An Empirical Study of Home User Intentions towards Computer Security

Annette M. Mills
University of Canterbury
annette.mills@canterbury.ac.nz

Natasha Sahi
University of Canterbury
nsa58@uclive.ac.nz

Abstract

Home computer users are solely responsible for implementing security measures on their devices. Although most computers have security software installed, the potential remains for security breaches, which makes it important for home users to take additional steps, such as not sharing one's password and using strong passwords, to secure their devices further. Drawing on protection motivation theory and findings from prior research, this study evaluates factors that influence individuals to implement additional security measures to protect their home computers. Using SmartPLS and responses from 72 home computer users, the results show that response efficacy, self-efficacy and subjective norms were significant in encouraging persons to implement additional security measures. Maladaptive rewards on the other hand acted as a significant detractor, while neither perceived vulnerability nor perceived severity was significant in relation to willingness to implement additional security measures.

1. Introduction

Home computers have become an ideal breeding ground for hacking, distributing, or holding sensitive information to ransom [1] Although home computers are sold with a base level of security, this is not always enough. To reduce the potential for security breaches, it is important that people take additional steps to secure their devices. These can include simple steps such as using strong passwords or backing up their data, and exercising caution when installing new applications or programs on a home computer or laptop. However, people often do not follow the advice of experts and take additional to secure their devices, resulting in a low level of security of home computing devices [1].

Understanding the home setting is important. Today many persons use personal devices for work related purposes. As more companies engage with individuals online, this results in a large amount of sensitive information being stored on personal computers (including documents related to banking and insurance), making it increasingly important to secure these devices. Most studies of information systems (IS) security however, have been in organizational settings [1, 2]. This research may not generalize readily to the home context due to differences such as the role of training, and the presence of sanctions and policies in organizations that govern compliance [1]. Hence it is important to examine the home setting, and understand how to motivate people to take extra steps to protect their home computers [3].

To address the research aim, this study draws primarily on Protection Motivation Theory [4] which has been successfully used to explain attitudes towards IS security compliance in organizations [5], as well as the protective security behaviors of home computer users [6]. The PMT assumes that the motivators behind protecting something is a result of a person's assessment of the perceived severity of a threat, probability of the threat occurring, the efficacy of the response behavior, and the confidence level in their ability to act upon the threat [4, 7]. The PMT is further extended by incorporating subjective norms (from the Theory of Reasoned Action) which has been commonly cited in the PMT literature as significant in explaining an individual's intention behind taking security –related actions [9, 10, 11] This paper reports on a study that investigates peoples' willingness to take *additional* protective measures to secure their home computers. By improving our understanding of people's beliefs about the protection of home computers, this study aims to provide insights that can usefully inform computer service providers and other organizations on how to design better support services and improve home computer security.

2. Prior Research

With the recognition that many security breaches are directly or indirectly caused by failure to comply with security policies, much of the early research on motivations regarding computer security has been in

URI: https://hdl.handle.net/10125/59921
ISBN: 978-0-9981331-2-6

the organizational context. With the rise in home computer use, individuals who own personal computers are also becoming more vulnerable to security breaches [12]. Therefore, it is important that they too apply security measures on their computers to reduce the potential for security breaches to occur [13]. This study aims to address this need.

Studies have used various theories to identify the factors influencing computer security behaviors [2]. The PMT in particular has been used in studies of IS security; these have found constructs that form threat and coping appraisals have significant impacts on the intention of individuals to take preventative computer security measures at work [5, 9, 10], and at home [2, 6, 11, 13, 15, 16, 17, 18, 19]. There have been mixed findings. For example, some found constructs such as perceived vulnerability to be significant [5], while others did not [15]. Others have focused on incorporating factors from other theories such as social influence from the Theory of Reasoned Action to better explain intention [2, 6, 9 13].

In the home context, most studies using the PMT focus on general security behaviors [2, 13, 17, 18, 20], or specific protective behaviors such as adoption of security on home wireless networks [19] or the use of password management systems [17]. However, what these studies do not address are the additional steps that people are encouraged to take to protect their devices and their data, and stay safe when they are online (e.g. not sharing their passwords with others, using different passwords for different devices and accounts, and backing up one's data) [21]. Thus the focus of this research is to bridge this gap by examining peoples' motivations to go beyond the basics and take additional steps to protect their home computers from threats.

3. Research Model

3.1 Protection Motivation Theory

Prior research has used many theories to examine protective behaviors. These include the Theory of Reasoned Action, the Theory of Planned Behavior and the Protection Motivation Theory. Of these, Protection Motivation Theory is particularly relevant to this study because of its explicit consideration of a threat and one's ability to cope with it.

Grounded in healthcare, Protection Motivation Theory (PMT) was developed to identify the cognitive processes that an individual faces when exposed to a threat [4]. According to the PMT [4, 7], protection motivation arises from consideration of a potential threat and one's desire to avoid the consequences of the threat. This involves two main cognitive processes – a *threat appraisal* and a *coping appraisal*. The *threat appraisal* identifies and evaluates the threat in terms of the perceived severity of and vulnerability to the threat, coupled with one's assessment of the rewards (i.e. maladaptive rewards) that may arise from <u>no</u>t taking protective actions. This means that even if a threat is perceived as likely and its impact severe, if the rewards for not taking an action are high enough this will negate the protective action.

Once an individual evaluates the threat, the *coping appraisal* follows. This consists of an assessment of *response efficacy, self-efficacy* and *response costs*. *Response efficacy* refers to the perceived effectiveness of reducing the threat, whilst *self-efficacy* refers to an individual's confidence in carrying out the responding protective action against the threat [2, 4]. The *response costs* are the costs incurred when performing the protective behavior, such as time, money, and overheads [4, 6, 14]. Overall, in the coping appraisal, the response efficacy and self-efficacy must be greater than the response costs for a protective action to be taken [7].

3.2 Hypothesis Development

The PMT states that if an individual assesses the perceived severity of a threat to be high, they are more likely to take protective actions to mitigate the threat [7]. In a study with psychology students high and low levels of threat severity were manipulated by displaying an unexpected virus warning message while participants browsed a website [14]. The findings showed that participants who were exposed to the high levels of severity were more likely to install anti malware. Dang-Pham and Pittayachawan [15] and Yoon et al. [11] also studied the protective computing behaviors amongst university students and found that severity positively impacted intention to take protective actions. Turning to home computer use, Jansen and van Schaik [6] and Woon et al. [19] both found a positive and significant relationship between severity and protective computing behaviors. This leads to the following hypothesis:

H_1: Perceived severity is positively related to intention to implement additional security measures.

When an individual perceives they are vulnerable to security incidents, he/she is more likely to adopt computer security measures (e.g. installing protective software) to mitigate the risk. Vulnerability has commonly been found to influence the intention to comply with security policies in an organizational context [9, 14]. However, these findings have been less consistent in relation to home computer security. While Jansen and van Schaik [6] and Woon et al. [19] found insignificant relationships between vulnerability and intention, in contrast, Thompson et al. [13] found that home computer users (individuals) who believed they were vulnerable to general security threats were more likely to engage in generic protective computing behaviors. Given that most studies suggest that vulnerability has a significant effect on intention, we propose that:

H_2: Perceived vulnerability is positively related to implement additional security measures.

Although Rogers [7] recognized the concept of perceived rewards arising from not performing a behavior, many IS security studies have excluded maladaptive rewards [10, 13, 17]. As such, little is known as to whether maladaptive rewards from not performing a protective behavior impact protection motivation [15]. Those that have examined maladaptive rewards return mixed findings. For example, while Dang-Pham and Pittayachawan [15] did not find a significant relationship between maladaptive rewards and intention to perform a security behavior, consistent with the PMT, others studies have found an inverse relationship between maladaptive rewards and intention within the IS security setting [5, 14]. For example, Boss et al. [14] found that maladaptive rewards inversely affected intention to comply to online security policies. Hence, we propose:

H_3: Maladaptive rewards are inversely related to intention to implement additional security measures.

The PMT suggests that if an individual believes a protective action will mitigate a threat, they are more likely to take action [7]. The relationship between response efficacy and intention has been consistently established in the general IS security literature [6, 9, 14, 17, 19, 20]. Response efficacy is also commonly the strongest variable that predicts the intention to perform a protective behavior [9]. For example, Dang-Pham and Pittayachawan [15] found that response efficacy directly affected intention to implement anti malware on personal computing devices. Yoon et al. [11] also found that response efficacy affected intention to implement general IS security measures on personal computers. Hence:

H_4: Response efficacy is positively related to intention to implement additional security measures.

If individuals believe they are able to carry out a protective behavior effectively, they are more likely to perform the behavior [7]. The relationship between self-efficacy and intention is supported in many studies of protective behaviors including the work setting [5, 9, 10, 14], and home computing setting [2, 6, 11, 13, 15, 16, 17, 18, 19]. A recent study of home users found self-efficacy was important in determining personal computing security intentions [13]. This finding was also supported by Menard et al. [17] who also studied security intentions in a home context. Hence it is expected that:

H_5: Self-efficacy is positively related to intention to implement additional security measures.

The PMT suggests that if an individual perceives the costs of implementing a protective behavior to be high, then it is unlikely that the preventative behavior will be adopted [7]. Response costs have been identified as a context and individual dependent construct [9]. As such, the impact of response costs may vary across contexts. For example, some studies have not found response costs to be significant in the organizational context [9; 17]; this may be so because factors such as time and money may not carry a personal cost to the individual. By contrast, in the home context, users are personally responsible for any costs and overheads involved in taking protective action. For example, a study of home users found that users would intend to take precautionary measures to secure their home wireless networks if response costs were reduced [19]. Similarly, Thompson et al. [13] found that response costs were significant in determining whether to perform personal computing security behaviors. Hence, we propose:

H_6: Response costs are inversely related to implement additional security measures.

Subjective norms derive from the Theory of Reasoned Action (TRA) [8]. This construct explains how social pressures on an individual can cause a behavioral response to an event [8]. Although not originally included in the PMT [13], this construct is commonly cited in PMT literature as explaining an individual's intention behind taking certain security actions [10, 11]. In IS security, Ifinedo [9] found that the compliance of other employees in organizations influenced others to comply also with IS security policies. Similarly, Tsai et al. [20] examined the online security behaviors of general MTurk users and found that the social circle of these users positively influenced their computer security behaviors. Likewise, we expect that the social circles of the participants will impacts intention to take additional security steps [8]. Hence we propose that:

H_7: Subjective norms are positively related to implement additional security measures.

Figure 1 summarizes the above hypotheses.

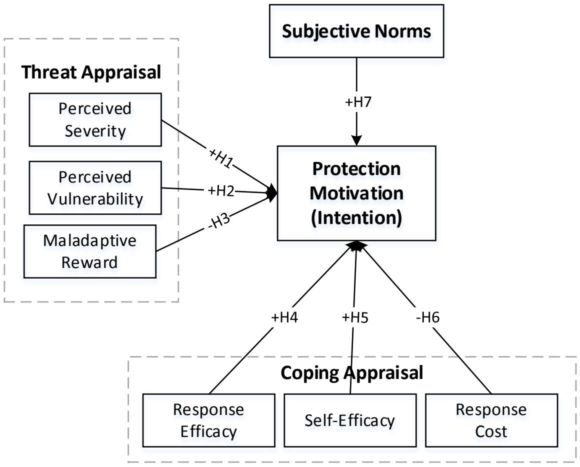


Figure 1. Research model

4. Methodology

This study surveyed individuals in New Zealand who owned a home computer or laptop. A link to the online survey hosted by Qualtrics was sent out to potential participants via organizational contacts and poster advertising on a university campus.

All items in the survey were adapted from prior research (See Table 1). Perceived severity (3 items), vulnerability (3 items), response efficacy (3 items), response costs (4 items), maladaptive rewards (5 items), and intention (6 items) were adapted from Boss et al. [14]. Self-efficacy (5 items), subjective norms (3 items) were adapted from Anderson and Agarwal [2] and Thompson et al. [13]. All items were measured using 7-point Likert scales anchored as “Strongly Disagree” to “Strongly Agree”.

This study used the Partial Least Squares approach to structural equation modelling (PLS-SEM) via Smart PLS 3.2.7 (with 500 resamples) to evaluate the research model [22]. PLS-SEM is suitable particularly for studies focused on prediction where the aim is to explain the variance observed in the dependent variable, as with this study which focuses on understanding protection motivation (i.e. operationalized as intention to implement additional security measures) [23]. This approach is also appropriate when there are many constructs included in the research model with the model being relatively complex compared to the sample size [23].

Table 1. Sample Items

Construct	Sample Item
Perceived Severity	If my home computer/laptop was affected by a security breach it would cause major problems
Perceived Vulnerability	My home computer/laptop is vulnerable to a security breach
Maladaptive Rewards	Not taking additional security measures to protect my home computer/laptop keeps me from being confused
Response Efficacy	Taking additional security measures will be effective in protecting my home computer/ laptop
Self-Efficacy	I feel comfortable taking additional measures to secure my home computer/ laptop
Response Costs	There is too much work associated with implementing additional security measures on my home computer/laptop
Subjective Norms	People whose opinions I value think that I should take additional security measures to protect my home computer/laptop
Intention (Protection Motivation)	I intend to take additional security measures to protect my home computer/ laptop

5. Results

Data were collected from 72 persons who responded. Of the respondents, 50% were female. Most were aged 18 to 34 years old (75%), and had an undergraduate (39%) or postgraduate degree (49%). The majority had owned their home devices for 5 years or more (81%); most persons owned a laptop only (72%). Most (93%) had read or heard about security breaches, and for 65% of the respondents their computer had been affected by a security breach (e.g. malware, virus).

The results of the tests of the measurement model showed outer loadings ranged from 0.688 to 0.972. Composite reliability ranged from 0.873 to 0.962, and the average variance extracted (AVE) from 0.697 to 0.895 (Table 2). Being greater than recommended cut-offs of 0.70, 0.70 and 0.50 respectively, these satisfied the tests for adequate construct reliability and convergence [23]. For discriminant validity, the results (Table 2) also showed the square root of the AVE values (shown on the diagonals) were greater than the correlations among the constructs indicating that the constructs were distinct from each other [23].

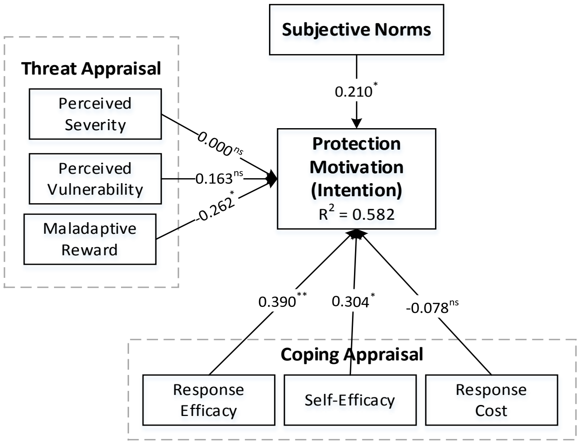
Table 2. Composite Reliability, AVE, and Discriminant Validity

	CR	AVE	PS	PV	MR	RE	SE	RC	SN	Int
PS	0.96	0.90	0.95							
PV	0.89	0.73	0.35	0.85						
MR	0.93	0.74	0.05	0.30	0.86					
RE	0.87	0.70	0.37	0.12	0.02	0.84				
SE	0.92	0.70	0.24	0.20	-0.03	0.69	0.84			
RC	0.90	0.70	0.10	-0.08	0.50	0.17	-0.02	0.84		
SN	0.95	0.87	0.06	-0.05	0.04	0.17	-0.07	0.16	0.93	
Int	0.97	0.82	0.27	0.19	-0.25	0.64	0.60	-0.13	0.22	0.91

Key: Perceived Severity (PS); Perceived Vulnerability (PV); Response Efficacy (RE); Self-Efficacy (SE); Maladaptive Rewards (MR); Response Cost (RC); Subjective Norm (SN); Intention (Protection Motivation (INT)

Note: The square root of the AVE for each construct is shown on the diagonals, and the correlations among the constructs on the off-diagonals.

For the structural model, attention is paid to the R^2 values (i.e. coefficient of determination) and path coefficients [23]. The R^2 value signals the goodness of fit of the model; the higher the R^2 value, the greater the fit, and the better the model will represent the data collected [24]. The results (Figure 2) showed an R-square value of 0.582 suggesting the model explained a moderate to substantial proportion of the variance observed for protection motivation [23].



Key: *** P≤0.001; ** p≤0.01; * P≤0.05; ns = Not Supported

Figure 2. The Results

For threat appraisal, the results (Figure 2) showed that maladaptive rewards (-0.262, p≤0.025) was strongly related to intention; H3 was supported, However perceived vulnerability (0.163, p=0.124) and perceived severity (0.000) were not significant in relation to intention; H1 and H2 were not supported. Turning to the coping appraisal, response efficacy (0.390, p≤0.003) and self-efficacy (0.304, p≤0.015) were both significant predictors of intention, whilst response cost (-0.078) was not. H4 and H5 were supported, but not H6. Subjective norms was also significant (0.210, p≤0.014), supporting H7.

6. Discussion

As more individuals are using their home computers and laptops for both work and personal use, a large amount of sensitive information is constantly being stored and exchanged on their devices [1]. Due to the increase in the potential for security breaches to occur with personal devices, it is important that people take steps to secure their devices beyond the base level of security that comes with each device. Indeed many breaches occur because of simple oversights on the users' part (e.g. using weak passwords, using the same passwords across multiple devices or applications, downloading applications from unknown sources, etc.) As such, the aim of our study was to determine what motivates persons to implement additional security measures on their home computers and laptops.

Contrary to prior studies [9, 13, 14, 16], the results showed that neither perceived vulnerability nor perceived severity were significant in relation to intention to implement additional security measures on home computers and laptops. The insignificant relationships for perceived severity and perceived vulnerability in relation to intention were not only inconsistent with the PMT, but also contrary to studies of security behaviors both in the workplace [5, 14], and at home [6, 13, 15, 11, 19]. An explanation for this inconsistency may be due to the threat appeal not being manipulated unlike Boss et al. [14] who found that a higher threat appeal led to a protective response, while a low threat appeal had less impact on intention.

The significant relationship between maladaptive rewards and intention is consistent with the findings of Boss et al. [14] and Vance et al. [5], suggesting that higher rewards would reduce intention to take extra steps to secure one's devices. Coupled with the non-significance of the perceived severity and perceived vulnerability, this finding is concerning as maladaptive rewards can further lower the level of the threat appraisal, such that persons do not feel it is necessary to take additional measures to protect their devices even if they believe these would protect their devices from potential harm (response efficacy) and they are capable of taking these steps (self-efficacy).

For the coping appraisal, the results identified response efficacy and self-efficacy as moderate predictors of intention to implement additional security measures on home computers. This is consistent with prior studies of home users [2, 6, 11, 15, 17, 19] and in the work place [9, 14]. Contrary to expectations [13], response costs did not have a significant impact on the protection motivation. However, this is consistent with some studies that have likewise found an insignificant relationship in organizations [9] and in home settings Menard et al. [17].

Altogether the results have implications for practice, in particular those who are responsible for promoting internet safety and cybersecurity among the public. The results show that what others think (i.e. subjective norms) coupled with coping appraisal (i.e. response efficacy and self-efficacy) are strong motivators for people to take protective actions. On the other hand, a low threat appraisal whether valid o not, will lessen the motivation to take protective actions. In addition, if the 'reward' of not taking protective actions (e.g. saving time, preventing confusion) is high enough this will further lessen the motivation to take protective actions. To motivate action, it is important to overcome the appeal of 'maladaptive rewards' by educating home computer users of their vulnerability to and potential severity of a security breach; high fear-appeal messages may serve to heighten the threat appraisal and motivate people to action [14].

It is further recommended that home users are provided with checklists and 'how-to' guides on additional security measures they should take to minimize risk; these can range from simple precautions (e.g. using strong passwords) to more sophisticated measures such as adjusting the default settings on their browser. Even if people are not confident to take very involved steps (or the costs are perceived as too high), the simple steps would go a long way to improve the security of home devices.

Consistent with prior research [9, 20], the results also highlighted the importance of social circles (e.g. family, friends) which can have a strong impact on protection motivation. Promoting the benefits and uptake of computer security measures through public education and awareness (See www.netsafe.org.nz), may further motivate people to adopt these measures.

6.1. Limitations

Notwithstanding the contributions of this study, there are some limitations that impact the findings and provide opportunities for future work. First this study was conducted in New Zealand; here there are many organizations that aim to ensure and educate the public about network and internet safety and security. As such, the findings may not apply in other countries where, for example, general internet or network safety is seen by the general public as a significant issue. Second, we did not test a comprehensive model of protection motivation. Future study may wish to extend the current model by including other factors such as fear, attitude and descriptive norms that may also impact behavior [2, 14]. The current sample of 72 responses though small, was enough to assess the model [23]. Given the number of weak or insignificant relationships (e.g. perceived vulnerability, perceived severity, response cost) it is expected that a greater number of responses may make smaller significances detectable, and shed more light on the predictors of intention.

7. Conclusion

This research focused on the implementation of *additional* security measures on home computers and laptops. While most studies have focused on organizational settings or the general perceptions of home users about security measures as a whole, this study recognizes that newer computers and software include a base level of security (e.g. Microsoft Essentials), that require little or no user action. However, this is not enough, and there are many steps, ranging from simple to more complex measures, that people can take to improve the security of their home device. This study therefore focused on the additional measures that people can take to secure their devices to identify what would encourage people to take these extra steps. By distinguishing these additional measures (e.g. not sharing passwords), this study contributes to the literature and to practice by understanding better, peoples' motivations to go beyond the basics to ensure the safety of their personal computing devices.

8. References

[1] Li, Y., and M.T. Siponen, "A Call for Research on Home Users' Information Security Behaviour", Proceedings: PACIS 2011 Proceedings, 112.

[2] Crossler, R.E., A.C. Johnston, P.B. Lowry, Q. Hu, M. Warkentin, and R. Baskerville, "Future Directions for Behavioral Information Security Research", Computers and Security, 32, February 2013, 90-101.

[3] Anderson, C.L. and R. Agarwal, "Practicing Safe Computing: A Multimedia Empirical Examination of Home Computer User Security Behavioral Intentions", MIS Quarterly, 34(3), 2010, 613-643.

[4] Rogers, R.W. "A Protection Motivation Theory of Fear Appeals and Attitude Change", The Journal of Psychology, 91(1), 1975, 93-114.

[5] Vance, A., M. Siponen, and S. Pahnila, "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory", Information and Management, 49(3), 2012, 190-198.

[6] Jansen, J., and P. van Schaik, “Comparing Three Models to Explain Precautionary Online Behavioural Intentions. Information and Computer Security, 25(2), 2017, 165-180.

[7] Rogers, R.W. “Cognitive and Psychological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. Social Psychophysiology: A Sourcebook”, in J. T. Cacioppo, and R. E. Petty (eds.), New York: The Guilford Press. 1983, 153-176.

[8] Ajzen, I. and M. Fishbein, “Attitude-behavior relations: A theoretical analysis and review of empirical research”, Psychological Bulletin, 84(5), 1977, 888-918.

[9] Ifinedo, P. “Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory”. Computers and Security, 31(1), 2012, 83-95.

[10] Johnston, A.C., and M. Warkentin, “Fear Appeals and Information Security Behaviors: An Empirical Study”, MIS Quarterly, 34(3), 2010, 549-566.

[11] Yoon, C., J.W. Hwang, and R. Kim, “Exploring Factors that Influence Students' Behaviors in Information Security”, Journal of Information Systems Education, 23(4), 2012, 407-415.

[12] Scott, P. (2017). “Fraud and Cyber Crime are now the Country's most Common Offences. The Telegraph. Retrieved from http://www.telegraph.co.uk/news/2017/01/19/fraud-cyber-crime-now-countrys-common-offences/

[13] Thompson, N., T.J. McGill, and X. Wang, “Security Begins at Home”: Determinants of Home Computer and Mobile Device Security Behavior”, Computers and Security, 70, September 2017, 376-391.

[14] Boss, S.R., D.F. Galletta, P.B. Lowry, G.D. Moody, and P. Polak, “What do Users have to Fear? Using Fear Appeals to Engender Threats and Fear that Motivate Protective Security Behaviors”, MIS Quarterly, 39(4), 2015, 837-864.

[15] Dang-Pham, D. and S. Pittayachawan, “Comparing Intention to Avoid Malware across Contexts in a BYOD-enabled Australian University: A Protection Motivation Theory Approach”. Computers and Security, 48, September 2015, 281-297.

[16] Liang, H., and Y. Xue, “Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective”, Journal of the Association for Information Systems, 11(7), 2010, 394-413.

[17] Menard, P., G.J. Bott, and R.E. Crossler, “User Motivations in Protecting Information Security: Protection Motivation Theory versus Self-Determination Theory”, Journal of Management Information Systems, 34(4), 2017, 1203-1230.

[18] White, G., T. Ekin, and L. Visinescu, “Analysis of Protective Behavior and Security Incidents for Home Computers”, Journal of Computer Information Systems, 57(4), 2017, 353-363.

[19] Woon, I., G.W. Tan, and R.A. Low, “Protection Motivation Theory Approach to Home Wireless Security”, Proceedings: ICIS, 2005, 31.

[20] Tsai, H.Y.S., M. Jiang, S. Alhabash, R. LaRose, N.J. Rifon, and S.R. Cotten, “Understanding Online Safety Behaviors: A Protection Motivation Theory Perspective”, Computers and Security, 59, June 2016, 138-150.

[21] Reeder, R., I. Ion, and S. Consolvo, “152 Simple Steps to Stay Safe Online: Security Advice for Non-Tech-Savvy Users”, IEEE Security and Privacy, 15(5), 2017, 55-64.

[22] Ringle, C. M., Wende, S., and Becker, J.-M. 2015. "SmartPLS 3." Boenningstedt: SmartPLS GmbH, http://www.smartpls.com.

[23] Hair, J.F., G.T.M., Hult, C. Ringle, and M. Sarstedt, “A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)”, 2017.