Jurnal Ilmiah Manajemen dan Bisnis
Volume 10, Number 1, 2025 pp. 100-110
P-ISSN: 2528-2077 E-ISSN: 2528-1208
Open Access: https://journal.undiknas.ac.id/index.php/manajemen/

Enhancing Customer Awareness of Cybersecurity Threats in E-Banking: A Study on the Role of AI-based Risk Communication Tools

Musawer Hakimi[1*], Ahmad Jamy Kohistani[2], Faqeed Ahmad Sahnosh[3], Abdul Wahid Samadzai[4], Wahidullah Enayat [5]
[1] Computer Science Department, Samangan University, Samangan, Afghanistan
[2] Department of Computer Engineering, Kaul Polytechnic University, Kabul, Afghanistan
[3]Information Systems Department, Kabul Education University, Kabul, Afghanistan
[4]Softrware Engineering Department, Kabul University, Kabul, Afghanistan
[5]Ondokuz Mayıs University, Samsun, Türkiye

ARTICLEINFO
Article history:
Received: 2025-02-01
Revised: 2025-03-29
Accepted: 2025-05-19
Available Online: 2025-06-25

Keywords:
Cybersecurity awareness; AI trust; e-banking security; risk communication; user behavior

DOI:
https://doi.org/10.38043/jimb.v10i1.6762

ABSTRACT
With This study investigates the intersection of user trust and cybersecurity awareness of AI-powered communication systems in e-banking. As the adoption of artificial intelligence by financial institutions was gaining momentum, little was known about how digitally active consumers distinguish between cybersecurity threats and real behavior and how they form their trust in emerging AI-powered risk communication systems. To address this gap, the current study used a mixed-methods approach of quantitative survey and qualitative interview data collection, from e-bank customers who were 18 to 65 years old and digitally literate. The results show a substantial gap between users' sensitivity to cybersecurity risks and their systematic use of protective measures; for example, password updates and multi-factor authentication activation. At the same time, the research points out that trust in AI-powered anti-fraud technologies is quite high, especially when it comes to AI's effectiveness in detecting threats. Yet, skepticism exists toward AI-powered chatbots and auto-notifications, with customers preferring human representatives for high-risk interactions. Above all, the study yields theoretical contribution by identifying age, exposure to digital technologies, and e-banking familiarity as robust predictors of AI trust, while education and income had minimal effect. In practice, the study offers policymakers and financial institutions actionable suggestions for advancing age-targeted cybersecurity education, user-informed AI messaging, and augmented transparency in AI communication design. By bridging the gap between action and awareness, and trust and technology adoption, this research contributes both to the evolving technology acceptance theory and to the practical deployment of AI in safe digital banking environments.

1. INTRODUCTION

The The banking industry has seen a remarkably quick digital transformation over the last decade due to the emergence of mobile and e-banking technology. This transformation has made it easier and faster for customers to do transactions with less dependency on physical branches (Sebastian et al., 2017). Unfortunately, this convenience comes at a price, as the digitization of banking has caused rampant characteristics of cyber security risks. Banks now have to deal with sophisticated cyber attacks, phishing scams, identity thefts, and data breaches that could harm the customer's funds and the institution's integrity (Creado & Ramteke, 2020). Robust, multi-level security architectures are now needed to maintain the integrity of the financial system and maintain consumer trust (Dermine, 2016).

Artificial Intelligence (AI) has emerged as a powerful ally in this process. Artificial intelligence-driven cybersecurity products ranging from machine learning-driven anomaly detection to predictive threat modeling and fraud analysis can follow threats in real time and enhance the response capability (Lallie et al., 2021; Muckin & Fitch, 2019). AI can potentially automate the analysis of customer actions, enhance biometric security, and facilitate threat intelligence sharing between institutions (VanBankers, 2016). But implementing AI tools in user-level systems practically turns out to be major hurdles. Users show little confidence in AI-based decisions, particularly when these applications are employed to replace human interaction, and AI-based notifications or

** Corresponding Author: Musawer Hakimi: musawer@adc.edu.in*

chatbots are met with distrust. In addition, users' adoption of AI is generally ahead of their digital literacy, negating the desired security outcomes.

Adding to the complexity, cybersecurity challenges with e-banking differ considerably globally. For the advanced economies in the U.S. and Western Europe, banks focus on leveraging next-generation AI and complying with robust data privacy laws (e.g., GDPR), but still have challenges dealing with complex attacks on lucrative accounts. Conversely, in regions such as South Asia or parts of Africa, there is minimal digital infrastructure and customer education that lead to more widespread errors through user complacency or low sensitivity, despite widening smartphone-banking coverage (Kshetri, 2021). These geographical differences highlight the imperative for adaptable, user-centric cybersecurity initiatives.

As financial institutions continue to heavily invest in AI-enhanced systems, the majority pay scant attention to one of the key aspects of digital defense customer cybersecurity awareness. Research indicates that the majority of end-users have minimal fundamental knowledge of threats on the net, making them ideal targets for phishing, malware, and social engineering (Farooq et al., 2015). Despite technology, banks will under-prioritize explicit user education, playing down its role in developing cybersecurity defenses (Albrechtsen & Hovden, 2009). This disparity reduces the performance of AI technology and potentially damages trust in online services, encouraging more dependence on and less satisfaction with these services (Svehla et al., 2016). The purpose of this study is to examine the relationship between cybersecurity awareness and user trust in AI-supported security communications in online banking. The study specifically looks at how digital awareness, response behavior, and perceived value of AI tools moderate user satisfaction, trust, and engagement with cybersecurity programs initiated by banks.

This awareness is crucial to crafting cohesive security policies that incorporate technical proficiency alongside shrewd human engagement. With the incorporation of cybersecurity training within the onboarding process of customers and the use of open, transparent communication via AI systems, banks can develop digital trust and customer loyalty (Mbama & Ezepue, 2018). Further, the findings from this study will be applied in informing policymakers and regulators on how to craft more target-oriented and comprehensive cybersecurity literacy programs, particularly in regions with technology adoption challenges.

State of the Art

Technology Acceptance Model (TAM) in e-banking

Several decades later, the Technology Acceptance Model (TAM) remains a powerful model for understanding consumer acceptance of e-banking technology. According to the TAM, perceived usefulness and perceived ease of use are the two basic driving components influencing the intention to adopt this new technology (Hidas, 2024). It would make sense to build on TAM, to also say that perceived security and trust matter to intention to adopt e-banking technologies, and that perceived usefulness is correlated with perceived security and trust associated with the highly sensitive financial information as stated (Johri & Kumar, 2023). Such research has shown that the use of AI-enabled banking shaped more by users confidence in the e-banking mechanism's security mechanisms as well as clarity/ease of use with the user interface (Rahman et al., 2023).

Risk Communication Theories (EPPM)

The Extended Parallel Process Model (EPPM) gives us some useful information on how customers think and react to cybersecurity threats. Good risk communication balances the likelihood of potential cyber threats with the efficacy of suggested protective behaviors to instill customer awareness, Undale and Shinde (2024) state. Apply of EPPM in digital banking means that customers must feel both threat and empowerment by current security controls, such as two-factor authentication or artificial intelligence-driven fraud detection methods (Riasat, Shah, & Gonul, 2025). Möller (2023) stresses that if two-way perception is absent, customers will not engage in safe habits and become more susceptible to cyber incidents.

Cybersecurity Threats in Digital Banking

Phishing, malware and social engineering are common threats that reduce customer security in the e-banking systems. Gupta (2025) provides an exhaustive overview of e-banking crime, noting that phishing attacks exploit customers' trust by masquerading as genuine banking messages, leading to credential theft and financial loss. Malware, in the guise of infected emails or compromised sites, offers a rogue means of access to banking apps and personal devices (Khan et al., 2023). Social engineering also exploits human psychology by manipulating customers into divulging sensitive information or bypassing security measures (Johri & Kumar, 2023). Despite technological countermeasures, these psychology-based vulnerabilities remain a top reason for cybersecurity breach (Saeed et al., 2023).

Customer Vulnerability Metrics

Quantifying customer vulnerability to cyber threats entails quantifying awareness, knowledge, and behavior. Johri and Kumar (2023) conducted a study in Saudi Arabia that indicated the majority of banking customers lack adequate cybersecurity knowledge and are therefore vulnerable to cyberattacks regardless of security protocols in place. Undale and Shinde (2024) emphasize that measuring using standardized tools is essential in quantifying customer preparedness, citing that a lack of knowledge and complacency increase exposure to risk. Dzerve et al. (2023) hypothesis that education in finance through digital innovation is critical to offsetting this weakness by offering customers needed information and skills to identify and respond to cyber threats effectively.

AI-Driven Solutions

Artificial intelligence, and more specifically machine learning (ML), plays a transformational role in detecting and preventing fraud in online banking. Johora et al. (2024) describe how ML models read transactional activity in real time and identify anomalies most probably fraudulent activity so that banks can respond in a timely fashion. Srivastava, Pandiya, and Nautiyal (2024) emphasize that the models learn independently from new data, refining detection accuracy against evolving cyber attacks. Karunambikai (2025) also refers to the implementation of blockchain technology along with AI to provide higher security and transparency for net banking transactions. These technologies significantly reduce fraud dangers, though their success depends on continuous revising and client cooperation in maintaining security protocols.

NLP for Chatbot Warnings

Natural Language Processing (NLP) boosts customer interaction through energizing AI chatbots to give timely cybersecurity warnings and recommendations. Sharma, Preet, and Gupta (2025) describe how NLP enables chatbots to analyze user queries and give context-specific recommendations to enhance customer awareness and engagement. This exchange complements users in detecting possible threats like phishing or malicious transactions, bridging the gap between human judgment and machine-based security systems. Munira and Jim (2024) highlight that chatbots fueled by AI not only provide reactive support but also proactive learning, thus improving users' overall cyber hygiene in online banking environments.

Synthesis of Existing Gaps

Even though AI-driven technologies have progressed significantly when it comes to fraud detection and cybersecurity, gaps in customer awareness and behavioral adaptation still remain. Rodrigues et al. (2022) make an observation that despite robust technical defense mechanisms, cybersecurity is compromised if end-users are not aware and vigilant. Johri and Kumar (2023) refer to a clear absence of customer awareness campaigns reaching or engaging all segments of users in the best possible manner. Furthermore, Tran (2025) also indicates that the lack of sufficient integrated frameworks combining AI innovations with educational interventions presents an image of a broken methodology which compromises cybersecurity resilience.

Additionally, existing measures of vulnerability are disparate and seldom account for future-oriented cyber threats and diverse customer profiles (Undale & Shinde, 2024). Literature also presents a research imbalance in terms of technology development being the main theme of most studies while neglecting the socio-psychological determinants of customer behavior (Dzerve et al., 2023; Saeed et al., 2023). Closing such gaps requires an integrated approach bridging AI technologies and focus, theory-driven awareness programs founded on models like TAM and EPPM.

2. METHOD

This study employs a sequential mixed-method design to explore the effects of cybersecurity awareness on trust in AI-based security software for e-banking. Triangulation of methods by employing both quantitative and qualitative approaches strengthens methodological triangulation and allows richer, more accurate, and credible understandings of behavioral patterns and personal narratives (Creswell & Plano Clark, 2018, cited in Dzerve et al., 2023).

The rationale for using the method here is that it can collect breadth (through surveys) and depth (interviews). While one could assert that quantitative data results in generalizations based on larger samples, qualitative data offered rich context, mainly in a space where trust in AI chatbots trails confidence in AI tools in general.

Research Design

In the quantitative phase of our research, the participants will have standardized questionnaire completed looking to understand their knowledge of cyber attacks (e.g., phishing, malware) and trust in bank communications based on AI, e.g., personalized messages versus standard AI messages (Johri & Kumar, 2023; Johora et al., 2024). This was followed by a qualitative phase, with semi-structured interviews between users and security officers in banks, for the purpose of asking them about their experience with AI chatbots, drivers and barriers to trust, and views on the role of AI in bank security (Hidas, 2024; Sharma et al., 2025).

The mixed-method approach was preferred over using only quantitative or qualitative methods because it is possible to cross-validate and converge data to raise the reliability of results specifically in quantifying rich user sentiment and confirming behavior patterns with statistical evidence.

Data Collection

Quantitative Survey

The survey included 384 e-banking clients, who were randomly sampled using stratified sampling to ensure they reflected different age groups and technology experience levels to provide representativeness. The sample size was calculated to achieve a 95% confidence level and 5% margin of error (Hameed & Nigam, 2023). A 15-item Likert scale questionnaire was completed using Google Forms to provide greater reach and convenience in handling data (Kaur, 2025).

Prior to launch, a pilot test of 30 respondents was done to confirm the internal consistency of the tool with Cronbach's alpha coefficients above 0.7 (Munira & Jim, 2024).

Qualitative Interviews

Twenty-five participants were purposively sampled: 20 bank customers (distributed by age and digital literacy) and 5 cyber-security bank officers. The sampling was by maximum variation in order to capture varied perspectives. There is a potential for bias, however, as the interviewer could have been representing users already somewhat acquainted with AI systems.

Interviews queried users about their perceived utility and limitations of AI tools in our case, skepticism of chatbots for the strict adherence to voice, the lack of emotional intelligence, rigid responses, and lack of personalized quality traits users would generally expect of human support systems (Srivastava et al., 2024).

This approach represents best practices in studying users' perceptions during periods of technological change in financial environments (Rodrigues et al., 2022).

Data Analysis

Quantitative data were analyzed using SPSS v28. Descriptive statistics were used to evaluate levels of awareness and trust in AI, and inferential statistics such as t-tests and ANOVA were used to analyze group differences. Above all, multiple regression analysis was conducted to identify the most influential predictors of AI alert trust, and how awareness, age, experience, and education affected this (Karunambikai, 2025).

Qualitative data were computed using thematic analysis by NVivo 14 with the use of open and axial coding. Inter-coder consistency was guaranteed at Cohen's kappa of 0.82, and member-checking also guaranteed credibility (Gupta, 2025; Ndukwe & Baridam, 2023).

Ethical Considerations

Ethical integrity is achieved through informed consent from all participants. In addition, survey responses were anonymous, and interviews were de-identified through participant codes for example ("Participant 1," "Participant 2"). Data security and participant privacy were maintained according to accepted ethical best practices for cybersecurity research (Möller, 2023; Undale & Shinde, 2024).

3. RESULT AND DISCUSSION

Results In this section, the results from the quantitative analysis are shared, with an initial summary of the demographics of the participants to contextualize the results relating to Cybersecurity awareness and trust in AI-based risk communication tools. The survey was completed by 384 e-banking customers collectively. The gender breakdown was almost even with men being represented by 50.0% and women at 49.5% of the sample; there were a very small number of people who opted out of reporting their gender (0.5%). The participants were included across a wide age range with the largest cohort being members aged 26–35 years (29.9%), the second

most represented cohort was aged 18-25 years (25.0%) and followed by 36-45 years (22.7%). Representation from the age groups above 45 decreased with 15.1% of respondents aged 46-55 years and only 7.3% being aged 56 and above. The representation of education levels was relatively high, where 47.4% reported having a bachelor's degree and 21.6% having a master's degree or better. Technology use patterns indicated moderate-high technology use: 44.0% reported they used technology for an average of 3-5 hours/day and 38.3% used technology for 6 or more hours a day. Furthermore, the largest number of participants reported using e-banking tools for over three years (60.1%); this indicated that the study had a relatively experienced and digitally literate level of participants. These demographic descriptions provide baseline context for identifying trends associated with Cybersecurity awareness and trust in Artificial Intelligence-backed security risk assessment tools.

Table 1. Demographic Characteristics of Survey Respondents

Variable	Category	Frequency (n)	Percentage (%)
Gender	Male	192	50.0
	Female	190	49.5
	Prefer not to say	2	0.5
Age Group	18–25	96	25.0
	26–35	115	29.9
	36–45	87	22.7
	46–55	58	15.1
	56 and above	28	7.3
Education Level	High school or below	42	10.9
	Diploma/Associate degree	77	20.1
	Bachelor's degree	182	47.4
	Master's degree or higher	83	21.6
Technology Use	Low (0–2 hrs/day)	68	17.7
(Self-reported usage)	Moderate (3–5 hrs/day)	169	44.0
	High (6+ hrs/day)	147	38.3
E-Banking Experience	Less than 1 year	41	10.7
	1–3 years	112	29.2
	More than 3 years	231	60.1

Table 2. Reliability Analysis of Survey Scales Using Cronbach's Alpha

Scale	Number of Items	Cronbach's Alpha (α)
Cybersecurity Awareness	5	0.81
Trust in AI-Based Risk Communication	5	0.79

The reliability analysis shows that both scales had acceptable to good internal consistency. The Cybersecurity Awareness scale had a Cronbach's alpha of 0.81, which is considered good reliability and indicates that measures are all measuring the same construct consistently. The Trust in AI-Based Risk Communication scale also had an alpha of 0.79, which is considered acceptable reliability for research purposes. These values provide a basis for using the scales in further analyses with assurance that the survey items consistently measure the intended psychological constructs. Reliability assessment of these scales adds strength to the validity of findings regarding user awareness and trust of AI tools.

Table 3. Descriptive Statistics for Customer Cybersecurity Awareness

Item	Mean (M)	SD	% Agree (4–5 on Likert scale)
I am aware of common cybersecurity threats in e-banking.	4.12	0.76	78.4%
I can recognize phishing emails/messages.	3.89	0.85	70.3%
I know how to secure my e-banking login credentials.	4.27	0.68	82.6%
I understand how malware can affect my banking data.	3.76	0.93	66.1%
I regularly update my passwords and app settings.	3.51	1.02	58.9%

Note: Awareness measured on a 5-point Likert scale (1 = Strongly disagree to 5 = Strongly agree).

Table 3 provides descriptive statistics for participants' self-reported e-banking cybersecurity awareness. Overall, our participants reported awareness of several important things. What matters most is reporting how to protect e-banking login credentials, where the mean was the highest (M = 4.27, SD = 0.68) with 82.6% of respondents agreeing or strongly agreeing with the statement. The second mark was (78.4%) was reported for awareness of common cybersecurity threats where mean was (M = 4.12, SD = 0.76) suggesting that majority of this customer base was informs of general issues. There was also a high confidence mean when recognized phishing emails/messages, (M = 3.89) and 70.3% agreement, suggest some weaknesses in recognizing the types of threats. Interestingly 66.1%, (M = 3.76) of our responds reported awareness in how malware impacts bank data, while the lowest value was for regular password and app updates, (M = 3.51, SD 1.02) and only 58.9% agree with the statement. The results demonstrate that e-banking users have a fairly strong base understanding of cybersecurity, less so in terms of practical behaviour like updating passwords regularly. The data suggest the distance between awareness and proactive security habits, which might provide an opportunity for educational interventions.

Table 4. Customer Trust in AI-Based Risk Communication Tools

Statement	Mean (M)	SD	% Trust (4–5 on Likert scale)
I trust AI alerts to notify me of suspicious banking activity.	4.01	0.79	76.0%
I feel reassured when AI-powered chatbots provide security updates.	3.78	0.88	69.5%
I prefer AI alerts over generic notifications from customer support.	3.62	0.91	63.2%
I believe AI can accurately detect fraud faster than human agents.	4.09	0.74	81.1%
I feel confident using AI-assisted security tools (e.g., 2FA chatbots).	3.94	0.81	73.7%

Note: Trust measured on a 5-point Likert scale (1 = Strongly disagree to 5 = Strongly agree).

Table 4 summarizes e-banking respondents' confidence in the AI-based risk communication tools. On the whole, findings suggest users exhibit a moderately high level of confidence in AI and related technologies. For instance, the highest mean was for believing that AI can correctly identify fraud faster than human agents (M = 4.09, SD = 0.74); 81.1% of participants indicated that they believed in this ability. This finding suggests that users understand AI is both more efficient and reliable in identifying a cyber threat when compared to human-based systems used for fraud detection. Users also reported a great deal of trust in AI alerts to notify them of suspicious activity (M = 4.01, SD = 0.79), with 76.0% of respondents agreeing with this statement demonstrating trust in AI's abilities in real-time monitoring. Likewise, 73.7% of users reported being confident using AI-assisted tools such as two-factor authentication (M = 3.94, SD = 0.81), which suggests they were open to using AI in some aspects of the security features online banking services offered. Slightly lower trust scores were provided by users when information from AI-powered chatbots stayed up-to-date (M = 3.78, 69.5%) and with users indicating they preferred AI alerts over messages from customer support (M = 3.62, 63.2%); thus, while users were confident in the performance of AI in accomplishing tasks, especially overall journey and real-time monitoring, they still appreciated elements of personal, human interaction. As these findings suggest, there are opportunities for banks and related institutions to increase confidence through stronger communication of functionality and more personalized interactions with AI applications like chatbots.

Table 5. Multiple Regression Analysis Predicting Trust in AI Alerts

Predictor Variable	B	SE B	β	t	p-value
Cybersecurity Awareness Score	0.42	0.06	0.45	7.00	< .001 **
Technology Use (hrs/day)	0.18	0.07	0.17	2.57	.011 **
E-Banking Experience (years)	0.21	0.05	0.22	4.20	< .001 **
Age	-0.05	0.04	-0.06	-1.25	.213
Education Level	0.07	0.06	0.06	1.17	.243

Model Summary: ***$R^2 = 0.39$, Adjusted $R^2 = 0.37$, $F(5, 378) = 48.54$, $p < .001$***

The results from the multiple regression revealed significant predictors of customer trust in alerts, as shown in Table 5. The regression was significant (F (5, 378) = 48.54, p < .001) and accounted for 39% of the

variance (R^2 = 0.39). In summary, cybersecurity awareness had the strongest and most significant predictive validity (β = 0.45, p < .001) indicating that holding all else constant, the more the user scored on the cybersecurity awareness questions, the more likely the user was to trust the AI-based alerts. Furthermore, both technology use (β = 0.17, p = .011) and experience with e-banking (β = 0.22, p < .001) were significant predictors indicating that familiarity with technology and digitalization builds trust in AI-based tools. Results also showed that age and education level were not significant, suggesting that behavioral and experiential factors play a larger role than demographic factors. These results indicate the need for awareness-building strategies to foster banking customer trust in AI-based applications.

Table 6. ANOVA Results: Differences in Cybersecurity Awareness by Age Group

Source	SS	df	MS	F	p
Between Groups	12.84	4	3.21	4.68	.001
Within Groups	257.40	379	0.68		
Total	**270.24**	**383**			

Post hoc (Tukey's HSD):

1. Significant difference between 18–25 and 46–55 age groups (p = .003)
2. No significant difference between 26–35 and 36–45 groups (p = .412)

Interpretation: Older users (especially those 46–55) reported lower awareness levels compared to younger cohorts, suggesting the need for age-targeted cybersecurity education.

Table 6 presents the outcomes of a ANOVA evaluation of the cybersecurity awareness score, which was conducted using age group. Overall, results indicated that age had a significant impact on awareness, F (4, 379) = 4.68, p = .001, demonstrating that awareness differed significantly by age group. In other words, age groups had significant differences in awareness.

The between group variation (SS = 12.84) and the within group variation (SS = 257.40) was categorically justified that age influences differences in knowledge about lay understanding about cybersecurity related events and actions. Post hoc analysis using Tukey's HSD test was utilized to measure the significant difference statistically observed between the youngest cohort (18–25 years) and and the 46 - 55 age cohort of (p = .003 - significant difference). This indicates that middle-aged users in the 46 – 55 year cohort have considerably less knowledge about cybersecurity than the younger users (18 – 25).

There were no significant differences between adjacent age groups (i.e., 26 - 35 and 36 - 45 ad 0.412) indicating great awareness heighted to users those two middle-age cohorts of users are close comparable regardless of their level of awareness.

Overall, there are significant distinctions and differences in the age cohorts analyzed in our study and that likely older cohorts, specifically those users in the 46 - 55, would need specific and tailored educational initiatives and funded awareness campaigns to help increase and write education and awareness around their digital understand to build their knowledge more effectively to manage their digital banking and related activities. Is this study could support these age development strategies there is some spacing to write out the age-based strategies we need to plug gaps in terms of their existing knowledge in the area of e - banking security.

Table 7. Thematic Summary of Interview Responses from Customers

Theme	Description	Frequency
Perceived Usefulness of AI Tools	AI tools help detect fraud quickly and provide peace of mind.	15
Skepticism Toward Chatbots	Concerns about chatbot accuracy and lack of human-like interaction.	11
Need for More Guidance	Users request tutorials and clearer messages from banks about threats.	14
Trust Based on Past Experiences	Trust in AI is linked to whether past alerts were accurate or helpful.	12
Preference for Personalization	Users trust alerts more when tailored to their behavior and language.	13

Note: Themes were identified through inductive thematic analysis using NVivo 14. Quotes were coded and clustered into categories during open and axial coding phases.

Twenty customers were interviewed about their perceptions and interactions with AI tools for the purposes of banking fraud detection, and from the interviews, five key themes emerged. The first theme, acceptance of the Perceived Usefulness of AI Tools, was reported more than any other theme, by 15 of the participants reported the usefulness of AI tools to quickly identify fraudulent activity. Many mentioned that these

tools provided a sense of security and peace of mind, and almost all of the participants mentioned confirming fraudulent activity by following up on alerts as quickly as possible to avoid losing money in the bank. Even though the majority of participants could see benefits of AI, 11 users brought up concerns of Skepticism Toward Chatbots. Users had mentioned that they were unsure if the answers provided by chatbots were accurate and felt like there was not the same naturalness and empathy in the exchanges found in communication with humans, which contributed to their skepticism in trusting AI-driven chatbots as legitimate sources of information or assistance.

Another prominent theme was a Need for More Guidance, with 14 users asking that banks provide clearer communication and tutorials. Participants mentioned that they wanted to have clear communication about how to interpret alerts and to identify potential threats. Participants suggested that receiving more guidance could help foster trust and encourage users to further engage with the AI tools by gaining confidence in their use. Trust Based on Previous Experiences was also very important. 12 respondents indicated that their trust in AI alerts was fairly dependent on their prior experiences of the accuracy and helpfulness

Table 8. Mean Cybersecurity Awareness by Age Group

Age Group	Mean Awareness Score	Standard Deviation (SD)	Sample Size (n)
18–25	4.02	0.72	96
26–35	3.95	0.75	115
36–45	3.89	0.78	87
46–55	3.61	0.81	58
56 and above	3.67	0.79	28

Table 8 reveals the average cybersecurity awareness scores across age groups and contributes to the explanation of how age impacts user knowledge of e-banking threats. The highest awareness score occurred in the 18-25 age group (M = 4.02), followed closely by the 26-35 group (M = 3.95). The younger groups had slightly lower standard deviations in scores indicating that the groups had more similar levels of awareness within their age groups. In contrast, users from the 46-55 age group had the lowest mean average awareness score (M = 3.61), and therefore could be a more vulnerable population in regard to phishing, malware, or insecure digital practices. Similarly, the cohort aged 56 and older exhibited a mean score slightly above users 46-55 (M = 3.67), but well below mean scores for ages 18-35. The data indicate that, as one ages, awareness declines which certainly supports the ANOVA and post hoc findings of a statistical difference from the youngest group initiated to the mid-older age groups.

The data underscores the need for age-specific awareness-raising activities, and in particular users aged 46 and older. Financial institutions should consider implementing tailored educational campaigns to promote awareness among these users, which would allow for the more supported and secure adoption of AI-enabled banking technology by these users, as well as increased trust in cybersecurity technologies across age demographics.

Discussion

The results from this research provide an important contribution to understanding the perceptions of cybersecurity and trust in AI-driven risk communication tools for consumers of e-banking, and contribute to the literature on banking digital transformation and cybersecurity. The relatively high level of cybersecurity awareness noted with the respondents, especially with regard to their responses about identifying common risks and protecting login credentials, reflects the heightened emphasis on user education following the surge in the digitalization of banking services (Dzerve et al., 2023; Munira & Jim, 2024). Yet the gap between awareness and persistent security behaviors like occasional password changes identified here highlights the ongoing issue of turning knowledge into proactive behavior a concern shared by Undale and Shinde (2024), who underscore that digital literacy by itself does not produce behavioral change without interventions targeted at it.

In line with prior research highlighting AI's game-changing role in fraud identification and risk messaging (Johora et al., 2024; Sharma et al., 2025), AI-based security tool trust was an emergent driver of user adoption. According to Rahman et al. (2023), there is the belief that financial institutions based on AI can improve the effectiveness of threat mitigation with the trust in AI to identify fraud quicker than agents.Lower trust in AI chatbots, however, also indicates the potential for improvement of AI experience design and personalization to limit distrust and support user satisfaction (Hameed & Nigam, 2023; Ndukwe & Baridam, 2023). This aligns with

work calling for AI-based systems to integrate technical competency with displays of empathy to develop trustworthy customer relationships (Jim & Munira, 2024).

In terms of demographics, there is a correlation between age and cybersecurity awareness, with middle-aged users being less aware and needing defined age ranges and educational programs for users in different groups (Johri & Kumar, 2023; Möller, 2023). With regard to the findings in this study, I was surprised that the behavioral variables dealing with technology adoption, and knowledge of e-banking were more indicative of trust in AI tools than demographic variables, so I posit that there are moderating influences on the differential effect of being aware of users being knowledgeable of technology in adoption models (Kaur, 2025; Riasat et al., 2025). All of these findings have ramifications on the larger issue of banking related digital transformation and cyber resilience. The combine capabilities of AI, and effective cybersecurity training can enable a user, and build some amount of trust that is relevant to overcoming cyber threats (Rodrigues et al., 2022; Tran, 2025).

Therefore, it should be the case that financial institutions develop comprehensive strategies that will not just only apply advanced components of AI, but also awareness for the user and engagement through open conversations and direct support for the user (Karunambikai, 2025; Srivastava et al., 2024).

4. CONCLUSION

This study provides robust evidence on the connection between user trust in AI-driven risk communication technology and cybersecurity awareness in an e-banking setting. The findings emphasize the digitally literate user persona namely, users aged 18 to 45 years with high levels of education and extensive e-banking history. Although these users exhibit a reasonable level of knowledge about cybersecurity threats, such as phishing and credential security (above 80% of users), there remains a significant awareness–action gap. Fewer than 60% of users responded that they only regularly updated their application settings or passwords, indicating that awareness does not necessarily result in proactive security action.

Users display a high level of trust in AI-based fraud detection systems in relation to their ability to detect suspicious behaviours more quickly and efficiently than humans. There is found in users, a suspicion of AI chatbots where uneasiness has arisen from athletes' prior experiences around being aware of their transparency, lack of empathy, and not having a human-like experience. This shows that while individuals desire to be able to use AI systems effectively, they have a vested interest in trusting the AI systems and being satisfied with the experience of using them.

Age was also a notable determinant of cybersecurity awareness, with users in the 46 + group having lower awareness scores. The regression results revealed that awareness, technology use, and e-banking experience significantly predicted the users' trust in AI tools; the demographic variables (age and education) were weak predictors. These results support the claim that demographic status is not the basis for trust; it is based on experiential and behavioral factors.

Policy and Practice Implications

Banks must act to close the awareness–action gap. Cybersecurity awareness activities must be action-oriented, not merely risk-focusing but also teaching users about usable controls such as regular password updates, app hygiene, and awareness of suspicious messages.

Given older users' relatively lower awareness rates, banks must make age-specific interventions such as easy user interfaces, user guide tutorial walkthroughs, and step-by-step visual explanations a priority. The interventions must be inclusive in tone as part of a wider approach to address different levels of technology skills.

To facilitate user trust in AI communication channels, it is critical for banks to rethink the design of AI chatbots with natural language understanding, transparency features and customization based purely on user actions and behaviours. Personalized alerting indicating actual spending, with consideration to the users' level of spending habits and preferences for the way it communicates with them, will develop trustworthiness and emotional connection.

Regulators, banks, and AI developers should collaborate to create explanatory AI frameworks and responsible digital engagement. Policy incentives for ongoing cybersecurity education can also further solidify public trust in AI systems as well as future-proofing digital banking infrastructure.

Banks, regulators, and suppliers must collaborate to embed AI into a people-cantered cybersecurity policy a proactive, educational, transparent, and inclusive one. Through the integration of technical innovation and targeted user engagement, e-banking systems can be made secure, robust, and reliable digital ecosystems for everyone.

5. REFERENCES

Dzerve, B., Spilbergs, A., Innuse, G., Ozolina, S., Stonane, A., & Maditinos, D. (2023). A Shift in Paradigm: the Financial Education Under the Influence of Digital Transformation. In *Digital Transformation, Strategic Resilience, Cyber Security and Risk Management* (Vol. 111, pp. 61-82). Emerald Publishing Limited. https://doi.org/10.1108/S1569-37592023000111A005

Gupta, S. (2025). Hacking the System: A Deep Dive into the World of E-Banking Crime. *The Techno-Legal Dynamics of Cyber Crimes https://doi.org/10.1109/ICIS64839.2024.10887499*

Hameed, S., & Nigam, A. (2023). Exploring India's Generation Z perspective on AI enabled internet banking services. *foresight*, *25*(2), 287-302. https://doi.org/10.1108/FS-10-2021-0213

Hidas, R. E. (2024). *Consumer acceptance of the usage of artificial intelligence in the banking sector* (Doctoral dissertation). http://hdl.handle.net/10400.14/47704

Jim, M. M. I., & Munira, M. S. K. (2024). The Role Of AI In Strengthening Data Privacy For Cloud Banking. *Innovatech Engineering Journal*, *1*(01), 10-70937. https://dx.doi.org/10.70937/faet.v1i01.39

Johora, F. T., Hasan, R., Farabi, S. F., Akter, J., & Al Mahmud, M. A. (2024). AI-Powered Fraud Detection in Banking: Safeguarding Financial Transactions. *The American journal of management and economics innovations*, *6*(06), 8-22. https://doi.org/10.37547/tajmei/Volume06Issue06-02

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

Jyothi, V. E., & Chowdary, N. S. (2024). Challenges and Artificial Intelligence–Centered Defensive Strategies for Authentication in Online Banking. *Artificial Intelligence Enabled Management: An Emerging Economy Perspective*, *105*. https://doi.org/10.1515/9783111172408-007

Karunambikai, R. (2025, April). Securing Net Banking Transactions: The Dynamic Duo of AI and Blockchain Technology. In *2025 8th International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 668-673). IEEE. https://doi.org/10.1109/ICOEI65986.2025.11013158

Kaur, S. (2025). Banking Transformation: Artificial Intelligence's Effect on the Current Financial Environment. In *Navigating Data Science in the Age of AI: Exploring Possibilities of Generative Intelligence* (pp. 131-145). Emerald Publishing Limited. https://doi.org/10.1108/978-1-83608-432-720251007

Khan, H. U., Malik, M. Z., Nazir, S., & Khan, F. (2023). Utilizing bio metric system for enhancing cyber security in banking sector: A systematic analysis. *Ieee Access*, *11*, 80181-80198. https://doi.org/10.1109/ACCESS.2023.3298824

Möller, D.P.F. (2023). Cybersecurity in Digital Transformation. In: Guide to Cybersecurity in Digital Transformation. Advances in Information Security, vol 103 . Springer, Cham. https://doi.org/10.1007/978-3-031-26845-8_1

Munira, M. S. K., & Jim, M. M. I. (2024). The Role Of AI In Strengthening Data Privacy For Cloud Banking. *Available at SSRN 5083379*. https://dx.doi.org/10.2139/ssrn.5083379

Ndukwe, E. R., & Baridam, B. (2023). A Graphical and Qualitative Review of Literature on AI-based Cyber-Threat Intelligence (CTI) in Banking Sector. *European Journal of Engineering and Technology Research*, *8*(5), 59-69. https://doi.org/10.24018/ejeng.2023.8.5.3103

Rahman, M., Ming, T. H., Baigh, T. A., & Sarker, M. (2023). Adoption of artificial intelligence in banking services: an empirical analysis. *International Journal of Emerging Markets*, *18*(10), 4270-4300. https://doi.org/10.1108/IJOEM-06-2020-0724

Riasat, I., Shah, M., & Gonul, M. S. (2025). Strengthening Cybersecurity Resilience: An Investigation of Customers' Adoption of Emerging Security Tools in Mobile Banking Apps. *Computers*, *14*(4), 129. https://www.mdpi.com/2073-431X/14/4/129

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), 6666. https://www.mdpi.com/1424-8220/23/15/6666

Rodrigues, A. R. D., Ferreira, F. A., Teixeira, F. J., & Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. *Research in International Business and Finance*, *60*, 101616. https://doi.org/10.1016/j.ribaf.2022.101616

Sharma, S., Preet, K., & Gupta, N. (2025). The Role of Artificial Intelligence in a New Paradigm: Redefining the Banking Landscape. In *Generative AI in FinTech: Revolutionizing Finance Through Intelligent Algorithms* (pp. 291-308). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-76957-3_15

Srivastava, A., Pandiya, B., & Nautiyal, N. S. (2024). Application of Artificial Intelligence in Risk Assessment

and Mitigation in Banks. *Artificial Intelligence for Risk Mitigation in the Financial Industry*, 27-52. https://doi.org/10.1002/9781394175574.ch2

Tran, T. N. (2025). Systematic Review of Cybersecurity in Banking: Evolution from Pre-Industry 4.0 to Post-Industry 4.0 in Artificial Intelligence, Blockchain, Policies and Practice. *arXiv preprint arXiv:2503.00070*. https://doi.org/10.48550/arXiv.2503.00070

Undale, P. S., & Shinde, V. (2024). Digital Transformation and Cyber Security: Unveiling Awareness. *Humanities & Language: International Journal of Linguistics, Humanities, and Education*, *1*(3), 191-197. https://doi.org/10.32734/ayr9wh15