INVESTIGATING THE DETERMINANTS OF COLLEGE STUDENTS INFORMATION SECURITY BEHAVIOR USING A VALIDATED MULTIPLE REGRESSION MODELS

Mofleh Al-diabat

Department of Computer Science, Al Albayt University, Jordan

ABSTRACT

The frequency, intensity and repercussions of information security breaches in higher education has prompted colleges and universities around the world to devote more resources to enhance technical and human controls capabilities. Research has repeatedly found that technical solutions to cybercrime are insufficient in preventing incidents. The present analysis utilizes the Health Belief Model (HBM) to explain users' computer security behavior by replicating an earlier research study. The study, however, applies the HBM model to a new context, higher education, and college students serve as the sample for this research. A validated questionnaire was employed to collect responses from 263 students attending a public state Midwestern university in the United States. Multiple Linear Regression mathematical analysis was conducted on the dataset collected to measure constructs of the information security of college students. Findings of this research suggest that perceived susceptibility, perceived benefits and self-efficacy are good determinants of information security behavior for college students at least on the sample observations. Further, the analysis supported the moderating logic of perceived severity on the effects of susceptibility, benefits, general security orientation, self-efficacy and cues to action. Findings of this research call upon higher education security administrators to enact more effective awareness and training programs based on real-work security incidents simulations and incorporating information security into the general education curricula.

KEYWORDS

Computer Security; Simulated Training; Security Indicators, Security Awareness

1. INTRODUCTION

A study by the Information and Communication Technology department at the University of Maryland reported that 55% of help desk queries involved the compromise of users' accounts [1]. EDUCAUSE, the leading non-profit organization in information security in higher education, reported that information security is the top Information Technology (IT) concern facing American universities and colleges in their IT divisions[2]. Many studies have established low levels of information security practice among college students, a serious problem posing them and their information to cyber criminals. Attempting to address the persistent knowledge and behavioral gap among students in regard to information protection measures, universities are taking more vigorous and aggressive approaches to improve the awareness, education, security and most importantly the practice of Information Systems (ISs) on their campuses[3,4,5].

In the quest against cybercrime such as phishing, governments have legislated national and international measures hoping to curb the frequency and intensity of information security incidents[5]. Further, private industry leaders have invested in the research and development of

DOI: 10.5121/ijcsit.2018.10608

new simulation programs, intelligent algorithms and protocols enhancing the overall security of information systems [7,8,9,10,11,12]. Despite the superiority of the technical solution such as machine learning technology to information security problems, the role of the machine in identifying, reporting, addressing and treating the incident, the human element of the problem is still the leading cause of information security breaches[13]. College students have exhibited low levels of awareness in identifying and effectively managing information security incidents. Therefore, universities are actively engaging students and staff in information security education and best practices aspiring to improve their information security performance.

While most tertiary education providers have formal information security policies, a small percentage of their students' body is aware of it, let alone practice its recommended information security behaviors. Therefore, the influence of such manuals and proposals on the attitudes, awareness, education, training and practice of students concerning information security is minimal. Further, such information security policies are often designed without reference to the observed empirical evidence concerning the predictors of college students' information security practice[3,5]. Theories of Planned Behavior, Protection Motivation, Deterrence, Health Belief, Use and Acceptance of Technology and others have been directly linked to students' information security behavior. Protection Motivation Theory and the Health Belief Model (HBM) have proven to be good frameworks encouraging students to implement measures of information security[14].

This study adds on[15] research on the determinants of information security behavior using new environment anddata sample for evaluating models of information security;this study scope is limited to college students in tertiary education rather than employees. The study formulates a new conceptual model based on the validated behavioral research model referred to as the HBM[16]. The research attempts to identify whether the HBM constitutes a good theoretical framework for evaluating college students' information security behavior. Based on the findings, the study designs an empirically-based program to be administered to college students in order to increase their education, awareness, and practice of information security.

The HBM is an appropriate framework since information security behavior, the outcome, is a good behavior attained through avoiding its risk factors, low education, awareness, training and efficacy related to information security risks[17]. To prevent incidents, students must possess high knowledge, skills and abilities associated with information security averting the dangers of not securing the outcome, good information security practice[18]. The findings of this study assist stakeholders specially students in the information security discipline establish the invariance, consistency and robustness of relationships linking the HBM to information security behavior across contexts.

2. LITERATURE REVIEW

Research on students' computer security behavior is an emerging area and still limited. In a 2010 study conducted by [19]at the Rochester Institute of Technology campus, students who have used non-conventional operating systems, Windows or Apple, such as Linux or Unix have higher safety practices compared to others. The same study concluded that the use of strict passwords was only found among 33% of the sample. The low information security adoption rate is consistent with an earlier investigation at the Indiana University of Pennsylvania where forty percent of respondents indicated that they do not update their anti-virus capability [20]. The same survey found that about fifty percent of respondents did not use passwords conforming to best security standards. The low computer security practice among students is confirmed by a 2017 Pew Research study that found only twelve percent of Americans to use a password management software and only three percent indicated that they use such functionality when selecting a password[21].

Few investigations have explicitly tested validated theories in explaining the variation of students' adoption and implementation of computer security. Studies have utilized several theories including the Theory of Planned Behavior, Protection Motivation Theory, Technology Acceptance Model and the Unified Theory of Use and Acceptance of Technology[22].

[22]classified technology and its related applications into two types: positive technologies and protective technologies. Computer security, as the authors concluded, is considered a preventive measure against information security risks, and therefore protective/preventive technology-oriented models suit its study more than positive technology models.

Computer security behavior is more inclusive than simply adopting a new useful technology. It protects critical information related to users including financial data, healthcare records and academic documents[23,24].Thus, models linked to healthcare like the HBM are relevant to investigating the security behavior of users. Further, in the literature on information security, no elaborate models exist compelling researchers to look elsewhere such as the behavioral science to model the computer security behavior.

The HBM has developed in the 1950s as a behavioral tool explaining the link between patients' attitudes towards their illnesses and their likelihoods of avoiding exacerbating actions to their conditions. The HBM is a value-expectancy based approach to healthcare outcomes. Expectancy represents the performance of the behavior done by the individual while value constitutes incentives, motives or barriers associated with the behavior in question. The attitude associated with the behavior is determined by the probability of the outcomes related to the behavior occurring and how much value attached by the individual to such outcomes [25]. The HBM has been widely applied in healthcare to study the likelihood of patients to engage in good nutritional, exercise and preventive healthcare behaviors. The model has also been applied to studying behaviors outside of healthcare including compliance with information security policies in organizations and immigration [26,27].

The HBM posits that an individual's perception of healthcare condition threat and her perception of the efficacy of an action to remedy the threat determine her adoption of the behavior in question[28]. Perception of threat is determined by two variables: perceived susceptibility to the threat and perceived severity of the threat. Perceived efficacy of the action addressing the threat, the attitudes towards the behavior, is determined by perceived benefits and barriers associated with it. In addition to those variables, three other important indicators compose the HBM: cues to action, self-efficacy, and general health orientation [29].

The explanatory constructs in the HBM applies nicely to the study of computer security. Perceived susceptibility and severity associated with healthcare threats are analogous to the threats associated with information security risks[30]. Users can potentially be damaged severely and are likely to fall victim to cyber criminals especially phishing attacks. Further, the cues to action and self-efficacy constructs in the HBM extends to information security where the users' confidence in her abilities to remedy and incident, and her understanding of the overall context surrounding the incident or a potential attack inform her behavior concerning information security[31]. Moreover, the perceived benefits and barriers of information security practice inform the users' decision to adopt or implement security measures such as changing passwords routinely[32,33].

3. Proposed Model

Much of survey-based studies model the dependent variable as the intention or the probability of engaging in the behavior contingent on the respondent's perception. This research follows the same logic behind [15] where the outcome is the self-reported engagement level in the behavior, the intensity of information security practice. Both modelling techniques suffer from self-report bias. Nevertheless, reporting about the engagement in the behavior itself is more objective compared to subjective perceptions about the intention or likelihood to engage in it.Figure 1 presents the proposed model which wasinspired by HBM of [15]. Nevertheless, our proposed model measures the information security indicators behavior rather than perception and therefore, all components including perceived benefits, perceived barriers and perceived susceptibility among others have been changed in the proposed model. This is since we are evaluating these elements in a computer security prospective and for tertiary education students rather in organization.

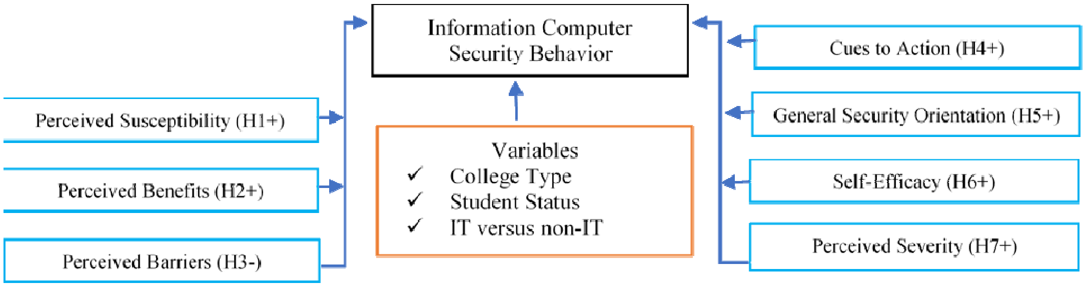

Figure 1. Proposed Model

3.1 Perceived Susceptibility

Perceived susceptibility represents the judgment of respondents' concerning the likelihood of possessing a health condition or a risk associated with the outcome in question. Individuals vary greatly with respect to their perceptions on this construct. On the one hand, one respondent may express sheer denial of developing the risk or the condition while another may confess a high likelihood of catching the disease, engaging in the risk factor or the behavior. With regards to information security, perceived susceptibility refers to the perceived likelihood of an information security risk or breech taking place. Presented with the same scenario, respondents will likely differ on their subjective judgments concerning perceived susceptibility. Given such information, one is more likely to hypothesize that:

H1 Higher perceptions of perceived susceptibility are positively associated with improved levels of information security behavior among college students.

3.2 Perceived Benefits

Perceived benefits represent the wide array of health-related advantages associated with the behavior in diminishing the risk of developing a disease or risk factor associated with the health condition. For instance, the wide range of health-related benefits associated with quitting smoking represent the perceived benefits of such an action in its effectiveness in reducing the risk of many health-related conditions. In the information security context, perceived benefits refer to the multitude of positive gains obtained from implementing computer security behaviors. Based on this logic, one hypothesizes that:

H2 More positive perceptions of the perceived benefits of computer security are associated with an increase in computer security behavior among college students.

3.3 Perceived Barriers

Perceived Barriers display the plethora of obstacles, challenges, and discomfort associated with engaging in an action to decrease the likelihood of developing a health condition. For instance, an obesity patient may find it inconvenient to quit eating or drinking certain foods and beverages. Regarding computer security behavior, one may find it difficult to learn computer security standards or deem them as obstacles to effective work performance. Based on this logic, one hypothesizes:

H3 Higher perceptions of perceived barriers associated with computer security behavior are negatively associated with computer security behavior implementation among college students.

3.4 Cues to Action

Cues to action refer to critical events signaling taking charge or initiative on the part of the respondent. For instance, coughing blood is an event where the patient learns about the severity of her case prompting action to be taken reducing the likelihood of developing a disease. In the computer security realm, students may receive emails on phishing incidents on campus or learn about information security scandals in their classrooms increasing their awareness and implementation of computer security behavior. Based on this understanding, one hypothesizes that:

H4 Higher perceptions of cues of action are positively associated with computer security behavior implementation among college students.

3.5 General Security Orientation

Broadly speaking, in the application of HBM, the general health orientation refers to the overall health well-being behavior sought by the individual. For instance, some people are found to practice health-related practices more than others. In other sub-disciplines within medical or public health research, this construct is referred to as healthcare literacy, knowledge or consciousness. Concerning information security behavior, some individuals may be predisposed more than others to practice privacy, confidentiality, or best security practices. Contingent on this interpretation, one hypothesizes:

H5 Higher levels of general security orientation are associated with higher levels of computer security behavior among college students.

3.6 Self-Efficacy

Self-efficacy refers to the overall level of confidence the individual possess regarding her ability to excel at a given behavior or practice [34]. In healthcare, self-efficacy oftentimes refer to the perceived ability of patients to follow recommended guidelines prescribed by physicians and healthcare staff to reduce the severity and risk of the associated disease. Within information security literature, self-efficacy represents the individual confidence in her ability to identify, address and remedy a potential or actual information security incident. Therefore, one hypothesizes:

H6 Higher levels of self-efficacy are associated with higher levels of computer security behavior among college students.

3.7 Perceived Severity

Perceived severity displays the individuals' judgement regarding the danger levels of the healthcare behavior or condition. Patients are likely to engage in behaviors reducing the likelihood of developing a disease evading the severity of the condition[35]. Within information security, the severity of incidents may result in loss of financial assets, reputational damage and litigation. They may also just simply compromise the privacy of individuals' information. At any rate, based on such logic, one hypothesizes that

H7 Higher levels of perceived severity are associated with higher levels of computer security behavior engagement among college students.

Consistent with previous research in information security behavior, perceived security is expected to moderate the relationship between all other determinants of the HBM and information security behavior. This is due to nature of information security behavior. Individuals try to avoid severe consequences linkedinability to comply with computer security standards, and thus the consequences impact vulnerability, barriersand self-efficacy of the individual.

Perceived severity is directly related to perceived susceptibility summing up to form perceived threat of a disease or an information risk. Therefore, once perceived severity increases, perceived susceptibility is expected to increase as well. Previous research has theorized that an individual has heightened perceptions of the severity of an outcome, they will take serious measures to shield herself from falling into that risk or negative outcome. Based on this logic, one hypothesizes that

H7a Perceived severity maximizes the impact of perceived susceptibility on college students' engagement in computer information security behavior.

Hypothesized that perceived severity minimizes the impacts of perceived barriers and benefits on computer information security behavior[15]. They argued that if the individual is facing a significant danger, she will be more likely to take serious protective measures downplaying the costs or inconvenience associated with the behavior, barriers. By the same token, the effectiveness of the measures become less important to the individual once she feels at danger and assume an active role in protecting herself from the risks associated with the disease or the information security risk.

H7b Perceived severity minimizes the impact of perceived benefits on college students' computer information security behavior.

H7c Perceived severity minimizes the impact of perceived barriers on college students' computer information security behavior.

On the other hand, cues to action aggrandize the protective behavior of individuals once outcomes are deemed significant. Individuals who perceive threats to be severe will take cures of action more seriously. By the same token, if individuals already practice standards and guidelines of security, their protective behavior is likely to increase once they believe the dangers associated with the outcome severe. Based on such logic, one hypothesizes:

H7d Perceived severity maximizes the impact of cues of action on college students' computer information security behavior.

H7e Perceived severity maximizes the impact of security orientation on college students' computer information security behavior.

Finally, perceived severity minimizes the impact of self-efficacy on computer information security behavior. Once individuals identify high potential risklinked with the behavior, they become protective regardless their confidence levels. Individuals across the board will be more alert and protective trying to avoid harsh consequences even if they lack any skills, abilities or knowledge regarding the behavior or measure. Based on this understanding, one hypothesizes that:

H7f Perceived severity minimizes the impact of self-efficacy on college students' computer information security behavior.

4. Research Design

The research strategy followed was the descriptive correlational design based on survey data collected from college students. The questionnaire developed for the analysis implemented best practices in item development and survey validation such as in [15]. We identify several domains of each construct then produced a pool of items measuring the specific elements of the construct. Face validity was established through consulting information security experts.

Previous research on the HBM has suffered from psychometric problems failing to report appropriate measures of reliability and validity. Further, informationsecurity research has not widely applied the HBM. Given such concerns, the present analysis utilizesquestionnaire that has been validated and its items carefully assessed and chosen.

The dependent variable, computer security behavior, is measured through respondents' reported care when opening emails with attachments. Computer security behavior ranges from routinely changing passwords to purchasing the most up-to-date security software. One of the most basic and common practices among college students is exercising caution when opening emails avoiding phishing schemes and other information security related risks. Therefore, this analysis utilizes such measure as to operationalizing the dependent variable.

4.2 Survey Validation

Survey validation entails the evaluation of the psychometric properties of the questionnaire. In the present study, an assessment of face, content and construct validity, as well as internal consistency as a reliability measure were conducted. Face validity refers to the judgement of the researcher and a panel of experts regarding the extent to which a pool of items on a questionnaire measure the intended construct. Following a series of interviews with academic and industry experts on information securitythe questionnaire has been refined to reflect changes recommended and validity was established. Content validity refers to the representation of items utilized in the questionnaire across the domains covered by the literature on the concerned constructs. Items utilized to form the questionnaire were drawn from previous studies. Further[15] reported conceptual validity statistics, Cohen Kappa's of 0.83 and placement ratio of 93% indicating high validity scores.

Table 1 displays the items and their corresponding constructs. The administration of the questionnaire followed the best practices guidelines recommended by survey research experts [39]. Such recommendations include the presentation of items in a neat layout and colored panels indicating higher credibility and legitimacy for conducting the research. Further, prior to the administration of the surveys on students, a pilot study with ten students was taken to indicate the clarity and ease of readability for the items indicating a 92% agreement rates with the phrases "items were easy to read and understand" and "items were clear." Notice that detailed instructions and examples were also provided in order to guide students' in their response patterns. The questionnaire was organized into distinct sections with defining statements preceding the items provided.

The survey was distributed to 10 classrooms at a large public Midwestern university in the United States. The classes ranged from introductory to advanced courses in Information Technology, Mathematics, Political Science, and Biology. The choice of courses was informed by the desire to obtain a wide range of college majors and disciplinary variation. Approvals from departments and instructors were obtained prior to the administration of the survey. The number of completed surveys that were all filled out after the conclusion of the classes and offered extra credit by the instructor were 263 out of 531 possible responses, generating a response rate of 49% which was higher than the rate of 31% in [15].

Table 1. Construct and Items

Construct	**Item**	**Source**
Behavior (BEH)	BEH1: Investigate the subject header of an email and the sender before reading the email. (agree/disagree)	[15]
	BEH2: Investigate if the filename of the attachment makes sense before reading the email. (agree/disagree)	[15]
	BEH3: when receiving an email attachment I should be careful as it may contain a virus. (agree/disagree)	[15]
	BEH4: I do not open email attachments if the email content seems suspicious. (agree/disagree)	[15]
Perceived Susceptibility (SUS)	SUS1: The chances of receiving an email attachment with virus are high. (agree/disagree)	[15]
	SUS2: There is a good possibility that I will receive an email attachment with virus. (agree/disagree)	[15]
	SUS3: I am likely to receive an email attachment with virus. (agree/disagree)	[15]
Perceived Severity (SEV)	SEV1: Having my computing machine infected by a virus once opening a suspicious email attachment is a serious issue for me. (agree/disagree)	[37]
	SEV2: Losing organizational data as a result of opening a suspicious email attachment is a serious issue for me. (agree/disagree)	[37]
	SEV3: If my computer is infected by a virus as a result of opening a suspicious email attachment, my daily work could be negatively affected. (agree/disagree)	[15]
Perceived benefits (BEN)	BEN1: Checking if the sender and subject make sense is (definitely/not) effective in preventing viruses from infecting my computer.	[15]
	BEN2: Checking if the filename of the email attachment makes sense is (definitely/not) effective in preventing viruses from infecting my computer.	[15]

	BEN3: Exercising care before opening email attachments is (definitely/not) effective in preventing viruses from infecting my computer.	[15]
Perceived barriers (BAR)	BAR1: Exercising care when reading emails with attachments is inconvenient. (agree/disagree)	[15]
	BAR2: Exercising care when reading emails with attachments is time-consuming. (agree/disagree)	[38]
	BAR3: Exercising care when reading emails with attachments would require considerable investment of effort other than time. (agree/disagree)	[37]
	BAR4: Exercising care when reading emails with attachments would require starting a new habit, which is difficult. (agree/disagree)	[38]
Cues to action (CUE)	CUE1: My organization distributes security newsletters or articles. (never/always)	[15]
	CUE2: My organization organizes security talks. (never/always)	[15]
	CUE3: My organizations' IT helpdesk sends out alert messages/emails concerning security. (never/always)	[15]
	CUE4: My organization constantly reminds me to practice computer security. (agree/disagree)	[15]
General security orientation (GEN)	GEN1: I read information security bulletins or newsletters. (agree/disagree)	[15]
	GEN2: I am concerned about security incidents and try to take action to prevent them. (agree/disagree)	[39]
	GEN3: I am interested in information about computer security. (agree/disagree)	[39]
	GEN4: I am constantly mindful about computer security. (agree/disagree)	[15]
Self-efficacy (SEF)	SEF1: I am confident of recognizing a suspicious email. (agree/disagree)	[15]
	SEF2: I am confident of recognizing suspicious email headers. (agree/disagree)	[15]
	SEF3: I am confident of recognizing suspicious email headers. (agree/disagree)	[15]
	SEF4: I can recognize a	[40]

	suspicious email attachment even if there was no one around to help me. (agree/disagree)	
Technical controls (CON1)	My organization ensures that my computer is protected from viruses by installing anti-virus software on my computer and/or the email server. (agree/disagree)	[15]
Security familiarity (CON2)	How would you rate yourself in terms of familiarity with computer security practices? (very familiar/not at all familiar)	[15]

Table 2 displays the results of validity and reliability analysis. First, Exploratory Factor Analysis generated a total number of 8 dimensions as specified by the proposed model in Figure 1. Second, the loadings indicated a direct relationship between each item and its specified construct as Table 1 suggested, confirming the face, content, and conceptual validity findings reported above. The right-most column displays the Cronbach's alphas per dimension indicating a reliable result, above the threshold of 0.70 suggested by [36]. Findings from Table 2 indicate adequate psychometric results obtained from the data for the survey utilized in this research.

Table 2. Reliability and validity tests

Construct and items	**Loading**	**Cronbach alpha**
BEH		0.71
BEH2	0.74	
BEH3	0.72	
BEH4	0.69	
BEH1	0.62	
SUS		0.81
SUS2	0.79	
SUS3	0.73	
SUS1	0.71	
SEV		0.73
SEV1	0.82	
SEV2	0.78	
SEV3	0.64	
BEN		0.77
BEN2	0.72	
BEN1	0.61	
BEN3	0.54	
BAR		0.87
BAR1	0.82	
BAR4	0.78	
BAR3	0.76	
BAR2	0.63	
GEN		0.81
GEN2	0.85	
GEN3	0.70	
GEN1	0.64	
GEN4	0.58	
CUE		0.82
CUE4	0.89	
CUE2	0.81	
CUE1	0.71	

CUE3	0.65	
SEF		0.81
SEF3	0.81	
SEF1	0.72	
SEF4	0.68	
SEF2	0.59	

To fit the model to the collected data, Multiple Linear Regression Analysis is utilized. This technique is suitable for evaluating the direction and strength of relationships among quantitative variables. Further, it helps researchers predict the value of a single dependent variable based on estimates of a set of independent variables. The method has been widely used in the information security literature and its output easily understood and incorporated into concrete recommendations for devising robust solutions to pressing problems such as the one in the present study is attempting to mitigate. The study proposed three models. The first model contains the seven independent variables on the left in Figure 1 and the information security behavior as the dependent variable. The second model utilizes interaction terms between perceived severity and the seven variables to test the moderating hypotheses. Finally, the third model incorporates control variables including students' status, age, major and college affiliation.

5. Results Analysis

Table 3 displays the demographic information of the sample surveyed at the university. Notice that most participants are relatively young reflecting the vulnerability of college students to potential cybercrime due to their lack of practical security experience. More males filled out the survey since many of the courses featured STEM classrooms where males disproportionally surpass females in numbers in such fields. Regarding the college affiliation, many courses were in Information Technology and Systems reflecting an advantage for the College of Technology and Business over others. This is consistent with the students' status variable where 42% of respondents indicated an IT-related major. The majority of the sample was enrolled in bachelors and masters programs.

Table 3 Demographics of respondents

Demographic	Category	Percentage (%)
Age	18-22	61
	23-30	23
	31-40	9
	>=41	7
Gender	Male	59
	Female	41
College	College of Technology	31
	College of Business	27
	College of Arts and Sciences	17
	College of Education	12
	College of Health and Human Services	13
Student Status	Undergraduate	58
	Masters	29
	Doctorate	6
	Other	7
Major	IT-Related	42
	Non IT-Related	58

Prior to the interpretation of the Multiple Regression Analysis output, a note on the fulfillment of the statistical technique assumptions is warranted. The inspection of tolerance values and Variance Inflation Factors indicated that the model possesses no serious violations of the multicollinearity assumption. Further, inspecting the residuals plot against predicted values indicated an adequate linear fit signaling no serious violations for the linearity, as well as the homoskedasticity assumptions.

Table 4 demonstrates the results from the Multiple Regression Analysis. Three models were fitted where the first model only included the direct effects, the second model included the interaction terms, and the third (complete model) included control variables. Notice that the addition of control variables(age, gender, students' status, college affiliation and whether the student is enrolled in an IT or non-IT major) does not change the explanatory power of the model, R^2, by much (5% change). It should be noted that perceived benefits, perceived susceptibility, self-efficacy and general security orientation were supported. Whereas, perceived severity, perceived barriers and cues to action were not able to statistically explain the disparity in computer security behavior. In addition, five interactive terms were derived to be significant in relation to the impact of perceived severity; these are cues to action, general security orientation, perceived benefits, perceived susceptibility and self-efficacy. All in all, the results of the analysis suggested that H1, H2, 5 and H6 were supported while H3, H4 and H7 were not. Further, H7a, H7b, H7d, H7e and H7f were supported while H7c was not.

This result confirms findings reported earlier, i.e.[15]. The first difference observed in both results was the significance of H5 in this study. Second, H7a was reported to be not significant by [15] while significant in this study, the moderating effect of perceived severity on perceived susceptibility and information security behavior. Despite such differences, the HBM seems to be an appropriate framework in explaining college students' behavior towards information security.

Table 4. Regression Models

Model	Model 1	Model 2	Model 3	
	Main effects	Interaction effects	Full	
Variables	Coefficient	Coefficient	Coefficient	Results
Perceived susceptibility	**0.41**	**0.39**	**0.38**	H1 supported
Perceived Benefits	**0.34**	**0.31**	**0.33**	H2 supported
Perceived Barriers	0.11	0.08	0.07	H3 not supported
Cues to Action	0.04	0.02	0.03	H4 not supported
General Security Orientation	**0.21**	**0.19**	**0.17**	H5 not supported
Self-efficacy	**0.38**	**0.33**	**0.36**	H6 supported
Perceived Severity	0.08	0.07	0.07	H7 not supported
Perceived Severity x perceived susceptibility		**0.18**	**0.17**	H7a not supported
Perceived Severity x Perceived Benefits		**-0.21**	**-0.19**	H7b supported
Perceived Severity x Perceived Barriers		0.09	0.7	H7c not supported
Perceived Severity x Cues to Action		**0.22**	**0.19**	H7d supported
Perceived Severity x General Security Orientation		**0.24**	**0.21**	H7e supported
Perceived Severity x self-efficacy		**-0.24**	**-0.19**	H7f supported
Gender			0.11	
Age			0.01	
IT or non-IT			0.03	

College Affiliation			0.04	
R^2	0.51	0.64	0.69	
Change in R^2		0.114	0.012	
Adjusted R^2	0.450	0.549	0.551	

6. Conclusions, Implications And Future Work

This research investigated different constructs related to HBM to address risks associated with information security for tertiary education students. Primary data from 263 students attending a public state Midwestern university in the United States have been collected based on designed questionnaire to achieve the aim(s) of the study. More importantly, Multiple Linear Regression mathematical analysis was conducted on the gathered observations to measure constructs of the information security especially when it comes to cybersecurity risks. Findings of this research show useful indicators to college students' information security behavior including perceived benefits, general security orientation, perceived susceptibility, and self-efficacy as they have been derived by performing due diligence when students are checking their emails. First, perceived susceptibility and perceived benefits are classic pre-cautionary measures taken by the user to reduce the chances of falling into a cybercrime scheme. Such measures are reinforced by a general security orientation where the user is more likely to exercise due diligence when opening emails with attachments. Further, the confidence level of the user in identifying and addressing the incident, self-efficacy, has been repeatedly found to be a positive predictor of information security behavior adoption and implementation.

This research revealed that cues to action, perceived barriers and perceived severity to be statistically not significant in forecasting information security behavior of college students at least on the dataset considered. First, perceived barriers indicate the information security care is inconvenient or difficult to learn by users. Such convictions are non-existent for the study's sample. First, college students are computer literate and have been previously exposed to cybercrime either through their circles, media or classrooms. Second, about 50% of the sample reported that their majors are IT-related indicating a high learning ability for computer security behavior. Therefore, students seemed to be more comfortable implementing information security practices and did not consider security as an inconvenience.

This study found cues to action to be a non-significant determinant for information security behavior. Cues to action are unclear and difficult to fathom by students. Personal computers are not equipped with visual software calling students for immediate action. By the same token, emails could be manipulated to seem real victimizing students to fall into phishing schemes. Further, students are not regularly reminded by the information security policy or the security program available through their college decreasing their awareness about information security. Therefore, the relationship between cues to action and information security behavior was not found to be strong by this research. One important findings of this study showed that perceived severity was not reported to be a good predictor of information security behavior. Such findings allude to the possibility that perceived severity may not be influential on its own in making college students practice security behavior. It is effective once interacted with other determinants such as cues to action and perceived benefits. Therefore, for a revised model to be constructed, perceived severity could not be eliminated since it was found to interact with other factors in the system.

This research marks one of the first systematic analyses investigating the determinants of information's security behavior among college students. It hasused a new sample confirming earlier findings. Such exercise is important for the development of theoretically-based solutions to information security problems facing students. New programs and initiatives should take into consideration the importance of significant constructs. This indicates that that universities should raise the awareness of benefits associated with information's security behavior. Further, universities should focus on practical training increasing the self-efficacy of students in addressing information security risks.

In near future we are going to investigate cybersecurity risks associated with college students particularly phishing attacks. Phishing involves stealing sensitive information from users such as usernames and passwords in order to access financial assets. Since phishers often targetnovice users who lack cybersecurity knowledge and computer self-efficacy. Therefore, educating novice users such as tertiary education students becomes crucial to keep them safe from cybersecurity attacks especially phishing. One promising approach to raise awareness is to develop interactive material (online, mobile, or simulated training) on the severity of phishing attacks, especially when they are surfing the internet. We will conduct simulated practical workshops possibly at the orientation level when students join the university to simulate real-world scenarios involving cybersecurity attacks on their users in a safe environment in order to track their vulnerability to phishing.At the end of the training, participantsarethen given the detailed report on the outcome informing them about their vulnerability to cybersecurity attacks and providing them with computer security material. We will then conduct in depth analyses on the data collection from the workshop to possibly proposed a visualization model for detecting phishing attacks. Finally, we are going also to investigate cybersecurity attacks by using mobile game. This cybersecurity awareness mobile game will be expose students to several scenarios related to information security especially cybersecurity attacks.

REFERENCES

1. UMBC (2017). Why College Campuses Are Big Targets for Cyber Attacks Ever wonder why YOUR account would ever be hacked? Retrieved from https://doit.umbc.edu/news/?id=70678

2. Dahlstrom, E., and Bichsel, J. (2014). ECAR Study of Undergraduate Students and Information Technology, 2014. Washington, DC: Educause.

3. Kim, B. (2014). Recommendations for information security awareness training for college students. Information Management & Computer Security, 22(1), 115-126.

4. Lin, Q., Wang, K., and Gao, L. (2015). Exploration on the Education Mode of Effectively Strengthening Security Awareness and Ability of Female College Students. Paris: Atlantis Press.

5. Shropshire, J., Warkentin, M., and Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. Computers & Security, 49, 177-191.

6. Peltier, T. (2016). Information Security Policies, Procedures, and Standards: guidelines for effective information security management. Boca Raton, Fl: Auerbach Publications.

7. Mohammad R., Thabtah F., McCluskey L., (2014) Predicting Phishing Websites based on Self-Structuring Neural Network. Journal of Neural Computing and Applications, (3)1-16. Springer.

8. Thabtah F., Kamalov F. (2017) Phishing Detection: A Case Analysis on Classifiers with Rules using Machine Learning. Journal of Information and Knowledge Management. World Scientific.

9. Thabtah F., Abdelhamid N. (2016) Deriving Correlated Sets of Website Features for Phishing Detection: A Computational Intelligence Approach. Journal of Information and Knowledge Management. 15, 1650042 (2016) [17 pages]. World Scientific.

10. Abdelhamid N, Ayesh A., Thabtah F. (2013) Phishing Detection using Associative Classification Data Mining. ICAI'13 - The 2013 International Conference on Artificial Intelligence, pp. (491-499). USA.

11. Mohammad R., Thabtah F., McCluskey L., (2013) Intelligent Rule based Phishing Websites Classification. Journal of Information Security (2), 1-17. ISSN 17518709. IET.

12. Qabajeh I, Thabtah F, Chiclana F (2018) A recent review of conventional vs. automated cybersecurity anti-phishing techniques. Computer Science Review 29, 44-55.

13. AlShboul R, Thabtah F, Abdelhamid N, Al-diabat M (2018) A visualization cybersecurity method based on features' dissimilarity Computers & Security 77, 289-303. 2018

14. Hajli, N., and Lin, X. (2016). Exploring the security of information sharing on social networking sites: The role of perceived control of information. Journal of Business Ethics, 133(1), 111-123.

15. Ng, B., Kankahali, A., and Xu, Y. (2009). Studying users' computer security behavior: a health belief perspective. Decision Support Systems, 46, 815-825.

16. Skinner, C., Tiro, J., and Champion, V. (2015). The health belief model. In Health behavior: theory, research, and practice, 5th ed. San Francisco (US): Jossey-Bass, 75-94.

17. Jones, C., Smith, H., and Llewellyn, C. (2014). Evaluating the effectiveness of health belief model interventions in improving adherence: a systematic review. Health psychology review, 8(3), 253-269.

18. Merkow, M., and Breithaupt, J. (2014). Information security: Principles and practices. London: Pearson Education.

19. L. Reznik, V. J. Buccigrossi III, J. Lewis, A. Dipon, S. Milstead, N. LaFontaine, K. Beck, and H. Silvia, "Security of computer use practice: The case of ordinary users survey," in Proceedings of the 5th Annual Symposium on Information Assurance (ASIA '11),), June 7-8, 2011, ser. SOUPS '07. New York, NY, USA: ACM, June 2011, pp. 167–168.

20. Tekerek, M., and Tekerek, A. (2013). A research on students' information security awareness. Turkish Journal of Education, 2(3).

21. Smith, A. (2017). Americans and Cybersecurity: Password Management and Mobile Security. Retrieved from http://www.pewinternet.org/2017/01/26/2-password-management-and-mobile-security/

22. Ngoqo, B., and Flowerday, S. (2015). Exploring the relationship between student mobile information security awareness and behavioural intent. Information & Computer Security, 23(4), 406-420.

23. Kang, R., Dabbish, L., Fruchter, N., and Kiesler, S. (2015, July). "My data just goes everywhere:" user mental models of the internet and implications for privacy and security. In Symposium on Usable Privacy and Security (SOUPS) (pp. 39-52). Berkeley, CA: USENIX Association.

24. Safa, N., Von Solms, R., and Futcher, L. (2016). Human aspects of information security in organisations. Computer Fraud & Security, 2016(2), 15-18.

25. Abraham, C., and Sheeran, P. (2005). The health belief model. In M. Conner, P. Norman (Eds.), Predicting Health Behaviour, Ch. 2. Berkshire (UK): Open University Press.

26. Groenewold, G., Bruijn, B., and Bilsborrow, R. (2006). Migration of the Health Belief Model (HBM): Effects of psychosocial and migrant network characteristics on emigration intentions in five countries in West Africa and the Mediterranean Region. The Population Association of America 2006 Annual Meeting, March 30–April 1, Los Angeles, CA, 2006.

27. Janz, N. and Becker, M. (1984). The health belief model: a decade later. Health Education Quarterly 11.

28. Rosenstock, I. (1974). The health belief model and preventive health behavior. Health Education Monographs 2.

29. Rosenstock, I., Strecher, V., and Becker, M. (1988). Social learning theory and the health belief model. Health Education Quarterly 15.

30. Conner, M. and Norman, P. (2005). Predicting health behaviour: a social cognition approach. In M. Conner and P. Norman (Eds.), Predicting Health Behaviour, Ch. 1. Berkshire, UK: Open University Press.

31. Chung, W., Chen, H., Chang, W., and Chou, S. (2006). Fighting Cybercrime: a review and the Taiwan experience. Decision Support Systems, 41 (2006).

32. Davis, F. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3).

33. Eccles, J. and Wigfield, A. (2002). Motivational beliefs, values, and goals. Annual Review Psychology, 53.

34. Compeau, D., and Higgins, C. (1995). Computer self-efficacy: development of a measure and initial test. MIS Quarterly, 19(2).

35. Cheung, C., Lee, Z., and Chan, T. (2015). Self-disclosure in social networking sites: the role of perceived cost, perceived benefits and social influence. Internet Research, 25(2), 279-299.

36. Nunally, J. (1978). Psychometric. New York: McGraw Hill.

37. Woon, I., Tan, G., and Low, R. (2005). A protection motivation theory approach to home wireless security. Proceedings of the Twenty-Sixth International Conference on Information Systems, Las Vegas, Nevada, USA.

38. Champion, V. (1984). Instrument development for health belief model constructs. Advances in Nursing Science, 6(3)

39. Chan, M., Woon, I., and Kankanhalli, A. (2005). Perceptions of information security in the workplace: linking information security climate to compliant behavior. Journal of Information Privacy and Security, 1(3).

40. Jayanti, R. and Burns, A. (1998). The antecedents of preventive health care behavior: an empirical study. Academy of Marketing Science Journal 26(1).