INSANIA
Journal of Islamic Studies and Humanity
Published by PT. Pilar Cendekia Indonesia
E-ISSN : XXXX-XXXX
ISSN : XXXX-XXXX

The Influence of Security Literacy, Levels of Concern About Fraud, and Trust in Islamic Banks on Customers' Verification Responses When Faced with Various Social Engineering Tactics

Rasmi[1], Hamida[2], Rusli[3], Sulkifra[4],
[1] Islamic Banking Study Program, Faculty of Islamic Economics and Business, State Islamic University of Palopo,Indonesia
[2] Islamic Banking Study Program, Faculty of Islamic Economics and Business, State Islamic University of Palopo,Indonesia
[3] Sharia Economics Study Program, Faculty of Islamic Economics and Business, State Islamic University of Palopo,Indonesia
[4] Islamic Banking Study Program, Faculty of Islamic Economics and Business, State Islamic University of Palopo,Indonesia

ARTICLE INFORMATION **ABSTRACT**

Keywords:
Customer Verification Response, Security Literacy, Level of Concern About
Fraud, Trust

Article History:
Received: 21 May 2026
Accepted: 28 May 2026
Published: 31 May 2026

ABSTRACT

This study aims to analyze the influence of security literacy, the level of concern regarding fraud, and trust in Islamic banks on customers' verification responses when faced with various social engineering tactics. The method used was a quantitative associative study employing a survey approach via a questionnaire distributed to 120 active Islamic bank customers in Indonesia. Data analysis was conducted using Structural Equation Modelling-Partial Least Squares (SEM-PLS). The results indicate that security literacy and trust in Islamic banks do not significantly influence customers' responses to verification. Conversely, the level of concern regarding fraud has a positive and significant effect; the higher the customers' level of concern, the greater their tendency to take preventive actions such as verifying information. These findings suggest that emotional factors, such as anxiety regarding the risk of fraud, influence protective behavior more than cognitive understanding or trust in the institution. This study makes a theoretical contribution to the literature on Islamic banking security and offers practical recommendations for banks and regulators to enhance customer literacy and vigilance against the threat of digital fraud.

***Corresponding Author at:**
Islamic Banking Study Program, Faculty of Islamic Economics and Business, **Jalan Tokasirang, Kel. Balandai, Kec. Bara, Palopo 91912, Indonesia.**
E-mail address: 2304020028@uinpalopo.ac.id.

1. INTRODUCTION

The performance of Islamic banking in Indonesia has improved significantly in recent years. This has been driven by various government strategies as well as international factors supporting the growth of this industry (Ahmed & Sur, 2023). According to data from the Financial Services Authority (OJK) in June 2020, the growth in Islamic banking financing reached 10.13 percent year-on-year, far surpassing the 1.49 percent growth in conventional bank credit during the same period. This solid performance reflects competent management and the ability of Islamic banks to provide financial value and security, supported by government backing, increasing public awareness, significant market potential, and strong financial performance. This growth demonstrates that Islamic banks are not merely an alternative but the primary choice for the public seeking to conduct financial transactions safely and in accordance with Sharia principles, while continuously enhancing performance through product innovation, improved services, and a commitment to Sharia principles. Thus, Indonesia's Islamic banking sector demonstrates the potential to become a leader in the global Islamic economy, expanding its market share and increasing its contribution to the global economy (Windasari et al., 2022).

Data from the Financial Services Authority (OJK) in 2024 reports that the development of Islamic banking over the past few years has seen significant progress. This is evidenced by the data in the table below.

Years	Number of Islamic Commercial Banks (BUS)	Number of Sharia Business Units (UUS)
2019	14	20
2020	13	26
2021	13	27
2022	13	27
2023	13	27

Source: Financial Services Authority, 2024

Although Islamic banks have recorded impressive growth in market share and digital innovation, these significant developments in the digital ecosystem bring with them a greater collective responsibility. This is because the ease of access to digital services is not necessarily accompanied by an increase in customers' capacity to deal with social engineering manipulation, and customers' perceptions and preparedness regarding social engineering-based fraud threats do not seem to be aligned (Wilson et al., 2024). This situation indirectly makes them easy targets for increasingly sophisticated cybercriminals. Fraudsters often impersonate bank representatives via phone, text messages (SMS/smishing), and email (phishing) (Yaqoob et al., 2023), or social media, using various tactics such as prize offers, fake emergency notifications, or urgent account verification requests (Polyzos et al., 2023). The success of these scams often depends on the perpetrators' ability to convince victims and exploit their lack of understanding regarding bank security procedures, as well as their high level of anxiety regarding potential financial loss (Asyhar & Permana, 2023). Additionally, the level of customer trust in Islamic banks—which is essential for their growth and customer loyalty—must also be considered a crucial factor. This trust can be a double-edged sword: on one hand, it builds loyalty, but on the other, it risks being exploited by fraudsters if not balanced by strong security literacy. Therefore, the roles of security literacy, fraud concern levels, and trust in Islamic banks in mitigating these risks warrant further exploration (Mohd Thas Thaker et al., 2024).This situation limits the choices of non-Muslim customers, who tend to seek more specific and diverse financial solutions tailored to their needs.

This study aims to conduct an in-depth analysis of the influence of Islamic banking security literacy, the level of fraud concern, and trust in Islamic banks on customers' verification responses when faced with various social engineering tactics (Legass & Durmuş, 2024a). Understanding these factors is expected to provide valuable insights for Islamic banks in designing more effective education and communication strategies to enhance customer awareness and resilience against online fraud threats, particularly in Indonesia (Zakiy, 2021). Thus, this study is expected to contribute to efforts to create a safer and more trustworthy Islamic banking transaction environment for all customers.

Previous studies have consistently shown that security literacy plays a crucial role in shaping cybersecurity behavior (Baltuttis et al., 2024), individuals with a good understanding of digital risks tend to be more vigilant and better able to recognize and respond effectively to various social engineering threats. Education on fraud tactics has been shown to reduce compliance with malicious requests, while levels of concern regarding fraud also encourage the adoption of protective measures (Wong et al., 2022). Nevertheless, fraudulent schemes often succeed, primarily due to victims' limited understanding of banking security procedures and their high anxiety regarding potential financial loss (Ma & McKinnon, 2022). In this context, active verification by customers becomes crucial, reflecting critical thinking and caution in verifying received information. On the other hand, in Islamic banking, which upholds the principles of justice, transparency, and ethical values, the level of customer trust in the bank is also a key factor (Abu ALHaija et al., 2024). This trust, while essential for loyalty, can influence how customers evaluate communications that appear to originate from the bank, including potential susceptibility to manipulative messages (Álvarez-González & Otero-Neira, 2023). Therefore, the interaction between security literacy, levels of fraud concern, and trust in Islamic banks in shaping customers' verification responses to various social engineering tactics still requires further exploration, especially given the current dynamics and developments in the Islamic banking system in Indonesia.

Although the literature on cybersecurity, online fraud, and financial literacy in the banking sector has grown rapidly, there are still several significant gaps that have not been adequately addressed (Laxman et al., 2024). First, most studies focus on conventional banking systems, while research on Islamic banking remains limited. This results in a lack of understanding of the unique dynamics of Islamic banks, which prioritize the principles of justice, transparency, and religious values, as well as how these characteristics influence customers' responses to security risks, including social engineering (Cele & Kwenda, 2025). Second, previous research generally only addressed one or two types of fraud schemes, such as phishing or vishing, without comprehensively examining how customers respond to the increasingly complex and diverse social engineering schemes, including smishing and pretexting (Salloum et al., 2021). Third, there is a lack of studies that simultaneously examine three key variables—security literacy, levels of concern regarding fraud, and trust in Islamic banks—in shaping customers' verification responses (Uddin, 2022). Yet, these three factors are believed to interact with one another and collectively influence how customers handle potential fraud. Therefore, research is needed to fill this gap to provide theoretical and practical contributions toward strengthening customer protection systems in the Islamic banking sector.

The novelty of this study lies in three main aspects that simultaneously fill gaps in the existing literature. First, this study focuses specifically on the context of Islamic banking, which has thus far been rarely addressed in research on cybersecurity and customer protection. In fact, Islamic banks have operational characteristics and customer relationships rooted in religious values and ethics, which can influence customers' perceptions and responses to social engineering threats (Farrag et al., 2022). Second, this study offers a comparative approach to customers' verification responses when facing various forms of digital fraud, ranging from phishing, vishing, and smishing to pretexting. Previous studies by Legass & Durmuş, (2024b) tended to be limited to one or two types of schemes, thus failing to provide a comprehensive picture of response differences based on the type of attack faced. Third, this study combines three key variables cybersecurity literacy, level of concern regarding fraud, and trust in Islamic banks to be analyzed simultaneously in influencing customers' verification responses. This approach offers a new contribution in explaining how cognitive (literacy), affective (concern), and relational (trust) factors interact to shape customers' cybersecurity behavior, particularly in the Islamic banking sector, which is rapidly expanding in the digital era (Alshurafat et al., 2024).

This study is expected to make significant contributions both theoretically and practically. From a theoretical perspective, this study expands the literature on cybersecurity behavior by integrating the context of Islamic banking an area that has been under-explored and highlights the role of Sharia values and the level of trust in banks in shaping customers' security responses to various social engineering tactics (Afzal et al., 2025). Additionally, this research offers a deeper understanding of the interaction between security literacy, concerns about fraud, and trust in Islamic banks in influencing customers' verification responses, and provides a comparative analysis of various fraud tactics such as phishing, vishing, smishing, and pretexting (Yusfiarto et al., 2024). Practically, the results of this study are relevant for Islamic banks to design more effective and context-specific security education and risk communication strategies, as well as to develop adaptive verification protocols based on the type of fraud scheme and customer characteristics. This study also provides valuable

input for regulators such as the OJK in formulating cybersecurity policies that are better suited to the Islamic banking ecosystem, while helping banks strengthen their protection systems and operational risk management against the ever-evolving threat of digital fraud.

2. LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

Customer Verification Responses

Customer Verification Responses to Various Social Engineering Tactics refer to specific actions taken by bank customers to verify the authenticity of identities, information, or requests when confronted with psychological manipulation tactics (social engineering) from unknown or potentially fraudulent parties (Daniel Ajiga et al., 2024). As an active self-defense mechanism, these responses vary depending on the method, ranging from ignoring suspicious messages, asking for clarification, refusing to provide sensitive information without verification through the bank's official channels, cross-checking information, to reporting the incident. Their effectiveness is influenced by understanding of the methods, security literacy, concerns about fraud, the ability to recognize manipulation tactics, and acting rationally (James & Garnett, 2024).

Customers' Verification Responses to Various Social Engineering Tactics can be measured through three general indicators: Frequency of Active Verification Actions, which reflects how often customers take the initiative to verify information when receiving suspicious communications through various channels such as asking for clarification or independently seeking out the bank's official contact information. Second, Compliance with Bank Security Guidelines measures the extent to which customers follow the bank's security procedures regarding verification, such as refusing to provide sensitive information over the phone or always verifying promotions through official channels. Third, Diligence in Evaluating Requests measures the level of caution and critical analysis customers apply to suspicious information or requests, including the ability to identify inconsistencies or emotional manipulation tactics (Grassegger & Nedbal, 2021).

Research by (Momoh et al., 2023) on the psychology of social engineering emphasizes that the success of attacks often depends on the exploitation of emotions and a lack of critical thinking on the part of the victim. Effective verification involves critical thinking and a refusal to act hastily. Additionally, previous research (Gallo et al., 2024) found that users who are more vigilant and have a better understanding of phishing tactics (aspects of security literacy that underpin verification) are less likely to fall victim.

Security Literacy

Cybersecurity literacy is an individual's ability to understand, evaluate, and apply cybersecurity principles and practices to protect themselves and their digital assets from threats (Nguyen et al., 2024). It goes beyond theoretical knowledge, encompassing practical skills, positive attitudes, situational awareness, and self-confidence. Individuals with high literacy are able to recognize threats, understand security principles, take proactive preventive measures, evaluate online information, and respond to threats in various situations (Radanliev, 2024). Cybersecurity literacy is a dynamic capability that requires continuous development and updating (Thomas & Sule, 2023).

The three indicators of cybersecurity literacy identified in previous research (Yovo & Gnedeka, 2023) are cybersecurity knowledge, cybersecurity behavior, and awareness of cybersecurity risks. First, security knowledge: this indicator measures an individual's understanding of basic cybersecurity concepts, common threats (such as phishing, malware, and social engineering), security principles (e.g., strong passwords, data privacy), and recommended security practices. Second, Security Behavior: This indicator measures the actual actions individuals take in their digital lives to protect themselves and their assets. Examples include the frequency of using strong and unique passwords, enabling two-factor authentication, the habit of verifying suspicious information, and responding to security alerts (Li & Liu, 2021). Finally, Awareness of Security Risks: This indicator measures individuals' understanding and perception of various cybersecurity threats and their potential impacts. This includes recognizing vulnerabilities in oneself and the systems used, as well as understanding the consequences of unsafe behavior. This awareness motivates individuals to take preventive actions (Krawczyk-soko, 2020).

Based on previous research conducted by (Khando et al., 2021) it was found that security knowledge (as a component of security literacy) is positively correlated with security behavior. Although it does not specifically address social engineering or verification, this study indicates that a better understanding of security tends to lead to safer actions. Additionally, research by (AlDaajeh et al., 2022) indicates that security training and education (aimed at improving literacy) can enhance awareness and understanding of threats, which in turn can influence user behavior, including the likelihood of being more cautious and performing verification. Furthermore, research (Montañez et al., 2022) indicates that increased knowledge of social engineering tactics significantly reduces the likelihood of users complying with malicious requests, which can be considered an effective form of verifying response (verifying the legitimacy of a request before acting). Based on the statements above, the proposed hypothesis is as follows:

H1: Security literacy has a significant effect on customers' verification responses when faced with various social engineering tactics.

Level of Concren About Fraud

The level of fraud concern refers to the degree of anxiety or fear an individual feels about the possibility of becoming a victim of fraud, whether online or offline. It is subjective in nature and is influenced by experience, risk awareness, information, and psychological characteristics. High levels of concern drive vigilance, skepticism toward suspicious requests, and the motivation to prevent financial loss or the compromise of personal data. While protective, excessive concern can lead to stress. This psychological aspect is crucial for understanding an individual's response to potential fraud threats (Lazarus et al., 2023).

According to research findings (Cao & Zhang, 2021) The level of fraud concern can be measured through three general indicators. First, Perceived Risk of Fraud reflects how individuals estimate the likelihood of fraud occurring and the magnitude of potential losses that may arise, including beliefs about the prevalence of fraud, feelings of vulnerability, and assessments of the danger posed by various types of fraud. Second, Cognitive Anxiety Related to Fraud measures how often and intensely individuals think about or feel anxious regarding the possibility of becoming a victim of fraud, such as concerns about the security of personal information or distrust of unfamiliar communications. Third, Fraud Avoidance Behavior observes the concrete actions individuals take to avoid potential fraud due to their concerns, such as being extremely cautious when providing personal information or avoiding certain online transactions.

Research in the psychology of fraud (Hassan et al., 2024) indicates that perceptions of risk and concerns about becoming a victim of fraud are key motivators for individuals to adopt protective behaviors. These behaviors may include more careful verification measures when encountering suspicious situations. These findings are also consistent with research conducted by (Hossain & Siddiqua, 2022) which shows that emotions such as the fear of losing money can influence financial decision-making. In the context of fraud, the fear of losing assets can encourage customers to be more cautious and perform verification. Based on these statements, the proposed hypothesis is as follows:

H2: The level of fraud concern influences customers' verification responses when facing various social engineering tactics.

Trust

Trust can be defined as a person's belief or sense of confidence in the integrity, competence, or truthfulness of an individual, group, agent, or system (Lewis & Marsh, 2022). Trust encompasses the expectation that the trusted party will act in a predictable, reliable manner that aligns with established expectations (Gkinko & Elbanna, 2023). Trust is crucial in various contexts, including personal relationships, business, government, and financial services such as banking. In the Sharia context, trust is vital to the reputation of Sharia banks; by prioritizing quality service, effective communication, and a commitment to Sharia principles, banks can build and maintain customer trust, thereby strengthening their reputation, performance, and long-term success (Junaidi et al., 2022).

Trust in Islamic banks is a crucial dimension of the customer-bank relationship, as evidenced by several key indicators adapted from the literature relevant to operational and cybersecurity contexts, as demonstrated in a study by (Chowdhury et al., 2022). First, Sharia integrity and compliance reflect customers' confidence that the bank's operations adhere to Islamic principles (fair, honest, transparent, and supervised by the Sharia Supervisory Board), fostering trust in the bank's official security advisories and skepticism toward suspicious

communications. Second, service competence and reliability measure customers' confidence in the professionalism of Islamic banks in providing efficient, secure, and reliable services, including the management of technology and security systems. These capabilities influence customers' confidence in the bank's fraud protection measures. Finally, good faith and customer protection measure the perception that the bank actively cares about customers' interests and financial security, thereby encouraging proactive reporting of suspicious activities because customers are confident the bank will respond effectively. These three indicators synergistically build a solid foundation of customer trust, influencing their verification-oriented behavior when facing social engineering threats (Garcia-Perez et al., 2023).

Based on previous research by Kim et al., (2024) which revealed that trust has a significant influence on the adoption of e-banking. Customer trust can encourage them to continue using digital services despite the risks, including the risk of social engineering-based fraud. This aligns with research by Cookman (2023) which explains that customers with a high level of trust in banking institutions tend to be more compliant with verification procedures and more vigilant against fraud attempts. Therefore, the following hypothesis is proposed:

H3: Trust has a positive influence on customers' verification responses when facing various social engineering tactics.

3. METHODOLOGY

This study employs an associative quantitative research method. According to Sugiyono (2019), associative quantitative research aims to identify the relationship between two or more variables. The study population consists of Islamic bank customers who use mobile banking services in Indonesia. The sample was selected using purposive sampling. Data collection was conducted via a Google Forms questionnaire, which was then directly distributed to the respondents. In this method, the sample size was determined using Ferdinand's formula because the exact size of the population in this study is unknown. According to Ferdianand (2014) the sample size is obtained by multiplying the number of research indicators by 5 to 10. Therefore, the sample size for this study was determined as follows: n = 12 × 10 = 120 samples.

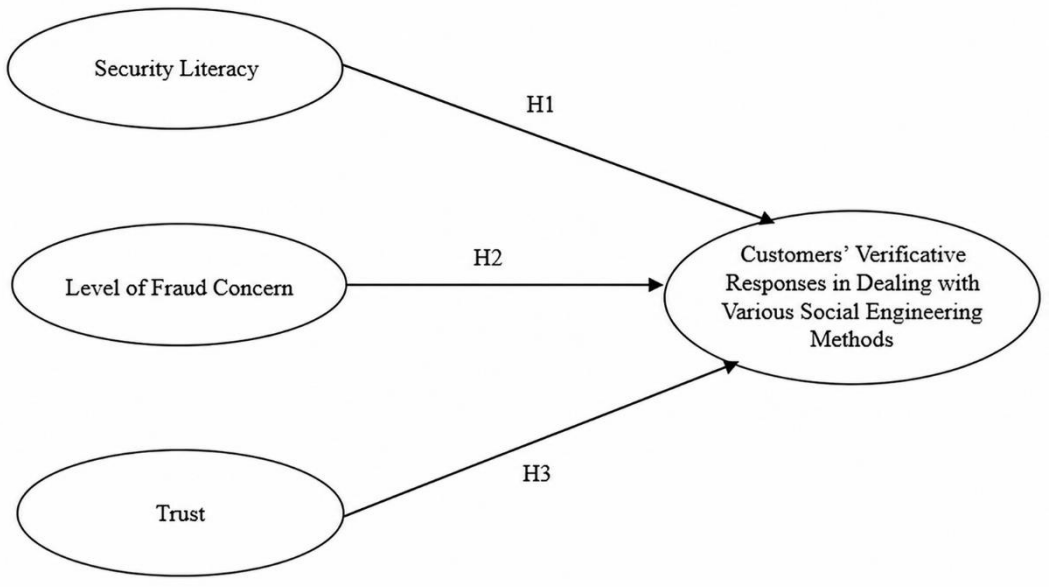


Figure 3.1 Customer Verification Response Model

This study employs variance-based structural equation modeling. It uses Partial Least Squares Structural Equation Modeling (SEM-PLS) to evaluate the measurement model and structural model and to test the research hypotheses. In addition, this study uses PLS to address the issue of non-normally distributed data.

4. DATA ANALYSIS AND INTERPRETATION

4.1. Respondent Demographics

Table 1.1 shows that the majority of respondents in this study are active customers of Islamic banks and have experience or knowledge regarding digital security risks (for example, they have received security notifications from the bank or encountered attempted fraud).

Table 1. Respondent Characteristics

Profile	Total	Percentage (%)
Gender		
Male	75	62,5%
Female	45	37,5%
Age		
18-25 Years	78	65%
26-35 Years	19	15,8%
36-45 Years	18	15%
>46 Years	5	4,2%
Highest Level of Education		
Elementary/Middle/High School	65	54,2%
Bachelor's/Master's/Doctorate	48	40%
Other	7	7,8%

Source: Primary Data Processing, Smart PLS4

4.2. Validity and Reliability

Validity and reliability tests are prerequisites that must be conducted before performing PLS-SEM analysis. The methods that can be used include those for assessing convergent validity, such as average variance extracted (AVE), factor loadings, and measures of reliability (composite reliability for this study).

Table 2. Validity and Reliability of the Measurement Model

Construct	Items	Loadings	Composite Reliability	AVE
Customer Verification Response			0.874	0.634
	Contact the bank directly if you receive a suspicious message	0.767		
	Follow the bank's security guidelines	0.828		
	Carefully review any request for personal information	0.782		
	Do not immediately trust requests for information from parties without official verification	0.808		
Security Awareness			0.861	0.608
	Banks never ask for PINs or OTPs over the phone or via text message.	0.850		
	Do not click on suspicious links.	0.708		
	It is dangerous to share personal information via social media.	0.774		
	Be wary of messages offering prizes in exchange for data.	0.779		
			0.884	0.605

	High risk of digital fraud.	0.775		
	Digital banking services carry potential security risks	0.795		
Fraud Concern Level	Concerned when accessing the bank via the internet/app.	0.705		
	Anxious when receiving unknown messages/calls.	0.777		
	Do not conduct online transactions if you feel security is not guaranteed.	0.831		
			0.902	0.606
	Sharia banks operate in accordance with Sharia principles.	0.762		
	Maintain integrity in every service provided to customers.	0.809		
	Reliable security systems and technology to protect customer data.			
Customer Trust	Capable of handling banking issues quickly and accurately.	0.770		
	Protect customers' interests and security.			
	Transparent and honest information.	0.773		
		0.769		
		0.787		

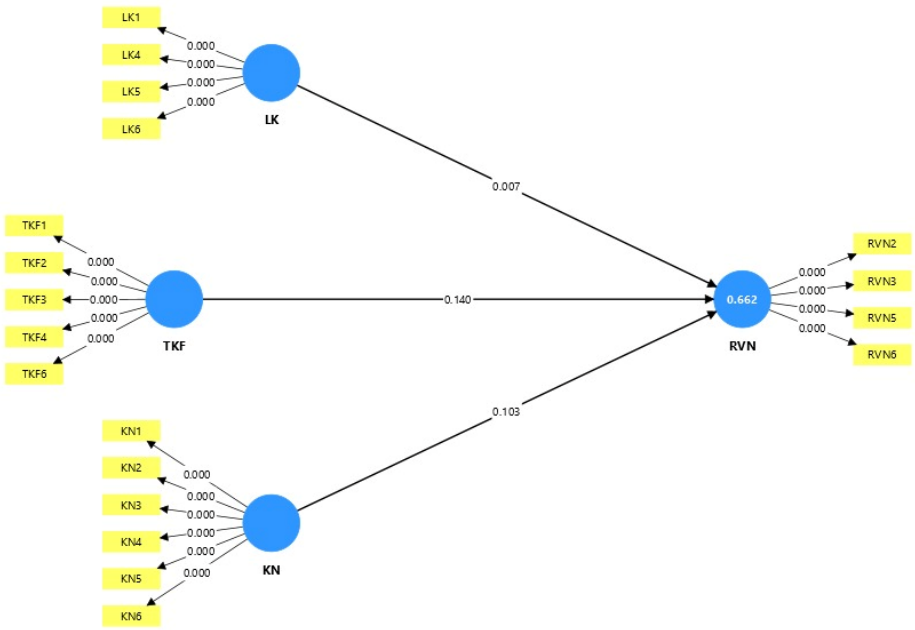
Source: Primary data processed using SmartPLS, 2025

Based on the table, it is evident that the validity and reliability tests for this study were conducted twice to ensure valid and reliable results. In the first round of testing, several constructs were excluded because they were not valid or reliable. In the second round of testing, valid and reliable constructs or variables were identified. As shown in the table above, the AVE values are greater than 0.50, indicating validity. Furthermore, these constructs are considered reliable because their composite reliability values exceed 0.70.

Hypothesis Testing

	STDEV	t-Statistic	P-Value	Hypothesis
LK > RVN	0.173	1.629	0.103	H1 : Rejected
TKF > RVN	0.152	2.679	0.007	H2 : Accepted
KN > RVN	0.143	1.477	0.140	H3 : Rejected

Source: Processed by the author, 2025



Ficture 1. SEM PLS Path Analysis Results

5. DISCISSION

The data analysis results indicate that the findings regarding the first hypothesis namely, that security literacy does not influence customers' verification responses when faced with various social engineering tactics are consistent with previous research (Washo, 2021). This finding suggests that even though customers possess knowledge of the basic principles of digital security, such knowledge does not automatically translate into tangible defensive behavior (Putrevu & Mertzanis, 2024). In the context of behavioral psychology, this phenomenon is known as the knowledge-behavior gap a condition where an individual understands a risk but fails to take appropriate preventive actions. This may be caused by a low level of internalization or critical awareness regarding digital fraud risks, resulting in knowledge remaining purely cognitive without the urgency to act (Yu et al., 2022). Additionally, customers' high trust in the security systems of Islamic banks may also be a factor that reduces vigilance (Qatawneh & Makhlouf, 2025). This is also stated in a study conducted by Nordhoff & Hagenzieker, (2024) which found that customers who place excessive trust (overtrust) in banks or technology tend to feel secure and do not feel the need to actively verify messages or requests for information they receive, even though they are aware of the potential dangers of social engineering. Situational factors can also be a cause; for example, customers may be in a hurry, tired, or distracted when receiving a social engineering attack, leading to reduced vigilance. On the other hand, digital fraud schemes are becoming increasingly sophisticated and often exploit the emotional vulnerabilities of victims, such as fear, panic, or even trust in authority figures (Zhou et al., 2024). In such situations, financial literacy alone is insufficient without emotional intelligence and the resolve to verify information.

Furthermore, the second hypothesis indicates that the level of concern about fraud has a significant effect on customers' verification responses when faced with various social engineering tactics. The higher a person's level of concern about potential fraud, the more likely that individual is to take protective measures to safeguard themselves (Cross, 2021). In the banking context, this is reflected in verification responses—cautious actions such as double-checking information, not immediately trusting suspicious messages, and confirming with the bank before providing personal data (Palma et al., 2024). Customers who feel anxious or worried about becoming victims of fraud tend to be more vigilant against various social engineering tactics, such as phishing, vishing, or smishing (Pangrazio & Bunn, 2024). This concern can trigger a self-defense mechanism in the form of increased alertness and caution when receiving unusual or suspicious information. This aligns with Protection Motivation Theory, which states that the perception of a threat (in this case, concern about fraud) will prompt individuals to take protective actions (Wu et al., 2024).

Finally, the third hypothesis suggests that trust does not have a significant effect on customers' verification responses when faced with various social engineering tactics (Admass et al., 2024). Although trust in banking institutions is a crucial element in building long-term relationships between banks and customers,

the level of trust does not always correlate directly with customers' vigilance or protective behavior in the context of digital fraud (Alawida et al., 2022). When facing social engineering tactics, verifiable responses are more triggered by direct threat factors, such as concerns about losing money or personal data, rather than by trust in the institution (Wu et al., 2024). Customers with high levels of trust in the bank may feel safe and protected, making them more likely to skip verifying suspicious information because they assume all communications from the bank are inherently safe (Bugandwa et al., 2021). Additionally, in the digital age, criminals often impersonate the bank with remarkable conviction. Thus, trust in the bank alone is insufficient to distinguish between genuine and fraudulent communications (Sogenbits & Turksen, 2024). Therefore, trust alone is insufficient to influence customers' decisions to take verifying actions. This finding is also consistent with several previous studies, one of which states that trust tends to influence loyalty or satisfaction but does not directly influence defensive behavior or vigilance against the risk of fraud (Cooke & Marshall, 2024).

6. CONCLUSION AND RECOMMENDATIONS

The results of the study indicate that security literacy does not have a significant effect on customers' verification responses, meaning that even though customers understand the basic principles of digital security, this knowledge does not always translate into active and preventive verification actions, reflecting the existence of a knowledge-behavior gap. Conversely, the level of concern regarding fraud has a positive and significant influence on verification responses; the higher a customer's anxiety or vigilance regarding potential fraud, the greater their tendency to take protective actions such as verifying received information. Meanwhile, trust in Islamic banks does not significantly influence verification responses, as high levels of trust can actually lead to overconfidence (overtrust), causing customers to become less vigilant and more vulnerable to fraud disguised as official communication from the bank.

For future research, it is recommended to include mediating and moderating variables such as self-efficacy, digital anxiety, or trust in technology to further explore the psychological mechanisms that influence customers' verification responses to digital fraud schemes. Additionally, a longitudinal approach can be employed to observe the dynamics of changes in customer behavior over time, particularly before and after educational interventions by the bank. Future research could also expand the respondent pool to include rural areas, regions outside Java, or Islamic boarding school communities to examine the role of religious values in shaping customers' levels of digital trust and vigilance. Equally important, a comparative study between Islamic banks and conventional banks can be conducted to determine whether the same patterns of influence from these variables also apply in the context of non-Islamic banking, thereby yielding a more comprehensive and practical understanding.

REFERENCES

Abu ALHaija, E., Lataifeh, A., Al-Haraizah, A., Meqdade, M., & Yousef, N. (2024). Ethical banking practices: a comparative analysis of Islamic and conventional banks in GCC countries. *International Journal of Ethics and Systems*, *December*. https://doi.org/10.1108/IJOES-08-2024-0254

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*(September 2023), 100031. https://doi.org/10.1016/j.csa.2023.100031

Afzal, M., Meraj, M., Kaur, M., & Shamim Ansari, M. (2025). How does cybersecurity awareness help in achieving digital financial inclusion in rural India under escalating cyber fraud scenario? *Journal of Cyber Security Technology*, *9*(2), 88–126. https://doi.org/10.1080/23742917.2024.2347674

Ahmed, S., & Sur, S. (2023). Change in the uses pattern of digital banking services by Indian rural MSMEs during demonetization and Covid-19 pandemic-related restrictions. *Vilakshan - XIMB Journal of Management*, *20*(1), 166–192. https://doi.org/10.1108/xjm-09-2020-0138

Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(10), 8176–8206. https://doi.org/10.1016/j.jksuci.2022.08.003

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Raymond Choo, K. K. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers and Security*, *119*. https://doi.org/10.1016/j.cose.2022.102754

Alshurafat, H., Arabiat, O., & Shehadeh, M. (2024). The intention to adopt metaverse in Islamic banks: an integrated theoretical framework of TAM and religiosity intention model. *Journal of Islamic Marketing*, *February*. https://doi.org/10.1108/JIMA-10-2023-0310

Álvarez-González, P., & Otero-Neira, C. (2023). Mergers and acquisitions success: examining customer loyalty. *Marketing Intelligence & Planning*, *41*(1), 48–61. https://doi.org/10.1108/MIP-02-2022-0074

Asyhar, A. N., & Permana, D. (2023). The Impact of Religious Obligation, Sharia Financial Literacy, and Promotion on Decision to Use the BSI Hasanah Card in Millenials Through Customer Awareness as a Mediation Variable. *International Journal of Innovative Science and Research Technology*, *8*(2), 1053–1060. www.ijisrt.com

Baltuttis, D., Teubner, T., & Adam, M. T. P. (2024). A typology of cybersecurity behavior among knowledge workers. *Computers & Security*, *140*(January), 103741. https://doi.org/10.1016/j.cose.2024.103741

Bugandwa, T. C., Kanyurhi, E. B., Bugandwa Mungu Akonkwa, D., & Haguma Mushigo, B. (2021). Linking corporate social responsibility to trust in the banking sector: exploring disaggregated relations. *International Journal of Bank Marketing*, *39*(4), 592–617. https://doi.org/10.1108/IJBM-04-2020-0209

Cao, G., & Zhang, J. (2021). Guanxi, overconfidence and corporate fraud in China. *Chinese Management Studies*, *15*(3), 501–556. https://doi.org/10.1108/CMS-04-2020-0166

Cele, N. N., & Kwenda, S. (2025). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime*, *32*(1), 31–48. https://doi.org/10.1108/JFC-10-2023-0263

Chowdhury, N., Katsikas, S., & Gkioulos, V. (2022). Modeling effective cybersecurity training frameworks: A delphi method-based study. *Computers & Security*, *113*, 102551. https://doi.org/10.1016/j.cose.2021.102551

Cooke, D., & Marshall, A. (2024). Money laundering through video games, a criminals' playground. *Forensic Science International: Digital Investigation*, *50*(February), 301802. https://doi.org/10.1016/j.fsidi.2024.301802

Cookman, D. (2023). European approach to remote customer onboarding solutions. *Journal of Money Laundering Control*, *26*(7), 213–223. https://doi.org/10.1108/JMLC-08-2023-0140

Cross, C. (2021). Theorising the impact of COVID-19 on the fraud victimisation of older persons. *The Journal of Adult Protection*, *23*(2), 98–109. https://doi.org/10.1108/JAP-08-2020-0035

Daniel Ajiga, Patrick Azuka Okeleke, Samuel Olaoluwa Folorunsho, & Chinedu Ezeigweneme. (2024). Designing Cybersecurity Measures for Enterprise Software Applications to Protect Data Integrity. *Computer Science & IT Research Journal*, *5*(8), 1920–1941. https://doi.org/10.51594/csitrj.v5i8.1451

Farrag, D. A. R., Murphy, W. H., & Hassan, M. (2022). Influence of category attitudes on the relationship between SERVQUAL and satisfaction in Islamic banks; the role of disruptive societal-level events. *Journal of Islamic Marketing*, *13*(4), 843–867. https://doi.org/10.1108/JIMA-08-2020-0228

Gallo, L., Gentile, D., Ruggiero, S., Botta, A., & Ventre, G. (2024). The human factor in phishing: Collecting and analyzing user behavior when reading emails. *Computers and Security*, *139*(December 2023), 103671. https://doi.org/10.1016/j.cose.2023.103671

Garcia-Perez, A., Cegarra-Navarro, J. G., Sallos, M. P., Martinez-Caro, E., & Chinnaswamy, A. (2023). Resilience in healthcare systems: Cyber security and digital transformation. *Technovation*, *121*(May 2022), 102583. https://doi.org/10.1016/j.technovation.2022.102583

Gkinko, L., & Elbanna, A. (2023). Designing trust: The formation of employees' trust in conversational AI in the digital workplace. *Journal of Business Research*, *158*(January), 113707. https://doi.org/10.1016/j.jbusres.2023.113707

Grassegger, T., & Nedbal, D. (2021). The role of employees' information security awareness on the intention to resist social engineering. *Procedia Computer Science*, *181*(2019), 59–66. https://doi.org/10.1016/j.procs.2021.01.103

Hassan, S., Ahmad, R., Katuk, N., Ghazali, N. N., Aripin, J. A., & Ali, F. (2024). Staying One Step Ahead: Exploring Protection Motivation Theory to Combat Cyber-fraud Among E-services Users. *Procedia Computer Science*, *234*(2023), 1364–1371. https://doi.org/10.1016/j.procs.2024.04.011

Hossain, T., & Siddiqua, P. (2022). Exploring the influence of behavioral aspects on stock investment decision-making: a study on Bangladeshi individual investors. *PSU Research Review*, *8*(2), 467–483. https://doi.org/10.1108/PRR-10-2021-0054

James, T. S., & Garnett, H. A. (2024). The Voter Experience Around the World: A Human Reflexivity Approach. *Representation*, *60*(2), 231–252. https://doi.org/10.1080/00344893.2023.2290714

Junaidi, J., Wicaksono, R., & Hamka, H. (2022). The consumers' commitment and materialism on Islamic

banking: the role of religiosity. *Journal of Islamic Marketing*, *13*(8), 1786–1806. https://doi.org/10.1108/JIMA-12-2020-0378

Khando, K., Gao, S., Islam, S. M., & Salman, A. (2021). Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers and Security*, *106*, 102267. https://doi.org/10.1016/j.cose.2021.102267

Kim, L., Wichianrat, K., & Yeo, S. F. (2024). An integrative framework enhancing perceived e-banking service value: A moderating impact of e-banking experience. *Journal of Open Innovation: Technology, Market, and Complexity*, *10*(3), 100336. https://doi.org/10.1016/j.joitmc.2024.100336

Krawczyk-soko, I. (2020). *Awareness of network security and customer value – The company and customer perspective*. *January*.

Laxman, V., Ramesh, N., Jaya Prakash, S. K., & Aluvala, R. (2024). Emerging threats in digital payment and financial crime: A bibliometric review. *Journal of Digital Economy*, *3*(April), 205–222. https://doi.org/10.1016/j.jdec.2025.04.002

Lazarus, S., Whittaker, J. M., McGuire, M. R., & Platt, L. (2023). What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021). *Journal of Economic Criminology*, *2*(March), 100013. https://doi.org/10.1016/j.jeconc.2023.100013

Legass, H. A., & Durmuş, M. E. (2024a). Factors determining the adoption of mobile banking in Ethiopian Islamic banks: extension of technology acceptance model (TAM). *Journal of Islamic Accounting and Business Research*, *April*. https://doi.org/10.1108/JIABR-02-2024-0051

Legass, H. A., & Durmuş, M. E. (2024b). Factors determining the adoption of mobile banking in Ethiopian Islamic banks: extension of technology acceptance model (TAM). *Journal of Islamic Accounting and Business Research*, *November 2024*. https://doi.org/10.1108/JIABR-02-2024-0051

Lewis, P. R., & Marsh, S. (2022). What is it like to trust a rock? A functionalist perspective on trust and trustworthiness in artificial intelligence. *Cognitive Systems Research*, *72*(February 2021), 33–49. https://doi.org/10.1016/j.cogsys.2021.11.001

Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, *7*, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Ma, K. W. F., & McKinnon, T. (2022). COVID-19 and cyber fraud: emerging threats during the pandemic. *Journal of Financial Crime*, *29*(2), 433–446. https://doi.org/10.1108/JFC-01-2021-0016

Mohd Thas Thaker, H., Lelchumanan, B., Ah Mand, A., & Khaliq, A. (2024). Push – pull – mooring determinants of non-Muslims' withdrawal from Islamic banking: evidence from Malaysia. *International Journal of Islamic and Middle Eastern Finance and Management*, *17*(1), 195–212. https://doi.org/10.1108/IMEFM-04-2023-0144

Momoh, I., Adelaja, G., & Ejiwumi, G. (2023). *Analysis of the Human Factor in Cybersecurity: Identifying and Preventing Social Engineering Attacks in Financial Institution*. *December*. https://doi.org/10.13140/RG.2.2.35640.52489

Montañez, R., Atyabi, A., & Xu, S. (2022). Social engineering attacks and defenses in the physical world vs. cyberspace: A contrast study. *Cybersecurity and Cognitive Science*, 3–41. https://doi.org/10.1016/B978-0-323-90570-1.00012-7

Nguyen, T. T., Tran, T. N. H., Do, T. H. M., Dinh, T. K. L., Nguyen, T. U. N., & Dang, T. M. K. (2024). Digital literacy, online security behaviors and E-payment intention. *Journal of Open Innovation: Technology, Market, and Complexity*, *10*(2), 100292. https://doi.org/10.1016/j.joitmc.2024.100292

Nordhoff, S., & Hagenzieker, M. (2024). "I will raise my hand and say 'I over-trust Autopilot'. I use it too liberally" – Drivers' reflections on their use of partial driving automation, trust, and perceived safety. *Transportation Research Part F: Traffic Psychology and Behaviour*, *107*(May), 1105–1124. https://doi.org/10.1016/j.trf.2024.09.021

Palma, A., Acitelli, G., Marrella, A., Bonomi, S., & Angelini, M. (2024). A compliance assessment system for Incident Management process. *Computers & Security*, *146*(August), 104070. https://doi.org/10.1016/j.cose.2024.104070

Pangrazio, L., & Bunn, A. (2024). Assessing the privacy of digital products in Australian schools: Protecting the digital rights of children and young people. *Computers and Education Open*, *6*, 100187. https://doi.org/10.1016/j.caeo.2024.100187

Polyzos, E., Samitas, A., & Syriopoulos, K. (2023). Islamic banking, efficiency and societal welfare: a machine-learning, agent-based study. *International Journal of Islamic and Middle Eastern Finance and Management*, *16*(4), 777–801. https://doi.org/10.1108/IMEFM-04-2022-0144

Putrevu, J., & Mertzanis, C. (2024). The adoption of digital payments in emerging economies: challenges and policy responses. *Digital Policy, Regulation and Governance*, *26*(5), 476–500. https://doi.org/10.1108/DPRG-06-2023-0077

Qatawneh, A. M., & Makhlouf, M. H. (2025). Influence of smart mobile banking services on senior banks' clients intention to use: moderating role of digital accounting. *Global Knowledge, Memory and Communication*, *74*(3/4), 1028–1044. https://doi.org/10.1108/GKMC-01-2023-0018

Radanliev, P. (2024). Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology*, *9*(1), 1–51. https://doi.org/10.1080/23742917.2024.2312671

Salloum, S., Gaber, T., Vadera, S., & Shaalan, K. (2021). Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey. *Procedia Computer Science*, *189*(2019), 19–28. https://doi.org/10.1016/j.procs.2021.05.077

Sogenbits, T., & Turksen, U. (2024). Cracking the code: Unveiling carding crime through the darknet-acquired criminal carding manual and the business model canvas. *Journal of Economic Criminology*, *5*(April), 100071. https://doi.org/10.1016/j.jeconc.2024.100071

Thomas, G., & Sule, M.-J. (2023). A service lens on cybersecurity continuity and management for organizations' subsistence and growth. *Organizational Cybersecurity Journal: Practice, Process and People*, *3*(1), 18–40. https://doi.org/10.1108/ocj-09-2021-0025

Uddin, M. N. (2022). Apartment purchase under Shirkah-ul Milk and shariah compliance in Islamic banks: the perception of bankers and clients in Bangladesh. *Journal of Islamic Accounting and Business Research*, *13*(2), 197–219. https://doi.org/10.1108/JIABR-09-2020-0300

Washo, A. H. (2021). An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports*, *4*, 100126. https://doi.org/10.1016/j.chbr.2021.100126

Wilson, S., Hassan, N. A., Khor, K. K., Sinnappan, S., Abu Bakar, A. R., & Tan, S. A. (2024). A holistic qualitative exploration on the perception of scams, scam techniques and effectiveness of anti-scam campaigns in Malaysia. *Journal of Financial Crime*, *31*(5), 1140–1155. https://doi.org/10.1108/JFC-06-2023-0151

Windasari, N. A., Kusumawati, N., Larasati, N., & Amelia, R. P. (2022). Digital-only banking experience: Insights from gen Y and gen Z. *Journal of Innovation and Knowledge*, *7*(2), 100170. https://doi.org/10.1016/j.jik.2022.100170

Wong, L.-W., Lee, V.-H., Tan, G. W.-H., Ooi, K.-B., & Sohal, A. (2022). The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities. *International Journal of Information Management*, *66*(May), 102520. https://doi.org/10.1016/j.ijinfomgt.2022.102520

Wu, S., Chen, H., Hou, L., Zhang, G. (Kevin), & Li, C.-Q. (2024). Using Eye-Tracking to Measure Worker Situation Awareness in Augmented Reality. *Automation in Construction*, *165*(November 2023), 105582. https://doi.org/10.1016/j.autcon.2024.105582

Wu, X., Duan, R., & Ni, J. (2024). Unveiling security, privacy, and ethical concerns of ChatGPT. *Journal of Information and Intelligence*, *2*(2), 102–115. https://doi.org/10.1016/j.jiixd.2023.10.007

Yaqoob, I., Salah, K., Jayaraman, R., & Omar, M. (2023). Metaverse applications in smart cities: Enabling technologies, opportunities, challenges, and future directions. *Internet of Things*, *23*(April), 100884. https://doi.org/10.1016/j.iot.2023.100884

Yovo, K., & Gnedeka, K. T. (2023). Assess the level and the determinants of household food security in Togo: The food expenditures approach. *Scientific African*, *20*. https://doi.org/10.1016/j.sciaf.2023.e01685

Yu, H., Fletcher, M., & Buck, T. (2022). Managing digital transformation during re-internationalization: Trajectories and implications for performance. *Journal of International Management*, *28*(4), 100947. https://doi.org/10.1016/j.intman.2022.100947

Yusfiarto, R., Supriani, I., Mutmainah, L., Hamdani, L., Khoirunnisa, A. N., & Ibrahim, M. H. (2024). Enabling Islamic internet-only banks acceptance: an empirical analysis of the UTAUT framework and Islamic compliance. *Journal of Islamic Marketing*, *15*(10), 2669–2693. https://doi.org/10.1108/JIMA-02-2022-0057

Zakiy, M. (2021). The strategy of Islamic economic colleges to prepare their graduates to work in Islamic banks. *Higher Education, Skills and Work-Based Learning*, *11*(5), 1130–1142. https://doi.org/10.1108/HESWBL-01-2021-0010

Zhou, S., Sun, X., Wang, Q., Liu, B., & Burnett, G. (2024). Development of a measurement instrument for pedestrians' initial trust in automated vehicles. *International Journal of Human-Computer Studies*, *191*(August 2023), 103344. https://doi.org/10.1016/j.ijhcs.2024.103344