Asia Pacific Fraud Journal
E-ISSN: 2502-695X, ISSN: 2502-8731
Volume 10, Issue 1 (January-June) 2025
*Asia Pacific Fraud Journal now has been accredited "**SINTA 3**" by Ministry of Research and Technology of The Republic of Indonesia (No SK. 225/E/KPT/2022).*
Available online at: http://apfjournal.or.id/index.php/apf

Cyber Security Awareness, Knowledge and Behavior of Digital Banking Users in Salatiga

✉Salma Faundria Nagari & Surya Raharja
Master of Accounting Program, Faculty of Economics and Business,
Diponegoro University, Indonesia

ARTICLE INFORMATION
Article History:
Received September 30, 2024
Revised May 19, 2025
Accepted June 1, 2025

DOI:
10.21532/apfjournal.v10i1.398

ABSTRACT
Digital banking has become one of the fastest-growing technological advances in the banking sector. This study aims to analyze the relationship between cybersecurity awareness, knowledge, and behavior among digital banking users in Salatiga City. Using a quantitative approach, data were collected from 200 respondents and analyzed with SmartPLS 4. The results show that cybersecurity knowledge has a significant positive influence on both awareness and behavior. Awareness also directly affects behavior. However, awareness does not significantly mediate the relationship between knowledge and behavior. This implies that while awareness is important, knowledge plays a more dominant role in shaping users' cybersecurity behavior. This study contributes to the banking industry by providing insights to enhance user cybersecurity through targeted education and awareness programs. Additionally, it enriches the academic literature on cybersecurity behavior in the context of digital banking users, particularly in developing regions. Future research is encouraged to explore other influencing factors such as motivation, perceived risk, or institutional support.

Keywords: Cybersecurity Awarness, Banking, Cybersecurity Knowledge, Digital Banking.

How to Cite:
Nagari, S. F., & Raharja, S. (2025). Cyber Security Awareness, Knowledge and Behavior of Digital Banking Users in Salatiga. *Asia Pacific Fraud Journal, 10*(1), 15-29. http://doi.org/10.21532/apfjournal.v10i1.398.

✉Corresponding author :
Email: salmafaundria@gmail.com

1. INTRODUCTION

The increasing role of technology has a significant impact on everyday life. This advancement is no exception in the banking sector. Information and internet technology has the potential to provide many conveniences for companies to become more successful and become winners in a business environment that is always changing rapidly. As one of the largest financial institutions, banks continually seek new ways to leverage technological developments to enhance banking services. Research by Barquin et al. (2019) indicates that banking customers in Indonesia show the highest interest in digital banking facilities in Asia, with urban populations averaging two to three digital banking products. Ramadhan & Purwandari (2023) found several factors that contribute to the swift transition to digital banking services, including the rise in internet and smartphone usage, the push for digitization, and the growth of e-commerce. Examples of digital transformation in banking services include Automated Teller Machines (ATMs), Internet Banking, and Mobile Banking (IDX Channel, 2023). The increase in digital banking has coincided with a rise in digital transactions. In 2023, there was a notable increase of 9.88% in digital transactions compared to the previous period, totaling IDR 4,499.1 trillion (IDX Channel, 2023). Generally, digital transformation provides internet banking and mobile banking options for customers to facilitate transactions like balance checks, financial transactions, transaction history reviews, and various financial and non-financial services. Additionally, mobile and internet banking allow customers to transact anytime and anywhere via mobile devices and internet connections.

However, the opportunity for technological development in banking also presents new challenges, such as vulnerabilities to cybercrime (Johri & Kumar, 2023). For instance, data from the National Cyber and Crypto Agency (BSSN) reported 495 million cyber attacks in 2020, a fivefold increase from the previous year (OJK, 2020). Cybersecurity is a critical issue in banking due to the continuous rise in cyber threats and attacks, which can lead to significant financial losses. In the current digital transformation, banks are continuously enhancing the security of digital services, including improving the confidentiality of customer data. Many cyber attacks on banking systems occur because users of digital banking services, such as mobile and internet banking, are often unaware of potential cyber threats (Johri & Kumar, 2023). Banks must strengthen their cybersecurity policies to protect against attacks and enhance customer satisfaction. However, active awareness among digital banking customers regarding the importance of cybersecurity is also essential for self-protection against fraud and banking crimes. Awareness of cybersecurity is a vital parameter for protecting activities related to digital transactions in today's digital transformation era. It is essential to explore and understand the level of customers' awareness, knowledge, and behavior regarding their cyber security. Given this phenomenon, enhancing security measures by users of digital services is necessary to raise awareness about the potential misuse of personal data. This study aims to determine the importance of the relationship between awareness, knowledge, and customer behavior regarding cybersecurity protection in the digital banking transformation era.

2. LITERATURE REVIEW AND HYPOTHESIS

Digital Transformation in Banking

The digital revolution of Industry 4.0 is marked by accelerated technological innovations with enhanced computing capacity and easier access to digital technology. Various technological advancements such as Applied AI, Cloud and Edge Computing, Big Data Analytics, Digital Trust Technology, Distributed Ledger Technology (DLT), Quantum Computing, and Virtual Reality are

widely utilized to meet current needs (IDX Channel, 2023). Digital transformation in banking in Indonesia is guided by Bank Indonesia to ensure adaptive and sustainable development. With the increasing use of information technology in banking, both banking companies and customers need to improve their banking security policies. Over time, the development of cybersecurity must be enhanced because awareness and knowledge of cybersecurity alone are insufficient to anticipate the diverse and evolving cyber threats. Research by The European Union Agency for Network and Information Security, (2017)and the long elimination half-life of around 130 min. Vecuronium and rocuronium are steroidal compounds with an intermediate duration of action (DUR90% 50-60 min indicates that the weakest factor in cybersecurity is the users themselves, highlighting the need for systematic strengthening. Additionally, research by McCormac et al., (2017) found that a higher level of cyber threat resilience corresponds with better capabilities, knowledge, attitudes, and behaviors in mitigating cyber threats.

Cybersecurity Awareness

The current use of the internet has transformed how people manage their social lives. The growth of the internet, along with the rise of digital media, has changed learning, communication access, and economic transactions (Mai & Tick, 2021). However, many internet users still face information security risks due to various cyber threats, ranging from simple to severe attacks. Cybercrime that occurs must be anticipated through strong security implementation from various aspects, namely related to people, process or technology. Of the three aspects, people or humans are the weakest gap in the computer network system because of the careless and negligent nature of humans (Kementerian Keuangan Republik Indonesia, 2024). One primary factor in information security risk is individual cybersecurity awareness. Many banking cyber attacks occur because users of digital banking services like mobile and internet banking lack awareness of potential cyber threats (Johri & Kumar, 2023)). Hackers (individual or collective) usually tend to seek out the most vulnerable users, namely those who have less information and awareness of cybersecurity.

Cybersecurity Knowledge

The banking industry continually seeks to enhance protections against various potential cyber threats that could lead to data breaches. According to Sundareswaran et al. (2018), data theft threats have been increasing over time. In this case, all parties involved, including banks and customers, must engage in protecting banking information security data. Knowledge about cybersecurity is critical for protecting activities related to digital transactions (Zwilling et al., 2022). Knowledge encompasses everything understood through personal experience and increases with experience. Without adequate knowledge of cybersecurity, digital banking users lack a foundation for decision-making and determining actions to enhance cybersecurity. Cybersecurity knowledge is vital for proactive protection against cyber threats, thereby reducing the risk of crimes (Abawajy, 2014). Therefore, one form of protection against cyber threats is for users to possess cybersecurity knowledge and to explore cybersecurity skills when using digital technology (Misra & Khurana, 2017). Customers can acquire cybersecurity knowledge from various prior experiences and information provided by banking institutions.

Cybersecurity Behavior

Behavior is a reaction to stimuli from external or internal sources. It results from a person's experiences and interactions with their environment. Efforts to protect information technology within cybersecurity systems focus on the most significant vulnerabilities that may experience threats and attacks. The evolving trends of cyber crimes and

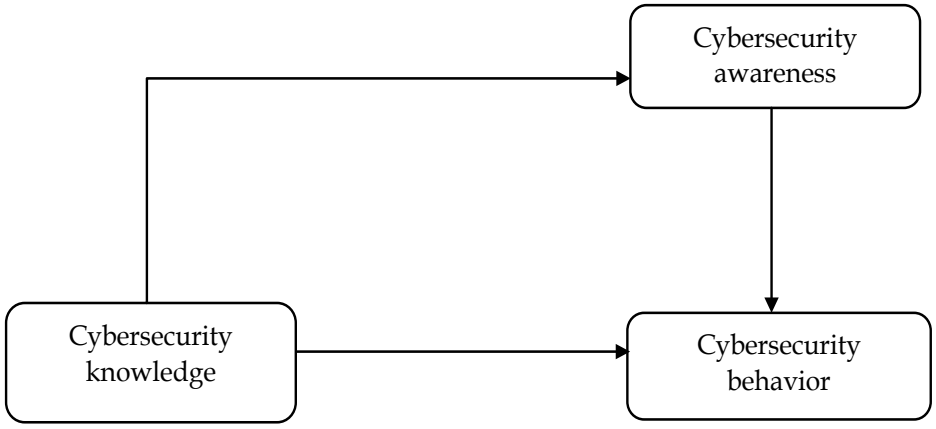
attacks in various sectors, including banking, highlight the increasing need for cybersecurity protection skills. These protections focus on the information technology devices used to avoid cyber threats like malware or data theft. Cybersecurity behavior can be defined as an individual's actions to secure or protect their personal information data. Prevention of fraud is an integrated effort that can reduce the factors that cause fraud (Sulistiyo & Yanti, 2022). Each person will make different decisions regarding actions to address problems, including managing cybersecurity in banking information technology. Understanding the cybersecurity behavior of digital banking users is an important step to protect individuals and organizations from phishing attacks and data breaches.

Several studies on cybersecurity have been conducted with varied results. Research by Al-Alawi & Al-Bassam, (2019) examined factors influencing cybersecurity awareness in banking, finding that cybersecurity knowledge and a security culture significantly impact awareness. Zwilling et al., (2022) studied the relationship between awareness, knowledge, and cybersecurity behavior within organizations, indicating that higher cybersecurity knowledge correlates with increased cybersecurity awareness. Awareness, knowledge, and cybersecurity behavior play crucial roles in maintaining cybersecurity. According to Sundareswaran et al. (2018) knowledge of cybersecurity enables technology users to be more aware of the likelihood of evolving cyber attacks. This awareness is crucial, as digital banking users need to understand how to avoid attacks and digital crimes. A lack of awareness among technology users, especially in banking, reflects low understanding of the importance of information security and the implementation of adequate security controls, leading to vulnerabilities in cybersecurity (Shaw et al., 2009). With sufficient awareness and knowledge, users of mobile and internet banking can address vulnerabilities in banking information technology (Figure 1).

Hypothesis Development

Cybersecurity awareness is a user's understanding of the risks and threats that exist in the digital sphere and vigilance to avoid potential cyberattacks. In the context of digital banking, users who have high cybersecurity awareness tend to understand the risks that can threaten their data and privacy. Such awareness is expected to influence user behavior in taking the necessary precautions in protecting their personal data. This is supported by the results of research conducted by Zwilling et al. (2022) where cybersecurity awareness has a significant effect on cybersecurity user behavior. In the banking sector, studies such as Al-Kumaim & Alshamsi (2023); and Johri & Kumar (2023), explored customer awareness and cybersecurity leadership in preventing

Figure 1. **Framework Used**



cyberattacks in Saudi Arabia and the UAE. This research collectively underlines the importance of cybersecurity awareness in shaping cybersecurity behavior in various sectors, especially the banking sector. Based on this explanation, the following hypothesis can be formulated:

H1: Cybersecurity awareness of digital banking users significantly influences cybersecurity behavior.

Cybersecurity knowledge is a user's understanding of the basic concepts and practices of security in the digital sphere, including recognition of cyber threats and protective measures taken to mitigate these risks. According to the Theory of Planned Behavior by (Cheng, 2017) individual behavior is shaped by attitudes, subjective norms, and perceived behavioral control, whereby adequate knowledge fosters positive attitudes toward security practices and enhances one's perceived ability to manage cyber risks. Empirical studies support this notion for instance, Hadlington (2017); and Ng & Xu (2007) found that individuals with higher levels of cybersecurity knowledge are more likely to adopt secure digital practices. In the use of digital banking facilities, knowledge of cybersecurity such as the use of strong passwords, two-factor authentication, and awareness of the dangers of phishing, is expected to be an encouragement to take safer actions in using digital banking services. Therefore, the more cybersecurity knowledge a digital banking user possesses, the more likely they are to exhibit behaviors that support secure and responsible use of digital financial services. Based on this explanation, the following hypothesis can be formulated:

H2: Cybersecurity knowledge of digital banking users significantly influences cybersecurity behavior.

Cybersecurity knowledge is an understanding of aspects of digital security such as how cyberattacks work, how to protect personal data, and effective preventive measures. It provides digital banking users with useful information to understand the various cyber risks they may face. In the cybersecurity domain, when individuals are knowledgeable about cyber threats, protection mechanisms, and safe digital practices, they become more capable of recognizing risks and developing a proactive awareness of potential threats. Empirical evidence supports this relationship, for instance, Abawajy (2014) emphasized that users with a higher understanding of cybersecurity are significantly more alert to cyber threats and more likely to identify suspicious activities. Similarly Zwilling et al. (2022) found that among mobile banking users, cybersecurity knowledge significantly improved users' awareness of digital fraud. As digital banking platforms become increasingly sophisticated and susceptible to evolving cyberattacks, users must rely on their knowledge to stay aware of vulnerabilities. Thus, cybersecurity knowledge does not merely equip users with technical information, it fundamentally shapes their vigilance, critical thinking, and capacity to interpret and react to potential cyber risks, making it a significant predictor of cybersecurity awareness in digital banking contexts. Based on this explanation, the following hypothesis can be formulated:

H3: Cybersecurity knowledge of digital banking users significantly influences cybersecurity awareness.

Cybersecurity awareness plays a critical mediating role in the relationship between cybersecurity knowledge and cybersecurity behavior. Knowledge serves as the foundation that shapes attitudes and awareness, which subsequently influence behavior. Knowledge of cybersecurity will shape users' awareness of potential risks, which in turn motivates them to act more vigilantly and carefully in the use of digital banking services. In this regard Ifinedo (2012) highlights that awareness acts as an essential cognitive-emotional bridge between knowledge and behavior, arguing that knowledge about cybersecurity risks

is more likely to lead to secure practices when users are also situationally aware of these risks. Research by Limna et al. (2023) and Zwilling et al. (2022) shows that cybersecurity knowledge indirectly increases security behavior through increased awareness. Based on this explanation, the following hypothesis can be formulated:

H4: Cybersecurity awareness mediates the relationship between cybersecurity knowledge and cybersecurity behavior.

3. METHODS

Data and Sample

This research is a quantitative descriptive study, with a descriptive and causal survey design. This approach was selected to gather data from a sample of digital banking users related to their levels of awareness, knowledge, and cybersecurity behavior. The approach enables exploration of causal relationships between these variables. The population in this study consists of all digital banking service users in the city of Salatiga, including users of mobile banking and internet banking applications. Given the size of the population, this study uses a purposive sampling technique, where the sample is chosen based on specific criteria. The respondent criteria for this study are: (1) Reside or have lived in Salatiga for at least six months, (2) Have used digital banking services (Mobile Banking or Internet Banking) for at least three months, and (3) Be aged between 17 and 60 years old.

The data collected is primary data sourced directly from respondents who meet these criteria, gathered through questionnaires. The primary instrument used in this study is a questionnaire consisting of three main sections: cybersecurity awareness level, cybersecurity knowledge, and preventive cybersecurity behavior in digital banking usage. The measurement scale is a Likert scale with five categories of agreement: 1 = Strongly Disagree (STS), 2 = Disagree (TS), 3 = Neutral (N), 4 = Agree (S), and 5 = Strongly Agree (SS).

Definition and Indicators of Variables

Cybersecurity Awareness

Cybersecurity awareness refers to the extent to which individuals recognize and understand cyber risks and threats when using digital services. It involves the ability to identify potential cyberattacks, risky behavior, and the importance of maintaining digital security.

Indicators :

a. Awareness of potential cyber threats (e.g., phishing, malware).
b. Awareness of safe digital banking practices.
c. Awareness of the consequences of unsafe behavior.
d. Attention to cyber alerts or notifications.

Cybersecurity Knowledge

Cybersecurity knowledge is defined as the level of understanding individuals have regarding technical and procedural aspects of digital security. It includes factual knowledge, skills, and comprehension of protective measures.

Indicators:

a. Knowledge of strong password practices.
b. Knowledge of two-factor authentication.
c. Understanding of secure network usage (e.g., avoiding public Wi-Fi).
d. Familiarity with common cyber fraud techniques.

Cybersecurity Behavior

Cybersecurity behavior refers to the actual actions and habits adopted by users to protect themselves from cyber threats while using digital banking services.

Indicators:

a. Regularly updating passwords.
b. Avoiding sharing credentials with others.
c. Checking for HTTPS or secure connections when logging in.
d. Avoiding accessing suspicious links or pop-ups.

Data Analysis

The collected data will be analyzed quantitatively using Structural Equation Modeling (SEM) or Partial Least Squares (PLS) to examine the relationships between variables and to understand the direct and indirect effects of each variable. Prior to instrument testing, data analysis will begin with descriptive statistical analysis to describe the characteristics of the respondents. The verification analysis technique used in this study includes validity and reliability tests to ensure that the questionnaire items directed at the respondents are accurately received and understood.

5. RESULTS AND DISCUSSION

Sample Discription

The respondents in this study are users of mobile banking services residing in Salatiga, aged between 17 and 60 years. The demographic characteristics of the respondents show that out of 200 respondents, the majority (68%) are aged between 20-30 years. Most respondents are private sector employees, comprising 47.5% of the total. All respondents have bank accounts and prefer using mobile banking services, with 45.5% using the MyBCA application (Table 1).

Validity and Reliability Testing (Outer Model

In the use of data analysis techniques using SmartPLS (Figure 2), there are three criteria to assess the model testing with the outer model: the results of convergent validity, discriminant validity, and composite reliability are provided in the appendix (see Table 2). The convergent validity criterion can be seen from the loading factor values. A loading factor value is considered valid if it has a standard value > 0.70. However, according to Hair et al. (2017) we were confident the interest in partial least squares structural equation modeling (PLSSEM loading factor values between 0.50 and

Table 1. **Sample Discription**

No	Demographic Characteristics	Category	Frequency (people)
1.	Gender	Male	90
		Female	110
2.	Age	< 20th	3
		21-30th	136
		31-40th	49
		41-50th	5
		>50th	7
3.	Banking Apps	MyBCA	91
		Brimo	45
		BNI Mobile	20
		Livin Mandiri	18
		Bima Bank Jawa Tengah	21
		Others	5
4.	Activity	ASN & BUMN	42
		Private employee	95
		Student	13
		Entrepreneur	21
		Others	29

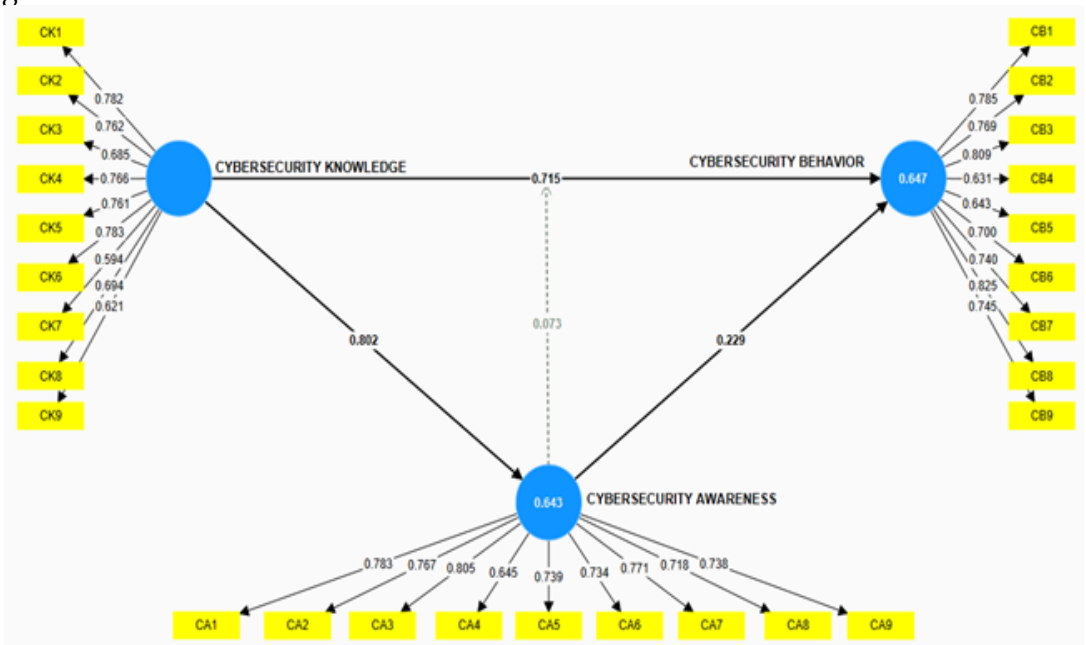
Source: Processed Primary Data

0.60 are considered to meet the criteria, supported by all AVE values on indicators being higher than the standard value of > 0.50. Table 2 shows that all loading factor values have met the convergent validity criteria. According to Hair et al. (2017) we were confident the interest in partial least squares structural equation modeling (PLSSEM, the discriminant validity criterion is used to ensure that each latent variable has a different concept from other variables. Discriminant validity can be seen from the cross-loading values of each indicator on the research variables; these values can be considered valid if each indicator of each latent variable is greater than the cross-loading values of other latent variable relationships. The test results indicate good discriminant validity as it shows high correlation compared to other constructs. The reliability criteria can be seen from Cronbach's alpha value and composite reliability value, with constructs considered valid if the composite reliability value > 0.70 (Hair et al., 2017) we were confident the interest in partial least squares structural equation modeling (PLSSEM). The test results (see Appendix 1, Table 2) conclude that all variables in the study meet the criteria and can be considered valid and reliable.

Hypothesis Testing (Bootstrapping)

Table 3 shows the results of hypothesis testing using bootstrapping, which aims to demonstrate the relationships and significance of each latent variable. To see the significance and strength of the relationships between the constructs used to test the hypotheses, the path coefficient values between constructs can be observed. According to Hair et al., (2017)we were confident the interest in partial least squares structural equation modeling (PLSSEM, the influence of the relationship between variables can be considered significant if the t-statistic value > t-table, with a confidence level of 95%, thus p-value < 0.05. The relationship between cybersecurity awareness and cybersecurity behavior is significant, with a t-statistic of 18.099 (greater than 1.96) and a p-value of 0.000. The original sample value is 0.666, indicating a positive effect. Therefore, hypothesis 1 is accepted, confirming that cybersecurity awareness

Figure 2. **Outer Model**



Source: Data Processing with SmartPLS, 2024

Table 3. **Hypothesis Testing of Path Coefficient**

	Original sample (O)	Sample mean (M)	Standard deviation (STDEV)	T statistics (|O/ STDEV|)	P values
Cybersecurity awareness -> Cybersecurity behavior	0.666	0.676	0.037	18.099	0.000
Cybersecurity knowledge -> Cybersecurity awareness	0.802	0.808	0.025	32.682	0.000
Cybersecurity knowledge -> Cybersecurity behavior	0.910	0.818	0.024	33.191	0.000
Cybersecurity Awareness X Cybersecurity Knowledge -> Cybersecurity Behavior	0.073	0.082	0.047	1.534	0.125

Source: Data Processing with SmartPLS, 2024

significantly and positively affects cybersecurity behavior. This suggests that digital banking users who are more aware of cybersecurity threats are more likely to engage in secure behavior. The relationship between cybersecurity knowledge and cybersecurity awareness also shows a significant result with a t-statistic of 32.682 and a p-value of 0.000. The original sample value is 0.802, indicating a strong positive influence. Thus, hypothesis 2 is accepted, supporting the conclusion that greater cybersecurity knowledge leads to higher awareness among digital banking users. The effect of cybersecurity knowledge on cybersecurity behavior is also statistically significant, with a t-statistic of 33.191 and a p-value of 0.000. The path coefficient value is 0.910, indicating a strong positive influence. Therefore, hypothesis 3 is accepted, showing that users with greater cybersecurity knowledge tend to exhibit safer behavior when using digital banking services. Hypothesis 4 examines whether cybersecurity awareness significantly mediates the effect of cybersecurity knowledge on cybersecurity behavior. Although the R-Square value for cybersecurity awareness is 0.643 (indicating substantial explained variance), the interaction term (Cybersecurity Awareness × Cybersecurity Knowledge) yields a t-statistic of 1.534 and a p-value of 0.125, which is greater than 0.05. This indicates that the mediating effect of awareness is not statistically significant. Thus, hypothesis 4 is rejected.

DISCISSION

The Relationship between Cybersecurity Awareness and Cybersecurity Behavior

The finding that cybersecurity awareness significantly influences cybersecurity behavior is theoretically supported by the Theory of Planned Behavior (TPB) (Ajzen, 1991), which posits that behavior is directly influenced by behavioral intention, which in turn is shaped by attitudes, subjective norms, and perceived behavioral control. In this context, cybersecurity awareness reflects an individual's attitudinal readiness their understanding of cyber threats and

belief in the importance of protective actions.When users are more aware of cybersecurity issues (e.g., phishing, password threats, or data breaches), they are more likely to perceive those threats as personally relevant and dangerous, which increases their motivation to act cautiously. This awareness leads to the adoption of behaviors such as using strong passwords, enabling two-factor authentication, or being cautious with suspicious links. Awareness, therefore, serves as a cognitive trigger that activates risk-avoidance behaviors. This result is in line with research conducted by Limna et al. (2023) and Zwilling et al. (2022) where cybersecurity awareness significantly affects users' cybersecurity behavior. This finding explains that individuals take protective action when they recognize a threat, understand its severity, and believe they can take effective steps to avoid it.

The Relationship between Cybersecurity Knowledge and Cybersecurity Awareness

The finding that cybersecurity knowledge significantly influences cybersecurity awareness supports the extended Knowledge Attitude Behavior model, where knowledge is considered a prerequisite for developing awareness. Users who have sufficient understanding of digital risks, types of cyber threats, and appropriate protection mechanisms tend to be more aware of their vulnerability and the seriousness of cybersecurity issues. In the context of digital banking, users with stronger knowledge (e.g., recognizing suspicious login behavior, understanding phishing indicators, or knowing the function of two-factor authentication) are more likely to be consciously aware of possible risks in their online interactions. This result aligns with the research conducted by Sundareswaran et al. (2018) and Zwilling et al. (2022) stating that higher cybersecurity knowledge among information technology users enables them to be more aware of cybersecurity. Therefore, cybersecurity knowledge functions as a cognitive framework that shapes how users perceive cyber threats, thereby enhancing their situational awareness.

The Relationship between Cybersecurity Knowledge And Cybersecurity Behavior

The significant effect of cybersecurity knowledge on cybersecurity behavior further reinforces the importance of knowledge as a direct driver of action. Unlike awareness, which represents understanding, behavior represents real-world application such as choosing strong passwords, avoiding public Wi-Fi for banking, or enabling biometric authentication. This finding is in line with the Theory of Planned Behavior by (Cheng, 2017), which propose that knowledge influences attitudes and perceived behavioral control, leading to the formation of intention and subsequent action. When users understand how their actions can protect them from threats, they are more likely to engage in preventive behavior. Moreover, this direct link suggests that in some cases, especially in routine digital activities like mobile banking, users may rely on their knowledge habitually without needing to engage in reflective awareness. For example, someone who has learned that public Wi-Fi is risky may simply avoid it as a matter of routine. This result is consistent with research conducted by Zwilling et al. (2022) that cybersecurity knowledge influences cybersecurity behavior.

Cybersecurity Awareness as a Mediator Between Cybersecurity Knowledge and Cybersecurity Behavior

The finding that cybersecurity awareness does not significantly mediate the relationship between knowledge and behavior suggests that while awareness is important, knowledge may directly influence behavior without necessarily passing through the awareness pathway. This can be due to users acting on habitual knowledge or training without needing to consciously reflect (automatic behavior), external motivations (e.g., employer rules or app restrictions) overriding personal

awareness, or even the possibility that awareness is present but not strong enough to translate into meaningful action. This finding contrasts with prior studies such as Zwilling et al. (2022) that found significant mediation, but aligns with Bada et al. (2019) who argued that awareness alone is insufficient to influence behavior if not supported by other factors such as motivation or social norms. In the context of digital banking in Salatiga, this implies that while awareness is important, it does not significantly bridge the relationship between knowledge and behavior suggesting a more direct effect of knowledge on behavior. These findings highlight the importance of cybersecurity education but also reveal that simply increasing awareness may not be enough to drive behavioral change. Practical implications include the need for more engaging and action-oriented cybersecurity training that translates knowledge into behavior.

Practical applications of these findings include:

a. Strengthening educational campaigns: Banks should introduce targeted training programs focusing on phishing awareness, password security, and fraud prevention.
b. Enhancing customer communication: Regular updates and alerts on emerging cyber threats can help users remain vigilant against new scams.
c. Encouraging secure banking practices: Promoting two-factor authentication (2FA) and biometric authentication can significantly reduce unauthorized access risks.
d. By implementing these strategies, the banking sector can enhance user cybersecurity behavior, ultimately reducing fraud cases and improving trust in digital banking services.

5. CONCLUSION

This study confirms that cybersecurity knowledge plays a critical role in shaping both the awareness and behavior of digital banking users in Salatiga. Knowledge has a direct and significant impact on behavior, and also significantly influences awareness. However, contrary to expectations, cybersecurity awareness does not significantly mediate the relationship between knowledge and behavior. The research results have important practical implications for the banking sector, especially for digital banking services. Banks can improve user cybersecurity through educational programs that focus on cybersecurity knowledge and awareness. Users will better understand the risks that exist with good knowledge. While user awareness can encourage them to turn security understanding into a real action in maintaining personal data security. This education program is expected to reduce the risks faced by users of digital services, and can increase customer confidence in digital banking services.

Despite these valuable insights, this study has certain limitations. The sample size is limited and may not comprehensively represent the entire population of digital banking users. Additionally, the reliance on self-reported survey data introduces the possibility of personal perception bias, which may not fully capture actual user behavior. Furthermore, the study primarily focuses on cybersecurity awareness and knowledge, without considering external factors such as bank security technologies and regulatory frameworks. Future research should address these limitations by expanding the sample size to include a more diverse and representative population of digital banking users. Employing a mixed-methods approach that combines both quantitative and qualitative data collection could provide deeper insights into cybersecurity behavior. Additionally, future studies should explore external variables such as the impact of security technologies, regulatory policies, and bank-led cybersecurity initiatives on user behavior. By incorporating these elements, future research can contribute to a more holistic understanding of the factors influencing cybersecurity behavior in digital banking environments.

REFERENCES

Abawajy, J. (2014). User preference of cyber security awareness delivery methods. *Behaviour and Information Technology*, *33*(3), 237–248. https://doi.org/10.1080/0144929X.2012.708787.

Al-Alawi, A. I., & Al-Bassam, S. A. (2019). Assessing the factors of cybersecurity awareness in the banking sector. *Arab Gulf Journal of Scientific Research*, *37*(4), 17–32. https://doi.org/10.51758/agjsr-04-2019-0014.

Al-Kumaim, N. H., & Alshamsi, S. K. (2023). Determinants of Cyberattack Prevention in UAE Financial Organizations: Assessing the Mediating Role of Cybersecurity Leadership. *Applied Sciences (Switzerland)*, *13*(10), 1-34. https://doi.org/10.3390/app13105839.

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. *International Conference on Cyber Security for Sustainable Society*. http://arxiv.org/abs/1901.02672.

Barquin, S., Gantes, G. de, HV, V., & Shrikhande, D. (2019). *Digital banking in Indonesia: Building Loyalty Aand Generating Growth*. McKinsey & Company.

Cheng, X. (2017). Applying the Theory of Planned Behavior to Influence Auditors' Knowledge-Sharing Behavior. *Dissertations*. University of South Florida.

Hadlington, L. (2017). Human Factors In Cybersecurity; Examining The Link Between Internet Addiction, Impulsivity, Attitudes Towards Cybersecurity, And Risky Cybersecurity Behaviours. *Heliyon*, *3*(7), 1-18. https://doi.org/10.1016/j.heliyon.2017.e00346.

Hair, J. F., Hult, G. T., Ringle, C., & Sarstedt, M. (2017). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). In Sage (Second Edi)*. SAGE Publications, Inc.

IDX Channel. (2023). *Transaksi Digital Banking Tembus Rp4.944 Triliun, Naik 9,8 Persen di Maret 2023*. IDX Channel. https://www.idxchannel.com/banking/transaksi-digital-banking-tembus-rp4944-triliun-naik-98-persen-di-maret-2023.

Ifinedo, P. (2012). Understanding Information Systems Security Policy Compliance: An Integration of The Theory of Planned Behavior and The Protection Motivation Theory. *Computers and Security*, *31*(1), 83–95. https://doi.org/10.1016/j.cose.2011.10.007.

Johri, A., & Kumar, S. (2023). Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia: A Study in the Era of Banking Digital Transformation. *Human Behavior and Emerging Technologies*, *2023*, 1-10. https://doi.org/10.1155/2023/2103442.

Kementerian Keuangan Republik Indonesia. (2024). *Cyber Security Awareness*. Kementerian Keuangan Republik Indonesia.

Limna, P., Kraiwanit, T., & Siripipattanakul, S. (2023). The Relationship between Cyber Security Knowledge, Awareness and Behavioural Choice Protection among Mobile Banking Users in Thailand. *International Journal of Computing Sciences Research*, *7*(November), 1133–1151. https://doi.org/10.25147/ijcsr.2017.001.1.123.

Mai, P. T., & Tick, A. (2021). Cyber Security Awareness and Behavior of Youth in Smartphone Usage: A Comparative Study between University Students in Hungary and Vietnam. *Acta Polytechnica Hungarica*, *18*(8), 67–89. https://doi.org/10.12700/APH.18.8.2021.8.4.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, *69*, 151–156. https://doi.org/10.1016/j.chb.2016.11.065.

Misra, R. K., & Khurana, K. (2017). Employability Skills among Information Technology Professionals: A Literature Review. *Procedia Computer Science*, *122*(May), 63–70. https://doi.org/10.1016/j.procs.2017.11.342.

Ng, B. Y., & Xu, Y. (2007). Studying users' computer security behavior using the Health Belief Model. *PACIS 2007 - 11th Pacific Asia Conference on Information Systems: Managing Diversity in Digital Enterprises*, *January 2007*.

OJK. (2020). *Cetak Biru Transformasi Digital Perbankan*. Otoritas Jasa Keuangan.

Ramadhan, T., & Purwandari, B. (2023). Analisis Tingkat Kesadaran Keamanan Informasi: Studi Kasus Pengguna Aplikasi Perbankan Digital di Indonesia Guna Mencegah Social Engineering. *Jurnal Syntax Idea*, *9*(1), 356–363.

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H. J. (2009). The Impact of Information Richness on Information Security Awareness Training Effectiveness. *Computers and Education*, *52*(1), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011.

Sulistiyo, A., & Yanti, H. B. (2022). Pengaruh Pengendalian Internal, Manajemen Risiko dan Whistleblowing System Terhadap Pencegahan Fraud. *Jurnal Akuntansi dan Pajak*, *23*(01), 1–11.

Sundareswaran, V., Divyalakshmi, M., & Poornirma, M. (2018). Study of Cybersecurity in Data Breaching. *International Journal of Advance Engineering and Research Development*, *5*(3), 270–276.

European Union Agency for Network and Information Security. (2017). *Cyber Security Culture in organisations*. European Union Agency for Network and Information Security

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269.

Appendix 1. **Results of Validity and Reliability Test**

NO	Variable	Validity					Reliability			
		Convergent Validity		Discriminant Validity						
		Loading Factor	AVE	Cross Loading	HTMT	Description	Cronch Alpha	Composite Reliability (rho_a)	Composite Reliability (rho_c)	Description
1	CA1	0.783	0.556	0.783	0.881	Valid	0.900	0.900	0.918	Valid
2	CA2	0.767		0.767		Valid				Valid
3	CA3	0.805		0.805		Valid				Valid
4	CA4	0.645		0.645		Valid				Valid
5	CA5	0.739		0.739		Valid				Valid
6	CA6	0.734		0.734		Valid				Valid
7	CA7	0.771		0.771		Valid				Valid
8	CA8	0.718		0.718		Valid				Valid
9	CA9	0.738		0.738		Valid				Valid
10	CK1	0.782	0.518	0.782	0.691	Valid	0.882	0.889	0.905	Valid
11	CK2	0.762		0.762		Valid				Valid
12	CK3	0.685		0.685		Valid				Valid
13	CK4	0.766		0.766		Valid				Valid
14	CK5	0.761		0.761		Valid				Valid
15	CK6	0.783		0.783		Valid				Valid
16	CK7	0.594		0.594		Valid				Valid
17	CK8	0.694		0.694		Valid				Valid
18	CK9	0.621		0.621		Valid				Valid

NO	Variable	Validity					Reliability			
		Convergent Validity		Discriminant Validity						
		Loading Factor	AVE	Cross Loading	HTMT	Description	Cronch Alpha	Composite Reliability (rho_a)	Composite Reliability (rho_c)	Description
19	CB1	0.785	0.550	0.785	0.881	Valid	0.897	0.908	0.916	Valid
20	CB2	0.769		0.769		Valid				Valid
21	CB3	0.809		0.809		Valid				Valid
22	CB4	0.631		0.631		Valid				Valid
23	CB5	0.643		0.643		Valid				Valid
24	CB6	0.700		0.700		Valid				Valid
25	CB7	0.740		0.740		Valid				Valid
26	CB8	0.825		0.825		Valid				Valid
27	CB9	0.745		0.745		Valid				Valid

Source: Validity and Reliability Test with SmartPLS, 2024