Confirmatory Factor Analysis of Phishing Susceptibility in Indonesia

Harris Simaremare[1], Muhammad Fikri[2], Zarina Shukur[3]
Electrical Engineering, Universitas Islam Negeri Sultan Syarif Kasim, Riau, Indonesia[1]
Informatics Engineering, Universitas Islam Negeri Sultan Syarif Kasim, Riau, Indonesia[2]
Center for Cyber Security (CYBER), Universiti Kebangsaan Malaysia, Malaysia[3]

***Abstract*—This study analyzes phishing susceptibility among Indonesian internet users through Confirmatory Factor Analysis (CFA) and covariance-based Structural Equation Modeling (SEM). The latent factors examined include perceived severity of the threat (PST), perceived barriers (PBR), perceived benefits (PBN), self-efficacy (SE), past success in detection (PSD), and phishing desensitization (PD), with phishing susceptibility (PS) as the dependent variable, derived from survey data of 150 respondents who had encountered phishing attacks. CFA results indicate a good model fit (RMSEA=0.064, CFI=0.92, etc.), while tests of six hypotheses reveal no significant positive correlations between these factors and PS. These findings challenge prior literature assumptions and underscore the need for mediating factors such as digital literacy or cultural norms to mitigate phishing vulnerability in Indonesia, offering implications for internet service providers and government policy.**

***Keywords*—Confirmatory Factor Analysis; cybersecurity awareness; Structural Equation Modeling; phishing susceptibility**

I. Introduction

Indonesia's rapid digital transformation has significantly fueled economic growth, especially in e-commerce. Public connectivity with various online platforms continues to rise. However, varying levels of cybersecurity awareness have resulted in increased vulnerability to cyber threats, especially phishing attacks.

Indonesia, one of Southeast Asia's largest digital economies, recorded over 212 million internet users in 2023, with 73% conducting online financial transactions. Despite this growth, cybersecurity measures have not kept pace, leaving users vulnerable to increasingly sophisticated phishing attacks. The National Cyber and Crypto Agency (BSSN) reported a 35% increase in reported phishing incidents in 2023, primarily targeting banking, e-commerce, and government services sectors. These attacks exploit gaps in user awareness, weak technological infrastructure, and limited regulatory oversight. According to the Indonesian Internet Service Providers Association (APJII), 65% of users are unaware of standard security protocols, making them susceptible to fake links and data theft.

Phishing attacks rely on social engineering, a manipulation technique that exploits human traits such as trust, fear, or curiosity, to obtain sensitive information or perform harmful actions. Attackers often send convincing emails or messages that appear to come from trusted sources –banks, government agencies, or acquaintances. These messages typically contain links or attachments leading to fake websites or malware. Common attack variants include spear phishing, which targets specific individuals or organizations using personalized details; whaling, which focuses on high-profile figures such as executives or officials; smishing, which is delivered via SMS; and pharming, which redirects users to fake websites without their knowledge. Phishing in Indonesia has evolved from generic email scams to highly localized social engineering tactics. Attackers exploit Indonesia's cultural and linguistic diversity, crafting messages that mimic trusted entities such as banks (e.g., Bank Central Asia), e-commerce platforms (e.g., Tokopedia, Shopee), and government agencies. For example, in early 2024, a phishing campaign posing as the Directorate General of Taxes stole the personal data of more than 5,000 taxpayers. The Indonesian Internet Service Providers Association (APJII) reports that 58% of users cannot distinguish real from fake URLs, while 42% reuse passwords across platforms, increasing credential theft risk.

Social engineering tactics, such as pretexting and baiting, thrive on Indonesians' high social media engagement – 160 million active users. A 2023 Kaspersky study found that 68% of phishing attacks in Indonesia originate from malicious links on WhatsApp and Instagram, often disguised as promotional offers or urgent notifications.

Recent studies highlight multiple factors driving phishing in Indonesia. The digital literacy gap between urban and rural populations influences the adoption of digital security practices, including two-factor authentication and robust password management [1]. Security design flaws in digital platforms remain a concern, particularly in the adoption of multi-factor authentication (MFA) across online services [2]. Cultural collectivism may increase susceptibility to phishing by reinforcing trust and compliance with requests perceived as beneficial to the group [3].

Confirmatory Factor Analysis (CFA) has emerged at the international level as a critical tool for modeling cybersecurity vulnerability. For example, studies on information security vulnerability awareness have used CFA to validate multi-criteria models of organizational awareness and control [4]. Similarly, CFA has been applied in cybersecurity risk research to test latent constructs such as vulnerability and control, demonstrating its usefulness in measuring security-related phenomena [5]. In behavioral cybersecurity research, CFA has also supported the validation of models explaining phishing-related security behavior among university students, further showing its value

for examining the psychological and organizational dimensions of cyber vulnerability [6]. An adapted Health Belief Model (HBM) study using CFA and Covariance-Based Structural Equation Modeling (CB-SEM) found that perceived severity and self-efficacy significantly predicted security behavior against email phishing attacks among Indonesian university students [6]. Despite these advances, no studies have adapted CFA to analyze Indonesia's unique socio-technical context, where cultural norms and infrastructure limitations intersect.

Most phishing research focuses on evaluation, detection, and technical prevention tools, such as anti-phishing browser toolbars, website security verification, firewalls, and antivirus software. However, these tools only block known attack patterns. As fraud tactics evolve, technical defenses lag behind. In [7], the authors argue that technology alone cannot overcome social engineering attacks, which exploit human behavior rather than system flaws.

Effective prevention must start from the victim's perspective. Raising user awareness and strengthening organizational policies are critical to heading off phishing attacks before they occur. In [8], the authors note that social engineering attacks often succeed due to user-related security breaches, making it essential to evaluate individual vulnerability [9]. Experimental studies have explored user susceptibility [9], [10], [11], but controlled experiments cannot fully replicate real-world attacks. Research should focus on users who have experienced or are able to identify phishing attacks.

This study adopts a quantitative approach to examine user vulnerability to phishing in Indonesia. Key parameters measured to determine the level of vulnerability include phishing desensitization (PD), past success in detection (PSD), perceived severity of the threat (PST), perceived benefits (PBN), self-efficacy (SE), perceived barriers (PBR), and phishing susceptibility (PS). Findings will inform preventive strategies for internet service providers, government agencies, and related organizations to reduce phishing risks.

II. Related Work

This section reviews prior empirical and theoretical work that motivates the research model and hypotheses. The literature is organized around the theoretical foundation (Health Belief Model), the constructs of interest, and existing evidence on phishing susceptibility measurement.

A. Theoretical Foundation: Health Belief Model

The Health Belief Model (HBM), originally developed in the field of public health, has been widely adapted to explain cybersecurity-related behavior. The HBM posits that individuals' likelihood of taking protective action is determined by their perceived severity of a threat, perceived susceptibility, perceived benefits of action, perceived barriers to action, and self-efficacy [6]. In the cybersecurity domain, Gwenhure [6] demonstrated that HBM constructs (particularly perceived severity and self-efficacy) significantly predicted security behavior against email phishing attacks among university students in an African context. Adane and Beyene [24] similarly applied HBM to examine online users' security behavior in phishing contexts, finding that perceived barriers significantly influence security behavior. Alturki et al. [10] extended HBM constructs to social gaming networks, identifying perceived threat severity, perceived barriers, perceived benefits, and self-efficacy as influencing factors in social engineering susceptibility. The current study adapts these constructs to the Indonesian context.

B. Phishing Susceptibility and Psychological Constructs

Phishing susceptibility refers to an individual's likelihood of being deceived by a phishing attack. Chen, Gaia, and Rao [11] established that past phishing encounters (including past success in detection and phishing desensitization) are significant predictors of susceptibility. Baki and Verma [18] conducted a systematic review of sixteen years of phishing user studies and identified perceived vulnerability and severity as relevant constructs, though without establishing direct links to susceptibility. Ribeiro, Guedes, and Cardoso [16] found in an empirical study that self-confidence in phishing detection may paradoxically increase susceptibility, while Lee, Gan, and Liew [15] demonstrated that high self-efficacy combined with a negative attitude toward online sharing significantly predicted susceptibility in instant messaging contexts. Halevi, Lewis, and Memon [12] and Tjostheim and Waterworth [13] further connected perceived benefits of information sharing with increased phishing vulnerability.

C. CFA in Cybersecurity Research

Confirmatory Factor Analysis has been employed extensively to validate latent construct measurement in cybersecurity research. Mejias et al. [4] used CFA to validate a multi-criteria model of information security vulnerability awareness in organizational settings. Rohan et al. [5] conducted a systematic literature review of cybersecurity scales and identified CFA as the dominant method for assessing construct validity in security awareness instruments. In the Indonesian context specifically, Gwenhure [6] employed CB-SEM to test a structural model of security behavior against phishing, providing the closest precedent for the current study. However, no prior work has applied CB-SEM to a sample of Indonesian internet users who have directly experienced phishing attacks, which is the distinctive contribution of the current study.

D. Gaps in the Existing Literature

Despite substantial prior literature, several gaps remain. First, most existing studies were conducted in Western or academic settings, limiting generalizability to Indonesia's diverse socio-cultural context. Second, the direct causal relationships between the selected HBM constructs and phishing susceptibility have not been simultaneously tested in a CB-SEM framework among Indonesian general internet users. Third, the role of contextual and cultural moderators (such as digital literacy gaps between urban and rural populations and collectivist cultural norms) has not been empirically integrated into structural models of phishing susceptibility. The present study addresses these gaps by testing all six constructs simultaneously in the Indonesian context using CB-SEM, with awareness that contextual factors may mediate or moderate the hypothesized relationships.

III. Methods

This study employed a quantitative approach using covariance-based Structural Equation Modeling (SEM) to test

relationships among latent variables influencing phishing susceptibility (PS). This design was chosen because it allows for simultaneous testing of theoretical models and assessment of overall model fit.

The research questionnaire was distributed to 150 respondents in Indonesia. The sampling technique used was purposive, with the inclusion criteria being age > 18 years and prior experience with phishing attacks. Data collection was conducted offline; respondents provided informed consent before completing the questionnaire.

The independent latent variables in this study were perceived severity of the threat (PST), perceived barriers (PBR), perceived benefits (PBN), self-efficacy (SE), past success in detection (PSD), phishing desensitization (PD), and the dependent variable was phishing susceptibility (PS). The instrument was a closed questionnaire using a 6-point Likert scale (1 = Strongly Disagree, 6 = Strongly Agree).

Construct validity was tested via Confirmatory Factor Analysis (CFA), and reliability was tested using Cronbach's Alpha (threshold ≥ 0.70). The proposed SEM model will be assessed using 19 cut-off values, namely SRMR (Standardized RMR), AGFI (Adjusted Goodness of Fit Index), ECVI (Expected Cross-Validation Index), AIC (Akaike's Information Criterion), PGFI (Parsimony Goodness of Fit Index), CAIC (Consistent Akaike's Information Criterion), IFI (Incremental Fit Index), NFI (Normed Fit) Index), RFI (Relative Fit Index), TLI/NNFI (Non-Normed Fit Index), NCP (Non-centrality Parameter), PNFI (Parsimony Normed Fit Index), RMR (Root Mean Square Residual), CMIN/Df, GFI (Goodness of Fit Index), Chi-square, CN (Critical N), CFI (Comparative Fit Index), and RMSEA (Root Mean Square Error of Approximation).

IV. PROPOSED MODEL

This study proposes a model to evaluate factors influencing phishing awareness and vulnerability among Indonesian users. While some studies have evaluated phishing through experiments or simulations, these approaches often produce context-specific results that cannot be generalized. Instead, this research focuses on user experiences and perceptions when faced with phishing attacks, which provide a broader understanding of real-world vulnerability.

Phishing attacks evolve rapidly based on target profiles. Experimental studies, such as controlled phishing simulations, capture only a subset of attack patterns. Consequently, findings from these studies may not reflect actual user behavior in diverse contexts. To address this gap, we drew on research evaluating user experiences with social engineering attacks, including [10] on social gaming networks and [11] on phishing email detection.

Fig. 1 illustrates the proposed model, which hypothesizes relationships between these constructs and phishing susceptibility. The model aims to identify latent factors that influence vulnerability and inform preventative strategies for Indonesian users.

The proposed model integrates factors identified in prior studies, adapted for Indonesia's socio-technical context. In [10], the authors identified the following factors: perceived threat severity, perceived barriers, perceived benefits, self-efficacy, competition, cooperation, and influence vulnerability to social engineering attacks, especially in social gaming networks. In [11], the authors stated that past success in detection and phishing desensitization influences social engineering attacks, namely phishing emails. Table I shows the details of the constructs and variables that will be used in this study.

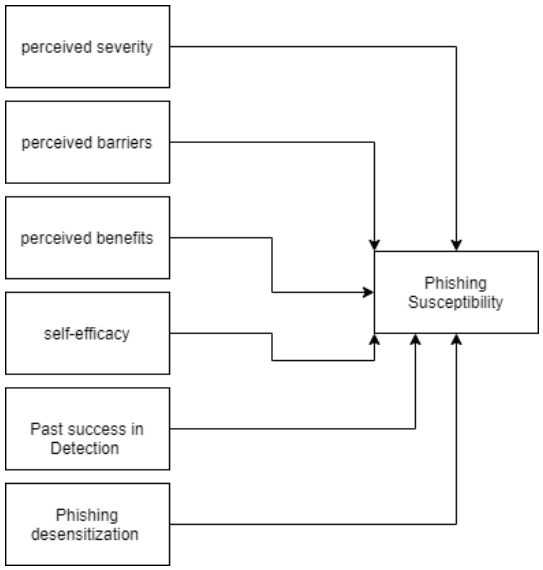

Fig. 1. Proposed model

Based on the literature review, this study proposes six hypotheses examining the relationship between phishing susceptibility (PS) and other identified factors:

A. H1: Phishing Susceptibility (PS) is Positively Correlated with Perceived Severity of the Threat (PST)

Research suggests that cyberattack warning messages are more credible when aligned with users' perceived severity (Jones et al., 2022). Baki & Verma (2023) identified perceived vulnerability and severity as influencing security behavior related to phishing attacks, but did not establish a direct link between the two factors. Therefore, further research is needed to confirm whether higher perceived severity increases phishing susceptibility.

B. H2: Phishing Susceptibility (PS) is Positively Correlated with Perceived Barriers (PBR)

Adane & Beyene (2023) found that perceived barriers significantly affect user security behavior in phishing contexts, using the Health Belief Model. This suggests that higher perceived barriers may increase susceptibility to phishing attacks. However, empirical evidence on the direct correlation between perceived barriers and phishing susceptibility remains limited. This study aims to demonstrate this link for a sample population that has experienced a phishing attack.

TABLE I. RESEARCH VARIABLES

Construct	Variable	Adapted from authors
perceived severity of the threat (PST)	Q1: Social engineering poses a risk to my safety and well-being at work.	[10]
	Q2: If I was a victim of social engineering while using email or SMS, it would be a serious issue.	
	Q3: When I consider social engineering attacks by email or SMS, I get melancholy.	
	Q4: Even considering the possibility of social engineering when utilizing SMS or email scares me.	
perceived barriers (PBR)	Q5: Taking care of myself would alter how I use the computer	[10]
	Q6: The time and effort required to use specialized software for security	
	Q7: Using SMS and email with caution makes me uneasy.	
	Q8: Using SMS or email carelessly is inconvenient.	
perceived benefits (PBN)	Q9: Being conscious of social engineering when using SMS and email keeps me safe from attacks.	[10]
	Q10: Investing in security software is a great way to lessen my exposure to social engineering attacks.	
	Q11: A social engineering attack is avoided by exercising caution.	
self-efficacy (SE)	Q12: I am generally safe from dangers of social engineering.	[10]
	Q13: I am aware of how to protect myself from social engineering scams.	
	Q14: It is simple to take the required security precautions to thwart social engineering attempts via email or SMS.	
past success in detection (PSD)	Q15: I have been effective at thwarting phishing attempts.	[11]
	Q16: The majority of the phishing attacks I had come across in the past had been repelled.	
	Q17: In the past, I was able to recognize phishing attempts and avoid falling for them.	
phishing desensitization (PD)	Q18: I shrug in response to news reports containing phishing stories.	[11]
	Q19: I ignore news reports about phishing scams.	
phishing susceptibility (PS)	Q20: I run the danger of falling prey to phishing scams.	[11]
	Q21: I am sure I will fall prey to phishing scams.	
	Q22: I could fall prey to phishing scams.	
	Q23: My likelihood of being phished is quite high.	
	Q24: Phishing emails are probably going to trick me.	

C. H3: Phishing Susceptibility (PS) is Positively Correlated with Perceived Benefits (PBN)

Individuals who perceive benefits in sharing personal information (e.g., through social media or phishing emails that offer rewards) may be more susceptible to phishing attacks [12], [13]. Additionally, if individuals perceive significant benefits in interacting with protective measures, their vulnerability may decrease [13], [14]. While these studies imply a relationship between perceived benefits in online behavior and phishing susceptibility, direct evidence linking the two factors is scarce, warranting further investigation.

D. H4: Phishing Susceptibility (PS) is Positively Correlated with Self-Efficacy (SE)

Several studies suggest that high self-confidence can increase susceptibility to phishing attacks. A study on instant messaging phishing found that higher self-efficacy and a negative attitude toward sharing personal information online significantly predicted phishing susceptibility [15]. Another study showed that individuals who considered themselves highly confident in detecting phishing attacks were more susceptible to phishing attacks [16]. This hypothesis tests whether self-efficacy has a positive correlation with phishing susceptibility.

E. H5: Phishing Susceptibility (PS) is Positively Correlated with Past Success in Detection (PSD)

Previous success in detecting phishing may influence susceptibility [11]. While experience and training can improve detection, they may also lead to false alarms and complacency [17]. Conversely, other studies have found that experience and knowledge can improve detection abilities and potentially reduce vulnerability [11], [17], [18], [19]. Given these mixed conclusions, this study examines whether past success in detection corresponds positively with phishing susceptibility.

F. H6: Phishing Susceptibility (PS) is Positively Correlated with Phishing Desensitization (PD)

Phishing desensitization refers to the reduction in a person's sensitivity after repeated exposure to phishing. In [20], the authors found that desensitization moderates the impact of recent phishing experiences, along with factors such as prior detection success. In [11], the authors also identified desensitization as a personal attribute influencing susceptibility. Furthermore, repeated exposure can weaken training effects and increase vulnerability [21]. Overall, studies suggest that

individuals who become desensitized to phishing attacks are more likely to fall victim. Based on the research above, this study hypothesizes a positive correlation between phishing desensitization and phishing susceptibility.

V. Results and Analysis

A. Pilot Analysis

The questionnaire was tested with 29 randomly selected respondents in Indonesia (Pekanbaru City, Riau Province).

Next, the validity of these 29 responses was tested using statistical analysis with SPSS. The following are the results of the data description for all questions. Table II presents the descriptive statistics.

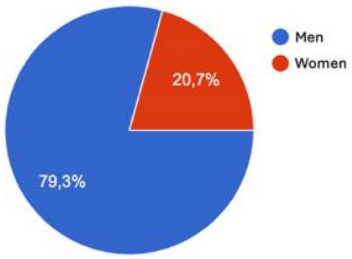

Fig. 2. Respondent demographics

TABLE II. Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation	Variance	Skewness		Kurtosis	
	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Q1	29	2	6	4.69	1.105	1.222	-1.031	.434	.799	.845
Q2	29	3	6	5.28	.841	.707	-.967	.434	.311	.845
Q3	29	1	6	4.66	1.203	1.448	-.987	.434	1.477	.845
Q4	29	1	6	4.62	1.237	1.530	-1.393	.434	2.121	.845
Q5	29	1	6	4.59	1.268	1.608	-1.280	.434	1.548	.845
Q6	29	2	6	4.48	.871	.759	-.814	.434	1.249	.845
Q7	29	1	6	3.55	1.378	1.899	-.599	.434	-.351	.845
Q8	29	1	6	4.45	1.298	1.685	-.825	.434	.319	.845
Q9	29	3	6	5.14	.789	.623	-.725	.434	.425	.845
Q10	29	1	6	4.24	1.215	1.475	-.756	.434	.850	.845
Q11	29	2	6	5.14	.915	.837	-1.491	.434	3.576	.845
Q12	29	1	6	4.31	1.285	1.650	-.740	.434	.368	.845
Q13	29	1	6	4.72	1.066	1.135	-1.493	.434	4.180	.845
Q14	29	1	6	4.31	1.168	1.365	-.660	.434	.755	.845
Q15	29	2	6	4.31	1.105	1.222	-.162	.434	-.858	.845
Q16	29	3	6	4.62	.728	.530	.145	.434	-.224	.845
Q17	29	2	6	4.52	.986	.973	-.531	.434	.235	.845
Q18	29	2	6	4.14	.990	.980	-.531	.434	-.206	.845
Q19	29	1	6	3.14	1.529	2.337	.460	.434	-.638	.845
Q20	29	1	6	3.41	1.547	2.394	-.200	.434	-.955	.845
Q21	29	1	6	3.55	1.404	1.970	-.280	.434	-.556	.845
Q22	29	1	6	3.86	1.156	1.337	-.903	.434	1.144	.845
Q23	29	1	6	3.55	1.378	1.899	-.072	.434	-.147	.845
Q24	29	1	6	3.55	1.549	2.399	.082	.434	-1.096	.845
Valid N	29									

The description of the data above shows that the skewness values are within the normal range for each question. The values range between -1 and 0, indicating that the questionnaire results are normally distributed.

1) Reliability testing: Reliability testing is used to determine the extent to which questionnaire produces consistent results when administered to the same respondents. The test was conducted using Cronbach's Alpha in SPSS. The results are as follows (see Table III):

TABLE III. Reliability Statistics

Cronbach's Alpha	N of Items
.819	24

Based on the above results, the total alpha value is 0.819. This value is greater than the critical r-value for N=24, which is 0.404. This indicates that all items in the questionnaire are reliable and that the overall test demonstrates strong internal consistency.

2) Validity testing: Validity testing was conducted to determine the extent to which the questions measure the intended constructs. Validity testing in SPSS used Pearson's bivariate correlation. Pearson's correlation analysis compared each question item score with the total score. The results are as follows (see Table IV to Table X):

a) Validity of Perceived Severity of the Threat (PST) Construct

The PST construct was measured using four items:

- Q1: Social engineering poses a risk to my safety and well-being at work.
- Q2: If I were a victim of social engineering while using email or SMS, it would be a serious issue.
- Q3: When I consider social engineering attacks by email or SMS, I get melancholy.
- Q4: Even considering the possibility of social engineering when utilizing SMS or email scares me.

TABLE IV. CORRELATION RESULTS FOR PST

		Q1	Q2	Q3.	Q4
SUM_PST	Pearson Correlation	.758**	.615**	.784**	.940**
	Sig. (2-tailed)	.000	.000	.000	.000
	N	29	29	29	29

For a significance level of alpha = 5% with N = 29, the critical r-value is 0.367. The validity test results show that the r-values for Q1 to Q4 are greater than 0.367, indicating that all PST construct questions are valid at the 5% significance level.

b) Validity of Perceived Barriers (PBR) Construct

The PBR construct was measured using four items:

- Q5: Taking care of myself would alter how I use the computer.
- Q6: The time and effort required to use specialized software for security.
- Q7: Using SMS and email with caution makes me uneasy.
- Q8: Using SMS or email carelessly is inconvenient.

TABLE V. CORRELATION RESULTS FOR PBR

		Q5	**Q5.**	**Q7**	**Q8**
SUM_PBR	Pearson Correlation	.598**	.825**	.682**	.742**
	Sig. (2-tailed)	.001	.000	.000	.000
	N	29	29	29	29
**. Correlation is significant at the 0.01 level (2-tailed).					

All correlation coefficients (r-values) for Q5 to Q8 exceed the critical value of 0.367, indicating that each item in the PBR construct is valid.

c) Validity of Perceived Benefits (PBN) Construct

The PBN construct was measured using three items:

- Q9: Awareness of social engineering techniques when using SMS and email keeps me safe from attacks.
- Q10: Investing in security software is a good way to reduce my exposure to social engineering attacks
- Q11: Social engineering attacks can be avoided by being careful.

TABLE VI. CORRELATION RESULTS FOR PBN

		Q9	**Q10**	**Q11**
SUM_PBN	Pearson Correlation	.693**	.815**	.739**
	Sig. (2-tailed)	.000	.000	.000
	N	29	29	29

All r-values for Q9 to Q11 are above 0.367, confirming that the PBN construct items are valid.

d) Validity of Self-Efficacy (SE) Construct

Since all r-values exceed the threshold of 0.367, the SE construct items are considered valid.

TABLE VII. CORRELATION RESULTS FOR SE

		Q12	**Q13**	**Q14**
SUM_SE	Pearson Correlation	.778**	.723**	.776**
	Sig. (2-tailed)	.000	.000	.000
	N	29	29	29

The SE construct was assessed using three items:

- Q12: I am generally safe from the dangers of social engineering (Q12).
- Q13: I am aware of how to protect myself from social engineering scams.
- Q14: It is simple to take the required security precautions to thwart social engineering attempts via email or SMS.

e) Validity of Past Success in Detection (PSD) Construct

The PSD construct includes 3 items:

- Q15: I've been effective at thwarting phishing attempts.
- Q16: The majority of the phishing attacks I had come across in the past had been repelled.
- Q17: In the past, I was able to recognize phishing attempts and avoid falling for them.

All r-values for Q15 to Q15 are above the critical value of 0.367, indicating that the PSD construct items are valid.

TABLE VIII. CORRELATION RESULTS FOR PSD

		Q15	**Q16**	**Q17**
SUM_PSD	Pearson Correlation	.852**	.736**	.730**
	Sig. (2-tailed)	.000	.000	.000
	N	29	29	29

f) Validity of Phishing Desensitization (PD) Construct

The PD construct was measured using two items:

- Q18: I shrug in response to news reports containing phishing stories.

- Q19: I ignore news reports about phishing scams.

TABLE IX. CORRELATION RESULTS FOR PD

		Q18	Q19
SUM_PD	Pearson Correlation	.666**	.876**
	Sig. (2-tailed)	.000	.000
	N	29	29

All r-values for Q18 and Q19 exceed the critical threshold of 0.367, confirming that the PD construct items are valid.

g) Validity of Phishing Susceptibility (PS) Construct

The PS construct consists of five items:

- Q20: I run the danger of falling prey to phishing scams.
- Q21: I'm sure I'll fall prey to phishing scams.
- Q22: I could fall prey to phishing scams.
- Q23: My likelihood of being phished is quite high.
- Q24: Phishing emails are probably going to trick me.

TABLE X. CORRELATION RESULTS FOR PS

		Q20	Q21	Q22	Q23	Q24
SUM_PS	Pearson Correlation	.828**	.816**	.727**	.872**	.840**
	Sig. (2-tailed)	.000	.000	.000	.000	.000
	N	29	29	29	29	29

B. Respondent Data Analysis

The research was conducted by distributing 150 questionnaires to respondents in Indonesia. Respondents were selected randomly, with the primary inclusion criterion being that they had received messages suspected to be phishing attacks. The demographic data collected from the respondents are presented in Fig. 2.

The data indicate that female respondents tend to have longer durations of interaction with information technology compared to their male counterparts.

1) Data reliability and validity testing: Based on the descriptive analysis (see Table XI), all variables were measured using responses from 150 participants. This sample size provides strong representativeness for the study. The highest average scores were observed in the SUM_PST (18.27) and SUM_PBR (18.23) variables, indicating that these two constructs were perceived most positively by respondents. In contrast, SUM_PD had the lowest average score (6.87), indicating a relatively low perception of this factor among respondents. In terms of data distribution, SUM_PS had the highest standard deviation and variance (6.884; 47.395), indicating a wide range of responses and high variability in how respondents assessed their susceptibility. SUM_SE had the lowest standard deviation and variance (2.279; 5.195), suggesting more consistent responses across participants.

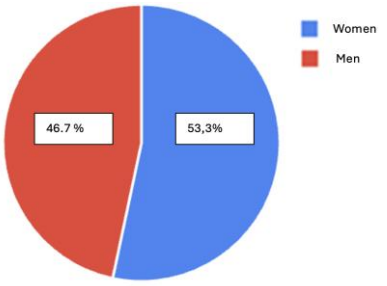

Fig. 3. Gender distribution

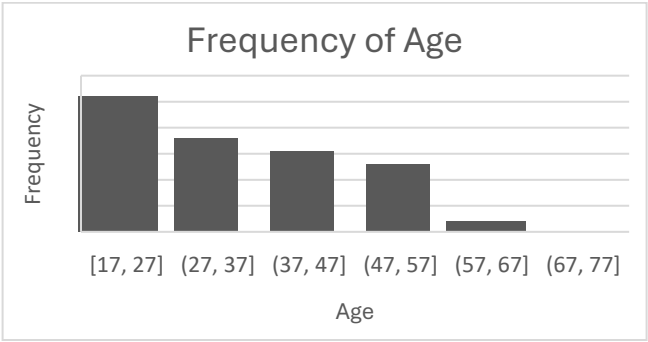

Fig. 4. Age distribution

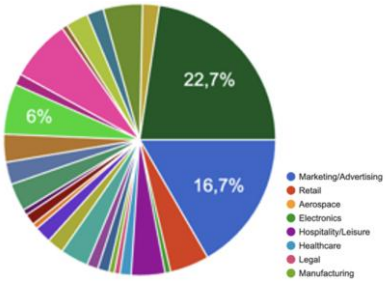

Fig. 5. Occupational background

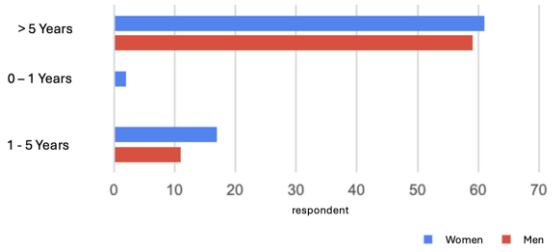

Fig. 6. Duration of interaction with information technology by gender.

Most variables exhibited negative skewness, indicating a tendency toward higher response values, with the exception of SUM_PD and SUM_PS, which had slightly positive skewness, thus approaching a normal distribution. Kurtosis analysis revealed a leptokurtic distribution for SUM_PBN (3.110), meaning responses were tightly clustered around the mean, while SUM_PD and SUM_PS had negative kurtosis, indicating a flatter, more evenly spread distribution. These findings suggest that most constructs were perceived positively with varying levels of consistency. SUM_PST and SUM_PBR emerged as the strongest constructs, based on both average scores and

consistency, while SUM_PD stands out as an area of concern due to its low average and broad variability, indicating a potential gap in user awareness or engagement with phishing-related content. Fig. 3, Fig. 4 and Fig. 5 shows the gender distribution, age distribution, and occupational background. Fig. 6 presents the duration of interaction with information technology by gender.

TABLE XI. DESCRIPTIVE DATA

	N	Range	Min	Max	Sum	Mean		Std. Deviation	Variance	Skewness		Kurtosis	
	Stat	Stat	Stat	Stat	Stat	Stat	Std. Error	Stat	Stat	Stat	Std. Error	Stat	Std. Error
SUM_PST	150	20	4	24	2740	18.27	.390	4.772	22.774	-1.082	.198	.464	.394
SUM_PBR	150	19	5	24	2735	18.23	.306	3.750	14.059	-.846	.198	.861	.394
SUM_PBN	150	14	4	18	2174	14.49	.222	2.719	7.393	-1.558	.198	3.110	.394
SUM_SE	150	10	2	12	1329	8.86	.186	2.279	5.195	-.797	.198	.078	.394
SUM_PSD	150	15	3	18	2064	13.76	.232	2.844	8.090	-1.270	.198	2.181	.394
SUM_PD	150	10	2	12	1030	6.87	.233	2.858	8.170	.094	.198	-1.115	.394
SUM_PS	150	25	5	30	2382	15.88	.562	6.884	47.395	.292	.198	-1.071	.394
Valid N (listwise)	150												

While most constructs show acceptable reliability ($\alpha > 0.6$), PBN and PBR fall slightly below the commonly accepted threshold. These constructs may benefit from refinement in future iterations of the instrument. The following are the reliability test results for each construct (see Table XII):

TABLE XII. CRONBACH'S ALPHA BY CONSTRUCT

Construct	Cronbach's Alpha
PST	0.805
PS	0.899
PBN	0.556
SE	0.673
PSD	0.718
PD	0.684
PBR	0.546

2) Validity analysis: Validity was assessed using Pearson's correlation between each item and its corresponding total construct score (SUM). All items demonstrated statistically significant correlations at a significance level of 0.000 ($p < 0.01$), confirming their validity. In the PST construct (Q1–Q4), correlations ranged from 0.729 to 0.851, indicating strong internal consistency. The PBR construct (Q5–Q8) had correlations ranging from 0.595 to 0.707; although Q6 had the lowest value (0.595), this value was still above the acceptable minimum (0.3–0.5) and was therefore still considered valid.

The PBN construct (Q9–Q11) demonstrated a high correlation of 0.622–0.779, showing strong alignment between items and the construct. The SE construct (Q12–Q14) had a very high correlation, especially Q12 (0.896), but Q14 showed the lowest correlation (0.499), which is still considered valid. The PSD construct (Q15–Q17) had a correlation range of 0.749–0.836, which consistently shows strong validity. The PD construct (Q18–Q19) showed near-perfect correlations of 0.870 and 0.874, respectively. Meanwhile, the PS construct (Q20–Q24) had consistently very high correlations (0.773–0.880), indicating that all items were highly representative of the construct.

The reliability and validity analysis confirm that the questionnaire is a robust instrument for measuring phishing susceptibility and related constructs. While a few items show relatively lower reliability or correlation values, they remain within acceptable limits. Overall, the instrument demonstrates strong psychometric properties and is suitable for further analysis and application.

C. Analysis of Indonesian Respondent Data

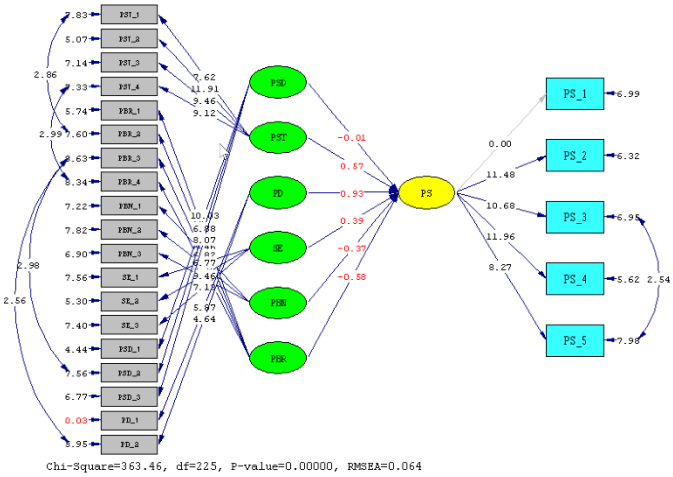

Fig. 7. Path diagram of Confirmatory Factor Analysis (CFA) results.

Based on the results of Confirmatory Factor Analysis (CFA) conducted using the path diagram (see Fig. 7), the model yielded a Chi-Square value of 363.46 with Degrees of Freedom (df) = 225 and p-value = 0.000. The RMSEA value of 0.064 is below the commonly accepted threshold of 0.08, indicating that the model demonstrates a good level of fit.

TABLE XIII. HYPOTHESES AND RESULTS

Hypothesis	Description	Result
H1	Phishing susceptibility (PS) is positively correlated with perceived severity of the threat (PST).	Not Supported
H2	Phishing susceptibility (PS) is positively correlated with perceived barriers (PBR).	Not Supported
H3	Phishing susceptibility (PS) is positively correlated with perceived benefits (PBN).	Not Supported
H4	Phishing susceptibility (PS) is positively correlated with self-efficacy (SE).	Not Supported
H5	Phishing susceptibility (PS) positively correlates with past success in detection (PSD).	Not Supported
H6	Phishing susceptibility (PS) positively correlates with phishing desensitization (PD).	Not Supported

This study proposed six hypotheses (H1–H6), each predicting a positive correlation between phishing susceptibility (PS) and six different psychological/perceptual variables: perceived severity (PST), perceived barriers (PBR), perceived benefit (PBN), self-efficacy (SE), past success in detection (PSD), and phishing desensitization (PD) (see Table XIII). Although prior literature provided theoretical and empirical support for these relationships, the results of hypothesis testing indicate that none of the proposed correlations were statistically significant (Not Supported). A comparison of each hypothesis and the results is described below:

1) H1: phishing susceptibility (PS) ↔ perceived severity of the threat (PST): Previous studies [18], [22] suggest that cyber warning messages are more effective when the perceived severity of the consequences aligns with the users' own perceptions. Perceived severity is recognized as a determinant of security behavior, although [18] do not explicitly link PST with PS. This study hypothesized a positive correlation between PST and PS. However, the results show no significant relationship between the two. This suggests that while users may perceive phishing threats as serious, this perception does not necessarily translate into safer behavior – such as avoiding risky email interactions. These findings support [23], who argue that risk perception does not always predict security-related decision-making.

2) H2: phishing susceptibility (PS) ↔ perceived barriers (PBR): In [24], the authors assert that perceived barriers significantly influence security behavior. The assumption is that higher barriers (e.g., time, effort, or complexity) may discourage users from adopting protection measures, thereby increasing susceptibility. However, this study found no significant correlation between PBR and PS. This discrepancy may indicate that perceived barriers affect technology adoption (e.g., multi-factor authentication), more than they influence phishing vulnerability directly.

3) H3: phishing susceptibility (PS) ↔ perceived benefits (PBN): In [12], [13], the authors argue that individuals who perceive benefits in sharing personal information tend to be more vulnerable to phishing. In [14], the authors also show that perceived benefits in protective measures can also influence phishing avoidance behavior. Despite this, the current study found no significant correlation between PBN and PS. These results suggest that perceived benefits from online behavior do not automatically increase vulnerability. Moderating factors such as digital literacy or security awareness may play a role. Even if users perceive benefits, high phishing awareness may still lead to cautious behavior.

4) H4: phishing susceptibility (PS) ↔ self-efficacy (SE): The literature [15], [16] suggests that high self-efficacy may lead to overconfidence, increasing phishing risk. However, this study found no significant relationship between SE and PS. This discrepancy may be due to the self-efficacy measured - reflecting actual ability rather than inflated confidence. These findings align with prior research showing that the influence of self-efficacy on security responses depends on domain knowledge and attack context [25].

5) H5: phishing susceptibility (PS) ↔ past detection PSD: In [11] and [17], the authors highlight that past success in phishing detection can influence vulnerability, though it may also lead to false positives. In this study, no significant correlation was found between PSD and PS. This may be due to attacker adaptation—as phishing tactics evolve, past experience may become less relevant. In [19], the authors support this, noting that phishing detection skills can decline when attack strategies change significantly.

6) H6: phishing susceptibility (PS) ↔ phishing desensitization (PD): In [11], [20], [21], the authors suggest that repeated exposure can lead to phishing desensitization, increasing PS. However, this study found no significant relationship between PD and PS. Repeated exposure to security warnings may lead to habituation, characterized by diminished attention and response to the repeated stimulus [26]. In this case, the expected desensitization effect may be neutralized.

Overall, none of the hypotheses (H1–H6) predicting a positive correlation between phishing susceptibility (PS) and the selected psychological or perceptual variables were empirically supported in this study. This outcome contrasts with findings from previous research, which provided both theoretical and partial empirical support for these relationships [11], [12], [13], [15], [16], [17], [18], [19], [21], [22], [24]. These differences may be due to methodological factors (measurement instruments, sample size, and respondent context) or contextual factors (changes in phishing trends, digital literacy, and cybersecurity culture in the research area).

D. Model Evaluation

The results of Structural Equation Modeling (SEM) indicate that the tested model falls within the acceptable fit category, with several indicators confirming overall adequacy and others highlighting areas for improvement (see Table XIV). Goodness-of-fit indices such as RMSEA (0.064 < ideal limit of 0.08), TLI/NNFI (0.91), IFI (0.93), and CFI (0.92) have met the ideal criteria of ≥ 0.90, suggesting that the model represents the data well. Additionally, AIC (513.46), CAIC (814.25), and ECVI (3.45) values are lower than those of the saturated and independence models, indicating that the model is efficient, not overly complex, and has strong generalization potential for other samples. Parsimony indices – PGFI (0.62) and PNFI (0.69) –

also confirm adequate simplicity, while the CMIN/df ratio (1.741) is well below the maximum limit of 3, reflecting a balanced trade-off between complexity and fit.

While the model meets most key criteria, several indicators fall short of ideal thresholds. NFI (0.84) and RFI (0.80) are below the recommended minimum of 0.90, suggesting that the model's relative fit could be improved. AGFI (0.77) is also low, indicating reduced fit when model complexity is considered. The SRMR (0.081) exceeds the ideal threshold of 0.05, implying that the covariance residuals between variables are not yet fully accounted for. Furthermore, the Critical N (CN) value of 106.46, below the recommended 200, suggests that the sample size used may be insufficient to support a model with perfect fit. Although the Chi-square p-value is significant (p = 0.00), rejecting the perfect fit hypothesis, this outcome is common in SEM with large sample sizes due to the test's sensitivity and should not be interpreted in isolation.

Although some indicators fall below ideal thresholds, the model meets most key SEM criteria, particularly incremental fit and parsimony measures, and is considered acceptable for exploratory analysis. To enhance model quality and approach a high-fit classification, it is recommended to review and refine indicators with low loading factors, optimize the measurement model, and apply theoretically justified modifications based on Modification Indices. Expanding the sample size could also increase model stability and improve the CN, AGFI, and SRMR values. With these improvements, this model can achieve stronger statistical and theoretical robustness.

TABLE XIV. MODEL FIT ASSESSMENT FOR THE INDONESIAN PHISHING MODEL

Model Fit Assessment	Cut-off Value	Indonesian Phishing Model	Result
AIC (Akaike's Information Criterion)	<AIC for saturated or Independence	AIC = 513.46 (AIC saturated=600.00; AIC independence =2508.68)	Good
Chi-square or p-value	>0.05	363.46 (P=0.00)	Fair
NFI (Normed Fit) Index)	>0.9	0.84	Fair
RMSEA (Root Mean Square Error of Approximation)	<=0.08	0.064	Good
RFI (Relative Fit Index)	>0.90	0.80	Fair
AGFI (Adjusted Goodness of Fit Index)	>0.90	0.77	Fair
CAIC (Consistent Akaike's Information Criterion)	<CAIC for saturated or Independence	CAIC = 814.25 (CAIC saturated=1803.191; CAIC independence =2604.94)	Good
ECVI (Expected Cross-Validation Index)	<ECVI for saturated or Independence	ECVI = 3.45 (ECVI saturated=4.03; ECVI independence =16.84)	Good
TLI / NNFI (Non-Normed Fit Index)	>=0.90	0.91	Good
IFI (Incremental Fit Index)	>90	0.93	Good
CFI (Comparative Fit Index)	>0.9	0.92	Good
GFI (Goodness of Fit Index)	approaching the value of 1 atau >0.9	0.83	Good
SRMR (Standardized RMR)	<0.05	0.081	Fair
PGFI (Parsimony Goodness of Fit Index)	>0.5	0.62	Good
RMR (Root Mean Square Residual)	approaching the value of 0	0.16	Good
PNFI (Parsimony Normed Fit Index)	>0.5	0.69	Good
CMIN / Df	<=3	1.741	Good
CN (Critical N)	>200	106.46	fair

E. Post-Hoc Statistical Power Analysis

Given that all six hypotheses were not supported, a post-hoc statistical power analysis was conducted to assess whether the null results reflect genuine absence of effects or insufficient statistical power. Using G*Power with the parameters of N = 150, α = 0.05, and effect sizes derived from comparable prior studies (r = 0.15 to r = 0.25, corresponding to small-to-medium effects in social science research), the estimated statistical power (β) ranged from approximately 0.18 to 0.42. These values fall substantially below the conventional threshold of 0.80, indicating that the study was underpowered to reliably detect effects of these magnitudes. This means the probability of a Type II error (failing to detect a true effect) was high. Consequently, the null results should be interpreted with caution: they may reflect genuine absence of relationships in this population, or they may be an artifact of insufficient statistical power. A sample of approximately 264–400 respondents would be required to achieve power ≥ 0.80 for the smallest expected effect sizes. Future research should prioritize larger samples to enable definitive conclusions.

VI. DISCUSSION

A. Interpretation of Null Findings

The rejection of all six hypotheses is a notable and theoretically meaningful outcome that warrants careful interpretation. The null results contrast with findings from foundational studies in the HBM-phishing literature [6][10][11][15][16][24]. At least three classes of explanation are plausible. First, the null results may reflect genuine contextual differences: psychological constructs validated in Western or controlled academic settings may not operate the same way among Indonesian general internet users who encounter real-world phishing. Cultural collectivism [3], differential digital literacy [1], and Indonesia's unique phishing landscape (e.g.,

WhatsApp and Instagram-based attacks [2]) may collectively moderate or suppress the relationships hypothesized by the HBM. Second, as demonstrated by the post-hoc power analysis (Section V E), the sample size of 150 was likely insufficient to detect small-to-medium effects, raising the probability of Type II errors across all six hypotheses. Third, two constructs (PBR, PBN) exhibited sub-threshold reliability (Cronbach's $\alpha < 0.60$), which attenuates structural path estimates and reduces the likelihood of detecting significant relationships even where true effects exist.

B. Comparison with Prior Literature

The present findings diverge from several key prior studies. Gwenhure [6] found that perceived severity and self-efficacy significantly predicted security behavior in an HBM model among university students. Adane and Beyene [24] found that perceived barriers significantly influence phishing-related security behavior. Chen et al. [11] established desensitization and past detection success as predictors of susceptibility. The divergence from these findings may be attributed to differences in sample characteristics (students vs. general population), the operationalization of constructs (the current instruments were adapted from English-language scales without full cross-cultural validation), and the measurement of susceptibility (self-report vs. behavioral measures). Notably, the Indonesian population sampled here consists of individuals who had already encountered phishing attacks, potentially introducing selection bias: those who survived prior attacks may have developed heuristic defenses that render the HBM constructs less predictive.

C. The Role of Unmeasured Mediating and Moderating Variables

A critical observation from this study is that the hypothesized direct effects of HBM constructs on phishing susceptibility were uniformly non-significant. This pattern may indicate that the relationships between these constructs and susceptibility are not direct but are mediated or moderated by variables not included in the current model. Digital literacy is a particularly compelling candidate: individuals with higher digital literacy may translate threat perceptions into protective behaviors more effectively [1], creating a suppressor effect on the direct PST–PS path. Cultural norms (e.g., collectivism, deference to authority) may moderate the extent to which perceived benefits or barriers influence behavior [3]. Attack-specific familiarity (that is, knowledge of the specific phishing tactics prevalent in Indonesia) may also moderate the effectiveness of self-efficacy as a predictor. Future studies should incorporate these variables as explicit mediators or moderators within extended HBM or Protection Motivation Theory frameworks.

D. Methodological Limitations and Recommendations

Several methodological limitations of this study should be acknowledged. The sample size of 150 respondents was insufficient for CB-SEM to achieve adequate statistical power for the hypothesized effect sizes, and the CN value of 106.46 confirmed this. The sub-threshold reliability of PBR and PBN indicates that these constructs were not adequately captured by the adapted measurement items in this population. Offline data collection in a single province (Riau) limits the generalizability of findings to the broader Indonesian population. Furthermore, all variables were measured by self-report, introducing the possibility of common method variance. Future research should address these limitations by: 1) expanding the sample to at least 300 respondents drawn from multiple Indonesian provinces; 2) revising or replacing the PBR and PBN items to improve cross-cultural validity; 3) incorporating behavioral or objective phishing susceptibility measures alongside self-report; and 4) including digital literacy, cultural orientation, and attack-type familiarity as additional constructs.

E. Implications

Despite the null hypothesis results, this study offers important practical insights. The finding that none of the measured psychological constructs significantly predict susceptibility suggests that standard awareness-raising interventions targeting threat perception or self-efficacy alone may be insufficient for the Indonesian context. Practitioners (including internet service providers (ISPs), the BSSN, and government agencies) should consider multi-layered interventions that address digital literacy gaps, provide culturally adapted phishing training, and integrate technical defenses with behavioral change programs. The high variability in PS scores (SD = 6.884) indicates that susceptibility is not uniformly distributed, suggesting that targeted interventions for high-risk subpopulations may be more effective than broad awareness campaigns.

VII. Conclusion

This study tested six hypotheses (H1–H6) predicting a positive correlation between phishing susceptibility (PS) and six psychological/perceptual variables, namely perceived severity (PST), perceived barriers (PBR), perceived benefits (PBN), self-efficacy (SE), past success in detection (PSD), and phishing desensitization (PD). Although prior research suggested these relationships, empirical analysis using Structural Equation Modeling (SEM) did not support any of the predicted correlations.

The findings indicate that psychological factors – often assumed to noticeably influence phishing vulnerability – showed no measurable direct effect among the respondents. This suggests that susceptibility may not be driven solely by perceptions but could involve other dimensions, such as digital literacy, social context, cultural security norms, or evolving attack strategies. These possibilities require further investigation rather than being interpreted as confirmed causes. In short, even individuals who perceive phishing threats as severe or have previous success in detection do not necessarily exhibit safer behavior.

The SEM model demonstrated an acceptable overall fit, with several indicators (RMSEA, TLI/NNFI, IFI, and CFI) meeting recommended thresholds, indicating adequate data representation. Parsimony indices (PGFI, PNFI) also confirmed the efficiency of the model, and the low CMIN/df ratio showed a balance between fit and complexity. However, weaknesses in NFI, RFI, AGFI, SRMR, and Critical N suggest the need for refinement – such as increasing sample size, improving the measurement model, and incorporating additional latent variables.

Overall, this study contributes to cybersecurity literature by challenging the assumption that higher threat perception or self-efficacy automatically reduces phishing vulnerability. Future research should investigate mediating or moderating variables that explain the gap between perception and behavior, enrich models with behavioral and contextual factors, and aim for designs that achieve both statistical robustness and real-world relevance in an era of evolving cyber threats.

Future research should expand sample sizes to at least 300 respondents, revise the PBR and PBN measurement items for the Indonesian context, incorporate digital literacy and cultural orientation as mediators or moderators, and consider behavioral phishing susceptibility measures alongside self-report instruments. Theoretically, extending the model to include Protection Motivation Theory constructs or cultural dimensions may improve explanatory power. Overall, this study contributes to the cybersecurity literature by demonstrating that standard HBM-derived constructs do not directly predict phishing susceptibility in the Indonesian general population context, and by providing a foundation for more contextually sensitive models of phishing vulnerability.

REFERENCES

[1] D. B. Utoyo, "Empowering Rural Communities through Digital Literacy: An Empirical Study of Former Women Migrant Workers in Panjer Village, Kebumen - Indonesia," in Proceedings of the 9th International Conference on Indonesian Social and Political Enquiries (ICISPE 2024), vol. 937, in Advances in Social Science, Education and Humanities Research, vol. 937. , Paris: Atlantis Press SARL, 2025, pp. 378–390. doi: 10.2991/978-2-38476-436-5_33.

[2] Rebecca Ling Ze Siew, Brendan Chan Kah Le, Lee Kai Yue, Nuri Nazirah Binti Ismail, Xavier Liong Zhi Hao, and Muhammad Faisal, "Enhancing Security in Industrial IoT: Authentication Solutions Leveraging Blockchain Technology," IJCTS, vol. 1, no. 3, pp. 87–105, Jul. 2024, doi: 10.62951/ijcts.v1i3.29.

[3] A. B. Yunas, Y. Rumanto, and N. Albart, "Blockchain and Green Sukuk Integration for Coastal Community Empowerment in Sustainable Blue Economy," Research Horizon, vol. 5, no. 2, pp. 415–426, 2025.

[4] R. J. Mejias, J. J. Greer, G. C. Greer, M. M. Shepherd, and R. Y. Reyes, "A model for information security vulnerability awareness," Computers & Security, vol. 151, p. 104305, Apr. 2025, doi: 10.1016/j.cose.2024.104305.

[5] R. Rohan, D. Pal, J. Hautamäki, S. Funilkul, W. Chutimaskul, and H. Thapliyal, "A systematic literature review of cybersecurity scales assessing information security awareness," Heliyon, vol. 9, no. 3, p. e14234, Mar. 2023, doi: 10.1016/j.heliyon.2023.e14234.

[6] A. K. Gwenhure, "University students' security behavior against email phishing attacks: insights from the health belief model," Journal of Cybersecurity, vol. 11, no. 1, p. tyaf034, Jan. 2025, doi: 10.1093/cybsec/tyaf034.

[7] K. D. Mitnick and W. L. Simon, The art of deception: Controlling the human element of security. Indianapolis, Indiana: Wiley, 2003.

[8] I. Ghafir et al., "Security threats to critical infrastructure: the human factor," The Journal of Supercomputing, vol. 74, no. 10, pp. 4986–5002, Oct. 2018, doi: 10.1007/s11227-018-2337-2.

[9] S. Anawar, D. L. Kunasegaran, M. Z. Mas'Ud, and N. A. Zakaria, "Analysis of phishing susceptibility in a workplace: A big-five personality perspectives," Journal of Engineering Science and Technology, vol. 14, no. 5, pp. 2865–2882, 2019.

[10] A. Alturki, N. Alshwihi, and A. Algarni, "Factors Influencing Players' Susceptibility to Social Engineering in Social Gaming Networks," IEEE Access, vol. 8, pp. 97383–97391, 2020, doi: 10.1109/ACCESS.2020.2995619.

[11] R. Chen, J. Gaia, and H. R. Rao, "An examination of the effect of recent phishing encounters on phishing susceptibility," Decision Support Systems, vol. 133, p. 113287, Jun. 2020, doi: 10.1016/j.dss.2020.113287.

[12] T. Halevi, J. Lewis, and N. Memon, "A pilot study of cyber security and privacy related behavior and personality traits," in Proceedings of the 22nd International Conference on World Wide Web, Rio de Janeiro Brazil: ACM, May 2013, pp. 737–744. doi: 10.1145/2487788.2488034.

[13] I. Tjostheim and J. Waterworth, "Exploring susceptibility to phishing: The Cognitive Reflection Test and other possible predictors," in Proceedings of the 57th Hawaii International Conference on System Sciences | 2024, diva-portal.org, 2024. [Online]. Available: https://www.diva-portal.org/smash/record.jsf?pid=diva2:1823232

[14] E. J. Williams and A. N. Joinson, "Developing a measure of information seeking about phishing," Journal of Cybersecurity, vol. 6, no. 1, p. tyaa001, Jan. 2020, doi: 10.1093/cybsec/tyaa001.

[15] Y. Y. Lee, C. L. Gan, and T. W. Liew, "Thwarting Instant Messaging Phishing Attacks: The Role of Self-Efficacy and the Mediating Effect of Attitude towards Online Sharing of Personal Information," IJERPH, vol. 20, no. 4, p. 3514, Feb. 2023, doi: 10.3390/ijerph20043514.

[16] L. Ribeiro, I. S. Guedes, and C. S. Cardoso, "Which factors predict susceptibility to phishing? An empirical study," Computers &Security. Elsevier, 2024. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167404823004686

[17] K. Singh, P. Aggarwal, P. Rajivan, and C. Gonzalez, "Training to Detect Phishing Emails: Effects of the Frequency of Experienced Phishing Emails," Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 63, no. 1, pp. 453–457, Nov. 2019, doi: 10.1177/1071181319631355.

[18] S. Baki and R. M. Verma, "Sixteen Years of Phishing User Studies: What Have We Learned?," IEEE Trans. Dependable and Secure Comput., vol. 20, no. 2, pp. 1200–1212, Mar. 2023, doi: 10.1109/TDSC.2022.3151103.

[19] S. Kleitman, M. K. H. Law, and J. Kay, "It's the deceiver and the receiver: Individual differences in phishing susceptibility and false positives with item profiling," PLoS ONE, vol. 13, no. 10, p. e0205089, Oct. 2018, doi: 10.1371/journal.pone.0205089.

[20] L. Q. Ribeiro, I. Guedes, and C. Cardoso, "Phishing: A Theoretical Approach and the Innovative Tools," in Advances in Digital Crime, Forensics, and Cyber Terrorism, N. Mateus-Coelho and M. Cruz-Cunha, Eds., IGI Global, 2023, pp. 76–93. doi: 10.4018/978-1-6684-8422-7.ch005.

[21] A. Sumner, X. Yuan, M. Anwar, and M. McBride, "Examining Factors Impacting the Effectiveness of Anti-Phishing Trainings," Journal of Computer Information Systems, vol. 62, no. 5, pp. 975–997, Sep. 2022, doi: 10.1080/08874417.2021.1955638.

[22] K. S. Jones, N. R. Lodinger, B. P. Widlus, A. S. Namin, E. Maw, and M. Armstrong, "Grouping and Determining Perceived Severity of Cyber-Attack Consequences: Gaining Information Needed to Sonify Cyber-Attacks," J Multimodal User Interfaces, vol. 16, no. 4, pp. 399–412, Dec. 2022, doi: 10.1007/s12193-022-00397-z.

[23] C. L. Anderson and R. Agarwal, "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions1," MIS Quarterly, vol. 34, no. 3, pp. 613–643, Sep. 2010, doi: 10.2307/25750694.

[24] Kibreab adane and B. Beyene, "Email and Website-Based Phishing Attack: Examining Online Users Security Behavior in Cyberspace Environment," IJISM, vol. 21, no. 1, Jan. 2023, doi: 10.22034/ijism.2022.1977800.0.

[25] R. T. Wright, M. L. Jensen, J. B. Thatcher, M. Dinger, and K. Marett, "Research Note —Influence Techniques in Phishing Attacks: An Examination of Vulnerability and Resistance," Information Systems Research, vol. 25, no. 2, pp. 385–400, Jun. 2014, doi: 10.1287/isre.2014.0522.

[26] C. B. Kirwan, D. K. Bjornn, B. B. Anderson, A. Vance, D. Eargle, and J. L. Jenkins, "Repetition of Computer Security Warnings Results in Differential Repetition Suppression Effects as Revealed With Functional MRI," Front. Psychol., vol. 11, p. 528079, Dec. 2020, doi: 10.3389/fpsyg.2020.528079.