International Journal of Information Science and Management
Vol. 21, No. 1, 2023, 243-260
DOI: 10.22034/ijism.2022.1977800.0 / https://dorl.net/dor/20.1001.1.20088302.2023.21.1.14.4

Original Research

Email and Website-Based Phishing Attack: Examining Online Users Security Behavior in Cyberspace Environment

Kibreab Adane
PhD. Student, Faculty of Computing & Software Engineering, Arba Minch University Institute of Technology, Arba Minch, Ethiopia.
Corresponding Author: kibreab.adane@amu.edu.et
ORCID iD: https://orcid.org/0000-0002-3021-5059

Berhanu Beyene
Associate Prof., Department of Computer Science, Ethiopian Civil Service University, Addis Ababa, Ethiopia.
berhanebeyene@gmail.com
ORCID iD: https://orcid.org/0000-0003-1398-0880

Received : 17 April 2022
Accepted: 16 May 2022

Abstract

Despite Emails and websites being widely used for communication, collaboration, and day-to-day activity, not all online users have the same knowledge and skills when determining the credibility of visited websites and email content. As a result, phishing, an identity theft cyber-attack that targets humans rather than computers, was born to harvest internet users' confidential information by taking advantage of human behavior and hurting an organization's continuity, reputation, and credibility. Because the success of phishing attacks depends on human behavior, using the Health-Belief Model, the study's objective is to examine significant factors that influence online users' security behavior in the context of Email and website-based phishing attacks. The model included eight predictor variables and was validated using quantitative data from 138 academic staff. The study findings exhibit that 4 out of 8 predictor variables, namely Perceived-Barriers, Perceived-Susceptibility, Self-efficacy, and Security-Awareness, are statistically significant in determining users' security behavior. The study's outcome is to assist in the appropriate design of both online and offline content for cyber security awareness programs, focusing on Email and website-based phishing attacks.

Keywords: Confidential Data, Health Belief Model, Online User, Phishing Attack, Security Behavior.

Introduction

The Internet has revolutionized individuals' and organizations' communication, collaboration, and day-to-day activity. Despite its multifaceted benefits, heavy reliance on the Internet has introduced various security challenges. Due to professional hackers are now aware that online users are becoming the weakest link in cyberspace, "Only amateurs attack machines; professionals target people" (Schneier, 2000). Phishing is a modern-day identity theft cyber-attack that targets humans rather than the computer system (Kathrine, Praise, Rose & Kalaivani 2019). Phishers leverage human behavior to capture personal information from online users via Email, websites, SMS, and social media. It deceives naive users and IT experts because attackers always follow novel strategies (PhishLabs, 2019; Kathrine et al., 2019).

Despite technology-based solutions such as phishing filters and popup blockers assisting online users in spotting fake websites and emails (Frauenstein, 2014), online users lack what security indicators signify; they ignore browser security warning alerts for monetary rewards (Kirlappos and Sasse, 2012), they do not want security warning alerts to disrupt their online activities, so they just focus on the areas of their interest that are most important to them (Krol, Moroz & Sasse 2012). The spelling errors in the URL structures, such as *"g00gle.com" and "google.com", "twitteer.com" and "twitter.com,*" may go unnoticed by online users. The cybercriminal uses this advantage to design and send the exact duplicates of legitimate websites. Afterward, fraudulent websites collect confidential information from unnoticed online users, potentially resulting in login credential compromise, data loss, and financial loss. The phishing attack lifecycle concepts presented in Figure 1 were taken from (Baadel & Lu, 2019; Patil & Dhage, 2019), with some modifications for our study. Anti-phishing interventions at any step in Figure 1 could avert Email and website-based phishing attacks.

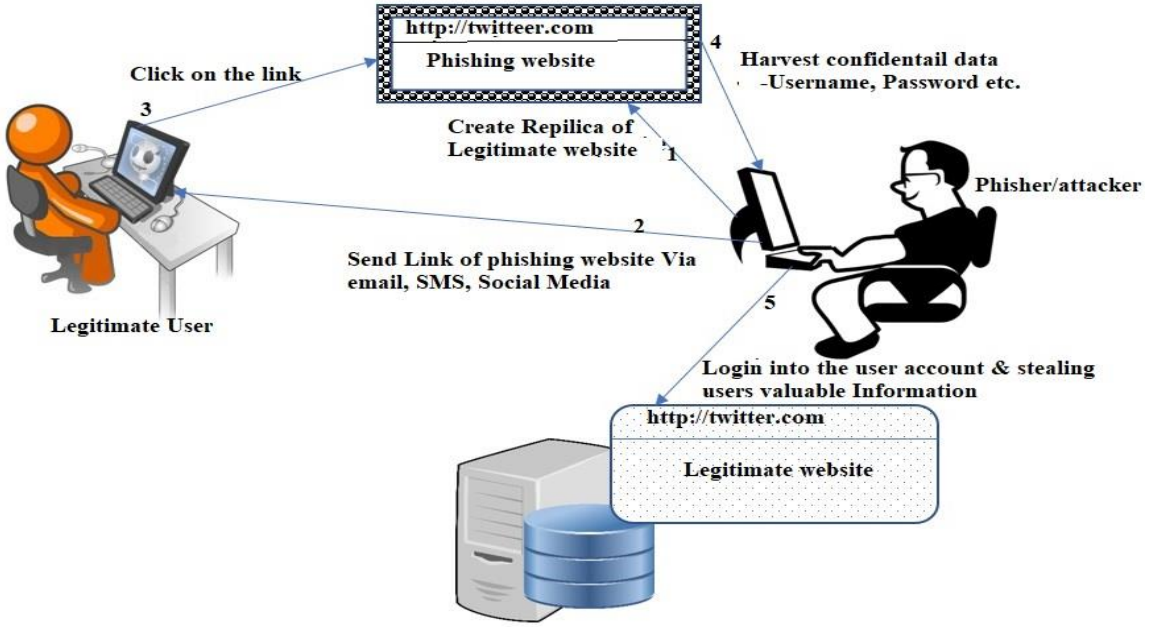

Figure 1: Example of Phishing Attack Life Cycles

Successful phishing attempts could result in catastrophic data loss, login credential compromise, ransomware infection, and financial loss (Proofpoint, 2020). Encryption ransomware was found in 93 % of all phishing emails (PhishMe, 2016). Unless a ransom is paid, internet users will be denied access to their data. Despite security awareness programs and phishing simulators, online users are still vulnerable to phishing emails (Williams, Hinds, & Joinson, 2018). Fake lottery or prize advertisements; impersonation or identity theft; computer or Internet faults; and promising big money in return) were among the main reasons for online users being exposed to phishing scams or fraud (EUC, 2020). Existing technological defenses will be ineffective against someone who does not follow acceptable Information security policies and procedures. Although training is beneficial, it will never be entirely successful (Pharris, 2019). Because the security of an organization's and online users' information cannot be ignored, technological protection alone has been proven to be insufficient to protect online users' sensitive information; this study is proposed to examine significant factors that influence

online users' security behavior in the context of Email and website-based phishing attacks using well known behavioral model i.e., Health Belief Model (HBM).

Health Belief Model, Research Gaps, Research Question, and Hypothesis

Health Belief Model (HBM)

In the 1950s, US public health centers adopted state-of-the-art preventive health care technology for screening health, vaccinating against flu, dental disease, and so on. However, this adoption was shown to be ineffective, as expected, due to individuals failing to follow disease prevention strategies for early detection. This led to the devising Health Belief Model (HBM) as one of the early attempts to fill the gaps in predicting patients' healthcare preventive behavior (Rosenstock, 1974; Williams, Madupalli, Karahanna & Duncan 2014). The core emphasis of the HBM was on analyzing the behavior of individuals to assess individuals compliance with medical treatments. According to (Chen, et al., 2011), individuals practicing disease prevention behaviors if they are: i) Perceived the seriousness of a given disease (i.e., Perceived Severity); ii) Perceived a greater chance of being suspect of disease (i.e., Perceived Susceptibility); iii) Perceived the positive outcome of following recommended action to their health (i.e., Perceived Benefits); iv) Perceived practicing the recommended action has less difficulty or obstacles to them (i.e., Perceived Barriers), and v) internal/external factors that stimulate or trigger them to carry out recommended health care behavior (i.e., Cues to Action).

The HBM model was widely used in various health studies to predict patients' healthcare behavior (Edwards, 2015). Due to conceptual similarities between preventive health care behavior and protective security behavior, it is now adapted to Information Security research (Claar, 2011; Williams et al., 2014). In the field of information system research, there are many theoretical models. The main focus of these models is on assessing technology adoption, techno-acceptance, user behavior intention, attitude, and beliefs (Claar, 2011; Williams et al., 2014). These models are more generic than the Health Belief Model (HBM) in examining significant factors influencing users' security behavior (Ng, Kankanhalli & Xu 2009). The HBM contained essential constructs such as perceived Severity, susceptibility, and Cues to Action, which are not found in popular Information System theoretical models (Claar, 2011; Williams et al., 2014). These are the core rationale for adapting the HBM in our study.

Research Gaps

In addition to predicting patients' compliance with acceptable healthcare behavior, HBM was used in determining: Email related users' security behavior (Ng et al., 2009), home computer users' security behavior (Claar, 2011; Edwards, 2015), employee's security behavior intentions at workplace (Williams et al., 2014), and in determining impacts of security awareness on employee's security behavior (Li. et al. 2016). Despite the relevance of the studies above' findings, examining significant factors that influence online users' security behavior in the context of both Email and website-based phishing attacks was not a significant focus of these studies. Since successful phishing attempts can result in catastrophic data loss, login credential compromise, ransomware infection, and financial loss (Proofpoint, 2020), addressing the gaps mentioned above in this study is a vital step.

Ng et al. (2009) used the HBM to investigate employees' email security behavior. They found that perceived susceptibility, perceived benefits, and self-efficacy are statistically significant in determining users' email security behavior. Claar (2011) used the HBM to

investigate home computer users' security behavior and found that perceived susceptibility, Severity, barriers, and self-efficacy are statistically significant in determining home computer users' security behavior. Perceived Susceptibility, Benefits, Severity, and Cues to Action were statistically significant in affecting users' security behavior intentions, according to Williams et al. (2014). Edwards (2015) used HBM to determine an association between security awareness and home computer users' security behavior and found that Perceived Susceptibility and privacy concerns are statistically significant in determining Home computer users' security behaviors. Li., et al. (2016) used HBM along with Protection Motivation Theory (PMT) to examine the impacts of security awareness on employees' security behavior and found that Perceived-susceptibility, Self-Efficacy, Perceived-severity, and response efficacy are statistically significant in determining employees' security behaviors.

However, the research findings demonstrated in the studies mentioned above are found to be inconsistent. Perceived Benefit is statistically significant in determining users' security behavior in the study (Ng, et al., 2009; Williams et al., 2014), while it is not statistically significant in the study (Claar, 2011; Edwards, 2015). In the study (Ng et al., 2009; Claar, 2011; Li. et al., 2016), Self-Efficacy is statistically significant in determining users' security behavior, while it is not statistically significant in the study (Williams et al., 2014; Edwards, 2015). In the study (Claar, 2011), Perceived barriers are statistically significant in determining users' security behavior, while it is not statistically significant in the study (Ng et al., 2009; Williams et al., 2014; Edwards, 2015, Li et al., 2016). Cues-To-Action is statistically significant in determining users' security behavior in the study (Williams et al., 2014), while it is not statistically significant in the study (Ng et al., 2009; Claar, 2011; Edwards, 2015; Li. et al., 2016). Edwards (2015) added two new constructs to HBM: security awareness and privacy concern, and found that security awareness is not statistically significant in determining users' security behavior, while privacy concern is. Therefore, this study balances the inconsistent research findings of previous studies by conducting both theoretical and empirical validation and filling research gaps in connection to Email and website-based security practices in the context of phishing attacks.

Research Objectives

The study is proposed to achieve the following key research objectives:

RO#1: To examine significant factors that influence online users' security behavior in the context of Email and website-based phishing attacks using Health Belief Model (HBM) Constructs.

RO#2: To identify the significant gaps in related studies to undertake theoretical and empirical validation so that it could assist in the appropriate design of online and offline content for cyber security awareness programs, with a focus on Email and website-based phishing attacks.

Research Questions

The study is proposed to answer the following key research questions:

RQ#1: Is the Perceived Severity of Email and website-based phishing attacks statistically significant

in determining users' security behavior?

RQ#2: Is the Perceived Susceptibility of Email and website-based phishing attacks

statistically
Significant in determining users' security behavior?

RQ#3: Is the Perceived Barriers of Email and website-based phishing attacks statistically significant
in determining users' security behavior?

RQ#4: Is the Perceived Benefits of Email and website-based phishing attacks statistically significant
in determining users' security behavior?

RQ#5: Is the Cues-To-Action of Email and website-based phishing attacks statistically significant in
determining users' security behavior?

RQ#6: Is the Self-Efficacy of Email and website-based phishing attacks statistically significant in
determining users' security behavior?

RQ#7: Is the Concern for the Privacy of Email and website-based phishing attacks statistically significant
in determining users' security behavior?

RQ#8: Is the Security Awareness of Email and website-based phishing attacks statistically significant
in determining users' security behavior?

Research Hypothesis

As shown in Table 1, the study contained eight predictor variables and their definitions in the study context to examine online users' security behavior in the setting of Email and website-based phishing attacks.

Table 1
HBM Constructs and Research Hypothesis

List of predictors	Definitions in the study context	Hypothesis
Perceived Severity	Perceived level of impact by online users as a result of not following the recommended cyber security policies and procedures in terms of (data loss, money loss, time loss, and system damage).	H1: the study assumes that the Perceived Severity is statistically significant in determining users Security Behavior in the context of Email & website-based phishing attack.
Perceived Susceptibility	The likelihood of online users becoming the suspect phishing attack.	H2: the study assumes that Perceived susceptibility is statistically significant in determining users Security Behavior in the context of Email & website-based phishing attack.
Perceived Barriers	Obstacles or inconvenience which can deter online users from practicing acceptable security behavior	H3: the study assumes that Perceived barriers are statistically significant in determining users Security Behavior in the context of Email & website-based

List of predictors	Definitions in the study context	Hypothesis
		phishing attack.
Perceived Benefits	Online users' perception about the positive outcome of following acceptable information security policies and procedures.	H4: the study assumes that Perceived benefits are statistically significant in determining users Security Behavior in the context of Email & website-based phishing attack.
Cues to Action	External factors that motivate or trigger online users to take the recommended security action or behavior.	H5: the study assumes that Cues to Action is statistically significant in determining users Security Behavior in determining users Security Behavior in the context of Email & website-based phishing attack.
Self-Efficacy	Online users' confidence in their ability to carry out protective security behavior on their own.	H6: the study assumes that Self-efficacy is statistically significant in determining users Security Behavior in the context of Email & website-based phishing attack.
Concern for Privacy	If online users perceive that their Privacy is can threatened or mishandled, sold to a third party by an online company, they may refuse to provide personal details online, they may remove their private information from online databases (Smith, Milberg & Burke,1996 ; Son & Kim, 2008)	H7: The study assumes that Concern For Privacy is statistically significant in determining users Security Behavior in the context of Email & website-based phishing attack.
Security Awareness	If online users are aware of cyber security including phishing, ransomware, safe and unsafe websites/emails, and password policies, they will exhibit acceptable security behavior against phishing attacks.	H8: the study assumes that Security awareness is statistically in determining users Security Behavior in the context of Email & website-based phishing attack.

Materials and Methods

Study Participants Background

The HBM model was validated using quantitative data gathered from 138 academic staff members from four Ethiopian public higher education institutions. The study participants were purposely chosen because they were expected to be active internet users due to the nature of their professions, such as online teaching, learning, and research. However, as far as relying on the Internet is concerned; the results of this study can have indirect applicability to other online users. The majority, 131(95%) of the study participants were males, while the remaining 7(5%) were females. 86(62 %) of study participants had masters' degrees, 23(17%) Ph.D. Students, 22(16%) had a Ph.D. degree and above, 5(4%) had First Degree, and 2(1%) were Master's degree students. The majority, 108(78%) of the study participants, did not receive the Information security training, 28 (20%) received the Information security training, and 2% of them indicated neutral/maybe. 98.6% of the study participants have used the Internet for sending &receiving emails, 94.2 % for searching/sharing teaching, learning, and research

materials, 90.6% view/posting to social media, 89.9% for downloading/uploading different files, 74.6% for reading News stories, 23.9% for online shopping and 21% for other online activities.

Survey Items Construction and Survey Administration Procedures

The survey items were produced by the researchers and modified from previous studies (Claar, 2011; Edwards, 2015; Ng et al., 2009; Williams et al., 2014). 35 survey items were evaluated using the Likert scale. Before creating the questionnaire, the researcher first clarified the operational definitions of HBM constructs; then, survey items were adapted from prior studies and self-developed within the context of each HBM construct, then each question was carefully crafted to ensure that it was professional looking and easy to understand for study participants, after that, each question is divided into sections with its own set of instructions. Google Cloud Form was used to prepare an online survey questionnaire. The institutional Email was used to send an online survey link to each study participant. This is because using an online survey has its own benefits, such as saving time, being easy to reach respondents from anywhere, eliminating missing values by enabling mandatory settings, and saving paper waste and travel costs. The respondents gave their consent to take part in the study. According to (Rea & Parker, 2005; Edwards, 2015), study participants will not respond to web-based/online surveys unless they have access to Email, a computer, and basic computer skills. This can be viewed as a disadvantage of conducting an online survey.

Before data collection began, the University Post Graduate Coordination office issued an approved permission letter for data collection, which was distributed to the study participants along with a detailed explanation of the study's objective. There is no personally identifying information collected in the contents of the online survey questionnaire. Each study participant was informed to complete each questionnaire within 15 minutes. An online survey yielded a 38.4% useable response rate (138 out of 359) throughout the data collection period, from October 26, 2021, to January 15, 2022. The online survey questionnaires used in our study can be found in Appendix I.

Data Analysis Tool

IBM SPSS version 28 was used to analyze the data, test the reliability and validity of items included in the survey, and test the hypothesis using multiple regression analysis.

Reliability and Construct Validity Analysis

Cronbach Alpha and the Composite Reliability (CR.) test were used to assess the internal consistency of all items in this study. The Cronbach alpha reliability scale value requires each item to score at least 0.7, and except at least 0.6 reliability scale value may be allowable for exploratory study (Ng et al., 2009). Due to the sensitivity of Cronbach's alpha to the number of items on the scale (Hair, Hult, Ringle & Sarstedt, 2017), the internal consistency reliability tends to be underestimated unless the Composite Reliability (CR) is used. CR value ranges between 0 and 1. At least a 0.6 CR value is allowable for exploratory study and a CR value less than 0.6 indicates the non-existence of internal consistency (Hair et al., 2017; Triwidyati & Tentama, 2020). Problems with the Perceived Barrier construct were identified while analyzing the internal consistency of items. The Perceived Barrier construct's reliability scale value is 0.538, which is unacceptable as per the Cronbach alpha rule of thumb. However, it was found

to be acceptable per the Composite Reliability (CR) rule of thumb (Hair et al., 2017). The overall Cronbach alpha reliability scale value is 0.833, which is within a good range.

Construct validity is a method of determining whether survey items measure what they are intended to measure, and convergent validity measures the degree to which items correlate positively with other items of the same construct (Hair et al., 2017; Triwidyati & Tentama, 2020). Principal Component Analyses (PCA) and the Varimax rotation method were used to conduct factor analysis. Nine components have at least one eigenvalue, accounting for 68.197 percent of the variance explained. The Kaiser–Meyer–Olkin (KMO) value is a statistical measure used to evaluate sample adequacy, and a KMO value of at least 0.6 indicates appropriate factor analyses (Cronbach & Meehl, 1955; Asanka, Arachchilage & Love, 2014). Our study sample's KMO value is =0.744, with a significance level of P<0.05 (approximate Chi-Squire= 2409.647 and df 595), indicating that it is suitable for Principal Component Analysis. The extracted communality values for each measurement item should be greater than 0.3. The commonality values of each measurement item in this study are all greater than 0.5, except for SB1 score=0.412. This is also a good signal for Principal Component Analysis. Convergent validity necessitates that all similar items be loaded under their respective construct, that the loading factor values of each item be >0.5, and that the Average Variance Extracted (AVE) be >0.5. Each of the 35 survey items was kept in the model because removing any of them would diminish the reliability scale value.

Table 2
Construct Reliability and Validity Analysis

Constructs	Item Loading	Cronbach α	CR	AVE
PSev1	0 .889			
PSev2	0.886			
PSev3	0.878	0.883	0.915	0.782
PSus1	0.696			
PSus2	0.804			
PSus3	0.719			
PSus4	0.640	0.766	0.808	0.514
PBen1	0.751			
PBen2	0.817			
PBen3	0.591	0.735	0.787	0.527
PBar1	0.582			
PBa2r	0.764			
PBar3	0.630	0.538	0.699	0.44
SE1	0.796			
SE2	0.830			
SE3	0.686			
SE4	0.749	0.888	0 .851	0.588
CTA1	0.731			
CTA2	0.750			
CTA3	0.730	0.736	0.781	0.543
CFP1	0.798			
CFP2	0.716			
CFP3	0.743			
CFP4	0.738	0.784	0.837	0.561

SA1	0.783			
SA2	0.762			
SA3	0.726			
SA4	0.771			
SA5	0.749	0.882	0.871	0.575
SB1	0.540			
SB2	0.648			
SB3	0.588			
SB4	0.755			
SB5	0.618			
SB6	0.578	0.766	0.792	0.39
Key for Abbreviations	PSev=Perceived-Severity;PSus=Perceived-Susceptibility;PBen=Perceived-Benefits;PBar=Perceived-Barriers; SE=Self-Efficacy; CTA=Cues-To-Action; CFA=Concern-For-Privacy; SA=Security-Awareness; SB=Security-Behavior; AVE=Average Variance Extracted; CR= Composite Reliability			

Hypothesis Test Results

According to the results of the multiple regression analysis, Perceived-Barriers (PBAR), Perceived-Susceptibility (PSUS), Self-efficacy (SE), and Security-Awareness (SA) were statistically significant predictors variables. In this study, 0.05 was used to test the significance level of the proposed hypothesis, as shown in Table 4. The model fit information shows a statistically significant value ($P<0.05$), with a Chi-square value =63.455 and df=8. This implies that the model fits the data well. According to Fagerland & Hosmer (2017), the null hypothesis for model goodness-of-fit tests is that the model fits the data well, while the alternative hypothesis is that the model does not fit the data well. A low p-value implies that something is wrong with the model in this circumstance. The deviation statistic has an advantage over the Pearson statistic in that it can compare many hierarchical models, while the Pearson statistic cannot (Collet, 1991; (Fagerland & Hosmer 2017). The model's Goodness Fit, as measured by the Deviance statistical measure, is equivalent to 1 in our study. This means that the model fits the data well or that the observed data matches the expected data exactly. Pseudo R-Square (R2) value based on the Nagelkerke statistical measure is=0.37, indicating a 37% change in the dependent variable (users' security behavior) as a result of the independent variables used in our study.

Table 4
Hypothesis Test Results (Multiple Regression Table)

Hypothesis	Standardized Estimates (β)	Std. Error	Wald	Df	Sig. level ($p<0.05$)	95% Confidence Interval	
						Lower bound	Upper Bound
H1: Perceived Severity determines users Security Behavior in the context of Email & website-based phishing attack.	0.238	0.129	3.390	1	0.066 Not Supported	-0.015	0.491
H2: Perceived	-0.402	0.194	4.293	1	0.038	-0.783	-0.022

Hypothesis	Standardized Estimates (β)	Std. Error	Wald	Df	Sig. level (p<0.05)	95% Confidence Interval	
						Lower bound	Upper Bound
Susceptibility determines users Security Behavior in the context of Email & website-based phishing attack.					Supported		
H3: Perceived Barrier determines users Security Behavior in the context of Email & website-based phishing attack.	-0.561	0.217	6.683	1	0.010 Supported	0.136	0.986
H4: Perceived Benefits determines users Security Behavior on relation to Email & website-based phishing attack.	0.347	0.220	2.496	1	0.114 Not supported	-0.083	0.777
H5: Cues to Action determines users Security Behavior in relation to Email & website-based phishing attack.	0.212	0.243	0.760	1	0.383 Not supported	-0.265	0.689
H6: Self- efficacy determines users Security Behavior in relation to Email & website-based phishing attack.	0.574	0.204	7.930	1	0.005 Supported	0.175	0.974
H7: Concern for Privacy determines users Security Behavior in relation to Email & website-based phishing attack.	0.161	0.211	0.582	1	0.445 Not supported	-0.253	0.575
H8: Security Awareness determines users Security Behavior in relation to Email & website-based phishing attack.	0.675	0.246	7.526	1	0.006 Supported	0.193	1.157

Discussion on the Key Research Findings

Figure 2 shows the empirical findings of the hypothesis test. The study findings are organized into eight research questions to make discussion easier.

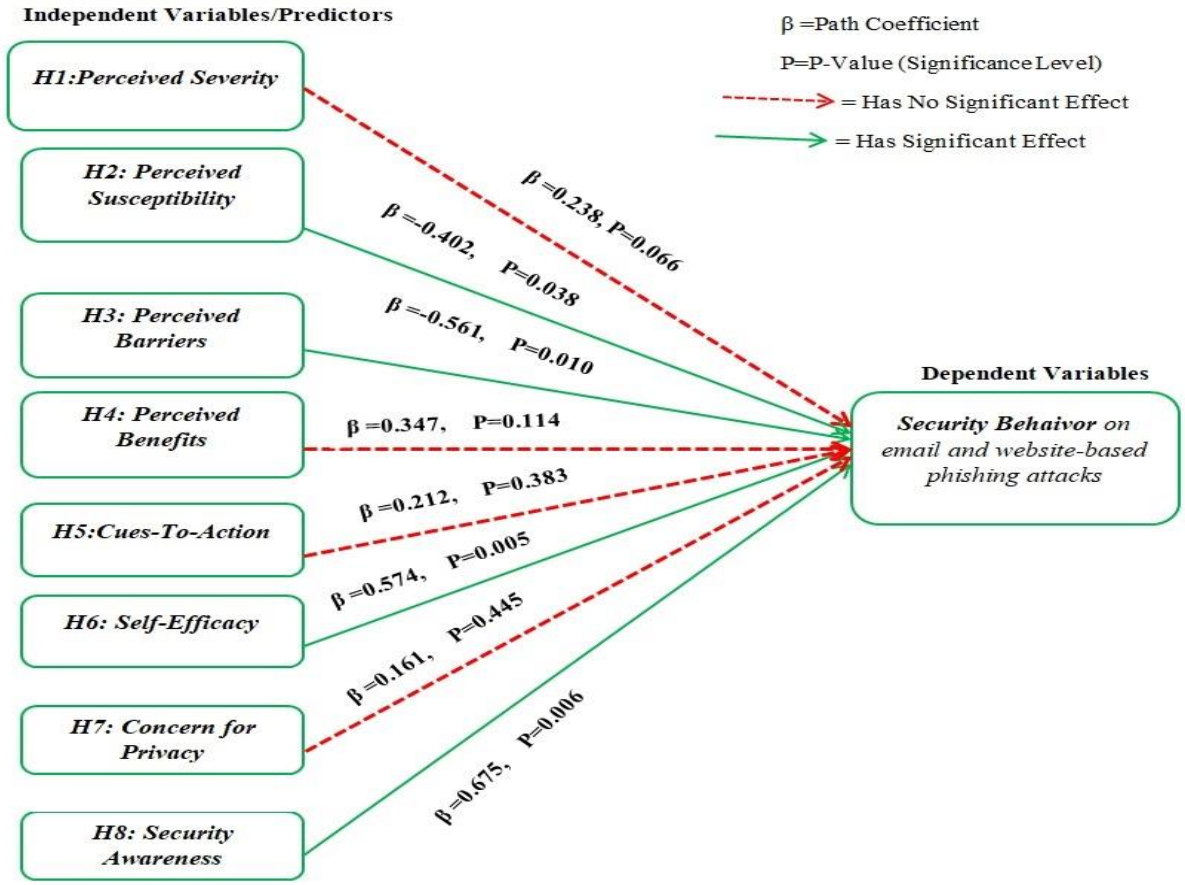

Figure 2: Empirical Findings of Hypothesis Test

RQ#1: Is the Perceived Severity of Email and website-based phishing attacks statistically significant in determining users' security behavior?

Perceived Severity was found to be statistically significant in determining home computer users' security behavior (Claar, 2011), employee's security behavior intentions at the workplace (Williams et al., 2014), and employee's security behavior (Li, Xu, He, Chen & Chen 2016). On the other hand, the findings of our study support the rejection of Hypothesis (H1) that states Perceived Severity is statistically significant in determining users' Security Behavior in the context of Email and website-based phishing attacks (β=0.238, P-Value=0.066). This is not a surprising research finding because some previous studies found Perceived Severity as a weak predictor in relation to Email related security behavior (Ng et al., 2009), and home computer users' security Behavior (Edwards, 2015). The findings of our study indicate that the perceived level of impact in terms of (data loss, money loss, time loss, and system damage) does not affect online users' willingness to exercise acceptable security behavior about Email and website-based phishing attacks.

RQ#2: Is the Perceived Susceptibility of Email and website-based phishing attacks statistically significant in determining users' security behavior?

According to (Claar, 2011; Edwards, 2015; Li et al., 2016; Ng et al., 2009; Williams et al., 2014), a positive and significant relationship exists between perceived vulnerability and user security behavior. Surprising findings in our study show an indirect (negative) significant

relationship between perceived vulnerability and users' security behavior regarding Email and website-based phishing attacks (β=-0.402, P-Value=0.038) and partially support the acceptance of Hypothesis (H2). The findings of our study indicate that if online users believe they are at high risk of being a phishing victim, they are less likely to engage in acceptable security behavior against Email and website-based phishing attacks.

RQ#3: Is the Perceived Barriers of Email and website-based phishing attacks statistically significant in determining users' security behavior?

Our study findings reveal that the Perceived barrier is statistically significant in determining users' security behavior about Email and website-based phishing attacks (β=-0.561, P-Value=0.010) and supports the acceptance of Hypothesis (H3). The findings of our study concur with the research findings that focused on examining home computer users' security behavior (Claar, 2011). The findings of our study indicate that if online users believe that exercising the recommended security measures is difficult or time-consuming, they are more likely to disregard them. Hence, minimizing barriers to Internet access is important for successfully combating Email and website-based phishing attacks.

RQ#4: Is the Perceived Benefits of an email and website-based phishing attacks statistically significant in determining users' security behavior?

Perceived Benefit was statistically significant in predicting employees' Email-related security behavior (Ng et al., 2009) and in predicting employees' security behavior intentions at work (Williams et al., 2014). On the other hand, our study's findings support the rejection of Hypothesis (H4) that states Perceived Benefit is statistically significant in determining users' Security Behavior in relation to Email and website-based phishing attacks (β=0.347, P-Value=0.114). This is not a surprising research finding because some previous studies found Perceived Benefit as a weak predictor in determining home computer users' security behavior (Claar, 2011; Edwards, 2015), and determining employee's security behavior (Li et al., 2016). The findings of our study indicate that if online users' perceived the positive outcome of exercising acceptable information security policies and procedures, they are less likely to exercise acceptable security behavior concerning Email and website-based phishing attacks.

RQ#5: Is the Cues-To-Action of an email and website-based phishing attacks statistically significant in determining users' security behavior?

In the study by Williams et al. (2014), Cues to Action are statistically significant in determining employees' security behavior intentions at the workplace. On the other hand, our study's findings support the rejection of Hypothesis (H5) that states Cues to Action are statistically significant in determining users' Security Behavior in relation to Email and website-based phishing attacks with (β=0.212, P-Value=0.383). This is not surprising research finding due to some previous studies found Cues to Action as a weak predictor in determining Email related security behavior (Ng et al., 2009), Home computer users' security Behavior (Claar, 2011; Edwards, 2015), and employees' security behaviors (Li. et al., 2016). The findings of our study indicate that if online users have exposure to security experience sharing by organizations, by communication media, and recommendations from security experts or peers are less likely to be triggered or motivated to exercise acceptable security behavior about Email and website-based phishing attacks.

RQ#6: Is the Self-Efficacy of Email and website-based phishing attacks statistically significant in determining users' security behavior?

Our findings reveal that Self-efficacy is statistically significant in determining users' security behavior about Email and website-based phishing attacks (β=-0.574, P-Value=0.005) and supports the acceptance of Hypothesis (H6). Our study findings concur with the findings of (Claar, 2011; Li et al., 2016; Ng et al., 2009). Our findings indicate that if the users are confident in their ability, he/she able to exercise the recommended security behavior in Email and website-based phishing attacks on their own. Therefore, increasing user confidence through regular cyber security training/capacity building is important to encourage the users to take the recommended actions.

RQ#7: Is the Concern for the Privacy of Email and website-based phishing attacks statistically significant in determining users' security behavior?

Edwards (2015) added a new construct, Concern for Privacy, to the Health Belief Model and found that Concern for Privacy is statistically significant in predicting Home computer users' security behavior, (Edwards, 2015). However, the findings of our study refuted the claim made by Edwards (2015). They supported the rejection of Hypothesis (H7) that states concern for Privacy is statistically significant in predicting online users' security behavior in response to Email and website-based phishing attacks (β=0.161, P-Value=0.445). The findings of our study indicate that if online users perceive that their Privacy can be threatened, mishandled, or sold to a third party by an online company, they may not refuse to provide personal details online. They may not remove their private information from online databases.

RQ#8: Is the Security Awareness of Email and website-based phishing attacks statistically significant in determining users' security behavior?

As the Concern for Privacy Construct, Security Awareness was a new construct added to Health Belief Model by Edwards (2015) who found that security awareness is not statistically significant in determining Home computer users' security behavior. However, the findings of our study refuted this claim. They supported the acceptance of Hypothesis (H8) that states Security Awareness is statistically significant in determining online users' Security Behavior in the context of Email and website-based phishing attacks with (β=0.675, P-Value=0.006). The findings of our study indicate that if online users are aware of human-centric cybersecurity threats such as phishing, ransomware, proper password handling, and how to discriminate between safe and risky websites, they will act securely.

Theoretical and Practical Implications

Previous studies used the Health Belief Model (HBM) to assess significant factors influencing users' security behavior when using a computer or the Internet. Despite the importance of the previous study, there is some inconsistency in these findings. The contents related to Email and website-based phishing attacks were not past studies' primary focus. This study fills these gaps by undertaking theoretical and empirical validation. Our study refuted the claim that stating security awareness is not statistically significant in predicting user security behavior (Edwards, 2015); the claim that stating perceived vulnerability has a significant positive relationship with users' security behavior (Claar, 2011; Edwards, 2015; Li et al., 2016; Ng et al., 2009; Williams et al., 2014), and the claim that stating Concern For Privacy is statistically significant in predicting users' security behavior (Edwards, 2015). The findings of our study would suggest that cyber-security practitioners and other concerned bodies consider

Perceived Susceptibility, Perceived Barriers, Self-Efficacy, and Security Awareness when designing both online and offline content concerning Email and website-based phishing attacks.

Conclusions and Future Research Work

To compete with the rest of the world, every individual and organization' is now relying on the Internet. However, email and website-based phishing attacks, on the other hand, are obstacles to this progress. Net-zens are now starting to question the trustworthiness of the Internet. Humans design, develop, adopt, and deploy the technology. Humans make extensive use of and misuse technology, either intentionally or unintentionally. Investing large sums of money in cutting-edge technology to secure the information of individuals and organizations has proven to be ineffective unless significant factors influencing online users' security behavior in cyberspace environment(s) are well understood. Because the success of Email and website-based phishing attacks primarily depends on human inadequacy or behavior, the study investigated significant factors that influence online users' security behavior using Health Belief Model, adapted from Health care literature. The study has made a great deal of effort to identify the significant gaps in previous studies and to undertake both theoretical and empirical validation to assist in the appropriate design of online and offline content for cyber security awareness programs, with a focus on Email and website-based phishing attacks. Before conducting the hypothesis test, the reliability and validity of each of the 35 online survey items were investigated. The study used a total of 8 predictor variables: Perceived (Severity, Barriers, Susceptibility, and Benefits), Cues-To-Action, Concern-For-Privacy, and Security Awareness. The findings exhibit that 4 out of 8 predictor variables, such as Perceived Barriers, Perceived Susceptibility, Self-efficacy, and Security-Awareness, were statistically significant in determining users' security behavior in the context of Email and website-based phishing attacks.

This study focused on assessing online users' security behavior in general and the security behavior of Ethiopian Higher Education Institutions' academic staffs in particular. Using the study's findings as a baseline, future researchers could include online users from various institutions for comparative result analysis and to generalize the study's findings at the national or international level. Although successfully combating Email and website-based phishing attacks requires a significant amount of effort focused on developing novel socio-technical anti-phishing solutions, the study focused on social-dimension anti-phishing solutions because humans use and misuse technology daily intentionally or unintentionally.

Acknowledgments

The authors thank all study participants, participating editors, and anonymous reviewers for their valuable suggestions and comments .They would like to thank Arba Minch University for providing the funding necessary for our study, which has the project code GOV/AMU/PHD/TH02/AMiT/FCSE/02/15, to be completed successfully.

References

Arachchilage, N. A. G. & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behavior*, 38, 304-312. https://doi.org/10.1016/j.chb.2014.05.046

Baadel, S. & Lu, J. (2019). Data Analytics: Intelligent Anti-Phishing Techniques Based on Machine Learning. *Journal of Information and Knowledge Management*, 18(1),1-20. https://doi.org/10.1142/S0219649219500059

Chen, M., Wang, R., Schneider, J. K., Tsai, C., Jiang, D. D., Hung, M. & Lin, L. (2011). Using the health belief model to understand caregiver factors influencing childhood influenza vaccinations. *Journal of Community Health Nursing*, 28(1), 29–40. https://doi.org/10.1080/07370016.2011.539087

Claar, C. L. (2011). *The adoption of computer security: An analysis of home personal computer user behavior using the health belief model*. Utah State University. Retrieved from http://digitalcommons.usu.edu/etd/878/

Collett, D. (1991) *Modelling Binary Data. Texts in Statistical Science Series*, Chapman and Hall, London

Cronbach, L. J. & Meehl, P. E. (1955). Construct validity in psychological test. *Psychological Bulletin*, 52, 281–302.

Edwards, K. (2015). *Examining the security awareness, information privacy, and the security behaviors of home computer users*. Doctoral dissertation, Nova Southeastern University. Retrieved from https://nsuworks.nova.edu/gscis_etd/947.

EUC (2020). Survey on scams and fraud experienced by consumers. *European Union Commission Fact Sheet*, 1-47.

Fagerland, M. W. & Hosmer, D. W. (2017). How to test for goodness of fit in ordinal logistic regression models. *Stata Journal*, 17(3), 668–686. https://doi.org/10.1177/1536867x1701700308

Frauenstein, E. D. (2014). *A framework to mitigate phishing threats*. Doctoral Dissertation, Nelson Mandela Metropolitan University, 1- 262. Retrieved from https://www.researchgate.net/publication/267512601

Hair, J. F., Hult, G. T. M., Ringle, C. M. & Sarstedt, M. (2017). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. New York: Sage Publications, 1-390.

Kathrine, G. J. W., Praise, P. M., Rose, A. A. & Kalaivani, E. C. (2019). Variants of phishing attacks and their detection techniques. In *Proceedings of the International Conference on Trends in Electronics and Informatics, ICOEI 2019*, 255–259. https://doi.org/10.1109/ICOEI.2019.8862697

Kirlappos, I. & Sasse, M. A. (2012). Security Education against Phishing: A Modest Proposal for a Major Rethink. *IEEE Security & Privacy Magazine*, 10(2), 24–32. https://doi.org/10.1109/msp.2011.179

Krol, K., Moroz, M. & Sasse, M. A. (2012). Don't work. Can't work? Why it's time to rethink security warnings. In *Seventh International Conference on Risks and Security of Internet and Systems (CRiSIS)*. https://doi.org/10.1109/crisis.2012.6378951

Li, L., Xu, L., He, W., Chen, Y. & Chen, H. (2016). Cyber Security Awareness and Its Impact on Employee's Behavior. In *10th International Conference on Research and Practical Issues of Enterprise Information Systems (CONFENIS)*, Vienna, Austria, 103-111. Retrieved from https://hal.inria.fr/hal-01630550

Ng, B., Kankanhalli, A. & Xu, Y. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, 46, 815-825. https://doi.org/10.1016/j.dss.2008.11.010

Patil, S. & Dhage, S. (2019). A methodical overview on phishing detection along with an organized way to construct an anti-phishing framework. In *Fifth International Conference on Advanced Computing & Communication Systems (ICACCS)* (pp. 588-593). IEEE.

Pharris, L. J. (2019). *Social engineering: How US businesses strengthen the weakest link*

against cybersecurity threats. Liberty University, 1-216. Retrieved from https://digitalcommons.liberty.edu/doctoral/2159

PhishLabs. (2019). 2019 Phishing Trends and Intelligence Report: The Growing Social Engineering Threat. PhishLabs, *Annual Report*, 1-30. Retrieved from https://info.phishlabs.com/hubfs/2019%20PTI%20Report/2019%20Phishing%20Trends%20and%20Intelligence%20Report.pdf

PhishMe. (2016). Q1 2016 Malware Review. PhishMe Intelligence, 2016 1st Quarter Active Threat Reports, 1–15. Retrieved from https://cofense.com/wpcontent/uploads/2017/10/Q1_2016_Malware_Review_PhishMe.pdf

Proofpoint (2020). State of the Phish: An in-depth look at user awareness, vulnerability and resilience, *Annual Report*, 1-48.

Rea, L. M. & Parker, R. A. (2005). *Designing & Conducting Survey Research: A Comprehensive Guide* (3rd ed.). Hoboken, NJ: John Wiley & Sons, Inc.

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

Schneier. B. (2000). Semantic Attacks: The Third Wave of Network Attacks. *Crypto-Gram Newsletter*. Retrieved from http://www.schneier.com/crypto-gram-0010.html

Smith, H. J., Milberg, S. J. & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*: *Management Information Systems*, 20(2), 167–195. https://doi.org/10.2307/249477

Son, J. Y. & Kim, S. S. (2008). Internet users' information privacy-protective responses: A Taxonomy and a nomological model. *MIS Quarterly: Management Information Systems*, 32(3), 503–529. https://doi.org/10.2307/25148854

Triwidyati, H. & Tentama, F. (2020). Validity and Reliability Construct of Subjective Well-being Scale. *International Journal of Sciences: Basic and Applied Research*, 51(2), 191–200. Retrieved from http://eprints.uad.ac.id/id/eprint/20150

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

Williams, E. J., Hinds, J. & Joinson, A. N. (2018). Exploring susceptibility to phishing in the workplace. *International Journal of Human Computer Studies*, 120, 1–13. https://doi.org/10.1016/j.ijhcs.2018.06.004

Appendix I

Table 3
List of Survey Items

Constructs	Items Description	Source
Perceived Severity (PSev.)	**PSev1:** Level of Impact on you, if your personal details are being stolen (password, credit card, SSN, Bank account details, etc.) as a result of visiting and sharing on fake websites. [No/Very Low Impact=1] to [Very High Impact =5]	Claar (2011).
	PSev2: Level of Impact on you, if someone has unauthorized access to your (Email, Facebook, Twitter, etc) account(s). [No/Very Low Impact=1] to [Very High Impact =5]	Self-developed
	PSev3: Level of Impact on you, if cybercriminal(s) denied you from accessing the entire data on your computer/mobile device until the requested money is paid. [No/Very Low Impact=1] to [Very High Impact =5]	Self-developed
Perceived Susceptibility (PSus)	**PSus1:** There is a chance you will open an email attachment/link with a virus. [Highly unlikely=1] to [Highly Likely=5]	Ng et al.(2009)
	PSus2: There is a chance your personal details were stolen (password, credit card, SSN, Bank account details, etc.) as a result of using an unsecured website. [Highly unlikely=1] to [Highly Likely=5]	Claar (2011)
	PSus3: There is a chance someone getting unauthorized access to my (computer, mobile device, Email, Facebook, etc) accounts. [Highly unlikely=1] to [Highly Likely=5].	Self-developed
	PSus4: There is a chance you will ignore the browser warning alert messages by only focusing on the core area of my interest. [Highly-unlikely=1] to [Highly Likely=5].	Self-developed
Perceived Barriers (PBar)	**PBar1:** Prior to opening an email with an attachment/URL link, exercising care needs to start a new practice, which is difficult. [Strongly Disagree=1] to [Strongly Agree=5].	Ng et al. (2009) and Edwards (2015)
	PBar2: When using the Internet, I have faced difficulty in interpreting browser security warning alert messages. [Strongly Disagree=1] to [Strongly Agree=5].	Self-developed
	PBar3: Configuring the security/privacy settings on the websites needs a great deal of effort. [Strongly Disagree=1] to [Strongly Agree=5].	Edwards(2015)
Perceived Benefits (PBen)	**PBen1:** Prior to opening an email with an attachment/ URL link, exercising care would help me to prevent (virus infection, data loss) from my computer/mobile device. [Strongly Disagree=1] to [Strongly Agree=5].	Ng et al. (2009).
	PBen2: Prior to engaging in any online activity, checking the presence of HTTPS or a key symbol icon/trust mark in the browser address bar would help me to protect my computer/mobile device from being hacked or infected with a virus. [Strongly Disagree=1] to [Strongly Agree=5].	Self-developed
	PBen3: Prior to opening an email with an attachment/ link, identifying the real identity of the sender would help me to reduce cybersecurity incidents. [Strongly Disagree=1] to [Strongly Agree=5].	Ng et al. (2009).
Cues to Action (CTA)	**CTA1:** If I heard about a recent experience with stolen (Email, Facebook, Twitter) login account(s), I would be more conscious of my login account(s) chances of being stolen. [Strongly Disagree=1] to [Strongly Agree=5].	Claar (2011)
	CTA2: If I read news about security incidents as a result of using unsecured Email or websites, I would be more concerned about my computer/mobile device a chance of being hacked. [Strongly Disagree=1] to [Strongly Agree=5].	Edwards (2015)
	CTA3: If I saw a browser security warning alert message about a security	

Constructs	Items Description	Source
	vulnerability, I would be more concerned about my computer/mobile devices' chance of being hacked. [Strongly Disagree=1] to [Strongly Agree=5].	Claar (2011)
Self-Efficacy (SE)	**SE1:** I am confident in my ability on distinguishing between secured and unsafe websites. [Strongly Disagree=1] to [Strongly Agree=5].	Self-developed
	SE2: I am confident in my ability on identifying malicious email attachments/links. [Strongly Disagree=1] to [Strongly Agree=5].	Ng et al.(2009) and Edwards (2015)
	SE3: I am confident in my ability on configuring the security or privacy settings on the websites I am using. [Strongly Disagree=1] to [Strongly Agree=5].	Edwards (2015)
	SE4: I am confident in my ability on understanding security warning alert messages. [Strongly Disagree=1] to [Strongly Agree=5].	Self-developed
Concern For Privacy (CFP)	**CFP1:** I am concerned that the private information I submit to online institutions could be misused. [Strongly Disagree=1] to [Strongly Agree=5].	Claar (2011) and Edwards (2015)
	CFP2: I am concerned that other people can see my private information on the Internet. [Strongly Disagree=1] to [Strongly Agree=5].	Edwards (2015)
	CFP3: I am concerned about submitting my private information to online institutions, because of what other people might do with it. [Strongly Disagree=1] to [Strongly Agree=5].	Edwards (2015)
	CFP4: I am concerned about submitting my private information to online institutions because it might be used in a manner that I did not expect. [Strongly Disagree=1] to [Strongly Agree=5].	Edwards (2015)
Security Behavior (SB)	**SB1:** Prior to replying to the received Email, I first check the real identity of the sender. [Strongly Disagree=1] to [Strongly Agree=5].	Small modification (Ng et al, 2009)
	SB2: I hover my mouse cursor over the attached link in my Email before clicking on it to check its legitimacy.[Strongly Disagree=1] to [Strongly Agree=5].	Self-developed
	SB3: Prior to engaging in any online activity, I check for HTTPS/ key icon/trust mark in the browser URL bar. [Strongly Disagree=1] to [Strongly Agree=5].	Edwards (2015)
	SB4: I do not reply and click on an email link that asks me to provide my username and password. [Strongly disagree=1] to [Strongly Agree=5].	Self-developed
	SB5: I do not reply to an email that promises attractive rewards in return, advertising lottery/ prize, OR urging me to upgrade/update security before the deadline. [Strongly Disagree=1] to [Strongly Agree=5].	Self-developed
	SB6: I pay attention to the browser security warning alert message when using the Internet. [Strongly Disagree=1] to [Strongly Agree=5].	Self-developed
Security Awareness (SA)	**SA1:** Level of awareness about Phishing [Completely unaware=1] to [Very aware=4].	Edwards (2015)
	SA2: Level of awareness about Ransomware [Completely unaware=1] to [Very aware=4].	Self-developed
	SA3: Level of awareness about accessing secured and unsecured websites. [Completely unaware=1] to [Very aware=4].	Edwards (2015)
	SA4: Level of awareness about configuring security or privacy setting on browser. [Completely unaware=1] to [Very aware=4].	Edwards (2015)
	SA5: Level of awareness about password policy. [Completely unaware=1] to [Very aware=4]	Self-developed