IT in Industry, vol. 9, no.1, 2021 Published online 19-Mar-2021

PROTECTION MOTIVATION THEORY FACTORS THAT INFLUENCE UNDERGRADUATES TO ADOPT SMARTPHONE SECURITY MEASURES

Marvin Schneider, Ph.D.[1] and Shawon Rahman, Ph.D.[2]

Abstract **- Because smartphones are ubiquitous in our society, and undergraduate students use smartphones extensively, it is necessary to understand how undergraduates can be protected from malicious hacker attacks, viruses, and malware. This quantitative study explores the influence of Protection Motivation Theory (PMT) constructs on security behaviors of undergraduate students. The primary focus of this quantitative study is to answer our primary research question: to what extent do the independent PMT variables (perceived threat severity, perceived threat vulnerability, self-efficacy, response efficacy, and response cost) explain undergraduate students' employment of smartphone security measures? The findings suggest that although all hypotheses were not supported by the analysis; however, self-efficacy and perceived threat vulnerability showed a statistically positive association with several smartphone security measures. However, none of the constructs showed a statistically significant association with using unsecured Wi-Fi in public places. The practical implications of the findings are for industry to focus on better design of smartphone hardware and software (such as antivirus apps) to protect users, and to increase self-efficacy among smartphone undergraduate users through training and education.**

Keywords **- Protection Motivation Theory, Avoidance Motivation, Smartphone Security, Fear Appeals Model, Antivirus, Self-efficacy**

1. INTRODUCTION

This study discusses whether undergraduate university students are taking the proper measures to protect undergraduate students' smartphones. Smartphones are pervasive in U.S. society, especially for university students. Specifically, according to Pew Research Center [1],the majority of the population (96%) of the United States own a smartphone. More than 50% of young adults report that each household contains three or more smartphones [2].

This section introduces the background of the smartphone security problem as it pertains to undergraduate students, and explains the foundations and constructs of protection motivation theory (PMT), a seminal theory proposed by Rogers[3]. The academic literature first applied PMT for health-related research [4]. Over time, PMT was adopted for general computer security research of students; however, there is scant literature with regards to how PMT can be applied to smartphone security practices of undergraduate students.

Jones and Chin [5] found it beneficial to study smartphone security practices as it pertains to the behavior of university undergraduate students because the students have a higher level of participation using smartphone apps than the general population, yet the students engage in dangerous smartphone security behavior [6]. Park and Drevin [7] studied undergraduate students and found that hackers are attacking the students' smartphones and installing malware on these devices as a result. Students use numerous apps, including personal banking and social media apps that present a high level of risk because of personal information and data used and shared. As a result, it becomes more necessary to protect the students' data and information from viruses and hacking attacks [8].

Because many students will be future employees of corporations both nationally and internationally, it is well reasoned to begin educating undergraduate students while the students are still in school, to apply better smartphone security practices [9]. Smartphones have become indispensable to many users, and especially so for undergraduate college students [10]. Because the smartphone has become so important and necessary for undergraduates, the protection of this device is critical for the smartphone user.

In general, what are the factors that influence security practices of undergraduate students? The research literature on smartphone security practices of undergraduate students indicates that demographic factors such as age [11] gender and class [12] influence smartphone security practices of undergraduate students. PMT factors, which include perceived threat severity,

[1]Full-Time Professor, Department of Computer Information Systems (CIS), DeVry University, New York, NY, USA
[2]Professor, Department of ComputerScience and Engineering, University of Hawaii-Hilo, Hilo, Hawaii 96720, USA.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

perceived threat vulnerability, self-efficacy, response efficacy, and response cost, are primarily applied to health-related studies [13] but have also been adopted for general computer security research of students [14]. It is not known, however, how PMT can be applied to smartphone security practices of undergraduate students.

Most of the studies on undergraduate students focused on demographics. Whereas Jones and Heinrichs [12] found that male students undertook a riskier approach to smartphone security, Mensch and Wilkie [15] discovered that male students are more likely to be compliant. Chongrui et al.[16] studied 347 undergraduate students in China and found differences between males and females in comparing cybersecurity [61] judgment and influence on actual measures taken.

Another factor included in the Mensch and Wilkie [15] study was the student's selected college major. Mensch and Wilkie's [15] research indicated that students who majored in information-technology-related subjects practiced the safest and most effective security practices. Recent studies conducted on the subject went beyond demographic factors to prove that PMT constructs can be employed to study general computer security situations of college students [4]. However, the above studies focused on general computer security, not smartphone security.

Other studies of college students focused on fear theories as applied to general computer security. The research included multiple security behaviors, including fear messages, password security practices, and filtering spam e-mails. Boss et al. [17] conducted a longitudinal and cross-sectional study on master of business administration students at select universities to study how users respond to different levels of fear messages. Warkentin et al. [18] conducted a study of threat messages of 17 college students and applied studies of PMT and fear theories.

In considering on how to state the problem as it applies to smartphone security of undergraduate students, one needs to review the prior research literature on smartphone security practices of undergraduate students. A review of the academic literature indicates that demographic factors such as age [15] as well as gender and class[12]influence smartphone security practices of undergraduate students, and that PMT factors, which include perceived threat severity, perceived threat vulnerability, self-efficacy, response efficacy, and response cost, are primarily applied to health-related studies[13] but have also been adopted for general computer security research of students [14]. According to Mousavi et al. [19], PMT might be used to discourage risky behavior but did not study smartphone security measures taken. Thus, it is not known how PMT can be applied to smartphone security practices of undergraduate students.

While looking at PMT theories, one can formulate the research question as applied to smartphone security for the population of undergraduate students. The primary research question asks: To what extent do the independent variables (perceived threat severity, perceived threat vulnerability, self-efficacy, response efficacy, and response cost) explain undergraduate students' employment of smartphone security measures?

What follows from stating the research questions is the formulation of the hypothesis. One null and one alternative hypothesis for each research question. The null hypothesis meant that there was no statistically significant relationship between each PMT construct to undergraduate students' employment of smartphone security measures. The other, alternative hypothesis postulated that there is a statistically significant relationship -- positive or negative -- between each PMT construct to undergraduate students' employment of smartphone security measures.

The remainder of the paper is divided into five sections. Section 2 presents a literature review as background on the topic of PMT as applied to various applications, such as health care, general computer security, and smartphone security. Section 3 explains the methodology used in the paper. Next, section 4 presents and discusses the study's results and explains why negative binomial regression was chosen as a model for statistical analysis. Section 5 presents and discusses future research recommendations. Finally, in section 6, the paper is summarized with research findings and conclusions.

2. LITERATURE REVIEW

This section examines the body of knowledge that relates protection motivation theory and related fear appeals theories to explain why people protect themselves. This section is divided into three subsections. The first section reviews the body of academic literature on the relevant PMT theories related to health care, general computer security, and smartphone security. The second section explains about the fear appeals model and how it relates to protection motivation theory.Finally, the third section explains why PMT was selected over the fear appeals model for this study and what are some advantages as well as limitations of using the PMT model for researching security behaviors.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

2.1. Background

PMT explains why people protect themselves. In his seminal research, Rogers in 1975 [3] first proposed PMT to explain how one uses protective actions to protect one's health. Later, Rogers in 1983 [20] added more factors to extend his theory to add constructs to explain how one can categorize the cognition factors that one uses to formulate the protective measures that one engages to combat threats. In the ensuing years, more research has been added on this topic. More recently, PMT has been applied to study health-related concerns. Jang and Yoon [21] used PMT to study how to motivate university students to decrease sodium intake, whereas Bai et al. [22] used PMT to study breast cancer survivors. With regards to the COVID-19 pandemic, Okuhara et. al [23] studied the PMT constructs as related to social lockdown and with regards to the influences of people staying at home.

PMT proposes that humans protect themselves first by recognizing the probability and severity of a threat, and secondly by trying to determine and implement an action or series of actions to cope with the threat. The main factors or constructs in PMT are perceived threat severity, perceived threat vulnerability, self-efficacy, response efficacy, response cost, perceived cost of compliance, and the perceived benefits when complying. Figure 1 depicts the model of PMT as it relates to smartphone security-related behaviors.

The first part of the PMT process is an appraisal of the threat. Lazarus [24] found out that an individual could split the appraisal process into primary and secondary appraisal processes. Lazarus [24] explained that first, the individual assesses the threat, and in the second part of the process, the individual subsequently assesses what kind of resources could be used to respond to the perceived threat situations. Keller and Block [25] later revealed that when the individual does not perceive the threat as dangerous or severe enough, then the person will not use a coping measure in addressing that threat. Anderson and Agarwal [26] later supported the research by Rogers [3], hence affirming information relating to PMT with regards to the health context. Anderson and Agarwal [26] further proposed that PMT could be extended to home computer users with regards to computer security protection motivation. Lastly, one can apply the theory to many problems and issues: personal, business, health issues such as diabetes [27], and various computer security situations [28].

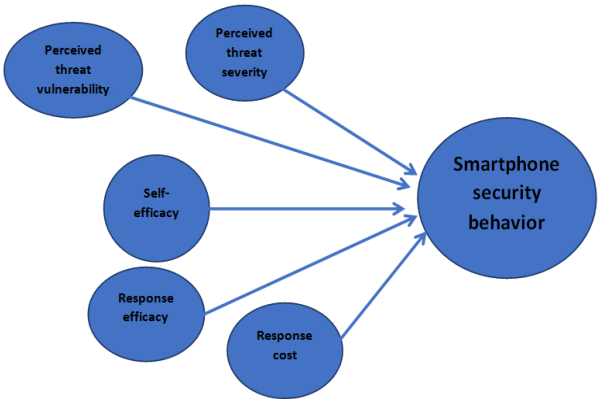

Figure 1: PMT Research Model

2.2. Fear Appeals Model as Related to Protection Motivation Theory

The fear appeals model (FAM) has similar constructs to the PMT model, but FAM tries to use fear to actively influence or motivate a person to change one's protective behavior [29]. An effective fear appeal would necessitate the individual to experience a fear perception, which would result in responding by increasing protective behavior. One of the constructs, social influence, is another factor in how people could be manipulated into experiencing fear. For security protection, FAM could be used by experimenting with different messages to the public to try to influence their protective behavior. Other researchers likewise explain that the agenda of fear appeals research is discovering ways to persuade people to embrace secure actions by presenting fear-inducing messages [17][57].

FAM can be applied to the computer or IT security, but also to other non-IT-related examples. Some of the examples are health-related. One such study by Terblanche-Smit and Terblanche [30] studied individuals that were shown advertisements regarding AIDS. FAM was used to explain if the message of the advertisements would influence user motivations and protective behavior. Meadows [31] studied if the format of the message, like narratives, could influence an undergraduate's intentions for measures to take with regards to prevention of skin cancer.

FAM is used to explain how one uses fear to take a certain action. In the study of computer security or smartphone security[58], the action is a protective action. Vos et al. [32] studied whether fear will lead male gamblers to seek help. The conceptual model presented in Figure 2 depicts how fear relates to perceived susceptibility, and how this translates to help-seeking behavioral intentions.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

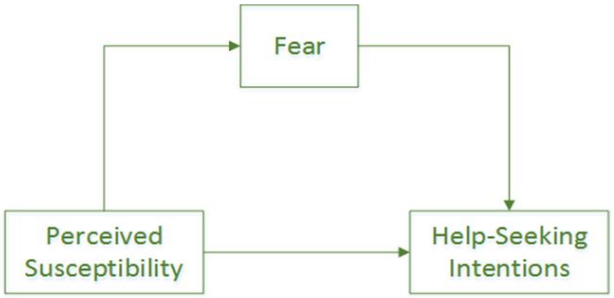

Figure 2: Avoidance Behavior and Fear versus Help-Seeking Behavioral Intentions

2.3. Why Protection Motivation Theory was Selected Over Fear Appeals Theory

PMT was selected because PMT enables the researcher to analyze the perceptions and protective behavior of the individual user. On the other hand, FAM was not selected, because the FAM theory places an emphasis on the use of fear and fear messages to actively manipulate or motivate a person to change one's protective behavior [29]. The use of fear and fear messages emphasized in FAM theory are external factors to the individual users' own perceptions [29]. Possibly, FAM could be applied for a different study to analyze how to craft messages to engage users to use smartphone protections. The research desired is to prove that the PMT constructs fit the proposed model for smartphone perceptions and behavior but does not involve creating messages for users. For this purpose, PMT provides a more suitable model than FAM.

PMT has wide-ranging applications. PMT can explain health protection, computer security, and other types of IT security, such as cloud security or smartphone security [52]. One type of computer security problem is phishing e-mail, which allows the hacker to trick or deceive by using an automated and seemingly benign method to gain access to users' protected information [56]. This problem is on desktops, bring your own devices (BYOD), [49][59] the Internet of Things (IoT) [50] [54] as well as mobile devices, such as smartphones [33]. Another, similar problem, but specific to malware on smartphones [51] is that the malware can spoof or disguise itself as a legitimate mobile app and thereby deceive the unsuspecting user [34] surveying the literature, there are limitations discussed by researchers regarding PMT. For example, not all of the PMT constructs predict well with security behaviors. Although the academic studies do not demonstrate the PMT model to be a perfect fit to explain security measures to be taken by a given population, the PMT model is useful when viewed individually for each construct. Most but not all constructs of PMT will show a statistical relationship to security behaviors. Another disadvantage that can be gleaned from the academic literature is that PMT theories might not be an exact fit for different models and cultures [35]. Finally, while PMT studies have made enviable progress for prediction of security intentions, those studies are limited in that actual behaviors were not measured or observed [17].

3. MATERIALS AND METHODS

This section describes the materials and methods that were used in this study. The section is divided into several subsections that explain various components of the methodology. The first part will present the research questions and hypothesis. The next section examines the instrumentation process and the survey instrument that is used in this study. Next will be presented validity and reliability. The next section presents sampling procedures. Finally, a brief synopsis of the data analysis will be described.

A quantitative nonexperimental research design was selected for this study. The study investigated the relationship between a set of independent variables and dependent variables. Because there were four dependent variables, the regression tests had to be run four times with the given independent variables. The independent variables were perceived as threat severity, perceived threat vulnerability, self-efficacy, response efficacy, and response cost [53][60].

The dependent variables were the actions taken to protect data and privacy on smartphones, which were changing passwords, using an antivirus app, backing up data, and using unsecured Wi-Fi in public places. Demographic data were collected and used to describe the characteristics of the sample. The theoretical framework upon which the study was based was the protection motivation theory (PMT) model, which was tested to explain the relationship of independent variables and dependent variables with statistical significance. The goal of this study was to contribute to the sparse body of literature on the effects of PMT constructs on measures that undergraduates employ to protect their smartphones. The research questions that mark this study are as follows:

3.1. Research Questions and Hypotheses

Five research questions were explored in this study. Each research question included the testing of paired null and alternative hypotheses. What follows are the research questions and their related hypotheses:

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Research Question 1: To what extent is the perception of threat severity predictive of undergraduate students' employment of smartphone security measures?

- H01: There is no statistically significant relationship between perceived threat severity to undergraduate students' employment of smartphone security measures.
- Ha1: There is a statistically significant relationship between perceived threat severity to undergraduate students' employment of smartphone security measures.

Research Question 2: To what extent is the perception of threat vulnerability predictive of undergraduate students' employment of smartphone security measures?

- H02: There is no statistically significant relationship between perceived threat vulnerability to undergraduate students' employment of smartphone security measures.
- Ha2: There is a statistically significant relationship between perceived threat vulnerability to undergraduate students' employment of smartphone security measures.

Research Question 3: To what extent is self-efficacy predictive of undergraduate students' employment of smartphone security measures?

- H03: There is no statistically significant relationship between self-efficacy to undergraduate students' employment of smartphone security measures.
- Ha3: There is a statistically significant relationship between self-efficacy to undergraduate students' employment of smartphone security measures.

Research Question 4: To what extent is response efficacy predictive of undergraduate students' employment of smartphone security measures?

- H04: There is no statistically significant relationship between response efficacy to undergraduate students' employment of smartphone security measures.
- Ha4: There isa statistically significant relationship between response efficacy to undergraduate students' employment of smartphone security measures.

Research Question 5: To what extent is response cost predictive of undergraduate students' employment of smartphone security measures?

- H05: There is no statistically significant relationship between response cost to undergraduate students' employment of smartphone security measures.
- Ha5: There is a statistically significant relationship between response cost to undergraduate students' employment of smartphone security measures.

3.2. Instrumentation

A survey instrument was used for this study. The instrument used a Likert 7-point scale from the adapted survey instrument from Cheolho et al. [14]. The survey uses a scaling that assigns a numeric value of 1–7 based on the participants' answers ranging from disagree completely to agree completely [14].

With regards to the survey instrument from Cheolho et al.[14], the word smartphone was substituted for a computer. The independent variables are the PMT constructs. Demographic information collected included age, gender, and class [12].

The following section delineates the questions that were asked as part of the survey.

3.2.1. Survey Instrument Questions

Measurement items are from [14]:

1. Are you an undergraduate student over the age of 18?
a) Yes
b) No

2. Have you used your smartphone for at least 12 months?
a) Yes
b) No

3. What is your age?

4. What is your gender?
a) Male
b) Female

5. What class are you in?
a) Freshman
b) Sophomore
c) Junior
d) Senior

Answer the items in Questions 6 through 8 using this scale:
a) DC = Disagree completely
b) D = Disagree
c) DS = Disagree somewhat
d) N = Neither agree nor disagree
e) AS = Agree somewhat
f) A = Agree
g) AC = Agree completely

6. To what extent do you agree or disagree with the following?
a) There is a chance that my personal information has been disclosed due to hacking.
b) The data on my smartphone are likely to be undermined by malicious software such as viruses.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

c) Losing data privacy as a result of hacking would be a serious problem for me.
d) Having the data in my smartphone destroyed by malicious software such as viruses would be a serious problem for me.

7. To what extent do you agree or disagree with the following?
a) I am able to protect my personal information from external threats.
b) I am able to protect the data on my smartphone from being damaged by external threats.
c) I am capable of responding to malicious software such as viruses.

8. To what extent do you agree or disagree with the following?
a) Using security technologies is effective for protecting confidential information.
b) Taking preventive measures is effective for protecting my personal information.
c) Enabling security measures on my smartphone is an effective way of preventing computer data from being damaged by malicious software such as viruses.
d) Acquiring new security technology to protect confidential information is annoying.
e) Maintaining security procedures (such as changing passwords regularly) to protect personal information is cumbersome.

9. How often have you changed your password in the past three months?

10. How often do you use an antivirus app to scan your smartphone in the past three months?

11. How often have you backed up your data in the past three months?

12. How often have you used unsecured Wi-Fi in public places in the past three months?

The survey instrument was created Cheolho et al. [14] and uses a Likert 7-point scale. The survey uses a scaling that assigns a numeric value of 1–7 based on the participants' answers ranging from disagree completely to agree completely [14]. The following section explains reliability and validity as it relates to the survey instrument.

3.2.2. Validity and Reliability

Abrahim et al. [36] explain that confirmatory factor analysis is an effective technique to test the theoretical underlining model and describes degree of item loading for each factor [37]. However, for the purposes of this study, confirmatory factor analysis was not necessary to perform, since the instrument was already validated by Cheolho et al. [14].

Reliability of the constructs was assessed using composite reliability. A value greater than 0.7 was considered satisfactory. However, for the purposes of this study, this test was not necessary to perform, since these tests were already conducted by Cheolho et al. [14].

Table 1: Model Reliability and Validity

Independent variable	CR	AVE	Independent variable				
			PV	PS	SE	RE	RC
PV	0.781	0.641	0.800				
PS	0.810	0.684	0.134†	0.827			
SE	0.891	0.735	−0.222**	0.004	0.858		
RE	0.854	0.661	−0.154†	0.274***	0.560***	0.813	
RC	0.709	0.550	0.328***	0.189†	−0.034	−0.073	0.741

Note. Diagonals represent the squared multiple correlations. CR = composite reliability, AVE =average variance extracted, PV = perceived threat vulnerability, PS = perceived threat severity, SE = self-efficacy, RE = response efficacy, RC = response cost.

†$p < 0.100$, *p < 0.050, **$p < 0.010$, ***$p < 0.001$.

As shown in Table 1, results indicate that the proposed model for independent variables achieved an appropriate level of reliability and validity. The composite reliability was greater than 0.7 for all measures. The average variance extracted was greater than 0.5 for all latent variables, which is an appropriate convergent validity

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.

For this study, the focus was on participants that were undergraduate students. Inclusion criteria requirements are for the participant to be an undergraduate student over the age of 18. Also, a participant needs to use a smartphone for at least 12 months. Exclusion criteria

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

requirements is for a participant, not an undergraduate student, and under the age of 18. Also excluded is a participant using a smartphone for less than 12 months.

One consideration was to select students from different universities. By doing so, the sample resembles the population of interest because it represented a broad selection of students. By using the platform of SurveyMonkey, this sample eliminated these concerns because the selection of the students was random and from a number of different types of universities. Additionally, the actual survey was taken outside of the school setting, allowing for greater impartiality [41].

The sample size was determined through Power analysis using G*Power was used to determine the size of the sample. Calculating a sufficient sample size is a necessary requirement for a successful academic research project. There are a variety of different methods for calculating adequate sample size. Westland [40] studied how to calculate the sample size. The calculations involve two bounds: One is a ratio of indicator variables to latent variables and the other is a function of power, minimum effect, and significance. Soper [39] used Westland's [40] calculations and developed an online calculator and determined sample size based on desired statistical power level, anticipated effect size, number of observed variables, number of latent variables, and probability level. The sample size used in this study was determined using G*Power 3 sample size calculation statistical software[38], setting the significance at 0.05, with an effect size of 0.15, for adequacy used a statistical power of .80, with the number of predictors of six, to calculate a total sample size of 84. This is the minimum sample size needed to conduct the research study. For a stronger result and smaller margin of error, a minimum of 200 respondents was used.

3.3. Data Analysis

The data included three main types of variables: categorical, interval (Likert-scale), and discrete variables. For continuous variables such as computed factor scores, the mean was used to assess the central tendency of the data and the standard deviation was used to assess the dispersion. Likert variables are treated as interval variables. According to Field [42], Likert-type variables can be treated as an interval variable. Field [42] considered Likert variables as scale type, in which each equal interval on the scale represents the equal differences of what is being measured.

Once the data was downloaded from the SurveyMonkey website, then the data analysis process began. The researcher loaded the data into IBM SPSS software for analysis. Before the analysis was conducted, the researcher ran tests on the data for completeness and accuracy. The following describes the variables that were used in the analysis (see Table 2):

Table 2: Analysis Variables

Variable	Independent/ dependent	Data type	Abbreviation
Gender	Independent	Categorical (binary)	
Class		Categorical (nominal)	
Age		Discrete (ratio)	
Perceived threat vulnerability (two items)		Interval (Likert-scale)	PV
Perceived threat severity (three items)		Interval (Likert-scale)	PS
Self-efficacy (three items)		Interval (Likert-scale)	SE
Response efficacy (three items)		Interval (Likert-scale)	RE
Response cost (two items)		Interval (Likert-scale)	RC
Changing the password within the last 3 months	Dependent	Count	
Using antiviruses within the last 3 months		Count	
Backing up data within the last 3 months		Count	
Using unsecure Wi-Fi within the last 3 months		Count	

Note. According to Field [42], Likert-type variables can be treated as an interval variable. Field [42] considered Likert variables as scale type, in which each equal interval on the scale represents the equal differences of what is being measured. The next section will present the results of the study.

4. RESULTS

The results of the data collected are presented in the following section. The section is partitioned into three subsections. The first section presents the demographics of the undergraduate student respondents to the study. The next section explains why negative binomial distribution was selected for the study, and why the other regression models needed to be rejected. The final section explains in a more thorough manner the results of the data analysis.

4.1. Demographics

The survey platform used to select the sample was SurveyMonkey. The sample of respondents was 200 randomly selected undergraduate college students that use smartphones. Inclusion criteria requirements are for the participant to be an undergraduate student over the age of 18. Also, a participant needs to use a smartphone for at

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

least 12 months. Exclusion criteria requirements for a participant is to give informed consent. If a participant does not give informed consent at the beginning of the survey, then the participant must exit the survey and is excluded from participation in the survey.

Although G*Power 3 sample size calculations obtained a result of a total sample size of 84; however, this is the minimum sample size needed to conduct the research study. For a stronger result and smaller margin of error, a minimum of 200 respondents was selected. The data collection process continued for 45 days to collect the participants' data, and then the survey was closed. There were 21 participants who did not complete the survey and no data were collected from the nonparticipating undergraduate college students.

Table 3 outlines the participant responses by age, gender, and class, and shows an even distribution.

Table 3: Study Sample Demographic Data

Demographic		n (%)
Age		30 ±10
Gender	Male	98 (41.7%)
	Female	137 (58.3%)
Class	Freshman	53 (22.8%)
	Sophomore	63 (27.2%)
	Junior	65 (28.0%)
	Senior	51 (22.0%)
N		235

Note. Of the 235 participants, three did not specify which class they were in.

4.2. Preliminary Analysis

In the preliminary analysis phase, Mahalanobis distance was used to identify outliers in the data. It is a multidimensional technique to assess how many standard deviations away a point is from the mean of the distribution.The study sample included 249 participants. Mahalanobis distance identified 14 participants as outliers. These 14 observations were excluded from the analysis. Thus, the final study sample included 235 participants. The average age of the study participants was 30 ±10 years. More women were included in the study sample (n = 137, 58.3%) compared to men (n = 98, 41.7%). Various classes were equally represented in the study sample (Table 4).

Table 4: Model Fit Thresholds

Measure	Threshold
Cmin/df	< 3 = good, < 5 = acceptable
Tucker–Lewis index	> 0.95 = excellent, > 0.9 = good
Comparative fit index	> 0.95 = excellent, > 0.9 = good
Standardized root mean square residual	< 0.08
Root mean square error of approximation	< 0.05 = good, 0.05–0.1 = moderate
Root mean square error of approximation 90% confidence interval	< 0.1

Table 5 presents descriptive statistics of the independent variables to include mean, median, and standard deviation.

Table 5: Independent Variable Descriptive Statistics

Variable	Mean	Median	SD	Range	Min	Max
Perceived threat vulnerability (PV)	4.27	4.50	1.623	6.00	1.00	7.00
Perceived threat severity (PS)	5.73	6.00	1.372	6.00	1.00	7.00
Self-efficacy (SE)	4.67	5.00	1.367	6.00	1.00	7.00
Response efficacy (RE)	5.60	6.00	1.004	5.00	2.00	7.00
Response cost (RC)	4.58	4.50	1.555	6.00	1.00	7.00

The highest average scores were observed for perceived threat severity (5.73 ±1.372) and response efficacy (5.6 ±1.004) and the lowest average score was observed for perceived threat vulnerability (4.27 ±1.623).

4.3. Full Analysis

The current section provides reasons for choosing negative binomial regression as the main statistical modeling tool and explains why other regression models were not suitable for the analysis. Before data was collected, it was assumed that perhaps linear regression modeling could be used. However, as explained below the over-dispersion of the data, caused this idea to be rejected.

Linear regression was considered for statistical modeling of the collected data in this study but was rejected. The reason is that linear regression assumes that the dependent variables need to be continuous; however, in this study the dependent variables were found to be count data. Since the linear regression model assumptions were violated, therefore this model could not be used. Count data can better fit other models, such as Poisson or negative binomial models [44]. Next, Poisson regression model was considered, but was rejected. Çetinkaya and Kaçıranlar [43] explained that Poisson regression is one

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

possible method to conduct statistical analysis on count data; however, there are other assumptions that need to be satisfied before Poisson can be considered. A formal test, such as Chi-square test, needs to be run to determine whether the data distribution for DV fits a Poisson distribution or not. Chi-square test is one method to show that the mean is significantly different from the variance for the dependent variables. There is concern for overdispersion, if the variance exceeds the mean. On the other hand, if variance is less than mean, it could signify less variation of the data or underdispersion [45].

Chi-square tests were run in a Poisson multiple regression analysis to formally test whether the data distribution fits a Poisson distribution or not. The findings were: changing password (DV1; $p = 0.916$), using an antivirus app (DV02; $p < .001$), backing up data (DV03; $p < .001$), and Wi-Fi in public places (DV04; $p < .001$). Since the P values for DV2, DV3, and DV4 are < .05, this indicates that the mean is significantly different from the variance for DV2, DV3, and DV4. Because the results of the Chi-square test determined for DV2, DV3, and DV4 that the mean is significantly different from the variance for the dependent variables; therefore, Poisson regression can be rejected as a possible model fit to the data.

Negative binomial regression provides for a best fit for assumptions for DV2, DV3, and DV4, but not for DV1. This conclusion was determined after running tests for each of the four DVs: Chi-square test, Goodness of Fit test, and tests to calculate the dispersion factor, theta. Chi-square tests were run in a negative binomial multiple regression analysis to formally test whether the data distribution fits a negative binomial distribution or not. The findings from the Chi-square tests were: changing password (DV1; $p = 0.999$), using an antivirus app (DV02; $p < .001$), backing up data (DV03; $p < .001$), and Wi-Fi in public places (DV04; $p < .001$). In addition, the dispersion factor, theta, was calculated for changing passwords (DV1; $\Theta = 3.57$, $p = 0.0417$), using an antivirus app (DV2; $\Theta = 0.2422$, $p = 0.8496$), backing up data (DV3; $\Theta = 0.2642$, $p = 0.2760$), Wi-Fi in public places (DV4; $\Theta = 0.3994$, $p = 0.1754$). For DV2, DV3, DV4, there is significant dispersion of data, signifying that a negative binomial model can be used; however, the results for DV1 signify that neither Poisson nor negative binomial regression provides any useful, predictive value.

4.4. Summary of the Results

This section presents the results of the hypothesis tests. What follows is a presentation of the hypothesis testing results, which were adjusted for age, gender, and class. Negative binomial regression analysis was used for hypothesis testing. B is number of failures to get number of successes in trials. For negative binomial regression analysis, β represents log odds of omnibus test.

The omnibus test asked the following question: To what extent are the independent variables (perceived threat severity, perceived threat vulnerability, self-efficacy, response efficacy, and response cost) associated with undergraduate students' employment of smartphone security measures? The omnibus hypotheses were as follows:

H0: There is no statistically significant association between the independent variables (perceived threat severity, perceived threat vulnerability, self-efficacy, response efficacy, and response cost) and students' employment of smartphone security measures (i.e., $\beta 1 = \beta 2 = \beta k = 0$).

HA: There is a statistically significant association between the independent variables (perceived threat severity, perceived threat vulnerability, self-efficacy, response efficacy, and response cost) and students' employment of smartphone security measures (i.e., at least one of the regression coefficients $\beta k \neq 0$).

Negative binomial regression analysis showed that the null hypothesis can be rejected as various independent variables showed a statistically significant association with at least one of the four dependent variables. SE showed a statistically significant positive association with using an antivirus app (DV2). SE ($OR = 1.293$, $p < 0.05$) and RC ($OR = 0.777$, $p < 0.05$) showed a statistically significant association with backing up data (DV3). None of the independent variables showed a statistically significant association with using unsecured Wi-Fi in public places (DV4). The previous results suggest that at least one of the β is significantly different from 0, which explains why the null hypothesis for the omnibus test was rejected.

Hypothesis Testing Results of Negative Binomial Regression for Research Subquestions

Research Subquestion 1. Research Subquestion 1 was as follows: To what extent is the perception of threat vulnerability predictive of undergraduate students' employment of smartphone security measures? The hypotheses were as follows:

H10: There is no statistically significant relationship between perceived threat vulnerability to undergraduate students' employment of smartphone security measures.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

H1A: There is a statistically significant relationship between perceived threat vulnerability to undergraduate students' employment of smartphone security measures.

Negative binomial regression analysis showed that the null hypothesis for Research Subquestion 1 can be rejected as PV showed a statistically significant negative association with using an antivirus app to scan the smartphone files within the last three months (OR = 0.813, p = 0.05). For each one-unit increase in PV, the odds of having used an antivirus app within the last three months decreased by 18.7% holding the remaining variables constant. In other words, individuals who perceive themselves as more vulnerable are less likely to have used an antivirus app within the last three months.

Research Subquestion 2. Research Subquestion 2 was as follows: To what extent is the perception of threat severity predictive of undergraduate students' employment of smartphone security measures? The hypotheses were as follows:

H20: There is no statistically significant relationship between perceived threat severity and undergraduate students' employment of smartphone security measures.
H2A: There is a statistically significant relationship between perceived threat severity and undergraduate students' employment of smartphone security measures.

Negative binomial regression analysis showed that the null hypothesis for Research Subquestion 2 can be accepted as PS did not show a statistically significant association with any of the three remaining dependent variables. It did not show a statistically significant association with DV2 (OR = 1.066, p > 0.05), DV3 (OR = 0.864, p > 0.05), or DV4 (OR = 0.966, p > 0.05).

Research Subquestion 3. Research Subquestion 3 was as follows: To what extent is self-efficacy predictive of undergraduate students' employment of smartphone security measures? The hypotheses were as follows:

H30: There is no statistically significant relationship between self-efficacy and undergraduate students' employment of smartphone security measures.

H3A: There is a statistically significant relationship between self-efficacy and undergraduate students' employment of smartphone security measures.

Negative binomial regression analysis showed that the null hypothesis for Research Subquestion 3 can be rejected as SE showed a statistically significant positive association with two of the dependent variables related to employment of smartphone security measures (DV2, and DV3). SE showed a statistically significant positive association with DV2 or using an antivirus app within the last three months (OR = 1.826, p < 0.001). For each one-unit increase in self-efficacy score, the odds of having used an antivirus app within the last three months increased by 82.6%, holding the remaining variables in the model constant. In other words, participants who are more confident in their self-efficacy were more likely to have used an antivirus app to scan their smartphone for viruses within the last three months. Finally, SE showed a statistically significant positive association with DV3 or backing up the data within the last three months (OR = 1.293, p < 0.05). For each one-unit increase in self-efficacy score, the odds of having backed up the data within the last three months increase by 29.3% holding the remaining variables in the model constant; that is participants who are more confident in their self-efficacy were more likely to have backed up the data within the last three months.

Research Subquestion 4. Research Subquestion 4 was as follows: To what extent is response efficacy predictive of undergraduate students' employment of smartphone security measures? The hypotheses were as follows:

H40: There is no statistically significant relationship between response efficacy and undergraduate students' employment of smartphone security measures.

H4A: There is a statistically significant relationship between response efficacy and undergraduate students' employment of smartphone security measures.

Statistical analysis using negative binomial regression showed that the null hypothesis for Research Subquestion 4 can be accepted as RE did not show a statistically significant association with DV2 (OR = 1.231, p > 0.05), DV3 (OR = 0.784, p > 0.05) or DV4 (OR = 0.948, p > 0.05).

Research Subquestion 5. Research Subquestion 5 was as follows: To what extent is response cost predictive of undergraduate students' employment of smartphone security measures? The hypotheses were as follows:

H50: There is no statistically significant relationship between response cost and undergraduate students' employment of smartphone security measures.

H5A: There is a statistically significant relationship between response cost and undergraduate students' employment of smartphone security measures.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Negative binomial regression analysis showed that the null hypothesis for Research Subquestion 5 can be rejected as RC showed a statistically significant negative association with backing up the data within the last three months (OR = 0.777, $p < 0.05$; i.e., for each one-unit increase in RC, the odds of having backed up the data within the last three months decrease by 22.3%, holding the remaining variables constant; that is, individuals who perceive security measures as annoying are less likely to have backed up their data within the last three months). Table 6 presents the summary of the model results.

Table 6: Summary of Results of Research Subquestion Alternate Hypotheses Based on Significance

Research Subquestion Alternate Hypothesis	Accepted/ rejected	Odds ratio (OR) statistic	*p* value
1. There is a statistically significant association between perceived threat vulnerability and undergraduate students' employment of smartphone security measures.	Reject	DV2 (OR = 0.813)	DV2 ($p = 0.05$)
2. There is a statistically significant association between perceived threat severity and undergraduate students' employment of smartphone security measures.	Accept	DV2 (OR = 1.066) DV3 (OR = 0.864) DV4 (OR = 0.966)	DV2 ($p > 0.05$) DV3 ($p > 0.05$) DV4 ($p > 0.05$)
3. There is a statistically significant association between perceived self-efficacy and undergraduate students' employment of smartphone security measures.	Reject	DV2 (OR = 1.826) DV3 (OR = 1.293)	DV2 ($p < 0.001$) DV3 ($p < 0.05$)
4. There is a statistically significant association between perceived response efficacy and undergraduate students' employment of smartphone security measures.	Accept	DV2 (OR = 1.231) DV3 (OR = 0.784) DV4 (OR = 0.948)	DV2 ($p > 0.05$) DV3 ($p > 0.05$) DV4 ($p > 0.05$)
5. There is a statistically significant association between perceived response cost and undergraduate students' employment of smartphone security measures.	Reject	DV3 (OR = 0.777)	DV3 ($p < 0.05$)

Note. DV2 = Dependent Variable 2, using an antivirus app; DV3 = Dependent Variable 3, backing up data; DV4 = Dependent Variable 4, using unsecured Wi-Fi in public places.

5. RECOMMENDATIONS FOR FURTHER RESEARCH

This section lists and explains recommendations that can be used for further academic research. Further research into smartphone security is a collaborative effort among academic researchers. Technologists and researchers can work together to create a better-designed smartphone that would be safer for undergraduate students to use. Academics and marketers can create better training materials and more effective training programs to better inform students. Although Posey et al. [47] emphasized better training programs for employees working in companies, similar security awareness and training programs could positively benefit students. Dang-Pham and Pittayachawan [46] studied university students in Australia and found that recurrent training programs can help the students maintain the confidence and self-efficacy needed to cope with threats of viruses and malware on their smartphones.

While threats of viruses and hacking may never be eliminated, through the efforts of technologists and researchers, these threats could be greatly reduced. The following are recommendations for future research:

- Future researchers should consider the implications of other mobile devices, such as iPads, Windows mobile devices, and other handheld portable devices, and not only smartphones.
- Our research focused on students in the United States. Future research could focus on other countries. Additionally, researchers might compare students in different regions of the country. Another grouping distinction might be to compare students of public colleges versus private colleges, and colleges of different tiers.
- Because data backup of smartphones is to cloud-based locations, researchers can study smartphone security as it relates to data integrity of data backed up and stored in the cloud[55].
- Researchers can explore how social media can influence smartphone perceptions, and how this might affect the PMT constructs, either as a mediator or as a separate construct. This would further advance the theories of Yoon and Kim[48]as to how social influences contribute to undergraduate students' smartphone perceptions.
- This research focused on smartphones but did not distinguish between Android and Apple smartphones. Understanding differences could better aid in product design and training of university students.
- Although our research focused on PMT constructs, researchers can further explore how demographics may influence smartphone perceptions and resultant behavior among university undergraduate students. The research could further advance the theories of Chin et al. [11] with regards to age, and Jones & Heinrichs [12] to gender and class.

The smartphone has been used by consumers for more than 10 years. When the smartphone was first developed, smartphones did not inherently contain malware or viruses. As a necessity, researchers needed to import viruses from desktop computers to smartphones in order to study threats. Research on smartphone protection has come far; however, there is still more to discover to help smartphone users better implement measures to protect their smartphones.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

6. CONCLUSION

The conclusion of this paper is presented in this section. This section presents the results of the study and the concluding reflections of the researcher. This study was designed so that the researcher can investigate undergraduate student measures employed for smartphone security. More specifically, PMT factors were investigated to relate to the smartphone security measures employed by undergraduate university students. The population delineated in this study included university undergraduate students over 18 years old. The student participants need to have a smartphone experience for at least 12 months. PMT served as the theoretical foundation for this study.

The benefits of PMT were demonstrated through the constructs including perceived threat severity, perceived threat vulnerability, self-efficacy, response efficacy, and response cost, which was statistically analyzed and associated with smartphone security behaviors: smartphone password changes, antivirus apps to clean viruses from a smartphone, smartphone data backup, and using unsecured Wi-Fi in public places.

The core research question asked why students do not adopt proper security measures to protect their smartphones. The study discovered that although the entire PMT model does not entirely explain these reasons, specific constructs had strong implications for influencing smartphone security measures. Specifically, self-efficacy, perceived threat vulnerability, and response cost influenced the adoption of smartphone security measures among undergraduate students. Perceived threat severity and response efficacy did not influence the adoption of smartphone security measures.

Self-efficacy influenced the adoption of smartphone security measures to a higher extent compared to the other two variables (perceived threat vulnerability and response cost) as it showed a statistically significant association with two of the security measures (using an antivirus app within the last three months and backing up the data within the last three months). Self-efficacy showed a statistically positive association with the employment of such measures; that is, higher self-efficacy is associated with a higher frequency of employing smartphone security measures. The other two factors (response cost and perceived threat vulnerability) only influenced one measure each (backing up the data within the last three months and using an antivirus app within the last three months, respectively).

Moreover, none of the five factors (independent variables) included in the study seemed to influence the use of unsecured Wi-Fi within the last three months. The findings of this paper contribute to academic research on smartphone security perceptions and how these perceptions can influence proper measures to protect one's smartphone.

REFERENCES

[1] Pew Research Center. (2018). Mobile fact sheet. www.pewinternet.org/fact-sheet/mobile/

[2] Pew Research Center. (2017). A third of Americans live in a household with three or more smartphones.www.pewresearch.org/fact-tank/2017/05/25/a-thirdof-americans-live-in-a-household-with-three-or-more-smartphones/

[3] Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93–114. doi.10.1080/00223980.1975.9915803

[4] Hanus, B., & Wu, Y. (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

[5] Jones, B. H., & Chin, A. G. (2015). On the efficacy of smartphone security: A critical analysis of modifications in business students' practices over time. International Journal of Information Management, 35, 561–571. doi.10.1016/j.ijinfomgt.2015.06.003

[6] Sharma, R., & Madhusudhan, M. (2017). Use of mobile devices by library and information science students in central universities of Uttar Pradesh. DESIDOC Journal of Library & Information Technology, 37, 293–302. doi.10.14429/djlit.37.4.11505

[7] Park, M., & Drevin, L. (2016). An investigation into the security behaviour of tertiary students regarding mobile device security. In CONF-IRM 2016 proceedings (Paper 63). aisel.aisnet.org/

[8] Kim, E. B. (2014). Recommendations for information security awareness training for college students. Information Managementand Computer Security, 22(1), 115–126. doi.10.1108/IMCS-01-2013-0005

[9] Raghavan, V., & Xiaoni, Z. (2017). An integrative model of managing software security during information systems development. Journal of International Technology & Information Management, 26(4), 83–109. pdfs.semanticscholar.org

[10] Konan, N., Durmuş, E., Bakır, A. A., & Türkoğlu, D. (2018). The relationship between smartphone addiction and perceived social support of university students' [sic]. International Online Journal of Educational Sciences,10(5), 244–259. doi.org/10.15345/iojes.2018.05.016

[11] Chin, A. G., Etudo, U., & Harris, M. A. (2016). On mobile device security practices and training efficacy: An empirical study. Informatics in Education, 15(2), 235–252. doi.org/10.15388/infedu.2016.12

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

[12] Jones, B. H., & Heinrichs, L. R. (2012). Do business students practice smartphone security? The Journal of Computer Information Systems, 53, 22–30. doi.org/10.1080/08874417.2012.11645611

[13] 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

[14] Cheolho, Y., Jae-Won, H., & Kim, R. (2012). Exploring factors that influence students' behaviors in information security. Journal of Information Systems Education, 23, 407–415. EBSCOhost database. (Accession No. 89084300)

[15] Mensch, S., & Wilkie, L. (2011). Information security activities of college students: An exploratory study. Academy of Information and Management Sciences Journal, 14, 91–116. www.abacademies.org

[16] Chongrui, L., Zhiqiang, W., Cong, W., Yan, L., & Hongjie, W. (2020, April). The Status Quo and Effects of Undergraduate Students' Cybersecurity Judgment: A study in China. Journal of Physics: Conference Series (Vol. 1486, p. 022011).

[17] Boss, S. R., Galletta, D. F., Lowry, P. B., 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. Management Information Systems [MIS] Quarterly, 39, 837–864. misq.org

[18] Warkentin, M., Walden, E., Johnston, A. C., & Straub, D. W. (2016). Neural correlates of protection motivation for secure IT behaviors: An fMRI examination. Journal of The Association for Information Systems, 17, 194–215.doi.org/10.17705/1jais.00424

[19] Mousavi, R., Chen, R., Kim, D. J., & Chen, K. (2020). Effectiveness of privacy assurance mechanisms in users' privacy protection on social networking sites from the perspective of protection motivation theory. Decision Support Systems, 135, 113323. doi: 10.1016/j.dss.2020.113323.

[20] Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo & R. Petty (Eds.), Social psychophysiology (pp. 153–177). New York, NY: Guilford Press.

[21] Jang, S. H., & Yoon, E. (2016). A comparative study on the awareness of health risks and the risk reduction measures related to sodium intake between female and male university students in Busan and Gyeongnam: An application of protection motivation theory. Korean Journal of Food & Cookery Science, 32(1), 136–146. doi.10.9724/kfcs.2016.32.1.136

[22] Bai, Y., Liu, Q., Chen, X., Gao, Y., Gong, H., Tan, X., Zhang, M., Tuo, J., Zhang, Y., Xiang, Q., Deng, F., Liu, G. (2018). Protection motivation theory in predicting intention to receive cervical cancer screening in rural Chinese women. Psycho-Oncology, 27, 442–449. doi.org/10.1002/pon.4510

[23] Okuhara, T., Okada, H., & Kiuchi, T. (2020). Predictors of staying at home during the COVID-19 pandemic and social lockdown based on protection motivation theory: A cross-sectional study in Japan. Healthcare (Basel), 8(4), 475. doi:10.3390/healthcare8040475

[24] Lazarus, R. S. (1991). Progress on a cognitive-motivational-relational theory of emotion. American Psychologist, 46, 819–834. doi.org/10.1037/0003-066x.46.8.819

[25] Keller, P. A., & Block, L. G. (1996). Increasing the persuasiveness of fear appeals: The effect of arousal and elaboration. Journal of Consumer Research, 22, 448–459. doi.org/10.1086/209461

[26] Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. Management Information Systems [MIS] Quarterly, 34, 613–643. doi.10.2307/25750694

[27] Morowatisharifabad, M. A., Abdolkarimi, M., Asadpour, M., Fathollahi, M. S., & Balaee, P. (2018). The predictive effects of protection motivation theory on intention and behaviour of physical activity in patients with type 2 diabetes. Open Access Macedonian Journal of Medical Sciences, 6, 709–714. doi.org/10.3889/oamjms.2018.119

[28] Rohani, H., Bidkhori, M., Eslami, A. A., Sadeghi, E., & Sadeghi, A. (2018). Psychological factors of healthful diet promotion among diabetics: An application of health action process approach. Electronic Physician, 10, 6647–6654. doi.org/10.19082/6647

[29] Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. Management Information Systems [MIS] Quarterly, 34, 549–566. misq.org

[30] Terblanche-Smit, M., & Terblanche, N. S. (2010). Race and attitude formation in HIV/Aids fear advertising. Journal of Business Research, 63(2), 121-125.

[31] Zhang Meadows, C. (2020). The Effects of Fear Appeals and Message Format on Promoting Skin Cancer Prevention Behaviors among College Students. Societies, 10(1), 21.

[32] Vos, S., Crouch, R., Quester, P., & Ilicic, J. (2017). Examining the effectiveness of fear appeals in prompting help-seeking: The case of at-risk gamblers. Psychology & Marketing, 34, 648–660. doi.org/10.1002/mar.21012

[33] Arlitsch, K., & Edelman, A. (2014). Staying safe: Cyber security for people and organizations. Journal of Library Administration, 54(1), 46–56. doi.10.1080/01930826.2014.893116

[34] Banuri, H., Alam, M., Khan, S., Manzoor, J., Ali, B., Khan, Y., & Zhang, X. (2012). An Android runtime security policy enforcement framework. Personal and Ubiquitous Computing, 16, 631–641. doi.10.1007/s00779-011-0437-6

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

[36] Abrahim S., Mir, B. A., Suhara, H., Mohamed, F. A., & Sato, M. (2019). Structural equation modeling and confirmatory factor analysis of social media use and education. International Journal of Educational Technology in Higher Education, 16, Art. 32.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

doi.org/10.1186/s41239-019-0157-y
[37] Byrne, B. M. (2010). Structural equation modeling with AMOS: Basic concepts, applications, and programming. New York, NY: Routledge
[38] Faul, F., Erdfelder, E., Lang, A.-G., & Buchner, A. (2007). G*Power 3: A flexible statistical power analysis program for the social, behavioral, and biomedical sciences. Behavior Research Methods, 39, 175–191. doi.10.3758/bf03193146
[39] Soper, D. (n.d.). Free statistics calculators: Home. www.danielsoper.com/statcalc/default.aspx
[40] Westland, J. C. (2010). Lower bounds on sample size in structural equation modeling. ElectronicCommerce Research and Applications, 9, 476–487. doi.10.1016/j.elerap.2010.07.003
[41] Wolf, E. J., Harrington, K. M., Clark, S. L., & Miller, M. W. (2013). Sample size requirements for structural equation models: An evaluation of power, bias, and solution propriety. Educational and Psychological Measurement, 73(6), 913–934. doi.10.1177/0013164413495237
[42] Field, A. (2009). Discovering statistics using SPSS (3rd ed.). Thousand Oaks, CA: Sage.
[43] Çetinkaya, M. K., & Kaçıranlar, S. (2019). Improved two-parameter estimators for the negative binomial and Poisson regression models. Journal of Statistical Computation & Simulation, 89, 2645–2660. doi.org/10.1080/00949655.2019.1628235
[44] Fox, J. (2016). Applied regression analysis and generalized linear models (3rd ed.). Thousand Oaks, CA: Sage.
[45] Hilbe, J. (2014). Modeling count data. New York, NY: Cambridge University Press.
[46] Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach. Computers & Security,48, 281–297. doi.org/10.1016/j.cose.2014.11.002
[47] Posey, C., Roberts, T. L., & Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. Journal of Management Information Systems, 32, 179–214. doi.10.1080/07421222.2015.1138374
[48] Yoon, C., & Kim, H. (2013). Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms. Information Technology & People, 26, 401–419. doi.10.1108/ITP-12-2012-0147
[49] Okonofua, Henry and Rahman, Shawon; "Cybersecurity: An Analysis of the Protection Mechanisms in a Cloud-centered Environment"; 2nd IEEE International Symposium on Security, Privacy and Trust in Internet of Things (SPTIoT 2018), August 1-3, 2018, New York, USA
[50] Rahman, Shawon and May, Yvonne; "Wireless Security Vulnerabilities and Countermeasures for an Airport"; 30th International Conference on Computers and Their Applications (CATA-2015), March 9-11, 2015, Waikiki Beach Marriott Resort & Spa, Honolulu, Hawaii, USA
[51] Rahman, Shawon and Jackson, George, Jr; "Survey of Malware Threats and Defense in Smartphones Applications"; The 2nd National Computing Colleges Conference (NC3 2017), February 22-23, 2017, Hail, Saudi Arabia.
[52] Faizi, Salman and Rahman, Shawon;" Securing Cloud Computing Through IT Governance"; International Journal of Information Technology in Industry (ITII), vol. 7, no.1, 2019, Pages: 1-14
[53] Jackson, George, and Rahman, Shawon; "Exploring Challenges and Opportunities in Cybersecurity Risk and Threat Communications related to the Medical Internet of Things (MIoT)", International Journal of Network Security & Its Applications (IJNSA), Vol. 11, No. 4, July 2019
[54] Dharmalingam, Vaishnavi and Rahman, Shawon; "Towards Cloud of Things from Internet of Things"; International Journal of Engineering and Technology, Vol. 7, No 4.6, 2018, Pages: 112-116
[55] Opala, Omondi John; Rahman, Shawon; and Alelaiwi, Abdulhameed; "The Influence of Information Security on the Adoption of Cloud computing: An Exploratory Analysis", International Journal of Computer Networks & Communications (IJCNC), Vol. 7, No. 4, July 2015
[56] Rader, A., Marc and Rahman, Syed (Shawon); "Exploring Historical and Emerging Phishing Techniques and Mitigating the Associated Security Risks"; International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.4, July 2013
[57] Faizi, Salman and Rahman, Shawon; "Effect of Fear on Behavioral Intention to Comply"; ACM the 4th International Conference on Information System and Data Mining (ICISDM2020), May 15-17, 2020, Hilo, Hawaii, USA
[58] Faizi, Salman and Rahman, Shawon; "Choosing the Best-fit Lifecycle Framework while Addressing Functionality and Security Issues"; 34th International Conference on Computers and Their Applications (CATA-2019), March 18-20, 2019, Waikiki Beach Marriott Resort & Spa, Honolulu, Hawaii, USA
[59] Okonofua, Henry and Rahman, Shawon; "Evaluating the Risk Management Plan and Addressing Factors for Successes in Government Agencies"; 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications (IEEE TrustCom-18), August 1-3, 2018, New York, USA
[60] Jackson, George and Rahman, Shawon ; "Security Governance, Management, and Strategic Alignment via Capabilities"; IEEE 4th Annual Conference on Computation Science and Computational Intelligence (CSCI), The 2017 International Symposium on Cyber Warfare, Cyber Defense and Security (ISCW), Dec 14-16, 2017, Las Vegas, Nevada, USA
[61] Loukaka, Alain and Rahman, Shawon; "Discovering New Cyber Protection Approaches From a Security Professional Prospective"; International Journal of Computer Networks & Communications (IJCNC) Vol.9, No.4, July 2017

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

ACKNOWLEDGMENT

Special thanks to Dr. Bruce Chapman for his invaluable advice, support, and encouragement to help complete this research project. Dr. Chapman is the Academic Director of Research at Capella University.

CONFLICTS OF INTEREST

The authors declare no conflicts of interest.

AUTHORS' SHORT BIO

Dr. Marvin Schneider has 36 years of experience in the field of Information Technology. For22 years he worked in business operations, management consulting and information systems, which included working for US Bank, Harris Bank, Genesis HealthCare Corporation, Publishers Clearinghouse, Bank of New York, and the Federal Reserve Bank of New York. His positions included business analyst, senior business analyst, management consultant, project manager, operations manager, and computer supervisor. For the last 14 years, Dr. Schneider, has been a full-time professor, teaching undergraduate and graduate courses at DeVry University in the subjects of computer programming, databases, and logistics. He has a PhD in General Information Technology.

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, and software testing and quality assurance. He has published over 125 peer-reviewed papers. He has been awarded and managed several federal and local grants including NSF, USDA, DOE, etc. 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.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731