International Journal of Tourism and Hospitality in Asia Pasific (IJTHAP)
Vol. 8 No. 2, pp.179-197, June, 2025
E-ISSN: 2654-7945 P-ISSN: 2685-8800
https://www.ejournal.aibpmjournals.com/index.php/IJTHAP

Click with Care: Understanding Cybersecurity Awareness in Digital Financial Transactions in Malaysia

Daisy Mui Hung Kee[1], Hui Ni Lim[1*], Boon Chuen Lim[1], Hui Yeng Lim[1], Shuet Enn Lim[1], Wei Yih Lim[1], A. J. Ali[1]
[1]Universiti Sains Malaysia, Jalan Sg Dua, 11800 Minden, Pulau Pinang, Malaysia
*Corresponding Email: huiniii13@gmail.com

ARTICLE INFORMATION

Publication information

Research article

HOW TO CITE
Kee, D. M. H., Lim, H. N., Lim, B. C., Lim, H. Y., Lim, S. E., Lim, W. Y., & Ali, A. J. (2025). Click with care: Understanding cybersecurity awareness in digital financial transactions in Malaysia. *International Journal of Tourism and Hospitality in Asia Pasific, 8*(2), 179–197.

DOI:
https://doi.org/10.32535/ijthap.v8i2.3993

Received: 18 April 2025
Accepted: 19 May 2025
Published: 20 June 2025

ABSTRACT

In today's digital age, cybersecurity awareness in financial transactions is critical, especially within the banking sector. Maybank, as Malaysia's top-ranked bank and one of the leading global financial institutions, must prioritize cybersecurity awareness to address increasingly sophisticated cyber threats. This study investigates the factors influencing cybersecurity awareness among Maybank customers, focusing on perceived usefulness, ease of use, trust, risk, and convenience. Data were collected through a survey of 204 users and analyzed using regression techniques. The results show that perceived risk is the strongest predictor of cybersecurity awareness, followed by perceived ease of use, perceived usefulness, and trust. Perceived ease of use is also significantly and negatively related to perceived risk, indicating that user-friendly systems reduce users' risk perceptions. Additionally, perceived convenience has a significant positive effect on both perceived trust and perceived risk, though it does not directly influence cybersecurity awareness. These findings highlight the critical roles of trust and risk perception in shaping user behavior and suggest that improving usability and fostering trust are key strategies for enhancing cybersecurity awareness. The study offers practical insights for financial institutions aiming to promote secure digital banking environments and strengthen customer engagement with cybersecurity practices.

Keywords: Cybersecurity Awareness; Digital Banking; Perceived Ease of Use; Perceived Risk; Perceived Trust; User Behavior

INTRODUCTION

In the digital age, cybersecurity awareness has emerged as an urgent and critical priority, particularly in the banking sector, where safeguarding sensitive customer data and financial transactions is essential to maintaining trust and operational integrity. As online banking and digital financial services continue to expand rapidly, the scale and sophistication of cyber threats have escalated in parallel, posing serious risks not only to financial institutions but also to the broader financial ecosystem. In Malaysia, the threat landscape is particularly severe. The Asia Scam Report 2024 reveals that Malaysia has the highest rate of online fraud revictimization in Asia, with victims being retargeted an average of 2.5 times (Bernama, 2024). This statistic underscores a pressing need to enhance public awareness and institutional vigilance in mitigating these persistent threats. As the country's top-ranked bank and a globally recognized institution listed among the top 200 global banks by The Banker magazine and the highest-ranking Malaysian company on the Forbes Global 2000 list, Maybank holds a pivotal role in setting industry standards for cybersecurity. Its leadership position brings both responsibility and expectation—to not only protect its customers but also to lead by example in building a resilient and secure digital banking environment.

Moreover, the importance of cybersecurity cannot be separated from broader issues of financial inclusion and economic empowerment. As digital financial platforms like online banking become essential tools for underserved populations, ensuring secure access is no longer a technical issue alone but a socio-economic imperative. Liang et al. (2024) emphasize that fintech innovation plays a transformative role in promoting financial inclusion by extending financial services to previously excluded demographics. Similarly, Kee and Anwar (2024) highlight the complex and interconnected nature of women's empowerment, gender inequality, and financial inclusion in developing countries, illustrating that access to secure digital financial services not only enhances individual financial security but also contributes to national economic resilience. In this light, cybersecurity awareness becomes a cornerstone for inclusive growth, as individuals who feel unsafe or distrustful of digital platforms are less likely to participate in the formal financial system. For a major financial institution like Maybank, fostering cybersecurity awareness is not merely about protecting data—it is about sustaining trust, enabling access, and contributing to social and economic development through secure digital inclusion.

The urgency of this issue is further reinforced by Malaysia's classification as a high-risk country for online financial fraud (Nawi et al., 2023). Consumers who rely on electronic payments are frequently targeted by sophisticated scams that exploit both technological vulnerabilities and human errors. A growing body of evidence suggests that the human factor remains one of the most significant weaknesses in cybersecurity. Shaukat et al. (2020) argue that users and employees often fail to adhere to basic security protocols, inadvertently creating entry points for unauthorized access and exploitation. This vulnerability is not merely theoretical. In a recent high-profile case, thirteen individuals—including four bank employees—were arrested in Malaysia for orchestrating the fraudulent withdrawal of RM24.2 million from fixed deposit accounts (Malay Mail, 2024). These incidents reveal a systemic issue in which both human behavior and institutional safeguards are falling short. According to the Malaysian Computer Emergency Response Team (MyCert), there were 5,198 cases of online fraud and 794 intrusion attempts reported between January 2022 and February 2023 (Musthafa, 2023), underscoring the urgent need for integrated, user-focused, and technologically sound approaches to cybersecurity.

Against this backdrop, the present study sets out to explore the behavioral dimensions of cybersecurity awareness in digital financial transactions, particularly focusing on key influencing factors such as perceived usefulness, perceived ease of use, trust, risk, and convenience. These variables have been widely studied in the Technology Acceptance Model (TAM) but have rarely been integrated into the context of cybersecurity awareness within digital banking in Malaysia. The objective of this research is to investigate how these interrelated factors shape users' awareness and engagement with cybersecurity practices. The significance of this study lies in its potential to inform the development of more targeted, user-centered security frameworks within the banking sector, especially in environments where digital adoption is high but awareness may lag behind. The novelty of the research emerges from its focus on behavioral intention and psychological constructs as mediators of cybersecurity awareness, rather than relying solely on system-based or technical evaluations. As a contribution, this study offers empirical insights that financial institutions can use to improve their cybersecurity strategies, enhance user trust, and ultimately ensure a safer and more inclusive digital financial ecosystem.

LITERATURE REVIEW

Cybersecurity Awareness

Cybersecurity refers to the protection of computers, networks, servers, and digital data from unauthorized access, destruction, or attacks in cyberspace. Given the growing interconnectedness of the world, cybersecurity has become a critical element of business strategy, as organizations must safeguard financial data, intellectual property, and their reputation (Alharbi & Tassaddiq, 2021). The importance of cybersecurity cannot be overstated. An attack on one individual or system can quickly escalate, affecting a large number of users or organizations. The cybersecurity threat is constantly advancing, with cyberattacks becoming increasingly sophisticated. 63% of Malaysians have encountered a scam either directly or indirectly, with 17% having been direct victims of banking or financial scams (The Association of Banks in Malaysia, 2024). The significance of cybersecurity is especially pronounced in the banking sector, where financial institutions are prime targets for sophisticated cyberattacks. These institutions face significant risks to both consumer data and operational integrity (Al-Alawi et al., 2023; Stanikzai & Shah, 2021). Cybersecurity practices are essential to protecting personal and organizational data from both internal and external threats (Akintoye et al., 2022). As digital banking advances, driven by technological advancements and the growing prevalence of online services, the convenience of these innovations is accompanied by a rising number of cybersecurity threats (Liu et al., 2022; Thach et al., 2021). This stresses the need for enhanced cybersecurity awareness among individuals, employees, and organizations across the public and private sectors to improve resilience to cyber threats (Zwilling et al., 2022). Achieving robust cybersecurity requires policy compliance, collaboration, and proactive measures, especially among financial institutions, to ensure the secure adoption of digital banking practices while maintaining the integrity of financial transactions (Johri & Kumar, 2023; Liu et al., 2022; Normalini & Ramayah, 2019; Thach et al., 2021).

The increasing number of cybersecurity firms over the past decade highlights the growing severity of cyber threats faced by organizations. In the banking sector, cyber threats include malware, spoofing, unencrypted data, compromised information, and unsecured third parties. Specific risks such as bank verification number scams, phishing, card theft, and banking fraud are prevalent in online transactions (Wang et al., 2020). The COVID-19 pandemic has also led to a shift in consumer behavior, with increased reliance on online shopping and digital payments (Aryani et al., 2021; Hashem, 2020).

As consumers engage in more online transactions using credit and debit cards, there is a growing need for stronger cybersecurity protections to safeguard these activities. The rapid growth of the technology industry, particularly in Artificial Intelligence (AI), further highlights the reliance on digital transactions and the need for robust security measures in online banking (Yeo et al., 2020). To enhance cybersecurity awareness, customers are encouraged to take proactive steps such as regularly updating their software, participating in antivirus programs, and using complex passwords (Cele & Kwenda, 2025). Platforms such as Sifu, which incorporate game techniques and AI, are helping software developers identify and address vulnerabilities in their systems, further contributing to improving cybersecurity awareness in industries, including banking (Gasiba et al., 2020). As online shopping continues to rise, the demand for secure digital transactions also intensifies, making it essential for banks to ensure the protection of customer accounts and online transactions.

Hypotheses Development

Perceived Usefulness

Perceived usefulness in the context of online banking refers to the extent to which customers believe that using online banking enhances their financial management, leading to improvements in efficiency, convenience, and overall quality of life (Kaulu et al., 2024; Tiwari, 2021). A key component of perceived usefulness is the security measures provided by banks, which ensure the safety and integrity of online transactions. These protective features are important in building customer confidence and encouraging users to perform various financial activities through online banking. Effective security measures not only enable customers to easily access their accounts but also facilitate secure payments, bill settlements, and fund transfers, thereby promoting quick and safe transactions (Kim & Song, 2024).

Kee, Hisam et al. (2021) highlighted that perceived usefulness plays a significant role in shaping customer behavior, influencing their intention to use online banking. Nevertheless, Yo et al. (2021) found that perceived usefulness and trust did not significantly affect customer satisfaction with the Shopee platform in Malaysia, suggesting that the impact of perceived usefulness can vary depending on the specific characteristics of the platform in question. Salem et al. (2019) emphasized that the success of online banking services is contingent upon several factors, including management simplicity, design transparency, functional reliability, and customer satisfaction. In this regard, online banking systems that effectively detect and mitigate fraudulent activities contribute significantly to perceived usefulness (Ahmad et al., 2024). Users can also enhance their security by adopting precautionary measures such as employing strong passwords, regularly updating their software, avoiding interactions with potential scammers, and monitoring their accounts frequently (Griffiths, 2023). Moreover, online banking's perceived usefulness is heightened by its user-friendly interface, which enables customers to manage their finances effectively, even without advanced technical skills (Bajwa et al., 2023). We, therefore, hypothesize that:

H1: Perceived usefulness has a positive effect on cybersecurity awareness in financial transactions.
H2: Perceived usefulness has a positive effect on perceived trust in financial transactions.
H3: Perceived usefulness has a positive effect on perceived risk in financial transactions.

Perceived Ease of Use of Cybersecurity Measures

Perceived ease of use plays a role in shaping cybersecurity awareness and practices in financial transactions, as users are more likely to adopt security measures when they

find them simple, intuitive, and convenient. In the context of online banking, consumers increasingly find it easy to perform tasks such as sharing information, making online purchases, and conducting financial transactions via smartphones and the Internet (Alzoubi et al., 2022). The growing reliance on digital platforms has made financial management more accessible and efficient, highlighting the importance of user-friendly cybersecurity features that simplify secure interactions (Yang et al., 2021). Banks that prioritize ease of use in their security protocols can foster a positive attitude toward cybersecurity by removing barriers to adopting safe practices (Kee, Hisam et al., 2021). This approach not only enhances user confidence in online banking but also reinforces the role of ease of use in driving customer satisfaction. Yo et al. (2021) demonstrated a strong relationship between perceived ease of use and customer satisfaction. Similarly, Kee, Gan et al. (2021) emphasized the importance of perceived ease of use in online purchasing behavior, noting that users are more likely to engage in transactions when they find the process straightforward and uncomplicated. Clear guidance and seamless design not only enhance cybersecurity awareness but also promote safer financial behaviors (Alharbi & Tassaddiq, 2021). Therefore, we propose the following hypotheses:

H4: Perceived ease of use has a positive effect on cybersecurity awareness in financial transactions.
H5: Perceived ease of use has a positive effect on perceived trust in financial transactions.
H6: Perceived ease of use has a positive effect on perceived risk in financial transactions.

Perceived Trust

Perceived trust plays a role in facilitating online transactions, acting as a mediator between customers' perceptions and their intentions to engage in financial activities (Kim & Peterson, 2017). Previous studies in e-commerce have highlighted trust as a key factor in influencing customers' purchase decisions and behaviors, with trust acting as a vital mediator in the relationship between antecedents and customers' intentions (Han et al., 2019). However, Yo et al. (2021) found that perceived trust, alongside perceived usefulness, did not significantly affect customer satisfaction with Shopee in Malaysia, suggesting that platform-specific dynamics may influence how trust operates in different contexts. Perceived trust is particularly important in online banking, where it mediates the effects of structural assurance on factors such as perceived usefulness, privacy or security risk, attitude, and behavioral intention (Han et al., 2019). Trust in online banking platforms is built through a combination of security measures, such as encryption, multi-factor authentication, and real-time alerts for suspicious activities. Maybank, for instance, strengthens customer trust in its online banking platforms through tools like Secure2u (a two-factor authentication system), advanced encryption for data protection, and proactive customer education on cybersecurity risks (Nair et al., 2020). These efforts address customers' concerns about privacy and security risks, ultimately fostering trust and cultivating positive attitudes and behavioral intentions toward using online banking services. It is hypothesized:

H7: Perceived trust has a positive effect on cybersecurity awareness in financial transactions.

Perceived Risk of Cybersecurity Threats

Perceived risk refers to users' subjective assessment of the potential losses they may incur while engaging with a particular system, especially in the context of online transactions (Makhitha & Ngobeni, 2021). It encompasses the expected negative outcomes or utility that consumers associate with using specific products or services,

highlighting the potential adverse consequences of a decision (Snyder & Blevins, 1986). In the context of online banking and financial transactions, perceived risk manifests in multiple dimensions, including financial, operational, and security risks. First, financial risk arises when cybersecurity measures are not followed during online transactions. Users may fear that inadequate protection could lead to significant financial losses, such as unauthorized withdrawals from their accounts. Second, the risk of cyberattacks, such as malware or phishing, increases when cybersecurity protocols are not robust, exposing users to threats that can compromise the confidentiality and integrity of their financial data. Third, the risk of system compromise refers to the potential destruction or disruption of bank operations when cybersecurity defenses are insufficient, leading to chaotic and insecure transaction environments. The lack of proper cybersecurity measures can render banking systems vulnerable to attacks, which may result in financial losses and a loss of operational integrity. These perceived risks are essential in shaping users' awareness of cybersecurity threats, prompting them to adopt more secure behaviors in their financial transactions. Thus, we hypothesize the following:

H8: Perceived risk has a positive effect on cybersecurity awareness in financial transactions.
H9: Perceived risk has a positive effect on perceived trust in financial transactions.

Perceived Convenience of Cybersecurity Tools

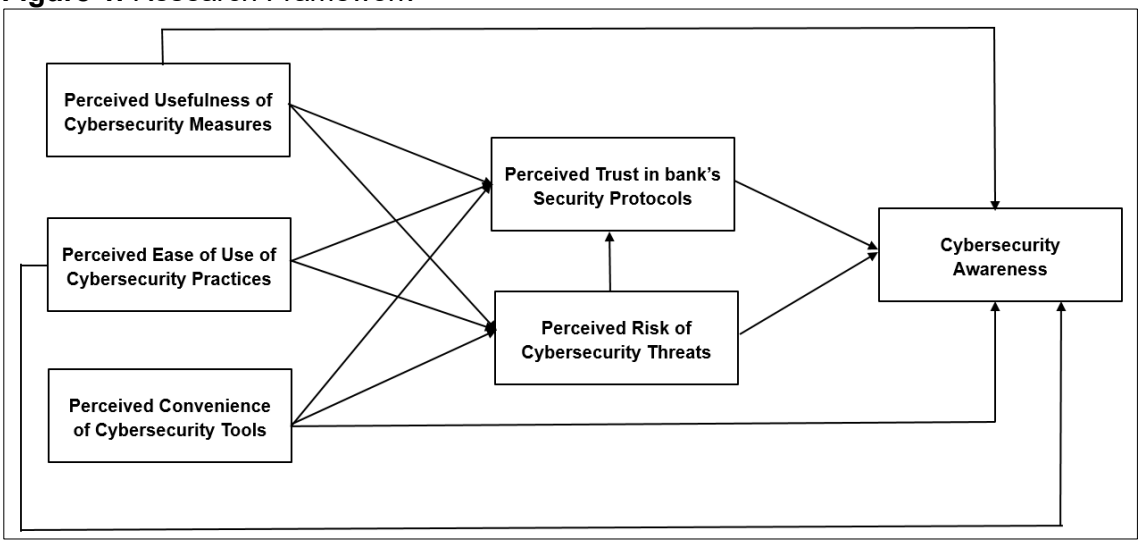
Perceived convenience plays a role in shaping users' attitudes and behaviors toward adopting digital services, particularly in online banking and cybersecurity practices. It refers to the ease with which users can interact with and utilize the security features embedded in digital platforms. In the context of online banking, perceived convenience can significantly influence users' perceptions of the effectiveness and practicality of cybersecurity measures, which are essential for maintaining safe and secure financial transactions. Yo et al. (2021) highlight the direct link between perceived convenience and customer satisfaction. Consumers are more likely to adopt cybersecurity measures if they perceive them as easy to implement and use (Dodge et al., 2023). Younger and tech-savvy populations may be more inclined to embrace cybersecurity practices if they perceive them as convenient and straightforward (Wongmahesak et al., 2025). This demographic tends to appreciate user-friendly interfaces and simplified security protocols that do not interfere with the convenience of their online activities. However, the adoption of cybersecurity measures can face resistance if users view these measures as cumbersome or time-consuming. In such cases, consumers may bypass security protocols altogether, potentially compromising the safety of their financial transactions. As highlighted by Folorunso et al. (2024), striking a balance between robust security and convenience is crucial to enhancing cybersecurity awareness and compliance. To ensure optimal user engagement with cybersecurity measures, digital platforms must prioritize ease of use without sacrificing security effectiveness. Therefore, we hypothesize:

H10: Perceived convenience has a positive effect on cybersecurity awareness in financial transactions.
H11: Perceived convenience has a positive effect on perceived trust in financial transactions.
H12: Perceived convenience has a positive effect on perceived risk in financial transactions.

Conceptual Framework

The study framework model is depicted in Figure 1.

Figure 1. Research Framework



RESEARCH METHOD

We employed a quantitative, cross-sectional survey design to examine the relationships between key variables influencing cybersecurity awareness in financial transactions. Data were collected via Google Forms. The final dataset consisted of 204 valid responses from Maybank customers in Malaysia.

Measures

Our study assessed perceived usefulness, ease of use, trust, risk, convenience, and cybersecurity awareness using a five-point Likert scale (1 = Strongly Disagree, 5 = Strongly Agree). All items, except for cybersecurity awareness, were adapted from prior research, including Yo et al. (2021). For cybersecurity awareness, we developed nine new items tailored to our study. Similarly, for perceived risk, three new items were created to measure users' perceptions of potential threats associated with online banking services. These items were designed to reflect the unique risks encountered in digital banking environments.

Perceived Usefulness

A 3-item scale was adapted to assess perceived usefulness. Cronbach's alpha was reported at 0.832. One of the sample items is, "The bank's security measures are useful, allowing me to access my account quickly and safely, making online transactions more efficient".

Perceived Ease of Use

This variable was assessed using three items focusing on the simplicity of understanding and using the bank's cybersecurity measures. A sample item is, "The bank's cybersecurity features are easy to use for securing my online transactions." Cronbach's alpha for this construct was reported at 0.830.

Perceived Trust

To evaluate the degree of users' trust in the bank's security protocols, three items were adapted. Example items include "I feel confident that the bank's security protocols reliably protect my financial information," with a Cronbach's alpha of 0.807, reflecting high reliability.

Perceived Risk

It is measured using three items that assess the user's perception of potential threats while using online banking services. A sample item includes, "I am aware of the financial risk if cybersecurity measures are not followed during online transactions." The Cronbach's alpha for this variable was 0.825.

Perceived Convenience

This variable was assessed using three items examining the ease and flexibility of using cybersecurity tools. A sample item is, "Using the bank's security features during online transactions is convenient for me." The Cronbach's alpha value for this measure was 0.756.

Cybersecurity Awareness

The dependent variable was measured using nine items to capture respondents' understanding and adherence to online security practices. A sample item is, "I understand the importance of using strong passwords to protect my financial transactions in online banking." Its Cronbach's alpha was 0.795.

RESULTS

Table 1. Respondents' Profile Summary (N=204)

Response	Frequency	Percentage (%)
Age		
18 – 25 years old	184	90.2
26 – 30 years old	17	8.3
31 – 35 years old	0	0
36 – 40 years old	3	1.5
Gender		
Male	75	36.8
Female	129	63.2
Location		
Pulau Pinang	45	22.1
Kedah	31	15.2
Perak	26	12.7
Selangor	16	7.8
Pahang	15	7.4
Johor	15	7.4
Negeri Sembilan	14	6.9
Melaka	10	4.9
Sarawak	9	4.4
Perlis	7	3.4
Kelantan	6	2.9
Terengganu	5	2.5
Sabah	5	2.5
Field of Study		
Business	95	46.6
Art	23	11.3
Humanities	19	9.3
Engineering	18	8.8
Computer Science	13	6.4
Management	6	3.0
Accounting	5	2.5

Mathematics	4	2.0
Nursing	3	1.5
Education	3	1.5
Food	2	1.0
Economics	2	1.0
Law	2	1.0
Industrial Technology	2	1.0
Communication	1	0.5
Applied Science	1	0.5
Biological Sciences	1	0.5
Aquaculture	1	0.5
Multimedia	1	0.5
HBP	1	0.5
Physics	1	0.5
Type of University		
Public University	184	90.2
Private University	20	9.8
Education Level		
Degree	189	92.6
Master	11	5.4
Doctorate	2	1.0
PhD	2	1.0
Frequency of Online Financial Transactions Usage		
Daily	133	65.2
Weekly	55	27.0
Monthly	12	5.9
Rarely	3	1.5
Never	1	0.5
Experience with Online Banking		
Less than 1 year	11	5.4
1 – 2 years	68	33.3
3 – 5 years	95	46.6
More than 5 years	30	14.7

Source: Processed Data (2025)

Table 1 provides a summary of the demographic characteristics of the respondents. The majority (90.2%) were between the ages of 18 and 25, reflecting a youthful participant base, likely familiar with digital platforms and online banking practices. In terms of gender, over half of the respondents were female (63.2%), indicating a slight predominance of women among the survey participants. Geographically, most respondents were from Pulau Pinang (22.1%) and Kedah (15.2%). In terms of educational focus, nearly half of the respondents (46.6%) were pursuing studies in Business-related programs. 90.2% were enrolled in public universities. 92.6% were pursuing a bachelor's degree qualification. When examining their habits, over half (65.2%) reported conducting online financial transactions daily. Regarding online banking experience, nearly half (46.6%) had 3 to 5 years of experience, suggesting a well-established familiarity with digital financial systems.

Table 2. Descriptive Statistics, Cronbach's Coefficient Alpha, and Zero-order Correlations for all study variables (N = 204)

Variables	1	2	3	4	5	6
Perceived Usefulness	0.832					

Perceived Ease of Use	0.774**	0.830				
Perceived Trust	0.002	0.004	0.807			
Perceived Risk	0.019	-0.002	0.546**	0.825		
Perceived Convenience	0.429**	0.483**	0.391**	0.358**	0.756	
Cybersecurity Awareness	0.435**	0.438**	0.385**	0.426**	0.477**	0.795
Mean	4.0327	3.9690	4.4559	4.5343	4.2157	4.3246
Standard Deviation	0.77242	0.83677	0.64387	0.58668	0.71980	0.44695

Note: N=204; *p < 0.05, **p < 0.01, ***p < 0.001. The diagonal entries represent Cronbach's Coefficient Alpha.

Table 2 outlines the descriptive statistics, reliability, and correlations among the study variables. The Cronbach's alpha values for perceived usefulness (0.832), perceived ease of use (0.830), perceived trust (0.807), perceived risk (0.825) and perceived convenience (0.756) confirm internal consistency and reliability, as all values exceed the threshold of 0.7 suggested by Hair Jr et al. (2014). Significant correlations were observed between most variables and cybersecurity awareness, with perceived ease of use ($r = 0.438$, $p < 0.01$) and perceived convenience ($r = 0.477$, $p < 0.01$) showing particularly strong relationships. These findings underscore the importance of user-friendly and convenient security measures in promoting cybersecurity awareness.

Table 3. Summary of Regression Analysis

	Cybersecurity Awareness	Perceived Trust	Perceived Risk
	Beta		
Perceived Usefulness	0.211*	-0.074	-0.014
Perceived Ease of Use	0.225*	-0.186	-0.218*
Perceived Convenience	0.103	0.513***	0.469***
Perceived Risk	0.282***	0.546***	
Perceived Trust	0.190**		
R^2	0.433		
F value	30.184		
Durbin-Watson Statistic	2.078		

Note: N = 204; *p < 0.05, **p < 0.01, ***p < 0.001

The results presented in Table 3 provide insights into the relationships proposed in the twelve hypotheses concerning the effects of perceived usefulness, ease of use, trust, risk, and convenience on cybersecurity awareness, perceived trust, and perceived risk in financial transactions.

H1 is supported by the regression coefficient for perceived usefulness ($\beta = 0.211$, $p < 0.05$), indicating a statistically significant positive effect on cybersecurity awareness. However, H2 is not supported, as perceived usefulness does not show a significant effect on perceived trust ($\beta = -0.074$, ns), and H3 is also unsupported, given the non-significant relationship between perceived usefulness and perceived risk ($\beta = -0.014$, ns).

For H4, the results confirm that perceived ease of use has a significant positive impact on cybersecurity awareness ($\beta = 0.225$, $p < 0.05$), supporting the hypothesis. In contrast, H5 is not supported since perceived ease of use has a non-significant negative relationship with perceived trust ($\beta = -0.186$, ns), and H6 is contradicted by a significant

negative effect on perceived risk (β = -0.218, p < 0.05), suggesting that ease of use actually reduces perceived risk rather than increasing it.

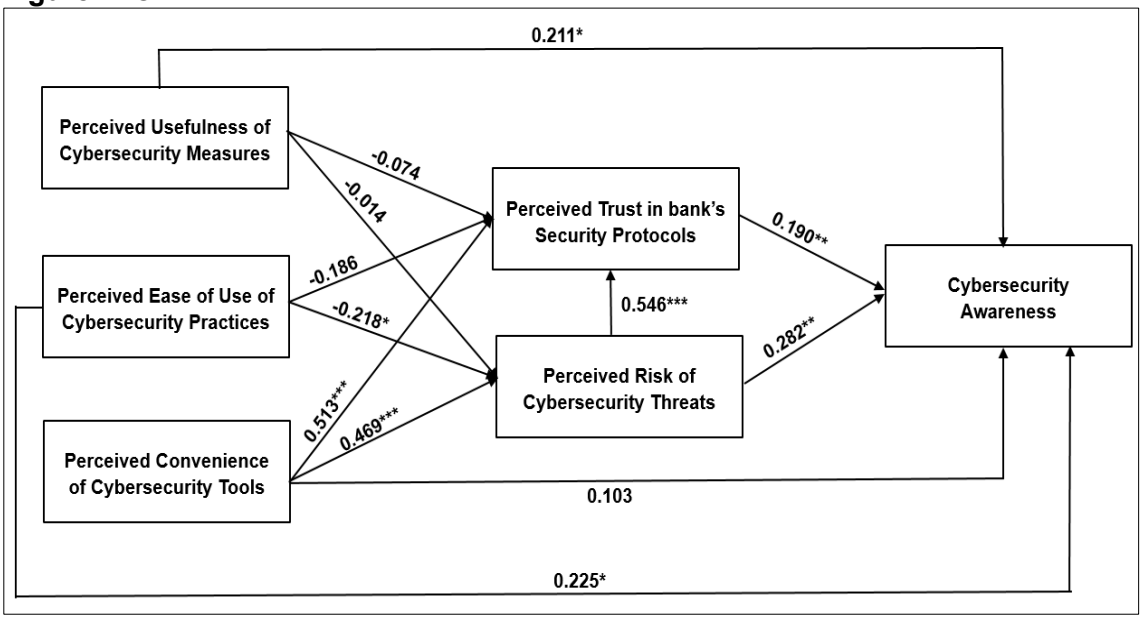
H7 is supported by a positive and statistically significant relationship between perceived trust and cybersecurity awareness (β = 0.190, p < 0.01), indicating that higher trust enhances awareness. Similarly, H8 is supported by a strong positive effect of perceived risk on cybersecurity awareness (β = 0.282, p < 0.001), showing that users who perceive higher risk are more aware of cybersecurity issues.

H9 is also supported, as perceived risk significantly and positively influences perceived trust (β = 0.546, p < 0.001), suggesting that awareness of potential risks enhances users' trust when appropriate safeguards are in place. H10, however, is not supported; perceived convenience does not significantly influence cybersecurity awareness (β = 0.103, ns). On the other hand, both H11 and H12 are supported: perceived convenience has a significant positive effect on perceived trust (β = 0.513, p < 0.001) and on perceived risk (β = 0.469, p < 0.001), indicating that users who find the service convenient tend to trust it more and are also more sensitive to associated risks.

Collectively, these findings show that cybersecurity awareness is most strongly influenced by perceived risk, followed by ease of use, usefulness, and trust. Meanwhile, perceived trust is most influenced by convenience and risk, and perceived risk is influenced significantly by both convenience and ease of use. These relationships highlight the complex interplay between usability, trust, and perceived danger in shaping users' cybersecurity awareness in digital financial environments.

The overview result of the hypothesized model is provided in Figure 2.

Figure 2. Overview Result



DISCUSSION

The findings of this study emphasize the critical role of perceived usefulness in fostering cybersecurity awareness among users. The results support H1, showing that perceived usefulness has a statistically significant positive impact on cybersecurity awareness (β = 0.211, p < 0.05). This aligns with the TAM, which posits that perceived usefulness is a

central factor influencing technology adoption. As noted by To and Trinh (2021), the perceived utility of banking technologies, including cybersecurity tools and mobile wallets, enhances user engagement by simplifying tasks and improving decision-making. When users believe that security features are genuinely useful in safeguarding financial transactions, they are more likely to be informed and proactive. In this context, financial institutions like Maybank could leverage advanced, user-centered features such as AI-driven threat detection and real-time fraud alerts to increase perceived usefulness. These proactive features offer tangible benefits, enhancing users' sense of control and security. However, while valuable, implementing such systems may incur substantial costs, require robust infrastructure, and present challenges like false positives or data privacy concerns. Ensuring transparency, investing in user education, and adhering to data protection regulations are vital steps for balancing innovation with user trust.

Perceived ease of use also plays a significant role in promoting cybersecurity awareness, as demonstrated by its positive and significant relationship ($\beta = 0.225$, $p < 0.05$), supporting H4. This result reinforces the TAM's principle that user-friendly design reduces resistance to technology adoption. Mator et al. (2021) highlighted that simplicity in interface design can lower users' hesitation. For Maybank, enhancing usability could include the integration of gamified tutorials or voice-assisted instructions for senior users or those with accessibility needs. Furthermore, perceived ease of use showed a significant negative effect on perceived risk ($\beta = -0.218$, $p < 0.05$), confirming H6 and indicating that easier systems can alleviate user concerns about cybersecurity threats. This is consistent with findings from Akinsola et al. (2021) and Kostyuk & Wayne (2021), who observed that user-friendly interfaces reduce anxiety and foster trust by demystifying technical procedures.

Perceived trust is another critical factor contributing to cybersecurity awareness, as evidenced by its positive influence ($\beta = 0.190$, $p < 0.01$), supporting H7. The trust that users place in the reliability and integrity of service providers directly enhances their confidence in managing digital financial transactions. Primandari and Suprapti (2022) emphasize that trust not only influences cybersecurity awareness but also serves as a bridge between perceived risk and user behavior. Institutions could strengthen trust through transparency strategies such as monthly security updates or establishing an independent cybersecurity advisory board. While these measures may increase confidence, they also present challenges, including resource demands and the potential for reputational risks if vulnerabilities are exposed. It is crucial to manage these initiatives with clear communication and user-friendly reporting to maintain customer reassurance.

Perceived risk exhibited the strongest influence on cybersecurity awareness ($\beta = 0.282$, $p < 0.001$) and significantly affected perceived trust ($\beta = 0.546$, $p < 0.001$), confirming both H8 and H9. This supports the Technology Threat Avoidance Theory, which asserts that awareness of potential digital threats prompts users to engage in protective behaviors. The relationship between risk and trust, supported by Damghanian et al. (2016), Kaur and Arora (2020), and Rouibah et al. (2016), indicates that a balanced perception of risk, neither exaggerated nor underestimated, can strengthen trust when users believe effective safeguards are in place. Aldas-Manzano et al. (2010) and Harridge-March (2006) further confirm the moderating role of trust in online transaction adoption. Maybank can apply this insight by prioritizing secure protocols like two-factor authentication, end-to-end encryption, and secure transaction alerts. Nonetheless, overly complex security systems could alienate less tech-savvy users, lead to alert fatigue, or introduce usability issues, especially when integrating across partners. To address this, security enhancements must be paired with a user-centered design approach that balances protection with accessibility.

Perceived convenience did not significantly influence cybersecurity awareness (β = 0.103, n.s.), indicating that ease or accessibility alone does not directly increase users' awareness levels, which rejects H10. However, convenience significantly influences perceived trust (β = 0.513, p < 0.001) and perceived risk (β = 0.469, p < 0.001), supporting H11 and H12. This suggests that convenience plays an indirect role in shaping cybersecurity awareness through its effects on trust and risk. The findings align with Lahcen et al. (2020), who noted that users' personal biases shape their risk and trust perceptions more directly than convenience itself. Maybank should ensure its cybersecurity tools are both easy to use and seamlessly integrated, enhancing user trust without sacrificing awareness. Features like one-click activation and partnerships with external payment systems may increase users' perception of secure and convenient access, reinforcing institutional credibility.

Lastly, as Frydenberg and Lorenz (2020) suggest, cybersecurity awareness is increasingly vital in the age of rising threats such as phishing and malware, especially for young users entering the workforce. The results of this study provide actionable insights for Maybank to improve its cybersecurity infrastructure and educational outreach. The institution may consider incorporating digital literacy programs or targeted campaigns to empower users with knowledge and tools that foster resilience against cyber threats. By enhancing users' digital competence and trust, Maybank can build a safer, more robust ecosystem for financial transactions in Malaysia.

CONCLUSION

This study offers a comprehensive understanding of the factors that influence cybersecurity awareness in the context of financial transactions. The findings highlight the critical roles of perceived risk, perceived trust, and perceived ease of use in shaping users' awareness and engagement with online security practices. Among these, perceived risk emerged as the strongest predictor of cybersecurity awareness, indicating that individuals who recognize potential threats are more likely to adopt protective behaviors. This finding aligns with the Technology Threat Avoidance Theory and underscores the importance for financial institutions to enhance risk communication and deliver clear, actionable security information to customers.

Perceived trust also significantly influenced cybersecurity awareness, reinforcing prior research that emphasizes the importance of institutional reliability and integrity in encouraging digital banking adoption. Maybank—and similar institutions—must therefore maintain transparent, consistent, and customer-centered security measures to reinforce user confidence and ensure continued engagement with secure digital services. While perceived trust was not the strongest predictor, its impact remains substantial, particularly as it also mediates the effect of perceived risk on user behavior.

Perceived ease of use was another key factor positively associated with cybersecurity awareness. The study confirmed that intuitive, user-friendly interfaces can reduce perceived risk and promote proactive cybersecurity behaviors. This affirms that usability is not merely a design preference, but a critical determinant of user engagement and safety. Maybank's ongoing efforts in this area could be further enhanced through features such as voice-activated assistance, gamified tutorials, or biometric authentication—tools that simplify interaction while reinforcing security.

Interestingly, perceived usefulness directly influenced cybersecurity awareness but had no significant effect on trust or risk perceptions, suggesting that while users recognize

the utility of secure systems, their trust and risk responses are influenced more by emotional and experiential factors than by functional attributes alone. Meanwhile, perceived convenience did not directly impact cybersecurity awareness, though it significantly influenced both trust and risk, indicating that convenience plays a more indirect role in shaping security behavior.

This study acknowledges several limitations. The exclusive focus on Maybank, while strategic due to its market leadership, limits the generalizability of the findings across other financial institutions. Additionally, the use of a cross-sectional survey design prevents observation of how cybersecurity awareness and perceptions evolve over time.

Future research should expand the scope to include multiple banking institutions across diverse regions or undertake cross-country comparisons to explore cultural and institutional influences on cybersecurity behavior. Longitudinal designs are also recommended to capture dynamic changes in trust, risk perception, and user behavior in response to technological innovation or emerging cyber threats. By deepening our understanding of these interrelated factors, future studies can provide actionable strategies for building a safer and more inclusive digital financial ecosystem.

LIMITATION

Several limitations must be acknowledged in this study. First, the focus on Maybank, while valuable due to its prominence as Malaysia's top bank and its global recognition, restricts the generalizability of the findings to other banking institutions or financial contexts. The specific operational practices, customer demographics, and digital strategies at Maybank may differ from those at other banks, potentially affecting cybersecurity awareness. Second, this study employed a cross-sectional design, which limits the ability to capture changes in factors influencing cybersecurity awareness over time. As cybersecurity threats and user behaviors evolve, the relationships between variables such as trust, risk perception, and convenience may also shift.

ACKNOWLEDGMENT

The authors gratefully acknowledge the contributions of informants, colleagues, and all individuals who supported this research through their insights and engagement. Their involvement greatly enriched the quality and depth of this study.

DECLARATION OF CONFLICTING INTERESTS

The authors have declared no potential conflicts of interest concerning the study, authorship, and/or publication of this article.

REFERENCES

Ahmad, I., Khan, S., & Iqbal, S. (2024). Guardians of the vault: Unmasking online threats and fortifying e-banking security, a systematic review. *Journal of Financial Crime, 31*(6), 1485–1501. https://doi.org/10.1108/JFC-11-2023-0302

Akinsola, J. E. T., Akinseinde, S., Kalesanwo, O., Adeagbo, M., Oladapo, K., Awoseyi, A., & Kasali, F. (2021). Application of artificial intelligence in user interfaces design for cyber security threat modeling. In *Software Usability*. IntechOpen. https://doi.org/10.5772/intechopen.96534

Akintoye, R., Ogunode, O., Ajayi, M., & Joshua, A. A. (2022). Cyber security and financial innovation of selected deposit money banks in Nigeria. *Universal Journal of Accounting and Finance, 10*(3), 643–652. https://doi.org/10.13189/ujaf.2022.100302

Al-Alawi, A. I., Al-Khaja, N. A., & Mehrotra, A. A. (2023). Women in cybersecurity: A study of the digital banking sector in Bahrain. *Journal of International Women's Studies, 25*(1), 306–321.

Aldas-Manzano, J., Ruiz-Mafe, C., Sanz-Blas, S., & Lassala-Navarré, C. (2010). Internet banking loyalty: evaluating the role of trust, satisfaction, perceived risk and frequency of use. *The Service Industries Journal*, *31*(7), 1165–1190. https://doi.org/10.1080/02642060903433997

Alharbi, T., & Tassaddiq, A. (2021). Assessment of cybersecurity awareness among students of Majmaah University. *Big Data and Cognitive Computing, 5*(2), Article 23. https://doi.org/10.3390/bdcc5020023

Alzoubi, H., Alshurideh, M., Kurdi, B., Alhyasat, K., & Ghazal, T. (2022). The effect of e-payment and online shopping on sales growth: Evidence from the banking industry. *International Journal of Data and Network Science, 6*(4), 1369–1380. http://dx.doi.org/10.5267/j.ijdns.2022.5.014

Aryani, D. N., Nair, R. K., Hoo, D. X. Y., Kee, D. M. H., Lim, D. H. R., Chandran, D. R., Chew, W. P., & Desai, A. (2021). A study on consumer behaviour: Transition from traditional shopping to online shopping during the COVID-19 pandemic. *International Journal of Applied Business and International Management, 6*(2), 81–95. https://doi.org/10.32535/ijabim.v6i2.1170

Bajwa, I. A., Ahmad, S., Mahmud, M., & Bajwa, F. A. (2023). The impact of cyberattacks awareness on customers' trust and commitment: An empirical evidence from the Pakistani banking sector. *Information and Computer Security, 31*(5), 635–654. https://doi.org/10.1108/ICS-11-2022-0179

Bernama. (2024, November 18). *Malaysia tops Asia in scam revictimisation rate*. Bernama. https://www.bernama.com/en/news.php?id=2364854

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

Damghanian, H., Zarei, A., & Siahsarani Kojuri, M. A. (2016). Impact of perceived security on trust, perceived risk, and acceptance of online banking in Iran. *Journal of Internet Commerce, 15*(3), 214–238. https://doi.org/10.1080/15332861.2016.1191052

Dodge, C. E., Fisk, N., Burruss, G. W., Moule Jr, R. K., & Jaynes, C. M. (2023). What motivates users to adopt cybersecurity practices? A survey experiment assessing protection motivation theory. *Criminology & Public Policy*, *22*(4), 849-868. https://doi.org/10.1111/1745-9133.12641

Folorunso, A., Wada, I., Samuel, B., & Mohammed, V. (2024). Security compliance and its implication for cybersecurity. *World Journal of Advanced Research and Reviews*, *24*(01), 2105-2121. https://doi.org/10.30574/wjarr.2024.24.1.3170

Frydenberg, M., & Lorenz, B. (2020). Lizards in the street! Introducing cybersecurity awareness in a digital literacy context. *Information Systems Education Journal, 18*(4), 33–45.

Gasiba, T. E., Lechner, U., & Pinto-Albuquerque, M. (2020). Sifu – A cybersecurity awareness platform with challenge assessment and intelligent coach. *Cybersecurity, 3*(1). https://doi.org/10.1186/s42400-020-00064-4

Griffiths, T. (2023). Protecting from online banking fraud: Risk awareness and prevention strategies. *Journal of the International Academy for Case Studies, 29*(S1), 1–2.

Hair Jr, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2014). *Multivariate Data Analysis*. Pearson Education.

Han, H., Yu, J., & Kim, W. (2019). An electric airplane: Assessing the effect of travelers' perceived risk, attitude, and new product knowledge. *Journal of Air Transport Management*, *78*, 33-42. https://doi.org/10.1016/j.jairtraman.2019.04.004

Harridge-March, S. (2006). Can the building of trust overcome consumer perceived risk online?. *Marketing Intelligence & Planning*, *24*(7), 746-761. https://doi.org/10.1108/02634500610711897

Hashem, T. N. (2020). Examining the influence of covid 19 pandemic in changing customers' orientation towards e-shopping. *Modern Applied Science*, *14*(8), 59-76. https://doi.org/10.5539/MAS.V14N8P59

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), 2103442. https://doi.org/10.1155/2023/2103442

Kaulu, B., Kaulu, G., & Chilongo, P. (2024). Factors influencing customers' intention to adopt e-banking: A TAM and cybercrime perspective using structural equation modelling. *Journal of Money and Business, 4*(1), 38–53. https://doi.org/10.1108/jmb-01-2024-0007

Kaur, S., & Arora, S. (2020). Role of perceived risk in online banking and its impact on behavioral intention: Trust as a moderator. *Journal of Asia Business Studies, 15*(1), 1–30. https://doi.org/10.1108/jabs-08-2019-0252

Kee, D. M. H., & Anwar, A. (2024). Women's empowerment, gender inequality, and financial inclusion: Evidence from a developing country. In *The Economics of Financial Inclusion* (pp. 193-209). Routledge.

Kee, D. M. H., Ang, V. W. N., Lee, Y. Y., Vehlan, L. S. A. S., Lee, L. X., Lee, S. M., & Ardel, M. R. (2024). Golden arches going green: The impact of fast-food restaurant's sustainability achievements on public image. *Advances in Global Economics and Business Journal, 5*(1), 27–43.

Kee, D. M. H., Gan, Z. W., Chan, Y. Q., Lee, H. T., Tan, X. Y., & Lee, S. W. (2021). Customer satisfaction and brand loyalty: A case study of Nestlé. *Advances in Global Economics and Business Journal, 2*(1), 13–26.

Kee, D. M. H., Hisam, N. N. B. N., Abd Rashid, N. H. B., Abdul Aziz, N. S. B., Mazlan, N. A. B., & Mahadi, N. A. Z. B. (2021). The impact of using cashless payment during the COVID-19 pandemic: A case study of Maybank. *International Journal of Accounting Finance in Asia Pacific, 4*, 1–12. https://doi.org/10.32535/ijafap.v4i2.1118

Kim, D., & Song, H. (2024). Designing an age-friendly conversational AI agent for mobile banking: The effects of voice modality and lip movement. *International Journal of Human-Computer Studies*, *187*, 103262. https://doi.org/10.1016/j.ijhcs.2024.103262

Kim, Y., & Peterson, R. A. (2017). A meta-analysis of online trust relationships in e-commerce. *Journal of Interactive Marketing, 38*(1), 44–54.

Kostyuk, N., & Wayne, C. (2021). The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public. *Journal of Global Security Studies*, *6*(2), ogz077. https://doi.org/10.1093/jogss/ogz077

Lahcen, R. A. M., Caulkins, B., Mohapatra, R., & Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, *3*, 1-18. https://doi.org/10.1186/s42400-020-00050-w

Liang, H., Kee, D. M. H., & Zainal, S. R. M. (2024). Leveraging fintech services to drive financial inclusion among women in development and emerging markets: A case study in Malaysia. In *The Economics of Financial Inclusion* (pp. 243-256). Routledge. https://doi.org/10.4324/9781032655185

Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology*, *13*, 927398. https://doi.org/10.3389/fpsyg.2022.927398

Makhitha, K. M., & Ngobeni, K. (2021). The influence of demographic factors on perceived risks affecting attitude towards online shopping. *South African Journal of Information Management*, *23*(1), 1-9. https://doi.org/10.4102/sajim.v23i1.1283

Malay Mail. (2024, June 19). Police: Four bank employees among 13 detained in RM24.2m bank fraud probe. *Malay Mail*. https://www.malaymail.com/news/malaysia/2024/06/19/police-four-bank-employees-among-13-detained-in-rm242m-bank-fraud-probe/140492

Mator, J. D., Lehman, W. E., McManus, W., Powers, S., Tiller, L., Unverricht, J. R., & Still, J. D. (2021). Usability: adoption, measurement, value. *Human factors*, *63*(6), 956-973. https://doi.org/10.1177/0018720819895098

Musthafa, A. (2023, April 5). Hundreds of thousands of ringgit lost in online banking thefts. *The Sun*. https://thesun.my/malaysia-news/hundreds-of-thousands-of-ringgit-lost-in-online-banking-thefts-CK10832671

Nair, R. K., Ganatra, V., Xiang, O. T., Kee, D. M. H., Ying, O. P., Xuan, T. J., ... & Mehta, V. (2020). A study on the winning steps Maybank undertake to gain and sustain customers. *Advances in Global Economics and Business Journal*, *1*(2), 45-54.

Nawi, N. H. A., Mohamed, S., & Ramdzan, M. R. (2023). Understanding the social commerce scam and consumers self disclosure. *International Journal of Business and Technology Management*, *5*(2), 251-262.

Normalini, M. K., & Ramayah, T. (2019). The impact of security factors towards internet banking usage intention among Malaysians. *Global Business and Management Research*, *11*(2), 241-251.

Primandari, I. D. A. A. Y., & Suprapti, N. W. S. (2022). The role of trust mediates the effect of perceived ease of use and perceived risk on intention to reuse QRIS payment methods. *International Journal of Business, Economics & Management*, *5*(3), 201-210. https://doi.org/10.21744/ijbem.v5n3.1942

Rouibah, K., Lowry, P. B., & Hwang, Y. (2016). The effects of perceived enjoyment and perceived risks on trust formation and intentions to use online payment systems: New perspectives from an Arab country. *Electronic Commerce Research and Applications*, *19*, 33-43. https://doi.org/10.1016/j.elerap.2016.07.001

Salem, M. Z., Baidoun, S., & Walsh, G. (2019). Factors affecting Palestinian customers' use of online banking services. *International Journal of Bank Marketing*, *37*(2), 426-451. https://doi.org/10.1108/IJBM-08-2018-0210

Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. *IEEE Access, 8*, 222310–222354. https://doi.org/10.1109/ICCWS48432.2020.9292388

Snyder, D. R., & Blevins, D. E. (1986). Business and university technical research cooperation: Some important issues. *Journal of Product Innovation Management: An International Publication of the Product Development & Management Association*, *3*(2), 136-144. https://doi.org/10.1111/1540-5885.320136

Stanikzai, A. Q., & Shah, M. A. (2021, December). Evaluation of cyber security threats in banking systems. In *2021 IEEE Symposium Series on Computational Intelligence (SSCI)* (pp. 1-4). IEEE. https://doi.org/10.1109/SSCI50451.2021.9659862

Thach, N. N., Hanh, H. T., Huy, D. T. N., Nga, L. T. V., Huong, L. T. T., & Vu, Q. N. (2021). technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets-the case in Vietnam. *International Journal for Quality Research*, *15*(3), 845-860. https://doi.org/10.24874/IJQR15.03-10

The Association of Banks in Malaysia. (2024, January 24). More than RM350 million in fraudulent transactions blocked during the first ten months of 2023. *The Association of Banks in Malaysia*. https://www.abm.org.my/press-releases/more-

than-rm350-million-in-fraudulent-transactions-blocked-during-the-first-ten-months-of-2023/

Tiwari, P. (2021). Electronic banking adoption in Ethiopia: an empirical investigation. *SN Business & Economics*, *1*(9), 112. https://doi.org/10.1007/s43546-021-00114-0

To, A. T., & Trinh, T. H. M. (2021). Understanding behavioral intention to use mobile wallets in vietnam: Extending the tam model with trust and enjoyment. *Cogent Business & Management*, *8*(1), 1891661. https://doi.org/10.1080/23311975.2021.1891661

Wang, V., Nnaji, H., & Jung, J. (2020). Internet banking in Nigeria: Cyber security breaches, practices and capability. *International Journal of Law, Crime and Justice*, *62*, 100415. https://doi.org/10.1016/j.ijlcj.2020.100415

Wongmahesak, K., Singh, B., & Kaunert, C. (2025). The complex interplay of generational differences, digital literacy, and cybercrime fear. *Asian Crime and Society Review*, *12*(1), 3-3. https://doi.org/10.14456/acsr.2025.3

Yang, M., Mamun, A. A., Mohiuddin, M., Nawi, N. C., & Zainol, N. R. (2021). Cashless transactions: A study on intention and adoption of e-wallets. *Sustainability*, *13*(2), 831. https://doi.org/10.3390/su13020831

Yeo, C., Kee, D. M. H., Mo, X. Y., Ang, H. E., Chua, S. M., Agnihotri, S., & Pandey, S. (2020). Technology advancement and growth: A case study of Huawei. *Journal of the Community Development in Asia Pasific*, *3*(1), 82-91. https://doi.org/10.32535/jcda.v3i1.711

Yo, P. W., Kee, D. M. H., Yu, J. W., Hu, M. K., Jong, Y. C., Ahmed, Z., ... & Nair, R. K. (2021). The influencing factors of customer satisfaction: A case study of Shopee in Malaysia. *Studies of Applied Economics*, *39*(12), 1–12. https://doi.org/10.25115/eea.v39i12.6839

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

ABOUT THE AUTHOR(S)

1st Author
Daisy Mui Hung Kee is an Associate Professor at the School of Management, Universiti Sains Malaysia. Her areas of interest are in Human Resource Management, Organizational Behavior, Work Values, Leadership, Entrepreneurship, and Psychosocial safety climate. Her current program of research focuses on Leadership and Psychosocial safety climate. She holds a PhD in Business and Management from the International Graduate School of Business, University of South Australia. She was the secretary of the Management Case Study Journal, Australia (2004-2006). She was the recipient of the Merdeka Award 2006 from the Australia Malaysia Business Council of South Australia (AMBCSA) by former South Australia Governor Sir Eric Neal (2006). The award recognizes the Most Outstanding Malaysian University students in South Australia. She earned her MBA from the School of Management, Universiti Sains Malaysia. She was awarded to the Dean's List for being one of the top MBA students (2003). Presently, she is an active academic and researcher supervising a number of MBA, MA, and PhD candidates with working experience across diverse industries. She has published a good number of journal papers during the course of her career. She has conducted a series of training sessions related to motivation and research at USM under the Professional and Personal Development (PPD) workshop.
Email: daisy@usm.my.
ORCID ID: https://orcid.org/0000-0002-7748-8230

2nd Author
Hui Ni Lim is currently an undergraduate student at Universiti Sains Malaysia.
ORCID ID: https://orcid.org/0009-0000-8162-0241

3rd Author
Boon Chuen Lim is currently an undergraduate student at Universiti Sains Malaysia.

4th Author
Hui Yeng Lim is currently an undergraduate student at Universiti Sains Malaysia.

5th Author
Shuet Enn Lim is currently an undergraduate student at Universiti Sains Malaysia.

6th Author
Wei Yih Lim is currently an undergraduate student at Universiti Sains Malaysia.

7th Author
A. J. Ali has been a senior lecturer at the School of Management, Universiti Sains Malaysia since 2003. He received his PhD from the University of Groningen, the Netherlands, with a thesis entitled “The intercultural adaptation of expatriate spouses and children”. He is now attached to the Department of International Business and has been teaching courses and conducting research in International Human Resource Management, International Management, International Business, Business Communication, and Organizational Behavior.
Email: aneesali15@yahoo.com