JOURNAL OF
INFORMATION SYSTEMS
APPLIED RESEARCH

Volume 11, Issue 3
December 2018
ISSN: 1946-1836

In this issue:

The **Journal of Information Systems Applied Research** (JISAR) is a double-blind peer-reviewed academic journal published by **ISCAP,** Information Systems and Computing Academic Professionals. Publishing frequency is three issues a year. The first date of publication was December 1, 2008.

JISAR is published online (http://jisar.org) in connection with CONISAR, the Conference on Information Systems Applied Research, which is also double-blind peer reviewed. Our sister publication, the Proceedings of CONISAR, features all papers, panels, workshops, and presentations from the conference. (http://conisar.org)

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the JISAR journal. Currently the target acceptance rate for the journal is about 40%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org. Special thanks to members of AITP-EDSIG who perform the editorial and review processes for JISAR.

2018 AITP Education Special Interest Group (EDSIG) Board of Directors

Journal of
Information Systems Applied Research

Student Intentions and Behaviors Related to Email Security: An Application of the Health Belief Model

Gregory Schymik
schymikg@gvsu.edu

Jie Du
dujie@gvsu.edu

School of Computing and Information Systems
Grand Valley State University
Allendale, MI 49456 USA

Abstract

Information security is an ongoing concern for all of us. Email is frequently the attack vector of choice for hackers and is a large concern for campus IT organizations. This paper attempts to gain insight into what drives the email security behaviors of undergraduate students at one midwestern public, master's granting university by surveying students in an introductory computing course about their email security behavior. The survey questions are developed based on the Health Belief Model and used to measure eight constructs including behavior, perceived barriers to practice, self-efficacy, cues to action, prior security experience, perceived vulnerability, perceived benefits, and perceived severity. The perceived benefits and self-efficacy variables were found to be the most important factors that affect students' security behavior. The findings of this study may help shed light on how universities can better prepare students to handle this critical information security concern.

Keywords: Email security behavior, health belief model, intentions, survey.

1. INTRODUCTION

People, the users of information systems, are still the biggest security concern for most IT organizations (Matthews, 2017). And email is still a popular attack vector for hackers. The US Internal Revenue Service (IRS) lists phishing scams in their "Dirty Dozen" tax scams for the 2017 filing year (Internal Revenue Service, 2017). Symantec's April 2017 Internet Security Threat Report noted that the rate of malicious emails being sent (1 in 131) was the highest it had seen in five years (Symantec, 2017). This is a particular concern on campuses. For the second year in a row, IT security has been identified as the biggest concern for campus IT departments and "phishing and social engineering attacks" was rated the highest concern amongst Higher Education Information Security Council working groups (Grama and Vogel, 2017). Given these concerns about email driven security attacks, the study of email security behavior by students is a timely and important endeavor.

This paper attempts to gain insight into such behavior at one midwestern public, master's granting university by surveying students in an introductory computing course about their email security behavior. The paper presents a brief discussion on the adoption of preventive behaviors and the health belief model and then describes the research model and methodology. It concludes with a presentation of the results and a discussion of their implications.

2. LITERATURE REVIEW

On its surface, the question of whether users will adopt security behaviors appears to be an obvious target for IT adoption research.

However, this research is not testing the adoption of a specific technology or technologies, it is testing the adoption of preventative behaviors. This is a significant difference. Those adopting technologies are thought to do so to gain some sort of advantage or positive result – the efficiency gains through the adoption of a new software package designed as part of a business process re-engineering effort, for example. Those adopting preventative behaviors, however, are believed to be doing so not to gain a positive result or benefit, but to avoid the repercussions associated with the occurrence of some avoidable or preventable problem – a ransomware attack, for example. Recent research in IT security behavior has suggested that this behavior is similar to a patient's preventative behavior in the health care industry, applying the health belief model (Rosenstock, 1974; Rosenstock, Strecher and Becker, 1988) to IT security situations (Ng, Kankanhalli and Xu, 2009; Claar and Johnson, 2010; Williams, Wynn, Madupalli, Karahanna and Duncan, 2014).

Health Belief Model/Security Belief Model

The management literature has referred to the health belief model (HBM) as "an expectancy model of health care decision making" (Walker and Thomas, 1982, p.188). It evolved out of the need to develop a theory that helped explain the failure of people to adopt preventative behaviors or accept testing to screen for diseases for which they exhibited no symptoms (Rosenstock, 1974). The parallel to the need to understand users' information security behavior is clear: IS security behavior researchers seek to understand what makes people adopt (or not adopt) specific behaviors that prevent the hacking of their system, which shows no current evidence of hacking. This model has been the basis of IS research attempting to understand the adoption of preventative behaviors associated with the use of email (Ng et al., 2009), the installation of anti-virus software on home computers (Claar and Johnson, 2010), and typical, recommended practices for preventing unauthorized access to their computers at work (Williams et al., 2014). Williams et al. (2014) renamed the model to the security belief model. For simplicity's sake, we will use the HBM when we refer to these models in this paper.

Table 1 summarizes the constructs used in the HBM and their use in recent information systems security research. The independent variables of the HBM are a person's perceived susceptibility to a condition, their perceived seriousness of a given health problem, their perception of how beneficial an action would be to their case, their perception of negative aspects of the action that might manifest as barriers to action that would prevent actions from being taken, their self-efficacy regarding the actions to be taken, and any triggers or other cues to action that might impact whether or not they adopt the behavior (Rosenstock, 1974; Rosenstock et al., 1988). These variables are easily adapted to IS research (see our explanation in the research model description below).

ROSENSTOCK (1974), ROSENSTOCK, ET AL. (1988)	NG, ET AL. (2009)	CLAAR AND JOHNSON (2010)	WILLIAMS ET AL. (2014)
PERCEIVED BENEFITS	BEN*	BEN	BEN*
PERCEIVED BARRIERS TO PRACTICE	BAR	BAR*	BAR
SELF-EFFICACY	SEF*	SEF*	SE
PERCEIVED SUSCEPTIBILITY	SUS*	VUL*	SUS*
CUES TO ACTION	CUE	CUE	CTA*
GENERAL HEALTH ORIENTATION	GEN	PXP	---
PERCEIVED SEVERITY	SEV	SEV	SEV*
INTERACTIONS			none hypothesized
GENDER		GEN	
AGE		AGE (xBAR*)	
EDUCATION		EDU (xBEN*)	
		PXP (xSEV*, xVUL*)	
	SEV (xBEN*, xCUE* xGEN*, xSEF*)		
R^2	.593	.304	.430
ADJ R^2	.549	.167	not reported

Table 1 - Model Composition -- Independent Variables and Interactions - * indicates significant relationships

Various moderating variables have been suggested. Demographic variables (gender, age, and education) are thought to have some impact on behavior in the HBM (Rosenstock, 1974). Ng et al. (2009) hypothesized that perceived severity would have a moderating effect on all other independent variables (IVs) and found significant interactions with perceived benefits, cues to action, general security orientation, and self-efficacy. Claar and Johnson (2010) hypothesized that prior experience, along with age, education, and gender would have moderating effects on all IVs except for cues to action and found significant interactions between age and perceived barriers to action, education and perceived benefits, and prior experience and perceived severity and self-efficacy. Williams et al. (2014) did not include any moderating variables in their security belief model.

3. RESEARCH MODEL

Our research model is based on the health belief model (Rosenstock, 1974, Rosenstock et al. 1988) that underlies the models tested in Ng et al. (2009), Claar and Johnson (2010) and Williams et al., (2014). All seven independent variables (IVs) and the dependent variable are taken directly from Ng et al. (2009) with one difference being the replacement of their general security orientation variable with Claar and Johnson's (2012) security experience variable (EXP).

The general health orientation variable from the health belief model is intended to represent a basic foundation or consistent behavior related to all health care decision situations (Walker and Thomas, 1982). Ng et al. (2009) defined a general security orientation variable and operationalized it as a set of questions related to subjects' self-awareness of and activities associated with general knowledge of information security. We followed Claar et al.'s (2010) approach to this variable and used a more direct measure of the subjects' experience with email-related information security problems. Given our subject group's age (young, typically traditional, undergraduate students), we feel that it is very likely that they have not had enough life experience to establish Ng et al.'s (2009) general orientation towards security. We see a direct measure of experience as a precursor to a general security orientation and believe it to therefore be a reasonable substitution.

3.1 Main-effects IVs

The dependent variable in the research model (Figure 1) is the subjects' self-reported email security behavior (BEH). Seven main-effects IVs are hypothesized: the perceived benefits of performing email security behaviors (BEN), the perceived barriers to entry of performing the behaviors (BAR), the subjects' belief in their ability to carry out security behaviors - their self-efficacy (EFF), the perceived vulnerability to email attacks (VUL), the existence of any cues to action regarding email security behaviors (CUE), the subjects' prior experience with email-related security issues (EXP) and the subjects' perceived severity of email-related security incidents (SEV).

- H1 – Perceived benefits (BEN) of practicing email security behaviors are positively related to email security behaviors.
- H2 – Perceived barriers (BAR) to practicing email security behaviors are negatively related to email security behaviors.
- H3 – Self-efficacy (EFF) is positively related to email security behaviors.
- H4 – Perceived vulnerability (VUL) to email-related security incidents is positively related to email security behaviors.
- H5 – Cues to action (CUE) are positively related to email security behaviors.
- H6 – Prior experience (EXP) with email-related security issues is positively related to email security behaviors.
- H7 – Perceived severity (SEV) of email-related security issues is positively related to email security behaviors.

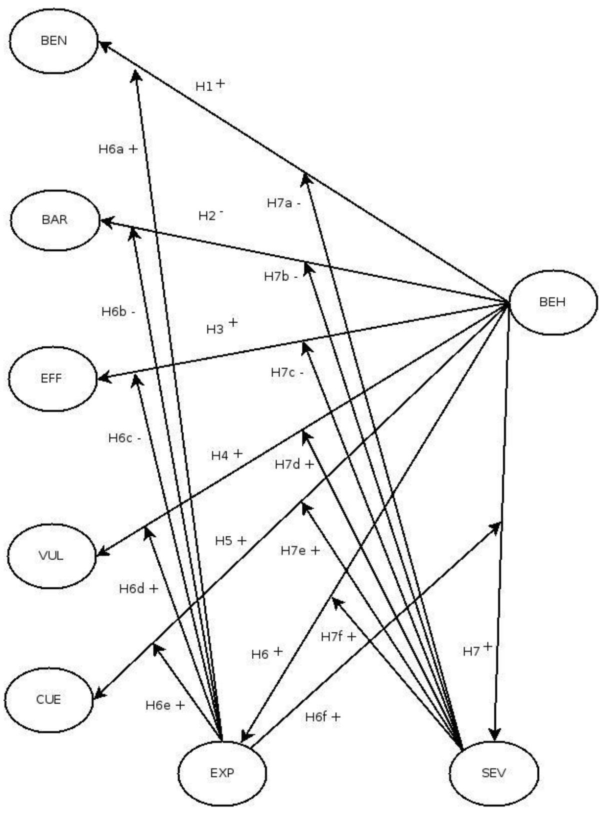


Figure 1 - Research Model

3.2 Interactions

We combine the Ng et al. (2009) and Claar and Johnson (2010) models and hypothesize that the subjects' prior experience with email-related security issues (EXP) and their perception of the severity of email security-related issues (SEV) are moderating variables. While the health belief model (see Rosenstock, 1974) implies several psychosocial variables (age, education, and gender) as moderators, we do not include these in our analysis. Our subject population falls in a narrow age range (96.5% are between the ages of 18 and 26), and subjects are typically first- or second-year undergraduate students. Such homogeneity suggests that we need not include these variables in the analysis. Gender differences will be analyzed and presented in future work.

3.2.1 Experience as a Moderator

We hypothesize that subjects' prior experience with email-related information security attacks would have a moderating effect on the other main-effects IVs. Claar and Johnson (2010) suggested this interaction in their research without explanation. We suggest that those who have had security issues related to email behaviors in the past would be influenced by those experiences in ways that would enhance the likelihood of any individual factor impacting their behaviors. A subject who has experienced email-related information security problems would probably more easily see the value of being diligent with emails (EXPxBEN), be expected to have a reduced focus on the difficulty of performing the appropriate preventative actions (EXPxBAR), give less weight to any perception of self-efficacy (EXPxEFF), have a better/more realistic understanding of their vulnerability to such problems (EXPxVUL), have a higher appreciation for the cues to action they might have seen (EXPxCUE), and have a better understanding of the severity of such problems (EXPxSEV),

- H6a – Prior experience with email-related security incidents increases the positive effect of perceived benefits on email security behaviors (EXPxBEN).
- H6b – Prior experience with email-related security incidents reduces the negative effect of barriers to practice on email security behaviors (EXPxBAR).
- H6c – Prior Experience with email-related security incidents reduces the positive effect of self-efficacy on email-related security behaviors (EXPxEFF).
- H6d – Prior experience with email-related security incidents increases the positive effect of perceived vulnerability on email security behaviors (EXPxVUL).
- H6e – Prior experience with email-related security incidents increases the positive effect of cues to action on email security behaviors (EXPxCUE).
- H6f – Prior experience with email-related security incidents increases the positive effect of perceived severity on email security behaviors (EXPxSEV).

3.2.2 Severity as a Moderator

Ng et al. (2009) relied on expectancy-value theory, protection motivation theory, and health belief model literature to hypothesize that perceived severity would have a moderating effect on the other IVs in the model. Based on their efforts, we hypothesize that perceived severity will have an influence on the remaining independent variables.

- H7a – Perceived severity of any email-related security incidents reduces the positive effect of perceived benefits on email security behaviors (SEVxBEN).
- H7b – Perceived severity of any email-related security incidents reduces the negative effect of barriers to practice on email security behaviors (SEVxBAR).
- H7c – Perceived severity of any email-related security incidents reduces the positive effect of self-efficacy on email security behaviors (SEVxEFF).
- H7d – Perceived severity of any email-related security incidents increases the positive effect of perceived vulnerability on email security behaviors (SEVxVUL).
- H7e – Perceived severity of any email-related security incidents increases the positive effect of cues to action on email security behaviors (SEVxCUE).
- H7f – Perceived severity of any email-related security incidents increases the positive effect of prior experience on email security behaviors (SEVxEXP)

4. METHODOLOGY

To test these hypotheses, an electronic Likert-scale questionnaire was implemented to survey the participants about their email security behaviors. The survey contains 35 questions. Except for the age and gender questions, all questions are focused on the eight constructs and are anchored on 5-point Likert scales. Undergraduate students who completed an introductory computing course in the winter 2016 semester or the fall 2016 semester were asked to complete the survey on Blackboard. The blackboard surveys allow students to complete the survey anonymously. A total of 153 students participated in this study (67 from Winter 2016 and 86 from Fall 2016). Ten responses were removed from the data set due to missing data issues (2 from Winter 2016 and 8 from Fall 2016).

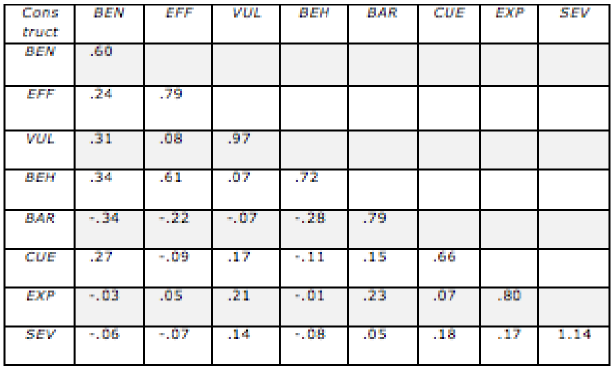
Thus, the data collection yielded 143 useable survey response sets. Table 2 summaries the demographics of the sample. Table 3 shows the descriptive statistics for all constructs. Table 4 shows the inter-correlations between constructs.

Demographic	*Category*	*Percentage*
Age	<19	14.7
	19-22	65.0
	22-26	16.8
	>26	3.5
Gender	Male	51.7
	Female	48.3

Table 2 – Subject Demographics

Construct	*Min*	*Max*	*Mean*	*SD*
BEH	2.00	5.00	4.12	0.72
EFF	1.75	5.00	3.88	0.79
VUL	1.00	5.00	3.56	0.97
BEN	2.20	5.00	4.16	0.60
BAR	1.00	5.00	2.56	0.79
CUE	1.67	5.00	3.84	0.66
EXP	1.00	4.67	1.80	0.80
SEV	1.00	5.00	3.41	1.14

Table 3 - Descriptive Statistics of Constructs



Construct	*BEN*	*EFF*	*VUL*	*BEH*	*BAR*	*CUE*	*EXP*	*SEV*
BEN	.60							
EFF	.24	.79						
VUL	.31	.08	.97					
BEH	.34	.61	.07	.72				
BAR	-.34	-.22	-.07	-.28	.79			
CUE	.27	-.09	.17	-.11	.15	.66		
EXP	-.03	.05	.21	-.01	.23	.07	.80	
SEV	-.06	-.07	.14	-.08	.05	.18	.17	1.14

Table 4 – Constructs' Inter-Construct Correlations

To incent completion of the survey, students were informed that those who completed the survey would be entered into a drawing for one of five gift cards (one $25 and four $15). Anonymity was preserved as responses were not associated with individuals. Email addresses of those who completed the surveys were retrieved – separately from responses – so that the gift card drawing could be completed.

4.1 Survey Development

The survey questions used for each construct (see the Appendix) were derived from those used in Ng et al. (2009) and Claar and Johnson (2010). The items in the survey focused on eight constructs including seven IVs and one dependent variable. All items are anchored on 5-point Likert scales.

4.2 Data Analysis

We conducted a three-step analysis to examine the effects of the key constructs on the email security behavior dependent variable (BEH). First, an exploratory factor analysis was done to extract the factors (latent variables) to validate our model constructs. Second, a multiple regression analysis was conducted using the SPSS calculated factor scores. The dependent variable was regressed on the seven IVs to determine the main effects (Model 1). Last, the moderating variables, perceived severity and prior experience were added into the regression model to examine the interaction effects of those IVs (Model 2).

4.2.1 Construct Validity and Reliability

We first conducted the factor analysis (using primary axis analysis) on the data set to extract the factors that influence students' email security behaviors. As expected, eight factors were extracted, which are consistent with the eight constructs shown in Figure 1. We use 0.5 as the factor loading threshold given the size of our data set (Hair, Tatham, Anderson, & Black, 1998). Accordingly, three survey questions having a factor loading lower than 0.5 were removed from further consideration:

- CUE3: If my computer is attacked by someone, I would be concerned I had improperly handled unsafe emails. (disagree/agree)
- EXP1: How frequently do you receive unsafe emails in your inbox(es)? (never/a great deal)
- SEV3: If my computer is infected by a virus as the result of unsafe email practices, my daily work/schoolwork/social life could be negatively affected. (disagree/agree)

We further examined internal consistency to test the interrelatedness of a sample of items. To evaluate the reliability of the data, Cronbach Alpha coefficients were calculated for each latent variable. The acceptable value of Cronbach Alpha should be at least 0.70 (Nunnally & Bernstein, 1994). Table 5 summarizes the factor loadings and Cronbach Alpha values for each item. The factor loadings for all items are greater 0.5 and the Cronbach Alpha values for all factors are greater than 0.7, which indicates that our survey questions load properly onto our model constructs, allowing us to proceed with our regression analysis and hypothesis testing.

Construct	*Item*	*Factor loadings*	*Cronbach Alpha*
BEH			0.789
	BEH1	.521	
	BEH2	.736	
	BEH3	.659	
	BEH4	.849	
BAR			0.775
	BAR1	.643	
	BAR2	.546	
	BAR3	.725	
	BAR4	.804	
EFF			0.922
	EFF1	.891	
	EFF2	.897	
	EFF3	.784	
	EFF4	.789	
CUE			0.811
	CUE1	.822	
	CUE2	.865	
	CUE4	.584	
EXP			0.809
	EXP2	.887	
	EXP3	.794	
	EXP4	.658	
VUL			0.95
	VUL1	.955	
	VUL2	.995	
	VUL3	.848	
BEN			0.913
	BEN1	.557	
	BEN2	.860	
	BEN3	.887	
	BEN4	.942	
	BEN5	.775	
SEV			0.83
	SEV1	.824	
	SEV2	.821	

Table 5. Construct Validity and Reliability

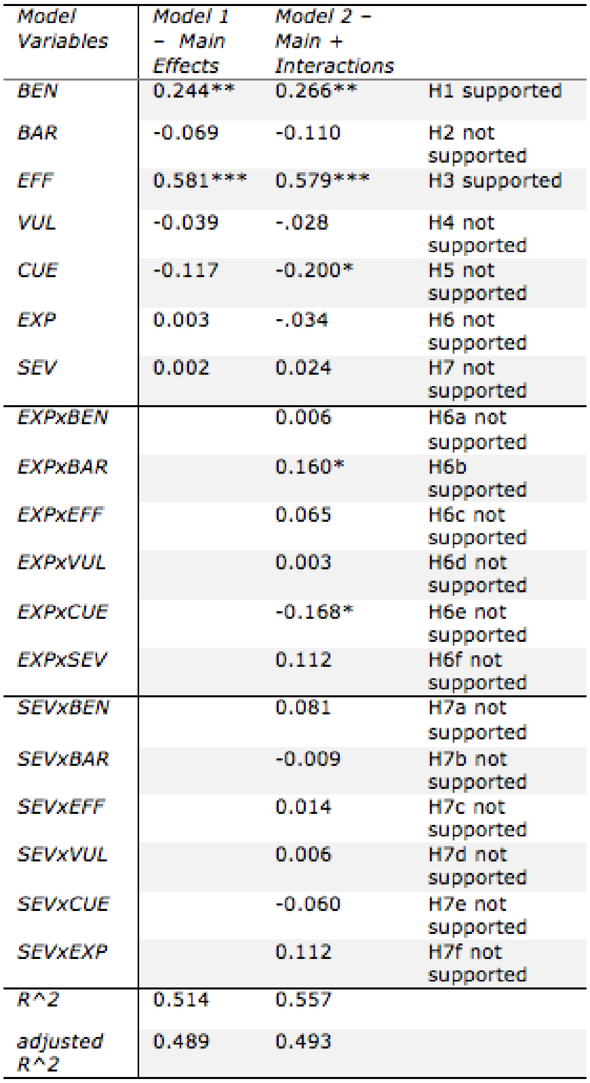
4.2.2. Hypothesis Testing

To test the hypotheses, a multiple regression analysis was conducted using SPSS. First, the dependent variable, email security behavior was regressed on the seven IVs to examine the main effects. Next, the moderator variables were considered to further evaluate the interaction effects of the prior experience and perceived severity on other constructs. Table 6 shows the results of hypothesis testing using moderated multiple regression. In Model 1, the latent variables, perceived benefits and self-efficacy had significant coefficients as expected. Both the perceive benefits and self-efficacy had a significant, positive effect on email security behavior. Thus, H1 and H3 were supported. In Model 2, the perceived benefits and self-efficacy still had a significant, positive effect on email security behavior. Besides that, prior experience also significantly reduced the negative effect of the perceived barriers on email security behavior. Thus, H6b was supported. It is interesting to find that the coefficients on cues to action and interactions between cues to action and prior experience are negative and significant, which is contradicting with our hypotheses. A detailed discussion is presented in the next section.

5. DISCUSSION

The results show that only three of the seven IVs - perceived benefits (BEN), self-efficacy (EFF), and cues to action (CUE) - are significant determinants of our subjects' email security behavior and that only two of them, BEN and EFF support our hypotheses. One possible explanation for these findings could be the relative immaturity of the subjects. These youngsters have likely failed to have enough experience with security issues in general to limit their rationalizations on this topic only to those that have the most immediate and easily identifiable impacts on their behaviors: their belief that they will benefit from the behaviors (BEN), the potential to reduce the risk of a security incident occurring, and their understanding of their own capabilities in regards to performing the behaviors (EFF). Self-efficacy may be the most easily assessable construct for these young subjects.

The remaining factors might require more life experience – or "wisdom" - before these individuals can truly appreciate and assess them. It might be difficult for these young, immature students to judge their vulnerability (VUL) to email-related security incidents or the true potential impact of such incidents (SEV) or truly understand the difficulty (or ease) of performing the security behaviors.



Model Variables	*Model 1 – Main Effects*	*Model 2 – Main + Interactions*	
BEN	0.244**	0.266**	H1 supported
BAR	-0.069	-0.110	H2 not supported
EFF	0.581***	0.579***	H3 supported
VUL	-0.039	-.028	H4 not supported
CUE	-0.117	-0.200*	H5 not supported
EXP	0.003	-.034	H6 not supported
SEV	0.002	0.024	H7 not supported
EXPxBEN		0.006	H6a not supported
EXPxBAR		0.160*	H6b supported
EXPxEFF		0.065	H6c not supported
EXPxVUL		0.003	H6d not supported
EXPxCUE		-0.168*	H6e not supported
EXPxSEV		0.112	H6f not supported
SEVxBEN		0.081	H7a not supported
SEVxBAR		-0.009	H7b not supported
SEVxEFF		0.014	H7c not supported
SEVxVUL		0.006	H7d not supported
SEVxCUE		-0.060	H7e not supported
SEVxEXP		0.112	H7f not supported
R^2	0.514	0.557	
adjusted R^2	0.489	0.493	

Table 6. Regression Model Coefficients – Hypothesis Tests

An interesting result is the negative coefficient associated with the cues to action variable (CUE). This finding is counter to our hypothesis. Upon reflection and a review of our survey questions that reflect on this construct, we can see a possible explanation. Here, again, are the questions that loaded on the construct:

- (CUE1) If I saw a news report or read a newspaper or magazine article about a crime related to unsafe emails, I would be more concerned about opening or clicking links within emails. (disagree/agree)
- (CUE2) If a friend were to tell me of a recent experience with identity theft related to a suspicious email, I would be more conscious of opening emails or clicking links within emails. (disagree/agree)
- (CUE4) If I received an email from the Help Desk of my university about risks posed by unsafe emails, I would be more concerned about opening emails or clicking links within emails. (disagree/agree)

This inconsistency in the results (significant coefficient but its sign being the opposite of our hypothesis) may be the result of a significant number of participants having a faulty perception of cues to action. The word ‘perception’ is key here. The questions asked are focused on a predicted response to a hypothetical situation, not a specific measurement of a cue to action, such as how often the IT helpdesk sends out alert messages. This might confound the results if the students’ predictions don’t necessarily line up with their self-reported behaviors.

Regarding the interaction effects, we did not find any significant effects between perceived severity and other core constructs. Again, this might be due to the subjects’ lack of awareness (or experience) of security attacks. We did find that the prior experience has a significant moderating effect on perceived barriers (EXPxBAR). This still fits that immaturity analysis: if a subject has prior experience of security attacks caused by unsafe emails, and he or she is more likely to underestimate the barriers, they will probably be more likely to take appropriate email security behaviors.

A significant difference exists between males and females in the latent variable scores for self-efficacy (EFF) and behavior (BEH) calculated during the exploratory factor analysis. These differences will be analyzed and presented in future research.

There are some limitations worth noting with this research. While the sample size was acceptable, a much larger sample would give more reliable statistical results. Finding ways to improve survey response rates would help with this. This survey was limited to students at a single university. Getting students from other schools to participate in the survey would help increase sample size and, more importantly, increase the diversity of the sample and therefore its external validity. Potential issues with the prior experience construct were noted above. The questions reflecting on this construct might need to be rethought. Finally, the applicability of these results is limited by the fact that our subjects were undergraduate students. It would be interesting to see how this same research question would be answered by a broader sample of the population at large.

We should note that Ng et al. (2009) ran a very similar survey with part-time, working students and individuals employed in IT-related organizations with a similar sample size and found only three significant determinants (equivalent to our BEN, EFF, and VUL) which match two of those we found to be significant. Both studies had similar R-squared numbers. Could this be an indicator that the HBM might not be the proper model to explain email security behavior? With our small sample sizes, such an inference might be unwise.

While it is difficult to infer anything from our study's CUE findings, the BEN and EFF significance findings indicate that campus IT departments and computing and technology instructors can make a substantial, positive impact on student email security behaviors by educating students on the risks they take by not practicing good email security behaviors and by educating them on how to properly execute email security behaviors. Since BEN and EFF have a significant impact on students' self-reported email behaviors, instructors and IT departments should work to increase students' knowledge about the perceived benefits of these behaviors and also work to improve students' email security self-efficacy.

The perceived benefits (BEN) result can be exploited by instructors through more detailed discussion, possibly through case studies, of the impacts of email security misbehavior. IT departments can send notices to students reminding them of the risks they are taking if they do not practice secure behaviors. Reports from IT departments to the students and staff regarding the costs the university faces by responding to security issues and what caused the issues in the first place could also help students understand the benefits of good practices. Something as simple as a monthly update from the IT department indicating the number of security-related helpdesk tickets were handled and the hours taken to mitigate those problems could provide a reminder to students to take IT security seriously.

The self-efficacy (EFF) result can be exploited by faculty by including specific lessons and assignments that teach students how to examine email headers – for legitimate sender information - without opening the email, how to review the URLs in links in emails and recognize phishing and pharming URLs before actually clicking on them, and other indicators that an email may not be legit (poor grammar, generic references to IT departments, unsolicited emails, unknown senders, etc.) IT departments can reinforce students' self-efficacy through reminders throughout their time on campus and possibly through testing the students and staff with mock SPAM and phishing/pharming emails that catch users that do not apply appropriate secure precautions when opening, reading, and taking action regarding emails and remind them that they just failed a test of their email security behaviors.

6. CONCLUSIONS

A survey was developed based on the HBM and conducted at a public university to understand students' intentions and behaviors when using emails. It is found that self-efficacy and the perceived benefits are the important factors that affect students' email security behaviors.

Understanding people's intentions and behaviors when using technologies is just the first step towards the goal of providing effective education and policies on security and privacy related to the use of technologies. This study sheds light on new endeavors that educators could try in the future to better educate students how to protect their security and privacy when using technologies.

7. REFERENCES

Claar, C. L., & Johnson, J. (2012). Analyzing home PC security adoption behavior. Journal of Computer Information Systems, 52(4), 20-29.

Grama, J., & Vogel, V. (2017). Information security: Risky business. EDUCAUSE Review, 52(1), 22.

Hair, J., Tatham, R., Anderson, R., & Black, W. (1998). Multivariate data analysis. London: Prentice-Hall.

Internal Revenue Service, 2017 https://www.irs.gov/uac/newsroom/phishing-schemes-lead-the-irs-dirty-dozen-list-of-tax-scams-for-2017-remain-tax-time-threat accessed 6/1/2017.

Ng, B. Y., Kankanhalli, A., & Xu, Y. C. (2009). Studying users' computer security behavior: A health belief perspective. Decision Support Systems, 46(4), 815-825.

Matthews, E. 2017. https://www.afcea.org/content/?q=node/17346/ accessed 6/1/2017.

Nunnally, J., & Bernstein, L. (1994). Psychometric theory. New York: McGraw-Hill Higher Ed.

Rosenstock, I. M. (1974). Historical origins of the health belief model. Health education monographs, 2(4), 328-335.

Rosenstock, I. M., Strecher, V. J., & Becker, M. H. (1988). Social learning theory and the health belief model. Health Education Quarterly, 15(2), 175-183.

Symantec (2017), Internet Security Threat Report, Volume 22. https://www.symantec.com/security-center/threat-report. accessed June 1, 2017.

Walker, L. R., & Thomas, K. W. (1982). Beyond expectancy theory: An integrative motivational model from health care. Academy of Management Review, 7(2), 187-194.

Williams, C. K., Wynn, D., Madupalli, R., Karahanna, E., & Duncan, B. K. (2014). Explaining Users' Security Behaviors with the Security Belief Model. Journal of Organizational and End User Computing (JOEUC), 26(3), 23-46.

Appendix

Survey Questions (Likert Scale End Points Indicated in Parentheses)

CONSTRUCT	Questions
BEHAVIOR (BEH)	(BEH1) Before opening an email, I first check if the subject and sender make sense. (never/every time)
	(BEH2) Before opening an email attachment, I first check if the filename of the attachment makes sense. (never/every time)
	(BEH3) Before clicking on a link in an email, I first check to see if the URL for the link makes sense. (never/every time)
	(BEH4) Before opening an email attachment, I first check to see if the contents and sender of the email make sense. (never/every time)
BARRIERS (BAR)	(BAR1) Being on the alert for unsafe emails is time consuming. (disagree/agree)
	(BAR2) The expense of being on the alert for unsafe emails is a concern for me. (disagree/agree)
	(BAR3) Being on the alert for unsafe emails would require changing my email habits, which is difficult. (disagree/agree)
	(BAR4) Being on the alert for unsafe emails would require substantial investment in effort other than time. (disagree/agree)
SELF-EFFICACY (EFF)	(EFF1) I am confident I can recognize unsafe emails. (disagree/agree)
	(EFF2) I am confident I can recognize unsafe email attachments. (disagree/agree)
	(EFF3) I am confident I can recognize unsafe links in emails. (disagree/agree)
	(EFF4) I can recognize unsafe emails even if no one was around to help me. (disagree/agree)
CUES TO ACTION (CUE)	(CUE1) If I saw a news report or read a newspaper or magazine article about a crime related to unsafe emails, I would be more concerned about opening or clicking links within emails. (disagree/agree)
	(CUE2) If a friend were to tell me of a recent experience with identity theft related to a suspicious email, I would be more conscious of opening emails or clicking links within emails. (disagree/agree)
	(CUE3) If my computer is attacked by someone, I would be concerned I had improperly handled unsafe emails. (disagree/agree)
	(CUE4) If I received an email from the Helpdesk of my university about risks posed by unsafe emails, I would be more concerned about opening emails or clicking links within emails. (disagree/agree)
PRIOR EXPERIENCE (EXP)	(EXP1) How frequently do you receive unsafe emails in your inbox(es)? (never/a great deal)
	(EXP2) How frequently have you be affected by unsafe emails? (never/a great deal)
	(EXP3) How recently have you been affected by unsafe emails? (never/in the last week)
	(EXP4) The level of impact I have experienced due to receiving unsafe emails is? (no impact/major impact)
PERCEIVED VULNERABILITY (VUL)	(VUL1) There is a good chance that I will receive an unsafe email. (disagree/agree)
	(VUL2) There is a good chance I will receive an email with an unsafe email attachment. (disagree/agree)

	(VUL3) There is a good chance I will receive an email containing links to phishing sites. (disagree/agree)
PERCEIVED BENEFITS (BEN)	(BEN1) Being on the alert for unsafe emails is effective in preventing viruses from infecting my computer. (disagree/agree)
	(BEN2) Checking if the sender and subject make sense before opening an email is effective in preventing viruses from infecting my computer. (disagree/agree)
	(BEN3) Checking if the filename of the attachment makes sense before opening an email is effective in preventing viruses from infecting my computer. (disagree/agree)
	(BEN4) Exercising care before opening email attachments is effective in preventing viruses from infecting my computer. (disagree/agree)
	(BEN5) Exercising care before clicking on links in emails is effective in preventing viruses from infecting my computer. (disagree/agree)
PERCEIVED SEVERITY (SEV)	(SEV1) Having my computer infected by a virus as the result of unsafe email practices is a serious problem for me. (disagree/agree)
	(SEV2) Putting the school's network at risk because of unsafe email practices is a serious problem for me. (disagree/agree)
	(SEV3) If my computer is infected by a virus as the result of unsafe email practices, my daily work/schoolwork/social life could be negatively affected. (disagree/agree)