997). For example, maladaptive rewards can be related to users' perception to save time or money by not following suggested safe InfoSec recommendations (Boss et al., 2015; Rogers & Prentice-Dunn, 1997). If these mistakenly perceived maladaptive rewards outweigh the perceived threat severity and vulnerability, users may choose the maladaptive responses by intending not to follow the recommended protective mechanisms. Conversely, threat must be greater than the maladaptive rewards for an adaptive response to happen (Boss et al., 2015).

Coping appraisal is the procedure of considering user's response efficacy, self-efficacy and the costs of accomplishing the adaptive response in relation to the fear-appeal (Floyd et al. 2000; Rogers & Prentice-Dunn, 1997). Response efficacy refers to a user's belief that an adaptive response will work in protecting the self or others (Floyd et al., 2000). Self-efficacy refers to a user's perception about self-ability and skill to perform the coping response (Floyd et al., 2000). Response cost refers to any cost (e.g., time, monetary cost) associated with the coping response (Floyd et al., 2000). In a coping appraisal process, response and self-efficacy must be greater than the response cost for an adaptive response to happen (Boss et al., 2015).

Protection intentions are about users' intention to protect themselves against the threat raised in the fear-appeal (Boss et al., 2015). Adaptive response refers to an intentional response to fear-appeal that protects self or others against the threat raised in the fear-appeal (Floyd et al., 2000; Rogers & Prentice-Dunn, 1997).

Despite the relevance of PMT in explaining InfoSec intention and behaviour, most of prior research investigated only the core element of PMT (partial nomologies). As a result, fear and maladaptive rewards were excluded from the PMT model (e.g., Dang-Pham & Pittayachawan, 2015; Hanus & Wu, 2016; Johnston & Warkentin, 2010; Liang & Xue, 2010). To address this gap, this study will develop a full nomology of PMT to explain InfoSec intentions.

Research Model and Hypotheses

This study proposes the research model that applies the full nomology of PMT to evaluate the impact of users' InfoSec awareness on their security protection intention through threat appraisal and coping appraisal mechanisms (See Figure 1).

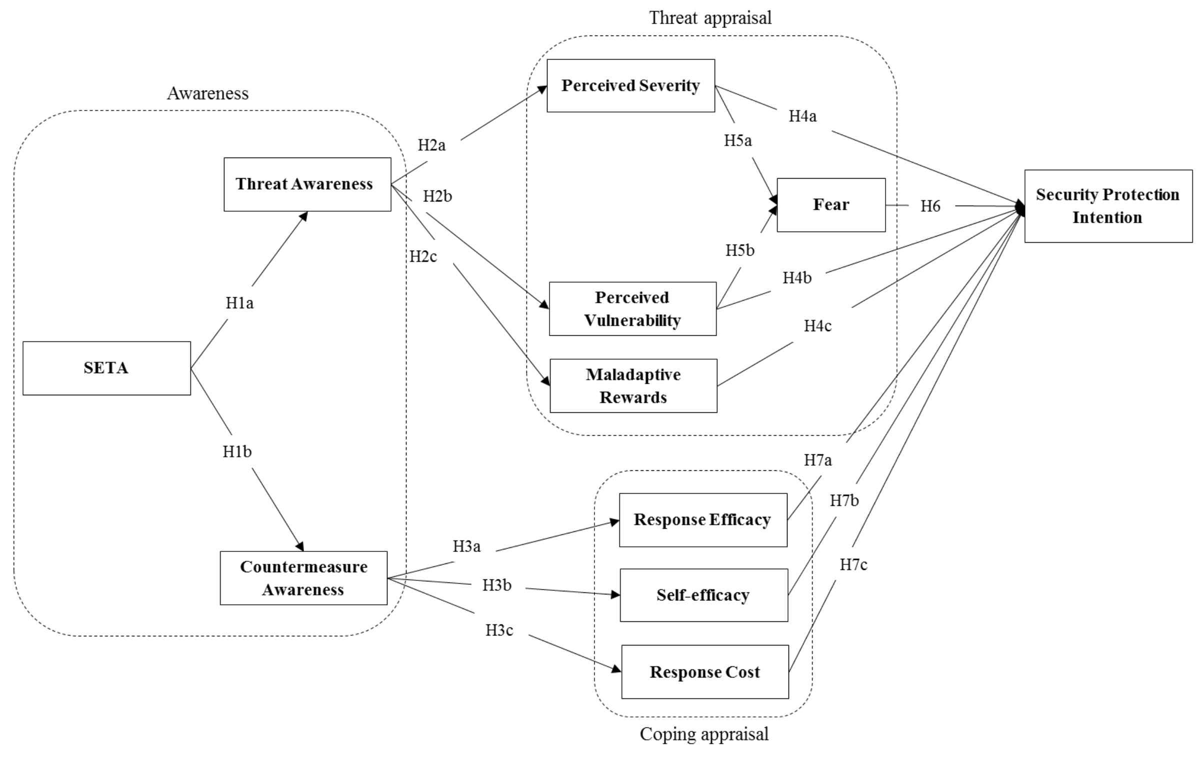

Figure 1. The research model

This study considers users' InfoSec awareness as a multidimensional variable that includes threat awareness and countermeasure awareness. SETA programmes are not only about providing different InfoSec contents for target audiences. They also provide general information about InfoSec environment, potential threats, and actions against InfoSec violations as well as raise users' awareness of accountability for their actions in a comprehensive way (D'Arcy et al., 2009) such as threat identifications and countermeasure actions (Hanus & Wu, 2016). For example, SETA workshops will be ineffective if users only learn about different types of countermeasures against potential threats, but do not learn how to recognise and identify these threats in the first place. Similarly, objectives of SETA programmes will not be successfully met, if users are only able to identify threats and risk but do not know how to avoid them. Both threat and countermeasure awareness is likely to materialise if target audiences are provided with proper InfoSec training programmes such as customised workshops, courses, posters, regular emails and brochures. Hence, we hypothesise:

H1a,b: SETA programme will positively influence users' threat and countermeasure awareness.

Users' knowledge about security threats results in more accurate anticipation about the vulnerability and risks associated with threats. A better understanding about the intensity of negative impact of threats and the likelihood of being impacted by those threats would enable users to better estimate the associated risks and to avoid them. In addition, previous research reported the positive association of users' threat awareness and perceived severity and vulnerability of threat (Hanus & Wu, 2016). The other element of threat appraisal that has been missing from previous research is maladaptive rewards that have an impact on the threat appraisal process (Boss et al., 2015). Users' knowledge and awareness about InfoSec threats and their negative impact would diminish their perception of earning pseudo-benefits from denying InfoSec guidelines known as maladaptive rewards. On the other hand, users would be able to estimate the likelihood of implementing solutions against InfoSec threat, if they are aware of these possible solutions (Hanus & Wu, 2016). If users know about available countermeasures against InfoSec threats, they are likely to recognise the benefit of recommended InfoSec responses to protect themselves. Similarly, if users obtain knowledge about potential solutions against threats, they would have higher confidence in their competencies to take these protective responses. Therefore, threat awareness will positively influence threat appraisal process through perceived severity and perceived vulnerability. Moreover, threat awareness will negatively influence maladaptive rewards. In contrast, countermeasure awareness positively influences coping appraisal through response efficacy, self-efficacy. Reversely, countermeasure awareness negatively influences response cost. Thus, we hypothesise:

H2a,b,c: Users' threat awareness will positively influence their perceived severity (H2a) and vulnerability of threat (H2b) and will negatively influence their maladaptive rewards perception (H2c).

H3a,b,c: Users' countermeasure awareness will positively influence their response efficacy (H3a) and self-efficacy (H3b), and will negatively influence their response cost perception (H3c).

PMT explains how users cognitively appraise positive or negative responses and are motivated to perform a certain behaviour (Dang-Pham & Pittayachawan, 2015). According to the extended model of PMT, threat appraisal involves three cognitive factors namely perceived vulnerability, perceived threat and maladaptive rewards (Boss et al., 2015). When users feel vulnerable against a threat, they would be more inclined to accomplish the recommended processes to counter such threat (Rogers, 1975). It is also reported that users' intention to perform InfoSec protection behaviours would increase if they perceive themselves to be vulnerable against threats (Dang-Pham & Pittayachawan, 2015). Similarly, users intend to be more protective if they perceive the severity of threat (Rogers, 1975). On the other hand, users' realised benefits of performing risky unsecure actions (maladaptive rewards) such as saving time, money or psychological pleasure or peer approval would weaken their intention to perform adaptive protective responses (Dang-Pham & Pittayachawan, 2015). Therefore, we hypothesise:

H4a: Users' perceived severity will positively influence their intention to perform InfoSec protective behaviours.

H4b: Users' perceived vulnerability will positively influence their intention to perform InfoSec protective behaviours.

H4c: Users' maladaptive rewards will negatively influence their intention to perform InfoSec protective behaviours.

Users engage in the cognitive appraisal when they are confronted with a stressful or negative emotional situation. In addition, the motivation to consider the threat further depends on users' perception of existing vulnerability. If users perceive a relevant and severe threat, then fear, which is a negative emotional response, is generated as an outcome. Previous studies found that threat vulnerability and threat severity predict fear (Floyd et al., 2000; Rogers & Prentice-Dunn, 1997). Therefore, we posit that:

H5a: Users' perceived severity will positively influence their perceived fear.

H5b: Users' perceived vulnerability will positively influence their perceived fear.

According to PMT and relevant empirical studies, invoking fear leads users to take protective instructions more seriously (Boss et al., 2015; Rogers, 1975). Ideally, a strong fear appeal should be introduced in order to measure fear and explore the role of fear in mediating the relationship between perceived severity, perceived vulnerability and security protection intention (Boss et al., 2015). Therefore, if a sense of InfoSec fear is emerged, a user is more likely to intend to perform security protection responses. Thus, we hypothesise:

H6: Users' fear will positively influence their intention to perform InfoSec protective behaviours.

PMT theorises that, parallel with the threat appraisal, users perform the coping appraisal that subsequently shapes their intention to perform protective behaviours. Users intend to engage in adaptive responses if they perceive that those behaviours are effective and they believe in their abilities to perform those behaviours (Boss et al., 2015; Rogers, 1975). Users' self-efficacy has an impact on their ability to perform protective tasks. Previous research found that users with a high level of self-efficacy performed InfoSec tasks in their workplace more than those with a low level of self-efficacy (Ifinedo, 2012). In contrast, the costs of performing the behaviours such as time required or inconvenience would diminish the intention to engage in protective behaviours (Rogers, 1975). Thus, users are reluctant to adopt the recommended InfoSec responses if they perceive that a considerable amount of resource (time, effort, and money) will be expended toward that effort (Ifinedo, 2012; Milne et al., 2000). As a result, we hypothesise:

H7a: Users' response efficacy will positively influence their intention to perform InfoSec protective behaviours.

H7b: Users' self-efficacy will positively influence their intention to perform InfoSec protective behaviours.

H7c: Users' response cost will negatively influence their intention to perform InfoSec protective behaviours.

Research Methodology and Pilot Data Analysis

We will conduct a cross-sectional field experiment and use a fear-appeal message to study user security protection intentions. Samples of tertiary students from two institutions in New Zealand have been selected. One group of participants will not receive a fear-appeal message. The other group of participants will receive a fear-appeal message that presents the actual statistics of cybercrimes in New Zealand such as different types of cyber-attacks, frequency of data losses and financial and non-financial harm of data loss. Then, an online survey will be administered to all participants. All measurement items in the survey instrument are adapted from previous studies (Boss et al., 2015; D'Arcy, Hovav & Galletta, 2009; Hanus & Wu, 2016), and measured on a seven-point Likert scale.

In order to fine-tune the survey, the questionnaire was evaluated and refined in two steps: pre-test and pilot study. The questionnaire was pretested with five knowledgeable experts. Modifications were made based on their comments. Then, a pilot study was conducted with the purpose of collecting a small set of data to refine the questionnaire and assess the reliability and validity of the measurement model. The pilot study was conducted with a sample of higher education students at a college in Auckland, New Zealand in February 2018. A comment box was provided for participants to give comments on the questionnaire at the end of the survey. Findings of the pilot study from 47 participants indicate that there are no major difficulties in understanding the instructions and questionnaire items. In the measurement model, all items exhibit high loadings (>0.65), except some items (TA3, TA4, TA8, TA9, FEAR1, MALR5, MALR6, RCOS1, RCOS2, RCOS4) from treat awareness, fear, maladaptive rewards, and response cost constructs. Besides these low loadings values, the rest range from 0.66 to 0.96 on their respective constructs. The items with lower than 0.65 loadings will be removed for the main study. The composite reliability of all constructs is 0.85 or higher, which indicates that the constructs are within accepted limits and therefore reliable. All items except the treat awareness construct had average variance extracted (AVE) values ranging from 0.55 to 0.89, which is considered adequate (>0.5, suggesting that convergent validity is sufficient. Reliability of all the indicators is acceptable except for a few indicators of treat awareness and fear (TA4, TA9 and FEAR1), which are removed from the questionnaire for the main study.

The planned procedural remedies for controlling common method bias (CMB) are the followings: providing clear and concise questions in the questionnaire and assuring respondents' anonymity. In addition, the Harmon single-factor test will be used to evaluate if such bias is indeed a problem in this study.

Expected Contributions

This research extends the current body of knowledge by examining both threat awareness and countermeasure awareness associated with SETA programme as predictors of coping and threat appraisal processes and subsequent security protection intentions. It offers an insight into the intricate relationship between InfoSec threat and countermeasure awareness and the cognitive processes involved in explaining users' InfoSec protection intentions. This study highlights the role of fear-appeal manipulations in InfoSec studies. This suggestion is in line with the report from Boss and colleagues (2015) that fear-appeal manipulation is a core component of the underlying protective behaviours, according to PMT. In addition, most previous studies (e.g., Marett et al., 2011) that applied fear-appeal manipulation used one sample for the model that may convolute the results by failing to identify the main differences among effective and ineffective threat and coping appraisals. In contrast, this study will use two samples, one with a fear-appeal manipulation and the other without fear-appeal manipulation, in order to test the differences of the underlying cognitive processes associated with InfoSec protection behaviours.

The findings of this study will have implications for practice. The findings help practitioners to identify important factors that influence users' InfoSec protection intention. In particular, practitioners may want to put more emphasis on the severity of threats, vulnerability of threats or fear-appeal based on the findings of study.

Practitioners can use the findings to put more emphasis in developing effective InfoSec awareness, educational and training programmes that incorporate both threat and countermeasure awareness within organisations. The findings can also be used to guide the design of InfoSec measures that balance the differences between users' perception about their InfoSec knowledge and protection actions and how they are intended to engage in InfoSec protection behaviours. Furthermore, these findings will be especially useful for higher education institutions that are considering or currently adopting bring your own device practices in classrooms to deliver appropriate InfoSec campaigns and courses to their students.

Limitations

The cross-sectional design of this study may limit the interpretation of the results. Hence, future studies may want to observe any changes in users' InfoSec protection intention and behaviours through fear-appeal conditions over time. Future research may investigate the impact of users' protective intentions on their actual protective behaviours and explore the possibility of InfoSec knowledge transfer between work and home settings.

Conclusion

Due to the prevalent role of digital technology and the Internet in people's lives, users' InfoSec awareness is important for the safe and secure global community. Drawing on the full explanation of PMT, this study offers in-depth insights into how users' InfoSec awareness shapes and motivates their InfoSec protection intentions. This research extends the current body of knowledge by introducing SETA programmes as an antecedent of threat and countermeasure InfoSec awareness, which are antecedents of InfoSec protection intentions mediated by coping and threat appraisals.

References

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and 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), pp. 837-864.

Dang-Pham, D., and Pittayachawan, S. 2015. "Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach," *Computers and Security* (48), pp. 281-297.

Dinev, T., and Hu, Q. 2007. "The centrality of awareness in the formation of user behavioral intention toward protective information technologies," *Journal of the Association for Information Systems* (8:7), pp. 386-408.

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

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

Hanus, B., and Wu, Y. A. 2016. "Impact of users' security awareness on desktop security behavior: A Protection Motivation Theory Perspective," *Information Systems Management* (33:1), pp. 2-16.

Ifinedo, P. 2012. "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Computers and Security* (31:1), pp. 83-95.

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

Liang, H., and Xue, Y. 2010. "Understanding security behaviors in personal computer usage: A threat avoidance perspective," *Journal of the Association for Information Systems* (11:7), pp. 394–413.

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

Milne, S., Sheeran, P., and Orbell, S. 2000. "Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory," *Journal of Applied Social Psychology* (30:1), pp. 106–143. doi:10.1111/jasp.2000.30.issue-1

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

Rogers, R. W. 1983. Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Ciacioppo and R. Petty (Eds.), Social psychophysiology. New York, NY: Guilford Press, pp. 153-176.

Rogers, R. W., and Prentice-Dunn, S. 1997. *Protection Motivation Theory,* in *Handbook of Health Behavior Research I: Personal and Social Determinants,* D. S. Gochman (ed.), New York, NY: Plenum Press, pp. 113-132.