CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

Volume 3, No. 2
October 2024
ISSN: 2832-1006

In this issue:

4. **Consumer Acceptance of Biometric Credit Cards as an Identify Proofing Mechanism**
Laura Poe, Longwood University

12. **Teaching Public Key Cryptography: A Software Approach**
David Carlson, Saint Vincent College

21. ***Teaching Case***
Digital Forensics and Incident Response (DFIR): A Teaching Exercise
Jennifer L. Breese, Penn State Greater Allegheny
Maryam Roshanaei, Penn State Abington College
J. Andrew Landmesser, Penn State Brandywine
Brian Gardner, Penn State Schuylkill

35. **Phishing: Gender Differences in Email Security Perceptions and Behaviors**
Jie Du, Grand Valley State University
Andrew Kalafut, Grand Valley State University
Gregory Schymik, Grand Valley State University

48. **Feasibility of Creating a Non-Profit and Non-Governmental Organization Cybersecurity Incident Dataset Repository Using OSINT**
Stanley J. Mierzwa, Kean University
Iassen Christov, Kean University

iscap
Information Systems
& Computing
Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

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 ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings 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 CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

Phishing: Gender Differences in Email Security Perceptions and Behaviors

Jie Du
dujie@gvsu.edu

Andrew Kalafut
kalafuta@gvsu.edu

Gregory Schymik
schymikg@gvsu.edu

School of Computing
Grand Valley State University
Allendale, MI 49401, USA

Abstract

Information security is a major concern for everyone nowadays. While substantial research exists on gender differences in education and technology, there appears to be very little research on gender differences in information security and that research examines a broad list of self-reported information security behaviors in a single study. Our research adds to the literature by examining in more depth one specific area of information security behavior: peoples' behavior relating to phishing attacks. This research attempts to investigate gender differences in email security perceptions and behaviors by surveying students, faculty, and staff at one midwestern public, master's granting university. The survey questions are developed based on the Health Belief Model. 414 usable survey response sets were collected and analyzed. The findings suggest that men and women have different perceptions on self-efficacy, vulnerability, barriers, cues to action, and self-reported security behaviors. While the Health Belief Model provides a relatively good fit in explaining email security behaviors for both men and women, each group appears to value each of the underlying factors differently. The findings shed light on how to design and conduct security training to increase adoption of protective email behaviors.

Keywords: Security behaviors, security perceptions, gender difference, phishing, health belief model, email.

Recommended Citation: Du, J., Kalafut, A., Schymik, G., (2024). Phishing: Gender Differences in Email Security Perceptions and Behaviors. *Cybersecurity Pedagogy and Practice Journal,* v3(n2) pp 35-47. https://doi.org/10.62273/PELX2965

Phishing: Gender Differences in Email Security Perceptions and Behaviors

Jie Du, Andrew Kalafut and Gregory Schymik

1. INTRODUCTION

Anyone paying attention to current events in academia has seen multiple reports of cyber-attacks on universities and many members of the academy can say, with confidence, that their institution has experienced some sort of significant cyber-attack resulting in some sort of network access by unauthorized persons with intentions to profit in some way from their attacks. A 2018 report on cybersecurity in education identifies the education industry as the lowest cybersecurity performer compared to all other industries (SecurityScorecard, 2018). According to atlasVPN (2022), over 80% of malware attacks around the world were found to be targeting the education industry. In 2021 alone, ransomware attacks against US schools and colleges have been estimated to have cost at least $3.5 billion in downtime (Bischoff, 2022). Most of these attacks are the result of successful phishing attacks.

Given the constant funding pressures faced by universities, they are forced to seek out lower cost solutions to security challenges. The most obvious of these low-cost solutions to problems caused mostly by human behaviors (responses to phishing attacks) is training the users of the systems to be vigilant against these phishing attacks. To do this, institutions must understand the drivers of those behaviors. A part of that understanding must include understanding the differences between security perceptions and behaviors between genders, assuming they occur, so that training can be better targeted to specific people to address their specific needs and tendencies. This paper attempts to aid in that understanding.

We follow others in the IS literature and apply the Health Belief Model - a theoretical model built off of the Technology Acceptance Model, the Theory of Planned Behavior, Protection Motivation Theory, and Expectancy-Value Theory – to the examination of the email security behaviors of students, faculty, and staff at a Midwest, master's-granting university in the United States. We previously investigated gender differences in email security perception and behaviors in male and female students. This paper expands on that earlier work (Du & Schymik, 2018) with a broader sample of students, faculty, and staff in the institution and aims to investigate the gender-related determinants to people's email security behavior, including whether these determinants are different between students and faculty/staff.

2. LITERATURE REVIEW

Gender Differences in Cybersecurity

Gender differences in a variety of cybersecurity issues have been investigated in previous literature. Anwar et al. (2017) investigated gender differences related to a wide variety of security issues, including email, malware, social media privacy, passwords, backups, and protection of sensitive information. They found significant differences in self-reported behaviors. However, since they considered a variety of behaviors in a single construct it is difficult to determine what specific behaviors are influenced by gender. McGill and Thompson (2021) studied gender differences in security and privacy behaviors, finding differences in 40% of the behaviors studied, with men practicing more preventive security and privacy behaviors than women.

Farooq et al. (2015) examined information security awareness, knowledge, and behaviors among university students, finding male students to have better awareness knowledge, and behaviors than female students. Conversely, McCormac et al. (2017) found better information security awareness among females, in a study of working Australians. Combined, these indicate that gender differences among students may not match those of employees, motivating our effort to study gender differences in the two populations separately.

More specific to email, the literature on gender differences and phishing attacks shows some mixed results on the subject. Sheng et al. (2010) found that women fell for phishing attacks more often that did men while Diaz et al. (2020), and Benenson et al. (2017) found no differences in susceptibility. Verkijika (2019) found no differences in mobile phishing avoidance motivation and behavior, but they did find that gender was a significant moderator of the effect of anti-phishing self-efficacy on both of those factors.

Health Belief Model

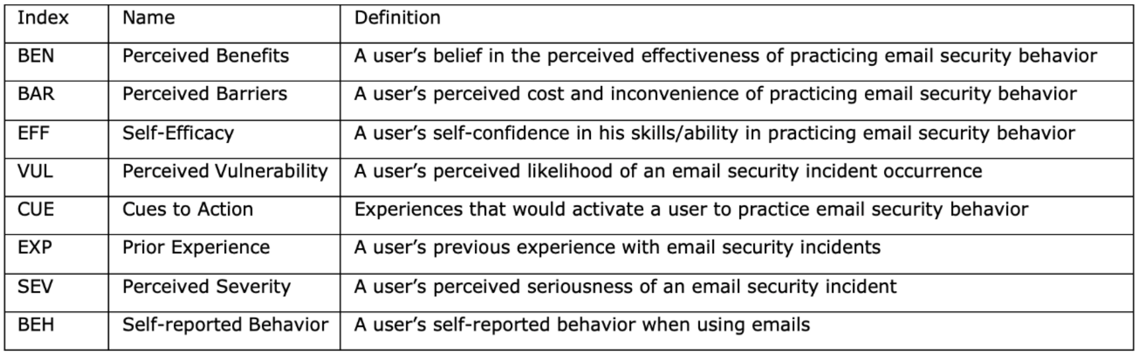
In healthcare, preventive healthcare behaviors are behaviors that will lessen the harmful effects of diseases, such as vaccination, diet, and exercise. In computer security, protective security behaviors are those behaviors that will lessen the harmful effects of security incidents, such as using antivirus software or checking URLs before clicking on them. Although the fields of healthcare and security are very different, these ideas are significantly similar: both are behaviors that people can follow in order to protect themselves from potential harm. Therefore, it is reasonable to consider that similar theories may explain both.

The Health Belief Model (HBM) was originally developed to explain preventive health behaviors (Rosenstock, 1974). In early versions of the model, a person's attitude towards preventive health behaviors was considered a function of the perceived susceptibility and perceived severity of the illness, as well as the perceived benefits and perceived barriers to performing the preventive health behavior. Later work, a decade after the original, added three additional variables: self-efficacy, cues to action, and general health orientation (Janz, 1984).

Relying on the similarity of the preventive health and protective security behaviors, the HBM has since been applied to explain protective security behaviors. Such applications have covered several security domains, including the use of email (Ng et al., 2009), the adoption of computer security software (Claar et al., 2013), and how to prevent unauthorized access to computers (Williams et al., 2014), and the use of antivirus software (Dodel & Mesch, 2017).

Health Belief Model and Gender Differences

In the healthcare field, differences in HBM factor significance by gender have been observed in several studies. For example, perceived barriers and self-efficacy were significant determinants of oral hygiene behaviors among males, while only self-efficacy was significant among females (Zetu et al., 2014). As a further example, gender has been shown to be a common modifying factor in applying the HBM to COVID-19 vaccine hesitancy (Limbu et al., 2022).



Index	Name	Definition
BEN	Perceived Benefits	A user's belief in the perceived effectiveness of practicing email security behavior
BAR	Perceived Barriers	A user's perceived cost and inconvenience of practicing email security behavior
EFF	Self-Efficacy	A user's self-confidence in his skills/ability in practicing email security behavior
VUL	Perceived Vulnerability	A user's perceived likelihood of an email security incident occurrence
CUE	Cues to Action	Experiences that would activate a user to practice email security behavior
EXP	Prior Experience	A user's previous experience with email security incidents
SEV	Perceived Severity	A user's perceived seriousness of an email security incident
BEH	Self-reported Behavior	A user's self-reported behavior when using emails

Table 1: The Definitions of Constructs in the Research Model

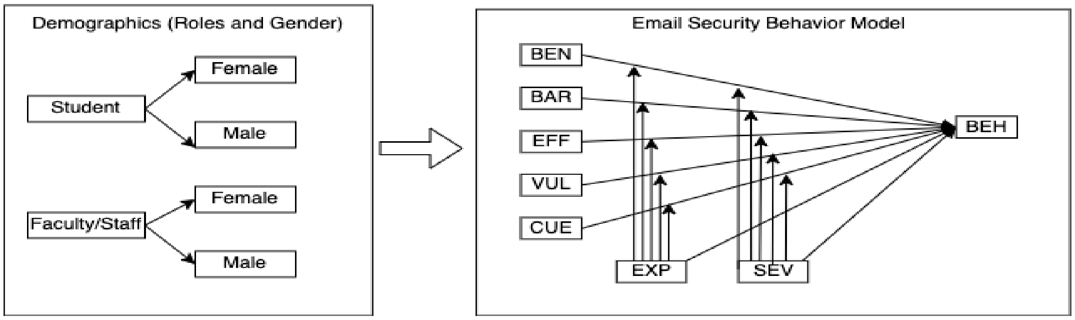


Figure 1: The Research Model

In the security field, gender differences in the HBM have been less explored. However, the problem has been approached by Anwar et al. (2017), who found significant gender differences on self-efficacy, prior experience, and computer skills among a group of employees. Their study does not include students. Fatokun et al. (2019) explored gender differences in the cybersecurity behaviors of students at Malaysian universities, using a model based off of the HBM combined with protection motivation theory. They found higher self-efficacy among males and higher perceived severity among females. Although they used a new model based on the health belief model, not the HBM itself, since these factors are also used in the HBM they may imply gender differences in the corresponding HBM constructs.

Although not much previous work appears to have been done on investigating gender differences in the application of the health belief model to cybersecurity, the fact that gender differences have been observed in cybersecurity, and the fact that gender differences have been observed in the application of the health belief model to healthcare, indicates that this may be a promising avenue to gain insight into the causes of gender differences in cybersecurity.

3. RESEARCH MODEL AND HYPOTHESES

This study aims to investigate gender-related determinants to peoples' email security behaviors and whether these determinants are different between their professional roles (e.g., Student vs faculty/staff). We hope that knowledge of such differences may shed light on how to design and conduct security training to increase adoption of beneficial email security behaviors. The research model used in this study is based upon the research model from our prior study (Schymik & Du, 2018) (see Figure 1). Demographics including professional role and gender are taken into consideration when examining people's email security behaviors. The model measures the main effects of the constructs and the interaction effects moderated by prior experience and perceived severity. Table 1 describes each construct.

Our research begins by asking two broad questions of the dataset collected in prior research. The first examines the latent variables in the model and asks if there are difference between the 8 latent variables generated by our subjects' survey responses between the genders.

- Q1: Do gender differences exist in our subjects' security perceptions and behaviors?

The second question looks at the results of the regression analysis performed using the latent factor scores and asks if gender impacts which factors in the model are significant.

- Q2: Do the factors that impact people's email security behavior differ by gender?

Gender differences were identified in our previous study (Du & Schymik, 2018). This study expands that research by surveying a larger sample including students, faculty, and staff at a university with aim of investigating the gender-related determinants to their email security behaviors. This larger sample population provides us the opportunity to explore whether professional roles (student vs faculty/staff) have an impact on email security perceptions and behaviors. It has been noted that the higher education workforce has higher levels of information security awareness than do students and might perceive information security compliance as a protective measure that may prevent security-breach-related disasters (Sari et al., 2016). Pursuing the suggestion that other underlying factors may have a significant effect on email security behavior (Greitzer et al., 2021) and noting that our latest work on this data set indicated differences between the two professional roles (Authors 2023, under review), we extend the initial research questions to investigate the impact professional role may have on gender differences in email security perceptions and behaviors:

- Q3: Do gender differences exist within the professional roles (student vs faculty/staff)?
- Q4: Do the factors that impact people's email security behaviors within professional roles differ by gender?

We originally posited two hypotheses:

- H1: There are gender differences in people's email security perception and behaviors.
- H2: Determinants of men's and women's security behaviors are different.

Acknowledging that these hypotheses may be too broadly defined, we focus on Q3 and Q4 above, and expand our two initial hypotheses to explore the within group gender differences:

- H3: Gender differences in people's email security perception and behaviors exist among students.
- H4: Gender differences in people's email security perception and behaviors exist among faculty/staff.
- H5: Determinants of security behaviors differ between genders among students.

- H6: Determinants of security behaviors differ between genders among faculty/staff.

Please note that due to page length limitations, the research questions and hypotheses are stated generically instead of listing one for each of the latent variables in the research model where appropriate.

4. METHODOLOGY

Participants and Procedure

The target population for this study was students, faculty, and staff at one midwestern public, master's-granting university in the United States. A random sample of the target population was contacted via email and invited to participate by completing an anonymous online questionnaire. The email provided the purpose and procedure to participants in this study along with other information required by the university. All participants were 18 or over and consented to participate.

Survey Development

An electronic Likert-scale questionnaire was developed to measure the constructs in our research model (see Appendix A). The first section of the survey contains 8 items on demographics. The second section of the survey contains 32 items to measure the participants' security perceptions and behaviors validated from prior research (Ng et al., 2009) (Claar et al., 2013). The items to measure the model constructs are anchored on a 5-point scale, which ranged from strongly disagree (1) to strongly agree (5) for most of the items. The scales used for the items that measure security behavior and prior experience are different. The 5-point Likert scale ranged from never (1) to every time (5) for security behavior and from never (1) to a great deal (5) for prior experience. The survey was anonymous and administered using the Qualtrics online survey platform. The Internal Review Board (IRB) of the university approved the study.

We sent out the survey to a random sample of students and a random sample of faculty/staff at the aforementioned university. After removing responses with missing data, the date collection yielded 417 remaining survey response sets. The gender question in the demographic section of the survey presented three options: male, female, and other. Only three responses chose "other" for this question. Due to the very small number of responses in this category, these responses were excluded from further analysis, resulting in 414 total response sets used in our analysis. The whole dataset contains 149 male subjects and 265 female subjects. Our sample shows a similar female to male ratio (64%/36%) to the gender distribution in the population (61%/39%) and thus is representative of the university community. Figure 2 shows the gender distribution in our datasets.

Data collected in this study were analyzed in three different datasets. The whole dataset contains all 414 response sets. Based on the participants' role at the university, the whole dataset was divided into a student dataset of 100 students and an employee dataset of 314 employees. Each dataset was further split into two gender groups.

To test the hypotheses for each dataset, a three-step analysis was conducted. First, an exploratory factor analysis was conducted to extract factors that impact the participants' email security behaviors. As a result, eight factors were extracted; these factors are consistent with the eight constructs in our research model. Cronbach Alpha coefficients were calculated for each latent variable..

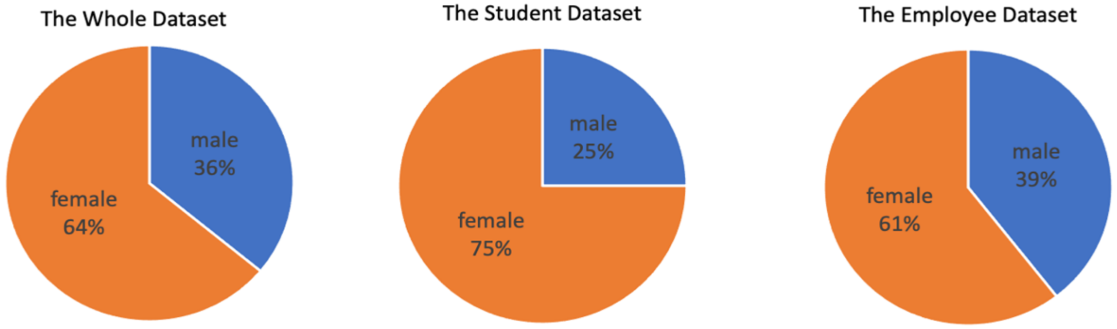


Figure 2: Gender Distribution Data Analysis

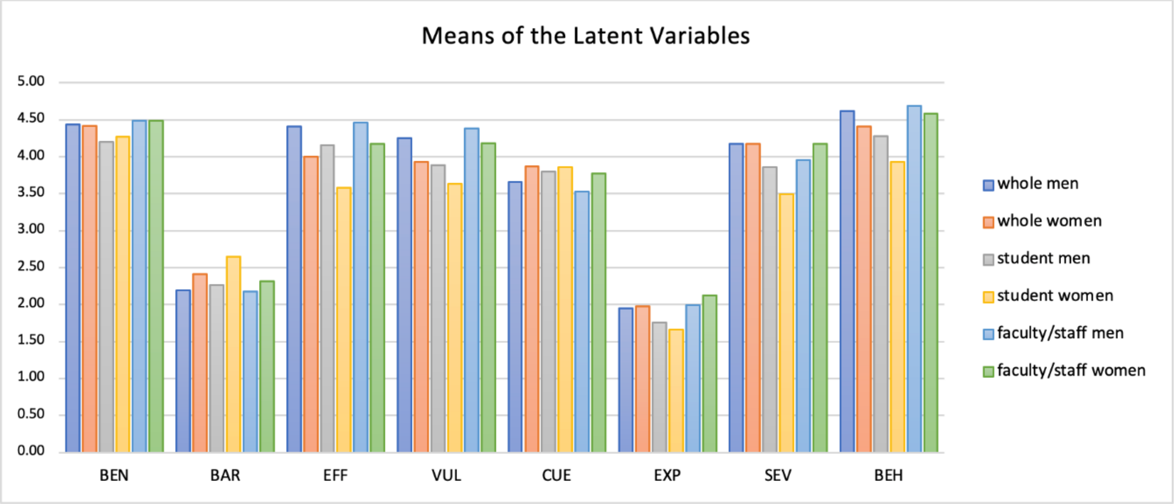


Figure 3: Means of the Latent Variables

All constructs exhibited acceptable construct validity and reliability, allowing us to proceed with our regression analysis. Second, an independent-samples two-tailed *t*-test was conducted to compare means of each latent variable in the two gender groups (see Figure 3) to investigate whether significant differences exist on any latent variable based on gender. Finally, a regression analysis (main effects first and interaction effects second) for each gender group in each dataset was conducted to examine whether women and men value the factors impacting their security behaviors differently. All the data were analyzed using IBM Statistical Package for Social Science (SPSS) version 25. All statistical tests were conducted with an alpha level of <0.05.

5. RESULTS

Gender differences were detected in all 3 datasets. In this section, the data analysis results were organized based on the dataset. In each dataset, the results of the *t*-test on the mean of each variable are reported first. An independent two-tailed *t*-test was run on each of the three datasets, resulting in 3 examinations (see Tables 2 – 4). Followed were the regression analysis results. The research model was assessed separately for each gender group in each of the three datasets, thus resulting in 6 examinations (see Tables 5 - 6).

Whole Dataset

For the whole dataset, the mean values between women and men were statistically different on five variables: EFF, VUL, BAR, CUE, and BEH. No gender differences existed on other factors. These results indicate support for H1. Table 2 shows the *t*-test results on the whole dataset. These results suggest that men have higher levels of perceived self-efficacy and perceived vulnerability, and self-report better security behaviors than women do. In contrast, women have higher levels of perceived barriers and cues to action than do men.

	Men		Women		t	P	Sign. Diff?
	(N=149)		(N=265)				
	Mean	SD	Mean	SD			
BEN	4.44	0.70	4.42	0.62	0.271	.787	ns
BAR	2.19	0.74	2.41	0.77	-2.828	.005	**
EFF	4.41	0.62	4.00	0.78	5.506	.000	***
VUL	4.25	0.73	3.93	0.81	4.079	.000	***
CUE	3.66	0.81	3.87	0.62	-2.849	.005	**
EXP	1.95	0.86	1.99	0.80	-0.437	.662	ns
SEV	4.17	0.97	4.17	0.85	-0.101	.919	ns
BEH	4.62	0.48	4.41	0.68	3.751	.000	***

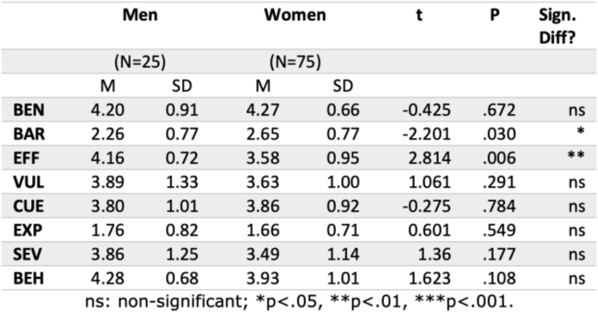
ns: non-significant; *p<.05, **p<.01, ***p<.001.

Table 2: Comparison of Means in the Whole Dataset

The results of the regression indicated that: (1) in the main effect model (see Table 5), while women's email behaviors are influenced by EFF, VUL, EXP, and BAR, men's email behaviors are only influenced by EFF, and (2) in the interaction effect model (see Table 6), EFF, EXP, VUL, BEN, EXPxBEN, EXPxVUL, and SEVxEFF are the significant determinants on women's email behavior while EFF remains the only significant factor that impact men's email behavior. These results support H2. These results suggest that while men's decision-making process regarding practicing protective email security behaviors is mainly influenced by their self-efficacy, women's decision-making process regarding the same behaviors is impacted by several factors (including self-efficacy, like men).

Student Dataset

For the student dataset, there was a significant difference in the mean values of EFF and BAR for men and women. No gender differences existed on other factors. H3 was supported. Table 3 shows the *t*-test results on the student dataset. These results suggest that the male students have higher self-efficacy to practice protective email behaviors than their female peers while the female students have higher perceived barriers of practicing protective email behaviors than their male peers.



	Men		Women		t	P	Sign. Diff?
	(N=25)		(N=75)				
	M	SD	M	SD			
BEN	4.20	0.91	4.27	0.66	-0.425	.672	ns
BAR	2.26	0.77	2.65	0.77	-2.201	.030	*
EFF	4.16	0.72	3.58	0.95	2.814	.006	**
VUL	3.89	1.33	3.63	1.00	1.061	.291	ns
CUE	3.80	1.01	3.86	0.92	-0.275	.784	ns
EXP	1.76	0.82	1.66	0.71	0.601	.549	ns
SEV	3.86	1.25	3.49	1.14	1.36	.177	ns
BEH	4.28	0.68	3.93	1.01	1.623	.108	ns

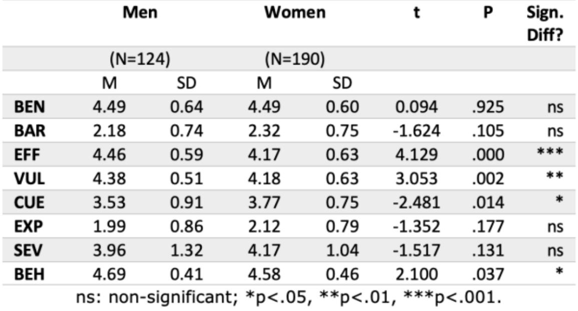
ns: non-significant; *p<.05, **p<.01, ***p<.001.

Table 3: Comparison of Means in the Student Dataset

The results of the regression show that: (1) in the main effect model (see Table 5), EFF and EXP are the two significant determinants for the email behavior in the female student group while EFF and BAR are the significant determinants to the male students' email behaviors, and (2) in the interaction effect model (see Table 6), EFF, EXP, and SEVxBAR are the significant determinants to the female students' email behaviors while no factor was found to significantly impact the male students' email behaviors. H5 was supported. These results in the main effect model suggest that self-efficacy is a factor that impact both the male and female students regarding their email behaviors. Besides self-efficacy, the female students are more influenced by prior experience while the male students are more focused on perceived barriers when practicing email behaviors. It is interesting to note that none of the factors impacted the male students' behaviors when the interaction effects were taken into consideration. This will be addressed in the discussion section.

Employee Dataset

There was a significant difference in the mean values of BEH, EFF, CUE, and VUL for the male and female employees. Table 4 shows the *t*-test results on the employee dataset. H4 was supported. These results suggest that the male employees had higher levels of self-efficacy and perceived vulnerability and self-reported better email security behaviors than their female peers. On the other hand, the female employees were more influenced by cues to action when practicing such behaviors than their male peers.

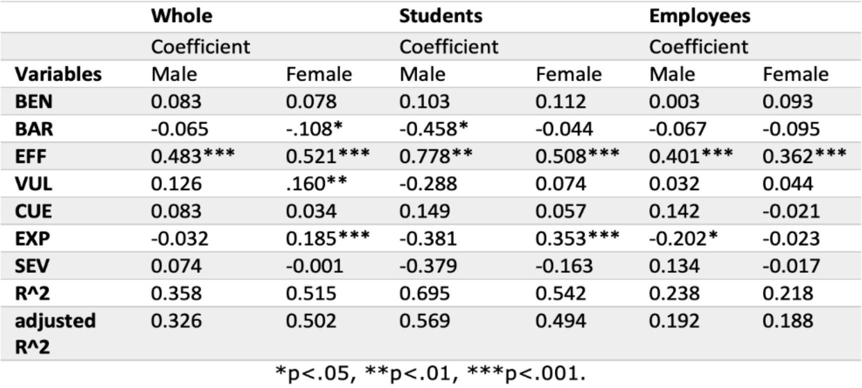


	Men		Women		t	P	Sign. Diff?
	(N=124)		(N=190)				
	M	SD	M	SD			
BEN	4.49	0.64	4.49	0.60	0.094	.925	ns
BAR	2.18	0.74	2.32	0.75	-1.624	.105	ns
EFF	4.46	0.59	4.17	0.63	4.129	.000	***
VUL	4.38	0.51	4.18	0.63	3.053	.002	**
CUE	3.53	0.91	3.77	0.75	-2.481	.014	*
EXP	1.99	0.86	2.12	0.79	-1.352	.177	ns
SEV	3.96	1.32	4.17	1.04	-1.517	.131	ns
BEH	4.69	0.41	4.58	0.46	2.100	.037	*

ns: non-significant; *p<.05, **p<.01, ***p<.001.

Table 4: Comparison of Means in the Employee Dataset

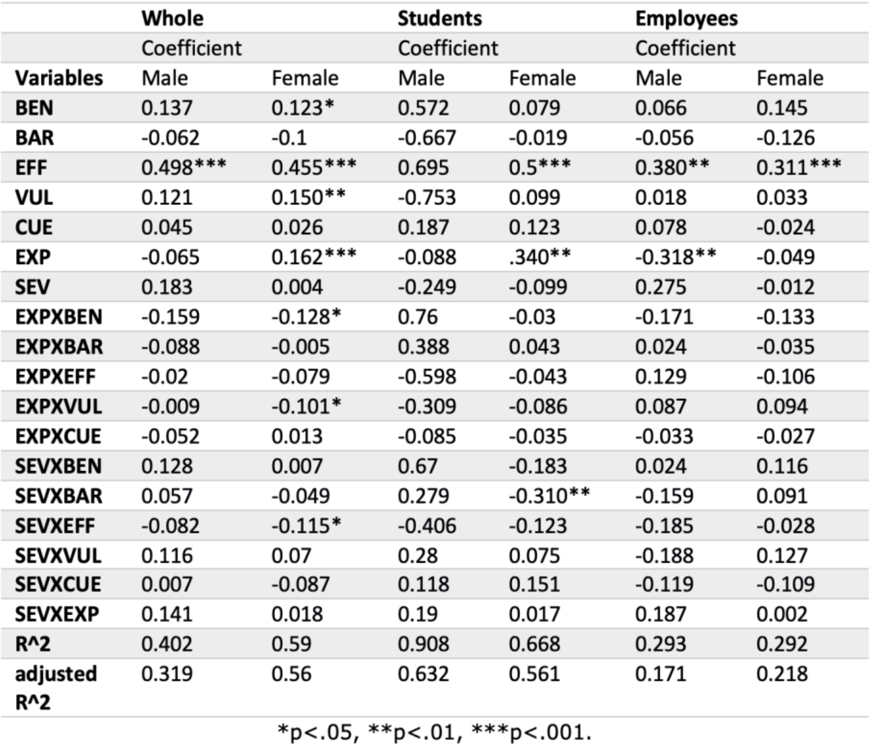
The results of the regression indicated that in the main effect model (see Table 5), EFF is the only determinant for the female employees' email behaviors while EFF and EXP are two significant determinants for the male employees' email behaviors.



	Whole		**Students**		**Employees**	
	Coefficient		Coefficient		Coefficient	
Variables	Male	Female	Male	Female	Male	Female
BEN	0.083	0.078	0.103	0.112	0.003	0.093
BAR	-0.065	-.108*	-0.458*	-0.044	-0.067	-0.095
EFF	0.483***	0.521***	0.778**	0.508***	0.401***	0.362***
VUL	0.126	.160**	-0.288	0.074	0.032	0.044
CUE	0.083	0.034	0.149	0.057	0.142	-0.021
EXP	-0.032	0.185***	-0.381	0.353***	-0.202*	-0.023
SEV	0.074	-0.001	-0.379	-0.163	0.134	-0.017
R^2	0.358	0.515	0.695	0.542	0.238	0.218
adjusted R^2	0.326	0.502	0.569	0.494	0.192	0.188

*p<.05, **p<.01, ***p<.001.

Table 5. Regression Results on Main Effects Model



	Whole		Students		Employees	
	Coefficient		Coefficient		Coefficient	
Variables	Male	Female	Male	Female	Male	Female
BEN	0.137	0.123*	0.572	0.079	0.066	0.145
BAR	-0.062	-0.1	-0.667	-0.019	-0.056	-0.126
EFF	0.498***	0.455***	0.695	0.5***	0.380**	0.311***
VUL	0.121	0.150**	-0.753	0.099	0.018	0.033
CUE	0.045	0.026	0.187	0.123	0.078	-0.024
EXP	-0.065	0.162***	-0.088	.340**	-0.318**	-0.049
SEV	0.183	0.004	-0.249	-0.099	0.275	-0.012
EXPXBEN	-0.159	-0.128*	0.76	-0.03	-0.171	-0.133
EXPXBAR	-0.088	-0.005	0.388	0.043	0.024	-0.035
EXPXEFF	-0.02	-0.079	-0.598	-0.043	0.129	-0.106
EXPXVUL	-0.009	-0.101*	-0.309	-0.086	0.087	0.094
EXPXCUE	-0.052	0.013	-0.085	-0.035	-0.033	-0.027
SEVXBEN	0.128	0.007	0.67	-0.183	0.024	0.116
SEVXBAR	0.057	-0.049	0.279	-0.310**	-0.159	0.091
SEVXEFF	-0.082	-0.115*	-0.406	-0.123	-0.185	-0.028
SEVXVUL	0.116	0.07	0.28	0.075	-0.188	0.127
SEVXCUE	0.007	-0.087	0.118	0.151	-0.119	-0.109
SEVXEXP	0.141	0.018	0.19	0.017	0.187	0.002
R^2	0.402	0.59	0.908	0.668	0.293	0.292
adjusted R^2	0.319	0.56	0.632	0.561	0.171	0.218

*p<.05, **p<.01, ***p<.001.

Table 6: Regression Results on Interaction Effects Model

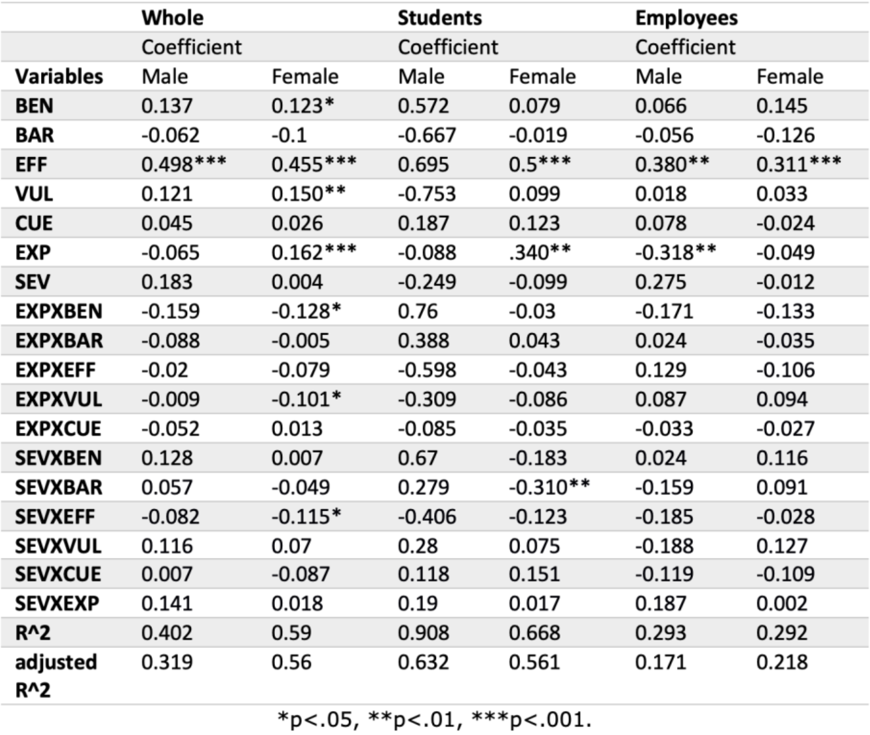
6. DISCUSSION

The results of the regression on the interaction effect model (see Table 6) are consistent with the findings of the main effect model: EFF is the only significant determinant on the female employees' email behavior while EFF and EXP are two significant determinants on the male employees' email behaviors. Therefore, H6 was supported. These results suggest that self-efficacy is a factor that impact both female and male employees' email behaviors. However, the male employees are also influenced by their experience of prior email security incidents even though they reported lower levels of prior experience than the female employees did.

Gender Differences on Security Perceptions and Behaviors

The results of this study show evidence of gender differences in people's security perceptions and behaviors. For the whole sample, there are statistically significant differences in terms of self-efficacy, vulnerability, barriers, cues to action, and self-reported email security behavior based on gender. Our findings of men having higher levels of self-efficacy and security behaviors are consistent with prior research (Anwar et al., 2017). Men are more confident of their capability to practice protective email behaviors and self-report higher levels of email security behaviors than women do. We also found that women perceive higher levels of barriers to practicing email security behaviors than men do. This might be related to women's lower levels of computer skills (Anwar et al., 2017) or less knowledge of computers (He & Freeman, 2009). It is interesting to find that our female participants reported a significantly lower likelihood of receiving unsafe email than the male participants did. The female participants did not feel more vulnerable to phishing email. Previous studies have found that women have a greater susceptibility to phishing email (Jagastic et al., 2007). Jagastic et al. (2007) utilized several roleplay tasks to measure people's susceptibility to phishing and they found that women are more likely than men to click on phishing links and giving information to phishing websites due to less technical training and less technical knowledge than men. The gap in women's perception of vulnerability and their actual security behaviors needs further exploration.

For the employee sample, the results are consistent with the findings in the whole sample except for perceived barriers. There is no significant difference in perceived barriers between our female and male employee participants. A possible explanation is that



	Whole		Students		Employees	
	Coefficient		Coefficient		Coefficient	
Variables	Male	Female	Male	Female	Male	Female
BEN	0.137	0.123*	0.572	0.079	0.066	0.145
BAR	-0.062	-0.1	-0.667	-0.019	-0.056	-0.126
EFF	0.498***	0.455***	0.695	0.5***	0.380**	0.311***
VUL	0.121	0.150**	-0.753	0.099	0.018	0.033
CUE	0.045	0.026	0.187	0.123	0.078	-0.024
EXP	-0.065	0.162***	-0.088	.340**	-0.318**	-0.049
SEV	0.183	0.004	-0.249	-0.099	0.275	-0.012
EXPXBEN	-0.159	-0.128*	0.76	-0.03	-0.171	-0.133
EXPXBAR	-0.088	-0.005	0.388	0.043	0.024	-0.035
EXPXEFF	-0.02	-0.079	-0.598	-0.043	0.129	-0.106
EXPXVUL	-0.009	-0.101*	-0.309	-0.086	0.087	0.094
EXPXCUE	-0.052	0.013	-0.085	-0.035	-0.033	-0.027
SEVXBEN	0.128	0.007	0.67	-0.183	0.024	0.116
SEVXBAR	0.057	-0.049	0.279	-0.310**	-0.159	0.091
SEVXEFF	-0.082	-0.115*	-0.406	-0.123	-0.185	-0.028
SEVXVUL	0.116	0.07	0.28	0.075	-0.188	0.127
SEVXCUE	0.007	-0.087	0.118	0.151	-0.119	-0.109
SEVXEXP	0.141	0.018	0.19	0.017	0.187	0.002
R^2	0.402	0.59	0.908	0.668	0.293	0.292
adjusted R^2	0.319	0.56	0.632	0.561	0.171	0.218

*p<.05, **p<.01, ***p<.001.

Table 6: Regression Results on Interaction Effects Model

perceived barriers might be moderated by prior experience with email security incidents. Our female employee participants reported higher levels of prior experience on email incidents than that of their male peers. The greater experience of email incidents might reduce our female employees' perceived barriers and possibly mediate the gender effect on it. It is also possible to argue that prior experience with email incidents is more likely to confound gender differences (Venkatesh et al., 2000).

For the student sample, the male students had higher self-efficacy while the female students had higher levels of perceived barriers when practicing email security behaviors. These findings are consistent with prior research (Anwar et al., 2017). It is interesting to note that several gender differences that existed in the whole dataset and the employee dataset were not present in our student dataset. Compared to the more diverse employee sample, our student sample is more homogeneous. It is possible that gender differences in perception could be potentially confounded by other demographic variables, such as education level and organization level (Venkatesh et al., 2000). This needs to be explored further.

Our findings indicate that women report higher levels of cues to action than men, which is inconsistent with prior research (Anwar et al., 2017). However, Anwar et al. (2017) used a form of cues to action question that asked only whether participants have received such queues. Using this type of CUE questions, they found that women are less sensitive to cues to action. We used a different form of cues to action in this study. The CUE questions used in our study focus on predicted responses to hypothetical situations (Claar et al., 2013), such as asking if the subject would be more careful about email security if his friend told him an email incident. The difference in the form of cues to action might explain the contradictory finding on cues to action. Our CUE questions lean more toward subjective norm, which refers to the perceived social pressure to perform and not to perform the behavior (Ajzen, 1991). Our findings that women more influenced by cues to action (e.g., weight the opinions of others' more highly than men) are supported in (Venkatesh et al., 2000; Venkatesh & Morris, 2000; McGill & Thompson, 2021).

Gender Differences in Determinants of Security Behaviors

The results of the regression in all 3 datasets indicate that the factors that impact men's email security behavior are different from the ones that impact women. The results in the whole dataset suggest that while men are more focused on their self-efficacy in their decision-making process regarding practicing protective email security behaviors, women are more balanced on their decision-making process, which is impacted by several factors, including perceived vulnerability, self-efficacy, prior experience, and perceived benefits. This is further supported by the similar variance in self-reported email security behaviors (W: 0.423, M: 0.498) explained by the significant determinants among women (VUL, EFF, EXP, BEN, EXPxBEN, EXPxVUL, and SEVxEFF) and men (EFF). Our finding is in line with the fact that women are more balanced in the adoption and usage decisions (Venkatesh et al., 2000).

When we examined the employee sample, self-efficacy was a significant factor that impacts both men's and women's email security behavior. Prior experience was a significant factor that impact men's security behavior but not women even though they reported higher levels of prior experience of email incidents. It is notable that gender differences in the employee dataset were somehow less compared to those in the whole dataset. Other important demographic variables, such as organization level and education could potentially confound gender differences (Venkatesh et al., 2000).

For the student sample, self-efficacy and prior experience significantly impact the female students' security behavior. A significant moderating effect of perceived severity on perceived barriers was also found in the female student group. It is interesting to note that we did not find any significant factors in the male student group by using the interaction effect model. When interaction effects were omitted, self-efficacy and perceived barriers are significant factors that impact our male students' security behavior.

As mentioned before, the focus of this paper is gender differences, and our results supported our hypotheses. It is notable that there are some unexpected findings in this study, such as the unexpected coefficient direction of prior experience in the whole dataset as well as the employee dataset. This needs further investigation.

Implications

Gender differences on security perceptions need to be considered when designing security training or awareness programs. The fact that women are more influenced by cues to action and have higher levels of perceived barriers of adopting security behaviors suggest that training differences should be targeted. For instance, incorporating interaction with close family members or friends in the training could help reduce perceived barriers in females (Dixon, 2014).

To maximize adoption of security behaviors, training might be tailored to emphasize factors that are salient to each gender group. For example, training needs to emphasize self-efficacy for men, while offering women a more balanced approach that includes self-efficacy, perceived benefits, perceived vulnerability, and prior experience, all of which are more important to women. Self-efficacy is a factor that impacts both men's and women's security behavior, while men have a higher reported self-efficacy than women do. This finding shed light on the importance of boosting women's self-efficacy via training programs to improve their security behaviors. The fact that women don't feel more vulnerable to security threats even though they have more prior experience of email incidents suggest a gap between their security perceptions and behaviors. Deploying phishing simulations and educating those who fail such simulations might help close this gap.

Substantial differences between students and faculty/staff were detected in our study. Self-efficacy was the only construct that shows gender-related differences in the student sample while multiple constructs (EFF, VUL, CUE, and BEH) show gender-related differences in the employee sample. Compared to our relatively young student sample, the employee sample has more diverse demographics such as age and education. Also, the employees in the university have gone through several security training sessions. These factors might contribute to the differences and warrant future investigation.

Limitations and Future Research Directions

Our research on gender differences of email security perceptions and behaviors focuses on the university setting in western culture. These issues should be addressed in other settings where email poses security threats. Another limitation of this study is the relatively small sample size for our male student group. While the sample size is acceptable (de Winter, 2013), a much larger sample size would give more reliable statistical results. Another limitation in the current work is the measurement of cues to action. The cues to action questions need to be refined in the future work to clearly measure subjects' responses to whether they have received such cues. Subjective norm, a factor that impact women more (Venkatesh et al., 2000; Venkatesh & Morris, 2000; McGill & Thompson, 2021) needs to be considered into the research model in the future.

Future research is necessary to fully understand gender differences by refining the current gender variable and adding more demographic variables. Future work should investigate gender as a psychological factor based on femininity and masculinity (Venkatesh et al., 2000; Venkatesh & Morris, 2000). Examining age, education level, and organization level in people's security perceptions and behaviors could be explored in the future work that might provide interesting insights (Fatokun et al., 2019).

7. CONCLUSION

This study examined gender differences in email security behaviors from two different measures. The findings reveal different perceptions on self-efficacy, vulnerability, barriers, cues to action, and self-reported security behaviors. The two genders appear to value each of the underlying factors differently. Several factors impact women's security behaviors, including self-efficacy, prior experience, perceived vulnerability, and perceived benefits while self-efficacy is the only factor that impacts men's security behaviors. The gender differences identified in this study provide evidence that gender plays a vital role in shaping people's security perceptions and thus impacting their behaviors. Security training and awareness programs can be designed and conducted more efficiently with these gender differences taken into consideration.

8. REFERENCES

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes*, 50(2), 179-211, doi: 10.1016/0749-5978(91)90020-T.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender Difference and Employees' Cybersecurity Behaviors. *Computers in Human Behavior*, 69, 437-443, doi: 10.1016/j.chb.2016.12.040.

atlasVPN. (2022). Over 80% of Malware Attacks Target Education Sector as Back-to-School Season Nears. Retrieved Feb. 27, 2023, from https://atlasvpn.com/blog/over-80-of-malware-attacks-target-education-sector-as-back-to-school-season-nears.

Benenson, Z., Gassmann, F., & Landwirth, R. (2017). Unpacking Spear Phishing Susceptibility. In *Proceedings of Financial Cryptography Workshops*, doi: 10.1007/978-3-319-70278-0_39.

Bischoff, P. (2022). Ransomware Attacks on Us Schools and Colleges Cost $3.56bn in 2021. Retrieved Feb. 27, 2023, from https://www.comparitech.com/blog/information-security/school-ransomware-attacks/.

Claar, C., Shields, R., Rawlinson, D., & Lupton, R. (2013). College Student Home Computer Security Adoption. *Issues in Information Systems*, 14(2), 139-148, doi: 10.48009/2_iis_2013_139-148.

de Winter, J. (2013). Using the Student' S T-Test with Extremely Small Sample Sizes. *Practical Assessment, Research, and Evaluation*, 18(1), 10, doi: 10.7275/e4r6-dj05.

Diaz, A., Sherman, A., & Joshi, A. (2020). Phishing in an Academic Community: A Study of User Susceptibility and Behavior. *Cryptologia*, 44, 53-67, doi: 10.1080/01611194.2019.1623343.

Dixon, L.J., Correa, T., Straubhaar, J., Covarrubias, L., Graber, D., Spence, J., & Rojas, V. (2014). Gendered Space: The Digital Divide between Male and Female Users in Internet Public Access Sites. *Journal of Computer-Mediated Communication*, 19(4), 991-1009, doi: 10.1111/jcc4.12088.

Dodel, M., & Mesch, G. (2017). Cyber-Victimization Preventive Behavior: A Health Belief Model Approach. *Computers in Human Behavior*, 68, 359–367, doi: 10.1016/j.chb.2016.11.044.

Du, J., & Schymik, G. (2018). Gender Differences on Students' Email Security Behaviors. In *Proceedings of the 24th Americas Conference on Information Systems,* 5, https://aisel.aisnet.org/amcis2018/SocialInclusion/Presentations/5.

Farooq, A., Isoaho, J., Virtanen, S., & Isoaho, J. (2015). Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors. In *Proceedings of IEEE Trustcom/BigDataSE/ISPA. Helsinki, Finland*, 352-359, doi: 10.1109/Trustcom.2015.394.

Fatokun, F., Hamid, S., Norman, A., & Fatokun, J. (2019). The Impact of Age, Gender, and Educational Level on the Cybersecurity Behaviors of Tertiary Institution Students: An Empirical Investigation on Malaysian Universities. *Journal of Physics: Conference Series,* 1339, doi: 10.1088/1742-6596/1339/1/012098.

Greitzer, F. L., Li, W., Laskey, K.B., Lee, J., & Purl, J. (2021). Experimental Investigation of Technical and Human Factors Related to Phishing Susceptibility. *ACM Transaction on*

Social Computing, 4(2), 1-48, doi: 10.1145/3461672.

Janz, N., & Becker, M. (1984). The Health Belief Model: A Decade Later. *Health Education Quarterly*, 11(1), 1-47, doi: 10.1177/109019818401100101.

Jagatic, T., Johnson, N., Jakobsson, M., & Menczer, F. (2007). Social Phishing. *Communications of the ACM*, 50(10), 94–100, doi: 10.1145/1290958.1290968.

Limbu, Y., Gautam, R., & Pham, L. (2022). The Health Belief Model Applied to Covid-19 Vaccine Hesitancy: A Systematic Review. *Vaccines*, 10(6), 973, doi: 10.3390/vaccines10060973.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual Differences and Information Security Awareness. *Computers in Human Behavior*, 69, 151-156, doi: 10.1016/j.chb.2016.11.065.

McGill, T., & Thompson, N. (2021). Exploring Potential Gender Differences in Information Security and Privacy. *Information & Computer Security,* 29(5), 850-865, doi: 10.1108/ICS-07-2020-0125.

Ng, B.-Y., Kankanhalli, A., & Xu, Y. (2009). Studying Users' Computer Security Behavior: A Health Belief Perspective. *Decision Support Systems*, 46, 815-825, doi: 10.1016/j.dss.2008.11.010.

Rosenstock, I. (1974). The Health Belief Model and Preventive Health Behavior. *Health Education Monographs*, 2(4), 354-386, doi:10.1177/109019817400200405.

Sari, P., Nurshabrina, N. & Candiwan (2016). Factor analysis on information security management in higher education institutions. In *Proceedings of the International conference on cyber and IT service management (2016)*, 1-5, doi: 10.1109/CITSM.2016.7577518.

Schymik, G. & Du, J. (2018). Student Intentions and Behaviors Related to Email Security: An Application of the Health Belief Model. *Journal of Information Systems Applied Research*, 11(3), 14-24, http://jisar.org/2018-11/ ISSN: 1946-1836.

Authors, 2023. Under review.

SecurityScorecard. (2018). 2018 Education Cybersecurity Report. Retrieved Feb. 27, 2023, from https://explore.securityscorecard.com/rs/797-BFK-857/images/SSC-EducationReport-2018.pdf.

Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L., & Downs, J. (2010). Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. Atlanta, Georgia, USA: Association for Computing Machinery*, 373–382, doi: 10.1145/1753326.1753383.

Venkatesh, V., & Morris, M.G. (2000). Why Don't Men Ever Stop to Ask for Directions? Gender, Social Influence, and Their Role in Technology Acceptance and Usage Behavior. *MIS Quarterly*, 24(1), 115-139, doi: 10.2307/3250981.

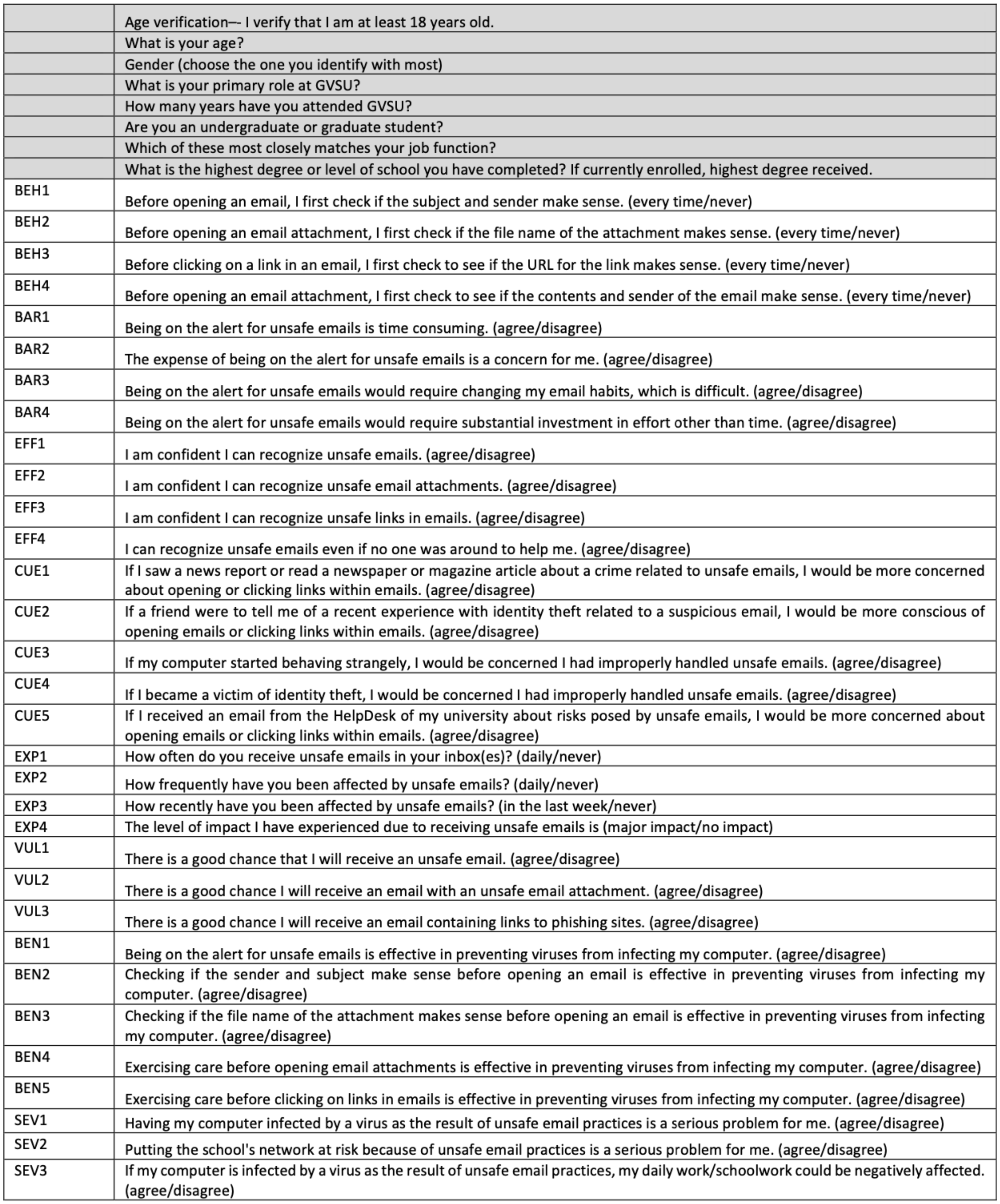
Venkatesh, V., Morris, M., & Ackerman, P. (2000). A Longitudinal Field Investigation of Gender Differences in Individual Technology Adoption Decision-Making Processes. *Organizational Behavior and Human Decision Processes*, 83(1), 33-60, doi: 10.1006/obhd.2000.2896.

Verkijika, S. (2019). If You Know What to Do, Will You Take Action to Avoid Mobile Phishing Attacks: Self-Efficacy, Anticipated Regret, and Gender. *Computers in Human Behavior*, 101, 286-296, doi: 10.1016/j.chb.2019.07.034.

Williams, C., Wynn, D., Madupalli, R., Karahanna, E., & K. Duncan, B. (2014). Explaining Users' Security Behaviors with the Security Belief Model. *Journal of Organizational and End User Computing*, 26(3), 23-46, doi: 10.4018/joeuc.2014070102.

Zetu, L., Zetu, I., Dogaru, C., Duţa, C., & Dumitrescu, A. (2014). Gender Variations in the Psychological Factors as Defined by the Extended Health Belief Model of Oral Hygiene Behaviors. *Procedia - Social and Behavioral Sciences,* 127, 358-362, doi: 10.1016/j.sbspro.2014.03.271.

APPENDIX A
Survey Questions



	Age verification–- I verify that I am at least 18 years old.
	What is your age?
	Gender (choose the one you identify with most)
	What is your primary role at GVSU?
	How many years have you attended GVSU?
	Are you an undergraduate or graduate student?
	Which of these most closely matches your job function?
	What is the highest degree or level of school you have completed? If currently enrolled, highest degree received.
BEH1	Before opening an email, I first check if the subject and sender make sense. (every time/never)
BEH2	Before opening an email attachment, I first check if the file name of the attachment makes sense. (every time/never)
BEH3	Before clicking on a link in an email, I first check to see if the URL for the link makes sense. (every time/never)
BEH4	Before opening an email attachment, I first check to see if the contents and sender of the email make sense. (every time/never)
BAR1	Being on the alert for unsafe emails is time consuming. (agree/disagree)
BAR2	The expense of being on the alert for unsafe emails is a concern for me. (agree/disagree)
BAR3	Being on the alert for unsafe emails would require changing my email habits, which is difficult. (agree/disagree)
BAR4	Being on the alert for unsafe emails would require substantial investment in effort other than time. (agree/disagree)
EFF1	I am confident I can recognize unsafe emails. (agree/disagree)
EFF2	I am confident I can recognize unsafe email attachments. (agree/disagree)
EFF3	I am confident I can recognize unsafe links in emails. (agree/disagree)
EFF4	I can recognize unsafe emails even if no one was around to help me. (agree/disagree)
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. (agree/disagree)
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. (agree/disagree)
CUE3	If my computer started behaving strangely, I would be concerned I had improperly handled unsafe emails. (agree/disagree)
CUE4	If I became a victim of identity theft, I would be concerned I had improperly handled unsafe emails. (agree/disagree)
CUE5	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. (agree/disagree)
EXP1	How often do you receive unsafe emails in your inbox(es)? (daily/never)
EXP2	How frequently have you been affected by unsafe emails? (daily/never)
EXP3	How recently have you been affected by unsafe emails? (in the last week/never)
EXP4	The level of impact I have experienced due to receiving unsafe emails is (major impact/no impact)
VUL1	There is a good chance that I will receive an unsafe email. (agree/disagree)
VUL2	There is a good chance I will receive an email with an unsafe email attachment. (agree/disagree)
VUL3	There is a good chance I will receive an email containing links to phishing sites. (agree/disagree)
BEN1	Being on the alert for unsafe emails is effective in preventing viruses from infecting my computer. (agree/disagree)
BEN2	Checking if the sender and subject make sense before opening an email is effective in preventing viruses from infecting my computer. (agree/disagree)
BEN3	Checking if the file name of the attachment makes sense before opening an email is effective in preventing viruses from infecting my computer. (agree/disagree)
BEN4	Exercising care before opening email attachments is effective in preventing viruses from infecting my computer. (agree/disagree)
BEN5	Exercising care before clicking on links in emails is effective in preventing viruses from infecting my computer. (agree/disagree)
SEV1	Having my computer infected by a virus as the result of unsafe email practices is a serious problem for me. (agree/disagree)
SEV2	Putting the school's network at risk because of unsafe email practices is a serious problem for me. (agree/disagree)
SEV3	If my computer is infected by a virus as the result of unsafe email practices, my daily work/schoolwork could be negatively affected. (agree/disagree)