Investigation of Individuals' Behavior towards Phishing Attacks Using the Health Belief Model

Danielle Ehizibue
University of Twente
PO Box 217, 7500 AE Enschede
the Netherlands
d.ehizibue@student.utwente.nl

ABSTRACT

Cybercrime, in particular social engineering attacks, continue to evolve rapidly as individuals' reliance on the Internet grows. Prior studies have repeatedly shown that cybersecurity is not just a technological problem, it requires an understanding of the behavior of people toward cyber security. Researchers have created many interventions to promote behavioral change against phishing attacks. However, these interventions are not effective for all individuals. Consequently, this research aims to obtain an understanding of individuals' behavior toward phishing prevention attacks using the Health Belief Model (HBM). An online questionnaire was conducted from December 23, 2021, to January 21, 2022. The questionnaire included demographic questions as well as questions related to each HBM construct, using a 7-point Likert scale. Before analyzing the results, the Cronbach's Alpha of each construct was computed and an Exploratory Factor Analysis was conducted to determine the reliability and validity of the questionnaire. Furthermore, ordinal regression analysis and binary regression analysis were performed to test the hypotheses. The results show that perceived severity, perceived barriers, self-efficacy, and perceived importance have a significant influence on the likelihood that an individual will perform phishing attack prevention behavior. These findings can be used to create effective and tailored cybersecurity interventions for individuals.

Keywords

Cybersecurity, Health Belief Model, Intervention, Phishing, Social engineering.

1. INTRODUCTION

Advances in Internet technology, have given rise to a multitude of cyberattacks on individuals as well as organizations [1]–[3]. In 2020, about 80 percent of individuals in the EU-27 accessed the Internet daily, 29 percent higher than in 2010 [4]. As the Internet enhances individuals' everyday lives, so the opportunities for cybercriminals increase regularly [5], [6]. One type of cybercrime is social engineering. Social engineering is primarily known as a non-technical type of attack whereby psychological tricks are used to deceive individual users to obtain unauthorized access to information systems [7]. For example, phishing, a widely used social engineering attack – generally performed via email, is the practice in which attackers send fraudulent messages to entice users to open a malicious attachment or a link directing to a fake website [8]. The impact of phishing attacks is severe, as it can result in financial loss, data loss, reputational damage, and several other damages to individuals and organizations [9]. Previous research has shown that individuals are still the weakest link in cybersecurity [10], [11]. Hence, attackers target people rather than attempting to exploit technical vulnerabilities. Researchers have developed interventions, for instance, awareness campaigns, security education, and training [12], [13]. The interventions aim to make individuals more aware of phishing and to change their behavior towards protecting themselves against phishing attacks. Nevertheless, some interventions have proven to be not effective [14], [15], as 'one size fits all' interventions do not provide the desired impact in changing users' behavior. According to [2], interventions that are tailored to the needs of an individual are more effective than those with a broad focus. Additionally, interventions are more likely to be successful when it is designed based on models and theories that explain or predict the specific behavior of an individual [16]. In this study, we examine the preventive behavior of individuals towards phishing attacks. Meaning the actions that an individual should perform to prevent losses as a result of a phishing attack, such as exercising caution when receiving a suspicious email or checking the legitimacy of an URL [17].

The theoretical framework used in this study is the Health Belief Model (HBM). The HBM is a model primarily used in the health domain to explain and predict various types of preventive health behavior, such as smoking, influenza vaccinations, dental visits, dieting, and exercising [18]. The HBM consists of six main constructs: *perceived susceptibility*, *perceived severity*, *perceived benefits*, *perceived barrier*s, *cues to action,* and *self-efficacy.* According to the HBM, individuals are more willing to take preventive action if they consider themselves personally vulnerable to the threat of a health risk (*perceived susceptibility*). Including when they perceive the threat and the consequences of not taking action to be serious (*perceived severity*). Moreover, the benefits, difficulties, or costs that may arise from performing the preventive action might motivate or withhold an individual to change their behavior (*perceived benefits, perceived barriers*). In addition, the HBM states that events or social influence can trigger an individual to change their behavior (*cues to action*) as well as *self-efficacy* – one's confidence in the ability to successfully perform the behavior. At last, other variables such as demographic (e.g. age, gender), sociopsychological and structural variables (e.g. knowledge about the disease) might influence an individual's health behavior. Previous studies also added *perceived importance* as an extension to the HBM [19]. This construct is defined as the amount of value that a person attaches to the outcomes of a particular behavior.

36th Twente Student Conference on IT, Febr. 4th, 2022, Enschede, The Netherlands. Copyright 2022, University of Twente, Faculty of Electrical Engineering, Mathematics and Computer Science.

Related work

The Health Belief Model can also be applied in the field of Cybersecurity. Although, very limited research has been done on the use of the Health Belief Model to explain phishing attack prevention behavior. Ng et al. [17] adopted the HBM as a theoretical framework to examine the computer security behavior of users. However, a modified version of the HBM was used, as the construct *general security orientation* was included. The authors conducted a survey on 134 employees to test the model. Their findings showed that the constructs perceived susceptibility, perceived benefits, and self-efficacy have a significant effect on users' behavior towards computer security. Moreover, Humaidi et al. [20] examined users' behavior towards Health Information Systems Security Policies. The authors constructed a research model based on an extended version of the HBM as their model included the additional construct *perceived working experience*. Perceived work experience, perceived severity, perceived benefits, cues to action, self-efficacy, and perceived barriers were found to be significant determinants of health information system's security policies compliance behavior. Furthermore, Claar [21] used six HBM constructs, and included socio-demographic variables (age, gender, education, and prior experience of attack) as moderators to predict computer security usage behavior. The results indicated that perceived susceptibility, perceived barriers, self-efficacy, and the interaction between age and perceived barriers were important predictors that influence a user to perform computer security usage behavior.

1.1 Research questions

The primary purpose of this research is to contribute to a better understanding of the phishing attack prevention behavior of individuals. Therefore we will examine the relationships between seven HBM constructs and the likelihood of phishing attack prevention behavior as well as an individual's actual behavior. This knowledge can be used to develop effective, tailored cybersecurity interventions to prevent phishing attacks.

The research question and hypotheses are described as follows:

RQ: To what extent could individuals' behavior towards phishing attack prevention be predicted?

- **H1:** The likelihood of performing phishing attack prevention behavior can be predicted using the HBM.
- **H2:** Individuals' actual phishing attack prevention behavior can be predicted using the HBM.

The remainder of the paper is structured as follows: Section 2 presents the research model. Section 3 describes the research methodology: the development and validation of the questionnaire. In Section 4, we present the results of our data analysis. Section 5 discusses the results, their limitations, and suggestions for future work. Finally, Section 6 concludes the paper and provides practical implications.

2. RESEARCH MODEL

Our research model is illustrated in Figure 1. The model was developed based on the Health Belief Model. The seven key constructs of this model are described as follows:

Perceived Susceptibility refers to an individual's belief of being susceptible to a phishing attack.

Perceived Severity refers to an individual's belief concerning the seriousness of being a victim of a phishing attack and its consequences if not taking action.

Perceived Benefits refer to an individual's belief in the positive outcomes of taking action to prevent phishing attacks.

Perceived Barriers refer to an individual's belief in the negative outcomes, such as difficulties or hindrances of taking action to prevent phishing attacks

Self-Efficacy refers to an individual's belief regarding his/her ability to successfully perform phishing attack prevention behavior.

Cues to action refer to the events that motivate or trigger an individual to take action to prevent phishing attacks. For example, news reports and awareness posters.

Perceived Importance refers to an individual's belief in the importance of outcomes when taking actions to prevent phishing attacks.

The above constructs, also called predicting variables, are independently related to the outcome variable 'likelihood of engaging in phishing attack prevention behavior' and 'an individual's actual behavior towards phishing attack prevention'(Figure 1).

The likelihood of engaging in phishing attack prevention behavior refers to whether individuals intend to perform preventive measures against phishing attacks. This is going to be predicted by the seven predictor variables.

Actual behavior towards phishing attack behavior refers to the actual behavior of an individual towards phishing attack prevention. This data was obtained from the phishing simulation that the UT security awareness program (PASSWORD) carried out. The results of the phishing simulation showed whether an individual clicked on a phishing link or not. The findings were combined with this study to predict one's actual behavior towards phishing attacks.

Moreover, the demographic variables age and gender, and structural variables: knowledge about phishing and prior victim of a phishing attack will be used as moderators between the relationship of the predictors and the outcome variables. This way it can be determined whether the differences in age, gender, knowledge of phishing, and prior victim influences the relationship between the predictor variables and the outcome variable. The hypotheses for the moderator variables are as follows: **H3)** Age significantly moderates the relationship between the individual beliefs *(perceived susceptibility, severity, benefits, barriers, self-efficacy, cues to action, perceived importance)* and phishing attack prevention behavior. **H4)** Gender significantly moderates the relationship between individual beliefs and phishing attack prevention behavior. **H5)** Knowledge of phishing significantly moderates the relationship between individual beliefs and phishing attack prevention behavior. **H6)** Prior victim of phishing significantly moderates the relationship between individual beliefs and phishing attack prevention behavior.

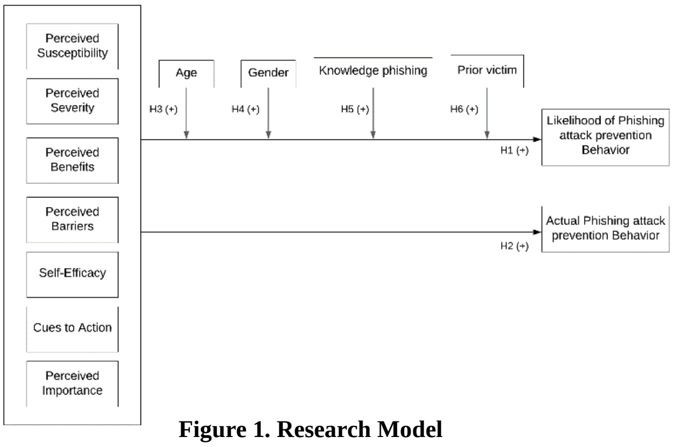

Figure 1. Research Model

3. METHODOLOGY

3.1 Questionnaire Development

The research model was tested using a questionnaire as a quantitative research method. The questionnaire was developed based on observations from existing literature. The questionnaire covered the following three parts:

1. Socio-demographic variables

First, the respondents were asked to state their gender. The variable 'gender' was measured as a categorical variable containing the following three categories: 'Male', 'Female' and 'Prefer not to say'. Second, an open-ended question was asked to assess the respondent's age. The variable 'age' was measured as a numerical value on a continuous scale. For instance, '20' means 20 years old. Further, the respondents were asked to state their study and the academic year they started the study. The variable 'study' was a categorical variable and included the following categories: 'Psychology', 'Health/Medicine' and 'Other'. 'Psychology' refers to the study of Psychology at the University of Twente (UT), 'Health/Medicine' refers to the studies of Technical Medicine and Biomedical Technology at the UT. 'Other' refers to other studies at the UT, for example, 'Communication Science'. Likewise, the variable 'academic year' was a categorical variable and included the following values: ' academic year 2021-2022', 'academic year 2021-2022', 'academic year 2020-2021', 'academic year 2019-2020' and 'academic year 2018-2019 or earlier'. For example, 'academic year 2021-2022' means that the respondent was registered for the study in the year 2021-2022.

2. Structural variables

Two questions were asked to assess the respondents' knowledge of phishing. Firstly, the respondents were asked if they know what phishing is. Hence, the variable 'knowledge' was a categorical variable, containing the values 'Yes' and 'No'. 'Yes' means that the respondent knows what phishing is, whereas 'No' means that the respondent does not know what phishing is. Also, the following question was asked to test their knowledge:

Complete the following sentence: Phishing is………..

(Option 1). the practice in which an attacker sends an enormous amount of data to a specific website, intending to shut down the website and make it unavailable for users.

(Option 2). the practice in which an attacker sends fraudulent messages to users to trick them into revealing their personal information. It is usually performed through email, convincing the user to click on a malicious link or attachment.

(Option 3). the practice in which an attacker repeatedly attempts to guess the password of a user, by using numerous combinations of numbers, letters, and symbols until the password is discovered.

Afterward, the correct answer was given to the respondents, which was Option 2: 'Phishing is the practice in which an attacker sends fraudulent messages to users to trick them into revealing their personal information. It is usually performed through email, convincing the user to click on a malicious link or attachment.'. Furthermore, the respondents were asked whether they had been a prior victim of phishing attacks in the past six months. The question was asked as follows: Have you been a victim of email phishing attacks (e.g. clicked on a malicious link, downloaded malware, revealed confidential data, or suspected fraudulent transactions) in the past 6 months?. The variable 'prior victim' was categorical, containing the values: 'Yes' and 'No'. 'Yes' means that the respondent has been a victim of a phishing attack(s), whilst 'No' means that the respondent has not been a prior victim of a phishing attack(s).

3. HBM variables

The third part of the questionnaire included questions related to each HBM construct. The HBM constructs were measured as items (i.e. single-sentence statements) using a 7-point Likert scale, from 1 (Strongly disagree) to 7 (Strongly agree). A 7-point Likert scale was chosen as this increases the reliability and validity of the items [22]. Most items used in the questionnaire were adapted from other studies. A total of 51 items were used to measure the HBM constructs. Appendix A presents the list of items that were used in the questionnaire. First of all, the HBM construct 'Phishing attack prevention behavior (BEH)' was measured using five items with a scale from 1 = strongly disagree to 7 = strongly agree. 'BEH' refers to the self-reported phishing attack prevention behavior of the respondent. For example, the respondents were asked to state their level of agreement or disagreement to the following statements related to 'BEH': "Before clicking on a link in an email, I will first check if the sender and subject of the email make sense." And "Before clicking on a link in an email, I will first check if the URL is legitimate". Next, the HBM construct 'perceived susceptibility' was coded as 'SUS' and measured using five items with a scale from 1 = strongly disagree to 7 = strongly agree. For instance, the following two statements were given to the respondents: "I will likely be a victim of an email phishing attack." And "There is a good possibility that my personal information (login credentials, bank account details, etc.) gets stolen and misused due to an email phishing attack.". Moreover, the HBM construct 'perceived severity' was coded as 'SEV' and was also measured using five items with a scale from 1 = strongly disagree to 7 = strongly agree. Examples of 'SEV' statements are: "Having my computer infected by a virus as a result of an email phishing attack is a serious problem for me." And "The thought of becoming a victim of an email phishing attack scares me.". Further, the HBM construct 'perceived benefits' was coded as 'BEN'. This construct contained nine items, measured with a scale from 1 = strongly disagree to 7 = strongly agree. For instance, the respondents were asked whether they agreed with the following statements: "Educating myself about phishing is effective in preventing becoming a victim of an email phishing attack. As well as, "Having anti-virus software is effective in preventing becoming a victim of an email phishing attack". The code 'BAR' was used for the HBM construct 'perceived barriers', this was also measured on a 7-point Likert scale. For example, the following statements were given: "I don't know how to find and get the right tools or software to prevent email phishing attacks." And "Exercising care when reading emails with links would require starting a new habit, which is difficult.". Moreover, the HBM construct 'self-efficacy' was coded as 'SEF' and also measured on a 7-point Likert scale using four items (e.g. "I can recognize a malicious URL from a legitimate URL." And "I can recognize a phishing email even if there was no one around to help me."). The HBM construct 'Cues To Action' was coded as 'CUE', containing seven items measured on a scale from 1 to 7 (strongly disagree – strongly agree). Examples of statements that were given are: "If I noticed a suspicious transaction on my bank account, I would be concerned about being a victim of an email phishing attack." And "If my family were to tell me of a recent experience with an email phishing attack, I would be more conscious of potentially falling victim to an email phishing attack.". Lastly, the HBM construct 'perceived importance' was coded as 'IMP' and also measured with a scale from 1 = strongly disagree to 7 = strongly agree. This construct contained six items. For example, the respondents were asked whether they disagreed or agreed with the following statements related to 'IMP': "Taking action to prevent email phishing attacks is important for me." And "Educating myself about email phishing attacks is important for me.".

3.2 Ethics Statement

This study was reviewed and approved by the BMS Ethics Committee of the University of Twente on December 17, 2021 (Reference number: 211390). Additionally, informed consent was obtained from the respondents, provided at the start of the questionnaire.

3.3 Data collection method

The questionnaire was conducted through Qualtrics[23], a web-based survey platform, and made available on Sona Systems[24] from 23 December 2021 till 21 January 2022. The questionnaire was administered to undergraduate students from the studies Psychology, Communication Science, Biomedical Technology, and Technical Medicine at the University of Twente. The questionnaire was also distributed through Gmail and social media platforms LinkedIn and WhatsApp. Additionally, the snowballing sampling method was used to increase the sample size.

3.4 Data analysis method

The data were processed and analyzed in Python 3. Besides, IBM SPSS 23.0 was used to run the hypothesis tests. Before conducting the hypothesis tests, the reliability and validity of the questionnaire were assessed.

3.4.1 Construct reliability and validity

The key constructs were measured with various items, hence it is significant to test the reliability of each construct to ensure that the set of items is consistent with each other. Cronbach's alpha was used to determine the internal consistency of the items. For internal consistency, a value of at least 0.7 is acceptable, whereas values of 0.6 and below are not acceptable [25]. The results in Table 1 show that the internal consistency of each construct has good reliability. The scale reliability of Behavior was improved from 0.686 to 0.810 with the removal of item BEH5. Item SEV1 was also removed, as this led to an increase of the scale reliability from 0.663 to 0.686.

Table 1. Reliability analysis

Construct	# of items	Cronbach's alpha
Behavior*	4	0.810
Perceived Susceptibility	5	0.738
Perceived Severity*	4	0.686
Perceived Benefits	9	0.791
Perceived Barriers	10	0.825
Self-Efficacy	4	0.844
Cues to action	7	0.782
Perceived Importance	6	0.883

* . Cronbach's alpha after removing one item.

Furthermore, an Exploratory Factor Analysis was performed to test the validity of the questionnaire. By conducting an EFA, it can be determined whether the set of items of each construct are correlated to each other. For instance, we assume that all five items of 'BEH' will be loaded and grouped. Before conducting the EFA, the Bartletts' test [26] and Kaiser-Meyer-Olkin (KMO)[27] were conducted to determine whether the sample data was appropriate. The Bartletts' test was statistically significant ($p < 0.001$) and the overall KMO of the data was 0.65. A value of KMO less than 0.5 is considered unacceptable[27]. Hence, the sample data was appropriate and the EFA could be performed. Eight factors based on HBM were extracted with an eigenvalue greater than 1. The items SUS2, SUS3, SEV2, SEV3, BEN4, BEN5, BEN9, and BAR10 were removed as results of the EFA since their factor loadings were < 0.50. The factor loadings of all HBM constructs can be found in Appendix B.

After assessing the construct reliability and validity, the scores of each item were combined into one single construct score. The descriptive statistics of each construct are shown in Table 2.

Table 2. Construct Descriptive Statistics: the means and standard deviations (SD)

Construct	Mean	SD
Behavior	5.93	1.00
Perceived Susceptibility	3.21	1.34
Perceived Severity	5.99	1.07
Perceived Benefits	5.71	0.77
Perceived Barriers	3.49	0.98
Self-Efficacy	4.51	1.22
Cues to action	5.64	0.71
Perceived Importance	5.06	0.99

3.4.2 Regression analyses

The data did not pass the test of normality, hence an ordinal regression analysis was performed for H1, and a binary logistic regression analysis was conducted for H2. For each analysis, our model was run twice. In the first model, the outcome variable was regressed on the predictors Perceived Susceptibility, Perceived Severity, Perceived Benefits, Perceived Barriers, Self-Efficacy, Cues to action, and Perceived Importance. In the second model, the moderator variables age, gender, knowledge about phishing, and prior victim to phishing attacks were included.

4. RESULTS

4.1 Demographic Profile of Respondents

A total of 160 responses were recorded. However, 79 responses remained after analyzing the data and removing uncompleted responses. Table 3 presents the socio-demographic characteristics of the respondents. A large portion of the respondents was female (n=52). Moreover, the mean age of the respondents was 20.2. A large majority of the respondents were between the ages of 18 and 24 (93.7%). 72% of the respondents (n=57) were Psychology students, 15.2% were from the study Biomedical Technology (n=12), followed by 12.7% Communication Science students (n=10). Slightly more than half (n=55) of the respondents reported that they knew what phishing meant. About three-fifths (n=61) have not been a victim of email phishing attacks in the past 6 months.

4.2 Hypothesis testing

4.2.1 The likelihood of phishing attack prevention behavior can be predicted using the HBM (H1)

An ordinal logistic regression analysis was conducted to determine the statistical significance of the hypotheses listed below:

H1a: *Perceived susceptibility is positively related to phishing attack prevention behavior.*

H1b: *Perceived severity to is positively related to phishing attack prevention behavior.*

H1c*: Individuals with high levels of perceived benefits will be more likely to adopt phishing attack prevention behavior.*

H1d: *Individuals with high levels of perceived barriers will be less likely to adopt phishing attack prevention behavior.*

H1e*: Individuals with high levels of self-efficacy are more likely to adopt phishing attack prevention behavior.*

H1f: *Individuals who have been exposed to high levels of cues to action are more likely to adopt phishing attack prevention behavior.*

H1g: *Individuals with high levels of perceived importance are more likely to adopt phishing attack prevention behavior.*

Table 3. Demographic characteristics of the respondents

Demographic	Frequency (n=79)	Percent (%)
Gender		
Male	27	34.2
Female	52	65.8
Age group		
< 18	1	1.3
18 – 24	74	93.7
> = 25	4	5.1
Study		
Psychology	57	72.2
Communication Science	10	12.7
Biomedical/Medicine	12	15.2
Knowledge about phishing		
Yes	55	69.6
No	24	30.4
Prior victim of phishing		
Yes	18	22.8
No	61	77.2

Table 4 shows the overall fit of both regression models that were run. First of all, the data needed to satisfy the proportional odds assumption to ensure that the test is not violated. The p-value of both models is not statistically significant ($p \geq 0.05$), therefore we have not violated the test of proportional odds, hence correct interpretations can be made [28]. Furthermore, both models showed a good fit to the data ($p \geq 0.05$) [29]. The pseudo R^2 of Nagelkerke is almost similar to the R2 of a linear regression analysis[29]. This means that the first model explains a 50.6% change in the outcome variable (phishing attack prevention behavior), as a result of the predictors. Whereas the second model explains 80.8% of the variance in the outcome variable. Table 5 displays the results of the ordinal logistic regression models that were run. In the first model, the main effects of the outcome variable (phishing attack prevention behavior) and the predictors (perceived susceptibility, perceived severity, perceived benefits, perceived barriers, perceived self-efficacy, cues to action, and perceived importance) were tested. Based on the outcomes of the first model, it can be seen that *H1a* is not supported by the model (β = 0.237, p = 0.240). *H1b* predicted that perceived severity would be positively related to phishing attack prevention behavior, this was supported as it was statistically significant (β = 0.502, p = 0.012). *H1c*, which predicted that perceived benefits would be positively related to phishing attack prevention behavior, was not supported (β = -0.94, p = 0.781). However, *H1d* was supported (β = -0.726, p = 0.019), which predicted that perceived barriers are negatively related to phishing attack prevention behavior. Also, *H1e* was supported, which predicted a positive relationship between self-efficacy and phishing attack prevention behavior (β = 0.822, p = 0.001). Furthermore, *H1f* was not supported by the model (β = 0.328, p = 0.282), whilst *H1g*, which predicted that perceived importance is positively related to phishing attack prevention behavior, was supported (β = 0.670, p = 0.013).

Next, the main effects of the moderating variables (age, gender, knowledge, and prior victim) and the two-way interactions were included in the second model. The results show that age did not significantly influence the relationship between the predictors (perceived susceptibility, perceived severity, perceived benefits, perceived barriers, perceived self-efficacy, cues to action) and the outcome variable, which was not supported by the model. In contrast, *H3g*, which predicted that age affects the relationship between perceived importance and phishing attack prevention behavior, was supported (β = 0.653, p = 0.046). Additionally, *H4a* which predicted that gender influences the relationship between perceived susceptibility and phishing attack prevention behavior was supported (β = -1.682, p = 0.021). Similarly, *H4f* was supported by the model, which indicated that gender affects the relationship between cues to action and phishing attack prevention behavior (β = 3.903, p = 0.006). Whereas hypotheses *H4b – H4e* and *H4g* were not supported by the model. Then, hypotheses *H5a – H5e* was not statistically significant, hence it was not supported. Nevertheless, *H5f* significantly predicted that knowledge about phishing affects the relationship between cues to action and phishing attack prevention behavior (H5f, β = 3.594, p = 0.012). Also, *H5g*, which predicted that knowledge about phishing, affects the relationship between perceived importance and phishing attack prevention behavior was supported (H7g, β = -3.426, p = 0.013). Lastly, the hypotheses *H6a-H6g*, which predicted that prior victim to phishing attacks influences the relationship between the predictors and the outcome variable were rejected, as there was no statistical significance.

Table 4 Ordinal logistic regression Model Fit

	Score test for the proportional odds assumption			Goodness-of-fit of overall model			
Model	**Chi-square**	**df**	**Significance**	**Chi-square**	**df**	**Significance**	**Pseudo R^2**
1	50.505	84	.999	867.254	1007	.999	0.506
2	250.366	468	1.000	4204.132	975	.000	0.808

Table 5 . Results of ordinal logistic regression analyses of HBM constructs and moderating variables.

	Predictor	β	Std. Error	p-value	EXP(β)	Results
Model 1	Perceived susceptibility	.237	.2017	.240	1.267	H1a rejected
	Perceived severity	.502	.2004	.012*	1.652	H1b accepted
	Perceived benefits	-.094	.3361	.781	.911	H1c rejected
	Perceived barriers	-.726	.3090	.019*	.484	H1d accepted
	Perceived self-efficacy	.822	.2486	.001**	2.275	H1e accepted
	Cues to action	.328	.3045	.282	1.388	H1f rejected
	Perceived importance	.670	.2692	.013*	1.955	H1g accepted
Model 2	Age*Perceived susceptibility	.043	.2453	.859	1.044	H3a rejected
	Age*Perceived severity	-.160	.2615	.542	.852	H3b rejected
	Age*Perceived benefits	.140	.3943	.723	1.150	H3c rejected
	Age*Perceived barriers	-.021	.3008	.944	.979	H3d rejected
	Age*Perceived self-efficacy	.246	.2519	.328	1.279	H3e rejected
	Age *Cues to action	.332	.3515	.345	1.394	H3f rejected
	Age*Perceived importance	.653	.3269	.046*	1.921	H3g accepted
	Gender*Perceived susceptibility	-1.682	.7264	.021*	.186	H4a accepted
	Gender*Perceived severity	.562	10.509	.593	1.755	H4b rejected
	Gender*Perceived benefits	-1.655	13.290	.213	.191	H4c rejected
	Gender*Perceived barriers	.744	15.425	.630	2.105	H4d rejected
	Gender*Perceived self-efficacy	.712	12.418	.566	2.038	H4e rejected
	Gender*Cues to action	3.903	14.059	.006**	49.533	H4f accepted
	Gender*Perceived importance	-1.632	12.115	.178	.196	H4g rejected
	Knowledge*Perceived susceptibility	-.667	10.654	.531	.513	H5a rejected
	Knowledge*Perceived severity	1.462	10.584	.167	4.315	H5b rejected
	Knowledge*Perceived benefits	2.362	14.671	.107	10.608	H5c rejected
	Knowledge*Perceived barriers	-.973	18.636	.602	.378	H5d rejected
	Knowledge*Perceived self-efficacy	1.597	11.022	.147	4.938	H5e rejected
	Knowledge*Cues to action	3.594	14.375	.012*	36.362	H5f accepted
	Knowledge*Perceived importance	-3.426	13.800	.013*	.033	H5g accepted
	Prior victim*Perceived susceptibility	-.701	10.956	.522	.496	H6a rejected
	Prior victim*Perceived severity	-.146	12.130	.904	.864	H6b rejected
	Prior victim*Perceived benefits	-3.383	17.715	.056	.034	H6c rejected
	Prior victim*Perceived barriers	1.580	25.028	.528	4.853	H6d rejected
	Prior victim*Perceived self-efficacy	-2.179	12.934	.092	.113	H6e rejected
	Prior victim*Cues to action	.424	25.059	.866	1.528	H6f rejected
	Prior victim*Perceived importance	-2.471	17.123	.149	.085	H6g rejected

*p ≤ 0.05; **p ≤ 0.01

4.2.2 H2: Individuals' actual phishing attack prevention behavior can be predicted using the HBM.

A binary logistic regression analysis was performed to determine the statistical significance of the following hypotheses:

H2a: *Perceived susceptibility is positively related to actual phishing attack prevention behavior.*

H2b*: Perceived severity is positively related to phishing attack prevention behavior.*

H2c: *Individuals with high levels of perceived benefits will be more likely to adopt phishing attack prevention behavior.*

H2d: *Individuals with high levels of perceived barriers will be less likely to adopt phishing attack prevention behavior.*

H2e: *Individuals with high levels of self-efficacy are more likely to adopt phishing attack prevention behavior.*

H2f: *Individuals who have been exposed to high levels of cues to action are more likely to adopt phishing attack prevention behavior.*

H2g: *Individuals with high levels of perceived importance are more likely to adopt phishing attack prevention behavior*.

In model 1, the main effects between the outcome variable 'Clicked' - this refers to individuals that clicked or not clicked on a phishing link (one's actual phishing attack prevention behavior) and the predictors were tested. Likewise, in model 2 the moderating variables (age, gender, knowledge, prior victim) were included to test the effect of each moderating variable. Firstly, the Hosmer & Lemeshow [25] test was conducted to test the fit of the models (Table 6). Both models were not significant ($p \geq 0.05$), this indicates that the models are a good fit. The classification tables of both binary logistic regression models are shown in Table 7. The classification table of model 2 shows that the actual observed values for individuals that not clicked on a link are 60+1 = 61. 60 of those cases were correctly predicted by the model, therefore the accuracy rate is 98.4%. On the contrary, there were 18+0 = 18 actual observed values of individuals that clicked on a link. Thus, 18+0+1 = 19 individuals expressed the intention to click on a link, but none was correctly predicted by the model, therefore the accuracy rate is 0.0%. The overall classification accuracy of model 1 is 75.9%, which means that 75.9% of the sample size was correctly predicted into the right group. Furthermore, the classification table of model 2 displays that the entire same size was correctly predicted by the model. The actual observed value of individuals that did not click on a link is 61. All of those cases were predicted accurately, this led to an accuracy rate of 100%. Additionally, the actual observations of individuals that clicked on a link were 18, and all were correctly predicted by the model, so the overall classification accuracy of model 2 is 100%.

Table 6 The overall fit of the model

Hosmer and Lemeshow Test

Model	Chi-square	df	Significance
1	7.696	8	.464
2	.000	8	1.000

Table 7. Classification tables of the results from the binary logistic regression models

				Predicted		
				Clicked		
	Observed			0 (= no)	1 (= yes)	Percentage correct
Model 1	Step 1	Clicked	0 (= no)	60	1	98.4
			1 (= yes)	18	0	0.0
		Overall percentage				75.9
	A cut-value of 0.500 was used					
Model 2	Step 1	Clicked	0 (= no)	61	0	100.0
			1 (= yes)	0	18	100.0
		Overall percentage				100.0
	A cut-value of 0.500 was used					

Subsequently, the results of the binary logistic regression analyses of both models are presented in Table 8. In the first model, the main effects of the outcome variable (actual phishing attack prevention behavior) and the predictors (perceived susceptibility, perceived severity, perceived benefits, perceived barriers, perceived self-efficacy, cues to action, and perceived importance) were tested. Based on the outcomes of the first model, it can be seen that hypotheses *H2a – H2g* are not statistically significant, therefore rejected. This means that the predictors variables (perceived susceptibility, perceived severity, perceived benefits, perceived barriers, perceived self-efficacy, cues to action, and perceived importance) are not positively related to actual phishing attack prevention behavior (H2a, β = -0.1.20, p = 0.656), (H2b, $\beta = 0.299$, p = 0.310), (H2c, $\beta = -0.298$, p = 0.490), (H2d, $\beta = -0.125$, p = 0.772), (H2e, $\beta = -0.394$, p = 0.250), (H2f, $\beta = 0.133$, p = 0.767), (H2g, $\beta = 0.354$, p = 0.362). In the same way, the hypotheses which predicted that age, gender, knowledge, and prior victim of phishing would have a significant interaction effect on the relationship between the predictor variables and the outcome variable was not statistically significant.

5. DISCUSSION

5.1 Discussion of results

The results of the study show that perceived severity, perceived barriers, self-efficacy, and perceived importance have a significant influence on the likelihood of an individual performing phishing attack prevention behavior. This means that an individual who perceives a phishing attack and its consequences as very serious would more likely perform phishing attack prevention behavior. Additionally, individuals with high levels of perceived barriers will be less likely to take preventive measures against phishing attacks. This indicates that the difficulties or inconveniences of taking preventive measures, demotivates an individual to perform phishing attack prevention behavior. Moreover, self-efficacy significantly influences phishing attack prevention behavior. This is not surprising, as previous studies have also shown that one's confidence in successfully performing security has a significant influence on the likelihood of engaging in preventive behavior [17], [21].

Table 8 Results of binary logistic regression analyses of HBM constructs and moderating variables

	Predictor	β	Std. Error	p-value	EXP(B)	Results
Model 1	Perceived susceptibility	-.120	.269	.656	.887	H2a rejected
	Perceived severity	.299	.294	.310	1.348	H2b rejected
	Perceived benefits	-.298	.431	.490	.742	H2c rejected
	Perceived barriers	-.125	.431	.772	.882	H2d rejected
	Perceived self-efficacy	-.394	.342	.250	.675	H2e rejected
	Cues to action	.133	.449	.767	1.143	H2f rejected
	Perceived importance	.354	.389	.362	1.425	H2g rejected

Moreover, our findings indicate that perceived importance is also a significant predictor of phishing attack prevention behavior. This indicates that individuals who perceive the benefits of taking actions as valuable will more likely practice phishing attack prevention behavior. Furthermore, of the moderating variables (age, gender, prior victim, and knowledge), it was shown that the change in age significantly influences the relationship between perceived importance and phishing attack prevention behavior. Similarly, our findings show that gender (male or female) influences the direction of the relationship between perceived susceptibility and phishing attack prevention behavior, including the relationship between cues to action and phishing attack prevention behavior. Knowing what phishing means also moderates the relationship between cues to actions and phishing attack prevention behavior. Besides, our findings indicate that the relationship between perceived importance and phishing attack prevention behavior is impacted by knowledge of phishing. On the contrary, perceived susceptibility, perceived benefits, and cues to action is not strongly associated to the likelihood of performing phishing attack prevention behavior.

Additionally, our findings show that the regression coefficients (β) of the predictor variables perceived susceptibility benefits, barriers and self-efficacy are negative, which indicates that these constructs demonstrate a decreasing likelihood on an individual's actual behavior towards phishing attacks, thus whether an individual intends to click on a phishing link. However, based on the results, that is not statistically significant. Moreover, individuals that are most likely to score high on perceived severity, cues to action, and perceived importance will more likely have the intention to click on a phishing link, but this is also not statistically significant according to the results.

5.2 Limitations and future work

This study only focused on phishing attack prevention behavior. However, there are also other types of social engineering attacks, therefore this study can be used as a guide for other researchers to investigate individuals' behavior on, for instance, baiting. Another limitation is that the sample size of this study was small and only included undergraduate students. Thus, for future work this exact research can be performed on a larger and/or different population.

6. CONCLUSION

This study aimed to examine individuals' behavior towards phishing attack prevention. The Health Belief Model (HBM) was used as a framework to identify the constructs that can predict individuals' behavior. Overall, the findings have shown that the perceptions of individuals towards the seriousness of a phishing attack, increase the likelihood that one will perform phishing attack prevention behavior. Thus, interventions that focus on the damages and losses that phishing attacks cause, can give individuals a realistic perception of the seriousness and consequences of a phishing attack[17]. Moreover, targeted security awareness education programs or training that teach problem-solving and decision strategies related to phishing could be used to overcome the perceptions of barriers to taking preventive measures against phishing attacks [19]. Besides, it will help individuals to gain the confidence to perform phishing attack prevention behavior. Moreover, self-efficacy among individuals can be increased by developing games to teach individuals about the steps needed to prevent phishing attacks [30].

7. REFERENCES

[1] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Rep.*, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

[2] J.-W. Bullee and M. Junger, "How effective are social engineering interventions? A meta-analysis," *Inf. Comput. Secur.*, vol. 28, no. 5, pp. 801–830, Aug. 2020, doi: 10.1108/ICS-07-2019-0078.

[3] D. Gritzalis and G. Tejay, "Cybercrime in the Digital Economy - Editorial," *Comput. Secur.*, vol. 38, pp. 1–2, Oct. 2013, doi: 10.1016/j.cose.2013.08.002.

[4] "Eurostat, 'Individuals frequently using the internet.'" Accessed: Nov. 28, 2021. [Online]. Available: https://ec.europa.eu/eurostat/databrowser/view/tin00092/default/bar?lang=en

[5] East Carolina University, H. Liang, Y. Xue, and East Carolina University, "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *J. Assoc. Inf. Syst.*, vol. 11, no. 07, pp. 394–413, Jul. 2010, doi: 10.17705/1jais.00232.

[6] P. N. Grabosky, "Virtual Criminality: Old Wine in New Bottles?," *Soc. Leg. Stud.*, vol. 10, no. 2, pp. 243–249, Jun. 2001, doi: 10.1177/a017405.

[7] S. Gupta, A. Singhal, and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," in *2016 International Conference on Computing, Communication and Automation (ICCCA)*, Apr. 2016, pp. 537–540. doi: 10.1109/CCAA.2016.7813778.

[8] N. Arachchilage and S. Love, "Security awareness of computer users: A phishing threat avoidance perspective," *Comput. Hum. Behav.*, vol. 38, pp. 304–312, Sep. 2014, doi: 10.1016/j.chb.2014.05.046.

[9] J. Ragucci and S. Robila, *Societal Aspects of Phishing*. 2006, p. 5. doi: 10.1109/ISTAS.2006.4375893.

[10] "The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within."

https://www.kaspersky.com/blog/the-human-factor-in-it-security/ (accessed Nov. 28, 2021).

[11] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy,” *Front. Comput. Sci.*, vol. 3, p. 6, 2021, doi: 10.3389/fcomp.2021.563060.

[12] J.-W. H. Bullée, L. Montoya, W. Pieters, M. Junger, and P. H. Hartel, “The persuasion and security awareness experiment: reducing the success of social engineering attacks,” *J. Exp. Criminol.*, vol. 11, no. 1, pp. 97–115, Mar. 2015, doi: 10.1007/s11292-014-9222-7.

[13] S. Sheng, M. Lanyon, P. Kumaraguru, L. Cranor, and J. Downs, *Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions*, vol. 1. 2010, p. 382. doi: 10.1145/1753326.1753383.

[14] N. Davinson and E. Sillence, “It won’t happen to me: Promoting secure behaviour among internet users,” *Comput. Hum. Behav.*, vol. 26, no. 6, pp. 1739–1747, Nov. 2010, doi: 10.1016/j.chb.2010.06.023.

[15] M. Bada, A. M. Sasse, and J. R. C. Nurse, “Cyber Security Awareness Campaigns: Why do they fail to change behaviour?,” p. 14.

[16] B. Rimer and K. Glanz, *Theory at a Glance: A Guide For Health Promotion Practice (Second Edition)*, 2nd ed. 2005.

[17] B.-Y. Ng, A. Kankanhalli, and Y. (Calvin) Xu, “Studying users’ computer security behavior: A health belief perspective,” *Decis. Support Syst.*, vol. 46, no. 4, pp. 815–825, Mar. 2009, doi: 10.1016/j.dss.2008.11.010.

[18] C. Abraham and P. Sheeran, “The Health Belief Model,” vol. 2, 2015.

[19] R. Orji, J. Vassileva, and R. Mandryk, “Towards an Effective Health Interventions Design: An Extension of the Health Belief Model,” *Online J. Public Health Inform.*, vol. 4, Dec. 2012, doi: 10.5210/ojphi.v4i3.4321.

[20] N. Humaidi, V. Balakrishnan, and M. Shahrom, “Exploring user’s compliance behavior towards Health Information System security policies based on extended Health Belief Model,” in *2014 IEEE Conference on e-Learning, e-Management and e-Services (IC3e)*, Dec. 2014, pp. 30–35. doi: 10.1109/IC3e.2014.7081237.

[21] C. L. Claar, “The Adoption of Computer Security: An Analysis of Home Personal Computer User Behavior Using the Health Belief Model,” p. 150, 2011.

[22] C. C. Preston and A. M. Colman, “Optimal number of response categories in rating scales: reliability, validity, discriminating power, and respondent preferences,” *Acta Psychol. (Amst.)*, vol. 104, no. 1, pp. 1–15, Mar. 2000, doi: 10.1016/S0001-6918(99)00050-5.

[23] “Qualtrics XM // The Leading Experience Management Software,” *Qualtrics*. https://www.qualtrics.com/uk/ (accessed Jan. 31, 2022).

[24] “Research related information | SONA Test Subjects Pool | Home,” *Universiteit Twente*. https://www.utwente.nl/en/bms/intranet/research/sona/ (accessed Jan. 31, 2022).

[25] R. Peterson, “A Meta-Analysis of Cronbach’s Coefficient Alpha,” *J. Consum. Res.*, vol. 21, pp. 381–91, Feb. 1994, doi: 10.1086/209405.

[26] H. Arsham and M. Lovric, “Bartlett’s Test,” in *International Encyclopedia of Statistical Science*, M. Lovric, Ed. Berlin, Heidelberg: Springer, 2011, pp. 87–88. doi: 10.1007/978-3-642-04898-2_132.

[27] H. F. Kaiser, “An index of factorial simplicity,” *Psychometrika*, vol. 39, no. 1, pp. 31–36, Mar. 1974, doi: 10.1007/BF02291575.

[28] B. Peterson and F. E. Harrell, “Partial Proportional Odds Models for Ordinal Response Variables,” *J. R. Stat. Soc. Ser. C Appl. Stat.*, vol. 39, no. 2, pp. 205–217, 1990, doi: 10.2307/2347760.

[29] C. Petrucci, “A Primer for Social Worker Researchers on How to Conduct a Multinomial Logistic Regression,” *J. Soc. Serv. Res.*, vol. 35, pp. 193–205, Apr. 2009, doi: 10.1080/01488370802678983.

[30] G. Baral and N. A. G. Arachchilage, “Building Confidence not to be Phished Through a Gamified Approach: Conceptualising User’s Self-Efficacy in Phishing Threat Avoidance Behaviour,” in *2019 Cybersecurity and Cyberforensics Conference (CCC)*, Melbourne, Australia, May 2019, pp. 102–110. doi: 10.1109/CCC.2019.000-1.

[31] V. L. Champion, “Revised susceptibility, benefits, and barriers scale for mammography screening,” *Res. Nurs. Health*, vol. 22, no. 4, pp. 341–348, 1999, doi: 10.1002/(SICI)1098-240X(199908)22:4<341::AID-NUR8>3.0.CO;2-P.

[32] V. L. Champion, “Instrument development for health belief model constructs,” *Adv. Nurs. Sci.*, vol. 6, no. 3, pp. 73–85, Apr. 1984.

[33] S. R. Boss, “Control, Perceived Risk and Information Security Precautions: External and Internal Motivations for Security Behavior.” 2007.

[34] E. K. Perrault, “Using an Interactive Online Quiz to Recalibrate College Students’ Attitudes and Behavioral Intentions About Phishing,” *J. Educ. Comput. Res.*, vol. 55, no. 8, pp. 1154–1167, Jan. 2018, doi: 10.1177/0735633117699232.

[35] R. LaRose, N. J. Rifon, and R. Enbody, “Promoting personal responsibility for internet safety,” *Commun. ACM*, vol. 51, no. 3, pp. 71–76, Mar. 2008, doi: 10.1145/1325555.1325569.

[36] D. Lee, R. Larose, and N. Rifon, “Keeping our network safe: a model of online protection behaviour,” *Behav. Inf. Technol.*, vol. 27, no. 5, pp. 445–454, Sep. 2008, doi: 10.1080/01449290600879344.

[37] V. L. Champion and C. R. Scott, “Reliability and Validity of Breast Cancer Screening Belief Scales in African American Women,” *Nurs. Res.*, vol. 46, no. 6, pp. 331–337, Dec. 1997.

APPENDIX

A. HBM constructs and coded items

Construct	Code	Items	Reference
Behavior (BEH)	BEH1	I exercise caution when I receive an email with a link.	[17]
	BEH2	Before clicking on a link in an email, I will first check if the sender and subject of the email make sense.	[17]
	BEH3	Before clicking on a link in an email, I will first check if the URL is legitimate.	[17]
	BEH4	I do not click on a link in an email if the content of the email looks suspicious.	[17]
	BEH5	I report phishing emails to help people avoid becoming victims.	Self-developed

Perceived Susceptibility (SUS)	SUS1	I will likely be a victim of an email phishing attack.	[18], [31]
	SUS2	I feel that my chances of receiving an email phishing attack are high.	[32]
	SUS3	I worry a lot about becoming victimized in an email phishing attack.	[32]
	SUS4	It is likely that my computer becomes infected by a virus as a result of an email phishing attack.	[21], [33]
	SUS5	There is a good possibility that my personal information (login credentials, bank account details, etc.) gets stolen and misused due to an email phishing attack.	[18], [21]

Perceived Severity (SEV)	SEV1	Email phishing attacks are harmful.	[34]
	SEV2	The thought of becoming a victim of an email phishing attack scares me.	[18]
	SEV3	If I become a victim of an email phishing attack, my daily work could be negatively affected.	[17]
	SEV4	Having my computer infected by a virus as a result of an email phishing attack is a serious problem for me.	[17]
	SEV5	Losing my personal information (login credentials, bank account details, etc.) due to an email phishing attack is a serious problem for me.	[17]

Perceived Benefits (BEN)	BEN1	Checking if the sender, subject, and link in an email make sense is effective in preventing becoming a victim of an email phishing attack.	[17]
	BEN2	Exercising care before clicking on a link in an email is effective in preventing becoming a victim of an email phishing attack.	[17]
	BEN3	Educating myself about phishing is effective in preventing becoming a victim of an email phishing attack.	Self-developed
	BEN4	Participating in a phishing simulation is effective in preventing becoming a victim of an email phishing attack.	Self-developed
	BEN5	Using two-factor authentication is effective in preventing becoming a victim of an email phishing attack.	Self-developed
	BEN6	Using warning and blocking tools in a web browser or email client (e.g. Gmail, Outlook) is effective in preventing becoming a victim of an email phishing attack.	Self-developed
	BEN7	Having anti-virus software is effective in preventing becoming a victim of an email phishing attack.	[35], [36]
	BEN8	Keeping my computer up to date with the latest security patches and updates is effective in preventing becoming a victim of an email phishing attack.	Self-developed
	BEN9	Asking family or friends for insights about phishing prevention is effective in preventing becoming a victim of an email phishing attack.	Self-developed

Perceived Barriers (BAR)	BAR1	Exercising care when reading emails with links is inconvenient.	[17]
	BAR2	Exercising care when reading emails with links is time-consuming.	[17]
	BAR3	Exercising care when reading emails with links would require a considerable investment of effort other than time.	[17]
	BAR4	Exercising care when reading emails with links would require starting a new habit, which is difficult.	[17]
	BAR5	I don’t know what to look for to detect phishing emails.	Self-developed
	BAR6	I am afraid I would not be able to detect phishing emails.	[18]
	BAR7	I feel insecure about detecting phishing emails.	Self-developed
	BAR8	Educating myself about phishing takes too much time.	Self-developed
	BAR9	I don’t know how to find and get the right tools or software to prevent email phishing attacks.	Self-developed
	BAR10	Asking family or friends for insights about phishing prevention is too uncomfortable.	Self-developed

Self-efficacy (SEF)	SEF1	I am confident of recognizing a phishing email.	[17]
	SEF2	I can recognize a phishing email even if there was no one around to help me.	[17]
	SEF3	I can recognize a malicious URL from a legitimate URL.	Self-developed
	SEF4	I am sure of the steps to follow to recognize a phishing email.	[37]

Cues To Action (CUE)	CUE1	If my family were to tell me of a recent experience with an email phishing attack, I would be more conscious of potentially falling victim to an email phishing attack.	[21]
	CUE2	If my friends were to tell me of a recent experience with an email phishing attack, I would be more conscious of potentially falling victim to an email phishing attack.	[21]
	CUE3	If my fellow students were to tell me of a recent experience with an email phishing attack, I would be more conscious of potentially falling victim to an email phishing attack.	[21]
	CUE4	If I saw a news report or awareness poster about phishing, I would be more conscious of potentially falling victim to an email phishing attack.	[21]
	CUE5	If I noticed a suspicious transaction on my bank account, I would be concerned about being a victim of an email phishing attack.	Self-developed
	CUE6	If I noticed suspicious log-in attempts on my social media account(s), I would be concerned about being a victim of an email phishing attack.	Self-developed
	CUE7	If I noticed suspicious log-in attempts on my webshop account(s), I would be concerned about being a victim of an email phishing attack.	Self-developed

Perceived Importance (IMP)	IMP1	Taking action to prevent email phishing attacks is important for me.	[19]
	IMP2	Exercising care when reading emails with links is important for me.	Self-developed
	IMP3	Educating myself about email phishing attacks is important for me.	Self-developed
	IMP4	Using tools to prevent email phishing attacks is important for me.	Self-developed
	IMP5	Staying alert for email phishing is important for me.	Self-developed
	IMP6	Having conversations about phishing prevention is important for me.	Self-developed

B. Table. Exploratory Factor Analysis: factor loadings of all HBM constructs

	Factor 1	Factor 2	Factor 3	Factor 4	Factor 5	Factor 6	Factor 7	Factor 8
BEH1	-0,345	0,172	**0,621**	0,039	-0,375	0,054	0,025	0,150
BEH2	-0,332	0,132	**0,580**	0,039	-0,301	0,086	0,033	0,008
BEH3	-0,272	0,422	**0,499**	-0,122	-0,215	0,114	0,008	-0,031
BEH4	-0,276	0,129	**0,578**	0,124	-0,116	-0,008	0,235	0,062
SUS1	**0,774**	0,059	-0,111	-0,077	0,118	-0,104	0,080	-0,137
SUS2	0,256	0,150	-0,119	-0,086	0,194	-0,190	0,218	-0,332
SUS3	0,088	0,270	0,292	0,153	0,087	-0,232	0,037	0,011
SUS4	**0,616**	0,288	0,138	0,036	0,277	-0,131	0,069	-0,211
SUS5	**0,519**	**0,452**	0,118	0,006	0,172	-0,199	0,031	-0,293
SEV2	0,129	0,110	0,381	0,348	0,074	0,016	0,118	-0,051
SEV3	-0,114	0,230	0,300	-0,074	0,057	0,178	0,033	-0,033
SEV4	0,045	0,098	**0,645**	0,041	0,080	0,210	0,054	-0,121
SEV5	0,053	-0,105	**0,500**	0,222	0,197	0,307	-0,059	0,099
BEN1	-0,138	0,159	0,194	0,080	-0,109	**0,747**	0,090	0,195
BEN2	-0,253	0,116	0,174	0,040	-0,157	**0,758**	0,062	0,079
BEN3	-0,028	**0,490**	0,273	-0,028	-0,123	**0,624**	-0,008	0,157
BEN4	-0,257	0,313	0,125	0,224	0,108	0,275	0,175	0,225
BEN5	-0,066	0,255	0,269	-0,100	0,177	0,211	0,144	0,290
BEN6	-0,128	0,174	0,006	0,017	0,057	0,310	-0,121	**0,504**
BEN7	0,171	0,182	-0,118	-0,031	-0,016	0,053	0,152	**0,784**
BEN8	0,127	0,160	0,048	0,020	-0,059	0,090	0,003	**0,712**
BEN9	-0,152	0,429	-0,039	0,140	-0,036	-0,208	0,076	0,418
BAR1	0,160	-0,080	-0,011	-0,029	**0,574**	-0,165	-0,033	0,060
BAR2	-0,009	-0,088	-0,054	-0,003	**0,784**	0,062	0,103	-0,204
BAR3	0,191	-0,002	0,028	0,044	**0,720**	-0,090	0,101	0,011
BAR4	0,372	-0,009	-0,206	-0,110	**0,612**	-0,123	0,012	0,151
BAR5	**0,726**	-0,240	-0,102	0,057	0,032	-0,025	0,025	0,083
BAR6	**0,626**	-0,357	0,103	0,080	0,182	0,173	0,092	-0,268
BAR7	**0,836**	-0,105	-0,005	0,122	0,084	-0,050	-0,050	0,096
BAR8	**0,788**	0,059	0,026	0,059	0,160	-0,119	-0,156	0,031
BAR9	**0,459**	-0,501	-0,071	0,156	0,136	0,212	-0,098	-0,113
BAR10	0,127	-0,158	0,133	-0,085	0,262	0,109	-0,090	-0,189
SEF1	**-0,792**	0,097	0,158	0,004	-0,134	0,120	0,178	0,036
SEF2	**-0,787**	0,065	0,188	-0,093	-0,162	0,187	0,104	-0,021
SEF3	**-0,523**	0,223	0,199	-0,137	-0,040	0,055	-0,015	-0,194
SEF4	**-0,758**	0,184	0,090	-0,209	0,063	0,015	-0,002	-0,072
CUE1	0,137	0,201	0,178	**0,853**	-0,025	-0,067	0,081	0,070
CUE2	0,138	0,155	0,078	**0,885**	-0,037	0,017	0,107	0,008
CUE3	0,153	0,126	-0,029	**0,819**	-0,079	0,132	0,002	0,028
CUE4	-0,221	**0,508**	0,148	0,203	-0,064	-0,049	0,253	0,344
CUE5	-0,037	0,026	-0,034	0,051	0,081	0,034	**0,706**	0,076
CUE6	-0,045	0,063	0,191	0,131	0,018	0,049	**0,880**	0,022
CUE7	-0,078	0,094	0,143	0,029	0,015	0,023	**0,942**	-0,045
IMP1	-0,040	**0,731**	0,155	0,158	-0,098	0,059	0,112	0,172
IMP2	-0,180	**0,563**	0,407	0,158	-0,241	0,326	0,131	-0,058
IMP3	-0,137	**0,690**	0,114	0,157	-0,046	0,273	-0,033	0,144
IMP4	0,019	**0,670**	0,000	0,158	0,027	0,222	-0,116	0,330
IMP5	-0,316	**0,462**	0,222	-0,029	-0,188	0,374	-0,017	-0,033
IMP6	-0,035	**0,668**	0,110	0,134	-0,050	0,100	0,081	0,056