# DOES DIGITAL NATIVE STATUS IMPACT END-USER ANTIVIRUS USAGE?

Gerrianne Roberts, Ph.D.[1] and Shawon Rahman, Ph.D.[2]

[1]Full-Time Professor, Department of Cybersecurity and Network Engineering Technology (CyNET), Valencia College, Orlando, Florida, 32811, USA
[2]Professor, Department of Computer Science and Engineering, University of Hawaii-Hilo Hilo, Hawaii 96720, USA

### *ABSTRACT*

*Due to the increasingly online nature of business (e-commerce), it is essential to understand how end-users can be protected from malicious online activities such as malware. Several factors have been examined in the research on this topic. Digital native status was identified as a factor that has not been investigated thoroughly. This study examined how the security decision-making process is impacted by digital native status by looking at Protection Motivation Theory. Digital Native Status was investigated as a mediating factor in the PMT model. Intent to use antivirus was utilized as the protective measure. The findings indicate that digital native status does not mediate Fear. However, other factors, such as Fear, self-efficacy, and response efficacy, play a part in the intent to use antivirus. Conversely, the other constructs in the model, response-costs and maladaptive rewards, did not have a relationship with antivirus usage. Practically speaking, employers and eCommerce businesses could use these findings to identify factors that play into their end-user behaviors. These findings can be utilized to help guide training programs and professionals researching end-user behavior. These findings also suggest that future research should focus on factors other than age.*

### *KEYWORDS*

*Protection Motivation Theory, Fear Motivation, Digital Native, Digital Immigrant, Information Privacy, Antivirus.*

## 1. INTRODUCTION

With the advent of the Internet, consumerism has shifted from a purely physical interaction model to an increasingly eCommerce model [1]. Many companies have successfully used digital communication models; however, digital communication has also introduced new information privacy challenges [2]. According to Bansal and Zahedi [3], there has been an increase in online privacy violations, leading to personal customer information exposure. This exposure, in turn, has created concern in the consumer community [3].

Information privacy concerns can quickly turn into violations of trust for consumers [2]. For example, in 2011, Sony experienced a significant data breach that resulted in consumer concern and customer lawsuits due to the violation of trust [4]. In the same year, multiple other attacks occurred that dampened consumer trust. Companies such as RSA (an information security provider), Best Buy, Target, Verizon, and more suffered breaches that ultimately lead to a severe violation of trust [4].

These types of breaches are not uncommon. Privacy Rights Clearinghouse (PRC) has archived over 9000 breach events from January 2005 to December 2018 [31]. Altogether, there were 12

DOI: 10.5121/ijcnc.2021.13207

billion records in these archives [31]. Many similar organizations have had similar results in their recording and reporting on information breaches [32]. Such trust violations are of concern to companies due to the potential loss of revenue. According to Tomlinson and Mayer [5], trust violations can have consequences such as loss of income (due to loss of sales) and other irreparable damages (such as legal consequences). Shackelford [4] claims that this loss can be upwards of $200 per consumer record lost, and potentially more per consumer.

Companies also face potentially severe legal consequences from breaches [6]. Lawsuits aimed at companies who have violated consumer privacy by illegally selling consumer information and illegally tracking consumer online behavior through their browser (mainly using "cookies" to track consumers' online behaviors) have brought more attention to the privacy issue. These incidents have spurred new legislation aimed at protecting consumers from breaches of privacy via online conduits such as company websites and online storefronts.

With the advent of these new laws and added protections to existing laws, companies have had to find better ways to protect their data to ensure privacy for individuals or businesses they keep information about. Companies have been accomplishing this task by studying how users interact with their stored data to create better mechanisms to secure user information [7].

These studies have found that, in general, users who are concerned about their privacy in an online environment will most likely take measures to protect their privacy, measures such as installing antivirus or changing privacy settings on social media [8]. These studies have also found that several factors play into those concerns. Researchers have identified factors such as ownership [9], generation [10], protection motivation [11, 28], and data handling [12] as motivating factors. These items represent common themes throughout the research; however, they are not representative of everything that goes into consumer concern; research on this topic is still being developed, and new factors are found every day.

Much of the research looking into motivations to take privacy precautions utilize fear motivation theory. In addition to the study by Boss et al. [11] (referenced for this study), there have been numerous studies. For example, Tsai et al. [13] looked at fear motivation and planned behavior and how they relate to the end user's intention to take privacy protections. Another study, by Chen, Beaudoin, and Hong [14], looks at online privacy concerns and how protection motivation theory, in addition to the Extended Parallel Process Model (EPPM), plays into those concerns. Such studies continue to examine fear motivation and how it affects the end-user in their decision to take privacy precautions in an online environment.

This study utilizes PMT by keeping the existing framework and introducing a mediating factor (i.e., digital native status). It is a well-known presumption of those in the information security industry that familiarity with technology plays a role in how one reacts to situations and what precautions they may take. One also assumes that if someone is a "digital native" (i.e., born after 1980 during the proliferation of technology), they will be more familiar with technology due to growing up with it rather than adopting it later in life [15]. Therefore, this study tested the theory that digital native status moderates fear and the adaptive response to Fear.

Looking at PMT and DNS, the research question was formed. It centered around the idea that digital native status would be examined using PMT. The main research question is, "To what extent do high fear levels relate to an increased usage of antivirus software when moderated by digital native status?". Other research questions were formed from the PMT model itself. Each subsequent question sought to understand the relationship between each construct and the protective measure of antivirus use. These questions were developed to identify any other factors that impacted the decision-making process and confirm previous research on the topic.

From the research questions came the hypothesis: one null and one positive for each question. The null hypothesis meant that there were not any relationships between the constructs being examined in each question. The other, the positive hypothesis, posited that there was a relationship. The section discussing methods and materials goes further into the questions and their related hypothesis.

The remainder of the paper is broken down into five additional sections. In section 2, a literature review is presented to provide background on the topic of PMT, current research, and digital native status. Next, in section 3, the methodology used in the paper is provided. Then, in section 4, the study's results are presented and discussed. In section 5, future research recommendations are discussed. Lastly, in section 6, the paper is closed with conclusions sheened from the research.

## 2. LITERATURE REVIEW

This section examines the state of the research as it pertains to protection motivation and digital native status. This section is divided into three main sections. The first section discusses the background of PMT and the current state of research. The second section discusses PMT itself. Lastly, the third section discusses digital native status.

### 2.1. Background

Fear motivation theory, also known as PMT, posits that behavior may change based on a response to an event that caused Fear [16]. This is typically considered an adaptive response or a protection response [11, 16]. Fear motivation has been the focus of several studies to better understand end-user behavior to create better control mechanisms for end-user privacy [9, 11, 14, 17]. The ultimate goal of these types of studies is to better comply with local, state, federal, and international laws and to bring a better experience to the end-user [11, 12].

PMT has been used in many studies in the information security realm. Studies by Boss et al. [11], Doane et al. [17], Ifinedo [18], and many more all use PMT to examine end-user behaviors when it comes to compliance with policies as well as with taking protection methods such as using antivirus. Boss et al. [11] studied PMT in the context of end-user behavior with backups and antivirus usage. Doane et al. [17] used PMT to explore how cyberbullying impacts risky online transactions. Lastly, Ifinedo [18] studied PMT to see how it affected employee compliance with security policies.

PMT states that there are positive relationships between Fear and adaptive measures. There are also positive relationships between response efficacy and adaptive measures and between self-efficacy and adaptive measures [11]. The theory also shows a negative relationship between maladaptive rewards and adaptive measures and between response costs and adaptive measures [11]. As a result of these relationships, high fear levels are thought to lead to more protective measures [11, 16, 17, 18]. Additionally, Boss et al. [11] found that using high fear appeal messages created more Fear. In those scenarios where Fear was elevated, users were more likely to take protective measures.

The relationships between the independent and dependent variables in the PMT model also suggest that individuals with high perceived response efficacy are more likely to use a protection method [11, 16, 18]. Ifinedo [18] found that this relationship was supported by empirical evidence. In Ifindedo's study, the data analysis indicated a positive relationship between response efficacy and the likelihood that an individual would use a protection method.

Boss et al. [11] found evidence that individuals with high maladaptive rewards were less likely to use protection methods. Boss et al. [11] posited that individuals who feel that they are rewarded for not taking protective measures would be less likely to use protection than individuals motivated by Fear. PMT posits that individuals who perceive the response cost to be high are less likely to take protective measures [11]. Scholars have suggested that this relationship is because individuals may feel that the costs are not worth the effort [11, 18]. Boss et al. [11] found evidence to support this conclusion, but the results of Ifinedo's [18] study did not indicate a link between response cost and protective measures. This lack of consistency in the research suggests a need for additional research.

PMT theory does not explicitly examine other factors' influence on the relationships between fear motivators and adaptive measures. Examples of potential mediating and moderating variables include age, gender, race, and education level. While age is similar to digital native status as it has to do with birth year, it is not considered the same. Age is a variable that increases the further away from birth year one gets, while digital native status has to do with being born before 1980 or in 1980 or after. There are only two groups with digital native status. This study aims to add to the theory by looking at digital native status as a possible mediating factor in how Fear plays into adaptive measures.

## 2.2. Protection Motivation Theory and the Research Model

The research model used in this study is the PMT model. The model was first introduced by Rogers in 1975 [16] and was meant to examine how Fear plays a role in the decision-making process. The model has been modified over the years to accommodate new research on the topic [11]. The model's current iteration includes several new constructs, such as maladaptive rewards and response costs [11]. In the current model, these new constructs, in addition to traditional constructs (such as Fear and self-efficacy), all play a role in how the end-user responds to fear.

The model used for this study is based on what is referred to as the full PMT model and is considered the most current iteration of the model [11]. In this version of the model, Fear is affected by the individual's threat appraisal. The threat appraisal is comprised of two factors: perceived threat severity and perceived threat vulnerability (i.e., how large is the threat and how likely it is to occur). If either is large, the individual is expected to have a higher level of Fear and is more likely to act on that Fear [19].

If the threat is deemed high enough to take action, then the individual will progress to what is known as the coping appraisal step. In this step, the individual will analyze the response efficacy, self-efficacy, and response costs factors to see if it is worth moving on to the actual response to the threat [19]. If the response costs are too high, or if any of the efficacy factors are too low, then the individual is not likely to move on to the response [19].

Lastly, if the threat is deemed high enough, and the efficacy factors are considered high enough, they will likely move on and take the protective measure. This behavior implicates that the individual would be likely to use antivirus to protect their online privacy in our study. This study introduces a few factor. This new factor is digital native status. Digital native status has to do with when an individual was born. If the individual was born before 1980, they are considered a digital immigrant (or someone who adopted technology later in life). If the person was born on or after 1980, they are considered a digital native because they have grown up during the digital age and are assumed to have used technology most of their life [20] (see Figure 1 Research Model).

## 2.3. Digital Natives and Digital Immigrants

The mediating factor for this study is Digital native status. Digital native is a term popularized by educator Marc Prensky in 2001 [15]. Prensky wrote about digital natives and digital immigrants in an article titled “Digital Natives, Digital Immigrants.” In the article, Prensky discusses how learning changes have occurred due to the shift in the way students use technology. Prensky coined the term “digital native” for students born after 1980 who grew up with technology.

Prensky [15] describes the phenomenon of the digital age as a “singularity” [15, p. 1] that has changed the way people think and interact with each other. According to Prensky, digital natives are “native speakers” [15, p. 1] of technologies such as video games, the Internet, and computers in general. Since they are native speakers, digital natives have an “accent” [15, p. 3] that digital immigrants do not. For example, Prensky describes the process of information gathering for digital natives as turning immediately to the Internet instead of traditional sources such as newspapers and magazines, as a digital immigrant would. Prensky posits that this is because “a language learned later in life,…goes into a different part of the brain” [15, p. 3].

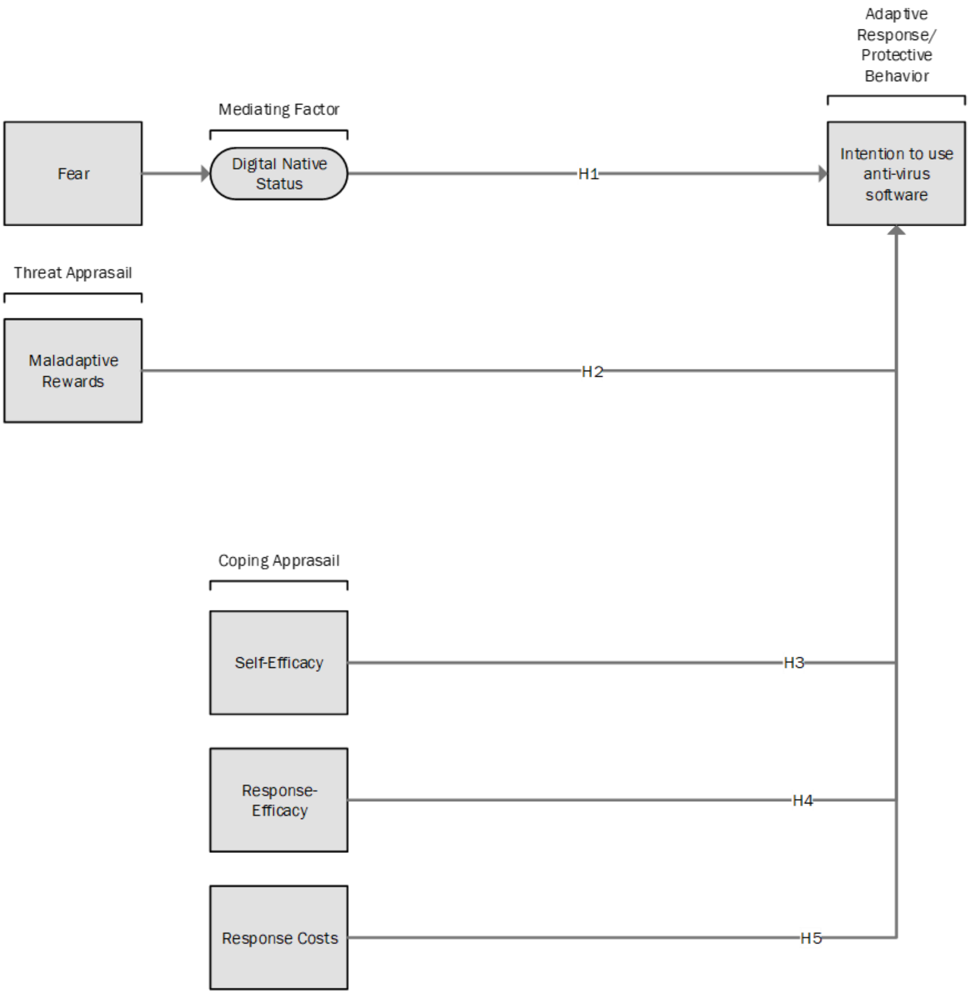

Figure 1 Research Model

Prensky followed up this article with a second article on digital natives and digital immigrants called “Digital Natives, Digital Immigrants, Part II: Do They Think Differently?” [21]. In this article, Prensky explores how growing up in a digital environment changes people’s thinking. Prensky posits that because one’s thinking patterns can vary based on experiences, growing up around technology changes how people think and therefore impacts their decision-making process and how they learn.

Prensky also posits that this change in the way digital natives think impacts how they develop their skills. In the article, Prensky suggests that digital natives may have lost their reflective ability (i.e., the ability to learn from experiences). Prensky is implying that their decision-making and thought processes may not have to do with prior experiences [21, 29, 30]. The change in the way digital natives think and their perceived increase in digital literacy are motivating factors behind using digital native status as a mediating factor in this study.

Others question whether or not digital native status impacts information literacy in the way implied by the very concept of the digital native. In 2017, Kirschner and De Bruyckere [35] questioned whether digital native status was real. They likened the idea to “yet-like creatures.” In 2019, Marksbury and Bryant [36], agreeing with Kirschner and De Bruyekere, did additional research on the topic and found that there may be something to the idea that digital literacy is not so native to the digital natives and more likely has to do with experiences, not age.

This clashing of ideas is one of the leading factors for this study.

The next section discusses the materials and methods used to conduct this study.

## 3. MATERIALS AND METHODS

This section presents the materials and methods used to conduct this study. First, a background is provided, then the section is broken into several sections describing different elements of the methodology. First, the research question and hypothesis are presented. The next section looks at instrumentation and presents the instrument used in the study. Validity and reliability are also discussed. Sampling procedures are then presented. In the last section, a brief overview of the data analysis process is presented.

A nonexperimental, correlational research design was chosen for this study. A survey instrument was used to collect data. The chosen approach allowed the researcher to quantitatively analyze the relationships between the different variables of interest in the study using linear regression analysis [22]. Data were collected via an online survey tool provided by QuestionPro. This approach was chosen as several related studies, such as the one by Boss et al. [11], utilized this methodology.

Seven variables were examined as part of the study. The four independent variables consisted of Fear, maladaptive rewards, response efficacy, self-efficacy, and response costs. Intent to use antivirus, the adaptive response, was examined as a dependent variable, and digital native status was examined as a mediating variable. Each of the independent variables was examined with the dependent variable to see if there was a relationship between them. The participants’ digital native status was then examined to determine if digital native status acted as a mediating factor between Fear and adaptive response.

A regression analysis was used to examine the relationships between the variables. Tabachnick and Fidell [22] noted that “Regression analyses are a set of statistical techniques that allow one to assess the relationship between one dependent variable (DV) and several independent variables (IVs)" [22, p. 117]. Regression analysis allowed the research questions to be answered via a simple analysis of the quantitative data to establish relationships between the various constructs and the intent to take adaptive measures by increasing the use of antivirus software. IBM SPSS was used to facilitate data analysis.

## 3.1. Research Questions and Hypotheses

Five research questions were investigated during the present study. Each research question was answered by testing a pair of null and alternative hypotheses. The research questions and their corresponding hypotheses were as follows:

**Research Question 1:** To what extent do high fear levels relate to increased usage of antivirus software when moderated by digital native status?

- **H01:** Higher levels of Fear are not related to increased usage of antivirus software when moderated by digital native status.
- **Ha1:** Higher levels of Fear are related to increased usage of antivirus software when moderated by digital native status.

**Research Question 2:** To what extent does higher acceptance of maladaptive rewards relate to increased usage of antivirus software?

- **H02:** Higher acceptance of maladaptive rewards do not lead to higher levels of usage of antivirus software
- **Ha2:** Higher acceptance of maladaptive rewards does lead to higher levels of usage of antivirus software

**Research Question 3:** To what extent do higher levels of response efficacy relate to increased usage of antivirus software?

- **H03:** Higher levels of response efficacy do not lead to higher levels of usage of antivirus software.
- **Ha3:** Higher levels of response efficacy do lead to higher levels of usage of antivirus software.

**Research Question 4:** To what extent do higher levels of self-efficacy relate to increased usage of antivirus software?

- **H04:** Higher levels of self-efficacy do not lead to higher levels of usage of antivirus software.
- **Ha4:** Higher levels of self-efficacy does lead to higher levels of usage of antivirus software.

**Research Question 5:** To what extent does higher response cost relate to increased usage of antivirus software?

- **H05:** Higher levels of response costs do not lead to higher levels of usage of antivirus software.
- **Ha5:** Higher levels of response costs lead to higher levels of usage of antivirus software.

## 3.2. Instrumentation

A survey instrument was used for this study. The survey instrument used was the same as the one used in the Boss et al. [11] study. The study consisted of two sub-studies. One looked at backup habits, and the other looked at antivirus usage. The sub-study questions that looked at antivirus were used with the author's permission for this study. The instrument asked questions about the various constructs and took responses in a 5-point Likert Scale format. A value of 5 represented agree, and a value of 1 represented disagree. The following section outlines the questions asked as part of the survey.

#### 3.2.1. Survey Instrument Questions

Measurement items (from Boss et al. [11]):

1) Intent to use anti-malware software
   a) I intend to use anti-malware software in the next three months.
   b) I predict I will use anti-malware software in the next three months.
   c) I plan to use anti-malware software in the next three months.
2) Threat severity
   a) If my computer were infected by malware, it would be severe.
   b) If my computer were infected by malware, it would be serious.
   c) If my computer were infected by malware, it would be significant.
3) Threat Vulnerability
   a) My computer is at risk of becoming infected with malware.
   b) It is likely that my computer will become infected with malware
   c) My computer may become infected with malware.
4) Response Efficacy
   a) Anti-malware software works for protection
   b) Anti-malware software is effective for protection.
   c) When using anti-malware software, a computer is more likely to be protected.
5) Self-Efficacy
   a) Anti-malware software is easy to use.
   b) Anti-malware software is convenient to use.
   c) I can use anti-malware software without much effort.
6) Fear
   a) My computer has a serious malware problem.
   b) My computer might be seriously infected with malware.
   c) The amount of malware on my computer is terrifying.
   d) I am afraid of malware.
   e) My computer might become unusable due to malware.
   f) My computer might become slower due to malware.
7) Maladaptive Rewards
   a) Not using an anti-malware application saves me time.
   b) Not using an anti-malware application saves me money.
   c) Not using an anti-malware application keeps me from being confused.
   d) Using an anti-malware application would slow down the speed of my access to the Internet.
   e) Using an anti-malware application would slow down my computer.
   f) Using an anti-malware application would interfere with other programs on my computer.
   g) Using an anti-malware application would limit the functionality of my Internet browser.
8) Response Costs
   a) The cost of finding an anti-malware application decreases the convenience afforded by the application.
   b) There is too much work associated with trying to increase computer protection through the use of an anti-malware application.
   c) Using an anti-malware application on my computer would require a considerable investment of effort other than time.
   d) Using an anti-malware application would be time-consuming

The survey was created by Boss et al. [11] using several surveys from previous research on malware. Boss et al. [11] vetted all of the survey questions. The following section discusses the reliability and validity of the survey instrument.

### 3.2.2. Validity and Reliability

Boss et al. (2015) tested the validity of the survey instrument using confirmatory factor analysis. They used STATA/SE version 3.1 to run the analysis. STATE/SE is a software application that allows for several statistical analyses, including factor analysis. Boss et al. tested both the convergent and the discriminant validity of the instrument. Testing indicated that the model fit was good, with values for the comparative fit index (CFI) at 0.948, the root mean square error of approximation (RMSEA) at 0.045, the Tucker-Lewis index (TLI) at 0.935, the coefficient of determination (CD) at 1.000, and an X2 value of 6067.02. This testing demonstrated that Boss et al. 's instrument was valid for measuring fear motivation and adaptive behavior.

Boss et al. (2015) tested their instrument's reliability by calculating the Cronbach's alpha coefficient for each construct. Cronbach's alpha tests for internal consistency and reliability through a complicated algorithm that results in an alpha value (α). This value represents the level of consistency among the items defining the construct [33]. All of the Cronbach's alpha scores reported by Boss et al. were higher than the acceptable threshold of .70. The lowest scores reported by Boss et al. were for the constructs of Fear (.755) and maladaptive rewards (.777). Scores between .70 and .80 are considered acceptable. The scores for threat vulnerability (.817), response costs (.845), and response efficacy (.898) all fell within the range of what is considered acceptable (i.e., .80 to .90). The remaining scores for threat severity (.915), self-efficacy (.929), and intent (.984) were above the threshold for excellent (i.e., above .90). Based on these scores, the instrument was considered reliable for use in the present study.

### 3.2.3. Sampling

Sampling for this study focused on participants that were regular internet users and were familiar with the basic concepts of information privacy. All participants were required to be over the age of 18 and were required to both live and work in the United States. A stratified random sampling technique was chosen to select the participants of this study. Two groups were formed – those classified as digital immigrants and one classified as digital natives. The two groups were formed to determine DNS status.

The sample size was determined through power analysis using G*Power [34]. When calculating the sample size, several parameters were considered, including effect size, power, and the number of predictors in the model. The desired effect size was small (i.e., 0.10), and the desired power was 0.95 (i.e., 95% confidence). There were five predictors in this study (fear level, maladaptive rewards, response efficacy, self-efficacy, and response costs). Based on these parameters, G*Power calculated the minimum necessary sample size to be 132 participants. Sixty-six in the digital immigrant group, and 66 in the digital native group.

QuestionPro facilitated the sampling process and used the desired stratified random sampling method. Members fitting the research criteria were randomly selected from QuestionPro's member database. Once selected, QuestionPro contacted the potential participants via email, informing them of the study's purpose and requesting that they complete the survey. Question Pro also facilitated the collection of data.

### 3.3. Data Analysis

The data analysis process began once the researcher downloaded the data from QuestionPro's website. The data was in a raw numeric format that included both nominal and ordinal data. Responses to questions about participants' gender and race constituted nominal data, and responses to the Likert-scale survey questions constituted ordinal data. The researcher loaded the raw data into the IBM SPSS tool for management and analysis. Before beginning the analysis, the researcher reviewed the data for accuracy and completeness. The researcher only modified data if there were any issues with outliers or deviations from normality. These modifications are described in the next chapter as part of the analysis. The analysis was done using the following techniques (see Table 1):

Table 1: Analysis Techniques by Research Question

| Research Question | Hypotheses | Analysis Type | Descriptive Statistics | Posthoc Analysis |
|---|---|---|---|---|
| 1 | $H_01$/ $H_a1$ | Multiple Linear Regression | Central Tendency, Median, Standard Deviation | *p*-values, beta coefficients, and *z*-tests |
| 2 | $H_02$/ $H_a2$ | Multiple Linear Regression | Central Tendency, Median, Standard Deviation | *p*-values, beta coefficients, and *z*-tests |
| 3 | $H_03$/ $H_a3$ | Multiple Linear Regression | Central Tendency, Median, Standard Deviation | *p*-values, beta coefficients, and *z*-tests |
| 4 | $H_04$/ $H_a4$ | Multiple Linear Regression | Central Tendency, Median, Standard Deviation | *p*-values, beta coefficients, and *z*-tests |
| 5 | $H_05$/ $H_a5$ | Multiple Linear Regression | Central Tendency, Median, Standard Deviation | *p*-values, beta coefficients, and *z*-tests |

In the next section, the results of the study are presented and discussed.

## 4. Results

The following section presents the results of the study and briefly discusses what they mean for the field. The section is divided into three sections. The first section looks at the demographics of the respondents to the study. The next section looks at the preliminary analysis and how the variables met normality. The last section discusses more thoroughly the data analysis and the results of the study.

### 4.1. Demographics

The sampling for this study was done using random stratified sampling. QuestionPro took in the requirements for the sample and provided the participants based on the researcher's needs. The sample requested was stratified into two groups: one containing digital immigrants and one containing digital natives. The following section discusses the sample that was obtained from QuestionPro.In the raw data, there were 183 samples. Since some of the surveys were not completed or did not meet additional criteria, some samples were removed. Twenty-four surveys were identified as incomplete or completely blank. Once the data was cleaned of the 24 incomplete or empty surveys, there were 159 participants in total. Of the 159 participants, 48 were male, 110 were female, and one participant was identified as third gender. Overall, males made up 30.2% of the respondents, females made up 69.2% of the respondents, and those who do not identify as either made up 0.6% of the respondents.

One hundred twenty-three people identified as white, 13 people who were black or African American, two people who were American Indian or Alaskan Native, seven people who were Asian, ten people of Hispanic or Hispanic Origin, and four people were two or more races. Those who identified as being white made up 77.4% of the participants. Black or African Americans made up 8.2% of the participants, American Indian or Alaskan Natives made up 1.3% of the respondents, those of Asian descent made up 4.4%, Hispanic or of Hispanic Origin made up 6.3%, and those who are two or more races made up 2.5%.

Twelve people were between the ages of 18-24, 58 were between 25-34, 28 between 35-44, 27 between 45-54, 18 were 55-64, and 16 were 65 or older. Those who are 18-24 made up 7.5% of the participants, those who are 25-34 are 36.5% of participants, 35-44 make up 17.6% of the participants, 45-54 make up 17%, 55-64 make up 11.3%, those that are 65 or older make up 10.1% of the total sample. 83 people were considered digital immigrants, and 76 were digital natives. Digital immigrants made up 52.2% of the sample, and digital natives made up 47.8% of the sample. The goal was 50%. The sample was within a small variance of this. All the participants were residents or citizens of the United States of America. The following table summarizes the demographics' results for the modified sample (after the incomplete surveys were removed).

Table 2: Demographic Characteristics

| Demographic | Category | Frequency | Percent |
|---|---|---|---|
| Gender | | | |
| | Male | 48 | 30.2 |
| | Female | 110 | 69.2 |
| | Third gender | 1 | 0.6 |
| Race | | | |
| | White | 123 | 77.4 |
| | Black or African American | 13 | 8.2 |
| | American Indian or Alaskan Native | 2 | 1.3 |
| | Asian | 7 | 4.4 |
| | Hispanic or of Hispanic Origin | 10 | 6.3 |
| | Two or more races | 4 | 2.5 |
| Age | | | |
| | 18-24 | 12 | 7.5 |
| | 25-34 | 58 | 36.5 |
| | 35-44 | 28 | 17.6 |
| | 45-54 | 27 | 17 |
| | 55-64 | 18 | 11.3 |
| | 65 and over | 16 | 10.1 |

| Demographic | Category | Frequency | Percent |
|---|---|---|---|
| Digital Native Status | | | |
| | Born before 1980 (digital immigrant) | 83 | 52.2 |
| | Born on or after 1980 (digital native) | 76 | 47.8 |

## 4.2. Preliminary Analysis

Scales were formed based on the study by Boss et al. [11]. Summary statistics on the scales are presented in Table 2. The normality of the scales was assessed using *z*-scores formed by dividing skewness by the standard error of skewness (*SK/SE*). Values above +/- 3.29 are indicative of departures from normality [22]. As shown, two of the scales, the dependent variable, Intent to Use Anti-Malware, and one of the independent variables, response efficacy, were negatively skewed. Before using these scales in the comparative analyses to test the hypotheses, a normalizing transformation was applied to the values, as recommended by [23].

Specifically, the scores were reflected (each score was subtracted from 6), and then the square root was taken of the result. In presenting the results, the directions of all relationships (either positive or negative) were adjusted to represent the original variables.

Table 3: Summary Statistics for Study Measures

| **Scales** | ***Mean*** | ***SD*** | ***Skewness*** | ***SE*** | ***SK/SE*** |
|---|---|---|---|---|---|
| Non-normalized scales | | | | | |
| Intent to use anti-malware | 3.92 | 1.09 | -0.82 | 0.19 | -4.28 |
| Response efficacy | 3.97 | 0.83 | -0.83 | 0.19 | -4.34 |
| Self-efficacy | 3.87 | 0.92 | -0.61 | 0.19 | -3.18 |
| Fear | 2.85 | 1.03 | 0.20 | 0.19 | 1.06 |
| Maladaptive rewards | 2.65 | 1.11 | 0.22 | 0.19 | 1.12 |
| Response costs | 2.72 | 1.04 | 0.19 | 0.19 | 0.96 |
| Normalized Scales (square root of reflected scores) | | | | | |
| Intent to use anti-malware | 1.40 | 0.37 | 0.45 | 0.19 | 2.35 |
| Response efficacy | 1.40 | 0.29 | 0.29 | 0.19 | 1.51 |

Once intent to use anti-malware was normalized, the z-value was brought down to 2.35, which is well within the tolerances for normality (West et al., 1995). Standard deviation and skewness were also reduced. Response efficacy was then normalized. The z-value was brought down to 1.51, which is also well within the tolerances for normality [22]. Standard Deviation and Skewness were also reduced.

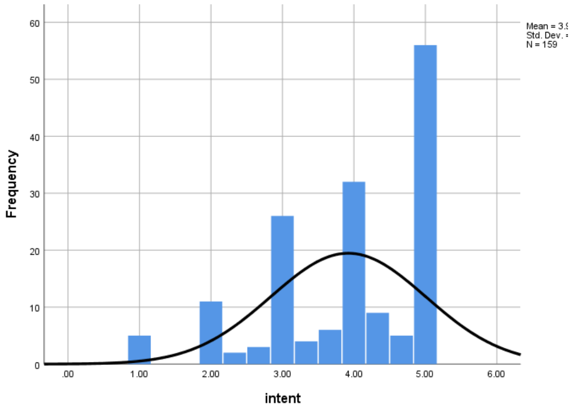

Figure 2 Intent to Use Malware Histogram, Before Transformation

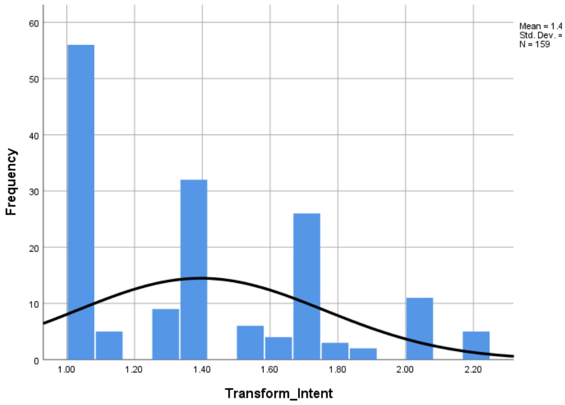

Figure 3 Intent to User Malware Histogram, After Transformation

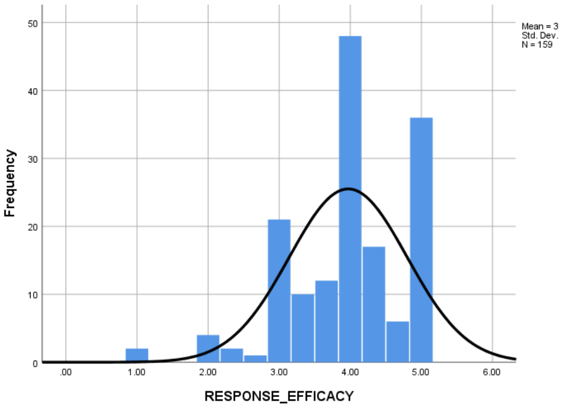

Figure 4 Response Efficacy Histogram, Before Transformation

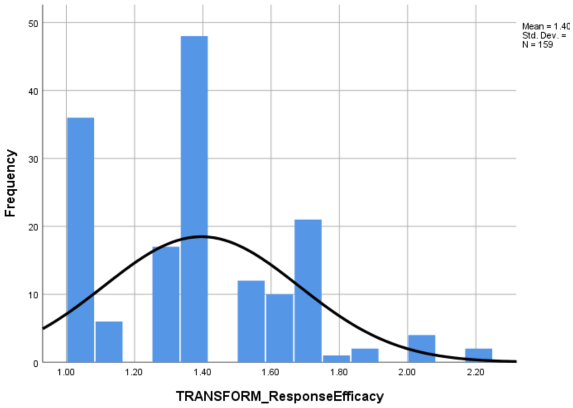

Figure 5 Response Efficacy Histogram, After Transformation

Self-efficacy met normality requirements with a z-value of -.318, which is just inside the tolerance for normality [22]. No normalization was needed for this construct. Fear met the normality requirements at 1.06, which is well within tolerance for normality [22]. No normalizations were required for this construct as well. Maladaptive rewards also met normality requirements with a value of 1.12. This value is within the tolerance for normality [22]. This construct also did not require normalization. Response costs met normality requirements with a value of 0.96. This value is well within tolerances for normality [22].

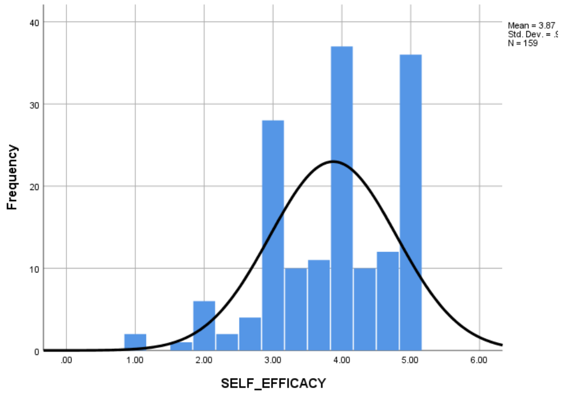

Figure 6 Self Efficacy Histogram

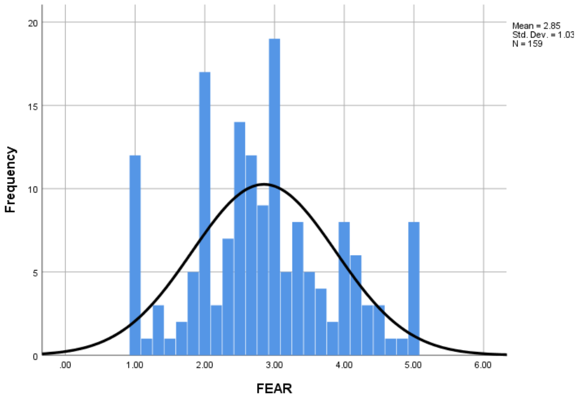

Figure 7 Fear Histogram

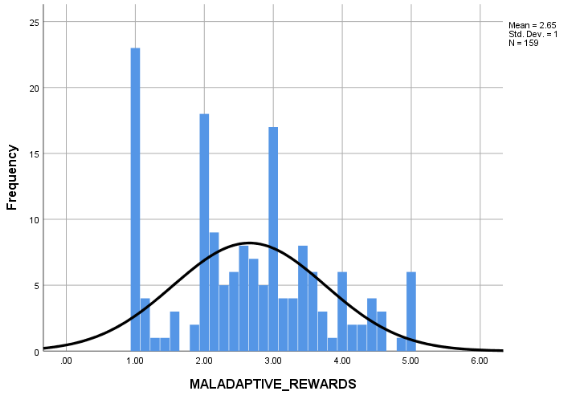

Figure 8 Maladaptive Rewards Histogram

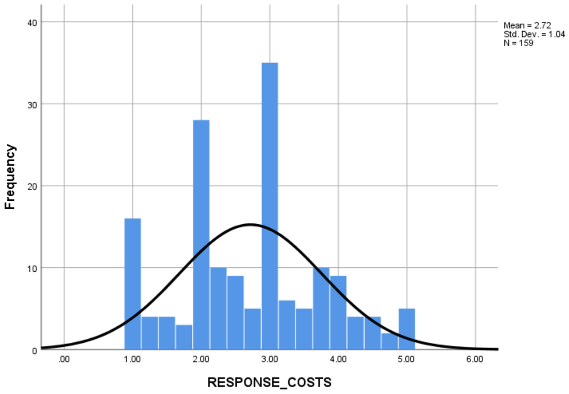

Figure 9 Response Costs Histogram

## 4.3. Full Analysis

The analysis found that several hypotheses could be supported, whereas several of the Null Hypotheses were supported (see Table 4 for a summary). This section details the testing that was done for each question and whether the null was accepted or rejected.

Table 4: Results of Data Analysis for All Hypotheses

| Hypothesis | Variable Entered | *F* | *p* | Null Accepted? |
|---|---|---|---|---|
| H1 | Fear | 12.43 | 0.001 | No |
| | DNSa | 0.04 | 0.839 | No |
| | Fear*DNS | 0.3 | 0.586 | No |
| H2 | Maladaptive Rewards | 0.03 | 0.856 | Yes |
| H3 | Response Efficacy | 125.09 | <0.001 | No |
| H4 | Self-Efficacy | 100.26 | <0.001 | No |
| H5 | Response Costs | 1.61 | 0.689 | Yes |

**Hypothesis 1:** Higher levels of Fear are related to increased usage of antivirus software when moderated by digital native status.

This hypothesis was tested using a multiple linear regression analysis using the normalized Intent to Use Anti-Malware scale as the outcome, and Fear as the predictor, moderated by Digital Native Status. The scales were standardized by subtracting the sample mean from the scores and dividing by the sample standard deviation to aid in interpretation. A cross-product was then created by multiplying the centered Fear values by digital native status, which was coded 1 for those born during or after 1980, and zero otherwise. The results are presented in Table 3. As shown, Fear was a significant predictor of the Intent to Use Ani-Malware (*F*(1,157) = 12.43, *p* = .001), explaining a minimal (7.3%) but non-random amount of the variance in the outcome. However, Digital Native Status did not add to the prediction (*F*(1,156) = 0.04, *p* = .839), nor did it moderate the effect of Fear on the outcome (*F*(1,155) = 0.30, *p* = .586). While there is not sufficient evidence to support the claim that digital native status moderates the relationship, the results support the rejection of the null hypothesis in that higher levels of Fear were significantly related to the increased usage of antivirus software.

Table 5: Linear regression on Intent to Use Anti-Malware using Fear as the predictor and Digital Native Status as a moderator

| *Step* | Variable Entered | R | $R^2$ | $R^2$ Change | F Change | df | p | β | t | p |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Fear | 0.271 | 0.073 | 0.073 | 12.43 | 1,157 | 0.001 | 0.228 | 2.03 | 0.044 |
| 2 | DNS[a] | 0.271 | 0.074 | 0.000 | 0.04 | 1,156 | 0.839 | 0.016 | 0.20 | 0.840 |
| 3 | Fear*DNS | 0.275 | 0.075 | 0.002 | 0.30 | 1,155 | 0.586 | 0.061 | 0.55 | 0.586 |

**Hypothesis 2:** Higher acceptance of maladaptive rewards does lead to higher usage of antivirus software.

This hypothesis was tested using a simple linear regression on Intent to Use Anti-Malware using Maladaptive Rewards as the predictor. As shown in Table 6, Maladaptive Rewards was not significantly predictive *(F* (1,157) = 0.03, *p* = .856). Therefore, the null hypothesis is accepted.

Table 6: Linear regression on Intent to Use Anti-Malware using Maladaptive Rewards as the predictor

| *R* | *R2* | *F* | *β* | *p* |
|---|---|---|---|---|
| 0.014 | 0.000 | 0.03 | -0.014 | 0.856 |

**Hypothesis 3:**Higher levels of response efficacy do lead to higher usage of antivirus software

This hypothesis was tested using a simple linear regression on Intent to Use Anti-Malware using Response Efficacy as the predictor. As shown in Table 7, Response Efficacy was significantly predictive *(F* (1,157) = 125.09, *p* < .001). This result supports the rejection of the null hypothesis.

Table 7: Linear regression on Intent to Use Anti-Malware using Response Efficacy as the predictor

| *R* | *R2* | *F* | *β* | *p* |
|---|---|---|---|---|
| 0.666 | 0.443 | 125.09 | 0.666 | < .001 |

**Hypothesis 4:**Higher levels of self-efficacy do lead to higher usage of antivirus software
This hypothesis was tested using a simple linear regression on Intent to Use Anti-Malware using Self-Efficacy as the predictor. As shown in Table 5, Self-Efficacy was significantly predictive *(F* (1,157) = 100.26, *p* < .001). This result supports the rejection of the null hypothesis.

Table 8: Linear regression on Intent to Use Anti-Malware using Self-Efficacy as the predictor

| *R* | *R2* | *F* | *β* | *p* |
|---|---|---|---|---|
| 0.624 | 0.39 | 100.26 | 0.624 | < .001 |

**Hypothesis 5:**Higher levels of response costs lead to higher usage of antivirus software

This hypothesis was tested using a simple linear regression on Intent to Use Anti-Malware using Response Costs as the predictor. As shown in Table 4, the Response Costs variable was not significantly predictive *(F* (1,157) = 1.61, *p* = .689). Therefore, the null hypothesis is accepted.

Table 9: Linear regression on Intent to Use Anti-Malware using Response Costs as the predictor

| *R* | *R2* | *F* | *β* | *p* |
|---|---|---|---|---|
| 0.032 | 0.001 | 1.61 | 0.032 | 0.689 |

### 4.4. Summary of the Results

First, it was found that for **Hypothesis 1: Higher levels of Fear are related to an increased usage of antivirus software** when moderated by digital native status, the construct of digital native status did not have a strong mediating effect on the relationship between Fear and increased usage of antivirus software. Multiple linear regression analysis using the normalized Intent to Use Anti-Malware scale as the outcome, and Fear as the predictor, moderated by digital native status, found that $F = 0.3$ and $p = 0.586$; $p$ is more than the alpha level of 0.05, so it is not significant.

It was also found that there was not a strong relationship between digital native status and intent to use anti-malware ($F = 0.04$ and $p = 0.839$, where $p$ is more than the alpha level of 0.05, so it is not significant). However, it was found that there is a significant relationship between Fear and usage of antivirus software ($F = 12.43$ and $p = 0.001$, where $p$ is less than the alpha level of 0.05, so it is significant), so the null hypothesis cannot be fully accepted and must be rejected.

Next, for **Hypothesis 2: Higher acceptance of maladaptive rewards does lead to higher usage of antivirus software**. It was found that maladaptive rewards did not significantly impact the intent to use antivirus. Using simple linear regression on Intent to Use Anti-Malware using maladaptive rewards as the predictor, it was found that $F = 0.03$ and $p = 0.856$, where $p$ is more than the alpha level of 0.05, so it is not significant. The null hypothesis was accepted. Maladaptive rewards is not predictive for the protective measure, intent to use anti-malware.

Next, it was found for **Hypothesis 3: Higher levels of response efficacy lead to higher usage of antivirus software**. There is a significant relationship between response efficacy and usage of antivirus software. Using simple linear regression on Intent to Use Anti-Malware using response efficacy as the predictor, it was found that $F = 125.09$ and $p = <0.001$, where $p$ is less than the alpha level of 0.05, so it is significant. The alternative hypothesis was accepted. This means that response efficacy is predictive for the protective measure of intent to use anti-malware.

For **Hypothesis 4: Higher levels of self-efficacy do lead to higher usage of antivirus software**. There was a significant relationship between self-efficacy and intent to use antivirus. Using simple linear regression on Intent to Use Anti-Malware using self-efficacy as the predictor, it was found that $F = 100.26$ and $p = <0.001$, where $p$ is less than the alpha level of 0.05, so it is significant. Since there was a significant relationship, the null hypothesis was rejected. This means that self-efficacy is also predictive for the protective measure of intent to use anti-malware.

Lastly, for **Hypothesis 5: Higher levels of response costs lead to higher usage of antivirus software**, there was not a significant relationship found. Using simple linear regression on intent to use anti-malware using response costs as the predictor, it was found that $F$ = 1.61 and $p$ = 0.689, where $p$ is more than the alpha level of 0.05, so it is not significant. In this case, the null hypothesis was accepted. This means that response costs are not predictive for the protective measure of intent to use anti-malware.

Figure 2 displays the results of the data analysis in graphical form. Overall, response efficacy, self-efficacy, and Fear showed significant relationships with the intent to use antivirus. Conversely, maladaptive rewards and response costs did not show enough of a relationship to be considered having an impact on intent to use antivirus. Digital native status also did not have a high enough of a relationship to be considered a mediating factor; however, since Fear did have an impact, the null hypothesis was not accepted for H1. The next section looks at recommendations for further research.

## 5. Recommendations for Further Research

This section looks at recommendations for further research. It details constructs and other items that have the potential to impact research on the topic. Further research should include fear manipulations, such as the fear appeals used in the Boss et al. [11] study. These manipulations have been shown to influence the results of studies on PMT, and therefore, they should be further examined. Other research has also looked at different methodologies for delivering these appeals [24]. The delivery methods of fear appeals might be something to consider in future research.

Further research should also incorporate a different mediating factor. Technology anxiety has been examined as a mediating factor in some studies using the technology acceptance model (TAM), and research has shown that such anxiety does have an impact on the decision-making process [25]. As such, it may be a factor to consider for future research. Other factors seen in research have been experience [26], security awareness [27, 37], and trust [26]. Researchers can consider a variety of variable relationships in future research.

Further research could also compare longitudinal data and one-time results. According to Boss et al. [11], fear levels may be affected by time. In one study, the fear appeal was drawn out, while in another, the fear appeal was acute and sudden [11]. In the study that used acute fear appeals, the results were more dramatic. The difference may have been due to the message’s sudden nature, making the fear appeal seem more immediate or extreme. Further studies can help clarify this phenomenon.

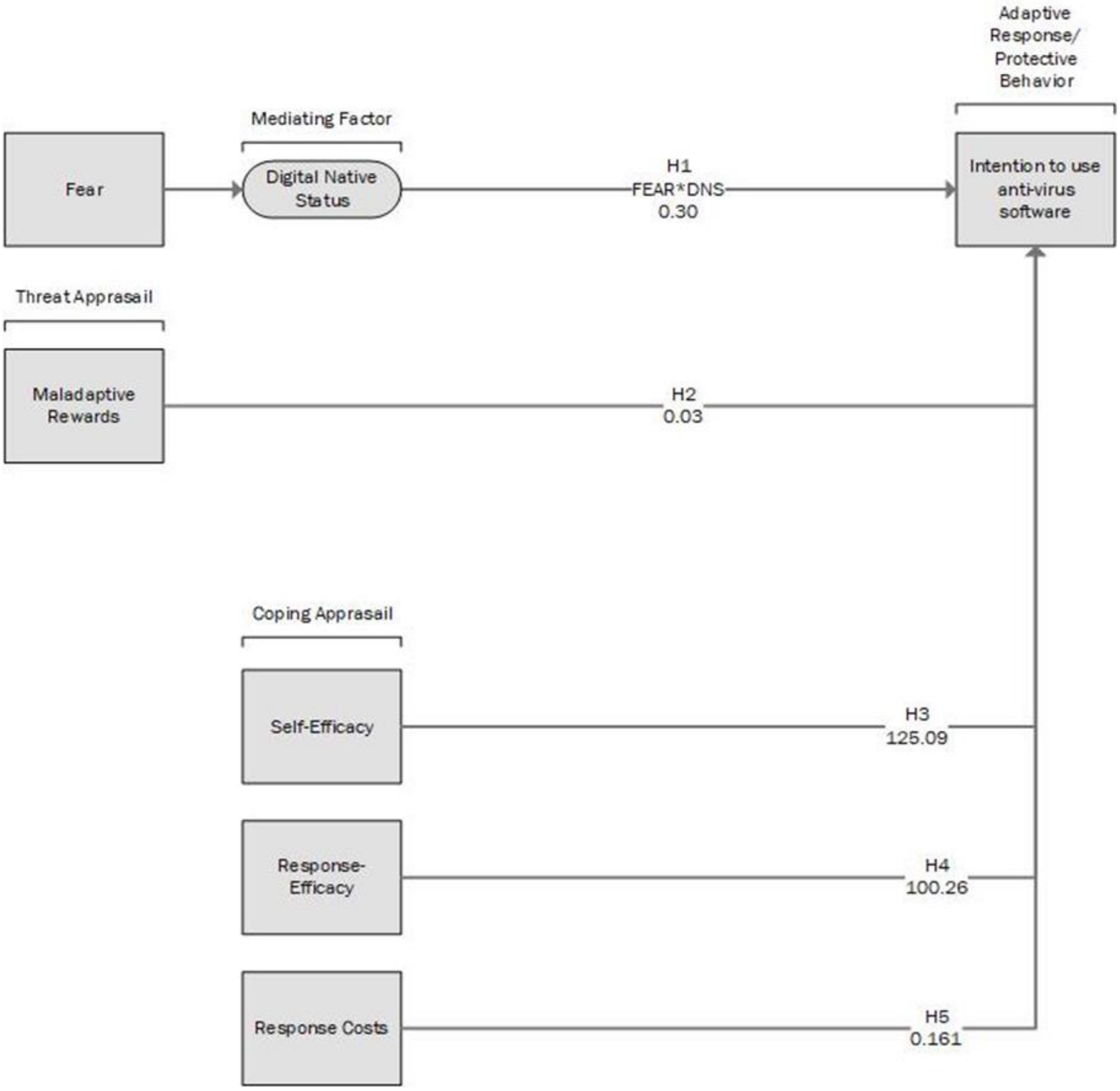

Figure 10 Results of the Data Analysis

Next, it is recommended to look at varied populations in future research. This study was limited to the United States; cultural factors could play a role in the study results. The results of this study may be limited to the United States population. Further research using different populations may net different results. The study was limited because only intent to use antivirus, not actual antivirus usage, was measured. There could be differences in the intention to use versus actual usage of antivirus software. Boss et al. [11] suggested that examining actual usage might yield more accurate results than just measuring intent. Looking at this action, an experimental approach may provide a more definitive answer on whether age or digital native status impacts PMT and antivirus usage.

Lastly, further research should examine fear appeals that vary in strength. Boss et al. [11] suggested that including fear appeals impacts the results of the study. However, no studies have examined how varying levels of Fear appeals impact behavior or how appeals that are too strong (i.e., elicit too much of a fear response) would affect the participant. This provides a possibility for future research. The next section concludes the study and provides some end-thoughts from the researcher.

## 6. CONCLUSION

This section concludes the paper. In this section, a discussion on the study, its results, and end-thoughts from the researcher are presented. End user behavior research has focused on many factors, including age. There is an assumption among some researchers that a person's age impacts their behavior in online environments. To better understand this phenomenon, the present study examined end-users' intentions to use antivirus software through the lens of digital native status. Typically, age is studied using cohort groups and not by digital native status. The intention of using digital native status was to understand if a combination of age and technological knowledge could help explain end-users' protective online behavior.

A nonexperimental survey research design and protection motivation theory were used to examine the assumptions associated with digital native status and end-users'behaviors. The present study specifically examined how digital native status mediated the relationship between Fear and intent to use antivirus software. It was found that digital native status did not mediate the relationship between Fear and intent to use antivirus software. Digital native status did not have any correlation at all with the intent to use antivirus software. While digital native status was not significantly related to fear or intent to use antivirus software, a strong positive relationship did exist between Fear and intent to use antivirus software. This significant positive relationship was consistent with previous research.

Previous research suggested that digital native status could impact decision making, as digital immigrants may not be as familiar with technology as their digital native counterparts. Technological familiarity is thought to have an impact on end-users' decision-making processes.This study found that digital native status does not seem to impact the decision-making process, previous research suggests that technology familiarity does and should be studied in more detail.

Relationships between intent to use antivirus software and other constructs in the PMT model were also examined as part of the present study. Other factors, such as self-efficacy, response-efficacy, response-costs, and maladaptive rewards, were examined to determine if these factors influenced end-users' intent to use antivirus software. It was found that self-efficacy and response-efficacy were significantly related to the intent to use antivirus software. The two constructs had a strong, positive relationship with the adaptive response of intent to use antivirus software. However, the results for the remaining constructs (i.e., maladaptive rewards and response-costs) were insignificant and not in line with previous research. The lack of a significant result may have been due to the absence of fear appeals in the present study. A more in-depth examination is needed to clarify these relationships between these factors in future research.

Overall, the present study confirmed that self-efficacy and response-efficacy are positively correlated with the intent to use antivirus software. The present study's findings also confirmed that Fear is positively correlated with the adaptive response of the intent to use antivirus software. Digital native status was not correlated with the adaptive response, however. The lack of a significant result regarding digital native status meant that the combination of age and technological familiarity does not seem to impact the decision-making process when it comes to PMT.

In practice, the present study's findings indicated that self-efficacy, response efficacy, and Fear were far more likely to contribute to better end-user Security than age, technological familiarity, maladaptive rewards, and response costs. Professionals should focus on creating training programs that bolster self-efficacy and response efficacy. It is also important to develop security controls that inform users about the threats and vulnerabilities they face when antivirus software is not used. According to Boss et al., fear appeals that properly explain a risk effectively drive end-user behavior.

The present study has left some questions about maladaptive rewards and response-costs unanswered. Most studies on PMT find that the two factors are negatively correlated to the adaptive response. However, a few studies, including this one, have found little to no relationship between the two constructs and the adaptive response. The lack of a scholarly consensus leaves the relationship between the two factors and the adaptive response unclear, at best. Further research should concentrate on these factors to provide more precise guidance for the variety of stakeholders with an interest in PMT and end-users' online security behaviors.

## CONFLICTS OF INTEREST

The authors declare no conflicts of interest.

## REFERENCES

[1] Fortes, N., & Rita, P. (2016). Privacy concerns and online purchasing behaviour: Towards an integrated model. *European Research on Management and Business Economics*, *22*, 167-176. doi:10.1016/j.iedeen.2016.04.002

[2] Bahmanziari, T., & Odom, M. D. (2015). Prospect theory and risky choice in the e-commerce setting: Evidence of a framing effect. *Academy of Accounting and Financial Studies Journal, 19*(1), 85-106. Retrieved from http://alliedacademics.org

[3] Bansal, G., & Zahedi, F. M. (2014). Trust violation and repair: The information privacy perspective. *Decision Support Systems*, *71*, 62-77. Retrieved from http://www.sciencedirect.com/science/article/pii/S0167923615000196

[4] Shackelford, S. (2012). Should your firm invest in cyber risk insurance? *Business Horizons*, *55*, 349-356. https://doi.org/10.1016/j.bushor.2012.02.004

[5] Tomlinson, E. C., & Mayer, R. C. (2009). The role of causal attribution dimensions in trust repair. *Academy of Management Review,34*(1), 85-104. doi:10.5465/AMR.2009.35713291

[6] FTC. (2015). *Privacy and security update*. Retrieved from https://www.ftc.gov/reports/privacy-data-security-update-2015

[7] Milne, G. R., Rohm, A. J., &Bahl, S. (2004). Consumers' protection of online privacy and identity. *Journal of Consumer Affairs*, *38*, 217-232. https://doi.org/10.1111/j.1745-6606.2004.tb00865.x

[8] Raine, L., & Duggan, M. (2016). *Privacy and information sharing.* Washington, DC: Pew Research Center.

[9] Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empiricalexamination of home user security behavioral intentions. *MIS Quarterly*, *34*, 613-643. doi:10.2307/25750694

[10] Jiang, M., Tsai, H. S., Cotten, S. R., Rifon, N. J., LaRose, R., &Alhabash, S. (2016).

[11] Generational differences in online safety perceptions, knowledge, and practices. *Educational Gerontology*, *42*, 621-634. doi:10.1080/03601277.2016.1205408

[12] Boss, S. R., Galletta, D. F., Lowry, B. P., Moody, G. D., &Polak, P. (2015). What do systems users have to fear? Using Fear appeals to engender threats and Fear that motivate protective security behaviors. *MIS Quarterly, 39,* 837-864. doi:10.25300/MISQ/2015/39.4.5

[13] Belanger, F., &Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*, 1017-1041. doi:10.2307/41409971

[14] Tsai, H. S., Jaing, M. J., Alabash, S., LaRose, R., Rifon, N. J., & Cotton, S. R. (2016), Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138-150. doi: http://dx.doi.org/10.1016/j.cose.2016.02.009.

[15] Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on internet scam victimization, online privacy concerns, and privacy protection behaviors. *Computers in Human Behavior, 70*,291-302. doi:10.1016/j.chb.2017.01.003

[16] Prensky, M. (2001). Digital natives, digital immigrants, part 1. *On the Horizon*, *9*(5), 1-6. https://doi.org/10.1108/10748120110424816

[17] Rogers, R. W. (1975) A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology*, *91*(1), 93-114. https://doi.org/10.1080/00223980.1975.9915803

[18] Doane, A. N., Boothe, L. G., Pearson, M. R., & Kelley, M. L. (2016). Risky electronic communication behaviors and cyberbullying victimization: An application of protection motivation theory. *Computers in Human Behavior*, *60*, 508-513. https://doi.org/10.1016/j.chb.2016.02.010

[19] Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95. doi:10.1016/j.cose.2011.10.007

[20] Herath, T., & Rao, H. (2009). Protection motivation and deterrence: A framework for security policy compliance in organizations. *European Journal of Information Systems*, *18*(2), 106-125. doi:10.1057/ejis.2009.6

[21] Gasser, U. P. J. (2008). Born digital: Understanding the first generation of digital natives. New York, NY: Basic Books.

[22] Prensky, M. (2001). Digital natives, digital immigrants, part II: Do they really think differently? *On the Horizon*, *9*(6), 1-9. https://doi.org/10.1108/10748120110424843

[23] Tabachnick, B. G., &Fidell, L. S. (2013). Using multivariate statistics (6th ed.). Upper Saddle River, NJ: Pearson Education, Inc.

[24] West, S. G., Finch, J. F., & Curran, P. J. (1995). Structural equation models with non-normal variables: problems and remedies. In R. J. Hoyle (Ed.), *Structural equation modeling: Concepts, issues and applications* (pp. 56-75). Thousand Oaks, CA: Sage Publications.

[25] Warkentin, M., Johnston, A., Walden, E., & Straub, D. (2016). Neural correlates of protection motivation for secure it behaviors: An frmi examination. *Journal of the Association for Information Systems*, *17*, 194 -215. https://doi.org/10.17705/1jais.00424

[26] Peral-Peral, B., Arenas-Gaitán, J., &Villarejo-Ramos, Á. (2015). From digital divide to psycho-digital divide: Elders and online social Networks/De la brecha digital a la brechapsico-digital: Mayores y redessociales.*Comunicar*, *23*(45), 57. https://doi.org/10.3916/c45-2015-06

[27] 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

[28] Hanus, B., & Wu, Y. A. (2016). Impact of users' security awareness on desktop security behavior: a protection motivation theory perspective. *Information Systems Management*,*33*(1),2-16. doi:10.1080/10580530.2015.1117842

[29] Gkioulos, V., Wangen, G., & Katsikas, S. (2017). User modeling validation over the security awareness of digital natives. *Future Internet*, *9*(3), 32. doi:10.3390/fi9030032

[30] Kirk, C. P., Chiagouris, L., Lala, V., & Thomas, J. D. (2015). How do digital natives and digital immigrants respond differently to interactivity online?: A model for predicting consumer attitudes and intentions to use digital information products. *Journal of Advertising Research*, *55*(1), 81-94. doi:10.2501/JAR-55-1-000-000

[31] Akçayır, G., Akçayır, M., & Dündar, H. (2016). What makes you a digital native? Is it enough to be born after 1980? *Computers in Human Behavior*, *60*, 435-440. doi:10.1016/j.chb.2016.02.089

[32] Hammouchi, H., Cherqi, O., Mezzour, G., Ghogho, M., & El Koutbi, M. (2019). Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time. Procedia Computer Science, 151, 1004-1009.

[33] Bonnett, D. G., & Wright, T. A. (2014). Cronbach's alpha reliability: Interval estimation, hypothesis testing, and sample size planning. Journal of Organizational Behavior, 36(1), 3-15. doi:10.1002/job.1960

[34] 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. https://doi.org/10.3758/brm.41.4.1149

[35] Kirschner, P. A., & De Bruyckere, P. (2017). The myths of the digital native and the multitasker. *Teaching and Teacher Education*, *67*, 135-142. doi:10.1016/j.tate.2017.06.001

[36] Marksbury, N., & Bryant, E. A. (2019). ENTER THE TWILIGHT ZONE: THE PARADOX OF THE DIGITAL NATIVE. *Issues in Information Systems*, *20*(2).

[37] Hassandoust, Farkhondeh, and Angsana A. Techatassanasoontorn. "Understanding users' information security awareness and intentions: A full nomology of protection motivation theory." *Cyber Influence and Cognitive Threats*. Academic Press, 2020. 129-143.

## AUTHORS

**Dr. Gerri Roberts** has almost 15 years of experience in the fields of Information Technology and Information Security. She has been teaching and training for over ten years. Dr. Roberts has held positions in project management, network support, application support, QA, training, and teaching. Currently, she is a full-time professor at Valencia College in Orlando, FL. She currently teaches programming, information security, networking, MS Server, computer hardware, and business information technology classes. She is also a mentor for the Cybersecurity club. She has a Ph.D. in Information Assurance and Security and several industry-recognized certifications. She is also a member of IEEE, ISC2, and CompTIA AITP.

**Dr. Shawon S. M. Rahman** is a Professor in the Department of Computer Science and Engineering at the University of Hawaii Hilo. His research interests include software engineering education, information assurance and security, web accessibility, cloud computing, software testing, and quality assurance. He has published over 125 peer-reviewed papers. Dr. Rahman is serving as the Member-at-large and Academic Advocate: Information Systems Audit and Control Association (ISACA) at the University of Hawai‘i at Hilo and Academic Advocate of the IBM Academic Initiative. He is an active member of many professional organizations, including IEEE, ACM, ASEE, ASQ, and UPE.