Scientific Research Publishing

Journal of Information Security, 2020, 11, 19-45
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Threat Perceptions, Avoidance Motivation and Security Behaviors Correlations

Fabrice Djatsa

Research and Development Department, Caelid Technology, Triangle, USA
Email: fdjatsa@caelid.com, fabricesonwa@ymail.com

How to cite this paper: Djatsa, F. (2020) Threat Perceptions, Avoidance Motivation and Security Behaviors Correlations. *Journal of Information Security*, **11**, 19-45.
https://doi.org/10.4236/jis.2020.111002

Received: October 28, 2019
Accepted: December 7, 2019
Published: December 10, 2019

Abstract

As the economy increases its dependence on the internet to increase efficiency and productivity in all aspects of society, close attention has been directed to solve the challenges related to internet security. Despite the large amount of resource invested so far in this area, cybersecurity challenges are still great as the media frequently report new cyber breaches. Although researchers acknowledge that great progress has been made in protecting digital assets, cybercriminals are still successful in their operations which are no longer limited to government entities and corporations but also individual computer users. To improve users' security posture, the researcher examined the relationship between Millennials' perceptions of cybersecurity threat, users' online security behaviors and avoidance motivation. The study focused on three constructs which are Perceived Threat (PTH), Online Security Behaviors (OSB) and Avoidance Motivation (AMO). The researcher administered a survey to 109 participants randomly selected in the United States. The Spearman's correlation test performed supported the analysis of the strength of the relationship and the level of significance between the independent variable and the dependent variables. The results from the statistical test provided enough evidence to fail to reject the null hypothesis related to relationships between PTH and OSB and to reject the null hypothesis regarding the relationship between PTH and AMO.

Keywords

Millennial, Perceptions, Threat, Avoidance Motivation, Online Security Behaviors

1. Introduction

The purpose of the study was to examine the relationship between Millennials' perceptions of cybersecurity threat, users' online security behaviors and avoidance motivation. The study focused on Millennials as the target population. A thorough review of the factors influencing the perceptions of cybersecurity threat supported the examination of the relationship between perceived threat, users' online security behaviors, and avoidance motivation. The health belief model served as the theoretical foundations to develop a model to examine the relationship between perceptions of cybersecurity threat, users' online security behaviors, and avoidance motivation. The theoretical framework allowed for a better understanding of how computer users perceived threat of a cyber-attack and the correlation between this factor, the online security behaviors and avoidance motivation that Millennials manifested on the internet. A quantitative approach supported the examination of the problem and the collection of the data. The investigation method was based on a web-based survey to gather data and test the model adapted from the health belief model. The survey provided insights into Millennials' threat perception, online security behaviors, and avoidance motivation.

The growing interest that researchers have in users' perceptions of cybersecurity risks is because individuals, as well as organizations, have become more dependent on technology and the internet to accomplish daily operations [1] [2]. The reliance on technology exposes users to various forms of cyber-attacks [1] [2] [3]. The increased use of the internet caused by users demanding great service delivery via the internet has made secure computing and cybersecurity a chief concern [4]. The US government has established a cyber command within the military whose mission is to protect against cyber-attacks from adversaries [5]. The public and private sectors seem to pay less attention to secure computing and cybersecurity practices [4]. The public sector relies on observations, friends, and media to assist with cyber defense strategies [6] [7] [8] [9].

Researchers in information security discipline have leveraged theories from other disciplines to study information security phenomena. The application of the theories in information security has been the subject of a lot of criticism [10]. Scholars have found that the findings based on the protection motivation theory within the information security literature are inconsistent with theoretical expectations [11].

Researchers used the health belief model to explain phenomena in information security [12]. Reference [13] used the health belief model to analyze home personal computer security adoption behavior. Reference [14] used the health belief model to examine user computer security behaviors. Both studies do not test the relationship between perceived threat, users' security behaviors and avoidance motivation. Both studies omitted perceived threat as an element impacting security behaviors. Reference [15] used the health belief model to examine home computer users' security awareness, information privacy, and security behaviors. The study solely relied on constructs from the health belief model and did not present any correlation between threat perception and security behaviors. Reference [15] focused security awareness, information privacy and their impact on home computer users' security behaviors.

The study contributed to a better understanding of the relationship between Millennials' perceptions of threat, cybersecurity practice, users' online security behaviors, and avoidance motivation. As a significant group of the population, Millennials constitute an essential part of the workforce for most organizations [16]. Millennials are the savviest generation regarding the use of information technology products [17] [18] [19]. The significance of the study was that it partially addresses security managers' concerns regarding the lack of studies on Millennials' security-related perceptions and behaviors [20]. There was a gap of knowledge on the understanding of the relationship between Millennials' perceptions of threat, cybersecurity practice, users' online security behaviors, and avoidance motivation. The study can help government agencies, businesses, and scholars understand Millennials' perception of cybersecurity threat, their online security behaviors and avoidance motivation. Organizations must understand users' online security behaviors and avoidance motivation to develop adequate training and policies materials [21]. The findings of the study can support the development of security tools and training tailored to Millennials. Researchers, scholars, and practitioners can take advantage of the study by using the knowledge gained to implement new measures that promote safe online behaviors. Scholars and researchers can build on the results of the study to develop new tools to improve information security.

In the following sections, the paper presents a discussion from scholars and researchers on a holistic approach to the importance of understanding threat perceptions to explain behaviors and motivation. The paper examines the role that perceptions of threat played in shaping online security behaviors and avoidance motivation. The paper presents a description of the methodology used, data analysis, and results.

2. Review of the Literature

2.1. Millennial Cybersecurity Posture

With the excessive number of cyber-attacks, ensuring the security of computer systems continues to be a challenge to organizations as well as to individuals. In the first quarter of 2016 report, the Anti-Phishing Working Group stated that the total number of unique phishing websites observed was 289,371. The number grew steadily from 48,114 in October 2015 to 123,555 observed in March 2016. The increase represents a 250% jump over six months [22]. Reference [23] reported that in 2016, there were 1209 total breaches with 1.1 billion identities exposed. Most Millennials have risky online security behaviors [24]. Reference [25] reported that as much as 66% of Millennials have connected to a public Wi-Fi network in previous months, and 42% shared a password with a non-family member in 2016. Millennials need to know the type of cyber-attacks they are vulnerable to and how their perceptions of cybersecurity threat affect their security behavior online [26]. Twenty percent of the surveyed participants have never changed the online banking password, and many Millennials use the same password to sign into different accounts/websites. Millennials often skip two-step authentications when they are available and engage in other risky behaviors [25]. It is not clear how the users' perceptions of cybersecurity threat influence online security behaviors [20].

2.2. Risk Perception in the Cyberspace

Media outlets increasingly report cyber-attacks and incidents. Every month, there are reports of significant incidents affecting hundreds of thousands of users [27]. Despite these reports, it is unclear if Millennials have the requisite knowledge to protect themselves [28]. Some users might have a false sense of security and expose themselves to security risks as a result [29]. The increased number of data breaches through hacking incidents has become a phenomenon of interest for internet security researchers [30]. As the breaches are targeting more online shopping sites, it is likely that users' knowledge and perceptions of the internet have changed over time [31] [32]. Although internet users are conscious of the potential cyber threats, it does not prevent them from connecting their computers and other smart devices to the internet [33].

Security awareness is one of the essential elements of information security management [34] [35]. Security awareness is the extent to which the members of an organization understand the importance of information security, individual responsibilities, and the minimum security required by the organization and behave accordingly. Today, practitioners and researchers agree that security awareness is critical to a successful and effective information security management and that it will be more cost-effective to invest in security awareness improvement than technology [36] [37]. The current knowledge of security awareness is limited because researchers have not studied the behavioral aspect of security awareness and its operationalization and conceptualization in existing research have been too broad for the most part [34].

2.3. Health Belief Model

In past security behavioral research, the research relies on constructs developed under the health belief model [14] [38]. Perceived severity, perceived susceptibility, perceived threat, perceived benefits, perceived barriers, cues to action, general security orientation, and self-efficacy are all factors in human behaviors. All these constructs have a particular influence on the security behaviors of computer end-users [15]. Cybersecurity awareness of risks influences users' attitudes and behaviors toward safety [39] [40]. Most of the studies conducted on the use of the internet and users' risk perceptions focused on scenarios that identified some of the variables in the risk equation as opposed to the type of threat that exists on the internet [41]. Studies that focused on the social impact of cyber-attacks are rare [42]. Below is outlined the construct under the health belief model which represent the dependent variable examined in the study:

Perceived threat. The construct defines the result of the individual's assessment of one susceptibility and the severity of the danger or disease [43]. The same construct applies in the cyberspace, where cyber-threats can impact internet users in various ways [44].

Below is a view of the theoretical framework (**Figure 1**).

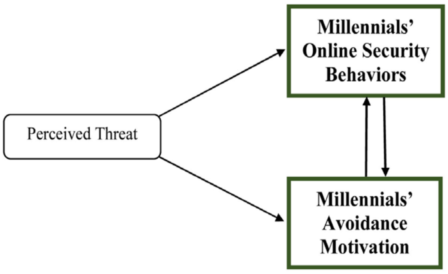
Millennials' Online Security Behaviors
Perceived Threat
Millennials' Avoidance Motivation

Figure 1. Theoretical framework.

3. Methodology and Data Analysis

3.1. Methodology

The quantitative methodology supported the approach of the study. In a quantitative method, applying deductive reasoning with the results and responses allows to move from specific to general [45]. Reference [46] developed a survey instrument (see Appendix A) that served as a basis to develop the survey instrument for the study. The researcher had received permission from the authors to use and modify the survey instrument. Validity and reliability are essential elements of a quantitative methodology [47]. A quantitative methodology fits because the variables to measure and the results are numerical data [48]. Quantitative methodology was appropriate as it is evidence-based practice in psychology and used to measure the changes in variables [49].

Survey research was appropriate because of the examination of the relationship between variables [50]. The objective was to examine the relationship between the perceptions of cybersecurity threat, users' online security behavior and avoidance motivation of Millennials. An analysis of the correlation helped determine the relationship between variables and make predictions [51].

3.2. Research Questions and Hypothesis

The dependent variables were the users' online security behaviors (OSB) and avoidance motivation. The independent variable was perceived threat (PTH).

3.2.1. Research Questions

RQ1: What is the relationship between Millennial's perceived threat of malware and users' online security behaviors?

RQ2: What is the relationship between Millennial's perceived threat of malware and users' avoidance motivation?

3.2.2. Hypotheses

H1o: A correlation does not exist between Millennials' perceived threat and users' online security behaviors.

H1A: A correlation does exist between Millennials' perceived threat and users' online security behaviors.

H2o: A correlation does not exist between Millennials' perceived threat and users' avoidance motivation.

H2A: A correlation does exist between Millennials' perceived threat and users' avoidance motivation.

3.3. Population and Sample

The population of research represents the group targeted, or the group referred to in the conclusion [52]. The population was Millennial in the United States who met a set of criteria as defined below. Millennials represent the largest generation in the US labor force, with more than one third participating in the labor force. As of 2017, roughly 35% or 35 million of Millennials were looking for work or working [53]. The population included Millennial professionals among Survey Monkey audience, who own a computer and have regular access to the internet. The study did not focus on a specific industry, and the participants had to be employed to meet the professionalism criteria. For the purpose of the study, a professional was defined as someone who uses professional knowledge and skills to address the issues that arise in the workplace [54]. Therefore, the target population criteria included: 1) any Millennials, which refers to individuals born between 1982 and 2000 [55], 2) participants must have a current job, 3) participants must own a computer, 4) participants must have regular access to the internet, and 5) participants must be accessible through the Survey Monkey platform. Survey Monkey has over 2.5 million daily respondents answering surveys on the platform [56]. The target population represented all the respondents on the platform who met the criteria above. The researcher did not obtain an estimation of the target population since Survey Monkey could not provide an estimate of how many Survey Monkey users met criteria a through d. The information collected from each participant during the survey process served as the primary data.

The sample size was determined by using the ANZMTG Statistical Decision Tree, which is a sample calculator that leverages the power calculation for Pearson's and Spearman's correlation method. The ANZMTG Statistical Decision Tree is a tool used to determine the sample size in function of the predefined criteria inputted in the tool. The tool confirmed that a sample size of 38 participants was appropriate with a power of $1 - \beta = 0.9$, a correlation coefficient of $\rho = 0.5$ for a large effect size, and a significance level of $\alpha = 0.05$, which are the only criteria relevant to calculating the sample size for the Spearman's correlation test [57] [58] [59]. With the given parameters, the ANZMTG Statistical Decision Tree analysis tool indicated a 90% confidence of obtaining the correct result if the study was repeated with different random samples. Additionally, the level of significance indicated that there is only a 5% risk of false-positive findings with a total sample size of 38 participants for a Spearman's correlation test [59] [60]. To ensure greater reliability of the findings, the author went beyond the recommended sample size and conducted the study with a sample size of 109 participants.

3.4. Data Collection

Participants received a clear and unambiguous statement regarding the voluntary nature of the survey. Also, the statement expressed the researcher's commitment to ensuring the participants' anonymity and the protection of PII. Survey Monkey served as a medium to collect data. The data collection process followed a sequence of ten steps as described below:

Step 1. The authors of the survey instrument (see Appendix A) leveraged for the study have granted permission to use and potentially modify the survey instrument selected. The instrument (Likert-type scales) was previously validated in previous studies [46]. In several studies, researchers have developed surveys by combining surveys or using questions from previously validated survey instruments [14] [61] [62].

Step 2. Modifications to the survey instrument consisted of replacing a word such as *spyware* with *malware*. The modifications were limited and did not affect any of the significant elements of the survey instrument. The modifications strengthened the content validity which is considered mandatory [63]. Content validity refers to the level to which inferences are legitimate to operationalize the theoretical constructs in the study [64].

Step 3. Survey Monkey was the platform used to conduct the survey. The researcher sent a letter to request permission and received authorization to use the Survey Monkey website.

Step 4. A Survey Monkey account was created to gain access to the products offered on the website. The survey instrument was created using a custom survey creation builder available on the Survey Monkey website.

Step 5. Invitations were sent to 155 Millennial who had met the targeting criteria. The invitation included the research topic, instructions on how to complete the survey, and a Uniform Resource Locator (URL) link that redirected participants to the online survey once they clicked on it.

Step 6. Once the potential participants clicked on the URL link in the invitation, they had to review an informed consent form which explained the nature of the research, the security measures in place to protect their anonymity and PII and the survey expectations. Participants had the choice to continue the survey or to exit the website [65].

Step 7. Participants who chose to continue with the survey moved on to the next page, where they had to answer four qualifying questions (see Appendix B) to verify their eligibility to participate.

Step 8. If the participants chose to exit the survey here, the survey did not collect their PII, and they were directed to a thank you page which expresses gratitude for their time. The website also automatically directed the participants who had completed the survey to a thank you page at the end. Survey Monkey saved the answers.

Step 9. At the end of the survey period, all data saved on Survey Monkey databases were downloaded on an external hard drive and analyzed.

Step 10. The data were encrypted and stored in a secure room. The researcher archived the data contained in the hard drive for 5 years [66]. After 5 years, the researcher will destroy the data.

4. Data Analysis

A quantitative, non-experimental, correlational design was the best fit because it facilitated the analysis of the relationship between dependent and independent variables [67]. A quantitative, non-experimental, correlational design supported cause-effect and causal relationship analysis [68]. The research design was useful to analyze strategies [69]. Correlation allowed the identification of the relationship that may exist between two or more variables [68]. The data analysis process followed a sequence of five steps as described below:

Step 1. A valid copy of SPSS (Statistical Package for Social Sciences) was obtained. SPSS was the statistical tool of choice to analyze the data collected. The data were analyzed using correlation analysis.

Step 2. All the data were entered into SPSS for non-parametric Spearman correlation analysis. Spearman's correlation was appropriate for the study as the variables were measured on scales that were ordinal, and the data were considered non-parametric [70]. The study met the three assumptions necessary for the use of Spearman's correlation test. All the variables for the study were measured on an ordinal scale, the observation values for the variables were paired, and there was a monotonic relationship between each pair of variables. Even if a monotonic relationship is difficult to observe, a Spearman correlation test still apply [71].

Step 3. The coefficient of correlation indicated the direction and strength of the relationship between the dependent and independent variables. It allowed for a better appreciation of the influence that one variable had on the other when there was a change in value. The measure of the coefficient of correlation supports all appropriate inferences to the general population [72]. The independent variables considered were perceived threat. The dependent variables were users' online security behaviors and avoidance motivation. The calculation of the coefficient of correlation helped to determine the direction and strength of the relationship between each pair of variables. The determination was based on the following measures: 1) 0.00 - 0.19 is considered as "*very weak*", 2) 0.20 - 0.39 is "*weak*", 0.40 - 0.59 is "*moderate*", 0.60 - 0.79 is "*strong*", and 0.80 - 1.0 is "*very strong*" [73].

Step 4. An interpretation of the statistical metrics such as median, mean, mode, standard deviation, variance, and count of information presented descriptive statistics of the sample. The non-parametric Spearman correlation analysis supported the decision of whether to reject or fail to reject each null hypothesis using a p-value threshold $p < 0.05$ to determine the level of significance.

Step 5. Additional analysis was conducted using the data collected with the second group of demographic questions which inquired about the participant's: 1) age group, 2) gender, 3) region, 4) household income, and 5) internet experience. The analysis aimed at identifying any trends related to each demographic category and to compare between categories and the independent variable. For the purpose of the study, avoidance behavior was relabeled as online security behaviors for data analysis.

4.1. Participant Demographics

The Survey Monkey website provided the researcher with the platform to administer the survey to the participants of the study. The targeted audience for the study included Millennial with or without a college degree, 35 job functions from writer to researcher, 19 options for industry from advertising and marketing to utilities/energy/extraction, and five job levels (owner/executive/C-level, senior management, middle management, intermediate, and entry-level). The first page of the survey contained the informed consent form. Participation in the survey required that each participant agreed to the consent form by clicking the "Yes" box to proceed to the next page where the participant had to answer three qualifying questions. The qualifying questions served as a second layer of screening. Participants who met the criteria had to answer "Yes" to each of the four questions to start answering the survey questions. Any selection of the "No" box on either page (informed consent or qualifying criteria) automatically disqualified the participant.

The demographic question of the survey focused on participants' number of years of internet experience. All the participants in the survey were Millennial. Participants had a diverse background, as they came from various regions within the United States and represented a broad spectrum of industry sectors. Survey Monkey website provided the platform through which the survey questions were administered. The participants were all members of the Survey Monkey pool of active users or panelists. In addition to the demographic question within the survey, Survey Monkey collected a few demographic data regarding the participants' age, gender, household income, region, and device type. The additional demographic questions were added to the survey questions for all participants to answer.

4.2. Presentation of the Data

The researcher downloaded and stored the data collected through the Survey Monkey website on a personal computer. The data was saved in an SPSS format/file and subsequently imported into SPSS Statistics Standard GradPack 24 for descriptive and correlation analysis. Participants' responses were organized into a demographic section and correlational statistics section. The demographic section presented the data about the participants' age group, gender, region, household income, and internet experience. The correlational variables section presented the result of the data preparation analysis and the correlation test.

A total of 155 participants agreed to take the survey study. From the total number of participants, four participants were disqualified because they did not agree to the Informed Consent form, 19 participants were disqualified because they did not meet the qualifying criteria, 23 of the participants who consented and qualified to participate in the study did not complete the survey. The remaining 109 participants who completed the survey represented the sample study. The researcher a larger sample even though the recommended sample size was determined with a power of $1 - \beta = 0.9$, which indicates a 90% confidence of obtaining the correct result if the study was repeated with different random samples. The power selected is superior to the minimum recommended value. Additionally, the significance level of $\alpha = 0.05$ met the recommended value for most academic studies [59].

Before starting the analysis of the data collected for the study, it was essential to measure and assess the reliability of the survey instrument. Cronbach's alpha test helped verify the survey instrument reliability. Cronbach's alpha is an appropriate test to measure the internal consistency and reliability of a research instrument [74]. The survey instrument centered around 44 statements which constituted the core questions in the survey. The core questions included: 1) five statements measuring the perceived susceptibility construct on a 7-point Likert scale, 2) ten statements measuring the perceived severity construct with a 7-point Likert scale, 3) five statements measuring the perceived threat construct with a 7-point Likert scale, 4) six statements measuring the perceived benefits construct with a 7-point Likert, 5) three statement measuring the perceived barriers construct with a 7-point Likert scale, 6) ten statement measuring the self-efficacy in cybersecurity with a 10-point Likert scale, and 7) three statements measuring the avoidance motivation construct with a 7-point Likert scale, and 8) two statements measuring the online security behaviors construct with a 7-point Likert scale.

A Cronbach's alpha test was performed to measure the internal validity and reliability of each variable considered in the study. Because the study examined several constructs, a test was performed for each variable to avoid inflating the value of alpha [75]. Reference [76] agreed that a Cronbach's alpha value 0.70 or above indicates an acceptable level of internal consistency and reliability. Reference [75] indicated that a Cronbach's alpha value between 0.70 and 0.95 is desirable to support the internal consistency and reliability of an instrument. A higher value may indicate redundancy in the instrument but is still reliable. Other researchers agreed that to confirm internal consistency reliability, the Cronbach alpha value should be at least 0.60 for exploratory studies and 0.70 for confirmatory studies [60]. Reference [77] indicated that 0.70 should be considered as an acceptable reliability coefficient.

An alpha value of 0.839 was measured for the five original questions for perceived threat (see **Table 1**). A coefficient greater than 0.8 is considered as good. This value indicates that there is a good internal consistency of the items in the scale measuring the perceived threat variable [78] [79].

Table 1. Perceived threat reliability statistics.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.839	0.834	5

An alpha value of 0.969 was measured for the three original questions for avoidance motivation (see Table 2). An alpha value greater than 0.9 is considered as excellent and indicates excellent internal consistency within the survey instrument measuring the avoidance motivation variable [79].

Table 2. Avoidance motivation reliability statistics.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.969	0.969	3

An alpha value of 0.926 was measured for the two original questions for online security behaviors (see Table 3). A coefficient greater than 0.9 is considered as excellent. This value indicates that there is an excellent internal consistency of the items in the scale measuring the online security behaviors variable [79].

Table 3. Online security behaviors reliability statistics.

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
0.926	0.926	2

4.3. Descriptive Analysis and Demographic Results

Table 4 presents the frequency distribution of the participants' number of years of internet experience. The table shows the different ranges under which each participant identified. Most participants had over 20 years of internet experience representing 45.0% of the sample. Participants representing 42.2% of the sample had between 11 and 20 years of internet experience, followed by 12.8% with 6 to 10 years of internet experience (see Table 4).

Table 4. Internet experience.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	6 - 10 years	14	12.8	12.8	12.8
	11 - 20 years	46	42.2	42.2	55.0
	>20 years	49	45.0	45.0	100.0
	Total	109	100.0	100.0	

Table 5 presents the frequency distribution of all the participants' age. Given that the sample only included Millennials, the age range could only vary between 19 to 37. The table shows that only two age groups were represented in the sample. Participants between the age of 25 to 29 had the highest percentage with 56.9% while the remaining of participants identified between 19 to 24 with 43.1% (see Table 5).

Table 5. Age.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	19 - 24	47	43.1	43.1	43.1
	25 - 29	62	56.9	56.9	100.0
	Total	109	100.0	100.0	

Table 6 presents the frequency distribution of the gender of all the participants. The table shows that most participants were female representing 67.9% of the sample. Male represented 32.1% of the participants (see Table 6).

Table 6. Gender.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	35	32.1	32.1	32.1
	Female	74	67.9	67.9	100.0
	Total	109	100.0	100.0	

Table 7 presents the frequency distribution that provides an insight into the income range of the participants. The table represents the household income of participants. Most participants earned from $50,000 - $74,999 representing 32.1%, while 21.1% earned from $25,000 - $49,999, and 18.3% earned from $75,000 - $99,999 (see Table 7).

Table 7. Household income.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	$25,000 - $49,999	23	21.1	21.1	21.1
	$50,000 - $74,999	35	32.1	32.1	53.2
	$75,000 - $99,999	20	18.3	18.3	71.6
	$100,000 - $124,999	11	10.1	10.1	81.7
	$125,000 - $149,999	9	8.3	8.3	89.9
	$150,000 - $174,999	5	4.6	4.6	94.5
	$175,000 - $199,999	5	4.6	4.6	99.1
	$200,000+	1	.9	.9	100.0
	Total	109	100.0	100.0	

4.4. Data Preparation and Screening Analysis

Table 8 presents the frequency distribution related to participants' perceived threat of a cyber-attack. The result included a total of 109 values corresponding to the sample size. There was no missing value, as each participant answered all the questions.

Table 8. Perceived threat.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	2	1.8	1.8	1.8
	Somewhat disagree	3	2.8	2.8	4.6
	Neither agree nor disagree	15	13.8	13.8	18.3
	Somewhat agree	27	24.8	24.8	43.1
	Agree	49	45.0	45.0	88.1
	Strongly agree	13	11.9	11.9	100.0
	Total	109	100.0	100.0	

Table 9 presents the frequency distribution related to participants' avoidance motivation by using anti-virus software. The result included a total of 109 values corresponding to the sample size. There was no missing value, as each participant answered all the questions.

Table 9. Avoidance motivation.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Disagree	7	6.4	6.4	6.4
	Somewhat disagree	9	8.3	8.3	14.7
	Neither agree nor disagree	11	10.1	10.1	24.8
	Somewhat agree	19	17.4	17.4	42.2
	Agree	31	28.4	28.4	70.6
	Strongly agree	32	29.4	29.4	100.0
	Total	109	100.0	100.0	

Table 10 presents the frequency distribution related to participants' online security behaviors of using anti-virus software. The result included a total of 109 values corresponding to the sample size. There was no missing value, as each participant answered all the questions.

Table 10. Online security behaviors.

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	12	11.0	11.0	11.0
	Disagree	15	13.8	13.8	24.8
	Somewhat disagree	14	12.8	12.8	37.6
	Neither agree nor disagree	12	11.0	11.0	48.6
	Somewhat agree	14	12.8	12.8	61.5
	Agree	21	19.3	19.3	80.7
	Strongly agree	21	19.3	19.3	100.0
	Total	109	100.0	100.0	

The researcher performed calculations to determine the mean, median, mode standard variation, and variance of each variable in examining the relationship between Millennials' perception of threat and users' avoidance motivation and online security behaviors. The survey questions were assessed using Likert scale ordinal variables with the following weighted formats: 1 = "strongly disagree", 2 = "disagree", 3 = "somewhat disagree", 4 = "neither agree nor disagree", 5 = "somewhat agree", 6 = "agree", and 7 = "strongly agree". Table 11 presents the result of the analysis, which indicates that perceived threat had the highest mean score (M = 5.44) of all the variables measured with a 7-point Likert scale. The mean indicates a substantial degree of likelihood that users may be more influenced by their perceptions of threat in adopting good online security behaviors. An assessment of the standard deviation indicates that users' online security behavior had the highest average distance from the mean (M = 4.36) with σ = 2.053, which indicates that participant online security behaviors were more spread out.

Table 11. Statistics.

		Perceived Threat	Avoidance Motivation	Online security Behaviors
N	Valid	109	109	109
	Missing	0	0	0
Mean		5.44	5.41	4.36
Median		6.00	6.00	5.00
Mode		6	7	6^a
Std. Deviation		1.075	1.523	2.053
Variance		1.156	2.319	4.213

a. Multiple modes exist. The smallest value is shown.

Factor analysis test was performed to allows the researcher to determine if factor extraction is necessary for data reduction by exploring the structure of the data [80]. The analysis was conducted on three factors (perceived threat, avoidance motivation, and online security behaviors) to determine the existence of variability between the set of elements. The scree plot below was used to make a determination. Reference [81] stated that in a scree plot, the eigenvalues are plotted in descending order against the factor numbers. The researcher inspected and counted the different values (corresponding the eigenvalue superior to 1) before the last drop to determine the number of factors. The following figures present the results obtained for each variable.

Figure 2 shows that only one component had an eigenvalue greater than one. Table 12 shows that one component explained 61% of the variance within the perceived threat variable. One item had the most impact on the variance.

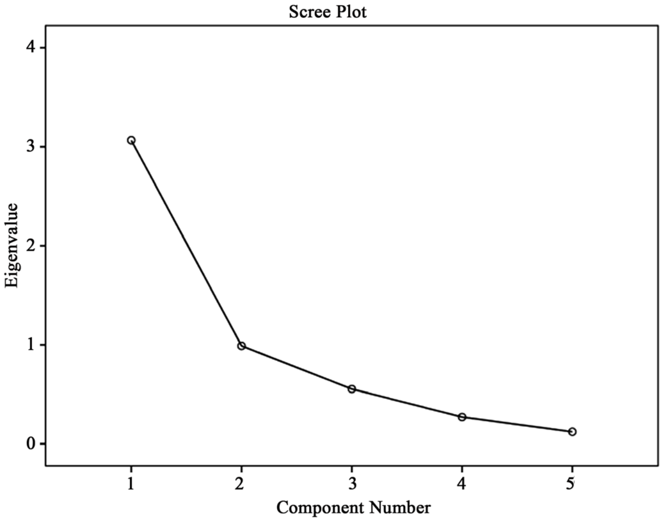

Figure 2. Scree plot of the five statements measuring perceived threat.

Table 12. Perceived threat total variance explained.

Component	Initial Eigenvalues		
	Total	% of Variance	Cumulative%
1	3.067	61.335	61.335
2	0.989	19.784	81.120
3	0.553	11.065	92.185
4	0.270	5.403	97.588
5	0.121	2.412	100.000

Figure 3 shows that only one component had an eigenvalue greater than one for avoidance motivation. **Table 13** shows that one components explained 94% of the variance within the avoidance motivation variable. One item had the most impact on the variance.

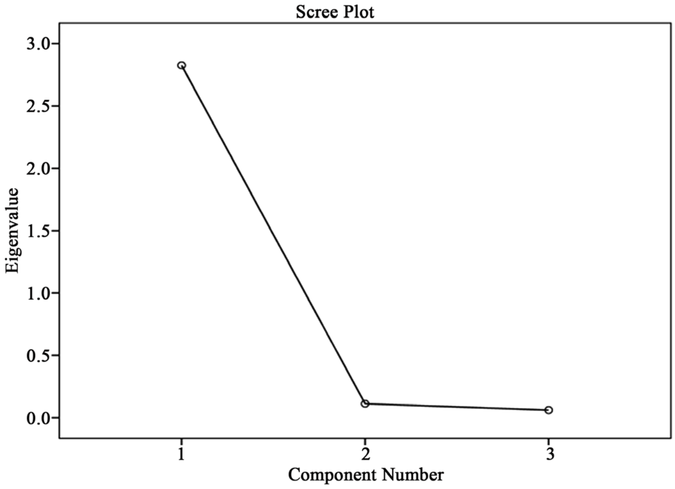

Figure 3. Scree plot of the three statements measuring avoidance motivation.

Table 13. Avoidance motivation total variance explained.

Component	Initial Eigenvalues		
	Total	% of Variance	Cumulative%
1	2.827	94.218	94.218
2	0.112	3.733	97.951
3	0.061	2.049	100.000

Figure 4 shows that only one component had an eigenvalue greater than one. Table 14 shows that one component explained 93% of the variance within the online security behaviors variable. One item had the most impact on the online security behaviors variance.

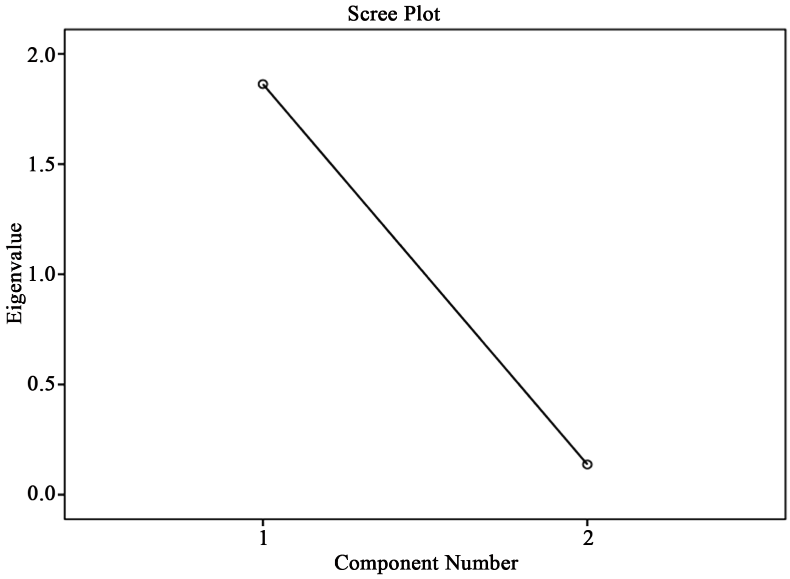

Figure 4. Scree plot of the two statements measuring online security behaviors.

Table 14. Online security behaviors total variance explained.

Component	Initial Eigenvalues		
	Total	% of Variance	Cumulative%
1	1.863	93.145	93.145
2	0.137	6.855	100.000

Spearman's correlation was selected as the best fit to analyze the data collected because the research design met the assumptions of the Spearman's correlation test [71]. First, the variables for the study were measured on an ordinal scale (7-point Likert scale). Second, the variables measured paired observations. Third, there was a monotonic relationship between each pair of variables, which are illustrated in the scatter plots below (see Figure 5 and Figure 6).

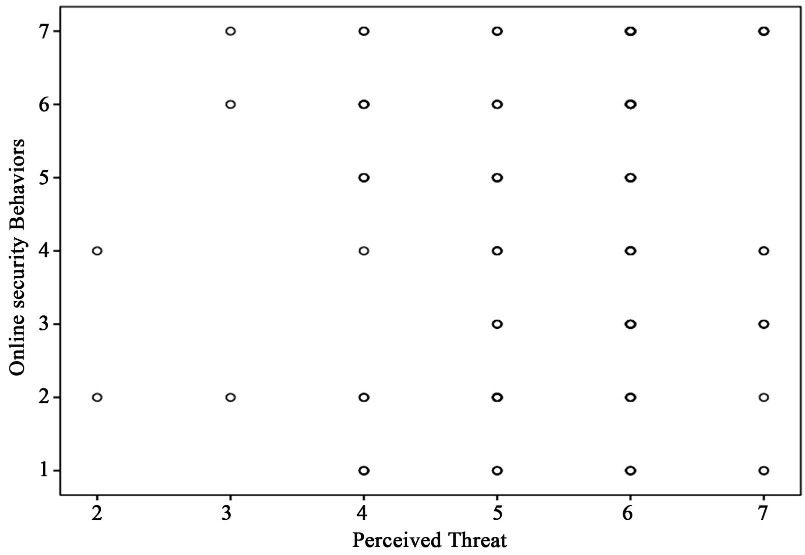

Figure 5. A simple scatter plot of online security behaviors and perceived threat.

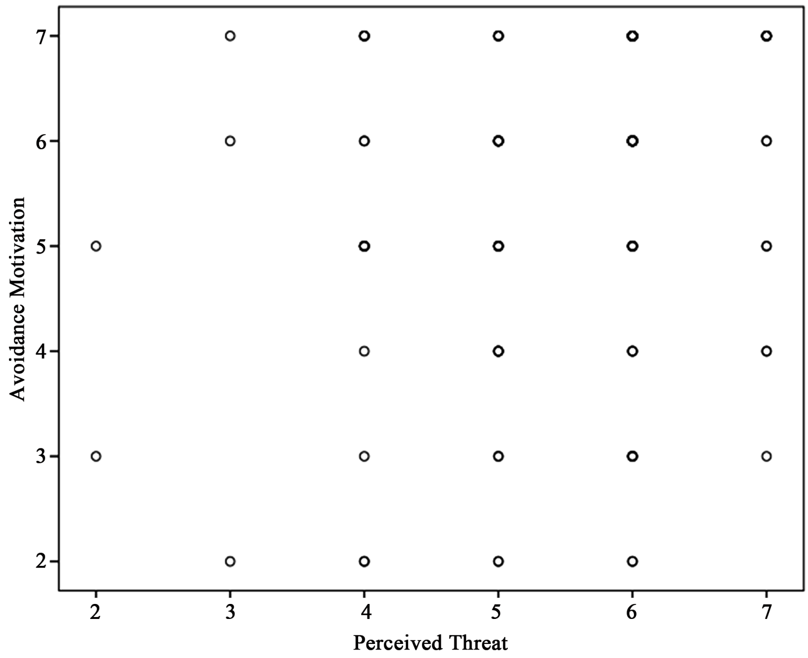

Figure 6. A simple scatter plot of avoidance motivation and perceived threat.

4.5. Research Questions

The two central research questions for the study were: 1) what is the relationship between Millennial's perceived threat of malware and users' online security behaviors? 2) what is the relationship between Millennial's perceived threat of malware and users' avoidance motivation? The dependent variables were the users' online security behaviors (OSB) and avoidance motivation (AMO). The independent variable was perceived threat (PTH). In the study, the researchers defined two hypotheses. A test of the two hypotheses helped determine if there was a significant relationship between Millennial' perceptions of threat, users' online security behaviors and avoidance motivation. The central research questions take into consideration the independent variable which produces the following research questions and hypotheses:

The first question and corresponding hypotheses developed in the study were the followings:

RQ1: What is the relationship between Millennial's perceived threat of malware and users' online security behaviors?

$H1_o$: A correlation does not exist between Millennials' perceived threat and users' online security behaviors.

$H1_A$: A correlation does exist between Millennials' perceived threat and users' online security behaviors.

Table 15 presents the result of the Spearman's correlation test, which showed that the coefficient correlation was 0.098, and the two-tailed significance level was 0.309. The finding showed that a very weak positive correlation existed between perceived threat and online security behaviors, and there was not a statistically significant relationship ($\rho = 0.098$, $0.309 > 0.05$). The result from the statistical test provided enough evidence to fail to reject the null hypothesis ($H1_o$) in support of the study.

Table 15. Spearman's correlation between PTH and OSB.

			Online security Behaviors	Perceived Threat
Spearman's rho	Online security Behaviors	Correlation Coefficient	1.000	0.098
		Sig. (2-tailed)		0.309
		N	109	109
	Perceived Threat	Correlation Coefficient	0.098	1.000
		Sig. (2-tailed)	0.309	
		N	109	109

The second question and corresponding hypotheses developed in the study were the followings:

RQ2: what is the relationship between Millennial's perceived threat of malware and users' avoidance motivation?

$H2_o$: a correlation does not exist between Millennials' perceived threat and users' avoidance motivation.

$H2_A$: a correlation does exist between Millennials' perceived threat and users' avoidance motivation.

Table 16 presents the result of the Spearman's correlation test, which showed that the coefficient correlation was 0.225, and the two-tailed significance level was 0.019. The finding showed that a weak positive correlation existed between perceived threat and avoidance motivation, and there was a statistically significant relationship ($\rho = 0.225$, $0.019 < 0.05$). The result from the statistical test provided enough evidence to reject the null hypothesis ($H2_o$) in support of the study.

Table 16. Spearman's correlation between PTH and AMO.

			Avoidance Motivation	Perceived Threat
Spearman's rho	Avoidance Motivation	Correlation Coefficient	1.000	0.225*
		Sig. (2-tailed)		0.019
		N	109	109
	Perceived Threat	Correlation Coefficient	0.225*	1.000
		Sig. (2-tailed)	0.019	
		N	109	109

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

5. Findings and Conclusions

5.1. Implications for Practice

The problem addressed in the study was that the relationship between Millennials' perceptions of cybersecurity threat and users' online security behaviors had not been identified [20]. There was a gap of knowledge on the understanding of the relationship between Millennial perceptions of cybersecurity threat, online security behaviors, and avoidance motivation. The findings of the study showed that a statistically significant correlation does not exist between the independent variable (PTH) and the dependent variable (OSB). On the other hand, the study showed that a statistically significant correlation does exist between the independent variable (PTH) and the dependent variable (AMO). The results of the correlation analysis indicated that Millennial professionals' perceived threat of a cyber-attack and the motivation to avoid it by installing and using anti-malware have a significant relationship. Enterprise leaders can leverage these findings and consider how they impact their organization's security posture. The study provides valuable insight into the Millennials' perceptions of cybersecurity threat. The knowledge gained from the study can help enterprise leaders tailor information assurance training for their Millennial staff as 45% of the participants agreed that malware presented a danger to their security.

5.2. Conclusions

A Spearman's correlation analysis was performed to determine the strength of the relationship between the independent variable (PTH) associated with cybersecurity risk perceptions, users' online security behaviors and avoidance motivation. Spearman's correlation was selected as the best statistical test because the study met the three assumptions necessary for the use of Spearman's correlation test. All the variables for the study were measured on an ordinal scale, the observation values for the variables were paired, and there was a monotonic relationship between variables.

The research questions for the study inquired about the relationship between the construct associated with Millennials' perceptions, users' online security behaviors and avoidance motivation. To answer these questions, the researcher developed two central research questions based on the independent variable: perceived threat (PTH); and the dependent variables which were online security behaviors (OSB) and avoidance motivation (AMO).

The first research question examined the relationship between Millennials' perceived threat and users' online security behaviors. The corresponding hypotheses were as follows: The null hypothesis ($H1_o$): A correlation does not exist between Millennials' perceived threat and users' online security behaviors. The alternative hypothesis ($H1_A$): A correlation does exist between Millennials' perceived threat and users' online security behaviors. **Table 15** presented the result of the Spearman's correlation test, which showed that the coefficient correlation was 0.098, and the two-tailed significance level was 0.309. The finding showed that a very weak positive correlation existed between perceived threat and online security behaviors, and there was not a statistically significant relationship ($\rho = 0.098$, $0.309 > 0.05$). The result from the statistical test provided enough evidence to fail to reject the null hypothesis ($H1_o$). Additional studies are required to support this finding given that studies on users' avoidance motivation are limited and do not directly address the relationship between perceived threat and avoidance motivation in a cybersecurity context.

The second research question examined the relationship between Millennials' perceived threat and users' avoidance motivation. The corresponding hypotheses were as follows: The null hypothesis ($H2_o$): A correlation does not exist between Millennials' perceived threat and users' avoidance motivation. The alternative hypothesis ($H2_A$): A correlation does exist between Millennials' perceived threat and users' avoidance motivation. **Table 16** presented the result of the Spearman's correlation test, which showed that the coefficient correlation was 0.225, and the two-tailed significance level was 0.019. The finding showed that a weak positive correlation existed between perceived threat and avoidance motivation, and there was a statistically significant relationship ($\rho = 0.225$, $0.019 < 0.05$). The result from the statistical test provided enough evidence to reject the null hypothesis (H_2O) in support of the study. This finding is consistent with findings elsewhere [48]. Reference [46] found that perceived threat positively affects avoidance motivation. This can inform businesses looking to sell anti-malware software to potential users. Governments, policy makers, executives and IT managers can rely on the findings when developing policies and cybersecurity awareness campaigns and training aimed at improving users' cyber threat awareness and motivate users to use security tools.

Acknowledgements

This study has benefited from the contribution received from Dr. Schmitt; whose guidance was instrumental in the completion of this paper. I could not be more grateful to have received and implemented some of her suggestions

Conflicts of Interest

The author has no conflicts of interest regarding the publication of this article.

References

[1] Barnard-Wills, D. and Ashenden, D. (2012) Securing Virtual Space: Cyber War, Cyber Terror, and Risk. *Space and Culture*, **15**, 110-123. https://doi.org/10.1177/1206331211430016

[2] Srivastava, S. (2012) Pessimistic Side of Information & Communication Technology: Cyber Bullying & Legislature Laws. *International Journal of Advances in Computer Science and Technology*, **1**, 14-20.

[3] Jones, C. and Mujtaba, B. (2006) Is Your Information at Risk? Information Technology Leaders' Thoughts about the Impact of Cybercrime on Competitive Advantage. *Review of Business Information Systems*, **10**, 7. https://doi.org/10.19030/rbis.v10i2.5320

[4] Williams, C.D. (2015) The Socialization of Secure Computing Practices for Home Internet Users: A Quantitative Analysis of Individual Perceptions. Doctoral Dissertation.

[5] Panetta, L. (2012) Sustaining US Global Leadership: Priorities for 21st Century Defense. US Department of Defense, Washington DC.

[6] Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S. and Combs, B. (1978) How Safe Is Safe Enough? A Psychometric Study of Attitudes towards Technological Risks and Benefits. *Policy Sciences*, **9**, 127-152. https://doi.org/10.1007/BF00143739

[7] Hali, S.M. (2000) The Role of Media in War. Defence Journal. http://www.defencejournal.com/2000/aug/role-media-war.htm

[8] Parsons, K., McCormac, A., Butavicius, M. and Ferguson, L. (2010) Human Factors and Information Security: Individual, Culture and Security Environment. No. DSTO-TR-2484, Command, Control, Communications and Intelligence Division DSTO Defence Science and Technology Organisation, Edinburgh.

[9] Pattinson, M. and Anderson, G. (2005) Risk Communication, Risk Perception and Information Security. In: *Security Management, Integrity, and Internal Control in Information Systems*, Springer, Berlin, 175-184. https://doi.org/10.1007/0-387-31167-X_11

[10] Oswick, C., Fleming, P. and Hanlon, G. (2011) From Borrowing to Blending: Rethinking the Processes of Organizational Theory Building. *Academy of Management Review*, **36**, 318-337. https://doi.org/10.5465/AMR.2011.59330932

[11] Warkentin, M. and Siponen, M. (2015) An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric. *MIS Quarterly*, **39**, 113-134. https://doi.org/10.25300/MISQ/2015/39.1.06

[12] Boss, S., Galletta, D., Lowry, P.B., Moody, G.D. 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**, 837-864. https://doi.org/10.25300/MISQ/2015/39.4.5

[13] Claar, C. and Johnson, J. (2012) Analyzing Home PC Security Adoption Behavior. *Journal of Computer Information Systems*, **52**, 20-29. https://doi.org/10.1108/09685221211235599

[14] Ng, B.-Y., Kankanhalli, A. and Xu, Y.C. (2009) Studying Users' Computer Security Behavior: A Health Belief Perspective. *Decision Support Systems*, **46**, 815-825. https://doi.org/10.1016/j.dss.2008.11.010

[15] Edwards, K. (2015) Examining the Security Awareness, Information Privacy, and the Security Behaviors of Home Computer Users. Doctoral Dissertation.

[16] DelCampo, R.G., Haggerty, L.A., Knippel, L.A. and Haney, M.J. (2011) Managing

the Multi-Generational Workforce: From the GI Generation to the Millennials. Gower Publishing, Ltd., Burlington.

[17] Haeger, D.L. and Lingham, T. (2014) A Trend toward Work-Life Fusion: A Multi-Generational Shift in Technology Use at Work. *Technological Forecasting and Social Change*, **89**, 316-325. https://doi.org/10.1016/j.techfore.2014.08.009

[18] Miller, K. and Murphrey, T.P. (2010) Catching Up with Our Students. Millennials and iGen: Is Agriscience Education Ready? *The Agricultural Education Magazine*, **83**, 20.

[19] S-O'Brien, L., Read, P., Woolcott, J. and Shah, C. (2011) Understanding Privacy Behaviors of Millennials within Social Networking Sites. *Proceedings of the American Society for Information Science and Technology*, **48**, 1-10. https://doi.org/10.1002/meet.2011.14504801198

[20] Wipawayangkool, K. and Villafranca, E. (2015) Exploring Millennials' Malware Awareness and Intention to Comply with Information Security Policy. *Review of Integrative Business and Economics Research*, **4**, 153.

[21] Li, L., He, W., Xu, L., Ivan, A., Anwar, M. and Yuan, X. (2014) Does Explicit Information Security Policy Affect Employees' Cyber Security Behavior? A Pilot Study. 2014 *Enterprise Systems Conference*, Shanghai, 2-3 August 2014, 169-173. https://doi.org/10.1109/ES.2014.66

[22] APWG (2016) Phishing Activity Trends Report, 1st Quarter 2016. Anti-Phishing Working Group. https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf

[23] Symantec (2017) Internet Security Threat Report. https://www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf

[24] Furnell, S. (2010) Jumping Security Hurdles. *Computer Fraud & Security*, **2010**, 10-14. https://doi.org/10.1016/S1361-3723(10)70067-1

[25] Raytheon (2017) Securing Our Future: Cybersecurity and the Millennial Workforce. https://www.raytheon.com/sites/default/files/2017-12/2017_cyber_report_rev1.pdf

[26] Sasse, M.A. and Flechais, I. (2005) Usable Security: Why Do We Need It? How Do We Get It? O'Reilly, Sebastopol.

[27] Coughlin, T.M. (2017) Cybersecurity Education for Adolescents and Non-Technical Adults. Master's Thesis.

[28] Furnell, S.M., Bryant, P. and Phippen, A.D. (2007) Assessing the Security Perceptions of Personal Internet Users. *Computers & Security*, **26**, 410-417. https://doi.org/10.1016/j.cose.2007.03.001

[29] Galvan, J.L. (2016) Student Motivations Regarding Online Security Implementation: A Qualitative Case Study. Doctoral Dissertation.

[30] Chakraborty, R., Lee, J., Bagchi-Sen, S., Upadhyaya, S. and Raghav Rao, H. (2016) Online Shopping Intention in the Context of Data Breach in Online Retail Stores: An Examination of Older and Younger Adults. *Decision Support Systems*, **83**, 47-56. https://doi.org/10.1016/j.dss.2015.12.007

[31] Anderson, K.B., Durbin, E. and Salinger, M.A. (2008) Identity Theft. *Journal of Economic Perspectives*, **22**, 171-192. https://doi.org/10.1257/jep.22.2.171

[32] Kang, R., Dabbish, L., Fruchter, N. and Kiesler, S. (2015) My Data Just Goes Everywhere: User Mental Models of the Internet and Implications for Privacy and Security. *Symposium on Usable Privacy and Security*, Pittsburgh, PA, 39-52.

[33] de Bruijn, H. and Janssen, M. (2017) Building Cybersecurity Awareness: The Need for Evidence-Based Framing Strategies. *Government Information Quarterly*, **34**,

1-7. https://doi.org/10.1016/j.giq.2017.02.007

[34] Siponen, M.T. (2000) A Conceptual Foundation for Organizational Information Security Awareness. *Information Management & Computer Security*, **8**, 31-41. https://doi.org/10.1108/09685220010371394

[35] Von Solms, B. (2001) Information Security—A Multidimensional Discipline. *Computers & Security*, **20**, 504-508. https://doi.org/10.1016/S0167-4048(01)00608-3

[36] Jones, D. (2007) Low Cost Security Tools: Employee Awareness. *Security*: *Solutions for Enterprise Security Leaders*, **44**, 90-91.

[37] Kelly, C. (2006) Awareness Trumps New Security Toys. *Computerworld-Newton Then Framingham Massachusetts*, **40**, 44.

[38] Claar, C.L. (2011) The Adoption of Computer Security: An Analysis of Home Personal Computer User Behavior Using the Health Belief Model. Doctoral Dissertation.

[39] Bryce, J. and Fraser, J. (2014) The Role of Disclosure of Personal Information in the Evaluation of Risk and Trust in Young Peoples' Online Interactions. *Computers in Human Behavior*, **30**, 299-306. https://doi.org/10.1016/j.chb.2013.09.012

[40] Dinev, T. and Hu, Q. (2007) The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies. *Journal of the Association for Information Systems*, **8**, 23. https://doi.org/10.17705/1jais.00133

[41] Byrne, Z.S., Dvorak, K.J., Peters, J.M., Ray, I., Howe, A. and Sanchez, D. (2016) From the User's Perspective: Perceptions of Risk Relative to Benefit Associated with Using the Internet. *Computers in Human Behavior*, **59**, 456-468. https://doi.org/10.1016/j.chb.2016.02.024

[42] Riek, M., Bohme, R. and Moore, T. (2016) Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transactions on Dependable and Secure Computing*, **13**, 261-273. https://doi.org/10.1109/TDSC.2015.2410795

[43] Skinner, C.S., Tiro, J. and Champion, V.L. (2015) The Health Belief Model. In: *Health Behavior*: *Theory*, *Research*, *and Practice*, 5th Edition, Jossey-Bass, San Francisco, CA, 75-94.

[44] Dodel, M. and Mesch, G. (2017) Cyber-Victimization Preventive Behavior: A Health Belief Model Approach. *Computers in Human Behavior*, **68**, 359-367. https://doi.org/10.1016/j.chb.2016.11.044

[45] McNabb, D.E. (2010) Research Methods for Political Science: Qualitative and Quantitative Approaches. ME Sharp Inc., New York.

[46] 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**, 394-413. https://doi.org/10.17705/1jais.00232

[47] O'Dwyer, L.M. and Bernauer, J.A. (2013) Quantitative Research for the Qualitative Researcher. Sage Publications, Thousand Oaks, CA.

[48] Nardi, P.M. (2018) Doing Survey Research: A Guide to Quantitative Methods. 4th Edition, Routledge, New York. https://doi.org/10.4324/9781315172231

[49] Martin, W.E. and Bridgmon, K.D. (2012) Quantitative and Statistical Research Methods: From Hypothesis to Results (Vol. 42). John Wiley & Sons, Hoboken, NJ.

[50] Punch, K. (2003) Survey Research: The Basics. Sage Publications, Thousand Oaks, CA. https://doi.org/10.4135/9781849209984

[51] Gay, L. and Airasian, P. (2000) Educational Research: Competencies for Analysis and Experience. 6th Edition, Prentice-Hall, Upper Saddle River, NJ.

[52] Bethlehem, J. and Biffignandi, S. (2011) Handbook of Web Surveys (Vol. 567). John

Wiley & Sons, Hoboken, NJ. https://doi.org/10.1002/9781118121757

[53] Fry, R. (2018) Millennials Are the Largest Generation in the U.S. Labor Force. Pew Research Center, Washington DC. https://www.pewresearch.org/fact-tank/2018/2004/2011/millennials-largest-generation-us-labor-force

[54] Kane, M.T. (1992) The Assessment of Professional Competence. *Evaluation & the Health Professions*, **15**, 163-182. https://doi.org/10.1177/016327879201500203

[55] U.S. Census Bureau (2015) Millennials Outnumber Baby Boomers and Are Far More Diverse. US Census Bureau, Suitland, MD. https://www.census.gov/newsroom/press-releases/2015/cb15-113.html

[56] Survey Monkey (2018) Diverse Recruitment. https://www.SurveyMonkey.com/collect/audience/?collector_id=232820799

[57] Lachin, J.M. (1981) Introduction to Sample Size Determination and Power Analysis for Clinical Trials. *Controlled Clinical Trials*, **2**, 93-113. https://doi.org/10.1016/0197-2456(81)90001-5

[58] Shuster, J.J. (2014) Sample Size Verification for Clinical Trials. *Clinical and Translational Science*, **7**, 60-62. https://doi.org/10.1111/cts.12115

[59] Suresh, K. and Chandrashekara, S. (2012) Sample Size Estimation and Power Analysis for Clinical Research Studies. *Journal of Human Reproductive Sciences*, **5**, 7. https://doi.org/10.4103/0974-1208.97779

[60] QFAB (2019) Statistical Decision Tree. https://www.anzmtg.org/stats/PowerCalculator/PowerCorrelation

[61] Ifinedo, P. (2014) Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialisation, Influence, and Cognition. *Information & Management*, **51**, 69-79. https://doi.org/10.1016/j.im.2013.10.001

[62] Lebek, B., Uffen, J., Neumann, M., Hohler, B. and Breitner, M.H. (2014) Information Security Awareness and Behavior: A Theory-Based Literature Review. *Management Research Review*, **37**, 1049-1092. https://doi.org/10.1108/MRR-04-2013-0085

[63] Straub, D., Boudreau, M. and Gefen, D. (2004) Validation Guidelines for Is Positivist Research. *Communications of the Association for Information Systems*, **13**, 380-427. https://doi.org/10.17705/1CAIS.01324

[64] Trochim, W.M.K. and Donnelly, J.P. (2008) The Research Methods Knowledge Base. 3rd Edition, Atomic Dog, Mason, 56-65.

[65] U.S. Department of Health and Human Services (1979) The Belmont Report. New York.

[66] Coulehan, M.B. and Well, J.F. (2006) Guidelines for Responsible Data Management in Scientific Research. Clinical Tools, Incorporated, Chapel Hill, NC.

[67] Gall, M., Gall, J. and Borg, W. (2007) Nonexperimental Research: Descriptive and Causal-Comparative Designs. In: Gall, M.D., Gall, J.P. and Borg, W.R., Eds., *Educational Research*: *An Introduction*, Pearson/Allyn & Bacon, Boston, MA, 298-330.

[68] Bless, C., Higson-Smith, C. and Kagee, A. (2006) Fundamentals of Social Research Methods: An African Perspective. Juta and Company Ltd., Cape Town.

[69] Belli, G. (2008) Nonexperimental Quantitative Research. *Lapan*, **1**, 59.

[70] Newson, R. (2001) Somersd-Confidence Intervals for Nonparametric Statistics and Their Differences. *Stata Technical Bulletin*, **10**, 47-55.

[71] Laerd (2018). Spearman's Rank-Order Correlation.

https://statistics.laerd.com/statistical-guides/spearmans-rank-order-correlation-statistical-guide.php

[72] Faul, F., Erdfelder, E., Lang, A.-G. and Buchner, A. (2007) G Power 3: A Flexible Statistical Power Analysis Program for the Social, Behavioral, and Biomedical Sciences. *Behavior Research Methods*, **39**, 175-191. https://doi.org/10.3758/BF03193146

[73] Field, A. (2009) Discovering Statistics Using SPSS. Sage Publications, Thousand Oaks, CA.

[74] Matkar, A. (2012) Cronbach's Alpha Reliability Coefficient for Standard of Customer Services in Maharashtra State Cooperative Bank. *IUP Journal of Bank Management*, **11**, 89-95.

[75] Tavakol, M. and Dennick, R. (2011) Making Sense of Cronbach's Alpha. *International Journal of Medical Education*, **2**, 53. https://doi.org/10.5116/ijme.4dfb.8dfd

[76] Hair, J.F., Anderson, R.E., Black, W.C., Tatham, R.L. and Babin, B.J. (2006) Multivariate Data Analysis (Vol. 6). Pearson Prentice Hall, Upper Saddle River, NJ.

[77] Nunnally, J.C. (1978) Psychometric Theory. 2nd Edition, McGraw-Hill, New York.

[78] George, D. and Mallery, P. (2003) SPSS for Windows Step by Step: A Simple Guide and Reference. 11.0 Update, 4th Edition, Allyn & Bacon, Boston, MA.

[79] Gliem, J.A. and Gliem, R.R. (2003) Calculating, Interpreting, and Reporting Cronbach's Alpha Reliability Coefficient for Likert-Type Scales.

[80] Jackson, J.E. (2003) A User's Guide to Principle Components. Hoboken, NJ: John Wiley & Sons, Inc., New York.

[81] Haugli, S.E. (2014) Factor Analysis of the Psychosocial Assessment Tool (PAT2.0) (Doctoral Dissertation). ProQuest Dissertations & Theses Global Database.

Appendix A

Survey Instrument

Perceived Susceptibility (1 = strongly disagree, 7 = strongly disagree)
It is extremely likely that my computer will be infected by spyware in the future
My chances of getting spyware are great
There is a good possibility that my computer will have spyware
I feel Spyware will infect my computer in the future
It is extremely likely that spyware will infect my computer
Perceived Severity (1 = innocuous, 7 = extremely devastating)
Spyware would steal my personal information from my computer without my knowledge
Spyware would invade my privacy
My personal information collected by spyware could be misused by cyber criminals
Spyware could record my Internet activities and send it to unknown parties
My personal information collected by spyware could be subject to unauthorized secondary use
My personal information collected by spyware could be used to commit crimes against me
Spyware would slow down my Internet connection
Spyware would make my computer run more slowly
Spyware would cause system crash on my computer from time to time
Spyware would affect some of my computer programs and make them difficult to use
Perceived Threat (1 = strongly disagree, 7 = strongly disagree)
Spyware poses a threat to me
The trouble caused by spyware threatens me
Spyware is a danger to my computer
It is dreadful if my computer is infected by spyware
It is risky to use my computer if it has spyware
Perceived Safeguard Effectiveness (1 = strongly disagree, 7 = strongly disagree)
Anti-spyware software would be useful for detecting and removing spyware
Anti-spyware software would increase my performance in protecting my computer from spyware
Anti-spyware software would enable me to search and remove spyware on my computer faster
Anti-spyware software would enhance my effectiveness in searching and removing spyware on my computer
Anti-spyware software would make it easier to search and remove spyware on my computer
Anti-spyware software would increase my productivity in searching and removing spyware on my computer
Perceived Safeguard Cost (1 = strongly disagree, 7 = strongly disagree)
I don't have anti-spyware on my PC because …
… I don't know how to get an anti-spyware software
… Anti-spyware software may cause problems to other programs on my computer
… Installing anti-spyware software is too much trouble.

Continued

Self-Efficacy (1 = not at all confident, 10 = totally confident)
I could successfully install and use anti-spyware software if …
… there was no one around to tell me what to do
… I had never used a package like it before
… I had only the software manuals for reference
… I had seen someone else doing it before trying it myself
… I could call someone for help if I got stuck
… someone else helped me get started
… I had a lot of time to complete the job
… I had just the built-in help facility for assistance
… someone showed me how to do it first
… I had used similar packages like this one before to do the job
Avoidance Motivation (1 = strongly disagree, 7 = strongly disagree)
I intend to use anti-spyware software to avoid spyware
I predict I would use anti-spyware software to avoid spyware
I plan to use anti-spyware software to avoid spyware
Avoidance Behavior (1 = strongly disagree, 7 = strongly disagree)
I run anti-spyware software regularly to remove spyware from my computer.
I update my anti-spyware software regularly.

Appendix B

Survey Questions

Qualifying Questions

1) Were you born between 1982 and 2000?

Yes □

No □

2) Are you currently employed?

Yes □

No □

3) Do you own a computer?

Yes □

No □

4) Do you have regular access to the internet?

Yes □

No □