MILLENNIALS' INFORMATION SECURITY HABITS AND PROTECTION MOTIVATION INTENTION: A QUANTITATIVE STUDY

by

Vidia Poleon

CALVIN LATHAN, EdD, Faculty Mentor and Chair

CLIFFORD BUTLER, PhD, Committee Member

RICHMOND ADEBIAYE, PhD, Committee Member

Todd C. Wilson, PhD, Dean

School of Business and Technology

A Dissertation Presented in Partial Fulfillment

Of the Requirements for the Degree

Doctor of Philosophy

Capella University

April 2020

Abstract

Millennial home personal computer users, people born between 1980 and 2000, vary from older generations in their way of thinking and decision-making. The millennial generation grew up with technology from a young age and are aware of how to manage many gadgets. However, the group is not as information security sensible as expected. The culture of continuous Internet use in home computing creates habits that potentially derail prescribed security responses to cyber threats producing unhealthy information security practices. Millennials' habituated tendencies reveal reasons why members of the group are not entirely adopting and implementing antivirus software. This quantitative, nonexperimental design study aimed to understand if prior information security experiences and habituated responses to compromised security events influenced millennial technology-oriented decision-making. The research question asked was as follows: Is there a significant association between millennials' information security habits and protection motivation factors that indicate an intention to install antivirus software? The theoretical framework of the protection motivation theory provided a basis for analysis to visualize the correlation between habituated actions and predictor variables to forecast millennials' intention to install antivirus software. A 24-question survey instrument with 23 items in a 7-point Likert style collected data from 257 participants. Bivariate correlational analysis indicated relationships with information security habits and provided potential reasons why habituated actions might influence implementing antivirus software among millennials. Perceived vulnerability, perceived severity, response efficacy, and self-efficacy variables showed significance using a *p*-value of 0.05, while rewards and response costs had no significance. Results from regression analysis with correlated variables illustrated avenues for future research with perceived severity and self-efficacy. Conclusions from the research indicated the need for

performing additional statistical tests to understand millennials' perceived risk and risk coping responses with information security habits as a moderator of protection motivation factors with intention to implement security software. Recommendations from the research included a focus on perceived severity and understanding millennials' self-efficacy or confidence to complete prescribed information security actions. All research recommendations would be enhanced with a mixed methods approach to decipher recipients' responses to survey questions with open-ended queries.

Dedication

I give all glory and honor to the Most-High God. He has been my closest friend in times of great need, never letting me feel alone or hopeless. God has helped me to reach heights that I never thought I would see. Family is my foundation and motivation. My family encouraged me to press onward towards the mark and finish this journey. Special thanks to my son and my parents.

Acknowledgments

Several people supported and inspired my efforts with this dissertation project, Kimberly Norton and Shirley Burton. However, close coordination and correspondence took place with my committee members, and the Committee Chair and Mentor. To my committee members, Dr. Richmond Adebiaye, Dr. Clifford Butler, and my committee Chair and Mentor, Dr. Calvin Lathan, thank you for the motivation, excellent advice, direction, and encouragement. Also, to my Milestone 11 reviewers, Dr. Schneider, Dr. Sharum, Dr. Chow, and Dr. Gottwald, thank you for your help and effort on my behalf. You all gave me your time and expertise to properly develop my work. I want to state my appreciation for the support and assistance of the advisors, faculty, and staff at Capella University. The transformation of the program, curriculum, and colloquia made the overall experience thought-provoking and worthwhile to complete.

I think this is the right place to acknowledge the Bible and how it aided me in understanding how to proceed with completing this enormous task. When I was overwhelmed with the mission of researching, understanding, formulating, and writing, and I felt like I did not know what I was doing, I thought about this scripture from the Bible: “For precept must be upon precept, precept upon precept; line upon line, line upon line; here a little, and there a little” (Isaiah 28:10, King James Version). With this scripture in mind, I would do at least something every day, whether it was 15 minutes, one hour, two hours, whatever. I was just grateful for the strength and confidence it gave me to continue to move forward, and before I knew it, I was finishing chapters.

Table of Contents

Acknowledgments vi

List of Tables x

List of Figures xi

CHAPTER 1. INTRODUCTION 1

Background of the Problem 2

Statement of the Problem 7

Purpose of the Study 7

Significance of the Study 8

Research Question 8

Definition of Terms 9

Research Design 11

Assumptions and Limitations 12

Assumptions 12

Limitations 15

Organization of the Remainder of the Study 17

CHAPTER 2. LITERATURE REVIEW 18

Methods of Searching 18

Theoretical Orientation for the Study 19

Review of the Literature 27

Synthesis of the Research Findings 46

Critique of the Previous Research Methods 48

Summary 50
CHAPTER 3. METHODOLOGY 52
Purpose of the Study 52
Research Questions and Hypotheses 53
Research Design 55
Target Population and Sample 55
Population 56
Sample 56
Power Analysis 57
Procedures 57
Participant Selection 57
Protection for Participants 58
Data Collection 59
Data Analysis 59
Instruments 62
Millennials and Antivirus Software Survey Instrument 62
Ethical Considerations 63
Summary 64
CHAPTER 4. RESULTS 66
Description of the Sample 66
Hypotheses Testing 72
Summary of the Hypotheses Testing 76

Summary 77
CHAPTER 5. DISCUSSION, IMPLICATIONS & RECOMMENDATIONS 78
Summary of the Results 78
Discussion of the Results 83
Conclusions Based on the Results 86
Limitations 88
Implications for Practice 89
Recommendations for Further Research 90
Recommendations Developed Directly From the Data 91
Recommendations Based on Delimitations 92
Conclusion 93
REFERENCES 95
APPENDIX A. SURVEY INSTRUMENT MEASURMENT ITEMS 107
APPENDIX B. LEVENE'S TEST FOR HOMOGENEITY OF VARIANCE 109

List of Tables

Table 1. Research Comparison Between Vance et al. (2012) and Yoon et al. (2012) 50

Table 2. Mean and Standard Deviation Descriptives With Skewness and Kurtosis Values 67

Table 3. Data Skewness Values Before and After Data Transformation 68

Table 4. Multicollinearity Assumption Test - Collinearity Variance Proportions..... 71

Table 5. Multicollinearity Statistics..... 71

Table 6. Habit Correlations (N = 257)..... 75

Table 7. Regression Analysis Results for Habit and Relationship Variables..... 76

Table 8. Pearson's r, Significance, and Hypothesis Results for Each Variable..... 76

List of Figures

Figure 1. Research model (Vance et al., 2012, p. 191). 5

Figure 2. PMT framework schema recreated from Rogers (1983, p. 183). 6

Figure 3. Model predictions (Vance et al., 2012, p. 191). 22

Figure 4. Linearity assumption confirmation 69

Figure 5. Homoscedasticity assumption confirmation 70

Figure 6. Normal distribution assumption confirmation 72

CHAPTER 1. INTRODUCTION

Internet connectivity is a prerequisite to managing the 21st-century lifestyle with online banking and finances, education, health management, work, and entertainment. The Internet's use surpasses imaginings with staggering effects on culture and the economy with the ability to change lives. Described as an intangible intricate, interconnected mechanism equivalent to the human nervous system, the Internet goes well beyond entrenchment into everyday life (Kleinrock, 2003). It diminishes the disparities of distance and time and shrinks the communication gap, creating global cyber villages with its immersive, ubiquitous experience (Kottke, 2017; Taylor, 2013; White, 2015). Despite the myriad of accolades for the Internet, it is now an avenue to cyber-attacks and calculated assaults against personal computing systems and networks (Alohali, Clarke, Li, & Furnell, 2018; Chenoweth, Gattiker, & Corral, 2019; Shropshire, Warkentin, & Sharma, 2015). Individual computer users contribute to data breaches when interacting on the Internet in unsecure ways, inspiring notions of a weak link in the virtual security chain (Glaspie & Karwowski, 2017; Mamonov & Benbunan-Fich, 2018; Martens, De Wolf, & De Marez, 2019; Van Bavel, Rodríguez-Priego, Vila, & Briggs, 2019).

The ubiquity of the Internet is potentially treacherous to home computer users who may be ill-equipped to handle securing personal devices and who are now the target of malware programmers, persons writing malicious code (Dang-Pham, Pittayachawan, & Bruno, 2016; Hanus & Wu, 2016). There is a crisis in home computing with four-fifths of homes being absent one or more security defenses against malware threats (White, Ekin, & Visinescu, 2017). Nthala and Flechais (2018) recommended additional research to understand the reasoning for the low adoption rate with home computing security practices. Empirical research with home computer

users might generate reasoning as to how members in this group make information security (IS) decisions.

Stewart, Oliver, Cravens, and Oishi (2017) noted that millennials liken the use of the Internet to breathing, drinking water, taking nourishment, and having shelter. Internet usage among millennials in terms of security actions and how these home computer users safeguard data with protective software, like antivirus software (AvSW), is a gap in IS literature. Thus, millennial home PC users might develop habituated actions that result in unhealthy IS practices (Thatcher, Wright, Sun, Zagenczyk, & Klein, 2018; White et al., 2017). Stewart et al. (2017) remarked that millennials' ideas on security and how members of the cohort depend on the Internet promotes scope for additional research. The purpose of this quantitative, nonexperimental design study is to understand if millennial home PC users' previous IS habituated actions influence decision-making and affect intention to install precautionary security software.

Background of the Problem

While Internet opportunities are, in most cases beneficial, the overwhelming use of cyber technology reveals numerous vulnerabilities that affect home PC users (Chenoweth et al., 2019; Hanus & Wu, 2016; Mills & Sahi, 2019; Nthala & Flechais, 2018; Tsai et al., 2016). The background of the problem involves home computers being the primary target for malware activities (Hanus & Wu, 2016). Mills and Sahi (2019) noted that home computers are the ultimate mechanism for malware and ransomware attacks. Approximately 90% of computers on the Internet are vulnerable to malware attacks because of conventional software prevalent on home PCs (Chenoweth et al., 2019; Tsai et al., 2016). The high statistical rate concerns malware

pitfalls on the Internet that disproportionately exposes home computers to malicious activities driving the need for additional research (Dupuis, Crossler, & Endicott-Popovsky, 2016; McGill & Thompson, 2017; Nthala & Flechais, 2018).

Within the power of home PC users is the option to protect computers, data, and online personas with conscious care cyber behavior, however these users might not understand how to maneuver in a threat-focused atmosphere. Home computer users are an unpredictable factor in Internet security, seen as a point of weakness in security continuity (Boss, Galletta, Lowry, Moody, & Polak, 2015; Dupuis et al., 2016; Glaspie & Karwowski, 2017; Mamonov & Benbunan-Fich, 2018; Van Bavel et al., 2019). Safa et al. (2015) noted that poor user behavior in IS matters creates opportunities for breach due to Internet users' impending "negligence, ignorance, lack of awareness, mischievous[ness], apathy, [or] resistance" (p. 65).

Information security habits have a dynamic role to play on the intention to perform IS activities. Habituated tendencies might promote additional security risk due to the longevity and reliance on automatic responses, which might be difficult to break (Carden & Wood, 2018; Howe, Ray, Roberts, Urbanska, & Byrne, 2012; Vance, Jenkins, Anderson, Bjornn, & Kirwan, 2018). Carden and Wood (2018) noted that habits have a dynamic role to play on the intention to perform IS activities, however, there may be limited change in behavior due to habituated tendencies. Responses to actions in new situations may remain constant, even with consistent, contextual references (Carden & Wood, 2018). Dupuis, Crossler, and Endicott-Popovsky (2012) stated that if home PC users neglect safe and secure cyber practices, federal agencies, private businesses, financial institutions, global markets, and even national security are all at increased risk.

Millennial home computer and Internet users are a group needing additional research as a home computer PC user segment (Stewart et al., 2017). Millennials are the largest generational group currently, technology-oriented from an early age, belong to a fast-paced era, and take risks due to a sense of invulnerability (Fry, 2016; Smith & Nichols, 2015). The literature highlights this group as risk-takers with online activities due to the 21st-century lifestyle, which promotes a fast tempo and potential for unhealthy security habits (Waljee, Chopra, & Saint, 2018). Millennials may miss the opportunity to safeguard PCs with the first line of defense in home security, installing antivirus software (AvSW). Understanding if millennials' history of IS behaviors that become habituated actions have influence on decision-making is a goal of the study.

Antivirus software can be protection against malware code loosed on the Internet that is deployed at a faster rate than the average millennial Internet home computer user can adapt (Loving, 2016; Razak, Anuar, Salleh, & Firdaus, 2016). Antivirus software is a programming package designed to scan, detect, and quarantine computer viruses (Wash & Rader, 2015; Webroot, 2018). Loving (2016) noted that the duty for averting malicious activity falls to AvSW suites to remedy increased home computer vulnerabilities.

This millennial home computer security research joins the conversation in the IS body of knowledge using the habit-to-intention phenomenon to address the gap in the literature. The study uses the habit theory and protection motivation theory (PMT) to observe the millennial generational group's behavioral intention to install AvSW (Rogers, 1983; Vance, Siponen, & Pahnila, 2012). Figure 1 shows the research model using the amended PMT framework. The contextual model has three components: sources of information, habits or previous automatic

behaviors, the cognitive mediating process, including threat appraisal and coping appraisal factors, and the coping action or intention.

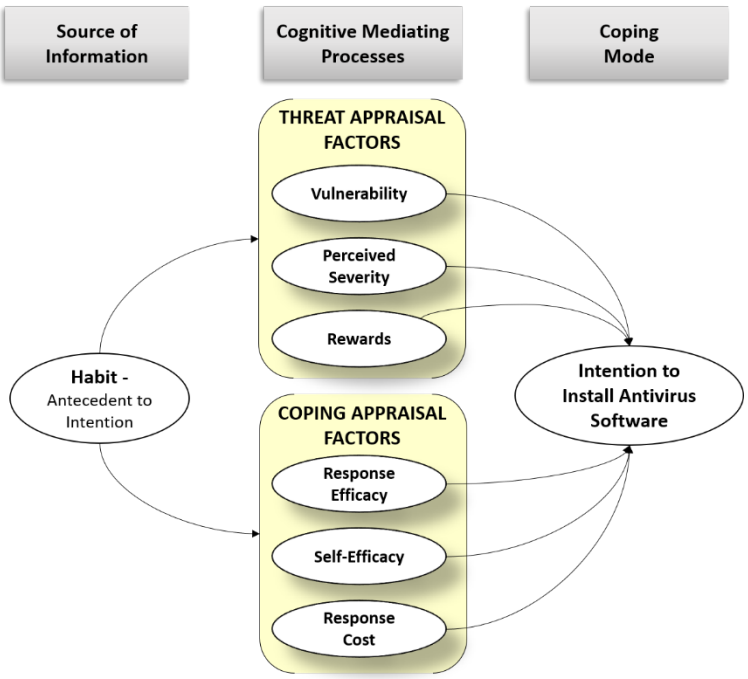

Figure 1. Research model (Vance et al., 2012, p. 191).
The research model illustrates the influence of habit as a source of information on the cognitive mediating process. Factors in the threat and coping appraisal processes show how habit potentially influences intention to install AvSW. Adapted from "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory," by A. Vance, M. Siponen, and S. Pahnila, 2012, *Information & Management*, *49*, pp. 191. Copyright 2016 by the American Psychological Association.

The PMT is an empirically proven theoretical framework for observing the process that survey participants go through when negotiating which security behaviors to employ (Crossler & Belanger, 2014). Literature reports that the PMT invokes a cognitive mediating process derived from informational sources about IS threats (Rogers, 1983). The cognitive mediating process of the PMT includes three factors from the threat appraisal process and three factors from the

coping appraisal process which influence behavior (Rogers, 1983). Each appraisal process estimates how research participants' responses would increase or decrease the likelihood of maladaptive or adaptive behaviors. Note the recreated schema of the PMT contextual framework in Figure 2 (Rogers, 1983, p. 168). The recreated image in Figure 2 shows the use of habit as an intrapersonal source of information to protection motivation factors concerning an IS threat. The modified PMT framework exposes the significance that habituated actions have on millennial's IS behaviors and practices, and how research participants may respond to cautions relating to cyber threats or hazards (Rogers, 1975; Rogers, 1983; Vance et al., 2012).

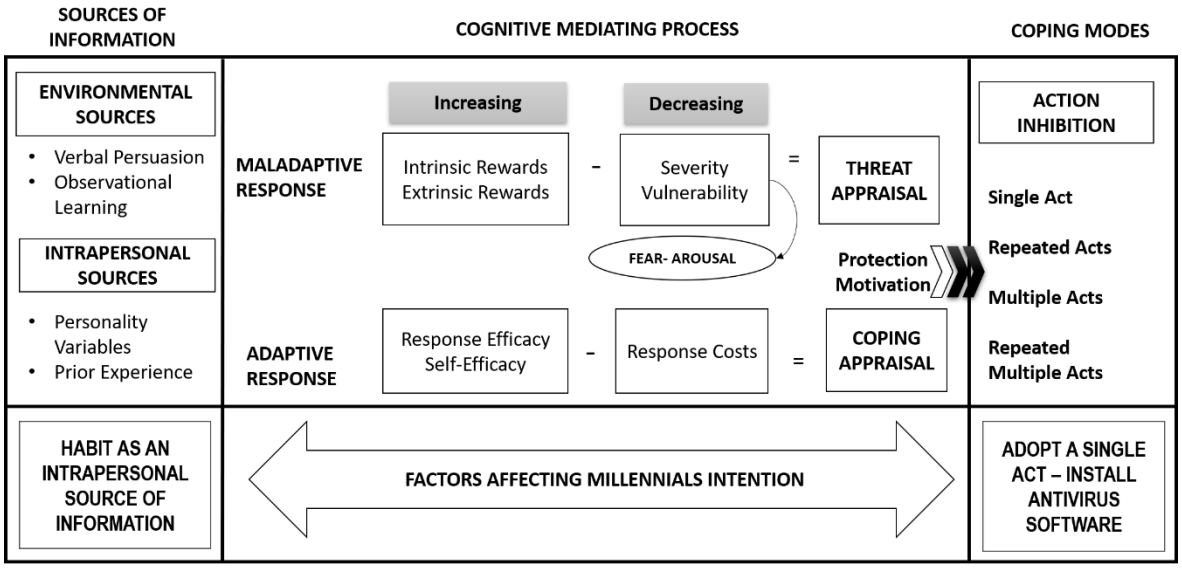

Figure 2. PMT framework schema recreated from Rogers (1983, p. 183).
The graphic shows the three sections of the protection motivation theory, the sources of information, the cognitive mediating process, and the coping modes, including how the equation works. Adapted from "Cognitive and Physiological Processes in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation," by R. W. Rogers, 1983, *Social Psychophysiology: A Sourcebook*, pp. 183. Copyright 2016 by the American Psychological Association.

Statement of the Problem

Home computer user's non-secure behavior that originates from prior experiences and habituated responses potentially promotes victimization due to cyber pitfalls. There is a gap in the literature concerning the habit-to-intention phenomenon that needs additional coverage in the IS body of knowledge (Dupuis et al., 2016; Howe et al., 2012; White, 2015). Dupuis et al. (2016) mentioned that IS literature needs further research on habit-to-intention topics and explains that while habit has been a part of various IS research, the notion of intention needs focus. Limayem, Hirt, and Cheung (2007) were among some of the first researchers to engage the habit-to-intention subject matter and purported that the relationship between behavioral intention and automatic IS responses is delicate. Researchers should exhaust the issue to obtain a better understanding of this multifaceted and complicated association. Norman, Boer, and Seydel (2005) recommended future research and development covering the influence of past behavior on intention. Thus, this millennial home computer research seeks to address this gap in the literature.

Purpose of the Study

Millennial's use of the Internet might compromise home PCs. The purpose of the study was to identify whether millennial home PC users' previous IS habituated actions influenced decision-making and affected intention to install precautionary security software. The research is necessary because it seeks to understand the habit-to-intention phenomenon using relevant applications of past IS behaviors and automaticity affecting the acceptance of recommended actions. Automaticity is routinized practices driven by behavioral frequency (Boehmer, LaRose, Rifon, Alhabash, & Cotten, 2015; Gardner, Abraham, Bruijn, & Lally, 2012). Millennial home

PC users might be ill-equipped to navigate the changing and evolving data security shifts due to several factors: rapidly advancing technology, malware, and unhealthy IS experiences (Ong & Chong, 2014; Smith & Nichols, 2015; Wash & Rader, 2015). Of consequence to this millennial home computer user study is how these criteria might affect the implementation of AvSW.

Significance of the Study

Researching the habituated actions of the millennial home PC user and factors that influence IS decision-making addresses the gap in the literature and has implications to practice (Dupuis et al., 2016). Another significance of the study is the importance of AvSW, the first line of defense against malware on home PCs, which empowers home computer users to protect personal data. Information security literature records increased Internet and home computing usage over the last 20 years (Carden & Wood, 2018; Fry, 2016). The increase in Internet usage inspires discussion on cybersecurity surrounding home PC user's behavioral intention with security concepts (Arachchilage, Love, & Beznosov, 2016; Boehmer et al., 2015; Crossler, Belanger, & Ormond, 2017; Dodel & Mesch, 2017; Tsai et al., 2016). These concerns create relevance to the IS community because the way individuals interact with computing technology has a role to play in managing protective software designed to thwart malware, increase personal security, and avoid adverse effects on PCs (Wash & Rader, 2015). The focus of the research concerned prior experiences and actions of millennials and how these actions might influence installing AvSW.

Research Question

The research question states the following: Is there a significant association between millennials' IS habits and protection motivation factors that indicate an intention to install

antivirus software? There were six PMT factors and hypotheses statements that captured the potential influence to install antivirus software.

Hypothesis 1: There is a positive correlation between millennials' IS habits and perceived vulnerability.

Hypothesis 2: There is a positive correlation between millennials' IS habits and perceived severity.

Hypothesis 3: There is a negative correlation between millennials' IS habits and intrinsic and extrinsic rewards.

Hypothesis 4: There is a positive correlation between millennials' IS habits and response efficacy.

Hypothesis 5: There is a positive correlation between millennials' IS habits and self-efficacy.

Hypothesis 6: There is a negative correlation between millennials' IS habits and response costs.

Definition of Terms

Behavioral intention. Behavioral intention is an individual's perceived proclivity or probability of implementing a required or recommended behavior (Conner & Norman, 2005; Rogers, 1975; Yoon, Hwang, & Kim, 2012). The abbreviation for behavioral intention is ITC in the study, short for intention to comply. The intention variable is the output of protection motivation factors in the contextual framework and is the most proximate forecaster of behavior (Conner & Norman, 2005). Information security literature alleges the direct correlation between behavioral intention and actual behavior (Dupuis et al., 2016).

Habit. Habit is the dependent variable in this millennial home PC user study. In the contextual framework, habit is the source of information for intention. The definition of a habit is a form of repetitive, automatized behavior measured in behavioral frequency related to specific situations (Shropshire et al., 2015; Vance et al., 2012; Verplanken & Orbell, 2003). A habit is an abstract concept generated by automaticity in response to cues (Verplanken & Orbell, 2003). Statements describing habits are goal-directed, a learned series of acts, or behaviors conducted with minimal cognitive processing (Verplanken, Aarts, & Van Knippenberg, 1997).

Perceived severity. Perceived severity, abbreviated as PS, is an independent variable. Woon, Tan, and Low (2005) defined perceived severity as the measurement of consequential seriousness surrounding a threatened event. It is the degree, depth, or magnitude to which millennials genuinely believe the threat of having a home computer compromised will occur. Perceived severity is part of the threat appraisal process, and covers IS threats like a computer data breach or data loss (Woon et al., 2005; Yoon et al., 2012).

Perceived vulnerability. Perceived vulnerability, abbreviated as PV, is an independent variable. Perceived vulnerability is the likelihood of the occurrence of an unwanted incident happening without instituting preventative measures (Vance et al., 2012, p. 191). It is the degree that a millennial believes in the susceptibility of a computer threat (Vance et al., 2012; Woon et al., 2005). Workman, Bommer, and Straub (2008) noted three susceptibilities as examples, the fear of being a victim of malware, the fear of having data compromised or becoming a victim of identity theft, and the fear of being infected by malware and having damage to data.

Response costs. Response costs, abbreviated as RC, is an independent variable. Response costs are discomforting measures imposed on millennials for adopting the recommended

behavior (Chenoweth et al., 2019; Rogers, 1975; Thompson, McGill, & Wang, 2017). Discomforting measures can be time or costs impositions that increase maladaptive responses, akin to unpleasant reinforcements or punishments (Rogers, 1983).

Response efficacy. Response efficacy, abbreviated as RE, is an independent variable. Response efficacy is the belief that the recommended IS protective behavior of installing AvSW will alleviate the cyber threat (Tsai et al., 2016). It is a millennial's faith in the recommended action. Together, response efficacy, self-efficacy, and response costs comprise the coping appraisal process.

Rewards. Rewards, abbreviated as R, is an independent variable. Rewards are motivations used in the PMT for preserving or developing unwanted IS behaviors (Rogers, 1975). Rewards are part of the threat appraisal process and are either intrinsic incentives - promoting perceived pleasure, or extrinsic motivations, inspiring social approval (Vance et al., 2012). Intrinsic or extrinsic rewards are actions associated with the perceived benefits of avoiding the desired action and decrease the likelihood of a millennial implementing the recommended behavior (Tsai et al., 2016; Yoon et al., 2012). An example of rewards is preserving time (Vance et al., 2012).

Self-efficacy. Self-efficacy, abbreviated as SE, is an independent variable. Self-efficacy is a millennial's perception of personal ability or confidence to implement a computer security function, like installing AvSW (Maddux & Gosselin, 2003; Meso, Ding, & Xu, 2013).

Research Design

The research design employed a quantitative, nonexperimental methodology, and survey design. Characteristics of survey research design drove the choosing of this method, namely the

simplicity of use, time efficiency, and inexpensive options that make data extraction and analysis more convenient (Field, 2009). The 7-point Likert scale instrument collects responses through 24 content questions structured around personal IS automaticity and intention with three scenarios constructed in a pattern of extremely unlikely to extremely likely. Likert scale surveys promote reliable, yet simple scaling without assumptions and long or difficult creation time and provide the added benefit of collecting data remotely (Andres, 2012; Fowler, 2009). The Millennials and Antivirus Software Survey Instrument incorporated the variables in the PMT, habit, perceived vulnerability (PV), perceived severity (PS), rewards (R), response efficacy (RE), self-efficacy (SE), response costs (RC), and behavior or intention (ITC). Of interest to the study are methodological, topic-specific, and measures assumptions.

Assumptions and Limitations

Assumptions

This quantitative, nonexperimental research design depends on the post-positivistic paradigm (Creswell, 2014; Crotty, 2012). Post-positivists, who hold to a determinism approach, state that for every observation, there exist conditions that could bring about no other event; therefore, the paradigm causes defined outcomes. Accordingly, post-positivists have a theoretical-based perspective, concerned with a reality that is observable, fixed, and measurable.

General methodological assumptions. The PMT framework defined and categorized the data with empirical testing to answer the research questions (Crotty, 2012). The bivariate analysis evaluated the relationships between variables noting any significance. The PMT variables are perceived vulnerability (PV), perceived severity (PS), rewards (R), response

efficacy (RE), self-efficacy (SE), and response costs (RC). Additional testing of correlated PMT variables with habit allowed for exploratory testing for future research.

Topic-specific assumptions. Topic-specific assumptions involve the identified area of research and associated topics within the body of knowledge. There are seven such assumptions in this quantitative, nonexperimental millennial home computer user research noted by Kreiner, Hollensbe, and Sheep (2009). The seven assumptions are

- meeting qualifications,
- understanding survey questions,
- protecting privacy,
- adhering to guidelines,
- establishing an IS theory,
- applying sampling, and
- noting limited bias.

The expectation that participants meet the criteria of being part of the millennials' generational group, which qualifies the individual to take the survey, is the first noted assumption. A second assumption is that participants should understand survey instructions, questions, terms, and definitions. This understanding includes the associated wording, designed to be uncomplicated, unambiguous, and understandable, written on an eighth-grade level. Third, there is a study standard for the participant's privacy protection (Collaborative Institutional Training Initiative [CITI] Program, 2014). There was no interaction between researcher and survey participants during data collection. Therefore, personal identifying information (PII) to

distinguish one survey taker from another was not retrieved. Thus, due to the low risk associated with the research design, there was no concern about the participant's privacy protection.

The fourth topical assumption was the understanding that academic research required an established study design and plan for conducting data analysis. The study employed a survey design with a 7-point Likert scale approach. The plan for data analysis was to use bivariate correlational testing. Correlational analysis has a set of assumptions associated with the testing choice. Four of these assumptions are linearity, homoscedasticity, absence of multicollinearity, and normal distribution (Antonius, 2003). The fifth assumption is that the research should be grounded in a well-established theory. This millennial home PC user research used a grounded and empirically tested theory called the PMT. The PMT, established by R. W. Rogers in 1975 and revised in 1983, has been around for approximately 40 years (Maddux & Rogers, 1983; Rogers, 1975; Rogers, 1983). Vance et al. (2012) introduced a contemporary adaptation of the theory integrating habit as the source of information to the cognitive mediating process of the framework.

Assumption six was the use of the commercial survey service that provided panelists associated with the millennials' group. However, using paid panelists might lead to practiced bias and data quality issues. An assumption of the study is that survey participants were free from bias and responded honestly to the survey questions with good recollection. The last assumption required that data collection adhere to the strict code of ethics in research identified in the American Psychologist Association (APA). The standard described that a researcher should be free from bias and must collect data to ethical parameters (American Psychologist Association, 2016). A final assumption noted that millennials – who are designated to be associated with

technology from an early age, described as technologically immersed, and part of the diminishing digital divide era, will have a home computer (Fry, 2016).

Assumptions about measures. Assumptions about measures included analytical assumptions for testing research data. There are several assumptions declared for correlational analysis. Four correlational assumptions are linearity, homoscedasticity, absence of multicollinearity, and normal distribution (Antonius, 2003). Linearity claims that there is a linear relationship between the dependent and independent variables. Homoscedasticity states that data values for dependent and independent variables have equal variances. The absence of multicollinearity asserts that there is no correlation between two or more independent variables. The use of parametric tests depends on an assumption that statistical data adheres to a type of distribution that is bell-shaped or normally distributed. The violation of parametric test assumptions changes the conclusion and interpretation of the results.

Limitations

Design limitations. A study's limitation surround impediments in design or methodology that could potentially affect or influence the interpretation of the research analysis and findings (Crotty, 2012). The four study limitations were (a) participant truthfulness, (b) researcher bias, (c) research design, and (d) Likert scale survey design. These limitations are recurrent pitfalls associated with survey research (Alreck & Settle, 1995; Baron, 1996; Clark, 2006; Cooper, Schindler, & Sun, 2006).

Participants' truthfulness in answering the questionnaire is an identified limitation. The integrity of the survey leaned on the honesty of both participants and the researcher. The generalizability of the sample group to the broader population depended on participants' integrity

and truthfulness with the millennial inclusion question, which pointedly asked if the participant was part of the millennial generation group.

The second limitation is bias on the part of the researcher, a frequent pitfall in research. The post-positivistic method uses descriptive statistics and correlational output to understand observations and analyses which notes that researchers should clarify any bias potential associated with data (Antonius, 2003; Creswell, 2014; Field, 2009). A review of all sides of the argument mitigated any personal bias in the research effort. While avenues of gathering data can ascribe to some bias, the standardized process implemented in the study safely minimized this concern.

The third limitation dealt with restrictions on recruitment, data gathering, and sample size. Recruitment might play a role as a limitation due to the procurement of paid panelists from the online survey service. The survey service, a procured, professional entity that allowed for no interaction between researcher and participant, provided survey takers. There was a potential that the acquired research participants might respond a certain way due to affiliation with the paid service. Along with the sample size, another limitation was the choice of convenience sampling. Convenience sampling was a limitation that could be remedied with simple random or probability sampling.

The final limitation refers to the use of Likert scales which has differing opinions on its use (Alreck & Settle, 1995; Baron, 1996; Cooper et al., 2006). Alreck and Settle (1995) noted that using the Likert scale for measurement might promote an inaccurate or incorrect interpretation of responses. Participants might have concerns with intensity, remembrance, and frame of mind when using Likert scale surveys.

Delimitations. The study's delimitations, or set boundaries, control the range of the study. The study researched the home computer user group and not mobile device users or mobile technology habits. While the study discussed habit as a variable, the habit theory in its entirety and neuroscience with habituated acts were out of scope for the study. The questionnaire did not request the survey participant's geographical location or age group. The next section summarizes what to expect in the remaining chapters.

Organization of the Remainder of the Study

Chapter 1 described the reason for the research effort and how the identified problem invoked the research question. Discussion on the theoretical framework, areas of interest from the literature review, and synthesis and critique of some areas of the research are segments found in Chapter 2. Chapter 3 mirrors Chapter 1 but gives additional detail and emphasis on the research methodology and provides procedural information to shape the statistical analysis. The data analysis results chapter, Chapter 4, reports outcomes. Chapter 5 refreshes readers on the results of the data analysis by summarizing the findings from Chapter 4, discussing implications to practice, and giving recommendations for further research.

CHAPTER 2. LITERATURE REVIEW

This literature review brought together a collection of articles surrounding the subject of home computer users, network security, malware, and millennials. An analysis of the literature concerning IS habits created a foundation for verifying whether the topic was worthy of researching. Key areas of interest covered in the literature review were Internet and home PC user cyber behavior leading up to the need for the research, millennials as the chosen segment of home PC users, and malware that drives the recommended action for intention. There is a gap in the IS body of knowledge concerning how IS habits affect protection motivation factors with home computer users and associated security behaviors.

The remaining sections of the literature review are the synthesis of research findings and a critique of previous research. The review used grounded and guided concepts collected from the literature review to formulate the foundation of the study through the evaluation of both original and contemporary research. Searching methods provided scope for research disparities and highlighted areas of focus that thereby exposed the gap in the literature and provided potential to contribute to the IS body of knowledge.

Methods of Searching

The depth of a literature review intricately depends on searching methods (Haeussinger & Kranz, 2017). The initial search for references uncovered Yoon et al.'s (2012) article through a database search for IS studies implementing the PMT framework. Yoon et al. included habit as a variable affecting intention denoting factors and motivators influencing college students' IS behaviors. The inspiration for using the habit construct in Yoon et al.'s study directed further reference mining for PMT studies implementing habit in the contextual model. Additional

surveying of the literature surfaced Vance et al.'s (2012) article. In the article, Vance et al. posited that habit was not merely a factor to intention, but the source of information due to past automatic experiences. These articles served as a base to structure this project. Various references on the topic of IS and PMT studies confirmed the subject area as viable.

Data mining of Summons, SAGE, ABI/INFORM, ProQuest, Google Scholar, and other databases produced relevant material to dissect the topic. Other databases mined were (a) Academic Search Premier, (b) Business Source Complete, (c) Computers and Applied Sciences Complete, and (d) ScienceDirect. Internet searches for information on millennials produced current reports on this talented population group. Keywords included behavior, computer security, fear appeals, habit, health belief model, home PC user, information security, intention, millennials, online safety, PMT, rewards, risks, security, self-efficacy, threat, and user behavior.

Theoretical Orientation for the Study

The underpinnings for this millennial home PC user research adhere to a social science theory based on post-positivistic philosophy (Crotty, 2012). Crotty (2012) noted that the theory Fascribes to the notion that any opinions, principles, beliefs, background, information, and standards of the researcher inspires the reviewed information. Knowledge encompasses human estimations. Patten (2014) defined a theory as a cohesive description of distinct observation bringing together potentially unrelated or contradictory information. Two merged approaches framed the theoretical foundation, the PMT, and the habit theory. The theories formed a contextual framework that incorporated habit as an antecedent of protection motivation factors in the cognitive mediating process that, in turn, potentially influenced intention.

Habit is essential to the formation of action, notes Bennett, Dodsworth, Noble, Poovey, and Watkins (2013). Bennett et al. (2013) noted that habit had always been an entry point into behavior construction. The perception of habit in research has an extensive history in social sciences dating back to 1890 (Limayem et al., 2007). Initial habit researchers sought to understand its usefulness and automaticity to invoke actions without much reasoning intervention (Aarts & Dijksterhuis, 2000; Limayem et al., 2007; Ramírez-Vizcaya & Froese, 2019). Aarts and Dijksterhuis (2000) stated that sources of information, regarding cognitive cues, had immediate power over behavior. Ramírez-Vizcaya and Froese (2019) noted the dualism of habit between mindfulness and mindlessness. The spontaneous nature of habituated tendencies dictates the minimal need for constant intentional control, associating habit with the mindlessness side of the dichotomy.

The correlation between past behavior and future behavior illustrates the influence that habit has on invoking an action that may aid in decision-making (Aarts & Dijksterhuis). Yoon et al. (2012) reported that adopters of technology might rely on past experiences to make IS decisions. Therefore, security habits may influence IS behaviors and intention. The influence of formed habituated tendencies that invoke behavior secured the habit variables' incorporation into the contextual framework. Vance et al. (2012) used the habit theory in the PMT framework because the use of habit in IS research was weak.

The PMT framework originated from observing health-related behaviors and was implemented to make observations more forthright and interpretable (Rogers, 1975). Rogers (1975) noted that the PMT was a meticulously deliberate and delimited framework that could make the tool amenable to empirical review and could add value and bring order to confusion.

The literature validated the explanatory power of the PMT to predict users' intention and to make comparisons more straightforward and consumable (Chenoweth et al., 2019; Safa et al., 2015).

As reported by Rogers (1975), the original design of the PMT dealt with fear appeal messages that ignited cognitive appraisal processes involving

- the noxious event or intensity of the threat,
- the likelihood of the threatened event occurring, and
- the efficacy of a suggested coping response.

Information security literature extended the PMT due to the framework's flexible application to various research concepts, like additions of social norms and habit variables. The literature indicated relevance for both the PMT, and fear appeals to information technology (IT) related behaviors (De Keyzer, Dens, & De Pelsmacker, 2017; Yoon et al., 2012). The application of this millennial home PC user research to the IS body of knowledge entailed understanding the practice of defending information from unauthorized access, disclosure, use, disruption, modification, or destruction of data (Whitman & Mattord, 2017). A second application was identifying a research participant's lack of motivation to act against IS threats even when presented with knowledge of risky online activities (Jansen & Van Schaik, 2017).

The PMT posits that an individual's cognitive appraisal of a threat inspires a protective behavior to alleviate an undesirable outcome that influences a transformation in the way individuals respond to stimuli (Vance et al., 2012). The new model for this quantitative, nonexperimental research effort surveying the millennial home PC user incorporates the three sections of the PMT, sources of information, the cognitive mediating process, and the coping mode, as seen in Figure 3.

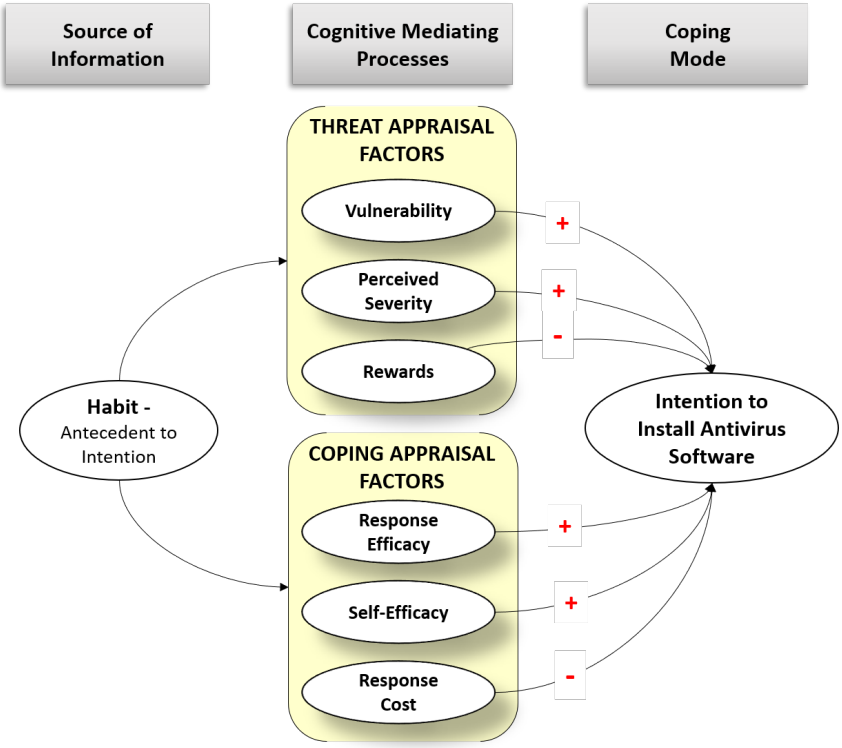

Figure 3. Model predictions (Vance et al., 2012, p. 191).
The graphic shows the modified contextual framework and the estimation of positive and negative outcomes for each predictor variable. Adapted from "Motivating IS Security Compliance: Insights from Habit and Protection Motivation Theory," by A. Vance, M. Siponen, and S. Pahnila, 2012, *Information & Management*, *49*, pp. 191. Copyright 2016 by the American Psychological Association.

The PMT framework works best on the intention to act rather than on predicting actual behavior (Maddux & Rogers, 1983; Rogers, 1983). Rogers' (1983) contextual framework specified that at the initiation of a threat, a cognitive mediating process occurs that causes an individual to analyze and evaluate risk. Jansen and Van Schaik (2017) proposed that the severity of Internet-related threats, or observations of threat susceptibility to cyber pitfalls, might provoke individuals to evade the undesirable outcome and institute the recommended posture.

Sources of information, the cognitive mediating process, and the coping process are the three sections of the PMT. Sources of information like traits or characteristics, personality variables, prior experience, and feedback from specific experiences, serve as antecedents to the cognitive mediating process originating from environmental or intrapersonal origins(Crossler & Belanger, 2014). Crossler and Belanger (2014) stated that environmental sources of information include vocal communications and observational research.

Conversely, examples of environmental sources are verbal persuasion and observational learning. Researchers in the IS body of knowledge posited that prior experience with both situational cues and habit influenced decision-making (Kurz, Gardner, Verplanken, & Abraham, 2015; Nilsen, Roback, Brostrom, & Ellstrom, 2012). Therefore, this millennial home PC user research effort used the established merged habit theory and PMT to examine the significance of habituated actions on intention (Vance et al., 2012). This theoretical merge allows for an understanding of how past and automatic IS behaviors can affect intention.

For the PMT model implemented here, habit is the antecedent to intention. The cognitive mediating process of the PMT's contextual framework divides into two appraisal processes, the threat appraisal process and coping appraisal process. Each process has three factors. The three elements in the threat appraisal process are perceived vulnerability, perceived severity, and intrinsic and extrinsic rewards. The three coping appraisal factors are response efficacy, self-efficacy, and response cost.

Threat Appraisal Process

Threat appraisal corresponds to understanding the source of the threat and its effect on maladaptive behavior. Norman et al. (2005) noted that the threat appraisal process concentrates

on the threat source and factors increasing or decreasing the likelihood of maladaptive responses. The three threat appraisal factors are

- vulnerability - the extent of an individual's perceived susceptibility to IS threats,
- severity - the depth and magnitude of an IS threat,
- reward - any intrinsic or extrinsic motivation to develop or keep positive IS behaviors.

Examples of the threat appraisal components are estimates of contracting a disease (perceived vulnerability), and forecasts of the criticality of an illness (perceived severity), noted Norman et al. (2005). The threat appraisal component should inhibit maladaptive responses (Vance et al., 2012; Yoon et al., 2012). Van Schaik, Jansen, Onibokun, Camp, and Kusev (2018) reported that threats are equivalent to users' risk assessment perceptions. For IS adaptation, the vulnerability of an IS threat equates to susceptibilities to cyber pitfalls on the Internet. A similar example of severity is the corruption of home computer data due to malware.

Norman et al. (2005) observed that while severity and vulnerability might prevent maladaptive responses, some intrinsic rewards, like perceived pleasure and extrinsic rewards, like social approval for not taking the recommended action, might have an opposite effect. Rewards negotiation pertains to reducing or altering the recommended behavior (Munafo & Albery, 2008). Both types of rewards, intrinsic and extrinsic, are motivational aids in facilitating the adoption of maladaptive behavior (Munafo & Albery, 2008; Woon et al., 2005). For example, if a home computer user can save time by avoiding installing AvSW, the PC user gains the reward of time for not performing the recommended action. The PC user acts maladaptively to the recommended action. Therefore, because of either the intrinsic or the extrinsic IS reward, a person might choose not to take precautionary data security measures. Rogers' (1983) model

shows that information sources drive responses, whether facilitating or inhibiting, which, in turn, influences behavior. Norman et al. (2005) communicated that the threat appraisal variables associate and compound together with the three coping appraisal factors to elicit protection motivation.

Coping Appraisal Process

The coping appraisal process relates to a millennial's belief in the ability to cope with and avoid cyber threats (Woon et al., 2005). Norman et al. (2005) noted that the coping appraisal process concentrates on the coping response that effectively confronts the threat, and the components that increase or decrease the likelihood of the adaptive response. The coping appraisal process explains a research participant's ability to manage or cope with a perceived computer threat. It consists of three coping appraisal factors:

- response efficacy – assurance in the perceived coping response to successfully alleviate the risk;
- self-efficacy – the extent of personal belief in the skill set needed to implement the protective behavior; and
- response cost – the associated cost to the user for enacting the protective action.

Response efficacy is the survey recipient's belief that implementing the recommended action will alleviate the threat (Norman et al., 2005). Self-efficacy pairs with response efficacy and evaluates the response (Maddux & Rogers, 1983). Self-efficacy is confidence in successfully negotiating and executing the endorsed course of action (Norman et al., 2005).

Response costs include expenses associated with instituting the recommended action. Researchers suggest that response costs can consist of time, money, and effort spent in enacting

the adaptive coping behavior (Chenoweth et al., 2019). Response cost relates to the cost of purchasing AvSW and the time it takes to implement and maintain the software. Home PC users' assessment of the value associated with performing the selected coping behavior hurts the adaptive behavior's implementation, promoting the maladaptive response.

The combined appraisal processes promote the intention to perform adaptive or maladaptive responses. Components of the threat appraisal response allow for evaluation and observation of the source of the threat. The coping appraisal process notes the individual's administration of the coping factors available to deal with the threat. From the literature, a premise of this quantitative methodological study posits that personal, informational sources about IS threats invokes a cognitive mediating process in millennials that appraises both positive and negative responses (Vance et al., 2012). The coping mode, the third section of the model, includes intention and other factors affecting behavioral intention. The cognitive mediating process section illustrates how the creation of fear-arousal is a prerequisite for acting on the severity and vulnerability of a perceived IS threat. Both the threat appraisal process and coping appraisal process generates protection motivation for the coping mode that can be either a single act, repeated acts, multiple acts, or repeated multiple acts (Rogers, 1975).

PMT Summary

The PMT is an empirically proven theoretical framework for observing the process that survey participants go through when negotiating which security behaviors to employ. The enhanced PMT framework provided the opportunity to integrate other variables lacking a clear connection into this coherent and substantive theory. The contextual model has three components: sources of information, the cognitive mediating process, threat appraisal and coping

appraisal factors, and the coping action or intention. The theory emphasizes coping with a menacing event using two appraisal processes in the cognitive mediating component, the threat appraisal process, and the coping appraisal process. This cognitive mediating process deploys essential properties of fear appeal arousing protection motivation factors that assist in coping with the threat, acting as an intervening variable that incites, sustains, and directs activity to protect oneself from danger. The theory can help interpret how a threat experience could influence attitude change, belief acknowledgment, and behavior alteration due to compelling communication. The review of the literature section exposes critical areas of interest in the research process. These areas include discussions on home computer users, including IS behaviors, millennial attitudes and IS posture, malware in the literature, and user responsibility in the cyber world.

Review of the Literature

The inspiration for this millennial home PC user project came about from a research call inspired by a gap in the literature with habit-to-intention. The literature stated that Internet and home PC users habituated IS practices created a weak security foundation. There was a call for research for the home PC user due to the powerful surge in Internet use and the push of various cyber technologies into mainstream online activities. The research importance for the study focused on the millennial generational group's past IS behavioral experiences and how habituated tendencies might affect the intention to implement AvSW. The literature review began with a focus on the theoretical framework and understanding of home computer users.

Why Research Home Computer Users?

The literature exposed several reasons for researching home PC users, including excessive availability of Internet and computer services, limited security knowledge about malware susceptibilities, and inadequate IS training directed to home computer users (Rantonen, 2014). Home PC users are not prepared to handle malware targeted towards home computer users, and due to rapid and ever-emerging malware, do not have enough security awareness knowledge concerning IS vulnerabilities and susceptibilities (Howe et al., 2012; Ong & Chong, 2014; Razak et al., 2016). The limited knowledge of home computer users comes from the reduced training opportunities available for this group, which leaves users untrained and ill-prepared to deal with security threats (Safa et al., 2015). Unlike workplace users who have trained professionals to support and troubleshoot IS issues and concerns, home computer users are exposed, and a lack of training may lead to frustration and apathy with security recommendations. These cited references and stated reasons for research confirm that home computing is an area for current research due to its increasing significance to information security.

Computer and Internet Availability

In the last decade, Internet and home computing availability increased to the broader population (Anderson & Agarwal, 2010; Lopez, 2015; Thompson et al., 2017; Wash & Rader, 2015). Anderson and Agarwal (2010) reported that over one billion people connected to the Internet in 2010. Wash and Rader (2015, p. 309) noted that over 76% of the U.S. accessed the Internet from home computers. Current literature indicated that personal computing became more of a lifestyle than a luxury due to increased availability and use (Lopez, 2015). Information

security conscious care behavior, antimalware protective software use, and IS awareness must increase to meet the security need of home computer users that are considered a potential point of weakness in security continuity.

Home computer user IS behavior. User behavior is the main factor in Internet security for home computing activities (Nthala & Flechais, 2018; Safa et al., 2015; Wash & Rader, 2015). Home computer users are ill-equipped to navigate the changing cyber landscape and evolving data security shifts. The literature communicated that bad IS habits have a direct role to play on the intention to perform positive IS activities and adequately manage data security (Wash & Rader, 2015). Nthala and Flechais (2018) noted that home PC users greatly influenced online security due to compromising behavior that potentially exposed other infrastructures to attack. Safa et al. (2015) considered user behavior as a vital factor in personal security protection.

It is everyone's responsibility to be safe online, but the literature noted the critical need to encourage home PC users to practice home computing security (Crossler et al., 2017; Tsai et al., 2016; White, 2015; White et al., 2017). Many researchers in the IS body of knowledge sought to understand what motivated Internet and home PC users to take personal responsibility for protecting data and digital personas (Boehmer et al., 2015; Crossler et al., 2017; Ion, Reeder, & Consolvo, 2015; Mills & Sahi, 2019; Safa et al., 2015; Tsai et al., 2016). Boehmer et al. (2015) argued that Internet users showed a lack of interest in implementing preventative measures, be it behavioral or technical, due to blindness to online safety concerns and the lack of personal responsibility acceptance. Present-day technology trends demand that millennial home PC users become aware of the heightened need for home computing security due to continuous availability and connectivity to the Internet.

Bad IS habits, Internet user's ignorance, or home security mistakes increase online risks with the potential for financial damage due to identity theft or data loss (Anderson, Vance, Kirwan, Eargle, & Jenkins, 2016; Cain, Edwards, & Still, 2018; White et al., 2017). On the other hand, healthy habits, like protecting one's PC with AvSW, have a positive effect on averting security threats (White et al., 2017). User habituated practices transcend safety beliefs, notes Cain et al. (2018). Therefore, directing and enhancing IS habits and self-efficacy strengthens continued security actions. Anderson et al. (2016) reported that computing decisions depend on individual users, and personal habits have a great deal to do with IS practices. Encouraging home computer users with security awareness messages while reinforcing the need for personal responsibility with online actions might reduce home computer users' security risks (Boehmer et al., 2015; Dodel, & Mesch, 2017; Shillair et al., 2015). Cybersecurity research emphasized the unattainable pursuit of cyber safety without directing human interaction towards proper security behaviors and awareness training.

Home computer users need for awareness and training.

Emerging technology. Three reasons for home computer user's security unpreparedness are emerging technology, the absence of knowledge and awareness to combat malware, and the lack of training directed to home computer users (Anderson et al., 2016; Crossler & Belanger, 2014; Mouakket, 2015; Safa et al., 2015). A reason for home computer user unpreparedness might be the boost in emerging technology. Friedman (2016) noted that technology transforms faster than human adaptability, a situation that Friedman considered confusing for many people. Malware code loosed on the Internet at viral rates is faster than what the average Internet and home PC user can adapt, which puts home PC users at immediate risk. The increase in emerging

technology leaves home PC users exposed due to the many malware exploits targeting home computer users, and the lack of knowledge to combat such activities.

Security knowledge and awareness. Previous security habits have an integral part to play in IS behaviors due to automatic actions that may be potentially harmful (Arachchilage et al., 2016; Crossler et al., 2017; Dang-Pham et al., 2016; Dodel & Mesch, 2017; Howe et al., 2012; Shillair et al., 2015; White, 2015). White (2015) mentioned that poor Internet and home computer security choices and actions might correspond to the confidence placed in technology. Relying on old habits to assist with new technological processes while being inundated with daily threats poses a risk for home computer users (Dodel & Mesch, 2017). Security postures and cultural tendencies are compromising behavioral traits that influence ways of thinking and affect IS decision-making (Arachchilage et al., 2016; Howe et al., 2012; Stewart et al., 2017; Thompson et al., 2017).

Users' negligence, apathy, ignorance, irrational or impractical attitudes, and behaviors promote the notion of being the weakest factor in IS infrastructures in the workplace and at home (Anderson et al., 2016; Safa et al., 2015). By mindlessly clicking on suspect hyperlinks, entertaining suspicious emails, disregarding warning messages, providing information to phishing scams, and missing open opportunities to protect home PCs with AvSW, users equip hackers with the tools to corrupt personal data (Safa et al., 2015). The speed of technology causes a lack of knowledge to handle precautions and risks, and security behaviors might also be stale to combat new technology.

A resistance to amending bad IS behavior might be due to old habits being difficult to change (Burns, Durcikova, & Jenkins, 2012; Carden & Wood, 2018; Lynam, 2000). Burns et al.

(2012) suggested that people do not always change habits due to hindrances and obstacles that arise related to IS risks. Resistance to changing behavior arises because routinized action creates etchings in neural pathways that work against new, corrective acts (Carden & Wood, 2018; Lynam, 2000). As such, bad habits prevail even with unfavorable outcomes.

Gap in knowledge and skill. Not only do bad IS practices create situations for security threats to find a foothold, but victims of previous malware exploits are prime targets for future attacks and revictimization if the behavior remains unchecked and uncorrected (Carden & Wood, 2018). The literature implied that Internet and home computing security carries an enormous weight of responsibility for the home PC user, and the lack of knowledge and skill are the culprit (Crossler et al., 2017; Safa et al., 2015; Tsai et al., 2016). Home PC users need knowledge and skill to install AvSW and to implement other security tasks.

Lack of directed learning. Home computer users do not have the training opportunities as workplace computer users. Training awareness campaigns could promote communications designed to dissuade home PC user's potential disregard of protective technologies and countermeasures (Arachchilage et al., 2016; Crossler et al., 2017; Dodel & Mesch, 2017). Messages should not necessarily be fear-provoking campaigns as such messages might lose intention and purpose (Boss et al., 2015; Warkentin & Siponen, 2015). Excessive negative, high-toned, and fear-invoking communication might reduce the required fear response, drastically weakening message acceptance (Boss et al., 2015; De Keyzer et al., 2017). De Keyzer et al. (2017) mentioned that drunk driving cases where awareness messages are high-toned, the results inundated individuals and attenuated the desired effect, as seen in cases of multiple drunk driving offenses. Awareness education campaigns might potentially reduce maladaptive behaviors and

promote adaptive or positive behavior change by promoting cybersecurity training for home computer users (Anderson et al., 2016; Hanus & Wu., 2016). The segmented home computer user group for the study are millennials.

Millennials

Millennials are the generational group of the new millennium, born between 1980 and 2000 (Dannar, 2013; Fry, 2016; Shafer, 2015). Literature coins millennials as the entitled generation, the Net generation, digital natives, and FaceBookers (Fry, 2016; Nnambooze & Parumasur, 2016; Omilion-Hodges & Sugg, 2019; Smith & Nichols, 2015). Waljee et al. (2018) noted that millennials are different from other generation groups, in values, beliefs, hopes, and philosophies. The generation group is more technologically aware and digitally savvy than the typical Internet user due to interacting with technology at an early age (Omilion-Hodges & Sugg, 2019). Millennials are the first generational group to come of age in the era of cable TV, home PCs, Internet, and mobile technology (Fry, 2016; Milkman, 2017; Waljee et al., 2018).

The group brings to society a new way of thinking in this post-millennium era, and it is not always positive. Milkman (2017) summed up the millennial mindset as "selfish, narcissistic, and politically disengaged" (p. 2). Contemporary research notes that millennials are lazy, acquiring the reputation of a generation that everyone loves to hate (Nnambooze & Parumasur, 2016). The way that millennials think and believe might reshape the nation for the next two decades (Fromm & Garton, 2013; Fry, 2016). The millennial or Net Generation might be a misunderstood generational group due to confronting an unstable or precarious labor market and visualizing racial and gender disparities and the vocalization of class inequalities (Milkman, 2017; Stewart et al., 2017). Millennials are the chosen population to observe in this

nonexperimental study because of the group's free security-conscious attitudes that might exemplify the dominant posture in personal computing (Dannar, 2013; Fry, 2016; Milkman, 2017; Shafer, 2015; Stewart et al., 2017; Waljee et al., 2018).

Fry (2016) reported that millennials are a significant generational group to research for several reasons. The literature categorizes millennials as optimistic, confident, and even open to change, having a sense of entitlement and a sense of humor (Omilion-Hodges & Sugg, 2019; Smith & Nichols, 2015). Another reason to poll millennials is that the group is part of the fast-food or right now generation, sometimes having expectations without reasoned values (Waljee et al., 2018). Millennials are the largest generation group, between approximately 70 to 80 million people (Fry, 2016). Another reason for the group's diversification is that millennials are well educated and technically savvy (Stewart et al., 2017). Millennials speak the language of technology, fully integrating technology into daily activities even from an early age (Fry, 2016; Milkman, 2017). Thus, there is a need for additional research with the millennial generation group to understand the groups' IS beliefs and intention to install AvSW (Fry, 2016; Milkman, 2017; Stewart et al., 2017; Waljee et al., 2018).

A sense of entitlement. Current literature proclaims that millennials' attitudes surround a sense of entitlement (Nnambooze & Parumasur, 2016; Stewart et al., 2017; Waljee et al., 2018; White, 2015). Nnambooze and Parumasur (2016) mentioned that the millennial generational group has a high sense of privilege. White (2015) also recorded the group as entitled, reporting that millennials expected constant rewards. Millennials' sentiment and entitlement are equivalent to narcissism, but other reports portray millennials as high achievers and productive participants in the workplace seeking involvement in communication cycles well beyond established roles

(Omilion-Hodges & Sugg, 2019; Stewart et al., 2017). White (2015) mentioned that some industries expect and exploit millennials' constant need for gratification and rewards, as well as the tendency to rely on others. Millennials could feel entitled due to having more opportunities and achievements than prior generations, like higher education (Stewart et al., 2017). Feelings of entitlement might transfer into breaking the rules or feeling that the rules do not apply (Stewart et al.). Alternatively, entitlement could transfer into the notions of confidence, high self-esteem, and assertiveness that members of the millennial generation are known to exhibit (Smith & Nichols, 2015). Part of the entitlement mindset is the need for immediate self-gratification and expediency.

Fast food babies. Millennials are the babies of the hyper-fast food era. Using the Internet as the tool for managing many life activities perpetuates a fast-food or right now mentality of instant gratification (Fry, 2016). Gallup research written by Fleming and Adkins (2016) reported that millennials are unattached, unimpeded, unrealistic, and idealistic embodying a fast food and instant gratification mentality. Shafer (2015) stated that millennials love changes and are versatile. Millennials have many distractions, like technology, social media, employment in a harsh economy, and family (Fry, 2016). Having access to technology from an early age makes millennials attention-deficient, the potential byproduct of excessive Internet connectivity, easy access to technology, and a mindset that values convenience, productivity, ease of use, and efficiency, with limited interest in information security (Waljee et al., 2018). Personal security and data protection may only get in the way of getting things done.

In a survey conducted on approximately 2000 individuals between the age of 16-35, statistics showed that the prevailing stereotype about the millennials' generation was a relaxed

attitude with security matters (Fry, 2016). Hines (2012) noted that a reason for millennials' attention deficient nature and laziness is the fearless mindset. However, noted Hines (2012), this fearlessness can also make millennials seem very foolish, allowing millennials to own to the negative coverage noted in the literature. The group carries the label of careless Internet users, especially with social media, labeled as instinctive, inattentive, and careless (Fry, 2016; Milkman, 2017). Boehmer et al. (2015) indicated that millennials could be more prone to participate in practices that enable hacker attacks due to irresponsibility, uniformity, and laxity about cyber threats. Millennials' disregard of security mindfulness in online and home computing activities drew interest for observation due to the size of the cohort.

The largest generational group. Millennials are responsible for a significant portion of the population, designated as the largest generational group presently, well beyond the count for baby boomers (Fry, 2016). Millennials account for approximately 75 million people in 2015 (Fry, 2016; McDonald, 2015; Waljee et al., 2018). By 2020 millennials will account for one out of three Americans due to influence the economy for the next two decades and reaching their peak in 2036 (Fromm & Garton, 2013; Fry, 2016; Stewart et al., 2017).

The millennial cohort likened to an American superpower and political dynamo, are targeted for political campaigns, marketing strategies, and product creation due to the size of the group. The Obama Administration embraced the beliefs and views of America's largest, most varied generational group (Fry, 2016; White, Hewitt, & Kruck, 2013). The Democratic Party allied with millennials to take the Presidential campaign in 2008 and 2012 and strategically realigning the Party. Millennial's opinions matter, not only due to the scale of the cohort but also

because many group members seek out societal involvement. Involvement could be due to time availability or the fact that many millennials seek information and educational attainments.

Well educated. Millennials follow the baby boomer's generation, exceeding their predecessors in cohort size, educational achievements, liberalism, and confidence (Fry, 2016; Milkman, 2017). In 2014, the Pew Research Center, surveying social and demographic trends, said that historically, millennials are the best-educated generation, with 34% of the group holding at least a bachelor's degree (Fry, 2016). Waljee et al. (2018) noted that increased educational statistics could equate to better labor-market prospects and earnings. However, millennials face a stagnant workforce, and do not see the benefit of educational accomplishments due to coming-of-age in a down economy, noted Fry (2016). As a result, millennials live with parents longer than prior generations and spend excess time on social media, which may perpetuate a relaxed, IS conscious care mindset (McDonald, 2015; Milkman, 2017). The combination of being technologically immersed, well-educated, confident, and bored might give rise to risky Internet behavior (White et al., 2017).

Technologically savvy. Millennials access to digital information since grade-school is without comparison to previous generations. The group is technologically savvy and digitally immersed, believing that a connection with technology makes them exceptional and unique (Dannar, 2013; Fry, 2016; Van Schaik et al., 2018). Ninety percent of millennials stay online, whether on personal computers or mobile devices, routinizing participation on social networks, and other online communication avenues (Dannar, 2013; Fry, 2016; Van Schaik et al., 2018). However, while millennials are tech-savvy and yearn for suitability online, they hold to a relaxed security mindset with the need for convenience, navigating the Internet without fear of being a

victim of cyber-attacks, promoting a higher likelihood of cyber threat risk (Fry, 2016; Safa et al., 2015; Shafer, 2015; Waljee et al., 2018).

Millennials and information security. Millennials are a technologically aware group embracing and adopting new high-tech innovations due to early exposure with computers and the Internet, but members exhibit poor IS behaviors. The literature reports that these digital natives can be arrogant Internet users who take unnecessary cyber risks with a low rating for the security of personal data and online privacy (Alohali et al., 2018; Bada, Sasse, & Nurse, 2019; Shropshire et al., 2015; Waljee et al., 2018). The result of the behavior makes millennials the prime target for malware exploits due to sacrificing personal security (Ion et al., 2015).

Millennials have the reputation of being known as a leaky generation due to a lack of attentive security behavior on the Internet. While millennials might be relaxed concerning IS matters, this group enjoys a fast-paced working environment, taking on challenging situations, being entrepreneurs, and pushing boundaries (Stewart et al., 2017). Millennials make quick judgment calls while online and value productivity while considering gains versus losses in online decision-making (Stewart et al., 2017; Waljee et al., 2018). However, although millennials have grown up with technology and are aware of how to manage many gadgets, the group might not be knowledgeable about managing home computing and Internet security (Ion et al., 2015; Wash & Rader, 2015). Waljee et al. (2018) noted that while millennials may have a level of concern about Internet safety, they are not preoccupied with the notion of online security, or perhaps millennials just do not know enough to care about personal data security.

Millennials and malware. Millennial home PC users are the prime target for malware exploits because poor IS behaviors create opportunities for malware breaches (White, 2015). The

cohort might not feel that personal information is worthy of top-secret status, but no one wants strangers poking around and performing malicious actions with private data (Cain et al., 2018). Some poor user behaviors are sharing accounts and passwords, incorrectly storing passwords, password promiscuity, downloading software from suspect sites, and not following recommended IS guidelines (Boss et al., 2015; Crossler et al., 2017; Ion et al., 2015). White et al. (2017) mentioned that another poor user behavior typical in-home computing is multiple users sharing a single computer.

Millennial cybersecurity concepts might not be much different from the rest of the world who are now sharing information every minute. Ball, Ramim, and Levy (2015) noted that people find securing personal information and hardening home computers cumbersome and frustrating. However, 95% of malware attacks occur in the home computing environment (Cain et al., 2018). Cyber-criminals prepare for unsuspecting Internet and home PC users ignorant of malware pitfalls and make money from the situation (Cain et al., 2018). Information security research indicates that technology alone is insufficient to apply complete protection for home PCs (Anderson et al., 2016; Arachchilage et al., 2016). Therefore, user security actions must rise to combat cyber threats.

Malware

Malware has become a formidable cyber threat in today's world of hyper-technology. The literature reports the heinous impact of malware on both corporations and home PC users, inspiring an answer to the growing situation by President Obama that America must embrace the rapidly growing threat from cyber-attacks (Crossler & Belanger, 2014; Hanus & Wu, 2016; White et al., 2013). A statement from former Cyber-criminals or malicious persons deploy these

unsanctioned access attacks for any or all the following: revealing vulnerabilities, altering functionality, disabling processes, destroying code, collecting and stealing data, or making unauthorized use of access (Alohali et al., 2018). These threats, some new, dynamic, and polymorphic, and others legacy-based, have multiplied into malicious and non-malicious acts raising the need for improved personal security habits (White, 2015). In 2014, "the year the hack went viral" (Shafer, 2015, para. 3), many cyber threats to companies and government agencies let the world know that no one is safe, least of all the average Internet user. Dupuis et al. (2012) noted that in 2007, 93% of malware code design had the home PC market in mind. This percentage only intensified in the last ten years (Razak et al., 2016).

Even with surprising malware statistics, Internet and home PC users continue to take risks in online activities despite security-conscious care messages promoting the intense need for cyber-safety (Carden & Wood, 2018). Research notes that Internet users are aware of the cyber threats associated with online access but are strangely unwilling to implement safe computing practices or install antimalware software applications (Nthala & Flechais, 2018; Wash & Rader, 2015). The heightened enumeration of malware codes depicts how grossly behind ordinary Internet users are compared to industry malware trends, which leave home networks exposed and unprotected. The risk of contracting malware is so high that it is inescapable without improved cyber hygiene (Ali, Murthy, & Kohun, 2016).

Concepts surrounding IS and IS risk. Information security for home PC users involves protecting personal computers and private data from malware (Rantonen, 2014). Information security is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction (Whitman & Mattord,

2017). Internet users concerned with security countermeasures should employ both tactical, technical, and behavioral measures. An example of technical skills is installing AvSW. Behavioral measures examples are updating passwords or keeping antimalware software up to date. The literature reports that technology and behavior help prevent malware exploits and disruptions (Safa et al., 2015). Technical IS has three pillars named confidentiality, integrity, and availability, referred to as the C~I~A triad; malware exploits violate the triad (Menard, Gatlin, & Warkentin, 2014). Descriptions of the C~I~A triad guide technical perspectives in both organizations and home computing environments (Menard et al., 2014).

An explanation of information security is the process of protecting C~I~A to avoid unlawful use, destruction, or adjustment of information assets and to ensure the balance of IS hazards and controls (Whitman & Mattord, 2017). Confidentiality incorporates information availability, keeping data private, and allowing access only to the intended person. Integrity allows for data modification by those authorized to change it and affects data trustworthiness. Availability deals with all aspects of having access to information. Careless and laissez-faire behaviors threaten the C~I~A triad of information on a personal level (Safa et al., 2015).

Malware in the literature. Advanced technologies have become increasingly efficient in producing pathways to malware attacks (Razak et al., 2016; White, 2015). White (2015) mentioned that the broad availability and connectivity of the Internet make the steady advancement of web-based technologies efficient in gathering and rendering malware. Ulterior motives to change computer processing functions existed since computers and programming originated (Razak et al., 2016). Findings from the literature noted that as home computing and Internet usage rose in the last 20 years, so did adverse security behaviors. The security world

deemed 2014 the year when cyber-attacks and malware became prevalent (Lopez, 2015). Lopez (2015) reported that the year 2014 generated 34% of all malware ever created. Hackers have subsequently deployed new malware code on the Internet every five seconds (Verizon, 2019). There were 75 million malware samples in 2014, reported Lopez (2015). Razak et al. (2016) reported that 170 million malware samples existed on the Internet in 2015. Lopez stated that there are nearly 30 million new malware strains every year. Antimalware software producers must continuously update data libraries and malware detection software to counteract more than 60,000 new malware exploits created daily (Webroot, 2018). Tsai et al. (2016) reported that 90% of computers on the Internet are more susceptible to malware attacks because of conventional software prevalent on home PCs.

Having an install of AvSW on each home PC and keeping the software updated increases home network protection (White, 2015). The literature notes that the lack of protective software on home PCs is a critical liability to personal data security. Chenoweth et al. (2019) reported that Internet users who know about the significance of anti-spyware tools do not install the software. Currently, four-fifths of existing home PC environments are absent one or more security defenses against malware threats (White et al., 2017). Wash and Rader's (2015) research found that home PC users do not use available security protection software in the form of antivirus, anti-spyware, and firewall software to reduce home computing security risks. As a result, all types of malware invade home PCs threatening personal data security upon connecting to the Internet (Lopez, 2015; Van Schaik et al., 2017). The situation demands proactive IS habits to thwart continued malware attacks and malware revictimization.

Malware trends. Developments in malware show that malicious codes shifted objectives from disrupting computer software and Internet service to actively seeking financial gain from user's stolen information (Razak et al., 2016). Arachchilage et al. (2016) conveyed that 75% of phishing scams, referred to as online identity theft, endeavor to steal usernames and passwords and online details of Internet users while targeting retail services, online payment systems, and financial institutions. Malware in the form of sophisticated viruses and spyware programs now attack anything connected to the Internet and deploy every minute, making it harder to spot and remedy (Chenoweth et al., 2019; Dias, Pinto, & Cruz, 2017; Verizon, 2019; Whitman & Mattord, 2017). Malware can embed in downloaded links with origins existing in favorite and trusted sites (Dias et al., 2017). Drive-by-downloads-malware installs on a computer without waiting for the user's consent or acceptance, from merely viewing an infected website, popup window, or email message (Cain et al., 2018). By just visiting the wrong web page, PCs can become compromised.

In general, Internet and home PC users do not draw upon the community knowledge about the magnitude of adverse effects associated with malware threats (Bada et al., 2019; Chenoweth et al., 2019). Additionally, Internet and home computer users are not eager to change bad habits and behaviors to avoid potential risks and lack core-computing protections, like installing AvSW on each home PC (Martens et al., 2019).

There is a correlation between security habits and home computing precautionary measures (White, 2015; White et al., 2017). White (2015) specified that protective behaviors might reduce victimization from Internet threats. However, while antimalware software can mitigate many malware threats, proper IS behavior must accompany software installation and

maintenance. Antivirus software might not avert every threat; however, it can assist in scanning software before malware installation, and warn Internet users of potentially unwanted programs. Antivirus software is considered the first line of defense against malware.

Future technologies create additional vulnerabilities. Future technologies, like the Internet of Things (IoT), allow for interconnection through a single household network and create other vulnerabilities. The definition of the IoT is "a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies" (Loving, 2016, p. 3). It is a network of smart devices, including software, electronics, and sensors, all network capable and able to communicate and exchange data via the Internet (Belanger & Crossler, 2019; Berte, 2018; ISTR, 2019). The IoT encompasses a myriad of artificially intelligent systems with the ability to collect data. Loving (2016) predicted that IoT technology would increase dangerous malware in home computing. The Internet of things boasts enhanced high-tech experiences with intelligent systems in smart homes, medical, retail, communications, automotive, and industrial (Thompson et al., 2017). The concept of IoT has implications for new and improved malware threats and poses new and unique security challenges to home technology users (Berte, 2018; ISTR, 2019; Nthala & Flechais, 2018).

Loving (2016) reported that projections of malicious software with IoT devices that can destroy data, procure data, or incorporate computers into botnets get worse with time, especially devices relying on email. As the vast number of devices adopting the IoT increases, so will the malware associated with IoT technology, reported Loving (2016). The IoT will impose a creative disruption in the cyber world, and home PC users must be ready (Addae, Sun, Towey, &

Radenkovic, 2019; Berte, 2018). Home computer users should actively observe technology evolutions and get an upgraded mentality with smart technology, like IoT.

The Goal: Conscious Care Behavior

With connectedness should come Internet conscious care behavior. Safa et al. (2015) defined conscious care behavior as instances when home PC users process the consequences of individual actions while online and avoid risky behavior. Conscious care behavior averts or counters invasive malware attacks by promoting a stop-and-think mindset and involves thinking about online activities before putting personal data in danger (Safa et al., 2015). Anderson and Agarwal (2010) defined a conscientious cybercitizen as motivated cyber-minded individuals who take necessary precautions to direct and control the security of PCs and home security.

Technology advances, but home computer user's online habits stay the same or trail the trends in malware, yet home computer users are the prime target for cyber threats. Thus, Internet conscious care appeals and home PC protection awareness campaigns should persist as Internet technology enhances. The human factor has a great deal to do with cybersecurity, and home computer users are at the helm of Internet security responsibility. In the workplace, it is the human element, not system vulnerabilities or weaknesses that are the leading cause of severe security breaches (Vance et al., 2012). Internet ubiquity and continued use increase security threats, and these threats should force Internet users to be more conscientious about PC security practices (White, 2015). It is everyone's responsibility to be safe online.

Synthesis of the Research Findings

The Population Group

Claar and Johnson (2012) reported the difficulty in defining the home PC user group. Howe et al. (2012) mentioned that there was no clearly recognized home computer user segmentation, or there was no way to enumerate the home computer user to classify the set for research because of the immensity of the group populous. The literature records researchers who chose to survey college students recommended a more diverse grouping of individuals for future research (Claar & Johnson, 2012; Meso et al., 2013; White et al., 2017; Yoon et al., 2012). Boehmer et al.'s (2015) population group included undergraduate and graduate students. It noted the exclusion of individuals in the same age group not enrolled in a four-year college or post-graduate studies as a limitation of the research. Yoon et al. (2012) recommended the extension of research to participants of a population group other than college students. Therefore, using a group that encompassed both students and working adults born between 1980 and 2000 covered this gap. This millennial home computer user research brought together three subgroups: (a) the college student base, (b) the non-student segment, and (c) the working or professional millennial–a subset of the generational group missed in research (Debevec, Schewe, Madden, & Diamond, 2013). Informational research on the group noted the need for academic, peer-reviewed research. The use of the millennial population group assisted in the enumeration of the home computer user and designation of group sampling.

Beneficial Use of Antivirus Software

A premise of this quantitative, nonexperimental research effort surveying millennial home PC users notes that malware exploits are a significant threat that home PC and Internet

users encounter online, and AvSW is the first line of defense against this threat. However, antagonists against this view argued that AvSW is almost dead (Spafford, 2014). Advocates against AvSW as a viable option against malware noted that the software could not avert or prevent the programming of new malware initiatives.

Razak et al. (2016) suggested that new forms of malware hide from AvSW protective software, which requires constant updates. Spafford (2014) reported that AvSW vendors were unable to quickly deploy software updates in defense against the rapid accumulation of new malware. Due to the extensive and costly upkeep, AvSW vendors could only detect 45% of malware attacks (Spafford, 2014). Many AvSW vendors had difficulty with next-to-realtime updates of data libraries and relied on legacy signature-based detection to block malware (Alohali et al., 2018; Dias et al., 2017). Thus, malware vendors decided to group AvSW with other software to combat the new trends in malware.

Antimalware vendors moved from a single detect-and-respond platform to security suites covering intrusion detection, data leak monitoring, hacking tracking, and identity theft protection (McGill & Thompson, 2017; Thompson et al., 2017; Tu, Turel, Yuan, & Archer, 2015). Marketers replaced the term antivirus with descriptive words denoting a grouping of services, like Internet Security, 360 Security, and Total Security, to promote a unified approach against malware (Berte, 2018). The reinvention of AvSW revived the dying protection recourse against malware, and it remains the foundation and first line of defense in home PC security management (Rubenking, 2019).

Advocates for AvSW's continued benefits note that the software has not lost its usefulness to protect personal computers from a myriad of cyber-attacks, and note that non-

believers continuous talk about the software being defunct only fuel malware programmers' resolve to continue with malicious activities. Hameed and Arachchilage (2019) noted that AvSW is one of a few methods that home computer users employ to protect personal systems from IS threats, however both technical and non-technical solutions will efficiently safeguard systems.

Wash and Rader (2015) mentioned that users might still not know how AvSW works, and perhaps the inconvenience of managing the installation and updates might be too much for some home computer users. Spafford (2014) noted that thoughts of the demise of AvSW might stem from the lack of acceptance of appeal messages denoting the dangers of malware exploits. These notions might contribute to the success of malware. Good cyber-hygiene practices cannot maneuver around all the pitfalls that malware programmers deploy, nor can it serve as a backup to make users aware of existing malware software on a computer as AvSW can (Alohali et al., 2018; Chenoweth et al., 2019; Shropshire et al., 2015). Therefore, both good cyber hygiene practices and the implementation of AvSW present a united front against malware. The real test to verify AvSW's usefulness and viability is whether millennial end-users install the software. The evaluation of previous research methods compared two empirical studies.

Critique of the Previous Research Methods

Two empirical studies that implemented habit in the PMT framework were Vance et al.'s (2012) and Yoon et al.'s (2012) studies. Each article represented excellence in research. This millennial home PC user study followed a quantitative, nonexperimental methodology that both Vance et al. and Yoon et al. used. Vance et al.'s (2012) sample included 210 survey recipients; however, 500 employees received emails. Yoon et al.'s (2012) final survey count was 202 survey

recipients. There were 209 initial survey recipients, and seven were incomplete. Yoon et al. (2012) did not note the original count of the students from the four classes prospected.

Vance et al. (2012) used an 11-point Likert scale survey instrument for a questionnaire. However, this millennial home computer user study used a 7-point Likert scale questionnaire aligned with Yoon et al.'s (2012) research. The literature noted that 11-point Likert scales might allow for a greater spread for data with more variance and more negative kurtosis, meaning there is less peaking around the mean or flattening (Dawes, 2012). Vance et al. (2012) implemented the common method bias (CMB) test to refute Likert scale limitations and alleviate concerns of bias in the data. Table 1 denotes the research design, sampling method, sample size, research instrument, setting, and statistical procedures for both articles.

Table 1.
Research Comparison Between Vance et al. (2012) and Yoon et al. (2012)

Research Components	Vance et al. (2012)	Yoon et al. (2012)
Research Design	Quantitative, survey	Quantitative, survey
Sampling	500 emails sent out	209 volunteers
Sample Size	210 survey respondents	202 acceptable surveys
Research Instruments	Survey, Likert scale, 11-point	Survey, Likert scale, 7-point
Setting	Workplace	College Campus
Statistical Procedures	Smart PLS 2.0, Pearson's *r*, one-way ANOVA, and AVE correlation	PLS, SEM, multiple regression, one-way ANOVA, AVE correlation, and CFA

Note. The table compares research efforts by Vance et al. (2012) and Yoon et al. (2012). Both studies included habit in the contextual framework.

Vance et al.'s (2012) study included employees as the population group and used the workplace setting. On the other hand, Yoon et al. (2012) used college students for the population group, and the college campus as the setting. The population group for this nonexperimental study was the millennial generational group, which incorporated some of Yoon et al.'s (2012) and Vance et al.'s (2012) population members. Vance et al. (2012) used partial least squares (PLS), multiple regression, *p*-value, one-way analysis of variance (ANOVA), and average variance extracted (AVE) calculations for analyzing data results. Yoon et al. (2012) employed all tests in addition to structural equation modeling (SEM) and confirmatory factor analysis (CFA). This quantitative, nonexperimental study used bivariate analysis with Pearson's r testing to determine the extent that each PMT factor varied from the habit variable.

Summary

The theoretical framework used in the study was the PMT with habit as a source of information. The theory has three sections, the source of information, the cognitive mediating

process, the threat and coping appraisals, and the coping mode. There was a gap in the literature with home computer user's habituated actions and IS decision-making. Research indicated that home PC users are an integral part of Internet security, but home computer users may exhibit risky security habits. These habits are central to understanding why IS remains such a critical issue with home PC users. The lack of training, emerging technologies, and reduced technical skills contributed to faulty IS behavior with home computer users causing individual users to be the weak link in security structures. Malware persists, and millennial home computer users must correct deficient Internet practices and incorporate precautionary protective barriers that combat security threats and other malware exploits. Synthesis of the literature defused questions about the essential topics of the research. The critique of the two articles that inspired this millennial home PC user research noted the strengths of empirical studies surrounding habit in the PMT framework. Chapter 3 explains the six hypotheses statements derived from the variables of the combined contextual framework, details the research methodology, and provides procedural information that shaped the statistical analysis.

CHAPTER 3. METHODOLOGY

Chapter 1 laid the foundation for the study and reported the research problem, methodology, design, and significance of the study. Chapter 3 gives additional information covered in Chapter 1 and describes the methods and procedures used to conduct the analytical process. The structure of Chapter 3 has several components, including the purpose of the study, the research question and hypotheses statements, the research design, and the target population and participant selection. Other subjects covered in this chapter are the procedures employed to conduct the study, the instrumentation elements used to collect the data, and any ethical considerations noted for the study.

Purpose of the Study

The purpose of this quantitative, nonexperimental study is to understand why millennial Internet and home computer users do not adequately protect personal computers with available security software. There was a gap identified in the literature concerning prior IS habits and how those experiences come to bear on present-day decision-making. The literature noted that empirical studies surrounding automatized, technology-oriented IS behavior has been insufficient (Addae et al., 2019; Ball et al., 2015; Carden & Wood, 2018; Chiu & Huang, 2015; Dang-Pham et al., 2016). This millennial home PC user research effort promoted that prior IS habits might play a role with home PC users installing AvSW. The primary purpose of the study was to continue the conversation in the IS body of knowledge concerning home PC users' lack of security software. Another purpose of the study was to investigate PMT factors that had significance with habit to promote the installation of AvSW. The merged framework examined whether habit or routine behavior had significance as an antecedent in the cognitive mediating

process of the PMT. The constructs were habit - used as a dependent variable, perceived vulnerability-PV, perceived severity-PS, rewards-R, response efficacy-RE, self-efficacy-SE, and response costs-RC as independent variables. These constructs served as guides to interpreting the statistical data.

Research Questions and Hypotheses

Research Question

Is there a significant association between millennials' IS habits and protection motivation factors that indicate an intention to install antivirus software? The research question had six hypothesis statements.

Hypotheses

Hypothesis 1: There is a positive correlation between millennials' IS habits and perceived vulnerability.

- Null: There is no statistically significant correlation between millennials' habituated IS practices and perceived vulnerability.
- Alternate: There is a statistically significant, positive correlation between millennials' habituated IS practices and perceived vulnerability.

Hypothesis 2: There is a positive correlation between millennials' IS habits and perceived severity.

- Null: There is no statistically significant correlation between millennials' habituated IS practices and perceived severity.
- Alternate: There is a statistically significant, positive correlation between millennials' habituated IS practices and perceived severity.

Hypothesis 3: There is a negative correlation between millennials' IS habits and intrinsic and extrinsic rewards.

- Null: There is no statistically significant correlation between millennials' habituated IS practices and rewards.
- Alternate: There is a statistically significant, negative correlation between millennials' habituated IS practices and rewards.

Hypothesis 4: There is a positive correlation between millennials' IS habits and response efficacy.

- Null: There is no statistically significant correlation between millennials' habituated IS practices and response efficacy.
- Alternate: There is a statistically significant, positive correlation between millennials' habituated IS practices and response efficacy.

Hypothesis 5: There is a positive correlation between millennials' IS habits and self-efficacy.

- Null: There is no statistically significant correlation between millennials' habituated IS practices and self-efficacy.
- Alternate: There is a statistically significant, positive correlation between millennials' habituated IS practices and self-efficacy.

Hypothesis 6: There is a negative correlation between millennials' IS habits and response costs.

- Null: There is no statistically significant correlation between millennials' habituated IS practices and response costs.

- Alternate: There is a statistically significant, negative correlation between millennials' habituated IS practices and response costs.

Research Design

The design employed in this millennial home PC user study was a quantitative, nonexperimental design. The study utilized bivariate analysis to see correlations between the factors and thereby answer the research question. The study also incorporated multiple regression testing with the correlated variables for exploratory analysis targeted for further research. Correlational analysis has several assumptions, including linearity, homoscedasticity, multicollinearity, and normality (Field, 2009). Violation of the various assumption tests could invalidate data. The assumption of linearity states that there is a linear relationship between the dependent and independent variables. The homoscedasticity assumption states that values for the dependent and independent variables have equal variances. The assumption of multicollinearity states that there is no correlation between two or more independent variables. Normality concerns adherence to a bell-shaped curve before running statistical tests. Tests employed in the study indicated adherence to assumptions. Chapter 4 displays tests and graphs for each assumption.

Target Population and Sample

The target population and sample section cover three subtopic areas: the population, the sample, and the power analysis for the sample. The home computer user group was challenging to enumerate; however, targeting the millennial home computer user allowed for a manageable representation. The sample section describes the count of survey recipients who completed the

questionnaire and highlights the sampling strategy. The power analysis subheading tells the derivation of the sample size.

Population

The research population group is millennial home PC users. There are approximately 70 to 80 million millennials in the United States. This group has grown to be the largest generational group currently. The millennial generational group is essential because of the influence of the cohort on the current economy. Millennial attitudes, beliefs, opinions, and trending actions have relevance for the next two decades. Quantitative studies emphasize generalizability to the broader population from the sample group (Delice, 2010).

Sample

The study used a sample of 257 survey recipients to understand the millennial mindset around IS protective technologies for the broader population. Included in the sample were millennials not attending college, college students, and working adults. The literature noted studies calling for diversification in research participants (Debevec et al., 2013; Meso et al., 2013; Smith & Nichols, 2015; Yoon et al., 2012). The study assumed that millennials, whose upbringing incorporated technology from an early age, are prone to attend college, and who are a part of the diminishing digital divide era, would have a home computer. Convenience sampling was the sampling choice because of its simplicity, cost savings, and ease of use in research. From posting the survey on Facebook, asking associates to forward the survey to potential participants, and using the survey service, all were variations of convenience sampling. Truly randomized sampling was a difficult endeavor to achieve with this research effort and the option was not chosen, although convenience sampling may be prone to some level of bias.

Power Analysis

The sample size provided the scope and boundary for data collection (Creswell, 2014). The GPower software tool aided in the selection of the appropriate number of survey participants for this millennial home PC user research. This free software calculated a sample size using an A Priori test that produced an estimation of 122 minimal recipients. The ratio of participant assumption noted that there should be 20 participants to each independent variable (IV; Field, 2009). The ratio for this study was 43 participants to each of the six variables. The study has more than double the minimum number of participants. Increasing the sample size assisted with reducing multicollinearity (Field, 2009). The results provided an adequate sample size of 122 using a *p*-value of 0.05, with a significance power of 0.95, and a medium effect size *of w* = 0.3 (Faul, Erdfelder, Buchner, & Lang, 2009). With the sample size specified, procedures involving participant selection commenced.

Procedures

The procedures section describes the analytical process of the study. Sections covered are participant selection, protection for participants, data collection, and data analysis. The data analysis section includes pre-data analysis and screening, descriptive statistics, and hypothesis testing.

Participant Selection

The broader population was home PC users overall. The chosen segment of the home PC user population was the millennial generational group. The study utilized various forms of convenience sampling to gather survey recipients. The survey, placed on the social media site, invited direct millennial associates to take the survey. A request for direct associates to forward

the survey to other potential participants was part of posting the survey to the social media page. The customized online website directed recipients to take the survey and had informed consent details and response as the first question of the survey. The process of these two efforts generated 26 recipients. The procurement of a survey service occurred when initial recruitment efforts failed to produce the required participants.

The survey service procured panelists aligned with recruitment specifications, and quickly fulfilled the research need, producing panelists to take the survey within five days. While the survey service required invoicing and purchasing of the service, the process had a good return on investment regarding the time it took to gather participants and start data analysis. The total number of recipients who completed the survey was 264, of which 26 were researcher attained, leaving 238 or approximately 90% generated by the survey service. The result was 257 completed surveys validated for data analysis.

Protection for Participants

All academic research must take into consideration protection for research participants. The main concern with participant protection for this quantitative survey researched involved the treatment of extracted information (Fowler, 2009). The research plan did not require surveying protected groups, such as veterans, children, disabled persons, or prisoners, nor depended on face-to-face interaction between researcher and participant. Thus, the research proposal anticipated a less than minimal magnitude of harm rating to participants (APA, 2016; CITI Program, 2014). Less than minimal risk is research where the probability or magnitude of possible harm to participants is not greater than that which would be encountered by individuals in regular activities of daily living (APA, 2016). Informed consent information placed at the

beginning of the survey required an affirmative response. The online survey did not connect participant names to answers because the questionnaire was an anonymous survey that did not require the capture of personally identifiable information (PII). Survey data will remain secured in a password protected cloud storage for at least seven years (APA, 2016). Data analysis began immediately after getting the needed count of survey participants.

Data Collection

The survey service took care of completing the recruitment for the desired number of recipients and finalized the data collection process in five days. The 7-point Likert scale survey made data collection fast, easy, and efficient. Data extraction and analysis could then begin with importing the extracted file into the SPSS analytical tool, the student version SPSS Statistics 24.

Data Analysis

The first step to managing the raw data was to compile the results into usable data, which took place in Microsoft Excel software. Correlational analysis computation with Pearson's r was the method used for hypothesis testing. The study used seven variables to check correlations for intention to install AvSW.

Pre-data analysis and screening. Research studies require pre-data analysis and screening procedures before performing statistical evaluations. Mertler and Vannatta (2013) reported that pre-screening data is a process designed to validate and bring confidence to more in-depth research analysis and should incorporate four criteria. The four items screened for in the

pre-data analysis were data accuracy, inspection for missing data, outliers testing, and fitness of assumptions testing. The first check for data accuracy was for response set bias.

Response set. The definition of response set bias is a socially motivated mindset where respondents endeavor to be communally correct (Mertler & Vannatta, 2013). Response set bias might lead to false answers and deception due to social desirability to be polite (Baron, 1996; Nederhof, 1985). A response-set in Likert scale surveys manifests in several ways. One avenue is to choose the same scoring choice for all the survey items. Departure from genuine responses due to social mindfulness, just avoiding selecting 'no', or giving a negative answer on a survey question is another manifestation of response set bias. A final form of response set bias is choosing the same response continuously (Baron, 1996; Furnham, 1986). It is a resignation to answering survey questions, and it can affect the validity and data quality of survey research (Nederhof, 1985). Likert scales can also promote socially desirable answers (Baron, 1996; Furnham, 1986). Baron (1996) added that Likert scale survey instruments might be responsible for distorting survey responses away from exact scores, creating skewness of statistical scoring. Carefully crafting questions and using the common methods bias (CMB) test avoided response set bias.

Missing data. Pre-screening for missing data, which required replacing blank cells with the column mean, was not needed due to the nature of the study (Field, 2009). There was no missing data associated with the study due to the structure of the survey instrument on the online site. If survey participants exited the questionnaire before completion the service would discard

the incomplete entries. Out of the 264 surveys received, seven required discarding due to incomplete responses.

Outliers. Outliers are cases of extreme values at either end of the distribution curve that might misrepresent data results (Mertler & Vannatta, 2013). These cases can skew data analysis, causing a factor to be insignificant when discarding the item would indicate significance (Mertler & Vannatta, 2013). The type of variables used in the study and associated scores disallowed for numbers to go to extremes. Thus, the type of data associated with the study did not need management for outliers.

Fitness of assumptions. The fitness of assumptions pre-data analysis screening checked for linearity, homoscedasticity, normality, and multicollinearity (Mertler & Vannatta, 2013). This millennial home PC user research placed significance on the fitness of assumptions because of the use of correlational testing. The study applied the four assumptions for fitness and adherence to parametric testing requirements, linearity, homoscedasticity, normality, and multicollinearity. Tests implemented in the study adhered to assumptions.

Descriptive statistics. Summarized data with the seven study variables, habit, perceived vulnerability-PV, perceived severity-PS, rewards-R, response efficacy-RE, self-efficacy-SE, and response costs-RC directed the research outcomes. Data transformation adjustments improved data interpretability and conformed data to parametric tests (Field, 2009). Using the data transformation option - square root with reflection brought habit, PV, PS, and RE into required valuations.

Hypothesis testing. Pearson's *r* correlational testing measured the strength of the relationship between variables using the correlation coefficient and noted significance with the

value. Field (2009, p. 153) stated that the classification of a correlation is either a small, medium, or large effect size denoting the magnitude of the relationship. Effect sizes are associated with hypothesis testing, power analyses, sample size preparation, and other meta-analyses (Field, 2009). A small effect size includes values in the range of 0 to .1. A medium effect size includes values between the range of >.1 to .3. A large effect size are values >.5. Also measured in this study was the direction of the effect size, either positive or negative.

Instruments

The name of the tool utilized for data collection was the Millennials and Antivirus Software Survey Instrument. The instrument, adapted from Vance et al.'s (2012) empirically tested tool, assisted in discovering the correlation between millennials' IS automaticity and PMT factors denoting potential intention to install AvSW. The permissioned questionnaire from Vance et al. had validity and repeatability. Scenario-based questions illustrated current trends in personal IS computing threats and susceptibilities for the typical home computer user.

Millennials and Antivirus Software Survey Instrument

A panel of 16 IS personnel, approximately 10% of the identified 122 recipients needed for research validity as indicated by the power analysis, consented to take the preliminary survey in off-hours as an initial step of instrument construction. The recipients weighted the ranked, categorized content, and identified the selected scenario questions to be useful. The Millennials and Antivirus Software Survey Instrument tool is a 24-question survey instrument, with 23 items in a 7-point Likert scale format. The tool incorporated several sub-scale scores: habit, intent to comply (ITC), perceived vulnerability (PV), perceived severity (PS), response efficacy (RE), response cost (RC), rewards (R), self-efficacy (SE), and Gender (G). The contextual framework

incorporated habit as an antecedent of intention. Thus, the survey instrument included parameters to examine the millennial generation group and Internet and home PC user tendencies to glean intention results while integrating several habit-oriented scenarios. Scenario questions changed to illustrate current trends in personal IS computing threats and susceptibilities. The scenario questions presented to survey recipients were in a 7-point Likert scale format ranging from extremely unlikely to extremely likely.

Validity. Part of pre-testing included content validity and management of survey items. This millennial home PC user research established analysis soundness with validity and study repeatability to reinforce findings and ensure acceptance by the broader scientific community. Scenario question validity happened with panel testing and using the Harman Factor Analysis test checked for validity (Field, 2009). A small panel of technology professionals assisted in the confirmation of the chosen questions.

Reliability.

Reliability signifies the repeatability or consistency of the research measurement. Data results should be more than just a one-time result or finding. The Cronbach's alpha (ά) test checked for reliability. With the survey instrument tool clarified and validity and reliability reviewed, the next evaluation was ethical considerations.

Ethical Considerations

Ethical considerations for the study included protection from harm, right to privacy, access to informed consent, and other protections, like research data storage, as stated in the APA (2016) guidelines. University guidelines set by governing bodies like APA (2016) and CITI (2014) set boundaries for the research. A University's Institutional Review Board (IRB)

validates the ethical implementation of human subject research and the unviolated rights of study participants.

Protection from harm did not apply to the study due to the nonexperimental design. Sensitive groups, like veterans or prisoners, were not part of the research group. Participants had the right to privacy and received notification of the purpose of the study in the informed consent information located in the online survey. The informed consent noted that there should be no concern for potential risks, discomfort, or adverse effects, as well as other rights, responsibilities, and noted inducements for the study (APA, 2016). There was no need for deception or ruses during the data collection process due to the nonexperimental nature of the study. The research did not fabricate any research data and avoided false and misleading statements, as noted in the APA (2016) guidelines.

Summary

Chapter 3 identified the research design as a quantitative, nonexperimental design using correlational analysis with Pearson's *r*. Exploratory regression analysis for further research was the second round of testing using all variables in the analysis. Convenience sampling generated survey recipients to take the survey in various venues, however, the most useful was a paid survey service. The sample size was 257 millennial survey participants that included non-college participants, college students, and working adults. Seven variables organized data for statistical analysis using the SPSS tool, the student version. Data transformations brought data for four variables, habit, PV, PS, and RE, into required valuations. The ethics review held to a less than minimal risk rating due to the limited interaction between survey participants. The study adhered

to all ethical standards set forth by governing bodies. The next chapter discusses the study's results.

CHAPTER 4. RESULTS

Chapter 3 discussed the research question and sub-questions, research design, data collection, data analysis, and instrumentation. The chapter also explained how the research effort adhered to the ethical standards of the academic research community with APA and the IRB. Chapter 4 conveys the data analysis results along with the analytical findings in a non-evaluative manner. Hypothesis statements and the associated correlational results guided the flow of Chapter 4. Sections found in this chapter include a description of the sample, hypothesis testing including assumptions testing, a summarization of the hypothesis testing, and the end of chapter summary.

Description of the Sample

The sample group entailed the millennial generational group, which consists of non-college participants, college students, and working adults born between 1980 and 2000. The prescribed sample size from GPower analysis was 122 using a *p*-value of 0.05, with a significance power of 0.95, and a medium effect size *of w* = 0.3. The study had more than double the number of required participants. The final count of surveys for data collection was 257. Table 2 shows the mean, standard deviation, and skewness totals for each variable. The standard deviation and skewness values should be between +1 and -1.

Table 2.
Mean and Standard Deviation Descriptives With Skewness and Kurtosis Values

Variables	Mean	Std. Deviation	Skewness	Kurtosis
Habit	24.17	4.357	-1.637	2.855
PV	11.79	2.742	-1.379	1.376
PS	11.82	2.420	-1.358	1.553
R	8.02	3.577	-0.039	-0.951
RE	12.12	2.314	-1.699	3.058
SE	16.30	3.775	-0.616	-0.244
RC	13.54	4.897	-0.266	-0.703

Note. N = 257; Skewness standard error = 0.152; Kurtosis standard error = 0.303

Research Question

Is there a significant association between millennials' IS habits and protection motivation factors that indicate an intention to install antivirus software?

Pre-Data Analysis

Validity and Reliability

The two tests used for validity and reliability were CMB and Cronbach's alpha. The response set bias check uses frequencies indicating the highest variance for one extracted variable, which threshold should not be greater than 50% (Field, 2009). Scenarios with greater than 50% would indicate a problem with bias. From the analysis, the highest value was 32%. The test result indicated that the instrument was valid and within parameters. The Cronbach's alpha evaluation is a measure of internal consistency; it is not a statistical test but a coefficient of

reliability. The Cronbach's alpha result was .725, an acceptable range above the .70 threshold for a reliability check (Field, 2009).

Assumptions Analysis

Tests in SPSS indicated skewness with the data. Data transformation using square root and reflection arithmetic resulted in negative skewness values, as seen in Table 3, into an acceptable range to avoid violation of parametric test assumptions. Linearity, homoscedasticity, and normality tests adhered to the fitness of assumptions after data transformation. See Figures 4, 5, and 6, respectively. Multicollinearity tests adhered to the assumption without data transformation, as seen in Tables 4 and 5.

Table 3.
Data Skewness Values Before and After Data Transformation

Variables	Before	After
Habit	-1.125	.490
PV	-1.167	.733
PS	-1.009	.516
R	-.098	Keep
RE	-1.242	.719
SE	-.363	Keep
RC	-.324	Keep

Note. The data showed skewness for all variables. Three variables, R, SE, and RC were within the -1 standard deviation parameter and did not need transformation. However, PV, PS, and RE were below -1 threshold. Using the square root data transformation option with reflection brought variables into a positive value with a standard deviation of less than 1.

Linearity.

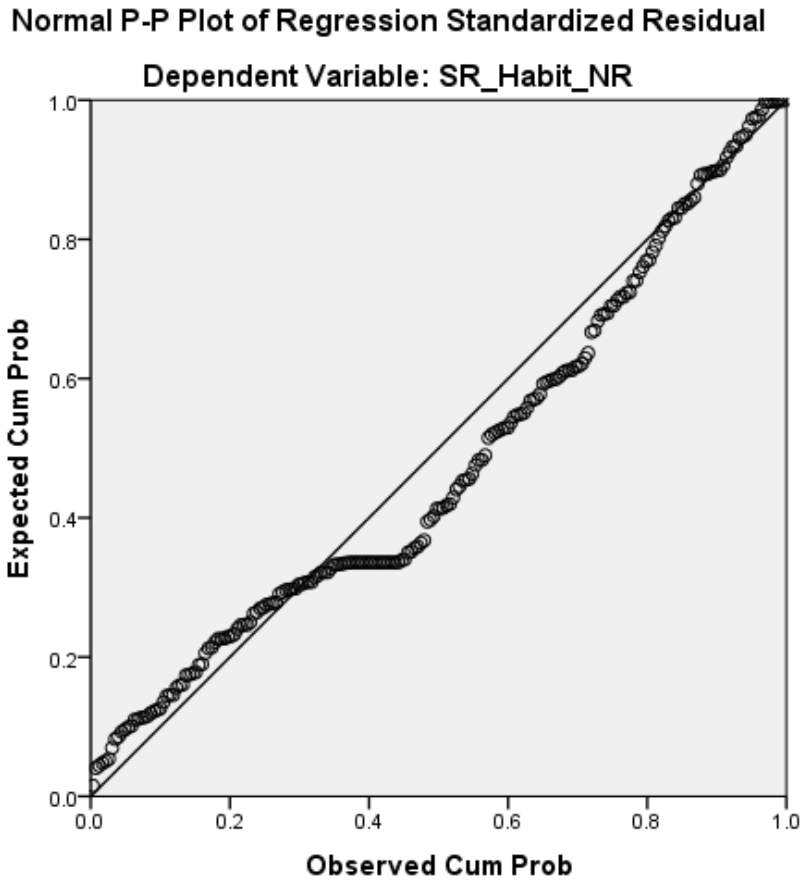

Figure 4. Linearity assumption confirmation.
The linear test displayed a graph with the values about the line.

Homoscedasticity.

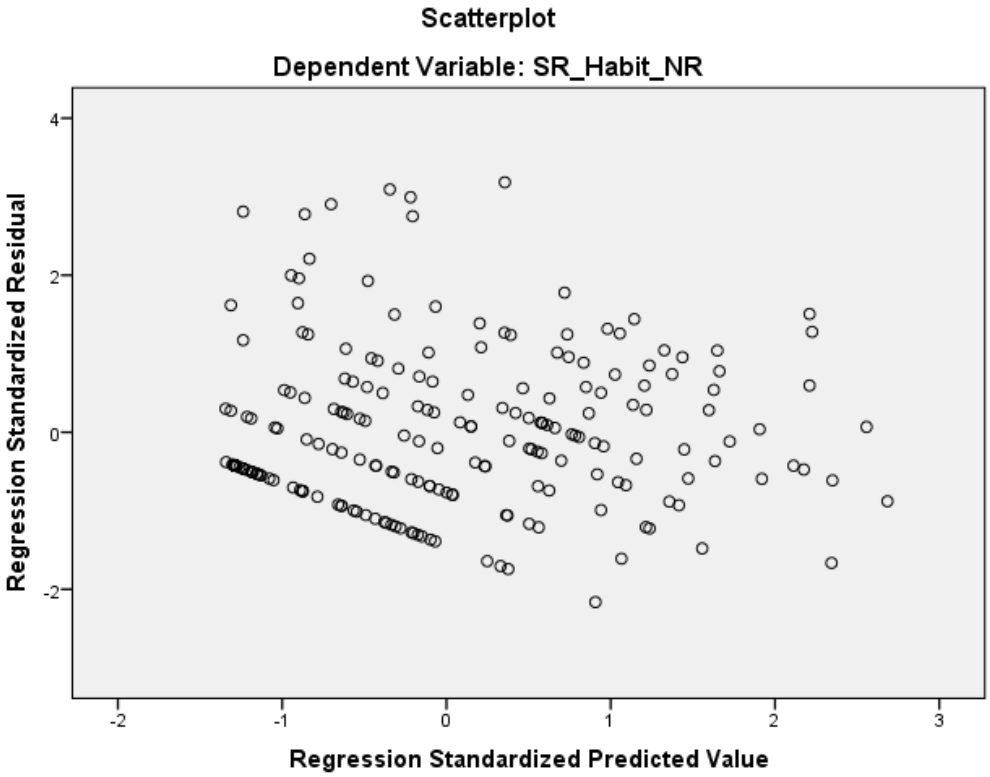

Figure 5. Homoscedasticity assumption confirmation.
Plot indicators for the homoscedasticity analysis showed a scattering of the values confirming homoscedasticity.

Multicollinearity.

Table 4.
Multicollinearity Assumption Test - Collinearity Variance Proportions

R	SE	RC	SR_PV_NR	SR_PS_NR	SR_RE_NR
0.00	0.00	0.00	0.00	0.00	0.00
0.08	0.00	0.03	0.06	0.02	0.02
0.09	0.12	0.02	0.00	0.01	0.03
0.08	0.00	0.02	**0.72**	0.03	0.25
0.07	0.00	0.10	0.04	**0.74**	**0.49**
0.67	0.01	**0.80**	0.17	0.19	0.00
0.00	**0.86**	0.01	0.01	0.01	0.21

Each variable set should have one high number, and all the others should be lower numbers. The bold text indicates high numbers.

Table 5.
Multicollinearity Statistics

Variables	Tolerance	VIF
R	0.405	2.469
SE	0.705	1.418
RC	0.396	2.525
SR_PV_NR	0.559	1.790
SR_PS_NR	0.432	2.313
SR_RE_NR	0.440	2.273

The collinearity statistics tolerance should not be greater than .09. No variables were above this threshold, which confirms the collinearity assumption using either the transformed variables or the primary variables.

Normality.

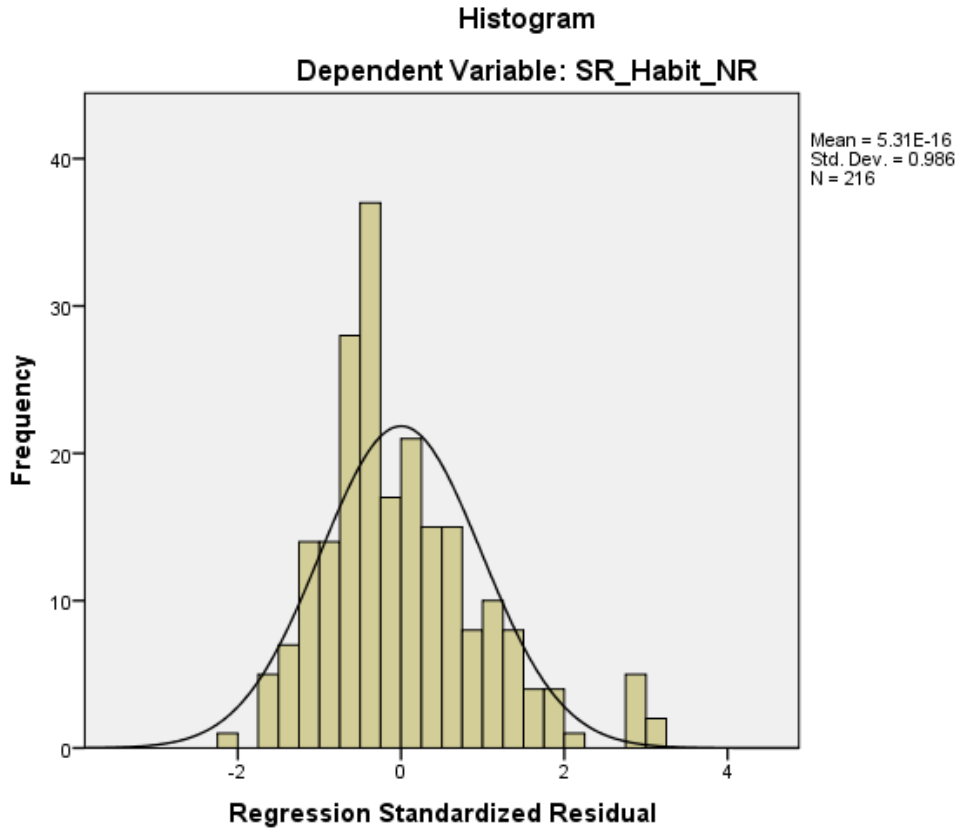

Figure 6. Normal distribution assumption confirmation.
The normality of the grouped variables shows a better bell-shaped curve; however, outliers extend beyond one standard deviation from 0.

Hypotheses Testing

Correlational testing using Pearson's *r* calculation for bivariate analysis showed the relationship between variables. The *p*-value expressed the probability that the correlation was due to chance. Any *p*-values equal to or less than .05 indicated that the result was not due to chance. The analysis reported the correlation coefficient (*r*) and associated significance.

Hypotheses

Hypothesis 1: There is a positive correlation between millennials' IS habits and perceived vulnerability.

- Null: There is no statistically significant correlation between millennials' habituated IS practices and perceived vulnerability.
- Alternate: There is a statistically significant, positive correlation between millennials' habituated IS practices and perceived vulnerability.

There was a positive, medium correlation coefficient effect between habit and PV, $r = 0.43$, $p < .001$. Hypothesis 1 was confirmed with rejection of the null hypothesis.

Hypothesis 2: There is a positive correlation between millennials' IS habits and perceived severity.

- Null: There is no statistically significant correlation between millennials' habituated IS practices and perceived severity.
- Alternate: There is a statistically significant, positive correlation between millennials' habituated IS practices and perceived severity.

There was a positive, large correlation coefficient effect between habit and PS with significance, $r = 0.597$, $p < .001$. Hypothesis 2 was confirmed with rejection of the null hypothesis.

Hypothesis 3: There is a negative correlation between millennials' IS habits and intrinsic and extrinsic rewards.

- Null: There is no statistically significant correlation between millennials' habituated IS practices and rewards.

- Alternate: There is a statistically significant, negative correlation between millennials' habituated IS practices and rewards.

There was a positive, low correlation coefficient effect between habit and R with no significance, $r = 0.11$, $p = 0.084$. Hypothesis 3 was disconfirmed with a failure to reject the null hypothesis.

Hypothesis 4: There is a positive correlation between millennials' IS habits and response efficacy.

- Null: There is no statistically significant correlation between millennials' habituated IS practices and response efficacy.
- Alternate: There is a statistically significant, positive correlation between millennials' habituated IS practices and response efficacy.

There was a positive, large correlation coefficient effect between habit and RE with significance $r = 0.654$, $p < .001$. Hypothesis 4 was confirmed with rejection of the null hypothesis.

Hypothesis 5: There is a positive correlation between millennials' IS habits and self-efficacy.

- Null: There is no statistically significant correlation between millennials' habituated IS practices and self-efficacy.
- Alternate: There is a statistically significant, positive correlation between millennials' habituated IS practices and self-efficacy.

There was a positive, large correlation coefficient effect between habit and SE with significance, $r = 0.513$, $p < .001$. Hypothesis 5 was confirmed with rejection of the null hypothesis.

Hypothesis 6: There is a negative correlation between millennials' IS habits and response costs.

- Null: There is no statistically significant correlation between millennials' habituated IS practices and response costs.
- Alternate: There is a statistically significant, negative correlation between millennials' habituated IS practices and response costs.

There was a positive, low correlation coefficient effect between habit and RC with no significance, $r = 0.046$, $p = 0.458$. Hypothesis 6 was disconfirmed with a failure to reject the null hypothesis. Table 6 shows the correlational values for the PMT variables.

Table 6.
Habit Correlations (N = 257)

Correlation	PV	PS	R	RE	SE	RC
Habit	.43*	.59*	0.11	.65*	.51*	0.05

* $p < .001$.

The correlational analysis indicated that PV, PS, RE, and SE were variables with significant relationships to habit. After performing a regression analysis test with the correlated variables as an exploratory tool, results indicated that the relationship between both PS and SE could explain 43.8% of the variance. Also, singularly, PS could explain 35% of the variance with the habit variable, as seen in Table 7.

Table 7.
Regression Analysis Results for Habit and Relationship Variables

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Sig. F Change	Durbin-Watson
PS	0.597	0.356	0.353	3.503	0.000	
PS and SE	0.665	0.442	0.438	3.267	0.000	1.840

* $p < .001$.

Summary of the Hypotheses Testing

The bivariate correlation analysis with habit and intention variables indicated a positive correlation between habit and PV, PS, RE, and SE. Given prior empirical studies and expected outcomes for each variable, PV, PS, RE, and SE variables resulted as predicted. The variables R and RC were not significantly correlated.

Table 8.
Pearson's r, Significance, and Hypothesis Results for Each Variable

Variables	*r* value	*s* value	Results	Correlation Effect Size
PV	$r = 0.431$	$s = 0.000$	Reject the null	Medium
PS	$r = 0.597$	$s = 0.000$	Reject the null	Large
R	$r = 0.108$	$s = 0.084$	Failed to reject the null	Medium
RE	$r = 0.654$	$s = 0.000$	Reject the null	Large
SE	$r = 0.513$	$s = 0.000$	Reject the null	Large
RC	$r = 0.046$	$s = 0.000$	Failed to reject the null	Small

Note. The table shows the Pearson's *r* correlation coefficient, significance, and hypothesis values for each variable.

Multiple regression analysis performed for future exploratory research indicated that two variables out of six, PS and SE, could explain the most variance with habit. These two variables

accounted for 43.8% of the variance with the habit variable. Singularly, PS could explain 35% of the variance.

Summary

The statistical analysis for habit indicated significant positive correlations with PV, PS, RE, and SE. However, there was no significant correlation between habit and R, and habit and RC. Exploratory regression analysis for the PMT predictor variables indicated that PS and SE should be areas for additional research.

CHAPTER 5. DISCUSSION, IMPLICATIONS & RECOMMENDATIONS

Chapter 5 represents the culmination of the research and notes statistical inferences derived from the data analysis. Understanding the potential application of the study's results within the IS body of knowledge and to the broader audience, given the empirical research in the literature, is the purpose of Chapter 5. This millennial home PC user research effort addressed the gap identified in the literature concerning previous IS behaviors as antecedents of protection motivation factors to invoke the recommended action of installing AvSW. Highlighting the IS attitudes and experiences of millennial home PC and Internet users was key to understanding why there may be resistance to secure home PCs from malware and other cybersecurity threats. The chapter presents the results for the research question and compares results to similar empirical research. Sections found in this chapter are the summary, discussion, and conclusions formed from the study's results. The chapter also covers a post-research review of the limitations of the study, implications to practice for practitioners, and recommendations for further research on the subject. The conclusion completes the chapter and the research effort.

Summary of the Results

The summary of the results section covers a restatement of the research question, hypothesis statements, and the theoretical basis of the study. Methodological and testing strategy summarization revives the reader's understanding concerning the nonexperimental nature of the study. Restating the study's findings recaps the results of each test.

Restatement of the Research Question

The research question stated: Is there a significant association between millennials' IS habits and protection motivation factors that indicate an intention to install antivirus software?

Six hypotheses statements made predictions for the outcome of each PMT factor. The variables for the study were perceived vulnerability-PV, perceived severity-PS, rewards-R, response efficacy-RE, self-efficacy-SE, and response costs-RC.

Hypotheses

Hypothesis 1: There is a positive correlation between millennials' IS habits and perceived vulnerability.

- Null: There is no statistically significant correlation between millennials' habituated IS practices and perceived vulnerability.
- Alternate: There is a statistically significant, positive correlation between millennials' habituated IS practices and perceived vulnerability.

There was a positive, medium correlation coefficient effect between habit and PV with significance, $r = 0.431$, and $s = 0.000$. As a result, there was a rejection of the null hypothesis for PV.

Hypothesis 2: There is a positive correlation between millennials' IS habits and perceived severity.

- Null: There is no statistically significant correlation between millennials' habituated IS practices and perceived severity.
- Alternate: There is a statistically significant, positive correlation between millennials' habituated IS practices and perceived severity.

There was a positive, large correlation coefficient effect between habit and PS with significance, $r = 0.597$, and $s = 0.000$. As a result, there was a rejection of the null hypothesis for PS.

Hypothesis 3: There is a negative correlation between millennials' IS habits and intrinsic and extrinsic rewards.

- Null: There is no statistically significant correlation between millennials' habituated IS practices and rewards.
- Alternate: There is a statistically significant, negative correlation between millennials' habituated IS practices and rewards.

There was a positive, low correlation coefficient effect size between habit and R with no significance, $r = 0.11$, and $s = 0.084$. Therefore, there was a failure to reject the null for R.

Hypothesis 4: There is a positive correlation between millennials' IS habits and response efficacy.

- Null: There is no statistically significant correlation between millennials' habituated IS practices and response efficacy.
- Alternate: There is a statistically significant, positive correlation between millennials' habituated IS practices and response efficacy.

There was a positive, large correlation coefficient effect between habit and RE with significance $r = 0.654$, and $s = 0.000$. As a result, there was a rejection of the null hypothesis for RE.

Hypothesis 5: There is a positive correlation between millennials' IS habits and self-efficacy.

- Null: There is no statistically significant correlation between millennials' habituated IS practices and self-efficacy.
- Alternate: There is a statistically significant, positive correlation between millennials' habituated IS practices and self-efficacy.

There was a positive, large correlation coefficient effect between habit and SE with significance, $r = 0.513$, and $s = 0.000$. As a result, there was a rejection of the null for SE.

Hypothesis 6: There is a negative correlation between millennials' IS habits and response costs.

- Null: There is no statistically significant correlation between millennials' habituated IS practices and response costs.
- Alternate: There is a statistically significant, negative correlation between millennials' habituated IS practices and response costs.

There was a positive, low correlation coefficient effect size between habit and RC with no significance, $r = 0.046$, and $s = 0.458$. Therefore, there was a failure to reject the null for RC.

Theoretical Understanding

The theoretical framework employed was a merged habit and protection motivation framework. Due to the nature of habit and its reinforcements, actions become repetitive and routine. Kurz et al. (2015) stated that past experiences and interactions with precautionary IS measures are the best predictors of future behavioral intentions and acceptance of the recommended action. With the idea of prior experiences coming to bear on PMT factors, a premise of this quantitative research effort was the supposition that habituated actions affected decision-making towards behavioral intention. The cognitive mediating process, comprised of threat and coping appraisal factors, signified mechanisms for evaluating maladaptive (negative) and adaptive (positive) responses to the recommended action. The PMT framework, with habit as a source of information, categorized millennials' maladaptive or adaptive responses giving insight into potential acceptance of the recommended action. From empirical studies with PMT

predictors, PV, PS, RE, and SE should have a positive effect on intention with significance, with R and RC having a negative effect. The findings supported expected outcomes for PV, PS, RE, and SE which had a positive effect on intention with significance; however, R and RC had a negative effect with no significance and were thus undetermined in this study.

Methodology and Testing Strategy

A quantitative, nonexperimental design delivered with a Likert scale 7-point survey used 257 participants to evaluate millennial's intention to install and maintain AvSW. Pearson's *r* bivariate correlational test analyzed the relationship between habit and PMT factors. A summarized recap of the findings delineated in Chapter 4 prefaces the discussion of results and provides a premise for the conclusions, implications to practice, and recommendations for further research.

Recap of Study Findings

The correlational analysis between habit and intention variables indicated that there was a relationship between PV, PS, RE, and SE. These variables resulted in a rejection of the null hypothesis. The variables R and RC did not have significance and had a positive correlation, thus failing to reject the null for these variables. Empirical tests for PMT indicate that R and RC should have a negative relationship, but instead had a positive result. Regression analysis with the PMT variables, analyzed for exploratory purposes for future directional research, indicated that two variables, PS and SE, could explain 43.8% of the variance with habit. Perceived severity could singularly explain 35% of the variance. Additional research using these variables could expound on millennials' perception of cyber severities and self-confidence in implementing security tasks.

Discussion of the Results

The threat appraisal factors, PV and PS, are grouped under the term perceived risk, and the coping appraisal factors, RE and SE, are grouped under the term risk coping for assessment and discussion purposes (Chenoweth et al., 2019). Chenoweth et al. (2019) found that when risk coping was low, perceived risk did not inspire an adaptive coping response, promoting an increase in adopting the maladaptive option instead. The remaining variables, R and RC, are grouped under the concept of maladaptive response.

Perceived Risk – PV and PS Discussion

Perceived vulnerability is a home computer user's conviction that a cyber threat will occur, and perceived severity encapsulates measurements of the seriousness of cyber threats. Ideas of heightened, perceived risks can bring about a change in behavior, noted Workman et al. (2008). The perceived risk variables increased the likelihood of installing the recommended action, stemming from previous encounters with security breaches (Thompson et al., 2017). The PMT posits that individuals are motivated to enact the recommended actions when the probability of perceived risk was in the medium to large correlation coefficient range. The higher the risk, the more individuals were encouraged to take preventative security measures. In this study, there was a positive, medium correlation coefficient between habit and PV, and a large correlation coefficient with habit and PS. The result could mean that millennials understand the vulnerabilities that they can encounter on the Internet with an excellent understanding of the likely impact of these pitfalls.

Risk Coping – RE and SE Discussion

An individual's idea about the assessment and efficacy of taking the recommended action and the aptitude to fulfill the act summarizes the coping appraisal or risk coping concept. There was a positive, large correlation coefficient effect size between habit and RE to implement the recommended action, which suggested that millennials were confident with installing AvSW for PC threat protection. Future research could test receptiveness to security software suites that can detect and respond to malware in a myriad of ways (Crossler & Belanger, 2014). Strategies that can be used together as an allied approach to manage home PC network and Internet practices, like intrusion detection, data leaks monitoring, tracking hacks, and prevention of further repercussions, might affirm millennials' assurance with RE (Rubenking, 2019).

Self-efficacy is a millennial's confidence in the ability to install and maintain AvSW. There was a large, positive correlation coefficient for SE and habit with significance. Boehmer et al. (2015) reported that SE was an essential predictor of intention to enact security measures. Further, Boehmer et al. (2015) reported that a survey participant with low levels of coping self-efficacy presented with a maladaptive response to situations requiring choosing the recommended action. Information security awareness practitioners should endeavor to encourage SE support with campaign efforts that create and maintain high SE levels via a progressive mastery of safety skills (Boehmer et al., 2015). The risk coping result in the study was a large correlation coefficient value. Using Chenoweth et al.'s (2019) findings as a benchmark, the result should inspire high levels of perceived risk and the adoption of the adaptive coping response.

Maladaptive Responses – R and RC Discussion

The maladaptive variables R and RC are undesired behaviors that serve to discount the danger and to decrease the fear response posed by a cyber threat (Boss et al., 2015). Maladaptive responses occur when the rewards or costs of instituting safety measures exceed the incentives or benefits of avoiding the potential threat. Protection motivation theory literature states that when an individual perceives that the IS costs of implementing the recommended action are high, the likelihood is low that the preventative IS action will be adopted (Mills & Sahi, 2019).

Survey participants stated that installing AvSW could disrupt routine work on home computers and could take time away from completing tasks online and performing routine Internet and home computing tasks. The results for R and RC seemed to drive reinforcement of the probability to perform the recommended action, unbalancing the contextual framework process (Rogers, 1983). From the results, respondents potentially felt that although costs associated with installing AvSW might be irritating, expensive, or inconvenient, they would continue to maintain belief in the adaptive action of installing AvSW.

There was no statistically significant correlation between millennials' habituated IS practices and R and RC. Studies have reported varying results and inconsistency with R and RC and noted that disparities might be due to the interpretation of cost valuation in terms of time and money (Crossler et al., 2017; Mills & Sahi, 2019; Yoon & Kim, 2013). Yoon et al. (2012) removed the rewards variable from the framework entirely, and Yoon and Kim (2013) removed R and RC due to inconsistency with other studies. Thompson et al. (2017) merged R and RC into one item due to the similarities between the variables. Further research to understand millennial's cost perceptions for implementing security software is a way forward.

Conclusions Based on the Results

Bivariate testing confirmed a relationship between habit and PV, PS, RE, and SE. Divergence from empirical studies occurred with R and RC. Regression analysis testing could give insight into the correlations between habit and PMT variables for the intention to install AvSW. Millennials understand that they are vulnerable to malware ploys and that these traps are severe with consequences that breach privacy and corrupt data and computers. The study diminished notions that millennials have a mindset of invincibility and overconfidence.

Costs did not significantly impact millennials, given the outcome of R and RC in the study. The low value placed on costs could be because expenses do not hamper millennials due to living with parents for a longer period than their generational predecessors. The study also indicated a discrepancy with the notion of short attention spans, showing a potentially different side that millennials would take the time out to install AvSW and not be hindered by time constraints and the compulsion to complete online activities. For this study, growing up with technology and being tech-savvy worked toward millennial's privacy and data security tendencies, indicating that the group does care about their presence online and digital information.

Comparison of the Findings With the Theoretical Framework and Previous Literature

Home computer user research seeks to uncover avenues to motivate individuals to engage in more secure IS behaviors. The bivariate results indicated additional research with the PMT factors. Further research could provide a better understanding of millennial home users' IS habituated actions with the intention to manage personal security.

Interpretation of the Findings

The statistical analysis noted relationships with some variables. However, due to the nature of correlational studies, extensive inferences could not be made from the findings. The research outcomes created opportunities for additional research to delve deeper into correlational findings. Results indicated relationships between habituated IS tendencies and PS, PV, RE, and SE that could potentially translate into the intention to install AvSW. Perceived severity and self-efficacy were statistically significant; exploratory regression analysis indicated that these two variables accounted for a high percentage of model variance. Focusing on either PS or SE could be a way to understand the extent of perceived severity of IS threats and the confidence to complete IS software installations for security protection.

Reasoning for test outcomes. Study limitations may account for divergence with R and RC, such as using a survey service. A different setting for procuring recipients might bring about other results in future research. The use of a survey service might present contingencies because users may not have a vested interest in the study. This millennial home computer user research was a correlational study that might benefit from enhanced questions on habits inspired by tools like the Self-Report Habit Index (Gardner, Abraham, Lally, & de Bruijn, 2012). This tool gives in-depth questions and opportunities for more insightful answers. Another noted dilemma in research is the need to supplement Likert scale surveys with face-to-face interviews. This design enhancement can incorporate questions that further promote additional dialog to give insight into participant's responses (Andres, 2012). Open-ended questions might allow respondents better recall and provide answers in greater detail.

Was the research question answered? The purpose of this quantitative, nonexperimental design study was to understand if millennial home PC users' previous IS habituated actions influenced decision-making and affected the intention to install precautionary security software. The research question stated: Is there a significant association between millennial's IS habits and protection motivation factors that indicate an intention to install antivirus software? The analysis noted correlations between several variables, PV, PS, RE, and SE; the correlations indicated that prior experiences, signified with the habit variable, could influence IS decision-making to secure personal devices. While correlation does not equate to causation, the research is reassuring and inspires additional empirical research directed towards all PMT variables.

Limitations

Limitations of the study may have an impact on the results of this millennial home PC user research. The limitations mentioned in Chapter 1 were participants' truthfulness, limited bias, data gathering, and generalizability to the larger population given sample size, paid panelists, and Likert scale use. The truthfulness or integrity of research participants was a limitation mitigated by explicitly asking participants about being part of the millennial generation group. It was an expectation that survey participants were honest. There was no bias due to the non-interactive nature of the study, which did not require face-to-face interaction between researcher and participant. The common method bias test assisted in calculating potential partiality in the research and indicated results within parameters. Another limitation that affected the generalizability of the study was the choice of convenience sampling. Convenience sampling was a limitation that could be remedied with simple random sampling, a

probability sampling option. Probability sampling is a straightforward and easy to understand sampling method that removes bias from the sample, but may be difficult to implement.

Procuring a paid survey service to generate survey recipients could be a study limitation. The inclusion of a survey service produced additional participants after first line recruiting methods failed. The constraint potentially transferred to the results due to the answers given by the participants being possibly insincere. As a recommendation for future studies, researchers should engage other research participants besides paid panelists. The final unmitigated limitation was Likert scale survey use.

Likert scale survey use might produce some limitations and biases. There might be additional opinions that the Likert scale format cannot address, for example, participant's intensity, remembrance, and frame of mind while taking the survey. A mixed methods approach to surveying research participants is mitigation for Likert scale use. The use of both a Likert scale and qualitative, open-ended question and answer sessions might provide a better understanding of the reason behind Likert scale responses.

Implications for Practice

There are several implications for practice from the study. Research on the habit-to-intention phenomenon concerning millennials IS mindset could generate better precautionary decision-making in home computing, create awareness about Internet security, and inspire safe Internet habits. Another implication for practice is research concerning security software costs and rewards that can serve to enhance communications to millennials, due to the notion that costs may not be a hindrance to this group. Millennial home computer users might have far-reaching power with Internet security due to the size of the group. Keeping SE levels high by promoting

confidence in managing security software implementation could influence Internet security (Furnell, Khern-am-nuai, Esmael, Yang, & Li, 2018; He, Yuan, & Tian, 2014; Rhee, Kim, & Ryu, 2009). More research with PS and SE could highlight other angles of these variables, given their strength with this millennial home PC user research.

Recommendations for Further Research

Four topics encompass recommendations for further research

- Recommendations developed directly from the data,
- Recommendations derived from methodological, research design, or other limitations of the study,
- Recommendations based on delimitations, and
- Recommendations to investigate issues not supported by the data but relevant to the research problem.

Recommendations developed directly from the data include suggestions for further research with millennials and PMT factors, given the statistical results. For recommendations from methodological research, using a mixed method approach to survey research surfaced. Applying a dual approach to inquiry can give insight into the 'why' associated with responses, understand different perspectives, and provide additional clarity. Also, using a more intense questionnaire tool like the Self-Report Habit Index and the use of other than paid panelists are two other suggestions concerning methodological recommendations.

For recommendations based on delimitations, which covers areas of research intentionally left out of the study, mobile technologies surfaced as a viable next step in habit-to-intention research. Also, looking ahead, mobile devices and the IoT - an effort to bring

everything online like, cars, TVs, medical devices, and more, will continue to increase mobile threats. Additional research to address this gap is recommended. For recommendations to investigate issues not supported by the data but relevant to the habit-to-intention problem, observing habit oriented IS disorders and new disorders that arise with excessive technology use, like the new iDisorder, arose (Bayer & LaRose, 2018). The identification of habit-oriented disorders might affect other research areas like neuroscience (Anderson et al., 2016; Mai, Parsons, Prybutok, & Namuduri, 2017). The following sections give an in-depth explanation of recommendations developed directly from the data and recommendations based on delimitations in the study.

Recommendations Developed Directly From the Data

Recommendations for further research derived directly from the statistical results included additional research with PS and SE. The two variables, PS and SE, had a large correlation coefficient effect size and could explain 43.8% of the variance with the habit variable, with PS accounting for 35% singularly. The results for R and RC were undetermined in this millennial home computer research. Maladaptive responses take place when the rewards or costs of instituting safety measures exceed the incentives or benefits of avoiding the potential threat. There is a need for additional research to answer whether millennials' restriction of time influenced IS decision-making to install AvSW. Another question for further research is, do nominal fees hamper millennials from implementing AvSW? The overarching question, however, was how vital is R and RC in the PMT contextual framework?

Another area for research diversification indicated directly from the data gathering is implementation of another sampling choice. Using probability instead of non-probability

sampling, which the study used convenience sampling, is a way to reduce bias in the study and promote generalizability. Convenience sampling may be prone to some level of bias. Truly randomized sampling was a difficult endeavor to achieve with this research effort and the option was not chosen.

Recommendations Based on Delimitations

Due to mobile technology's exclusion from this home PC user study, there is a recommendation for further research to understand how habituated tendencies manifest with mobile technology use. McGill and Thompson's (2017) study noted that participant's security mindset and self-efficacy were lower with mobile devices than with the operation of PCs and that an increase of threats exposes mobile technology research as a gap in the IS body of knowledge. Also, there is a need for research on mobile device security due to cell phones undertaking many home PC functions (Alsaleh, Alomar, & Alarifi, 2017; Belanger & Crossler, 2019; Tu, Adkins, & Zhao, 2019; Wolf, Kuber, & Aviv, 2018). Wolf et al. (2018) noted that mobile user participants reported information and data security concerns due to mistrust in associated technologies and other situational risks. Symantec's ISTR (2019) communicated that mobile devices and the IoT are areas for additional research. Understanding mobile technology security and the associated habituated tendencies with mobile devices will address the emerging gap in the literature.

Summary

The chapter covered a recap of the study's findings and discussed the outcomes related to prior empirical discoveries generating conclusions based on the results. The interpretation of the study findings noted that PV, PS, RE, and SE adhered to predicted outcomes for the PMT but

diverged with R and RC. The study's limitations also drove additional research in procuring other than paid panelists for the sample group and employing a mixed methods approach. Implications for practice for researchers could include research with all factors of the PMT, especially PS and SE, as noted by exploratory research, and R and RC since the two variables diverged from expected outcomes. Recommendations for future research covered PS and SE research, along with investigations on mobile technology, habit formation, habit transformation, and mobile device disorders.

Conclusion

The exponential growth of Internet-enabled technologies has exposed home computer users to endless cyber threats. From the comfort of a personal domicile, Internet and home PC users can shop, bank, trade stocks, socialize and communicate with friends and family, do homework, research facts, work, date or match-make, and enjoy entertainment. However, while accepting these indispensable opportunities, Internet and home PC users interact on a dangerous platform fraught with malware, cyber threats, and other cyber-pitfalls. Most homes have at least one computer in the 21st-century American home. However, four-fifths of home computers lacked one or more security safeguards against malware in 2017.

Millennials impact all aspects of the economy, politics, and marketing campaigns due to the size of the group and their need for involvement. The study observed millennial home computer users to understand mindsets around protective security software and observe the impressions that prior IS habits had on the intention to install AvSW. The research question was: Is there a significant association between millennial's IS habits and protection motivation factors

that indicate an intention to install antivirus software? Six subquestions, driven by the habit and PMT variables, produced hypotheses for the study.

The research analysis noted relationships with significance between previous IS habituated experiences and PV, PS, RE, and SE. There was a positive Pearson's *r* valuation for PV, PS, RE, and SE, with a large correlation effect size for PS, RE, and SE. The research results indicated that due to the large effect size of risk coping variables, RE and SE, and the medium to high effect size of the perceived risk variables, there should be inspiration to adopt the recommended action. The Pearson's *r* valuation for R and RC were not significant predictors of behavior associated with automaticity as an antecedent; the results were inconclusive.

It was unspecified whether millennials would be willing to give up extrinsic and intrinsic rewards and adopt the recommended action. It was also unspecified if the costs associated with installing AvSW hampered millennial's potential implementation of AvSW. Additional research could add value to understand millennial's causation in relationship with R and RC, or whether there is a need to manipulate R and RC in the PMT framework. Implications for practice for researchers were exploring millennial home computer user habituated actions with emerging technology. Recommendations for future research indicated viable paths for developing the IS body of knowledge through research covering a mixed methods approach for observation, mobile technology, and habit research, including habit formation with IS habituated disorders and habit transformation.

REFERENCES

Aarts, H., & Dijksterhuis, A. P. (2000). The automatic activation of goal-directed behaviour: The case of travel habit. *Journal of Environmental Psychology*, *20*, 75-82. doi:10.1006/jevp.1999.0156

Addae, J. H., Sun, X., Towey, D., & Radenkovic, M. (2019). Exploring user behavioral data for adaptive cybersecurity. *User Modeling and User-Adapted Interaction*, 1-50. doi:10.1007/s11257-019-09236-5

Ali, A., Murthy, R., & Kohun, F. (2016). Recovering from the nightmare of ransomware – How savvy users get hit with viruses and malware: A personal case study. *Issues in Information Systems, 17*, 58-69. Retrieved from http://www.iacis.org

Alohali, M., Clarke, N., Li, F., & Furnell, S. (2018). Identifying and predicting the factors affecting end-users' risk-taking behavior. *Information & Computer Security*, *26*, 306-326. doi:10.1108/ICS-03-2018-0037

Alreck, P. L., & Settle, R. B. (1995). *The survey research handbook: Guidelines and strategies for conducting a survey* (2nd ed.). Chicago, IL: McGraw-Hill.

Alsaleh, M., Alomar, N., & Alarifi, A. (2017). Smartphone users: Understanding how security mechanisms are perceived and new persuasive methods. *PloS One*, *12*, 1-35. doi:10.1109/COMST.2017.2651741

American Psychological Association. (2016). Ethical principles of psychologists and code of conduct. *American Psychologist, 57,* 1060-1073. doi:10.1037/0003-066X.57.12.1060

Anderson, B., Vance, A., Kirwan, C. B., Eargle, D., & Jenkins, J. L. (2016). How users perceive and respond to security messages: A neuroIS research agenda and empirical study. *European Journal of Information Systems*, *25*, 364–390. doi:10.1057/ejis.2015.21

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly*, *34*, 613–643. doi:10.2307/25750694

Andres, L. (2012). *Designing & doing survey research.* London, UK: SAGE. doi:10.4135/9781526402202

Antonius, R. (2003). *Interpreting quantitative data with SPSS*. London, UK: SAGE. doi:10.4135/9781849209328

Arachchilage, N. A. G., Love, S., & Beznosov, K. (2016). Phishing threat avoidance behaviour: An empirical investigation. *Computers in Human Behavior*, *60*, 185–197. doi:10.1016/j.chb.2016.02.065

Bada, M., Sasse, A. M., & Nurse, J. R. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *Sustainable Society Network,* 118–131.

Ball, A. L., Ramim, M. M., & Levy, Y. (2015). Examining users' personal information sharing awareness, habits, and practices in social networking sites and e-learning systems. *Online Journal of Applied Knowledge Management*, *3*, 180–207. Retrieved from http://www.iiakm.org/

Baron, H. (1996). Strengths and limitations of ipsative measurement. *Journal of Occupational and Organizational Psychology*, *69*, 49–56. doi:10.1111/j.2044-8325.1996.tb00599.x

Bayer, J. B., & LaRose, R. (2018). Technology habits: Progress, problems, and prospects. In B. Verplanken (Ed.), *The psychology of habit: Theory, mechanisms, change, and contexts* (pp. 111–130). Cham, Switzerland: Springer. doi:10.1007/978-3-319-97529-0_7

Belanger, F., & Crossler, R. E. (2019). Dealing with digital traces: Understanding protective behaviors on mobile devices. *The Journal of Strategic Information Systems*, *28*(1), 34-49. doi:10.1016/j.jsis.2018.11.002

Bennett, T., Dodsworth, F., Noble, G., Poovey, M., & Watkins, M. (2013). Habit and habituation: Governance and the social. *Body & Society*, *19*, 3-29. doi:10.1177/1357034X13485881

Berte, D. R. (2018). Defining the IoT. *Proceedings of the International Conference on Business Excellence, 12*, 118-128. doi:10.2478/picbe-2018-0013

Boehmer, J., LaRose, R., Rifon, N., Alhabash, S., & Cotten, S. (2015). Determinants of online safety behaviour: Towards an intervention strategy for college students. *Behaviour & Information Technology*, *34*, 1022–1035. doi:10.1080/0144929X.2015.1028448

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly*, *39*, 837–864. Retrieved from https://www.misq.org/

Burns, M. B., Durcikova, A., & Jenkins, J. L. (2012). On not falling for phish: Examining multiple stages of protective behavior of information system end-users. Retrieved from https://aisel.aisnet.org/

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of Information Security and Applications*, *42*, 36-45. doi:10.1016/j.jisa.2018.08.002

Carden, L., & Wood, W. (2018). Habit formation and change. *Current Opinion in Behavioral Sciences*, *20*, 117-122. doi:10.1016/j.cobeha.2017.12.009

Chenoweth, T., Gattiker, T., & Corral, K. (2019). Adaptive and maladaptive coping with an IT threat. *Information Systems Management*, *36*, 24-39. doi:10.1080/10580530.2018.1553647

Chiu, C., & Huang, H. (2015). Examining the antecedents of user gratification and its effects on individuals' social network services usage: The moderating role of habit. *European Journal of Information Systems, 24*, 411-430. doi:10.1057/ejis.2014.9

Claar, C. L., & Johnson, J. (2012). Analyzing home PC security adoption behavior. *Journal of Computer Information Systems*, *52*, 20–29. doi:10.1080/08874417.2012.11645573

Clark, I. L. (2006). *Writing the successful thesis and dissertation: Entering the conversation*. Upper Saddle River, NJ: Prentice Hall.

Collaborative Institutional Training Initiative Program. (2014). Human subjects research (HSR) series. Retrieved from https://citiprogram.org

Conner, M., & Norman, P. (2005). *Predicting health behaviour*. London, UK: McGraw-Hill Education.

Cooper, D. R., Schindler, P. S., & Sun, J. (2006). *Business research methods* (9th ed.). New York, NY: McGraw-Hill Irwin.

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). Los Angeles, CA: SAGE.

Crossler, R., & Belanger, F. (2014). An extended perspective on individual security behaviors: Protection motivation theory and a unified security practices (USP) instrument. *ACM SIGMIS Database*, *45*, 51–71. doi:10.1145/2691517.2691521

Crossler, R. E., Belanger, F., & Ormond, D. (2017). The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. *Information Systems Frontiers*, 1-15. doi:10.1007/s1079

Crotty, M. (2012). *The foundations of social research. Meaning and perspective in the research process.* Thousand Oaks, CA: SAGE.

Dang-Pham, D., Pittayachawan, S., & Bruno, V. (2016). Factors of people-centric security climate: conceptual model and exploratory study in Vietnam.

Dannar, P. R. (2013). Millennials: What they offer our organizations and how leaders can make sure they deliver. *The Journal of Values-Based Leadership*, *6*, 1-13. Retrieved from https://scholar.valpo.edu

Dawes, J. G. (2012). Do data characteristics change according to the number of scale points used? An experiment using 5 point, 7 point, and 10 point scales. *International Journal of Market Research*, *50*, 61–77. doi:10.1177/147078530805000106

Debevec, K., Schewe, C. D., Madden, T. J., & Diamond, W. D. (2013). Are today's millennials splintering into a new generational cohort? Maybe! *Journal of Consumer Behaviour*, *12*, 20–31. doi:10.1002/cb.1400

De Keyzer, F., Dens, N., & De Pelsmacker, P. (2017). Don't be so emotional! How tone of voice and service type affect the relationship between message valence and consumer responses to WOM in social media. *Online Information Review*, *41*, 905-920.

Delice, A. (2010). The sampling issues in quantitative research. *Educational Sciences: Theory and Practice*, *10*, 2001–2018. Retrieved from http://www.edam.com

Dias, J. P., Pinto, J. P., & Cruz, J. M. (2017). A hands-on approach on botnets for behavior exploration. In *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security - Volume 1: WICSPIT,* (pp. 463–469). Portugal: Porto. doi:10.5220/0006392404630469

Dodel, M., & Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human Behavior*, *68*, 359–367. Retrieved from doi:10.1016/j.chb.2016.11.044

Dupuis, M., Crossler, R., & Endicott-Popovsky, B. (2012). The information security behavior of home users: Exploring a user's risk tolerance and past experiences in the context of backing up information. In *The Dewald Roode Information Security Workshop, Provo, Utah*. *ResearchGate*, 1-34. Retrieved from https://www.researchgate.net/publication/305778441

Dupuis, M. J., Crossler, R. E., & Endicott-Popovsky, B. (2016). Measuring the human factor in information security and privacy. In *2016 49th Hawaii International Conference on System Sciences (HICSS),* Kauai, Hawaii: IEEE, 3676-3685.

Faul, F., Erdfelder, E., Buchner, A., & Lang, A. G. (2009). Statistical power analyses using G* Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*, 1149–1160. doi:10.3758/BRM.41.4.1149

Field, A. (2009). *Discovering statistics using SPSS*. London, UK: SAGE

Fleming, J., & Adkins, A. (2016). Data security: Not a big concern for millennials. *Gallup*. Retrieved from https://news.gallup.com

Fowler, F. J., Jr. (2009). *Survey research methods*. Thousand Oaks, CA: SAGE. doi:10.4135/9781452230184.n1

Friedman, T. L. (2016). *Thank you for being late: An optimist's guide to thriving in the age of accelerations (version 2.0, with a new afterword)*. New York, NY: Picador/Farrar Straus and Giroux.

Fromm, J., & Garton, C. (2013). *Marketing to millennials: Reach the largest and most influential generation of consumers ever.* Saranac Lake, NY: AMACOM.

Fry, R. (2016). This year, millennials will overtake baby boomers. *Pew Research Center and FactTank*. Retrieved from http://www.pewresearch.org

Furnell, S., Khern-am-nuai, W., Esmael, R., Yang, W., & Li, N. (2018). Enhancing security behaviour by supporting the user. *Computers & Security*, *75*, 1-9. doi:10.1016/j.cose.2018.01.016

Furnham, A. (1986). Response bias, social desirability, and dissimulation. *Personality and Individual Differences*, *7*, 385–400. doi:10.1016/0191-8869(86)90014-0

Gardner, B. (2012). Habit as automaticity, not frequency. *European Health Psychologist*, *14*, 32–36. Retrieved from https://ehps.net/ehp/index.php/contents

Gardner, B., Abraham, C., Lally, P., & de Bruijn, G. J. (2012). Towards parsimony in habit measurement: Testing the convergent and predictive validity of an automaticity subscale of the Self-Report Habit Index. *International Journal of Behavioral Nutrition and Physical Activity*, *9*(102), 1-12. doi:10.1186/1479-5868-9-102

Glaspie, H. W., & Karwowski, W. (2017). Human factors in information security culture: A literature review. In: Nicholson D. (Eds.) *Advances in human factors in cybersecurity*. *AHFE 2017. Advances in intelligent systems and computing*, *vol. 593* (pp. 269-280). Warren: Springer. doi:10.1007/978-3-319-60585-2_25

Haeussinger, F., & Kranz, J. (2017). Antecedents of employees' information security awareness-review, synthesis, and directions for future research. *Association of Information Systems*. *Proceedings of the 25th European Conference on Information Systems (ECIS), Guimarães, Portugal, 2017,* (pp. -). Retrieved from https://aisnet.org/default.aspx

Hameed, M. A., & Arachchilage, N. A. G. (2019). On the impact of perceived vulnerability in the adoption of information systems security innovations. *arXiv preprint arXiv:1904.08229*. doi:10.5815/ijcnis.2019.04.02

Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: a protection motivation theory perspective. *Information Systems Management*, *33*, 2-16. doi:10.1080/10580530.2015.1117842

He, W., Yuan, X., & Tian, X. (2014). The self-efficacy variable in behavioral information security research. In *2014 Enterprise Systems Conference* (pp. 28-32). IEEE. doi:10.1109/ES.2014.52

Hines, B. (2012). Generation Y, I think we have problems. *Techopedia.* Retrieved from https://www.techopedia.com

Howe, A. E., Ray, I., Roberts, M., Urbanska, M., & Byrne, Z. (2012). The psychology of security for the home computer user. In *2012 IEEE Symposium on Security and Privacy*, 209-223. Washington, DC: IEEE. doi:10.1109/SP.2012.23

Internet Security Threat Report. (2019). *Symantec Corporation*. Retrieved from https://www.symantec.com

Ion, I., Reeder, R., & Consolvo, S. (2015). ". . . no one can hack my mind": Comparing expert and non-expert security practices. In *2015 Symposium on Usable Privacy and Security [SOUPS]* (pp. 327-346). Ottawa, Canada: USENIX.

Jansen, J., & Van Schaik, P. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information & Computer Security*, *25*, 165-180. doi:10.1108/ICS-03-2017-0018

Kleinrock, L. (2003). An Internet vision: The invisible global infrastructure. *Ad Hoc Networks*, *1*, 3–11. Retrieved from https://www.lk.cs.ucla.edu

Kottke, J. (2017). How has the Internet changed in the last 10 years? Retrieved from https://kottke.org

Kreiner, G. E., Hollensbe, E. C., & Sheep, M. L. (2009). Balancing borders and bridges: Negotiating the work-home interface via boundary work tactics. *Academy of Management Journal, 52*, 704–730. doi:10.5465/amj.2009.43669916

Kurz, T., Gardner, B., Verplanken, B., & Abraham, C. (2015). Habitual behaviors or patterns of practice? Explaining and changing repetitive climate-relevant actions. *WIREs Climate Change, 6*, 113–128. doi:10.1002/wcc.327

Limayem, M., Hirt, S. G., & Cheung, C. M. K. (2007). How habit limits the predictive power of intention. The case of information system continuance. *MIS Quarterly, 31*, 705-737. doi:10.2307/25148817

Lopez, M. (2015). Pandalabs neutralized 75 million new malware samples in 2014. *PandaLabs MediaCenter*. Retrieved from https://www.pandasecurity.com

Loving, J. H. (2016). Analyzing malware remediation in the expanding home network. In *TPRC 44: The 44th Research Conference on Communication, Information, and Internet Policy 2016* (pp. 1-30). Schertz, TX: TPRC. doi:10.2139/ssrn.2756799

Lynam, R. (2000). *The works of Samuel Johnson, LL.D.* In *R. Harris (*Ed.) *The vision of Theodore, the hermit of Teneriffe.* London: George Cowie, pp.273-285. (Scanned and corrected by Robert Harris, 2000). Retrieved from https://www.virtualsalt.com/lit/theodore.htm

Maddux, J. E., & Gosselin, J. T. (2003). Self-efficacy. In M. R. Leary & J. P. Tangney (Eds.), *Handbook of self and identity* (pp. 218-238). New York, NY: The Guilford Press. doi:10.1080/10413209308411310

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology, 19*, 469 - 479. doi:10.1016/0022-1031(83)90023-9

Mai, B., Parsons, T., Prybutok, V., & Namuduri, K. (2017). Neuroscience foundations for human decision making in information security: A general framework and experiment design. In *Information Systems and Neuroscience* (pp. 91–98). Bath, UK: Springer. doi:10.1007/978-3-319-41402-7_12

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*, 32-44. doi:10.1016/j.chb.2018.01.028

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams, and cybercrime in general. *Computers in Human Behavior*, *92*, 139-150. doi:10.1016/j.chb.2018.11.002

McDonald, N. C. (2015). Are millennials really the "go-nowhere" generation? *Journal of the American Planning Association, 81*, 90-103, doi:10.1080/01944363.2015.1057196

McGill, T., & Thompson, N. (2017). Old risks, new challenges: Exploring differences in security between home computer and mobile device use. *Behaviour & Information Technology*, *36*, 1111-1124.

Menard, P., Gatlin, R., & Warkentin, M. (2014). Threat protection and convenience: Antecedents of cloud-based data backup. *Journal of Computer Information Systems*, *55*, 83-91. doi:10.1080/08874417.2014.11645743

Mertler, C. A., & Vannatta, R. A. (2013). *Advanced and multivariate statistical methods* (5th ed.). Glendale, CA: Pyrczak.

Meso, P., Ding, Y., & Xu, S. (2013). Applying protection motivation theory to information security training for college students. *Journal of Information Privacy and Security*, *9*, 47–67. doi:10.1080/15536548.2013.10845672

Milkman, R. (2017). A new political generation: Millennials and the post-2008 wave of protest. *American Sociological Review*, *82*, 1-31. doi:10.1177/0003122416681031

Mills, A., & Sahi, N. (2019). An empirical study of home user intentions towards computer security. In *Proceedings of the 52nd Hawaii International Conference on System Sciences* (pp. 4834 – 4840). doi:10.24251/HICSS.2019.583

Mouakket, S. (2015). Factors influencing continuance intention to use social network sites: The Facebook case. *Computers in Human Behavior*, *53*, 102–110. doi:10.1016/j.chb.2015.06.045

Munafo, M., & Albery, I. P. (2008). Social cognitive models and: Protection motivation theory. In *Key Concepts in Health Psychology* (pp. 42 – 76). London, UK: SAGE UK. Retrieved from Credo Online Reference Service

Nederhof, A. J. (1985). Methods of coping with social desirability bias: A review. *European Journal of Social Psychology*, *15*, 263–280. doi:10.1002/ejsp.2420150303

Nilsen, P., Roback, K., Brostrom, A., & Ellstrom, E. (2012). Creatures of habit: Accounting for the role of habit in implementation research on clinical behaviour change. *Implement Science, 7*, 53. doi:10.1186/1748-5908-7-53

Nnambooze, B. E., & Parumasur, S. B. (2016). Understanding the multigenerational workforce: Are the generations significantly different or similar? *Corporate Ownership and Control*, *13*, 224–237. doi:10.22495/cocv13i2c1p4

Norman, P., Boer, H., & Seydel, E. R. (2005). Protection motivation theory. *Open University Press,* 81-126. Retrieved from http://doc.utwente.nl/53445/1/K469____[1].pdf

Nthala, N., & Flechais, I. (2018). Informal support networks: an investigation into home data security practices. In *Fourteenth Symposium on Usable Privacy and Security* (pp. 63-82). Retrieved from https://www.usenix.org/system/files/conference/soups2018/soups2018-nthala.pdf

Omilion-Hodges, L. M., & Sugg, C. E. (2019). Millennials' views and expectations regarding the communicative and relational behaviors of leaders: exploring young adults' talk about work. *Business and Professional Communication Quarterly*, *82*, 74-100. doi:10.1177/2329490618808043

Ong, L., & Chong, C. (2014). Information security awareness: An application of psychological factors–A study in Malaysia. In *2014 International Conference on Computer, Communications, and Information Technology [CCIT 2014]* (98 – 101). Bejing, China: Atlantis Press. doi:10.2991/ccit-14.2014.27

Patten, M. L. (2014). *Understanding research methods: An overview of essentials* (9th ed.). Glendale, CA: Pyrczak.

Ramírez-Vizcaya, S., & Froese, T. (2019). The enactive approach to habits: New concepts for the cognitive science of bad habits and addiction. *Frontiers in psychology*, *10*. doi:10.3389/fpsyg.2019.00301

Rantonen, K. (2014). Explaining information security behavior: Case of the home user. Retrieved from http://urn.fi/URN:NBN:fi:jyu-201505121832

Razak, M. F., Anuar, N. B., Salleh, R., & Firdaus, A. (2016). The rise of "malware": Bibliometric analysis of malware study. *Journal of Network and Computer Applications*, *75*, 58–76. doi:10.1016/j.jnca.2016.08.022

Rhee, H., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security, 28*, 816–826. doi:10.1016/j.cose.2009.05.008

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*, 93–114. doi:10.1080/00223980.1975.9915803

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

Rubenking, N. J. (2019). The best security suites for 2019. *PC Magazine*. Retrieved from https://www.pcmag.com

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53*, 65-78. doi:10.1016/j.cose.2015.05.012

Shafer, D. (2015). Four reasons why millennials should care about safer internet day. *Crunch Network*. Retrieved from https://techcrunch.com

Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., LaRose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*, 199–207. doi:10.1016/j.chb.2015.01.046

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177–191. doi:10.1016/j.cose.2015.01.002

Smith, T. J., & Nichols, T. (2015). Understanding the millennial generation. *The Journal of Business Diversity, 15*, 39–47. Retrieved from https://www.researchgate.net

Spafford, E. C. (2014). Is anti-virus really dead. *Computers & Security*, *44*. doi:10.1016/S0167-4048(14)00082-0

Stewart, J. S., Oliver, E. G., Cravens, K. S., & Oishi, S. (2017). Managing millennials: Embracing generational differences. *Business Horizons*, *60*, 45-54. doi:10.1016/j.bushor.2016.08.011

Taylor, S. (2013). The next generation of the Internet revolutionizing the way we work, live, play, and learn. *Cisco Internet Business Solutions Group (IBSG).* Retrieved from https://www.cisco.com

Thatcher, J. B., Wright, R. T., Sun, H., Zagenczyk, T. J., & Klein, R. (2018). Mindfulness in information technology use: Definitions, distinctions, and a new measure. *MIS Quarterly*, *42*, 831-847. doi:10.25300/MISQ/2018/11881

Thompson, N., McGill, T. J., & Wang, X. (2017). "Security begins at home": Determinants of home computer and mobile device security behavior. *Computers & Security*, *70*, 376-391. doi:10.1016/j.cose.2017.07.003

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138–150. doi:10.1016/j.cose.2016.02.009

Tu, C. Z., Adkins, J., & Zhao, G. Y. (2019). Complying with BYOD security policies: A moderation model based on protection motivation theory. *Journal of the Midwest Association for Information Systems, 2019*, 1-28. doi:1017705/3jmwa.00004

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: An empirical examination. *Information & Management*, *52*, 506-517. doi:10.1016/j.im.2015.03.002

Van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies*, *123*, 29-39. doi:10.1016/j.ijhcs.2018.11.003

Vance, A., Jenkins, J. L., Anderson, B. B., Bjornn, D. K., & Kirwan, C. B. (2018). Tuning out security warnings: A longitudinal examination of habituation through fMRI, eye tracking, and field experiments. *MIS Quarterly*, *42*, 355-380. doi:10.25300/MISQ/2018/14124

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*, 190–198. doi:10.1016/j.im.2012.04.002

Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, *78*, 283-297. doi:10.1016/j.chb.2017.10.007

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547-559. doi:10.1016/j.chb.2017.05.038

Verizon. (2019). 2019 data breach investigations report. *Information Security*, 1–7. Retrieved from https://enterprise.verizon.com/

Verplanken, B., Aarts, H., & Van Knippenberg, A. (1997). Habit, information acquisition, and the process of making travel mode choices. *European Journal of Social Psychology*, *27*, 539–560. doi:10.1002/(SICI)1099-0992

Verplanken, B., & Orbell, S. (2003). Reflections on past behavior: A self-report index of habit strength. *Journal of Applied Social Psychology*, *33*, 1313–1330. doi:10.1111/j.1559-1816.2003.tb01951.x

Waljee, J. F., Chopra, V., & Saint, S. (2018). Mentoring millennials. *Journal of the American Medical Association*, *319*, 1547-1548. doi:10.1001/jama.2018.3804

Warkentin, M., & Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly*, *39*, 113–134. doi:10.25300/MISQ/2015/39.1.06

Wash, R., & Rader, E. (2015). Too much knowledge? Security beliefs and protective behaviors among united states internet users. In *Eleventh Symposium on Usable Privacy and Security 2015* (pp. 309-325). Retrieved from https://www.usenix.org

Webroot. (2018). What is antivirus software? Retrieved from https://webroot.com

White, G. L. (2015). Education and prevention relationships on security incidents for home computers. *Journal of Computer Information Systems*, *55*, 29–37. doi:10.1080/08874417.2015.11645769

White, G. L., Ekin, T., & Visinescu, L. (2017). Analysis of protective behavior and security incidents for home computers. *Journal of Computer Information Systems*, 57, 353–363. doi:10.1080/08874417.2016.1232991

White, G. L., Hewitt, B., & Kruck, S. E. (2013). Incorporating global information security and assurance in IS education. *Journal of Information Systems Education*, *24(1)*, 11–16. Retrieved from https://http://jise.org/

Whitman, M. E., & Mattord, H. J. (2017). *Management of information security* (5th ed.). Boston, MA: Cengage Learning.

Wolf, F., Kuber, R., & Aviv, A. J. (2018). How do we talk ourselves into these things? Challenges with adoption of biometric authentication for expert and non-expert users. *UMBC Student Collection*, 1-7. doi:10.1080/0144929X.2018.1436591

Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security. In *Twenty-sixth international conference on information systems [ICIS]* (pp. 367-380). Las Vegas, NV. Retrieved from http://aisel.aisnet.org/icis2005

Workman, M., Bommer, W. H., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, *24*, 2799-2816. doi:10.1016/j.chb.2008.04.005

Yoon, C., Hwang, J., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. *Journal of Information Systems Education, 23*, 407–415. Retrieved from https://http://jise.org/

Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace. *Information Technology & People, 26*, 401–419. doi:10.1108/ITP-12-2012-0147

APPENDIX A. SURVEY INSTRUMENT MEASURMENT ITEMS

Construct	Research Instrument
Habit	• Habit1: I should periodically remove viruses and malicious software [from my computer] • Habit2: I automatically send suspicious emails to my recycle bin • Habit3: I do not download software from suspicious websites. • Habit4: Complying with personal computer and information security practices like, 1)Don't trust suspicious emails or suspicious links 2)Ensure that antivirus software is up to date and apply updates when necessary, and 3)Ensure that you have a strong password because it is the first line of defense to data protection, is something you do without thinking about it.
Intention	**ITC1:** Lana loans her computer that uses for all of her financial management to her next neighbor, giving her neighbor full access to her personal information. Two months later, Lana finds that her social security number is being used in New York by someone with a very similar name. Lana realizes that she should trust no one with her personal information. What is the chance that you would do what Lana did in the described scenario? **ITC2:** Jason know the three P's of Internet Security, 1) Practices: don't trust suspicious emails or suspicious links 2) Patches: ensure that antivirus software is up to date and apply malware updates when necessary, and 3) Password: ensure that you have a strong password is the first line of defense to data protection. Jason is browsing websites and the antivirus program on his computer alerts him that a virus has been install [on his computer]. Jason decides to take care of the virus problem later. I would act in the same way as Jason did if I was in a similar situation.
Perceived severity	**PS1**: Losing data as a result of malware (spyware) attack would be a serious problem for me. **PS2**: Lana loans her computer that uses for all of her financial management to her next neighbor, giving her neighbor full access to her personal information. Two months later, Lana finds that her social security number is being used in New York by someone with a very similar name. Lana realizes that she should trust no one with her personal information. **If I did what [Lana] did, I would have serious information security problems and there could be repercussions, like loss of money**.
Perceived vulnerability	**PV1**: Lana loans her computer that uses for all of her financial management to her next neighbor, giving her neighbor full access to her personal information. Two months later, Lana finds that her social security number is being used in New York by someone with a very similar name. Lana realizes that she should trust no one with her personal information. **I could be subject to an information security threat if I did what Lana did.** **PV2**: Gina and her family share one computer which Gina uses to do all her online banking and purchasing. Gina's husband downloaded software from a suspect site and thereby downloaded spyware unto the family's computer. In 24 hours' time, Gina and her family racked up thousands of unexplained charges and the money in their bank account had been siphoned nearly dry. **My personal information would be vulnerable if I did what Gina's husband did.**

Response efficacy	**RE1**: Taking malware preventative measures for my computer protects my personal information. **RE2**: Enabling security measures on my computer is a great process to prevent my personal data on my computer from being lost or damaged by malware.
Self-efficacy	**SE1**: I feel comfortable protecting my personal computer from Internet malware threats (installing antivirus software, creating separate user accounts, not giving anyone my passwords, or free access to my computer, etc...) **SE2**: I am capable of removing viruses and other malware from my computer. **SE3**: Jason know the three P's of Internet Security, 1)Practices: don't trust suspicious emails or suspicious links 2)Patches: ensure that antivirus software is up to date and apply malware updates when necessary, and 3)Password: ensure that you have a strong password is the first line of defense to data protection. Jason is browsing websites and the antivirus program on his computer alerts him that a virus has been install [on his computer]. Jason decides to take care of the virus problem later. **I could easily do the opposite of what Jason did without thinking about it.**
Response cost	**RC1**: There are too many things I need to know and pay for when I think of enabling computer security measures and malware prevention measures. **RC2**: Installing computer security, like antivirus software, to protect against malware is annoying. **RC3**: Changing passwords and employing other security procedures to protect personal information is painful for me.
Rewards	**R1**: Jason know the three P's of Internet Security, **Practices:** don't trust suspicious emails or suspicious links, **Patches:** ensure that antivirus software is up to date and apply malware updates when necessary, and **Password:** ensure that you have a strong password is the first line of defense to data protection. Jason is browsing websites and the antivirus program on his computer alerts him that a virus has been install [on his computer]. Jason decides to take care of the virus problem later. **If I did the opposite of what Jason did I would save on computer learning time.** **R2**: Not installing an antivirus software or seeing that it is up to date saves on my personal time.

APPENDIX B. LEVENE'S TEST FOR HOMOGENEITY OF VARIANCE

Variables	Levene's Test for Equality of Variances		t-test for Equality of Means						
	F	Sig.	t	df	Sig.	Mean Difference	Std. Error Difference	Lower	Upper
	0.036	0.849	0.808	214	0.420	0.366	0.453	-0.812	1.544
Habit			0.801	177.140	0.424	0.366	0.457	-0.823	1.556
	0.200	0.655	-0.268	214	0.789	-0.075	0.278	-0.797	0.648
PV			-0.267	180.319	0.789	-0.075	0.279	-0.801	0.652
	0.282	0.596	0.617	214	0.538	0.146	0.237	-0.469	0.761
PS			0.609	173.979	0.543	0.146	0.240	-0.478	0.770
	7.147	0.008	4.714	214	0.000	2.224	0.472	0.998	3.450
R			4.515	155.148	0.000	2.224	0.493	0.939	3.508
	0.450	0.503	0.346	214	0.730	0.081	0.235	-0.530	0.693
RE			0.339	170.395	0.735	0.081	0.240	-0.543	0.706
	0.028	0.868	3.033	214	0.003	1.354	0.446	0.194	2.514
SE			3.021	179.673	0.003	1.354	0.448	0.187	2.521
	6.265	0.013	2.820	214	0.005	1.855	0.658	0.146	3.565
RC			2.699	154.621	0.008	1.855	0.687	0.063	3.648

Note. The test indicates that the variances are approximately equal. The independent sample t-test has a p-value of .001. Significance (Sig.) is a 2-tailed test.