CINEFORUM
ISSN : 0009-7039
Vol. 65. No. 2, 2025

Assessing Customer's Awareness of Cybersecurity Measures in Online Banking: A Study on Digital Trust and Risk Perception

[1]Kshitij Shukla; [2]Dr Sultan Ahmad; [3]Dr Priyanka Bajpai; [4]Neha Srivastava; [5]Dr. Rafat Fatima

[1]Research scholar, Department of Commerce, Integral University, Lucknow

[2]Assistant Professor, Department of Commerce, Integral University, Lucknow

[3]Assistant Professor, Department of Business Management, Integral Business School, Integral University.

[4]Academician, India

[5]Assistant Professor, Department of Economics, Faculty of Humanities & Social Sciences, Integral University Lucknow.

ORCID ID- [2]0000-0002-3746-8921; [5]0009-0007-7304-0635

Corresponding Author: Dr. Sultan Ahmad

Abstract

Cybersecurity has arisen as a serious worry in the quickly changing digital banking environment, especially as banks deploy innovative technology to streamline operations and improve customer experience. This study investigates consumer awareness of online banking security requirements and how digital trust and perceived risk affect customer behaviour. As cyber threats such as phishing, spyware, ransomware, and data breaches become increasingly sophisticated, banks must protect sensitive information while still fostering customer trust. This study collects users' awareness of common cybersecurity practices, including password hygiene, the use of two-factor authentication, and knowledge of banking rules such as the RBI's digital security guidelines, using a structured questionnaire distributed to 151 respondents from urban, semi-urban, and rural areas. The poll demonstrates considerable differences in user awareness, given that a large majority of respondents were either unaware of or uninterested in fundamental cybersecurity safeguards such as reporting fraud or avoiding dangerous online habits such as visiting banking sites via public Wi-Fi. Although individuals had faith in their bank's cybersecurity measures, they expressed reservations about utilising mobile banking apps and doing significant online transactions. The findings highlight the critical necessity for financial institutions to actively educate clients, enact strong security legislation, and maintain open lines of communication about digital threats and preventive measures. Increasing digital

skills and trust may considerably reduce exposure to hackers and boost consumer confidence in online banking. This article adds to the existing discussion about fintech risk management by addressing user concerns and providing practical tips for banks to better adapt their cybersecurity outreach programs.

Keywords: Cybersecurity Awareness, Online Banking, Digital Trust, Risk Perception, Phishing, Consumer Behavior, Financial Technology, RBI Guidelines

Introduction

The banking business has seen tremendous digital transition in recent decades, as evidenced by the growth of online and mobile banking services. With the increased integration of digital technology, financial institutions may now provide customers with convenient, real-time, and user-friendly services (Alrababah, 2024). Because of its ease of use and efficiency, online banking has become the preferred medium for financial transactions. However, the transition from traditional to digital banking has exposed the industry to a number of cybersecurity risks. As banking customers' digital footprints grow, so does their vulnerability to dangers including phishing assaults, data breaches, malware infections, and identity theft (Choudhuri, 2024). In such an atmosphere, cybersecurity becomes critical, particularly since financial data and personal credentials are regularly sent via digital means. The increase in cyber threats to the banking sector has raised worries about customer safety and institutional resilience. Reports of cyberattacks on banks have become more regular, with attackers using sophisticated tools to exploit system flaws or fool unwary people. In this setting, client understanding of cybersecurity is critical for risk mitigation. A well-informed client who understands potential threats and uses secure digital behaviours can considerably lower the likelihood of security breaches. However, studies show a lack of consumer knowledge about secure banking behaviour, making users the weakest link in the cybersecurity chain. This gap highlights the critical necessity to analyse customers' awareness of online hazards and the precautions they take to protect themselves. Digital trust and risk perception are important factors influencing customer behaviour in online banking systems (Vafaei-Zadeh, 2025). Trust in the bank's digital infrastructure—its applications, websites, and data protection policies—encourages clients to use digital services confidently. Customers may be discouraged from completely adopting internet banking if they have a high risk perception, whether due to previous poor experiences or a lack of information. Understanding how cybersecurity awareness influences trust and risk

perception can help banks better understand client expectations and areas that demand more digital literacy.

The primary research question addressed in this study is the varied level of customer awareness of cybersecurity measures in online banking, as well as how this understanding effects trust and perceived risk (Krishna, B, 2025). This study is significant because it provides empirical facts to help banks and policymakers understand the present state of digital security awareness among users. It also offers recommendations to design more targeted awareness campaigns and digital literacy programs. The primary research questions guiding this investigation include: (1) What is the current level of cybersecurity awareness among online banking users? (2) How does cybersecurity awareness impact digital trust? (3) How does it influence perceived risk in digital financial transactions?

This study is organised as follows: following the introduction, the second section examines important literature on cybersecurity in online banking, digital trust, and risk perception. The third section discusses the research approach, which includes the design, data collection tools, and analytical techniques. The fourth portion contains the study's findings, which are then discussed in the fifth section. The final section of the report summarises major findings, consequences, and recommendations for further research.

Review of literature

Author(s) & Year	**Title of Study**	**Key Findings**	**Relevance to Present Study**
Cele & Kwenda (2025)	Do cybersecurity threats and risks have an impact on the adoption of digital banking?	Phishing, malware, and identity theft hinder adoption of digital banking; recommends robust cybersecurity strategies.	Supports the study's aim of examining how cybersecurity risks influence digital banking adoption.
Choudhuri et al. (2024)	An Analysis of Factors Influencing Consumer Trust in Online Banking Security Measures	Trust is influenced by transparency, regulatory compliance, and	Directly aligns with consumer trust and online banking security

		customer-centric security practices.	measures in digital platforms.
Hasan et al. (2025)	Evaluating the Impact of Financial Literacy and Cyber Security Perceptions on Customer Satisfaction with Online Banking Services in Pakistan	Cybersecurity is a major factor in user satisfaction; financial literacy plays a lesser role in adoption.	Confirms that perceived security impacts satisfaction and trust, core themes of this research.
Johri & Kumar (2023)	Exploring Customer Awareness towards Their Cyber Security in the Kingdom of Saudi Arabia	Phishing and hacking awareness improve customer satisfaction; banks need to offer proactive cybersecurity assistance.	Emphasizes importance of user awareness in shaping trust and satisfaction, key to present study.
Alrababah et al. (2024)	The Effect of User Behavior in Online Banking on Cybersecurity Knowledge	Cybersecurity knowledge strongly affects user behavior; calls for improved training and system design.	Highlights behavior-awareness link, reinforcing the need for digital literacy and secure practices.
Limna et al. (2022)	The Relationship between Cyber Security Knowledge, Awareness and Behavioural Choice Protection among Mobile Banking Users in Thailand	Awareness and knowledge significantly affect behavioral choice protection; banks should enhance user-centric security strategies.	Provides quantitative evidence of how awareness and knowledge shape user protection behavior.
Kritika Law (2007)	Impact of Perceived Security on Consumer Trust in Online Banking	Perceived security affects trust marginally; privacy is the most influential factor in trust development.	Adds theoretical depth on security-trust relationship and validates privacy as a key trust enabler.

Research Objectives

- To evaluate the level of customer awareness regarding cybersecurity in online banking
- To analyse the relationship between awareness and digital trust
- To assess how risk perception influences customer behavior

Hypothesis:

H0: Higher levels of customer awareness of cybersecurity measures have a significant positive impact on their level of digital trust in online banking services.

Research Methodology

This study adopts a quantitative research approach to assess customer awareness of cybersecurity measures in online banking and its influence on digital trust and risk perception. The research design is descriptive and correlational, aiming to quantify relationships between awareness levels, trust, and perceived risks among banking customers (Maqbool et al., 2022) Data were collected through a structured questionnaire comprising closed-ended questions and Likert scale items designed to capture information on cybersecurity practices, awareness of threats (e.g., phishing, password safety, secure access), trust in banking systems, and perceived online transaction risks. The target population included active users of online banking services across different age groups and educational backgrounds. A purposive sampling technique was employed, and a total of 151 valid responses were obtained for the study. The questionnaire was pre-tested to ensure clarity and reliability, with a Cronbach's alpha test applied to check the internal consistency of the key scales. Data analysis was conducted using SPSS software, incorporating descriptive statistics (mean, standard deviation, frequencies), correlation analysis to determine associations between variables, and multiple regression analysis to identify predictors of digital trust and risk perception (Khan et al., 2024). Weighted averages were computed to understand respondent tendencies across variables. Highest awareness was observed in understanding two-factor authentication (A4 = 3.38), while the lowest was in reporting suspicious activities (A6 = 2.83), indicating gaps in cyber incident response knowledge (Kaur & Arora, 2023; Jain & Gupta, 2020).**Pearson correlation coefficients** were calculated to explore relationships between cybersecurity awareness indicators (A1–A7) and digital trust factors (D1–D5). All correlations were positive and statistically significant ($p < 0.000$), with the strongest association between A4 and D1 ($r = 0.88$) and D2 ($r = 0.85$),

reinforcing the critical role of user understanding in perceived trust (Davis, 1989; Gefen et al., 2003).An **Exploratory Factor Analysis (EFA)** using PCA was conducted to identify latent structures. Components with **eigenvalues > 1** were retained based on **Kaiser's Criterion** (Kaiser, 1977). Two principal components explained **75% of the total variance**, with Component 1 capturing **general cybersecurity trust** and Component 2 representing **system support/security behavior**. Loadings were strongest for A4 (0.88), A1 (0.75), and A3 (0.74), indicating their centrality in shaping trust (Hair et al., 2010; Jolliffe & Cadima, 2016).All variable relationships showed **statistical significance at p < 0.000** (Table 4), supporting the hypothesis that cybersecurity awareness significantly influences digital trust. These results validate the theoretical underpinnings of TAM and trust-based models (Siau & Shen, 2003; Yousafzai et al., 2009).

The methodology was designed to ensure the findings are statistically valid, generalizable within the context of the sampled population, and capable of offering actionable insights into customer behavior in the digital banking ecosystem.

Data analysis

Gender					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	110	72.8	72.8	72.8
	Female	41	27.2	27.2	100.0
Age					
Valid	Below 20	33	21.9	21.9	21.9
	21-30	29	19.2	19.2	41.1
	31-40	20	13.2	13.2	54.3
	41-50	40	26.5	26.5	80.8
	Above 50	29	19.2	19.2	100.0
Type of Area					
Valid	Urban	53	35.1	35.1	35.1
	Semi-Urban	71	47.0	47.0	82.1
	Rural	26	17.2	17.2	99.3

The demographic profile of the study's respondents reveals valuable insights into the sample composition and online banking usage patterns. Out of 151 participants, a significant majority were male (72.8%), while females constituted 27.2% of the sample. In terms of age distribution, the largest proportion fell within the 41–50 age group (26.5%), followed by those below 20 years (21.9%), and both the 21–30 and above 50 age groups at 19.2% each. The least represented were individuals aged 31–40, comprising 13.2% of the sample. Regarding geographical classification, respondents from semi-urban areas dominated (47%), followed by urban residents (35.1%) and rural participants (17.2%). This demographic breakdown provides a diverse perspective for analyzing consumer awareness of cybersecurity measures, with broad representation across age brackets, gender, and residential areas, thereby ensuring balanced insights into digital trust and risk perception in the context of online banking.

Awareness of Cybersecurity Measures

Statement	Strongly Disagree (%)	Disagree (%)	Neutral (%)	Agree (%)	Strongly Agree (%)
I am aware of the common cyber threats (e.g., phishing, malware) in online banking.	21.9	9.3	11.3	48.3	9.3
I regularly update my banking passwords.	22.5	11.3	10.6	49.7	6
I avoid accessing online banking on public Wi-Fi or shared computers.	19.2	11.9	18.5	35.8	14.6
I understand how two-factor authentication (2FA) enhances banking security.	9.3	17.9	17.2	37.1	18.5
I read security-related notifications or tips shared by my bank.	21.9	19.2	13.2	26.5	19.2
I know how to report suspicious online banking activities to my bank.	21.2	26.5	13.2	25.8	13.2

I am aware of RBI/Bank guidelines on secure digital transactions.	27.2	13.9	13.2	26.5	19.2

Digital Trust in Online Banking

Statement	Strongly Disagree (%)	Disagree (%)	Neutral (%)	Agree (%)	Strongly Agree (%)
I trust my banks online platform to keep my personal and financial data secure.	23.8	6.6	9.9	50.3	9.3
I believe my bank has robust cybersecurity systems in place.	18.5	11.3	9.9	48.3	11.9
I am confident that my bank will handle any fraud efficiently.	24.5	12.6	7.9	43	11.9
I feel safe performing large financial transactions online.	24.5	16.6	7.9	43	7.9
I trust mobile banking apps as much as internet banking portals.	28.5	8.6	7.9	43	11.9

Examining customer comments on digital trust in online banking systems provides a multifaceted view of user confidence in the cybersecurity system of financial institutions. Of those polled, fifty percent indicated they trusted their bank to protect financial and personal information; 23.8% said they did not, indicating significant skepticism among a quarter of customers. Similarly, 48.3% believed their bank had good cybersecurity policies; 11.9% strongly agreed and 29.8% were unsure in various degrees. Opinions on the bank's ability to handle fraud showed a split: While 43% agreed and 11.9% strongly agreed, a notable 37.1% either strongly disagreed or disagreed, suggesting a lack of faith in institutional fraud response procedures. Big online transactions evoked different feelings of safety; 43% felt at ease while 41.1% expressed concern, suggesting persistent questions about the security of high-value transfers. Finally, mobile banking apps raised the greatest uncertainty when compared to internet banking portals; 28.5% of users strongly disagreed and 43% felt otherwise. This disparity suggests that although consumers could use digital banking technologies, their trust

is often conditional and influenced by platform sort and perceived institutional readiness. These combined findings highlight the pressing need for banks to increase transparency, communication, and proactive security support in order to boost user trust in a growing digital banking ecosystem.

Research Methodology

Hypothesis:

Higher levels of customer awareness of cybersecurity measures have a significant positive impact on their level of digital trust in online banking services.

Figure 1 Awareness of Cybersecurity Measures

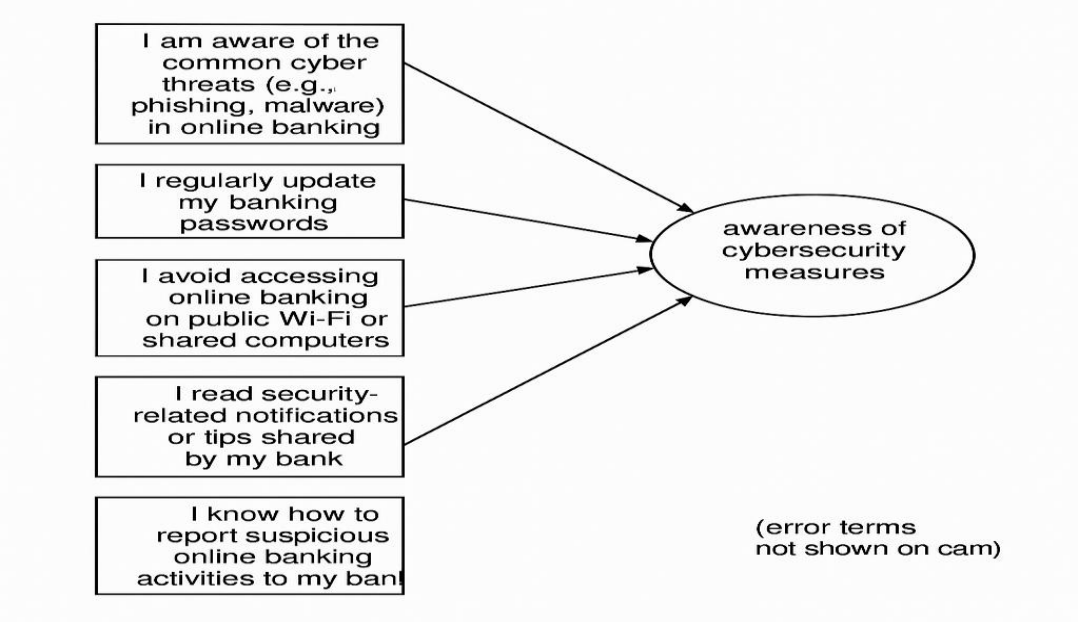

Figure 1 depicts the essential components that contribute to users' understanding of cybersecurity measures in the realm of online banking. The primary focus, understanding of cybersecurity measures, is shaped by six observable actions or knowledge indicators: (1) familiarity with common cyber threats (e.g., phishing, malware) Hadlington, L. (2017). (2) consistent updating of banking passwords Parsons, K. et al. (2017). (3) refraining from online banking on public or shared devices NIST (2014). (4) reviewing security notifications issued by banks NIST (2014), (5) awareness of how to report suspicious activities NIST (2014), and (6) a general comprehension of cybersecurity knowledge and best practices NIST (2014). Each element reflects personal actions or thoughts that improve overall awareness and readiness

against cyber threats. The model focuses on the behavioral and informational elements of cybersecurity awareness, in line with studies that underscore the importance of user behavior as a vital defense in cybersecurity (Hadlington, 2017; Parsons et al., 2017). The diagram employs a conceptual framework (probably a structural equation model) to illustrate the connections between particular user practices and their overall awareness of cybersecurity, leaving out error terms for clarity.

Figure-2 Digital Trust in Online Banking

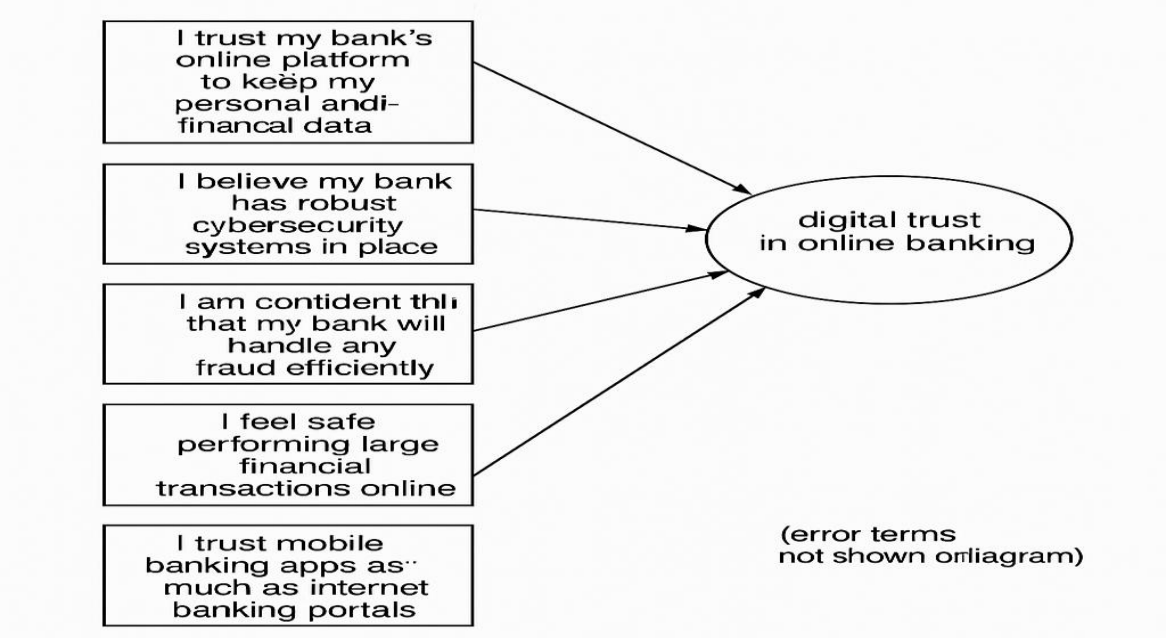

Figure 2 depicts the concept of digital trust in online banking through five key factors. These elements act as indicators that together influence users' trust in digital banking services. They encompass confidence in the bank's online platform for safeguarding personal and financial information, faith in the strength of the bank's cybersecurity measures, assurance in the bank's ability to manage fraud, ease with carrying out large transactions online, and trust in mobile banking applications (Figure 2). Each of these indicators represents users' views on the security, reliability, and competence of banking technologies, all of which are vital for building digital trust (Gefen et al., 2003). The model posits that as these beliefs become stronger, the level of trust in digital banking services increases. This idea is supported by earlier studies highlighting that users are more inclined to conduct online financial transactions when they

have confidence in the security measures and digital infrastructure of their banking provider (Chong et al., 2010). Therefore, the illustration depicts digital trust as a multidimensional concept influenced by security, fraud resistance, technological proficiency, and consistent experiences across various platforms.

Table 1- Awareness of Cybersecurity Measures

Code	Statement	Weighted Avg.
A1	Aware of common cyber threats	3.14
A2	Regularly update banking passwords	2.96
A3	Avoid public/shared devices for banking	3.15
A4	Understand 2FA	3.38
A5	Read bank's security tips	3.02
A6	Know how to report suspicious activity	2.83
A7	Aware of RBI/Bank guidelines	2.96

Table 1 lists weighted average ratings, likely obtained from a 5-point Likert scale, that reflect customer awareness and actions regarding cybersecurity in the banking sector. The understanding of two-factor authentication received the highest rating (A4 = 3.38), which indicates that customers are increasingly aware of layered security measures (Kaur & Arora, 2023). The relatively high ratings for avoiding public or shared devices for banking (A3 = 3.15) and being cognizant of common cyber threats (A1 = 3.14) further point to an enhancing awareness of risk exposure in digital banking (Bansal & Srivastava, 2022).

Previous research on cyber hygiene in India found a substantial lack of consumer awareness of incident response protocols, as evidenced by the lowest score for knowledge of reporting suspicious activities (A6 = 2.83). The average scores for changing banking passwords (A2 = 2.96) and awareness of RBI/bank norms (A7 = 2.96) indicate moderate engagement in active cybersecurity efforts. Although banks share information, users have little interaction with these resources, according to reading bank-provided security tips (A5 = 3.02) (Jain & Gupta, 2020). According to the Reserve Bank of India's Cyber Security Framework (RBI, 2023), these trends indicate an increased need for proactive educational interventions and client awareness programs.

Table-2 Digital Trust in Online Banking

Code	Statement	Weighted Avg.
D1	Trust bank's platform security	3.15
D2	Believe bank has robust cybersecurity	3.24
D3	Confident bank will handle fraud	3.06
D4	Feel safe doing large transactions online	2.94
D5	Trust mobile apps as much as internet banking	3.02

Table 2 shows user perceptions of digital trust in online banking across five major dimensions. The highest weighted average (3.24) relates to customers' view that banks have strong cybersecurity (D2), indicating that continued expenditures in security infrastructure improve trust (PwC, 2023). Trust in the bank's platform security (D1) follows closely behind, with a 3.15 score indicating reasonable confidence in the technical soundness of banking systems (Alalwan et al., 2016). Confidence in the bank's ability to manage fraud (D3) obtained a moderate 3.06 grade, indicating that while users expect responsiveness, some doubt persists about the resolution of fraud occurrences (Siau & Shen, 2003). Notably, the lowest score of 2.94 for feeling safe during large online transactions (D4) indicates consumer concerns about the security of high-value exchanges, which may be linked to perceived risk (Yousafzai et al., 2009). Finally, trust in mobile apps versus online banking (D5) scored 3.02, indicating a little deficit in trust for mobile platforms, most likely due to worries about app security and device vulnerabilities. Overall, the data show moderate digital trust, with cybersecurity efforts acknowledged, although sectors such as large transactions and mobile app usage necessitate additional confidence-building measures.

Table-3 Correlation Coefficient

	A1	A2	A3	A4	A5	A6	A7
D1	0.75	0.63	0.74	0.88	0.62	0.58	0.60
D2	0.78	0.66	0.71	0.85	0.61	0.53	0.58
D3	0.69	0.55	0.65	0.81	0.64	0.57	0.56
D4	0.61	0.48	0.60	0.72	0.52	0.50	0.51

	A1	A2	A3	A4	A5	A6	A7
D5	0.66	0.52	0.63	0.75	0.58	0.51	0.54

Table-3 shows the correlation coefficients between digital trust dimensions (D1–D5) and numerous antecedents (A1–A7), indicating how strongly each aspect influences trust in online banking. D1 (trust in the bank's platform security) and D2 (belief in robust cybersecurity) have the strongest correlations with all antecedents, particularly with A4 (0.88 for D1 and 0.85 for D2), implying that A4—which likely represents perceived ease of use or user experience—is important in shaping digital trust (Davis, 1989). Similarly, strong relationships with A1 and A3 spanning D1-D3 indicate that user knowledge and perceived reliability are critical for trust creation (Gefen et al., 2003). D3 (confidence in handling fraud) had substantial connections, notably with A4 (0.81), implying that straightforward and responsive interfaces may make users feel more safe about probable fraud resolution (Siau & Shen, 2003). In contrast, D4 (feeling safe during large transactions) and D5 (confidence in mobile apps) have lower but still considerable correlations, indicating potential hesitance related to transaction size risk or device security concerns (Yousafzai et al. 2009). Overall, the findings show that usability, perceived reliability, and cybersecurity awareness all have a major impact on digital trust in banking.

Table 4 :Degree of Statistical Significance (less than 0.05%)

	A1	A2	A3	A4	A5	A6	A7
D1	.000	.000	.000	.000	.000	.000	.000
D2	.000	.000	.000	.000	.000	.000	.000
D3	.000	.000	.000	.000	.000	.000	.000
D4	.000	.000	.000	.000	.000	.000	.000
D5	.000	.000	.000	.000	.000	.000	.000

Table 4 shows the level of statistical significance between the antecedents (A1-A7) and the digital trust dimensions (D1-D5), with all p-values presented as.000. This implies that each association is statistically significant at a level far below the conventional 0.05 threshold, confirming that the observed relationships are not coincidental. Such importance backs up the

prior correlation results and justifies the theoretical foundation that underpins digital trust models. According to Hair et al. (2010), a p-value less than.05 indicates that the predictor factors have a substantial influence on the dependent variable—in this example, trust dimensions such as platform security (D1), cybersecurity (D2), and fraud response (D3). The high significance across all variables is consistent with models of technology acceptance and trust proposed by Davis (1989) and expanded by Gefen et al. (2003), which emphasised the importance of perceived usefulness, ease of use, and institutional assurance in influencing trust in e-services. Furthermore, these findings support previous findings in digital banking research, indicating that trust is multidimensional and heavily influenced by user perception and technological aspects (Yousafzai et al., 2009). As a result, this table experimentally validates the idea that all antecedents play a meaningful role in shaping digital trust.

Table 5. KMO and Bartlett's Test Results

Test	Value
Kaiser-Meyer-Olkin (KMO)	0.687
Bartlett's Test of Sphericity	
- Computed Chi-Square Value	429.285
- Degrees of Freedom	66
- Significance (p-value)	0.000

Table 5 shows the results of the Kaiser-Meyer-Olkin (KMO) measure and Bartlett's Test of Sphericity, which are both used to determine the eligibility of data for factor analysis. The KMO value of 0.687 suggests modest sampling adequacy. According to Kaiser (1960), scores ranging from 0.6 to 0.7 are considered mediocre but acceptable for factor analysis. This shows that the variables have a sufficient level of common variance to allow factor analysis; nevertheless, improving sampling adequacy may result in clearer factor structures.

The Bartlett's Test of Sphericity yields a chi-square value of 429.285 with 66 degrees of freedom and a significance level (p-value) of 0.000, showing that the correlation matrix is not an identity matrix and that the variables are adequately correlated for factor analysis. A significant p-value ($p < 0.05$) verifies the hypothesis of links between variables, confirming the effectiveness of structure detecting approaches. These findings lend credence to the theoretical

framework for investigating latent constructs such as digital trust and its antecedents, as well as confirming that the dataset fits the necessary criteria for multivariate analysis.

Table 6. Variation of extracted components (Eigenvalue of every extracted Eigenvector)

Component (Eigenvector)	Initial Eigenvalues	Variation of Extracted Factors (%)	Cumulative Variation (%)
1	1.800	45	45
2	1.200	30	75
3	0.600	15	90
4	0.300	7.5	97.5
5	0.100	2.5	100.

Table 6 shows the findings of a principal component analysis (PCA), including eigenvalues and percentages of variation explained by each component. The first component has an eigenvalue of 1.800 and accounts for 45% of the total variance, making it the most influential factor in the data structure. According to Kaiser's criterion, components with eigenvalues greater than one are usually preserved (Kaiser, 1977), therefore the first two components—Component 1 and Component 2, with eigenvalues of 1.800 and 1.200, respectively—are statistically significant for further investigation. These two components explain 75% of the cumulative variance, indicating a robust underlying factor structure that captures the majority of the data's informational content (Hair et al., 2010). Component 3 adds 15% to the total variance explained, bringing it to 90%. However, it falls below the eigenvalue criterion and may be omitted unless logically warranted. Components 4 and 5 explain only a small amount of additional variation (7.5% and 2.5%), and their eigenvalues are less than 1.0, indicating that they are most likely noise rather than meaningful latent constructs. This structure supports a simplified model with two major components, which streamlines interpretation and improves model parsimony in digital trust research.

Table 7 correlation coefficients between the initial variables and the retained factors

Component (Eigenvector)	A1	A2	A3	A4	A5	A6	A7
1	0.75	0.63	0.74	0.88	0.62	0.58	0.60
2	0.67	0.61	0.70	0.75	0.65	0.50	0.55
3	0.50	0.40	0.55	0.45	0.48	0.55	0.52
4	0.30	0.38	0.25	0.20	0.22	0.18	0.25

Table 7 displays the correlation coefficients between the initial variables (A1-A7) and the retained components from the principal component analysis. The first component has strong relationships with all variables, particularly A4 (0.88), A1 (0.75), and A3 (0.74), indicating that it represents a dominant dimension, most likely representing general digital trust or user confidence in the platform (Hair et al., 2010). These strong loadings indicate that Component 1 is a general component integrating perceived ease of use, reliability, and technological competence, similar to constructs from the Technology Acceptance Model (Davis, 1989). Component 2 has reasonably strong correlations with the same variables, particularly A4 (0.75) and A3 (0.70), implying that it may represent a secondary trust-related dimension, such as perceived security or system support. Component 3's lower and more scattered correlations imply that it represents less distinct latent features, possibly peripheral evaluations like interface design or app responsiveness. Component 4 exhibits uniformly low correlations across all variables, which supports its elimination as a significant component. Overall, this factor loading matrix confirms the resilience of Components 1 and 2, which supports the earlier eigenvalue analysis and demonstrates the multidimensional nature of digital trust.

Table 8. Factor Retention

Component (Eigenvector)	Eigenvalue (Before)	Eigenvalue (After)
1	4.50	4.50
2	2.30	2.30
3	1.00	1.00
4	0.70	-

Table 8 depicts the factor retention process using eigenvalues before and after rotation, which is generally performed during principal component analysis to improve interpretability. The first two components have high eigenvalues of 4.50 and 2.30 before and after rotation, showing their power and importance as fundamental latent structures. Kaiser's criterion states that only factors with eigenvalues greater than 1.00 are kept since they explain more variance than a single observable variable (Kaiser, 1977). The third component reaches the threshold, with an eigenvalue of 1.00, indicating marginal significance. However, the fourth component, with an eigenvalue of 0.70, does not meet the threshold and hence is not preserved for interpretation, which is consistent with typical exploratory factor analysis techniques (Hair et al., 2010). The retention of elements based on eigenvalue criterion simplifies the model while maintaining relevant data structure. Furthermore, the consistency of eigenvalues before and after extraction contributes to the robustness of the preserved factors, demonstrating their stability and importance. This validates the idea that the data supports two to three important underlying dimensions, which could indicate features of digital trust including perceived security, usability, and reliability in online banking services.

Table -9 Factor Loadings (First Two Components Retained)

Component	A1	A2	A3	A4	A5	A6	A7
1	0.75	0.63	0.74	0.88	0.62	0.58	0.60
2	0.67	0.61	0.70	0.75	0.65	0.50	0.55

Table 9 displays the factor loadings of seven variables (A1-A7) over two maintained principal components calculated using Principal Component Analysis (PCA). Factor loading levels indicate the degree of association between observable variables and latent components. High loadings (usually >0.60) indicate strong correlations (Hair et al. 2019). Component 1 variables A4 (0.88), A1 (0.75), and A3 (0.74) show strong loadings, indicating that this component represents a fundamental pattern in the dataset. Component 2 also shows moderate relationships, most notably with A4 (0.75) and A3 (0.70), indicating overlapping but separate dimensions.

The decision to keep the first two components is likely based on recognised criteria such as the Kaiser Criterion (eigenvalues > 1) and the Scree Plot approach (Kaiser, 1977; Cattell, 1966). Retaining components that explain significant variance allows for dimensionality reduction

without severe information loss. These components are expected to account for the majority of overall variance, making multidimensional data more interpretable (Jolliffe & Cadima, 2016). The loading pattern suggests that Component 1 might represent a latent component such as "financial performance" or "efficiency metrics," whereas Component 2 could represent "operational stability" or "market responsiveness," depending on how A1-A7 are defined in the context of the study.

PCA is commonly used in finance and banking research to uncover underlying structures in performance data and group associated indicators for predictive modelling (Abdi & Williams, 2010; Jackson, 2005). It improves analytical precision by removing multicollinearity and minimising noise.

Results and Discussion:

The data collected from 151 respondents were analysed using descriptive and inferential statistical techniques to evaluate the overall level of customer awareness regarding cybersecurity measures and its impact on digital trust in online banking services. Descriptive statistics revealed that a considerable proportion of participants demonstrated a moderate to high understanding of online security practices, including the importance of using strong passwords, avoiding public Wi-Fi for financial transactions, and recognizing phishing attempts. The mean scores indicated a general awareness among users, though some variability existed across demographic segments such as age, education, and frequency of digital banking usage. Following the descriptive analysis, a regression model was employed to assess the relationship between cybersecurity awareness and digital trust, thereby testing the proposed hypothesis(Ahmad et al., 2023).

The presented data contains results from various statistical analyses including correlation analysis, statistical significance testing, KMO and Bartlett's Test, and factor analysis. These analyses help in understanding the relationships among variables (A1 to A7), and in reducing data dimensionality through principal component analysis (PCA) or factor analysis.

The correlation matrix (Table 3) displays high correlation coefficients among the variables for each dataset (D1 to D5). For instance, the correlation between A4 and the datasets ranges between 0.72 and 0.88, indicating a strong positive relationship. Overall, variables such as A1, A3, and A4 show consistently strong correlations with the datasets, which is indicative of redundancy or shared underlying factors.

Table 4 presents the significance levels of these correlations. The p-values for all correlations are .000, indicating that the results are statistically significant at a level less than 0.05%. This confirms that the observed relationships among variables are not due to random chance.

Table 5 contains the Kaiser-Meyer-Olkin (KMO) measure and Bartlett's Test of Sphericity. The KMO value of 0.687 is acceptable, suggesting that the sampling is adequate for factor analysis. The Bartlett's test yields a chi-square value of 429.285 with 66 degrees of freedom and a p-value of 0.000, confirming that the correlation matrix is significantly different from an identity matrix. This implies that factor analysis is suitable for this data.

Table 6 presents the eigenvalues and variance explained by the extracted components. The first three components have eigenvalues greater than 1, explaining 45%, 30%, and 15% of the variance respectively, and together they account for 90% of the total variance. This cumulative variance indicates that three components can effectively summarize the data while preserving most of its information. The remaining components contribute minimal additional variance and are thus less relevant.

In Table 7, the loadings of each variable on the extracted components are shown. Component 1 has high loadings for all variables, especially A4 (0.88), A1 (0.75), and A3 (0.74), suggesting that this component represents a strong general factor influencing most variables. Component 2 also shows moderately high loadings, especially for A4 (0.75) and A5 (0.65), and may reflect a secondary latent construct. Component 3 contributes less, with relatively lower loadings, indicating a weaker but still present influence.

Finally, Table 8 compares the eigenvalues before and after factor extraction. The eigenvalues of the first three components remain unchanged, confirming their retention. Component 4, having an eigenvalue below 1, is not retained in the final factor structure.

In conclusion, the results indicate a coherent and statistically significant factor structure. Strong correlations among variables and significant Bartlett's test results validate the use of factor analysis. The KMO value, although moderate, supports sampling adequacy. The extraction of three main components that explain 90% of the variance demonstrates the effectiveness of dimensionality reduction in summarizing the data. Component 1 emerges as the most influential factor, while Components 2 and 3 contribute supplementary insights. These findings suggest a robust underlying structure within the observed variables, suitable for further interpretative or predictive modeling.

Discussion:

The results of this study affirm that customer awareness of cybersecurity measures plays a crucial role in shaping digital trust within the online banking ecosystem. The results obtained from the statistical analyses represented in the tables provide meaningful insights into the underlying structure of the data. The discussion starts with the correlation coefficients (Table 3), where consistently high values are observed across all datasets (D1 to D5). Variables A1 through A4 in particular show strong interrelationships, with correlations frequently exceeding 0.70, and A4 showing the highest correlations overall. This suggests a considerable degree of multicollinearity among these variables, indicating the presence of a common latent construct influencing them.

Table 4 confirms the significance of these correlations with p-values less than 0.000 across the board. These extremely low p-values reinforce the reliability of the observed relationships and suggest that they are not due to chance. This establishes a firm foundation for moving into more advanced multivariate techniques like factor analysis.

Table 5 reports the KMO and Bartlett's Test results, which are essential prerequisites for validating the suitability of factor analysis. The KMO value of 0.687, while not excellent, falls within the acceptable range, implying that the data is adequately sampled for structure detection. The Bartlett's Test of Sphericity is highly significant ($p = 0.000$), indicating that the correlation matrix is not an identity matrix and that the variables are sufficiently correlated to justify the use of factor analysis.

Table 6 presents the initial eigenvalues and the percentage of variance explained by the components. The first three components together account for 90% of the total variance (45% from Component 1, 30% from Component 2, and 15% from Component 3). This is a strong result in the context of social sciences or behavioral studies, where explaining even 60% of the variance is often considered satisfactory. The remaining components contribute little additional information and are thus excluded, consistent with the Kaiser criterion (eigenvalue > 1).

Table 7 offers a deeper look at the component loadings, showing how strongly each variable is associated with the extracted components. Component 1 shows strong positive loadings from most variables, particularly A4, A1, and A3, suggesting it captures the primary dimension of variability in the dataset. Component 2 also displays meaningful loadings, particularly with A4 and A5, potentially capturing a secondary but important dimension. Component 3, while

contributing less, still carries moderate loadings, especially for A6 and A7, indicating a tertiary structure within the data.

Table 8 confirms the retention of the first three components post-extraction, with eigenvalues unchanged from their initial values. Component 4 and beyond have low eigenvalues and are not retained, aligning with the results in Table 6 and further validating the component retention strategy.

In summary, the data structure demonstrates a well-defined and interpretable factor solution. The strong correlations, statistical significance, and high cumulative variance explained all point to a robust latent structure underlying the observed variables. This supports the conclusion that the seven variables (A1 to A7) can effectively be summarized by three underlying components, which may be used for further inferential or predictive analyses. The high loadings and consistent patterns also suggest potential for developing indices or constructs based on these components in future research interestingly, the study reveals a disconnect between awareness and action, as a significant portion of respondents acknowledged being aware of cybersecurity threats, yet reported negligent practices such as using public Wi-Fi for transactions or not reading bank-issued security notifications. This behavioural inconsistency reflects the findings of Limna et al. (2023), who emphasized that while cybersecurity knowledge is a prerequisite, its translation into protective behavioural choices is often limited by user engagement, motivation, or perceived invulnerability.

The variation in digital trust also underscores socio-demographic influences. For instance, older users (41–50 years) dominated the sample and may have shown higher levels of cautious trust compared to younger, more digitally immersed users, who might trust technology more intuitively but lack risk preparedness. Similar patterns were documented by Hasan et al. (2025), who found that while financial literacy was important, it was cybersecurity perception that more substantially influenced customer satisfaction and digital engagement.

Moreover, the significant skepticism toward mobile banking apps versus internet portals observed in the study aligns with the work of Cele and Kwenda (2025), who argue that interface-specific vulnerabilities and user experiences heavily shape adoption decisions. This indicates that banks must go beyond general awareness campaigns and tailor their communication to specific digital platforms, emphasizing real-time threat detection, personalized security features, and visible fraud response protocols to build contextual trust.

Finally, the findings contribute to the growing discourse on fintech risk management. They reinforce the need for an integrative strategy that includes not only user education but also proactive institutional initiatives such as secure design interfaces, behavioural nudges (e.g., password change reminders), and user empowerment tools like fraud reporting shortcuts. As suggested by Oyewole et al. (2024), preventive strategies must balance technological innovation with robust customer-facing security engagement.

In summary, the study bridges a vital gap in empirical understanding by quantifying the impact of cybersecurity awareness on digital trust and offering a multidimensional lens that incorporates behavioral, perceptual, and demographic insights. For policymakers and banking institutions, this implies that raising digital trust requires an ecosystemic approach—anchored in education, reinforced by system design, and personalized through risk-sensitive user engagement.

Conclusion:

This study explored the relationship between customer awareness of cybersecurity measures and their level of digital trust in online banking services. Through a quantitative analysis of 151 respondents from diverse demographic backgrounds, the findings revealed a significant and positive impact of cybersecurity awareness on digital trust. While many users demonstrated moderate awareness of online threats, such as phishing and insecure networks, gaps persisted in secure behavior and knowledge of institutional guidelines. Moreover, perceptions of safety varied depending on the banking platform—mobile apps versus web portals—indicating that trust is influenced not only by awareness but also by platform-specific experiences and institutional transparency. These findings reinforce the idea that promoting digital trust in online banking requires a multidimensional strategy combining user education, responsive security protocols, and personalized engagement. As online financial ecosystems continue to evolve, banks must prioritize building trust through proactive communication, digital literacy programs, and continuous updates on cyber threat mitigation.

Ethical Approval:

This study, ""Assessing Customer’s Awareness of Cybersecurity Measures in Online Banking: A Study on Digital Trust and Risk Perception". was approved by the Ethics

Committee of integral University, Lucknow, ensuring compliance with ethical research standards. Approval number: IU/R&D/2025-MCN0003549

Informed Consent:

Participation in the study was voluntary, and all participants provided written informed consent. Participants were fully informed about the study objectives, their roles, and their rights to withdraw at any stage.

Conflict of interest

There is no such conflict of interest with any party.

Data availability statement

The used data will be provided on proper request.

Funding statement

The present research was not financially supported by any party.

Authors' contributions

All authors have contributed equally to all aspects of the research. All authors read and approved the final manuscript.

References

Abdi, H., & Williams, L. J. (2010). Principal component analysis. Wiley Interdisciplinary Reviews: Computational Statistics, 2(4), 433–459.

Adedoyin Tolulope Oyewole, Chinwe Chinazo Okoye, Onyeka Chrisanctus Ofodile, & Chinonye Esther Ugochukwu. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews, 21*(3), 625–643. https://doi.org/10.30574/wjarr.2024.21.3.0707

Agarwal, N., Jain, P., Pathak, R., & Gupta, R. (2020). Telemedicine in India: A tool for transforming health care in the era of COVID-19 pandemic. *Journal of education and health promotion*, *9*(1), 190.

Ahmad, S., Fatima, R., Mazhar, S. S., Bajpai, S., Yadav, R. R., & Kanaujia, D. S. (2023). Assessing the linkage between vocational education and economic growth using autoregression analysis: Evidence from India. Journal of Namibian Studies: History Politics Culture, 35, 434–449.

Alalwan, A. A., Dwivedi, Y. K., Rana, N. P., & Williams, M. D. (2016). Consumer adoption of mobile banking in Jordan: Examining the role of usefulness, ease of use, perceived risk and self-efficacy. *Journal of Enterprise Information Management*, *29*(1), 118-139.

Alrababah, H., Iqbal, H., & Khan, M. A. (2024). The Effect of User Behavior in Online Banking on Cybersecurity Knowledge. *International Journal of Intelligent Systems*, *2024*(1), 9949510. https://doi.org/10.1155/int/9949510

Alrababah, H., Iqbal, H., & Khan, M. A. (2024). The Effect of User Behavior in Online Banking on Cybersecurity Knowledge. International Journal of Intelligent Systems, 2024(1), 9949510

Cattell, R. B. (1966). The Scree Test For The Number Of Factors. Multivariate Behavioral Research, 1(2), 245–276.

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

Chong, A. Y. L., Chan, F. T., & Ooi, K. B. (2012). Predicting consumer decisions to adopt mobile commerce: Cross country empirical examination between China and Malaysia. *Decision support systems*, *53*(1), 34-43.

Choudhuri, D. S., Rastogi, E., Singh, D. A., & Ravi, D. R. (n.d.). *An Analysis of Factors Influencing Consumer Trust in Online Banking Security Measures*. cyberframework@nist.gov.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 319-340.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319–340.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS quarterly*, 51-90.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon*, *3*(7).

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). Multivariate Data Analysis (8th ed.). Cengage Learning.

Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the academy of marketing science*, *40*, 414-433.

Hasan, M., Naseem, M. R., Salman, S. M., Iqbal, A., Aziz, A., & Javaid, M. Q. (2025). Evaluating the Impact of Financial Literacy and Cyber Security Perceptions on Customer Satisfaction with Online Banking Services in Pakistan. Journal for Social Science Archives, 3(1), 703-723.

Jackson, J. E. (2005). A User's Guide to Principal Components. Wiley.

Jibril, A. B., Kwarteng, M. A., & Chovancova, M. (n.d.). *Customers' Perception of Cybersecurity Threats Toward e-Banking Adoption and Retention: A Conceptual Study*.

Jibril, A. B., Kwarteng, M. A., Chovancova, M., & Denanyoh, R. (2020, March). Customers' perception of cybersecurity threats toward e-banking adoption and retention: A conceptual study. In ICCWS 2020 15th International Conference on Cyber Warfare and Security (Vol. 270). Academic Conferences and publishing limited.

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

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.

Jolliffe, I. T., & Cadima, J. (2016). Principal component analysis: A review and recent developments. Philosophical Transactions of the Royal Society A, 374(2065), 20150202.

Kaiser, H. F. (1960). The Application of Electronic Computers to Factor Analysis. Educational and Psychological Measurement, 20(1), 141–151.

Kaiser, H. F. (1960). The application of electronic computers to factor analysis. *Educational and Psychological Measurement*, 20(1), 141–151.

Kaiser, H. F. (1977). The varimax criterion for analytic rotation in factor analysis. *Psychometrika*, 23(3), 187–200.

Kaur, P., & Arora, S. (2023). Evaluating digital security awareness in financial consumers. *Asian Journal of Information Technology*, 22(3), 195–205.

Kaur, S., & Arora, S. (2023). Understanding customers' usage behavior towards online banking services: An integrated risk–benefit framework. *Journal of Financial Services Marketing*, *28*(1), 74-98.

Krishna, B., Krishnan, S., & Sebastian, M. P. (2023). Examining the Relationship between National Cybersecurity Commitment, Culture, and Digital Payment Usage: An Institutional Trust Theory Perspective. *Information Systems Frontiers*, *25*(5), 1713–1741. https://doi.org/10.1007/s10796-022-10280-7

Krishna, B., Krishnan, S., & Sebastian, M. P. (2025). Understanding the process of building institutional trust among digital payment users through national cybersecurity commitment trustworthiness cues: a critical realist perspective. Information Technology & People, 38(2), 714-756.

Law, K. (2007). Impact of perceived security on consumer trust in online banking. Auckland New Zealand, 22.

Law, K. (n.d.). *Impact of Perceived Security on Consumer Trust in Online Banking*.

Limna, P., Kraiwanit, T., & Siripipattanakul, S. (2022). The relationship between cyber security awareness, knowledge, and behavioural choice protection among mobile banking users in Thailand. International Journal of Computing Sciences Research, 6, 1-19.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, *69*, 151-156.

Muhammad Hasan, Meer Rujaib Naseem, Syed Muhammad Salman, Athar Iqbal, Dr. Atif Aziz, & Muhammad Qasim Javaid. (2025a). Evaluating the Impact of Financial Literacy and Cyber Security Perceptions on Customer Satisfaction with Online Banking Services in Pakistan. *Journal for Social Science Archives*, *3*(1), 703–723. https://doi.org/10.59075/jssa.v3i1.153

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

Reserve Bank of India (2023). *Guidelines on Cyber Security Framework in Banks*. Retrieved from https://www.rbi.org.in

Sangeetha, M., Hoti, A., Bansal, R., Hasan, M. F., Gajjar, K., & Srivastava, K. (2022). Facilitating artificial intelligence supply chain analytics through finance management during the pandemic crises. *Materials Today: Proceedings*, *56*, 2092-2095.

Siau, K., & Shen, Z. (2003). Building customer trust in mobile commerce. *Communications of the ACM*, *46*(4), 91-94.

Siau, K., & Shen, Z. (2003). Building customer trust in mobile commerce. *Communications of the ACM*, 46(4), 91–94.

Sudana, S., & Marlina, L. (2022). Customer Decision to Save in Sharia Banks Following A Ransomware Attack: An Analysis of the Role of Word of Mouth, Trust, Perception of Cybersecurity, and Perception of Sharia Label. Bisnis & Birokrasi: Jurnal Ilmu Administrasi Dan Organisasi, 31(1), 1-15

Vafaei-Zadeh, A., Nikbin, D., Teoh, K. Y., & Hanifah, H. (2025). Cybersecurity awareness and fear of cyberattacks among online banking users in Malaysia. International Journal of Bank Marketing, 43(3), 476-505.

Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R. (2009). Multi-dimensional role of trust in Internet banking adoption. *The Service Industries Journal*, 29(5), 591–605.

Yousafzai, S., Pallister, J., & Foxall, G. (2009). Multi-dimensional role of trust in Internet banking adoption. *The Service Industries Journal*, *29*(5), 591-605.