A Work Project, presented as part of the requirements for the Award of a

Master Degree in Management from NOVA School of Business and Economics

ACCESSING THE DETERMINANTS OF MILLENNIALS' ONLINE PROTECTIVE BEHAVIOUR: HOW THEIR PROTECTION MOTIVATION TRANSLATES INTO ACTUAL USE BEHAVIOUR

Ana Sofia Rocha de Medeiros

student no. 4257

A Project carried out on the Master in Management Program, under the supervision of:

Prof. Luis F. Martinez

January of 2019

Table of Contents

ACCESSING THE DETERMINANTS OF MILLENNIALS' ONLINE PROTECTIVE BEHAVIOUR: HOW THEIR PROTECTION MOTIVATION TRANSLATES INTO ACTUAL USE BEHAVIOUR

Abstract

This research focuses on assessing the determinants of Millennials Protection Motivation (or Security Intentions) on their actual Use Behaviour when navigating online in terms of the protective measures they adopt. For this purpose, the proposed model integrates variables from two widely accepted behavioural theories, the Protection Motivation Theory and the Reasoned Action Approach. Hence, an online survey was conducted, relying on 236 responses, which were analysed through hierarchical multiple regression. Results show a gap between Security Intentions and Use Behaviour and indicate Safety Habit Strength and Actual Control as significant at predicting Use Behaviour. Differently to published literature, this research analyses not only behavioural intention, but also the user's actual Use Behaviour.

Keywords: Security Intentions; Protection Motivation; Use Behaviour; Online Security.

Acknowledgements

This accomplishment would not have been possible without all the help and support I had during the last few months. I would like to start by expressing my sincere appreciation to my work project advisor, Professor Luis F. Martinez, for his patience, guidance and continuously helping me at any point of this process. Secondly, I would like to thank to my family and friends for always being there for me and motivating me to constantly do better.

1. Introduction

"Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. (...) Cyber-attacks know no borders and no one is immune."

Jean-Claude Juncker, European Commission President, 13th September 2017

In today's society, businesses and individual citizens rely on digital services and technologies for their everyday activities. Sectors, such as transport, energy, health and finance have become increasingly dependent on network and information systems to run their core businesses (European Commission, 2017), while individuals increasingly trust their most personal information to systems that in return provide them with a greater commodity and quality of life. The commonly found issue, is that most times these distinct users are not fully aware of the dangers that they incur just on a daily basis. The World Bank (2014) stated that despite the rise of the levels of penetration of Internet use at a world-level, behaviours in order to protect the users own privacy have not progressed at the same pace (Ögütçü et al., 2016).

Additionally, the rapid growth of technology is converting cyberattacks to be more sophisticated, specialized and concentrated in nature (KPMG, 2017), as attackers are targeting specific organizations and individuals through initiatives that are organization-oriented, such as malware (computer programs that invade the devices as they are connected to the Internet), theft of intellectual property and corporate espionage, or user-oriented, which include identity theft, credit card fraud, phishing and malware (Hunton, 2009).

As this type of criminal activity continues to increase, cybercrime damages are estimated to cost close to $6 trillion annually in 2021 (Cybersecurity Ventures, 2017). These predictions, aligned with the growing number of internet users (Gartner, 2017) and the introduction of new technologies reinforce that "cybercriminal activity is one of the biggest challenges that humanity will face [over] the next two decades" (Cybersecurity Ventures, 2017). As a consequence of the potential loss for any company, most organizations are now investing in training their employees to anticipate and prevent incidents related with

cybercriminal activity. Although this contributes to the awareness of cybercrime as a society's problem, home users (or individual users) are still lacking training and knowledge as they are not subject to any preparation before using the Internet. Consequently, both individuals and corporations will continue to bear the costs of cybercrime, as the users or their relatives' past experience might influence their feelings of trust regarding the systems and platforms of companies, such as online banking or online shopping, and therefore, lead users to avoid using them or even blame the organization for any security incident related with their lack of preventative behaviour, transforming in a loss for the corporation and its reputation.

As the dangers for society, individuals and the economy increase at a concerning rate, even the individuals who lack training before navigating online are starting to be more aware of their vulnerability considering some have already experienced threats related to scams that risk their personal information and may eventually harm their professional reputation (Tsai el al., 2016). This negative experience continues to contribute to a growing sense of unsafety when navigating online. Additionally, a recent study by the European Commission (2017), has concluded that 86% of the European Citizens believe that the risk of becoming a cybercrime victim is actually increasing. All this leads to an increase in the user's risk perception, which would be expected to result in additional preventative measures taken by the user. However, there is a discrepancy between realizing that there is a threat and taking an actual behaviour to prevent a certain outcome (Tsai el al., 2016).

In summary, it is of extreme importance to understand home users, their behavioural intention and their actual behaviours when using the Internet. This way, it becomes possible to understand and even predict how users will try to protect their information and adapt their behaviour to the increasing dangers of cybercrime.

2. Literature Review

Considering the strong impacts of cybercrime related activity, its causes, drivers and effects have been widely studied in the past (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 centred in the implications for organizations (Saridakis et al., 2015). As already mentioned, contrarily to employees in a work setting, home users are not subject to training (Anderson et al., 2010), and frequently, 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), this type of users "represent a significant point of weakness in achieving the security of the cyber infrastructure". Thus, home users, exemplify an interesting area of study.

A recent study from the European Commission (2017) states that 51% of the European citizens do not feel well informed about cyber threats and, has already mentioned, 87% believe the risk of becoming a victim of cybercrime is currently increasing. These values are rather concerning, as they reflect 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, from the user lack of knowledge relative to cybercrime it is possible to reach another widely mentioned topic in the literature review which is cybercrime awareness. According to Dodge et al. (2007), the variable awareness is hard to characterize due to the "user's individual nature". Moreover, 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 analyse its influence on the user's behavioural intention and actual protective behaviour. Current approaches include the Rational Choice Theory (RCT), the Reactance Theory and the Justice Theory, which are once again focused in the organizational context. On the other hand, Rogers (1975, 1983) has proposed the Protection

Motivation Theory (PMT) which is based on the Theory of Reasoned Action (Fishbein et al., 1975).

2.1. Protection Motivation Theory (PMT)

Commonly found in academic literature (e.g. Tsai et al. 2016, Boss et al. 2015, Crossler et al. 2014), the PMT tries to explain the reasons that lead to protective behaviours and how individual users undertake those behaviours (Rogers, 1975, 1983). Currently, the PMT has gained numerous supporters has it has been extended to understand the drivers for online safety behaviour, 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 behaviours 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 behaviours (Tsai et al., 2016). Also, Tsai et al. (2016), was able to establish a strong link between behaviour intentions of home users and online habit strength, as in accordance with LaRose et al. (2007).

Most existent research tries to comprehend and predict Security Awareness and, consequently, Security Intentions (Tsai et al., 2016; Boss et al., 2015). However, there is a literature discrepancy related to security related behaviours. This translates in the inexistence of further research that analyses how home user's Protection Motivation (or Security Intentions) convert into actual Use Behaviours when using the Internet. Boss et al. (2015) wrote about this issue, still, his study focuses mostly on Fear Appeals instead on the actual study of the individual's Use Behaviour.

Consequently, it is important to further comprehend the existent models that attempt at explaining people's actual behaviour, so it is possible to understand the effect of behavioural intentions on the user's behaviour. From existent literature, the most relevant models at studying individual's behaviour are the Theory of Reasoned Action (TRA) and the Theory of

Planned Behaviour (TPB), and both aim at predicting individual's behaviour based on intentions and pre-existing attitudes (Fishbein & Ajzen, 1975; Saridakis et al., 2015). From these theories, many have been derived. One of the most widely studied is the Reasoned Action Approach (RAA).

2.2. Reasoned Action Approach (RAA)

Firstly described by Fishbein and Ajzen (2010), the same authors of the Theory of Reasoned Action (Fishbein & Ajzen, 1975) and the Theory of Planned Behaviour (Ajzen, 1991). The RAA has been commonly used in the past to predict people's behaviour in diverse subjects, such as Health (Conner et al., 2017), Agriculture (Hulst et al., 2016) and Consumer Behaviour (Liu et al., 2017). In terms of online behaviour, its applications have been extended to the study of several areas ranging from online shopping behaviour (Chang et al., 2005, Zhou et al., 2007) to the adoption of social networks (Pinho et al., 2011) and of online banking (Hanafizadeh et al., 2013). According to this theory, Attitudes, Perceived Norms, and Perceived Control guide the user's behavioural intentions and actual behaviour. Also, Behavioural Intention is stated as the best single predictor for Use Behaviour, since the stronger intentions have a greater probability of transforming into actual behaviours. Equally, the RAA also states that Use Behaviour is moderated by the variable Actual Control, which includes the user's skills, abilities and the environmental factors (Ajzen & Fishbein, 2010). As stated in this theory, people are only able to perform a certain behaviour if they have the requisite skills and abilities, and if there are no environmental constraints preventing them from acting on their specific behavioural intentions.

In brief, intention is described as a strong predictor for Use Behaviour, however, current literature is not able to fully explain the influence of Protection Motivation on Millennials Use Behaviour. Also, published literature does not consider other variables which might be significant at predicting Use Behaviour applied to this field of study.

2.3. 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 Behaviour* 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 & Fishbein, 2010). For that reason, Cohort Theory was used, allowing for a greater understanding of the actual behaviour of a specific generation as generational cohorts differ not only in age but also in education, relationship 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 considered cohorts are Baby Boomers (born from 1946 to 1960), followed by 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, the main research question should be formulated as: How does *Protection Motivation* (or *Security Intentions*) affect Millennials' online *Use Behaviour*? And which other factors may influence their *Use Behaviour*?

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 objective of analysing the existence of discrepancies among *Security Intentions* and *Use Behaviour* and which other variables may influence Millennials *Use Behaviour,* 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 considered variables were: *Response Costs, Response Efficacy, Subjective Norms* and *Safety Habit Strength*. *Response Costs*, which should evolve in the opposite direction of *Protection Motivation* as individuals will show a gretaer intentions to perform protective measures when costs are lower (Tsai et al., 2016). According to *Response Efficacy*, the more effective a behaviour is perceived to be, the more individuals will intend to adopt it. As for *Subjective Norms*, they relate with the influence that individuals have on each other (Ajzen, 1991). And *Safety Habit Strength* is related with individual's routine of performing protective behaviours (Tsai et al., 2016).

Thus, 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 increases the Protection Motivation of Millennials.*

H_{1e}: *Safety Habit Strength increases the Protection Motivation of Millennials.*

Now that we are considering Millennials' *Protection Motivation*, the model should also try at predicting the user's overall *Use Behaviour* 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 Behaviour*.

This leads to hypothesis H_2, as presented below.

H_2: *Protection Motivation positively affects Millennials' online Use Behaviour.*

As for the RAA, it is described by the authors as a unified approach that accounts for any behaviour, and in result, should 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

behavioural intention in online banking, having 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, it is expected that the created model has a good explanatory power. Since the main objective of this paper is to explain which variables may affect the Millennials' *Use Behaviour*, 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 behavioural performance (Fishbein & Ajzen, 2010).

Hence, leading to hypothesis H_3, presented below.

H_3: *Actual Control positively influences Millennials Use Behaviour.*

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 their own destiny, and thus, claim responsibility for their own actions (Workman et al., 2008). Also, this variable has, in the past, been incorporated by some authors in the PMT (Workman et al., 2008). This way, 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:

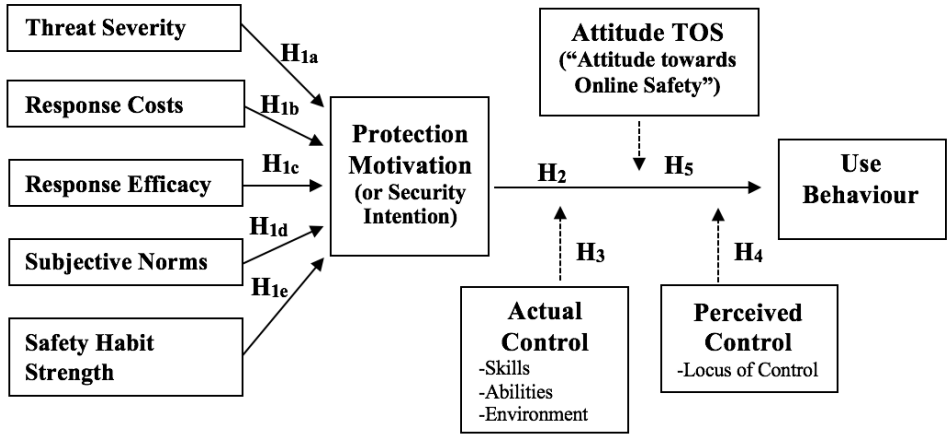
H_4: *Locus of Control positively influences Millennials Use Behaviour.*

Lastly, considering that a positive attitude towards a certain behaviour is considered to positively influence that behaviour (Fishbein & Ajzen, 1975), the variable *Attitude towards Online Safety* (*Attitude TOS*) was incorporated in the model.

Therefore, this leads to hypothesis H_5, as presented below:

H_5: *Attitude towards Online Safety positively influences Millennials Use Behaviour.*

Figure 1. Self-made based on the PMT and RAA.



3. Methodology

3.1. Procedure and Participants

In order to understand the influence of *Security Intentions* on Millennials *Use Behaviour*, research was conducted through a web-based survey constructed with Qualtrics Survey software. The questionnaires were distributed randomly using social media (e.g. Facebook, LinkedIn), from 28th October to 27th November of 2018, and asked participants to respond to an 8-minute anonymous survey. The survey relied on Snowball sampling and comprised questions related with the respondents' own experience, perception, behavioural intention and past behaviour. Additionally, it included questions related with demographic information, such as Birth Year and Nationality.

As the analysis focuses on Millennials, there was a constraint related to Birth Year, meaning valid responses had only participants born between 1981 and 1999. Consequently, from the 267 distributed questionnaires, 31 were not considered for the analysis, as the age of the respondents was not inside the stated parameter. In terms of characteristics of the 236 respondents, 71.6% were female and 26.4% were male, and from all valid respondents 75.8% had a Higher degree course. As for nationality, 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. Other nationalities included, for example, the UK, Angola, China, Switzerland, Japan, Pakistan and Singapore. Respondents were summarised in function of their Gender, Age and Education level in **Table 1.** and **Table 2.**, as presented below.

Table 1. Sample Characterization by Birth Year (frequency).

Birth Year				Total
1981-1985	1986-1990	1991-1995	1996-1999	
15	15	79	127	**236**

Table 2. Sample Characterization by Education Level (frequency).

High School graduate	Some college	Bachelor degree	Master degree	Professional degree	PhD	Total
25	28	124	51	4	4	**236**

3.2. Measures

The survey entailed measures from previous published literature, that where adapted considering the proposed Research Question. The variable *Threat Severity* was modified from published literature by Liang and Xue (2010) and Tsai el al. (2016) and the items were measured using the same scale as the authors: a five-point Likert-type scale, ranging from Extremely Harmful (5) to Not Harmful at all (1); *Response Efficacy* was modified from published literature by the same authors and the items were measured using a five-point Likert-type scale, ranging from Strongly Agree (5) to Strongly Disagree (1); *Subjective Norms* was adapted from the research of Anderson et al. (2010) and Tsai et al. (2016) and it was measured using a five-point Likert-type scale, ranging from Strongly Agree (5) to Strongly Disagree (1); *Response Costs* was based on the research of Liang and Xue (2010) and was measured on a five-point Likert-type scale, ranging from Strongly Agree (5) to Strongly Disagree (1); *Safety Habit Strength* was adapted from Venkatesh et at. (2012) and Tsai et al. (2016) and was measured with a five-point Likert-type scale, ranging from Strongly Agree (5) to Strongly Disagree (1); *Protection Motivation* (or *Security Intentions*) was modified from the research of Agarwal (2010), Liang and Xue (2010) and Tsai el al. (2016) and was measured using a five-point Likert-type scale, ranging from Strongly Agree (5) to Strongly Disagree (1); *Actual Control* was self-developed

according to the definition of Ajzen and Fishbein (2010) and was measured using a five-point Likert-type scale, ranging from Strongly Agree (5) to Strongly Disagree (1); *Attitude towards Online Safety* was adapted from Mishra et al. (2014) and was measured with a five-point Likert-type scale, ranging from Strongly Agree (5) to Strongly Disagree (1); *Locus of Control* was adapted from Workman et al. (2008) and was measured with a five-point Likert-type scale, ranging from Strongly Agree (5) to Strongly Disagree (1); And, finally, *Use Behaviour* was derived from the *Protection Motivation* variable, but focused on the user's current behaviour instead of intentional and was measured using a five-point Likert-type scale ranging from Strongly Agree (5) to Strongly Disagree (1).

For each variable, a Cronbach's Alpha was computed as a measure of reliability. As visible in **Table 3.**, the obtained values were in all cases greater than 0.70, which translates in a satisfactory level of internal consistency. Moreover, **Table 3.** also provides a summary for the studied variables, the items that constitute each of them and their sources.

Table 3. Summary of variables measurement and their sources.

Measure	Items	Source	Cronbach's Alpha
Threat Severity	Malware is a general term that refers to computer programs that invades your computer, tablet or cell phone as you use the Internet. How harmful to you would malware be if... 1. The information is used to commit crimes against me. 2. It makes my computer run more slowly. 3. It reveals my passwords to online criminals. 4. It reveals my credit card information.	Adapted from Liang and Xue (2010) and Tsai et al. (2016).	.753
Response Efficacy	Rate the following according to your experience and perception when navigating online. 1. Protective software would be useful for detecting and removing malware. 2. Protective software would increase my performance in protecting myself from malware. 3. Protective software would enable me to search and remove malware faster.	Adapted from Liang and Xue (2010) and Tsai el al. (2016)	.803
Subjective Norms	Rate the following according to your experience and perception when navigating online. 1. Friends who influence my behaviour would think that I should take measures to secure myself online. 2. Significant others who are important to me would think that I should take measures to secure myself online. 3. My peers would think that I should take measures to help secure the Internet.	Adapted from Anderson and Agarwal (2010) and Tsai et al. (2016)	.905

Response Costs	Rate the following according to your experience and perception when navigating online. 1. I do not know how to get security protections. 2. Security protections may cause problems to other programs on my computer. 3. Using security protections is too much trouble.	Adapted from Liang and Xue (2010)	.723
Safety Habit Strength	Rate the following according to your experience and perception when navigating online. 1. The use of security protections has become a habit for me. 2. Using security protections has become natural to me. 3. Online security protection is something I do automatically. 4. Online protection is something I do without thinking. 5. Online safety protection is part of my regular routine.	Adapted from Venkatesh et al. (2012) and Tsai et al. (2016)	.919
Protection Motivation (or Security Intentions)	Thinking of your future actions, indicate the degree to which you agree or disagree with the following statements regarding your likelihood of implementing security measures to protect yourself online. 1. I intend to take security measures to protect myself when using the internet. 2. I intend to change my passwords more often. 3. I intend to use passwords that are harder to guess. 4. I intend to change my browser security settings to a higher level. 5. I intend to learn how to be more secure online. 6. I will update my protective software regularly.	Adapted from Anderson and Agarwal (2010), Liang and Xue (2010) and Tsai el al. (2016).	.856
Actual Control (skills, ability, environment)	Rate the following according to your experience and perception when navigating online. 1. I have the necessary skills to secure myself when using my computer. 2. Taking necessary security measures is easy. 3. I feel comfortable taking measures to secure my computer. 4. I do not feel nervous when I think about online security issues. 5. In general, I am safer from online threats in my home. 6. I feel safer from online threats when connecting through the Wi-Fi of someone I know.	Personal elaboration according to Ajzen and Fishbein (2010)'s definition of each variable	.790
Attitude TOS	Rate the following according to your experience and perception when navigating online. 1. I like to feel protected when I navigate online. 2. Taking protective measures benefits me. 3. Taking protective measures is worth it.	Adapted from Mishra et al. (2014)	.853
Locus of Control	Rate the following according to your experience and perception when navigating online. 1. Keeping my information safe is within my control (5). 2. I believe that is within my control to protect myself from security violations.	Adapted from Workman et al. (2008)	.832
Use Behaviour	Thinking of your actions, indicate the degree to which you agree or disagree with the following statements regarding your behaviour online. 1. I do take security measures to protect myself when using the internet. 2. I do change my passwords often. 3. I do use passwords that are harder to guess. 4. I do change my browser security settings to a higher level. 5. I do try to learn how to be more secure online. 6. I do update my protective software regularly.	Derived from the Protection Motivation variable, but focused on the user's current behaviour instead of intentional	.738
Demographic variables	1. Education Level. 2. Nationality. 3. Gender. 4. Birth Year.		

4. Data Analysis and Results

Table 4. Mean (M), Standard Deviation (SD) and Correlations between variables.

Variable	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
Threat severity (1)	1									
Response efficacy (2)	.415*	1								
Subjective norms (3)	.265*	.368**	1							
Response costs (4)	.055	.104	.355**	1						
Safety Habit Strength (5)	.148**	.289**	.240**	-.108	1					
Protection Motivation (6)	.292*	.395**	.399**	.097	.396**	1				
Actual Control (7)	-.105	.017	.096	.078	.450**	.137**	1			
Attitude TOS (8)	.416*	.587**	.321**	.001	.361**	.361**	0.020	1		
Locus of Control (9)	.059	.184**	.249**	-.054	.390**	.271**	.408**	.259**	1	
Use Behaviour (10)	.157**	.276**	.254**	-.045	.530**	.446**	.304**	.321**	.212**	1

* correlation is significant at the 0.05 level (2-tailed).
** correlation is significant at the 0.01 level (2-tailed).

Table 4., on the side, illustrates the correlation matrix for all variables, with the exception of the demographic variables. According to the displayed results, *Response Costs* is the only variable that is not significantly correlated with *Use Behaviour* and also, the only variable which is not significantly correlated with *Protection Motivation* (or *Security Intentions*). Furthermore, all the other variables, namely, *Threat Severity, Response Efficacy, Subjective Norms, Safety Habit Strength, Actual Control, Attitude towards Online Safety* and *Locus of Control,* are significantly correlated with *Use Behaviour* and *Protection Motivation*. Also, the two variables, *Use Behaviour* and *Protection Motivation,* are positively correlated with each other (r = 0.446). The strongest correlation with *Use Behaviour* is *Safety Habit Strength* (r = 0.530), while the strongest correlation for *Protection Motivation* is *Use Behaviour* (r = 0.446).

All the valid responses for the variables *Threat Severity, Response Cots, Response Efficacy, Subjective Norms* and *Safety Habit*

Strength were divided between "low" (0 - 2.4) and "high" (2.5 - 5), allowing to study whether having a higher or lower level of these five variables influences the level of Millennials' *Protection Motivation*, which also ranges from 0 to 5. To do so, the results of an independent t-test analysis are presented in the next paragraphs, alongside with a regression analysis, with *Protection Motivation* as the dependent variable, as shown in **Table 5.** below.

Table 5. Regression with Protection Motivation as the dependent variable.

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	

For the variable *Threat Severity*, findings suggest that, on average, individuals that perceive it at a higher level (M =3.914, SD = 0.750), have a higher *Protection Motivation* than individuals with a "low" *Threat Severity* (M = 2.750, SD=1.681, t: t(232) = 3.00, p = 0.018 < 0.05). Also, when considering the regression in **Table 5.**, *Threat Severity* has a significance level between 0.05 and 0.10, meaning that it is possible to support hypothesis H_{1a} with a 90% confidence level.

As for the variable *Response Costs,* when comparing the mean value for "low" *Response Costs* (M = 3.903, SD = 0.710) with a "high" value for this variable (M = 3.887, SD = 0.832), it is visible that the mean value does not vary considerably from one scenario to the other (t: t(231) = -0.155, p = 0.071 > 0.05). Additionally, the regression presented in **Table 5.**, leads to rejecting hypothesis H_{1b} as the significance level is 0.745, consequently, it is not possible to state that *Response Cots* influences the user's *Protection Motivation*.

According to the obtained results, a higher *Response Efficacy* (M = 3.906, SD = 0.752*)* is responsible for a greater *Protection Motivation*, than a lower *Response Efficacy* (M = 3.201, SD = 1.937, t: t(232) = 1.776, p = 0.0001 < 0.05). Moreover, as shown in **Table 5.**, *Response*

Efficacy has a significance level inferior to 0.05, meaning that it is possible to support hypothesis H_{1c} with a 95% confidence level.

When comparing the scenario with a "higher" value for the variable *Subjective Norms* (M = 3.988, SD = 0.710) with the scenario with a "lower" value (M = 3.333, SD = 0.968, t: t(231) = 4.582, p = 0.042 < 0.05), it is visible that, on average, higher *Subjective Norms* are responsible for a higher *Protection Motivation*. This conclusion is reinforced by the results obtained in the regression analysis, in **Table 5.**, as the significance level is 0.001, we are able to support hypothesis H_{1d} with a 95% confidence level.

As for the fifth variable, according to our findings, Millennials with a "high" *Safety Habit Strength* (M = 3.993, SD = 0.704), have, on average, a higher *Protection Motivation*, when compared to individuals with a lower *Safety Habit Strength* (M = 3.612, SD = 0.921, t: t(232) = 3.432, p = 0.028 < 0.05). Correspondingly, this is sustained by the regression presented above in **Table 5**., with a significance level of 0.00001, meaning we are able to support hypothesis H_{1e} with a 95% confidence level.

In summary, we are able to state that the variables *Threat Severity*, *Response Efficacy, Subjective Norms* and *Safety Habit Strength* have a positive influence on Millennials *Protection Motivation*. And, according to the regression analysis in **Table 5.**, are able to predict, approximately, 30.9% of its variability.

To test for the remaining hypotheses, a hierarchical multiple regression was performed with *Use Behaviour* as the dependent variable. For this analysis, three different models were created, which are displayed in **Table 6.**, presented in the next page.

Table 6. Hierarchical multiple regression with *Use Behaviour* as the dependent variable.

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	R^2=.351		Adjusted R^2=.195		R=.593	R^2=.351		Adjusted R^2=.293		R=.603	R^2=.363		Adjusted R^2=.338	

From **Model 2**, it is possible to state that *Protection Motivation* has a positive influence on Millennials *Use Behaviour*. As a result, hypothesis H_2 is supported by the analysis. However, as predicted, this variable is only able to estimate about 29.9% of the variation of *Use Behaviour*. This being said, **Model 3** was estimated as an attempt to analyse whether the estimators for *Protection Motivation* could increase the explanatory power of our model. By adding the variables *Response Efficacy, Subjective Norms, Safety Habit Strength, Response Costs* and *Threat Severity* we are able to explain approximately 35.1% of the variation of Millennials *Use Behaviour*. From this newly added variables, *Threat Severity, Response Costs, Subjective Norms* and *Response Efficacy* have shown not to be good predictors for *User Behaviour* as the significance level is superior to 0.10. As a result, *Protection Motivation* and *Safety Habit Strength* are the only significant variables when estimating the dependent variable.

With the objective to further explain the dependent variable, *Actual Control, Attitude towards Online Safety (TOS)* and *Locus of Control* were added in **Model 4**. This last model is able to explain approximately 36.3% of the variation of *Use Behaviour*. As for the newly added

variables, *Actual Control* significance level is between 0.05 and 0.10, and, therefore, we are able to support hypothesis H_3 with a 90% confidence level. Nonetheless, hypothesis H_4 and H_5 are not supported, as *Locus of Control* and *Attitude TOS* have a significance level superior to 0.10.

5. Discussion

Previous research supports that variables such as *Response Efficacy, Subjective Norms, Response Costs* and *Safety Habit Strength* are able to 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 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 Behaviour* when navigating online in terms of the protective measures they adopt. As described in hypothesis H_2, although *Security Intentions* positively influence *Use Behaviour*, this research has found that there is a gap between the two variables, considering that *Protection Motivation* only explains partially the variation of *Use Behaviour* (approximately 29.9%). This being the case, this research has also focused at explaining which factors may originate this variance between behavioural intentions and actual behaviour. 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 Behaviour*. As seen in **Model 3** and **Model 4**,

from the variables initially used in the PMT to estimate *Protection Motivation*, *Safety Habit Strength* has proven to be the only strong predictor for *Use Behaviour*. These conclusions are rather interesting, meaning Millennials do consider these five factors when deciding on a behaviour, however, later on, *Safety Habit Strength* relies as the only significant factor they rely when behaving in a certain manner.

Additionally, new factors were added to the analysis as an attempt to optimize our capability to explain *Use Behaviour*. As stated in hypothesis H_3, *Actual Control* has proven to be a good predictor for *Use Behaviour*, as it was able to increase our ability to explain the dependent variable to 36.3%. As proven by **Model 4,** the user's skills, abilities and environment play an important role in explaining *Use Behaviour*. Lastly, hypothesis H_4 and H_5 were not supported by **Model 4**, and consequently, *Perceived Control* (*Locus of Control*) and *Attitude towards Online Safety* are not able to further explain the variation of *Use Behaviour*. However, has stated before, there is a positive correlation between *Use Behaviour* and the two variables, *Attitude towards Online Safety* ($r = 0.321$, $p < 0.010$) and *Locus of Control* ($r = 0.211$, $p < 0.010$), which can indicate these variables may have been suppressed by the others.

5.1. Theoretical Implications

The suggested model confirms the strong link between intention and habit strength, which is a significant predictor for *Protection Motivation* in the PMT (LaRose et al., 2007, Tsai et al., 2016). Moreover, this research adds on previous literature by establishing a strong connection between *Safety Habit Strength* and *Use Behaviour*, which can be justified in accordance with Verplanken and Wood (2006) explanation: as people, by creating a habit, develop an "automaticity" when acting under similar circumstances.

Differently to published literature, this research analyses not only individual's behavioural intention, but also the actual protective behaviour the user chooses to adopt when navigating online by joining variables from two widely mentioned behavioural models in the

literature review, which are the PMT and RAA. Notably, this research is able to emphasise the existent gap between behavioural intention and actual behaviour, and consequently, integrate new variables that allow to understand the drivers for Millennials protective behaviours in terms of measures they adopt when navigating online. By adding *Actual Control* to our model, we are able to conclude that the users' skills, abilities and environment are relevant when undertaking a certain behaviour.

5.2. Practical Implications

In terms of practical implications, these findings are important for users and governments considering they may be used to improve overall online safety, as Cybercrime damages are estimated to cost close to $6 trillion annually in 2021 (Cybersecurity Ventures, 2017). Additionally, organizations can also benefit from helping users to be better protected when navigating online, as some industries rely on the customer feeling safe for their everyday business. For example, lack of security has been said to be the greatest inhibitor for online banking (Rotchanakitumnuai et al., 2003). Moreover, data privacy is becoming more important for the consumer each day, reinforcing the need for a safer customer experience. Consequently, if governments and corporations are able to understand the motivators behind the adoption of protective measures online, they can incentivise this type of safety behaviour.

Considering that Millennials' behaviour is significantly influenced by their habit strength, educating individual users for topics related with online security may constitute the best drive to influence their *Protection Motivation* and *Use Behaviour*, as it may help to form the habit of implementing greater security measures. As *Actual Control* has shown to have an impact on the users' *Use Behaviour*, another practical contribution from this research which can also influence Millennials *Use Behaviour,* relates with advocating for a stronger *Actual Control* by training the user's skills and abilities, This will, consequently, better prepare the

user for their online journey, which can, eventually, translate in a greater security online and an overall gain for society.

5.3. Limitations and Suggestions for Future Research

Considering past research focuses mainly on the study of behavioural intentions, this research has added new value to this field of research. However, it was subject to several limitations which can, ultimately, lead to suggestions for future research. Firstly, measuring *Use Behaviour* is quite challenging as users might not be totally honest relative to the way they express their behavioural intention and actual behaviour. A recommendation for future research may relate with having other forms of data collection, which can include the observation of behaviour instead of asking for the respondent opinion. Secondly, measuring the variable *Actual Control* also presents some difficulties, as respondents may not have an accurate perception of their environment, skills and abilities. Thirdly, this research focuses on the behaviour of Millennials, meaning it would be interesting that future research would study the differences for other generational cohorts and even compare them. Lastly, future research should also try at predicting other influencers of *Use Behaviour* by increasing the explanatory power of the model and considering other variables, such as Personal Responsibility and Threat Susceptibility, which some authors have included in the PMT.

6. Conclusion

All in all, this research was able to establish a gap between behavioural intention and actual behaviour in terms of protective measures Millennials adopt when navigating online. In addition, the formulated model was able to propose *Safety Habit Strength* and *Actual Control*, which include individual's skills, abilities and the environment factor, as significant when explaining Millennials *Use Behaviour*. These findings can contribute to improving the overall

security of the cyberspace as it becomes easier to influence Millennials to adopt a safer behaviour when navigating online.

7. References

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

Anderson and Agarwal (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. *MIS Quarterly*, 34(3), p.613.

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*, Heidelberg: Springer, pp. 265–300.

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), pp.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), pp.548-554.

Bruijn, H. and Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1), pp.1-7.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly*, 34(3), pp.523-548.

Chang, M., Cheung, W. and Lai, V. (2005). Literature derived reference models for the adoption of online shopping. *Information and Management*, 42(4), pp. 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, pp. 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, pp. 90-101.

Cybersecurity Ventures (2017). 2017 Cybercrime Report: Cybercrime damages will cost the world $6 trillion annually by 2021. [online] Available at: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ [Acessed 20th September of 2018].

Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quartely*, 13(3), pp. 319–340.

Dodge, R., Carver, C. and Ferguson, A. (2007). Phishing for User Security Awareness. *Elsevier*, 26(1), pp. 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].

Federal Trade Comission (2018). Annual Summary of Complaints Reported by Consumers. [Online]. Available at: https://www.ftc.gov/news-events/press-releases/2018/03/ftc-releases-annual-summary-complaints-reported-consumers. [Accessed on 18th September 2018].

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

Fishbein, M. and Ajzen, I. (2010). Predicting and Changing Behavior: The Reasoned Action Approach. Taylor & Francis.

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

Gartner (2017). Global IT Spending in 2018. [Online]. Available at: https://www.gartner.com/en/newsroom/press-releases/2018-01-16-gartner-says-global-it-spending-to-reach-37-trillion-in-2018. [Accessed at 21st September of 2018].

Hanafizadeh, P., Keating, B. and Khedmatgozar, H. (2014). A systematic review of Internet banking adoption. *Telematics and Informatics*, 31(3), pp. 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, pp 303-314.

Hunton, P. (2009). The growing phenomenon of crime and the Internet: A cybercrime execution and analysis model. *Computer Law & Security Review*, 25(6), pp. 528–535.

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

KPMG (2017). KPMG Cybercrime Survey Report Insights and Prespectives. [Online]. Available at: https://assets.kpmg.com/content/dam/kpmg/in/pdf/2017/12/Cyber-Crime-Survey.pdf. [Accessed at 4th September 2018].

Kritzinger, E. and Solms, S. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Society,* 29(8), pp. 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, pp. 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, pp. 394–413.

Liu, Y., Segev, S. and Villar, M. (2017). Comparing two mechanism for green consumption: cognitive-affect behaviour vs. theory of reasoned action. *Journal of Consumer Marketing*, 34(5), pp. 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, pp. 29-40.

Ögütçü, G., Testik, O. and Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computer and Security*, 56, pp. 83-93.

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), pp. 116–129.

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

Riek, M., Bohme, R. and Moore, T. (2015). Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transaction on Dependable and Secure Computing*, 12(2), pp. 261-273.

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

Rogers, R. (1983). Cognitive and physiological processes in fear appeals and attitude change: a revised theory of protection motivation. *Social Psychophysiology,* pp. 153-177.

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

Rotchanakitumnuai, S. and Speece, M. (2003). Barriers to Internet banking adoption: a qualitative study among corporate customers in Thailand. International Journal of Bank Marketing, 21(6/7), pp.312-323.

Ryder, N. (1965). The Cohort as a Concept in the Study of Social Change. *American Sociological Review*, 30, pp.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, pp. 320-330.

Shillair, R., Cotten, S., Tsai, H., Alhabash, S., LaRose, R. and Rifon, N. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, 48, pp.199-207.

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*, pp. 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, pp. 157–78.

Verplanken, B. and Wood, W. (2006). Interventions to break and create consumer habits. Journal of Public Policy & Marketing, 25, pp. 90–103.

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), pp. 2799-2816.

World Bank (2014). World Development Indicators. [Online]. Available at: https://openknowledge.worldbank.org/bitstream/handle/10986/18237/9781464801631.pdf?sequence=1. [Accessed on 5th September 2018].

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), pp. 448–84.

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