Jur. Ilm. Kel. & Kons., Mei 2025, p: 121–133 Vol. 18, No. 2
p-ISSN : 1907 – 6037 e-ISSN : 2502 – 3594 DOI: http://dx.doi.org/10.24156/jikk.2025.18.2.121

PHISHING AWARENESS AND SECURITY CONCERNS: ANALYZING THE ROLE OF ANTI-PHISHING KNOWLEDGE AND INTERNET EXPERIENCE IN ONLINE BANKING USERS

Rista Junita Nur'aini, Megawati Simanjuntak*)

Department of Family and Consumer Sciences. Faculty of Human Ecology, IPB University, Lingkar Kampus street IPB Darmaga, Bogor, 16680, Indonesia

*)*E-mail: mega_juntak@apps.ipb.ac.id*

Abstract

Phishing has become Indonesia's most prevalent cybercrime from 2017 to 2022, primarily due to the collection of users' personal information. The purpose of this study is to examine how security concerns are impacted by social engineering, internet experience, anti-phishing expertise, and phishing awareness. The Technology Threat Avoidance Theory (TTAT) model lends credence to this study. A quantitative methodology was employed, conducted through online surveys. To enrich the discussion, six of these respondents participated in in-depth interviews as a complementary approach. Data analysis was performed using LISREL 8.80 and SPSS 26. The findings demonstrated that internet experience and anti-phishing knowledge significantly increased phishing awareness. Furthermore, security concerns were significantly impacted by anti-phishing expertise. The results of further analysis revealed that social engineering had no significant effect on phishing awareness. In addition, Internet experience did not significantly affect security concerns. Based on the research results, user understanding can be enhanced by creating educational media that can be disseminated via social media.

Keywords: anti-phishing knowledge, influence of social engineering, internet experience, phishing awareness, security concern

Kesadaran akan *Phishing* dan Masalah Keamanan: Menganalisis Peran Pengetahuan *Anti-Phishing* dan Pengalaman Internet pada Pengguna Perbankan Online

Abstract

Phishing telah muncul sebagai kejahatan siber yang paling sering terjadi di Indonesia antara tahun 2017 hingga 2022, terutama karena pengumpulan informasi pribadi pengguna. Tujuan dari penelitian ini adalah untuk menguji bagaimana masalah keamanan dipengaruhi oleh rekayasa sosial, pengalaman Internet, keahlian anti-phishing, dan kesadaran akan phishing. Penelitian ini didukung oleh Model Teori Penghindaran Ancaman Teknologi (TTAT). Metodologi yang digunakan dalam penelitian ini adalah kuantitatif, yang dilakukan melalui survei online. Sebanyak 207 responden dipilih menggunakan metode *voluntary sampling*. Untuk memperkaya analisis, enam dari 207 responden tersebut berpartisipasi dalam wawancara mendalam sebagai pendekatan pelengkap. Analisis data dilakukan dengan menggunakan LISREL 8.80 dan SPSS 26. Temuan menunjukkan bahwa pengalaman internet dan pengetahuan anti-phishing memiliki pengaruh signifikan terhadap peningkatan kesadaran terhadap phishing. Selain itu, keahlian anti-phishing secara signifikan mempengaruhi masalah keamanan. Hasil analisis lanjutan menunjukkan bahwa *influence of social engineering* tidak memiliki pengaruh signifikan terhadap *phishing awareness.* Selain itu, *internet experience* juga tidak memiliki pengaruh signifikan terhadap *security concern.* Berdasarkan temuan ini, pemahaman pengguna dapat ditingkatkan melalui pembuatan media edukasi yang dapat disebarluaskan melalui platform media sosial.

Kata kunci: pengalaman internet, pengetahuan *anti-phishing*, rekayasa sosial, kekhawatiran terhadap keamanan, kesadaran terhadap *phising*

INTRODUCTION

Technological advancements continue to progress each year, particularly in the area of internet usage. During the COVID-19 pandemic, an additional 35 million people began using the internet. According to research by the Indonesian Internet Service Providers Association (APJII, 2024), the internet penetration rate stands at approximately 79.5

Article history:
Received November 30, 2024
Received in revised April 24, 2025
Accepted April 25, 2025

percent, with 50.7 percent of users being male and 49.1 percent being female. Internet penetration in Indonesia has steadily increased, according to the latest data released by APJII. In 2024, internet penetration in Indonesia reached 78.19 percent, showing a 1.4 percent increase compared to the previous year. Internet penetration is widespread across Indonesia, with urban areas showing a penetration rate of 69.5 percent, while 30.5 percent of the population resides in these areas (APJII, 2024).

The increase in internet users has raised significant concerns about how it is being utilized. One of the key concerns is the threat of phishing. Phishing is a form of cybercrime that deceives users into revealing their personal information and bank account credentials through social engineering tactics (Anti-Phishing Working Group [APWG], 2020). Phishing attacks typically target data such as personal information, account details, and financial data (Fanasafa, 2022). Most individuals who fall victim to phishing do so due to a lack of public awareness about the risks associated with such attacks (Annur, 2022).

During the pandemic, global cyberattacks increased by 125 percent by 2021, targeting both companies and individuals. This surge was largely driven by cybercriminals taking advantage of network vulnerabilities as businesses transitioned to remote work. In 2021, Asia emerged as the continent most affected by cyberattacks, accounting for 26 percent of all incidents, followed by Europe (24%), North America (23%), the Middle East and Africa (14%), and Latin America (13%). According to the latest report from the National Cyber Security Index (NCSI), Indonesia's cybersecurity index score is 63.64 points, reflecting a 16.23 percent improvement from the previous year (e-Governance Academy Foundation, n.d.).

In the second quarter of 2022, Indonesia reported 5,579 phishing cases, marking an increase of 41.52 percent compared to the first quarter of 2022 (Annur, 2022). The Anti-Phishing Working Group identified 165,772 phishing websites in 2020, the majority of which targeted the financial sector (Fanasafa, 2022). This shift is due to changes in business processes, which transitioned from manual or offline methods to digital platforms via websites or applications (Sakti et al. 2018). In 2022, the National Cyber and Encryption Agency (BSSN) reported 164,131 phishing email cases in Indonesia, with 59,210 cases involving personal emails. Additionally, 52,744 cases were linked to group email usage, and 52,177 phishing cases were categorized under other sources (Sadya, 2023).

Based on the description above, this research is interesting because it introduces novel elements compared to previous research by Farhana et al. (2021), particularly in its exploration of anti-phishing knowledge, the influence of social engineering on phishing awareness, and the addition of the variable Internet experience. This study investigates the impact of anti-phishing knowledge, Internet experience, and phishing awareness on security concerns. Although cybersecurity studies are relatively abundant, research that integrates phishing awareness, anti-phishing knowledge, Internet experience, and security concerns remains limited. Existing studies typically examine these variables separately or within specific domains, such as e-commerce or websites (e.g., Rao et al., 2022; Wijaya et al., 2023). Therefore, this study fills a gap in the literature and contributes to a more integrated understanding of phishing and cybersecurity behaviors.

Phishing is a dangerous form of social engineering aimed at deceiving individuals into revealing personal or confidential information (Ferreira & Teles, 2019). Phishing includes various types, such as email, spear, whaling, web, SMS, and vishing (Fanasafa, 2022). Anti-phishing knowledge enhances consumer security, helping them avoid phishing threats (Farhana et al., 2021). Anti-phishing knowledge is an important factor in helping individuals avoid phishing (Baral & Arachchilage 2019; Farhana et al., 2021).

Internet usage experience refers to an individual's ability to use and access websites online. An individual's experience can stem from cognitive, social, affective, and physical sources (Zhang, 2016). When using the Internet, it is crucial to consider factors such as understanding an individual's perceptions, attitudes, and behavior in an online environment (Soto et al., 2015). In addition to Internet usage experience, social engineering can influence an individual to take certain actions. Social engineering is a technique that bypasses security systems by exploiting vulnerabilities (Huwaidi & Destya, 2022).

Social engineering attacks include physical, social, reverse social engineering, technical, and socio-technical approaches (Krombholz et al., 2014). Security also influences an individual's use of the internet. According to *Kamus Besar Bahasa Indonesia* (KBBI), security refers to a state that is free from danger and disturbances.

Awareness is necessary to mitigate the threat of phishing, such as changing passwords and scanning the computer to be used (Muniandy et al., 2017). A strong password includes lowercase letters, uppercase letters, numbers, and special characters, which can help prevent phishing attacks (Farhana et al., 2021).

This research is grounded in the Technology Threat Avoidance Theory (TTAT) model, which explores information technology (IT) user behavior in addressing technology-related threats through the influence of anti-phishing knowledge and self-efficacy (Arachchilage & Love, 2014). TTAT explains how individuals respond to technological threats by taking avoidance actions, which are shaped by their perceptions of vulnerability and the severity of the threat (Carpenter et al., 2019). The theory emphasizes that individuals are more likely to adopt avoidance strategies when they perceive a threat (Wu et al., 2024). TTAT also considers factors such as the persistence of the threat, the cost of self-protection, and the individual's confidence in managing the threat (Rifai et al., 2023).

Moreover, TTAT has proven relevant in various cybersecurity-related studies, including research on how information security professionals handle threats and how threat perception on mobile devices affects avoidance behavior (Domingo et al., 2022; Session & Muller, 2022). Therefore, in this study, TTAT serves as an appropriate framework to explain how online banking users react to phishing threats based on their knowledge and experience, as well as how their security awareness and concerns contribute to avoidance behavior toward cyber threats.

The results of this study are important for stakeholders, such as the government, in creating legislation related to phishing and educating the public about phishing crimes. In addition, this research is important for financial service providers, especially online financial service providers, in raising consumer awareness about personal data confidentiality and the presence of phishing behaviors that threatens Indonesian consumers.

Based on this background, this study aims to analyze the relationship between respondent characteristics, anti-phishing knowledge, internet experience, the influence of social engineering, phishing awareness, and security concerns among bank users. Finally, we analyzed the impact of anti-phishing knowledge, Internet experience, social engineering, and phishing awareness on security concerns among bank users. Therefore, the framework of this study is based on the research by Farhana et al. (2021), as illustrated in Figure 1.

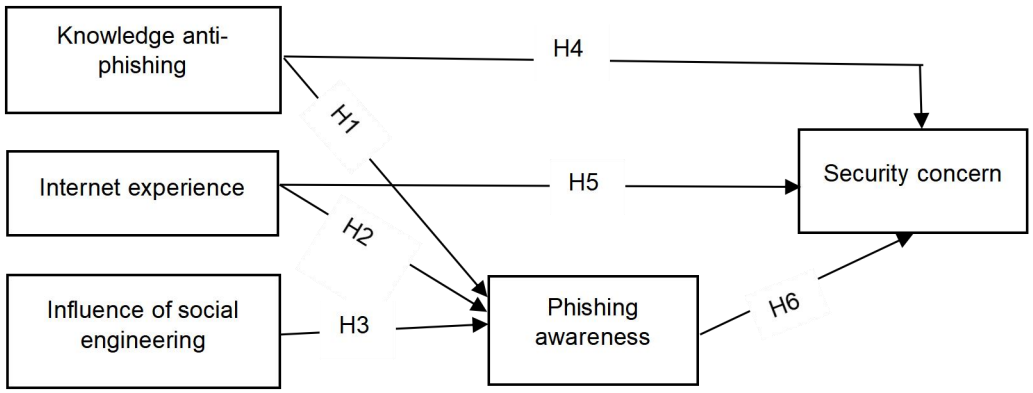

Figure 1. Conceptual Framework

Referring to the framework in Figure 1, the proposed hypothesis is as follows:

H1 : Anti-phishing knowledge affects phishing awareness
H2 : Internet experience affects phishing awareness
H3 : Influence of social engineering affects phishing awareness
H4 : Anti-phishing knowledge affects security concern
H5 : Internet experience affects security concern
H6 : Phishing awareness affects security concern

METHODS

Research Design, Location, and Time

This study used a quantitative approach, complemented by in-depth interviews. The research was conducted using an online survey, with in-depth interviews added to enhance the data gathered through the quantitative approach. study employed a cross-sectional design, meaning the research was conducted at a single point in time. The study was conducted between January and February 2024 in Indonesia.

Sampling Technique

The population selected in this consisted of internet users, particularly online banking users in Indonesia, selected through a voluntary sampling technique. Online banking users were chosen for this study due to their high vulnerability to phishing attacks and elevated exposure to digital security risks. A total of 212 respondents were initially selected, meeting the criteria of being Indonesian citizens aged 19–34 years and active online banking users. However, five respondents were excluded from the analysis because they did not meet the specified criteria. As a result, the final sample size for this study was 207 respondents. The sample size of 207 complies with the guidelines of Hair et al. (2019), which suggest a sample size 5 to 10 times the number of estimated coefficients (34), yielding a recommended range of 170 to 340. Therefore, this sample size is deemed sufficient for analysis. To further enrich the discussion, six participants from the 207 respondents took part in in-depth interviews. The in-depth interviews served as a complementary method, offering additional insights that enhanced the quantitative findings.

Procedures for Data Collection

Data collection commenced after receiving permission from the Department of Family and Consumer Sciences, Faculty of Human Ecology, IPB University. The data collection process began with the selection of samples, who also served as respondents. Respondents were online banking users who consented to participate in the entire data collection process. Before completing the survey, respondents first signed an informed consent form, indicating their willingness to answer all research questions. The survey was administered online to the respondents.

Measurement and Assessment of Variables

Anti-phishing knowledge refers to the subjective knowledge of consumers regarding phishing behavior. This variable is measured using six indicators on a 1–5 Likert scale, ranging from "not very suitable" to "very suitable." Question items assessing anti-phishing knowledge include the ability to understand the URL used and to recheck emails received before making transactions. The anti-phishing knowledge questionnaire obtained a Cronbach's alpha value of 0.776. All indicators for this variable were adopted and slightly modified from the measurement items proposed by Farhana et al. (2021).

Internet experience refers to consumer behavior when using the Internet. The measurement consisted of 10 indicators. The internet experience variable was measured on a 1–5 Likert scale, ranging from "never" to "always," with a Cronbach's alpha reliability coefficient of 0.830. Question items assessing internet experience include using the internet to form social identity and to engage in interpersonal relationships. All indicators for this variable were adopted and slightly modified from the measurement items proposed by Gupta and Bashir (2018).

Social engineering refers to the influence of the social environment on individual behavior. The six indicators are measured on a 1–5 Likert scale, ranging from "not very suitable" to "very suitable." Question items on the influence of social engineering include being easily panicked and following directions from individuals claiming to represent an agency. The influence of the social engineering questionnaire obtained a Cronbach's alpha value of 0.762. All indicators for this variable were adopted and slightly modified from the measurement items proposed by Farhana et al. (2021).

Phishing awareness refers to the consumer awareness of phishing behavior. Phishing awareness was measured using six indicators on a 1–5 Likert scale, ranging from "very unaware" to "very aware," with a Cronbach's alpha reliability of 0.920. Question items on phishing awareness include understanding the meaning of phishing crimes, recognizing identities that should not be disseminated, and being aware of the dangers of phishing crimes. All indicators for this variable were adopted and slightly modified from the measurement items proposed by Farhana et al. (2021).

Security concerns refer to consumer behavior related to maintaining data security. The six indicators are measured on a 1–5 Likert scale, ranging from "never at all" to "very often." The security concern questionnaire obtained a Cronbach's alpha value of 0.653. Question items on security concern include installing an antivirus application on the device and changing passwords regularly, at least twice a year. All indicators for this variable were adopted and slightly modified from the measurement items proposed by Farhana et al. (2021) and Kairupan and Rahman (2022).

Data Analysis

The data obtained were processed using SPSS 26 and Lisrel 8.80. For de scriptive analysis, the top two boxes and bottom two boxes were used for each variable, assigning an index value of 0-100 to ensure consistency. Each variable was then categorized into three groups: low (≤60), medium (60.01–79.99), and high (≥80). Additionally, LISREL 8.80 was used to analyze the influence of anti-phishing knowledge, internet experience, the influence of social engineering, and phishing awareness on security concerns. One of the key advantages of LISREL is its ability to simultaneously estimate parameters across multiple models, which is particularly valuable in research that explores relationships among several constructs.

RESULTS

Characteristics of Respondents

In this research, a total of 189 female respondents (91.3%) were the majority, while 18 male respondents (8.7%) participated. The majority of respondents were in the 19–25 age range, totaling 192 respondents (92.8%), while 15 respondents (7.2%) were aged 26 to 34 years. The respondents were spread across 20 provinces in Indonesia, with the highest representation from West Java Province (43%).

Most online banking consumers in this study were high school graduates (62.8%), with a small proportion having junior high school education (0.5%) or D1/D2 education (0.5%). In terms of occupation, the most common jobs among respondents were students (32.4%) and those not working (30%), while the smallest groups were housewives (0.5%) and volunteers (0.5%). Regarding income, most respondents earned above Rp1,000,000 (38.2%) or between Rp1,000,000 and Rp3,000,000 (44.4%). Only a few respondents had an average income above Rp11,000,000 (0.5%). These findings provide valuable insights into the demographic characteristics of the respondents, which may influence their perspectives and behaviors related to online banking.

Internet Usage Intensity

This study also gathered data on respondents' internet usage intensity based on several criteria. These criteria included average daily internet usage, frequently used internet applications, frequency of online banking use, and reasons for using online banking. The results showed that the majority of respondents (65.2%) used the internet for more than 5 hours per day. Respondents mentioned a variety of internet applications they used most frequently. However, three internet applications were identified as the most widely used. These applications were WhatsApp (91.8%), Instagram (78.7%), and Twitter/X (67.1%). The majority of respondents (90.8%) used online banking one to three times per day. Respondents stated that the main reasons for using online banking were its ease of access (91.8%), flexibility (84.5%), and time-saving benefits (85%). Additionally, respondents noted that online banking is more practical (1.9%) and does not require much time (35.7%). These findings highlight the increasing reliance on internet-based services, especially online banking, driven primarily by convenience and efficiency.

Descriptive Analysis of Each Variable

The following table (Table 1) provides a detailed descriptive analysis of the key variables measured in this study. Each category highlights the number of respondents (Count, n) and their corresponding percentage (%) within each classification.

Anti-Phishing Knowledge. Based on the data in Table 1, 50.7 percent of respondents fall into the medium category for anti-phishing knowledge. This indicates that most respondents possess a moderate level of awareness about phishing threats, though there remains room for improvement in both understanding and prevention. This finding is supported by the following in-depth interview excerpts:

> *"I've read about phishing on social media platforms like Instagram and Twitter because a lot of people share information there."* – (AA, 26 years old)

Table 1 Overview of Respondent Distribution (n = 207)

Variable	Category	Count (n)	Percentage (%)
Anti-Phishing Knowledge	Low (≤60.00)	65	31.4
	Medium (60.01–79.99)	105	50.7
	High (≥80.00)	37	17.9
Internet Experience	Low (≤60.00)	13	6.3
	Medium (60.01–79.99)	87	42.0
	High (≥80.00)	107	51.7
Influence of Social Engineering	Low (≤60.00)	197	95.2
	Medium (60.01–79.99)	8	3.9
	High (≥80.00)	2	1.0
Phishing Awareness	Low (≤60.00)	28	13.5
	Medium (60.01–79.99)	68	32.9
	High (≥80.00)	111	53.6
Security Concern	Low (≤60.00)	133	64.3
	Medium (60.01–79.99)	58	28.0
	High (≥80.00)	16	7.7

> "*Regarding the padlock symbol on the link address, honestly, I don't pay much attention because I usually click links from Google search results and rarely open ones sent through chat."* – (D, 23 years old)

Internet Experience. Data from Table 1 shows that 51.7 percent of respondents have a high level of internet experience. This indicates that over half of the respondents engage intensively and diversely with the internet, which may enhance their ability to recognize and respond to threats such as phishing. The following interview excerpts support this finding:

> "*It's very important because the more we know about social media, the more aware we become of the crimes that frequently occur. Especially in this 4.0 era, where all news is on social media, we have to be smart in finding reliable information."* – (HR, 24 years old)

> "*It depends on how you use the internet. If you use it to find information, it can reduce your chances of falling victim to phishing."* – (AA, 26 years old)

Influence of Social Engineering. Analysis of Table 1 shows that 95.2 percent of respondents are not influenced by social engineering tactics, placing them in the low-risk category. This suggests a strong level of awareness regarding social manipulation attempts that aim to steal personal data or sensitive information. This result is supported by the following interview responses:

> "*We can't fully trust an institution; we need to stay cautious. It's okay to be suspicious as long as it protects us in the long run."* – (D, 23 years old)

> "*For me personally, even if it's a trusted institution, I wouldn't trust it 100 percent because the account is mine, the data is mine, so I still need to be careful. However, some people don't understand the importance of protecting themselves, so it depends on whether they fully trust others, even trusted institutions.*" – (HR, 24 years old)

Phishing Awareness. Based on Table 1, 53.6 percent of respondents demonstrate a high level of awareness about phishing threats. Respondents recognize that phishing is a harmful activity that can lead to both financial and psychological harm. The following in-depth interview responses support this finding:

> "*Personally, I'm aware of this crime because it's currently very prevalent. The usual modus operandi involves sending files in APK format, which, if unchecked, can hack our accounts."* – (HR, 24 years old)

> "*Phishing crimes are extremely dangerous because, in addition to financial losses, they can cause psychological harm, as victims may experience trauma afterward.*" – (DE, 26 years old)

Table 2 Overall model fit (n = 207)

Goodness-of-fit	Cut-off-Value	Results	Keterangan
RMSEA	≤ 0.08	0.041	Good fit
RMR	≤ 0.1	0.057	Good fit
GFI	0.80 – 0.90	0.92	Good fit
AGF	< 1; ≥ 0.9	0.89	Good fit
IFI	< 1; ≥ 0.9	0.97	Good fit
NF	< 1; ≥ 0.9	0.92	Good fit
CFI	< 1; ≥ 0.9	0.97	Good fit

Security Concern. Table 1 shows that 64.3 percent of respondents exhibit a low level of security concern. This suggests that most respondents may not prioritize security when accessing information or managing their personal data. The following interview responses support this finding:

"*I rarely change passwords because I'm afraid I'll forget them if I use a new one, and I usually use the same password for all applications."* – (KH, 21 years old)

"*I usually change passwords once a year or when I have free time, and make sure they are unrelated to myself so others can't easily guess them."* – (KK, 25 years old)

Model Fit Evaluation Results

To determine how well the proposed model fits the observed data, this study assesses model fit. The evaluation process involves several steps, including assessing the fit of the measurement model, the overall model, and the structural model (Hair et al., 2019). To assess overall model fit, various goodness-of-fit indices were used, including RMSEA, RMR, GFI, AGFI, IFI, NFI, and CFI. Table 2 shows the model fit results according to the established criteria. The results indicate that all indices meet the required thresholds, confirming that the model has a good fit.

The regression analysis results show that all model fit tests can be accepted and clearly explained. One absolute fit index used to adjust for chi-square sensitivity in large sample sizes is the Root Mean Square Error of Approximation (RMSEA). An RMSEA value of 0.08 or lower is considered acceptable for model fit. The computed RMSEA value is 0.041, which meets the criteria for excellent fit, indicating that the model is acceptable. Additionally, the model showed an RMR value of 0.057, along with a GFI of 0.92, AGFI of 0.89, IFI of 0.97, NFI of 0.92, and CFI of 0.97, all of which indicate a good model fit.

Factors Affecting Security Concern

Prior to analyzing the structural model, the measurement model was assessed for both validity and reliability. Reliability was evaluated using Cronbach's Alpha (threshold > 0.6), and validity was assessed through factor loadings (threshold > 0.5). Although most items had loadings above 0.5, two items with loadings around 0.4 were retained based on theoretical importance and satisfactory overall reliability.

Additional hypothesis testing was conducted using the empirical model by examining the path coefficients and t-values in the structural equation model. A relationship between variables is considered significant if β > 0.05 and the t-value exceeds 1.96. Conversely, the effect is deemed insignificant if β < 0.05 and the t-value is below 1.96. Table 3 displays the SEM model estimation results based on the analysis of direct effects.

The results in Table 3 indicate significant positive direct effects for three variables: anti-phishing knowledge (PAP) on phishing awareness (PA) (β = 0.36; |t-value| = 4.10), Internet experience (IE) on phishing awareness (PA) (β = 017; |t-value| = 2.25), and anti-phishing knowledge (PAP) on security concern (SC) (β = 0.41; |t-value| = 3.27). Accordingly, hypotheses H1, H2, and H4 were supported in this study. In contrast, the results show no significant effect for the following relationships: influence of social engineering (IS) on phishing awareness (PA) (β = -0.03; |t-value| = -0.39), Internet experience (IE) on security concern (SC) (β = -0.05; |t-value| = -0.57), and phishing awareness (PA) on security concern (SC) (β = 0.02; |t-value| = -0.24). Therefore, hypotheses H3, H5, and H6 were rejected.

Table 3 Estimation results of direct effects on the SEM model (n = 207)

Variable Effect			Coef. Path	|*t-val*|	Conclusion	Description
Anti-Phishing Knowledge (PAP)	→	Phishing Awareness (PA)	0,36	4,10	Significant	Accept H1
Internet experience (IE)	→	Phishing Awareness (PA)	0,17	2,25	Significant	Accept H2
Influence of Social Engineering (IS)	→	Phishing Awareness (PA)	-0,03	-0,39	Not Significant	Reject H3
Anti-Phishing Knowledge (PAP)	→	Security Concern (SC)	0,41	3,27	Significant	Accept H4
Internet Experience (IE)	→	Security Concern (SC)	-0,05	-0,57	Not Significant	Reject H5
Phishing Awareness (PA)	→	Security Concern (SC)	0,02	0,24	Not Significant	Reject H6

DISCUSSION

Age is one of the study participants' characteristics that is linked to their knowledge of anti-phishing techniques, according to the analysis results. A respondent's level of anti-phishing expertise tends to increase with age. This aligns with findings from other studies, which indicate that both knowledge and cognitive maturity generally improve with age (Gultom et al., 2021). Age influences an individual's ability to understand and process information, as mental maturity and comprehension typically improve over time. Additionally, maturity in decision-making and action tends to increase with age (Astuti & Iswati, 2023). There was no correlation found between gender and anti-phishing knowledge. This is consistent with earlier research, which reported no significant relationship between gender and knowledge, as both men and women generally have equal access to information (Lestari et al., 2023).

Similarly, no correlation was found between anti-phishing knowledge and education level. These results align with previous studies that found no direct connection between formal schooling and knowledge acquisition. This is due to the fact that knowledge can also be gained through experience and environmental exposure (Wulandari et al., 2021). However, this finding contrasts with earlier studies suggesting a correlation between higher education and broader knowledge (Dewi & Farida, 2018). One of the things that can affect how someone receives information is their level of education; generally, the more educated a person is, the more effectively they comprehend new information (Lestari et al., 2023).

In addition, internet experience is associated with respondent characteristics such as gender and domicile. The findings of this study are consistent with previous studies suggesting that gender is related to internet experience. Men and women have different physiological traits. Women may face a higher risk of becoming victims of incidents compared to men, reflecting behavioral differences tied to gender (Nurhafizha et al., 2023). Other research has indicated that work status also correlates with internet experience. Specifically, individuals employed in formal sectors tend to use the internet more frequently for work purposes, whereas those in informal sectors typically use the internet mainly for communication (Saputri, 2021).

The study also found a relationship between respondents' residence and most recent educational attainment and the influence of social engineering. However, these results contradict earlier studies that suggested a gender correlation with the impact of social engineering. Research by Parsons et al. (2019) highlighted that gender differences can shape individuals' understanding of social engineering, as different social principles exist between men and women. Furthermore, phishing awareness is associated with the respondent characteristics of age, occupation, and income. A study by Parsons et al. (2019) found that younger respondents were more likely to detect phishing emails, with 20 percent of respondents demonstrating this ability.

These findings contradict earlier research that suggested no correlation between age and phishing awareness, with younger individuals being just as knowledgeable and vigilant about phishing as older individuals (Gavett et al., 2017). Additionally, previous studies have indicated a correlation between gender and phishing awareness. According to Ge et al.'s research findings from 2021, men tend to be

more aware of phishing threats than women. This is based on the observation that men are more likely to elaborate on the emails they receive compared to women.

Furthermore, security concern was found to be related to respondent characteristics such as age and education. These results contradict previous studies that indicated a relationship between gender and security concerns. In the research, gender was found to influence the understanding of security concerns, with female respondents demonstrating less awareness of security issues compared to male respondents (Schoenmakers et al., 2023).

The results indicate that anti-phishing knowledge has a positive effect on phishing awareness, supporting previous studies (Farhana et al., 2021; Lee et al., 2023). According to cognitive theory, cognition involves processing information through observation, thinking, imagination, remembering and judging, selectively, and problem solving (Alahmad, 2020). Acquiring anti-phishing knowledge can reduce an individual's vulnerability to phishing attacks. As a person's understanding of phishing crimes increases, they become more cautious about sharing personal data online (Lee et al., 2023). However, possessing strong anti-phishing knowledge does not necessarily guarantee awareness of phishing threats on bank websites, the Internet, or social media platforms (Farhana et al., 2021). This aligns with previous research, which found that many individuals are still unaware of consumer protection measures (Azizah et al., 2022).

Additionally, internet experience is positively correlated with phishing awareness, in line with earlier studies that highlight how experience in using the internet enhances awareness of phishing threats. This is largely mediated by the tendency to check and delete suspicious emails (Ge et al., 2021). Moreover, the frequency of internet use can influence an individual's vulnerability to phishing scams. Research by Ribeiro et al. (2024) suggests that increased internet usage for leisure purposes can reduce vulnerability to phishing, as information about phishing crimes is widely shared on social media platforms.

The analysis results reveal that the influence of social engineering did not significantly influence phishing awareness, contradicting previous studies that suggested social engineering negatively impacts awareness of phishing crimes (Farhana et al., 2021). A majority of respondents did not exhibit panic when receiving messages from authority figures, which could indicate a lack of heightened vigilance regarding potential threats. Previous research indicated that greater awareness of social engineering tactics led to increased susceptibility to evolving social engineering threats (Muniandy et al., 2017). This may be explained by the fact that only 25 percent of respondents had encountered discussions of social engineering in newspapers or online news outlets (Farhana et al., 2021).

However, earlier studies have suggested that social engineering does play a significant role in phishing awareness. Trust in others has been found to positively influence the likelihood of an individual sharing personal information (Rahayu et al., 2023). Furthermore, the presence of social engineering tactics can significantly impact how individuals respond to phishing emails (Parsons, 2019).

This analysis reveals that security concerns are positively influenced by anti-phishing knowledge, aligning with prior studies that suggest anti-phishing knowledge significantly shapes individuals' behaviors. A person's actions are often driven by their intention and purpose when seeking information (Ramadhan & Asandimitra, 2019). Information security is not solely reliant on technical tools or technologies; it also depends on the individuals within an organization who are responsible for safeguarding data and implementing solutions in response to security issues (Darwis et al., 2019).

On the other hand, Internet experience does not significantly impact security concerns. This outcome is consistent with previous research, which found no clear relationship between experience and behavior (Ramadhan & Asandimitra, 2019). Behaviors are influenced by various factors, including the level of interactivity, emotional state, personnel, and past experiences (Urdea & Constantin, 2021). Furthermore, social interactions play a crucial role in shaping behavior, as experiences are often influenced by the information gathered from the surrounding environment (Ahmed et al., 2022). Experience, in this context, helps individuals decide the appropriate behaviors to adopt (Chen et al., 2021).

In contrast to prior studies, the phishing awareness variable in this study did not significantly influence security concerns. Previous research suggests that awareness plays a vital role in shaping behavior, particularly regarding internet security. A higher level of awareness about phishing crimes is generally associated with an increased sense of security

in online activities (Verkijika, 2019). However, some studies argue that individuals' lack of motivation to protect personal data might hinder the connection between awareness and behavior (Farhana et al., 2021), even though phishing awareness is crucial for ensuring security.

The findings of this study contribute to the Technology Threat Avoidance Theory (TTAT), which explains how users of information technology respond to threats by adopting protective behaviors (Session & Muller, 2022). The results strengthen the TTAT framework, particularly the influence of anti-phishing knowledge and internet experience on phishing awareness. This suggests that a person's experience with the internet and their understanding of anti-phishing practices can help mitigate technological threats. Additionally, the significant effect of anti-phishing knowledge on security concerns further supports the idea that awareness and education regarding phishing can empower individuals to avoid online threats, especially those resulting from insufficient understanding of data protection measures.

This study has several limitations. Firstly, the questionnaire distribution focused only on respondents aged 19–34 years. Additionally, during the in-depth interviews, some potential sources who met the criteria declined to participate. Furthermore, the study's results cannot be generalized to the broader population due to the use of non-probability sampling methods.

CONCLUSION AND SUGGESTIONS

The results of the Structural Equation Modeling (SEM) analysis reveal that both anti-phishing knowledge and internet experience significantly influence phishing awareness. In contrast, social engineering was found to have no significant effect on phishing awareness. This indicates that individuals with higher anti-phishing knowledge and more experience using the internet tend to be more aware of phishing risks. Additionally, while anti-phishing knowledge has a significant impact on security concerns, internet experience and phishing awareness were not found to influence security concerns. This suggests that consumers with higher levels of security knowledge are more cautious in protecting their personal accounts.

Given these findings, it is essential to enhance anti-phishing knowledge and consumer security in online banking through targeted education on phishing risks, utilizing platforms such as social media, which are frequented by consumers. Consumers should actively seek information about phishing through news outlets and social media. They can also increase their account security by enabling two-factor authentication, updating passwords at least once a year, and avoiding easily guessable passwords. Governments should take measures to better safeguard consumers' personal data and prevent data leaks. Furthermore, clearer regulations and more severe penalties for cybercrime perpetrators are needed to create a deterrent effect, as many consumers feel that the current lack of strong punishments for cybercriminals diminishes the effectiveness of existing measures. Future research should build on this study by exploring additional factors such as self-efficacy, motivation, and consumer behavior to further enhance awareness and reduce vulnerability to phishing attacks.

ACKNOWLEDGMENTS

We express our gratitude to the respondents who participated in this research on phishing awareness and security concerns.

REFERENCES

Ahmed, B., Zada, S., Zhang, L., Sidiki, S. N., Contreras-Barraza, N., Vega-Muñoz, A., & Salazar-Sepúlveda, G. (2022). The impact of customer experience and customer engagement on behavioral intentions: Does competitive choice matter? *Frontiers in Psychology, 13*, 1–14. https://doi.org/10.3389/fpsyg.2022.864841

Alahmad, M. (2020). Strengths and weaknesses of cognitive theory. *Budapest International Research and Critics Institute-Journal (BIRCI-Journal), 3*(3), 1584–1593. https://doi.org/10.33258/birci.v3i3.1088

Annur, C. M. (2022, August 23). *Ada 5 ribu serangan phishing terjadi di RI pada kuartal II-2022, ini lembaga yang paling banyak diincar*. Databoks – Katadata. Retrieved April 6, 2023, from https://databoks.katadata.co.id/datapublish/2022/08/23/ada-5-ribu-serangan-phishing-terjadi-di-ri-pada-kuartal-ii-2022-ini-lembaga-yang-paling-banyak-diincar

Asosiasi Penyelenggara Jasa Internet Indonesia. (2024, February 7). *APJII jumlah pengguna internet Indonesia tembus 221 juta orang*. https://apjii.or.id/berita/d/apjii-

jumlah-pengguna-internet-indonesia-tembus-221-juta-orang

Anti-Phishing Working Group. (2020). *Phishing activity trends report, 2nd quarter 2020*. https://docs.apwg.org/reports/apwg_trends_report_q2_2020.pdf

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

Astuti, F., & Iswati, K. D. (2023). Hubungan karakteristik dan tingkat pengetahuan masyarakat Desa Welahan Wetan tentang penggunaan vitamin C sebagai pencegahan COVID-19. *Damianus Journal of Medicine, 22*(2), 88–97. Retrieved from https://ejournal.atmajaya.ac.id/index.php/damianus/article/view/4108

Azizah, S. N., Simanjuntak, M., & Muflikhati, I. (2022). Consumer complaint behaviour in Indonesia: Role of knowledge and self-confidence. *Jurnal Ilmu Keluarga dan Konsumen, 15*(1), 90–101. https://doi.org/10.24156/jikk.2022.15.1.90

Baral, G., & Arachchilage, N. A. G. (2019). Building confidence not to be phished through a gamified approach: Conceptualising user's self-efficacy in phishing threat avoidance behaviour. In *Proceedings of the 2019 Cybersecurity Cyberforensics Conference (CCC 2019)* (pp. 102–110). IEEE. https://doi.org/10.1109/CCC.2019.000-1

Carpenter, D., Young, D. K., Barrett, P., & McLeod, A. (2019). Refining technology threat avoidance theory. *Communications of the Association for Information Systems, 44*, Article 22, 380-407. https://doi.org/10.17705/1cais.04422

Chen, X., Jiao, C., Ji, R., & Li, Y. (2021). Examining customer motivation and its impact on customer engagement behavior in social media: The mediating effect of brand experience. *SAGE Open, 11*(4), 1–16. https://doi.org/10.1177/21582440211052256

Darwis, D., Junaidi, A., & Wamiliana. (2019). A new approach of steganography using center sequential technique. *Journal of Physics: Conference Series, 1338*(1), 1–8. https://doi.org/10.1088/1742-6596/1338/1/012063

Dewi, M. A. C., & Farida, Y. (2018). Tingkat pengetahuan pasien rawat jalan tentang penggunaan antibiotika di Puskesmas Wilayah Karanganyar. *JPSCR Journal of Pharmaceutical Sciences and Clinical Research, 3*(1), 27. https://doi.org/10.20961/jpscr.v3i1.15102

Domingo, W. G., Nicolas, K., MIT, J. A. G., Lardizabal, E. N., Gonzales, V., & Cruz, A. D. (2022). Smsecurity: Security system and SMS notification cum face recognition. *International Journal of Computer Science and Information Technology, 14*(1). https://doi.org/10.5121/ijcsit.2022.141

Farhana, N., Zaharon, M., & Ali, M. M. (2021). Factors affecting awareness. *Asia-Pacific Management Journal, 16*(2), 409–444. http://doi.org/10.24191/APMAJ.V16i2-15

Ferreira, A., & Teles, S. (2019). Persuasion: How phishing emails can influence users and bypass security measures. *International Journal of Human-Computer Studies, 125*, 19–31. https://doi.org/10.1016/j.ijhcs.2018.12.004

Gavett, B. E., Zhao, R., John, S. E., Bussell, C. A., Roberts, J. R., & Yue, C. (2017). Phishing suspiciousness in older and younger adults: The role of executive functioning. *PLoS One, 12*(2), 1–16. https://doi.org/10.1371/journal.pone.0171620

Ge, Y., Lu, L., Cui, X., Chen, Z., & Qu, W. (2021). How personal characteristics impact phishing susceptibility: The mediating role of mail processing. *Applied Ergonomics, 97*, 14. https://doi.org/10.1016/j.apergo.2021.103526

Gultom, D. K., Arif, M., Azhar, M. E., & Mukmin. (2021). Peran mediasi brand satisfaction pada pengaruh self congruity terhadap brand loyalty. *Jurnal Ilmu Manajemen dan Bisnis, 22*(1), 72–85. https://doi.org/10.30596/jimb.v22i1.5633

Gupta, S., & Bashir, L. (2018). Social networking usage questionnaire: Development and validation. *Turkish Online Journal of Distance Education, 19*(4), 214–227. https://dergipark.org.tr/tr/download/article-file/556241

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Prentice Hall.

Huwaidi, M. Z., & Destya, S. (2022). Mencegah serangan rekayasa sosial dengan human firewall. *Justin: Jurnal Sistem dan Teknologi Informasi, 10*(1). https://doi.org/10.26418/justin.v10i1.44280

Kairupan, V. A., & Rahman, A. A. (2022). Analisis kesadaran cybersecurity pada pengguna media sosial di kalangan mahasiswa Kota Bandung. *Jurnal Darma Agung, 30*(1), 1164–1173. https://doi.org/10.46930/ojsuda.v30i1.3167

Fanasafa, I. (2022, March 25). *Waspada! Kejahatan phishing mengintai anda*. Direktorat Jenderal Kekayaan Negara. https://www.djkn.kemenkeu.go.id/kpknl-purwakarta/baca-artikel/14851/Waspada-Kehajatan-Phishing-Mengintai-Anda.html

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2014). Advanced social engineering attacks. *Journal of Information Security and Application, 22*, 113–122. https://doi.org/10.1016/j.jisa.2014.09.005

Lee, Y. Y., Gan, C. L., & Liew, T. W. (2023). Thwarting instant messaging phishing attacks: The role of self-efficacy and the mediating effect of attitude towards online sharing of personal information. *International Journal of Environmental Research and Public Health, 20*(4), 23. https://doi.org/10.3390/ijerph20043514

Lestari, F., Rahmawati, R., & Martono, A. (2023). Hubungan karakteristik pasien terhadap pengetahuan dalam penggunaan obat antibiotik di Puskesmas Seginim Kabupaten Bengkulu Selatan. *Bencoolen Journal of Pharmacy, 3*(2), 3–15. Retrieved from https://ejournal.unib.ac.id/index.php/bjp/index

Muniandy, L., Muniandy, B., & Samsudin, Z. (2017). Cybersecurity behaviour among higher education students in Malaysia. *Journal of Information Assurance & Cybersecurity,* 1–13. https://doi.org/10.5171/2017.800299

e-Governance Academy Foundation. (n.d.). *National cyber security index*. Retrieved May 13, 2023, from https://ncsi.ega.ee/ncsi-index/?order=rank

Nurhafizha, D., Dianingati, R. S., & Annisa, E. (2023). Hubungan persepsi dengan perilaku penggunaan internet sebagai media pencarian informasi obat selama pandemi Covid-19 pada masyarakat di Kota Semarang. *Jurnal Research in Pharmacy, 3*(2), 83–91. https://ejournal2.undip.ac.id/index.php/generics/article/view/20057

Parsons, K., Butavicius, M., Delfabbro, P., & Lillie, M. (2019). Predicting susceptibility to social influence in phishing emails. *International Journal of Human-Computer Studies, 128*, 17–26. https://doi.org/10.1016/j.ijhcs.2019.02.007

Rahayu, I. L., Syarifa, R., Akmalia, L. R., Samosir, M. S., Puja Hanggrita, E., Muflikhati, I., & Simanjuntak, M. (2023). Willingness to share data pribadi dan kaitannya dengan penyalahgunaan data konsumen e-commerce di Indonesia: Pendekatan mixed methods. *Jurnal Ilmu Keluarga dan Konsumen, 16*(3), 274–287. https://doi.org/10.24156/jikk.2023.16.3.274

Ramadhan, A. Y., & Asandimitra, N. (2019). Determinants of financial management behavior of millennial generation in Surabaya. *Jurnal Minds: Manajemen Ide dan Inspirasi, 6*(2), 129. https://doi.org/10.24252/minds.v6i2.9506

Rao, K., Rao, R. S., Abraham, A., & Gabralla, L. A. (2022). Multilayer stacked ensemble learning model to detect phishing websites. *IEEE Access, 10*, 79543–79552. https://doi.org/10.1109/access.2022.3194672

Ribeiro, L., Guedes, I. S., & Cardoso, C. S. (2024). Which factors predict susceptibility to phishing? An empirical study. *Computer and Security, 136*, 12. https://doi.org/10.1016/j.cose.2023.103558

Rifai, A., Meliyani, A., Chyntia, P., & Sakti, I. A. (2023). Penerapan metode technology threat avoidance theory terhadap tingkat kesadaran data privasi pengguna media sosial. *Journal of Information System Research (JOSH), 4*(3), 1026-1032. https://doi.org/10.47065/josh.v4i3.3081

Sadya, S. (2023, March 28). *Ada 164.131 kasus email phishing di Indonesia pada 2022*. DataIndonesia.id. https://dataindonesia.id/digital/detail/ada-

164131-kasus-email-phising-di-indonesia-pada-2022

Sakti, M. A. J., Achsani, N. A., & Syarifuddin, F. (2018). Online banking implementation: Risk mapping using ERM approach. *Bulletin of Monetary Economics Bank, 20*(3), 279–306. https://doi.org/10.21098/bemp.v20i3.824

Saputri, W. L. (2021). Karakteristik pengguna dan pemanfaatan internet pada penduduk bekerja di Kota Samarinda. *BESTARI: Buletin Statistik dan Aplikasi Terkini, 1*(2), 79–87. https://bestari.bpskaltim.com/index.php/bestari-bpskaltim/article/view/36

Schoenmakers, K., Greene, D., Stutterheim, S., Lin, H., & Palmer, M. J. (2023). The security mindset: Characteristics, development, and consequences. *Journal of Cybersecurity, 9*(1), 1–15. https://doi.org/10.1093/cybsec/tyad010

Session, W., & Muller, S. R. (2022). Technology threat avoidance factors affecting cybersecurity professionals' willingness to share information. *Annals of Computer Science and Information Systems, 34*, 209–213.

Soto, P., Monila, A. F., Lopez, C. C., & Colomo, N. R. (2015). The effect of information overload and disorganisation on intention to purchase online. *Online Information Review, 38*(4), 543–561. https://doi.org/10.1108/OIR-01-2014-0008

Urdea, A. M., & Constantin, C. P. (2021). Exploring the impact of customer experience on customer loyalty in e-commerce. *Proceedings of the International Conference on Business Excellence, 15*(1), 672–682. https://doi.org/10.2478/picbe-2021-0063

Verkijika, S. F. (2019). If you know what to do, will you take action to avoid mobile phishing attacks: Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior, 101*, 286–296. https://doi.org/10.1016/j.chb.2019.07.034

Wijaya, A. S., Rohimi, U. E., & Asyifah, A. (2023). The effect of information security systems on service quality in e-commerce systems. *Journal of World Science, 2*(4), 566–570. https://doi.org/10.58344/jws.v2i4.276

Wu, X., Zhou, Z., & Chen, S. (2024). A mixed-methods investigation of the factors affecting the use of facial recognition as a threatening AI application. *Internet Research, 34*(5), 1872-1897. https://doi.org/10.1108/intr-11-2022-0894

Wulandari, A., Rahman, F., Pujianti, N., Sari, A. R., Laily, N., Anggraini, L., Muddin, F. I., Ridwan, A. M., Anhar, V. Y., Azmiyannoor, M., et al. (2021). Hubungan karakteristik individu dengan pengetahuan tentang pencegahan coronavirus disease 2019 pada masyarakat di Kecamatan Pungging Mojokerto. *Jurnal Kesehatan Masyarakat Indonesia, 4*(1), 46–51. https://doi.org/10.52646/snj.v4i1.97

Zhang, A. B. J. A. K. T. (2016). Towards a unified customer experience in online shopping environments: Antecedents and outcomes. *International Journal of Quality and Service Science, 8*(1), 102–119. https://doi.org/10.1108/IJQSS-07-2015-0054