Assessing the Determinants of Millennials' Online Protective Behavior: How their Protection Motivation Translates into Actual Use Behavior

Ana S. Medeiros[1], Luis F. Martinez[2], and Luisa M. Martinez[3]

[1] Researcher

Nova School of Business and Economics, Universidade Nova de Lisboa

24081@novasbe.pt

[2] Associate Professor of Marketing

Nova School of Business and Economics, Universidade Nova de Lisboa

luis.martinez@novasbe.pt (corresponding author)

[3] Assistant Professor of Marketing

IPAM Lisboa and UNIDCOM/IADE, Universidade Europeia

luisa.martinez@universidadeeuropeia.pt

Abstract. This research assesses the determinants of Millennials protection motivation (or security intentions) on their actual use behavior when navigating online, considering the protective measures they adopt. Accordingly, we propose a model integrating variables from two widely accepted behavioral theories, the Protection Motivation Theory and the Reasoned Action Approach. An online survey was conducted, relying on the responses of 236 participants from different nationalities, which were analyzed through hierarchical multiple regression. Results show a gap between security intentions and use behavior and indicate safety habit strength and actual control as significant predictors of Millennials' use behavior. By focusing not only on the users' behavioral intentions but also on their actual use behavior, this research seeks to extend the previous literature on the topic.

Keywords. Online Security; Protection Motivation; Reasoned Action Approach; Security Intentions; Use Behavior.

1 Introduction

Considering the strong impacts of cybercrime related activity, its causes, drivers, and effects have been widely studied (e.g., Anderson et al 2013; Lagazio et al 2014; Romanosky 2016). A review of the literature suggests that although cybersecurity is a very current and commonly studied topic, most research is centered

Medeiros, A.S., Martinez, L.F., & Martinez, L.M. (2020). Assessing the determinants of Millennials' online protective behavior: How their protection motivation translates into actual use behavior. In F. J. Martínez-López and S. D'Alessandro (Eds.), *Advances in Digital Marketing and eCommerce: First International Conference, 2020 (pp. 153-162)*. Cham, Switzerland: Springer Proceedings in Business and Economics. https://doi.org/10.1007/978-3-030-47595-6_20

on the implications for organizations (Saridakis et al 2015). As mentioned above, unlike employees in a work setting, home users are not subject to training (Anderson et al 2010), and often are not aware of the risks of using the Internet, as they do not have any knowledge preparation for their online journey (Kritzinger et al 2010). Moreover, as stated by Anderson et al. (2010; p. 613), this type of user "represent[s] a significant point of weakness in achieving the security of the cyber infrastructure". Thus, home users are an interesting area of study.

A study from the European Commission (2017) states that 51% of the European citizens do not feel well informed about cyber threats and, as mentioned above, 86% believe the risk of becoming a victim of cybercrime is currently increasing. These values reveal that most individuals do not feel prepared to face these current threats that result from their personal experiences, other persons' experiences, and the news media (Tsai et al 2016). Furthermore, the user lack of knowledge relative to cybercrime touches upon another widely mentioned topic in the literature review which is cybercrime awareness. According to Dodge et al. (2007), varying awareness is hard to characterize due to the 'user's individual nature'. Since several models have been proposed to study the individual's threat perception (Kritzinger et al 2010; Poepjes et al 2012), it is noteworthy to instead analyze its influence on the user's behavioral intention and actual protective behavior. Current approaches include the Rational Choice Theory (RCT), the Reactance Theory, and the Justice Theory. As an alternative, Rogers (1975, 1983) has proposed the Protection Motivation Theory (PMT), which is based on the Theory of Reasoned Action (Fishbein et al 1975).

2 Protection Motivation Theory

Commonly found in academic literature (e.g., Boss et al 2015; Crossler et al 2014), the Protection Motivation Theory (PMT) seeks to explain the reasons that lead to protective behaviors and how individual users undertake those behaviors (Rogers 1975, 1983). The PMT has gained many supporters as it has been extended to understand the drivers for online safety behavior, namely in the context of individual users, as it accounts for the discrepancy between realizing threats and taking protective actions (Tsai et al 2016). The model states that protective behaviors are motivated by Threat Appraisals, determined by the user's perceived vulnerability and susceptibility to risks, and Coping Appraisals, based on self-efficacy, response efficacy, and response costs associated with safe or adaptive behaviors. Also, Tsai et al. (2016), established a strong link between behavior intentions of home users and online habit strength, as in accordance with LaRose et al. (2007). Most published research seeks to comprehend and predict Security Awareness and, consequently, Security Intentions (e.g., Boss et al 2015). However, there is a literature discrepancy related to security related behaviors. This translates into the absence of further research that analyzes how home user's Protection Motivation (or Security Intentions) convert into actual Use Behaviors when using the Internet. Boss et al. (2015) wrote about this issue, but even so, his study focus-

Medeiros, A.S., Martinez, L.F., & Martinez, L.M. (2020). Assessing the determinants of Millennials' online protective behavior: How their protection motivation translates into actual use behavior. In F. J. Martínez-López and S. D'Alessandro (Eds.), *Advances in Digital Marketing and eCommerce: First International Conference, 2020 (pp. 153-162).* Cham, Switzerland: Springer Proceedings in Business and Economics. https://doi.org/10.1007/978-3-030-47595-6_20

es mostly on Fear Appeals instead on the actual study of the individual's Use Behavior. Consequently, it is important to further comprehend the models that attempt to explain people's actual behavior, in order to understand the effect of behavioral intentions on the user's behavior. From the literature, the most important models for studying individual's behavior are the Theory of Reasoned Action (TRA) and the Theory of Planned Behavior (TPB), both of which aim to predict individual's behavior based on intentions and pre-existing attitudes (Fishbein & Ajzen 1975; Saridakis et al 2015). From these theories, many more have been derived. One of the most widely studied is the Reasoned Action Approach (RAA).

3 Reasoned Action Approach

The Reasoned Action Approach (RAA) was first described by Fishbein and Ajzen (2010), the same authors of the Theory of Reasoned Action (Fishbein and Ajzen 1975) and the Theory of Planned Behavior (Ajzen 1991). The RAA has been commonly used to predict people's behavior in diverse areas, such as Health (Conner et al 2017), Agriculture (Hulst et al 2016) and Consumer Behavior (Liu et al 2017). In terms of online behavior, its applications have been extended to the study of several areas ranging from online shopping behavior (Chang et al 2005 Zhou et al 2007), the adoption of social networks (Pinho et al 2011), and online banking (Hanafizadeh et al 2013). According to this theory, Attitudes, Perceived Norms, and Perceived Control guide the user's behavioral intentions and actual behavior. Also, Behavioral Intention is stated to be the best single predictor for Use Behavior, since the strongest intentions have the greatest probability of transforming into actual behaviors. Equally, the RAA also states that Use Behavior is moderated by the variable Actual Control, which includes the user's skills, abilities, and environmental factors (Ajzen and Fishbein 2010). As stated in this theory, people are only able to perform a certain behavior if they have the requisite skills and abilities, and if there are no environmental constraints preventing them from acting on their specific behavioral intentions. In brief, intention is described as a strong predictor for Use Behavior. However, current literature is not able to fully explain the influence of Protection Motivation on Millennials' Use Behavior. Also, published literature does not consider other variables which might be influential at predicting Use Behavior applied to this field of study.

4 Development of the Research Hypotheses

Considering the gap identified in the literature review, the suggested research proposal focuses on understanding the influence of Protection Motivation (or Security Intentions) in the Use Behavior of home users in terms of the security measures they adopt. Also, it was considered that context and external factors such as age, gender, and experiences might have an influence in adopting certain security precautions (Ajzen and Fishbein 2010). For that reason, Cohort Theory was used, allowing for a greater understanding of the actual behavior of a specific generation as generational cohorts differ not only in age but also in education, relationship

Medeiros, A.S., Martinez, L.F., & Martinez, L.M. (2020). Assessing the determinants of Millennials' online protective behavior: How their protection motivation translates into actual use behavior. In F. J. Martínez-López and S. D'Alessandro (Eds.), *Advances in Digital Marketing and eCommerce: First International Conference, 2020 (pp. 153-162)*. Cham, Switzerland: Springer Proceedings in Business and Economics. https://doi.org/10.1007/978-3-030-47595-6_20

with peers, and past experiences (Ryder 1965). Therefore, for the purpose of this research we will follow the generational cohorts proposed by Brosdahl and Carpenter (2011). The cohorts considered are Baby Boomers (born from 1946 to 1960), Generation X (from 1961 to 1981), and Millennials (from 1981 to 2000). Moreover, knowing that Millennials are most likely to fall for cybercrime than any other generational cohort, (Federal Trade Commission, 2018), we will focus this study on this specific generational cohort. Consequently, our research question should be formulated as: *How does Protection Motivation (or Security Intentions) affect Millennials' online Use Behavior? Specifically, which other factors may influence their Use Behavior?*

To respond to our research question, we combined variables from two models, the Protection Motivation Theory (PMT) and the Reasoned Action Approach (RAA), with the goal of analyzing the existence of discrepancies among Security Intentions and Use Behavior and which other variables may influence Millennials Use Behavior, in the context of security precautions adopted by home computer users.
For the purpose of this research, Threat Severity was considered as a representative of Threat Appraisals, as some authors have already described it as an important predictor of Security Intentions (Zahedi et al 2015). However, there are some contradictory research results on the significance of this variable as a predictor for Protection Motivation (Tsai et al 2016). As for Coping Appraisals, the variables considered were: Response Costs, Response Efficacy, Subjective Norms, and Safety Habit Strength. Response Costs should evolve in the opposite direction of Protection Motivation, as individuals will show a greater intention to perform protective measures when costs are lower (Tsai et al 2016). According to Response Efficacy, the more effective a behavior is perceived to be, the more individuals will intend to adopt it. Subjective Norms relate with the influence that individuals have on each other (Ajzen 1991). Safety Habit Strength is related with an individual's routine of performing protective behaviors (Tsai et al 2016). This leads to hypotheses H_{1a}, H_{1b}, H_{1c}, H_{1d}, and H_{1e}, as follows.

H_{1a}: Threat Severity increases the Protection Motivation of Millennials.
H_{1b}: Response Costs decrease the Protection Motivation of Millennials.
H_{1c}: Response Efficacy increases the Protection Motivation of Millennials.
H_{1d}: Subjective Norms increase the Protection Motivation of Millennials.
H_{1e}: Safety Habit Strength increases the Protection Motivation of Millennials.

As we are considering Millennials' Protection Motivation, the model should also seek predict the user's overall Use Behavior in terms of the security measures he/she adopts when navigating online. The next step was to study the influence of Millennials' Protection Motivation on their Use Behavior. This leads to hypothesis H_2, as presented below.

H_2: Protection Motivation positively affects Millennials' online Use Behavior.

Medeiros, A.S., Martinez, L.F., & Martinez, L.M. (2020). Assessing the determinants of Millennials' online protective behavior: How their protection motivation translates into actual use behavior. In F. J. Martínez-López and S. D'Alessandro (Eds.), *Advances in Digital Marketing and eCommerce: First International Conference, 2020 (pp. 153-162)*. Cham, Switzerland: Springer Proceedings in Business and Economics. https://doi.org/10.1007/978-3-030-47595-6_20

As for the RAA, it is described by the authors as a unified approach that accounts for any behavior, and should therefore also be applicable to our Research Question (Jansen et al 2017). In 2017 Jansen and Schaik combined the PMT and RAA to study the precautionary behavioral intention in online banking, and concluded that the variables of the integrated model are strong predictors for that specific research topic. Following this rationale, by considering variables present in both the PMT and RAA, we expect that the model created has good explanatory power. As the main objective of this paper is to explain which variables may affect the Millennials' Use Behavior, the variable Actual Control was incorporated. Actual Control includes the user's relevant skills, abilities, and environment conditions that may act as barriers or facilitators for behavioral performance (Fishbein and Ajzen 2010). This leads to hypothesis H_3, presented below.

H_3: Actual Control positively influences Millennials' Use Behavior.

Considering the discrepancies between the user's Actual Control and what he/she perceives, it is also imperative to incorporate in the model a variable that translates the Perceived Control. In current literature this variable is described as the perception about being able to control one's own destiny, and thus, claim responsibility for one's own actions (Workman et al 2008). Also, this variable has been incorporated by some authors in the PMT (Workman et al 2008). A high Locus of Control may imply a greater sense of responsibility for online safety (Jansen et al 2017). Based on this, we arrive at hypothesis H_4, as follows:

H_4: Locus of Control positively influences Millennials' Use Behavior.

Lastly, considering that a positive attitude toward a certain behavior is considered to positively influence that behavior (Fishbein and Ajzen 1975), the variable Attitude toward Online Safety (Attitude TOS) was incorporated in the model (Figure 1). This leads to hypothesis H_5, as presented below:

H_5: Attitude toward Online Safety positively influences Millennials' Use Behavior.

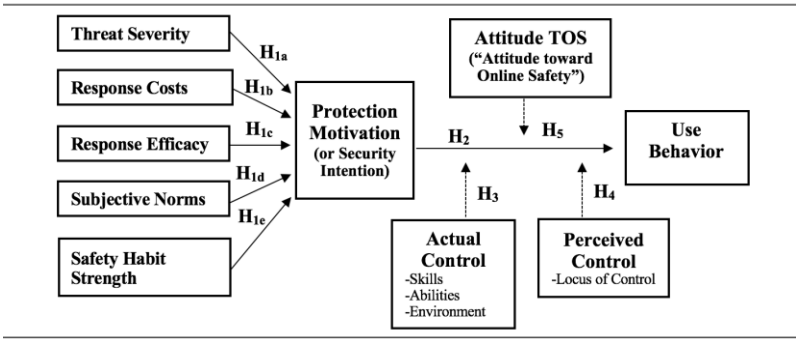

Fig. 1: The research model based on the Protection Motivation Theory (Rogers 1975) and the Reasoned Action Approach (Fishbein and Ajzen 2010).

Medeiros, A.S., Martinez, L.F., & Martinez, L.M. (2020). Assessing the determinants of Millennials' online protective behavior: How their protection motivation translates into actual use behavior. In F. J. Martínez-López and S. D'Alessandro (Eds.), *Advances in Digital Marketing and eCommerce: First International Conference, 2020 (pp. 153-162)*. Cham, Switzerland: Springer Proceedings in Business and Economics. https://doi.org/10.1007/978-3-030-47595-6_20

5 Methodology

Our research was conducted through a web-based survey constructed with Qualtrics software. We considered 236 valid respondents (from 267): 71.6% were female and 26.4% were male; 75.8% had a Bachelor's degree or higher; 22 countries were represented in the sample (including 55.9% of respondents from Portugal, 9.3% from the USA, 5.1% from France, and 3.4% from Germany). The variable *Threat Severity* was modified from Liang and Xue (2010) and Tsai el al. (2016), and the items were measured using the same scale used by those authors; *Response Efficacy* was modified from literature of the same authors; *Subjective Norms* was adapted from the research of Anderson et al. (2010) and Tsai et al. (2016); *Response Costs* was based on the research of Liang and Xue (2010); *Safety Habit Strength* was adapted from Venkatesh et al. (2012) and Tsai et al. (2016); *Protection Motivation* (or *Security Intentions*) was modified from the research of Agarwal (2010), Liang and Xue (2010), and Tsai et al. (2016); *Actual Control* was self-developed according to the definition of Ajzen and Fishbein (2010); *Attitude toward Online Safety* was adapted from Mishra et al. (2014); *Locus of Control* was adapted from Workman et al. (2008); and, finally, *Use Behavior* was derived from the *Protection Motivation* variable, but focused on the user's current behavior instead of intentional behavior. For each variable, a Cronbach's Alpha was computed as a measure of reliability. The values obtained were greater than .70, which translates into a satisfactory level of internal consistency.

6 Results and Discussion

Previous research supports that variables such as Response Efficacy, Subjective Norms, Response Costs, and Safety Habit Strength could predict individual's intention to undertake protective measures when navigating online (Tsai et al 2016). Similarly, our research suggests that Response Efficacy, Subjective Norms, and Safety Habit Strength are good predictors for Millennials' Protection Motivation. However, the same does not apply to Response Costs, considering that in our results this variable has little effect on Millennials' Security Intentions. As for the variable Threat Severity, past research is contradictory, as some authors believe that the variable has a negative significance when predicting Security Intentions (Tsai et al 2016) and others state that the variable has no explanatory power. Our research suggests that this variable is not a significant predictor for Protection Motivation, as suggested by LaRose et al. (2007).

The main objective of this research was to understand the impact of Protection Motivation (or Security Intentions) on Millennials' Use Behavior when navigating online in terms of the protective measures they adopt. As described in hypothesis H_2, although Security Intentions positively influence Use Behavior, this research has found that there is a gap between the two variables, considering that Protection Motivation explains only partially the variation of Use Behavior (approximately

Medeiros, A.S., Martinez, L.F., & Martinez, L.M. (2020). Assessing the determinants of Millennials' online protective behavior: How their protection motivation translates into actual use behavior. In F. J. Martínez-López and S. D'Alessandro (Eds.), *Advances in Digital Marketing and eCommerce: First International Conference, 2020 (pp. 153-162)*. Cham, Switzerland: Springer Proceedings in Business and Economics. https://doi.org/10.1007/978-3-030-47595-6_20

29.9%). This being the case, this research has also focused on explaining which factors may give rise to this variance between behavioral intentions and actual behavior. According to our findings, even though the variables Threat Severity, Response Efficacy, and Subjective Norms are good predictors for Protection Motivation (**Model 1**), the same does not apply when estimating Use Behavior. As seen in **Model 3** and **Model 4**, from the variables initially used in the PMT to estimate Protection Motivation, Safety Habit Strength revealed to be the only strong predictor for Use Behavior. These conclusions are rather interesting, meaning that Millennials do consider these five factors when deciding on a behavior. However, later on, Safety Habit Strength becomes the only significant factor they rely on when behaving in a certain manner. Results are shown in Tables 1 and 2.

Additionally, new factors were added to the analysis to optimize our ability to explain Use Behavior. As stated in hypothesis H_3, Actual Control was found to be a good predictor for Use Behavior, as it was able to increase our ability to explain the dependent variable to 36.3%. As shown by **Model 4,** the user's skills, abilities, and environment play an important role in explaining Use Behavior. Lastly, hypotheses H_4 and H_5 were not supported by **Model 4**, and consequently, Perceived Control (Locus of Control) and Attitude toward Online Safety are not able to further explain the variation of Use Behavior. However, as stated above, there is a positive correlation between Use Behavior and the two variables Attitude toward Online Safety ($r = 0.321$, $p < .01$) and Locus of Control ($r = 0.211$, $p < .01$), which can indicate that these variables may have been suppressed by the others.

Variable	B	S.E.	β	T	Sig.
(constant)	.971				
Response Efficacy	.201	.074	.178	2.731	.007
Subjective Norms	.180	.052	.227	3.465	.001
Safety Habit Strength	.220	.047	.280	4.674	.00001
Response Costs	.015	.047	.020	.326	.745
Threat Severity	.148	.078	.117	1.904	.058
	R = .555		**R^2 =**. 309	**Adjusted R^2 =** .293	

Table 1: Regression with Protection Motivation as the dependent variable.

7 Conclusion

This research was able to establish a gap between behavioral intention and actual behavior in terms of protective measures that Millennials adopt when navigating online. In addition, the model formulated was able to determine that Safety Habit Strength and Actual Control, which include individual's skills, abilities, and the environment factor, are significant when explaining Millennials' Use Behavior. One important limitation is that measuring Use Behavior can be quite challenging, as users might not be totally honest in the way they express their actual behavior. These findings can contribute to improving the overall security of the cyberspace as it becomes easier to influence Millennials adopting a safer online behavior.

Medeiros, A.S., Martinez, L.F., & Martinez, L.M. (2020). Assessing the determinants of Millennials' online protective behavior: How their protection motivation translates into actual use behavior. In F. J. Martínez-López and S. D'Alessandro (Eds.), *Advances in Digital Marketing and eCommerce: First International Conference, 2020 (pp. 153-162)*. Cham, Switzerland: Springer Proceedings in Business and Economics. https://doi.org/10.1007/978-3-030-47595-6_20

Variable	Model 2					Model 3					Model 4				
	B	S.E.	β	T	Sig.	B	S.E.	β	T	Sig.	B	S.E.	β	T	Sig.
(constant)	1.576					1.120					.837				
Protection Motivation	.429	.057	.446	7.591	.00001	.243	.062	.252	3.909	.00001	.247	.067	.419	1.999	.00001
Response Efficacy						.048	.070	.044	.692	.490	.057	.076	.053	.753	.452
Subjective Norms						.051	.050	.067	1.024	.307	.053	.050	.070	1.060	.290
Safety Habit Strength						.298	.046	.394	6.473	.00001	.270	.052	.357	5.203	.00001
Response Costs						-.042	.044	-.560	-.956	.340	-.039	.044	-.053	-.887	.376
Threat Severity						-.013	.073	-.010	-.171	.864	.003	.075	.003	.042	.966
Actual Control											.117	.061	.126	1.932	.055
Locus of Control											-0.60	.048	-0.078	-1.246	.214
Attitude TOS											.013	.092	.011	.143	.886
	R=.446	**R²**=.351		**Adjusted R²**=.195		**R**=.593	**R²**=.351		**Adjusted R²**=.293		**R**=.603	**R²**=.363		**Adjusted R²**=.338	

Table 2: Hierarchical multiple regression with *Use Behavior* as the dependent variable.

Medeiros, A.S., Martinez, L.F., & Martinez, L.M. (2020). Assessing the determinants of Millennials' online protective behavior: How their protection motivation translates into actual use behavior. In F. J. Martínez-López and S. D'Alessandro (Eds.), *Advances in Digital Marketing and eCommerce: First International Conference, 2020 (pp. 153-162)*. Cham, Switzerland: Springer Proceedings in Business and Economics. https://doi.org/10.1007/978-3-030-47595-6_20

Acknowledgments

This work was funded by Fundação para a Ciência e a Tecnologia (UID/ECO/00124/2013, UID/ECO/00124/2019 and Social Sciences DataLab, LISBOA-01-0145-FEDER-022209), POR Lisboa (LISBOA-01-0145-FEDER-007722, LISBOA-01-0145-FEDER-022209) and POR Norte (LISBOA-01-0145-FEDER-022209). The authors declare that they have no conflict of interest. All procedures performed in studies involving human participants were in accordance with the ethical standards of the institutional and/or national research committee and with the 1964 Helsinki declaration and its later amendments or comparable ethical standards. Informed consent was obtained from all individual participants included in the study.

References

Ajzen, I. (1991). "The theory of planned behavior." *Organizational Behavior and Human Decision Processes, 50*(2), 179–211.

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

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M.J.G., Levi, M., Moore, T., and Savage, S. (2013). "Measuring the cost of cybercrime." In R. Böhme (Ed.), *The economics of information security and privacy* (pp. 265–300). Heidelberg: Springer.

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

Brosdahl, D., and Carpenter, J. (2011). "Shopping orientations of US males: A generational cohort comparison." *Journal of Retailing and Consumer Services, 18*(6), 548–554.

Chang, M., Cheung, W., and Lai, V. (2005). "Literature derived reference models for the adoption of online shopping." *Information and Management, 42*(4), 543–559.

Conner, M., McEachan, R., Lawton, R., and Gardner, P. (2017). "Applying the Reasoned Action Approach to understanding health protection and health risk behaviors." *Social Science & Medicine, 195*, 140–148.

Crossler, R., Johnston, A., Lowry, P., Hu, Q., Warkentin, M., and Baskerville, R. (2013). "Future Directions for Behavioral Information Security Research." *Computers & Security, 32*, 90-101.

Dodge, R., Carver, C., and Ferguson, A. (2007). "Phishing for user security awareness." *Computers & Security*, 26(1), 73-80.

European Commission (2017). Resilience, deterrence and defence: Building strong cybersecurity in Europe. [online] Available at: https://ec.europa.eu/digital-single-market/en/news/resilience-deterrence-and-defence-building-strong-cybersecurity-europe [Acessed 24th September of 2018].

Fishbein, M., and Ajzen, I. (1975). "*Belief, attitude, intention, and behavior*." Reading, MA: Addison-Wesley Publishing Company.

Fishbein, M., and Ajzen, I. (2010). "*Predicting and changing behavior: The Reasoned Action Approach."* New York: Taylor & Francis Group.

Hanafizadeh, P., Keating, B., and Khedmatgozar, H. (2014). "A systematic review of Internet banking adoption." *Telematics and Informatics, 31*(3), 492–510.

Hulst, F., and Posthumus, H. (2016). "Understanding (non-)adoption of conservation agriculture in Kenya using the Reasoned Action Approach." *Land Use Policy, 56*, 303–314.

Jansen, J., and Schaik, P. (2017). "Comparing three models to explain precautionary online behavioural intentions." *Information & Computer Security, 5*(2), 165–180.

Medeiros, A.S., Martinez, L.F., & Martinez, L.M. (2020). Assessing the determinants of Millennials' online protective behavior: How their protection motivation translates into actual use behavior. In F. J. Martínez-López and S. D'Alessandro (Eds.), *Advances in Digital Marketing and eCommerce: First International Conference, 2020 (pp. 153-162)*. Cham, Switzerland: Springer Proceedings in Business and Economics. https://doi.org/10.1007/978-3-030-47595-6_20

Kritzinger, E., and Solms, S. (2010). "Cyber security for home users: A new way of protection through awareness enforcement." *Computers & Society, 29*(8), 840–847.

Lagazio, M., Sherif, N., and Cushman, M. (2014). "A multi-level approach to understanding the impact of cybercrime on the financial sector." *Computers & Society, 45*, 58–74.

LaRose, R., Rifon, N., and Wirth, C. (2007). "Online safety begins with you and me: Getting Internet users to protect themselves." *Paper presented at the 57th International Communication Association Conference*.

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), 394–413.

Liu, Y., Segev, S., and Villar, M. (2017). "Comparing two mechanisms for green consumption: cognitive-affect behaviour vs. theory of reasoned action." *Journal of Consumer Marketing, 34*(5), 442–454.

Mishra, D., Akman, I., and Mishra, A. (2014). "Theory of Reasoned Action application for Green Information Technology acceptance." *Computers in Human Behavior, 36*, 29–40.

Pinho, J., and Soares, A. (2011). "Examining the technology acceptance model in the adoption of social networks." *Journal of Research in Interactive Marketing, 5*(2/3), 116–129.

Poepjes, R., and Lane, M. (2012). "An Information Security Awareness Capability Model (ISACM)." *Australian Information Security Management Conference (SECAU 2012).*

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

Rogers, R. (1983). "Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation." In J.T. Cacioppo and R.E. Petty (Eds.), *Social Psychophysiology: A sourcebook* (pp. 153–177). New York, Guilford Press.

Romanosky, S. (2016). "Examining the costs and causes of cyber incidents." *Journal of Cybersecurity*, 2(2), 121–135.

Ryder, N. (1965). "The Cohort as a Concept in the Study of Social Change." *American Sociological Review, 30*, 843–861.

Saridakis, G., Benson, V., Ezingeard, J., and Tennakoon, H. (2015). "Individual information security, user behaviour and cyber victimisation: An empirical study of social networking users." *Technological Forecasting and Social Change, 102*, 320–330.

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

Venkatesh, V., Thong, J., and Xu, X. (2012). "Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology." *MIS Quarterly, 36*, 157–178.

Workman, M., Bommer, W., and 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.

Zahedi, F., Abbasi, A., and Chen, Y. (2015). "Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance." *Journal of the Association for Information Systems, 6*(16), 448–484.

Zhou, L., Dai, L., and Zhang, D. (2007). "Online shopping acceptance model: A critical survey of consumer factors in online shopping." *Journal of Electronic Commerce Research, 8*(1), 41–62.

Medeiros, A.S., Martinez, L.F., & Martinez, L.M. (2020). Assessing the determinants of Millennials' online protective behavior: How their protection motivation translates into actual use behavior. In F. J. Martínez-López and S. D'Alessandro (Eds.), *Advances in Digital Marketing and eCommerce: First International Conference, 2020 (pp. 153-162).* Cham, Switzerland: Springer Proceedings in Business and Economics. https://doi.org/10.1007/978-3-030-47595-6_20