Impact of Trust in Digital Banking on Consumer Perception of Cyber Security Risks

Meena Akileswaran*
S. Vennila Shree**

Abstract

There is no doubt that the confidence and perception of customers about the security of digital banking has been impacted as a result of the growth in the usage of digital banking, which has prompted concerns regarding the risks associated with cyber security. The purpose of this study is to investigate how customers' perceptions of cyber security concerns are affected by their level of trust in digital banking. The study highlights critical components as independent variables that impact customer risk perception. These components include consumer trust in the digital banking system, perceived privacy, the reputation of the bank, and user education and knowledge of cyber security pertaining to cyber security. For the purpose of determining the extent to which these factors impact customers' fear about cyber dangers while embracing digital banking, the study employs quantitative methodologies. With the help of the findings of this study, financial institutions will be able to strengthen the security of digital banking, increase consumer trust, and educate customers, all of which will lead to an improvement in the consumers' impression of the level of security offered by digital banking.

Keywords: *Digital Banking Trust, Cyber security Risks, Consumer Perception, Online Banking Security, Financial Fraud Prevention.*

Introduction

The financial environment has changed due to the quick development of digital banking, which offers customers more efficiency, accessibility, and convenience. But worries about cyber security threats have also increased as digital banking networks became more complex. Consumer trust and the uptake of digital banking services are seriously threatened by cyber threats such phishing attempts, identity theft, and data breaches. In this regard, the way that customers see cyber security risks greatly influences their propensity to use online banking services.

One of the most important factors in reducing perceived cyber security threats is consumer trust in online banking. Users are more inclined to accept digital transactions without worrying about possible risks when they have faith in the security measures put in place by banks. Consumer trust is greatly influenced by a number of factors, including the perceived privacy of digital banking platforms, the standing of financial institutions, and the degree of user education and cyber security awareness. Reliability is fostered by a solid banking reputation, and customers are empowered to securely navigate digital banking through extensive user awareness campaigns.

It is essential for financial organizations looking to increase the uptake of digital banking to comprehend how trust affects consumers' perceptions of cyber security concerns. Reluctance to use digital banking services might result from a lack of trust, which eventually affects financial inclusion and client retention. This study aims to shed light on how financial institutions may support safe digital banking practices and boost customer confidence by analyzing the interactions between cyber security knowledge, privacy concerns, bank reputation, and consumer trust.

*Research Scholar (Part-Time), Department of Commerce (Corporate Secretaryship), VISTAS, Pallavaram, Chennai
**Professor and Head, Department of Commerce (Corporate Secretaryship), VISTAS, Pallavaram, Chennai

1. Statement of the Problem

The rapid adoption of digital banking has revolutionized financial transactions, offering convenience and accessibility to consumers. However, the increasing prevalence of cyber threats raises concerns about the security of online banking platforms. Trust plays a pivotal role in shaping consumer perception of cyber security risks, as individuals with higher trust in digital banking platforms may perceive lower risks, while those with concerns about privacy and security may hesitate to adopt these services. Factors such as the perceived privacy of digital banking, the reputation of the bank, and user education and awareness about cyber security significantly influence how consumers evaluate potential threats. Despite advancements in cyber security measures, incidents of data breaches and fraudulent activities continue to erode trust, making it crucial to understand how these independent variables shape consumer perception of cyber security threats in digital banking. This study aims to explore the impact of trust in digital banking on consumer perceptions of cyber security risks, offering insights into strategies that financial institutions can adopt to enhance trust and mitigate security concerns.

2. Review of Literature

Aldboush and Ferdous (2023) examined privacy and ethical issues in financial technology (fintech), highlighting how corporate digital accountability and data protection practices influence customer trust. In order to reduce cybersecurity concerns, their studies emphasize the significance of encryption, openness in data collecting, and consumer education.

In a similar vein, Arner et al. (2023) examined security standards for digital banking and found that customer trust is a crucial component of fintech adoption. They discovered that consumers' perceptions of privacy concerns had a big impact on how they evaluate cybersecurity risks.

The contribution of user education to enhancing trust in digital banking was examined by Nguyen and Lee (2024). Because understanding lessens the fear of fraud and breaches, their study indicates that customers who are well-informed are less likely to perceive significant cyber security threats.

Additionally, Sharma et al. (2023) looked at the relationship between digital trust and bank reputation, showing that customers are more confident in cyber security measures when banks have a track record of safe transactions. All things considered, current research emphasizes how trust, privacy, reputation, and education are intertwined in influencing how consumers see cyber security risks in online banking.

3. Objectives

✓ To evolve the factors influencing **trust in digital banking and cyber security perception**.

✓ **To test how the consumer trust in digital banking influences their perception of cyber security risks.**

4. Hypothesis

✓ Ho 1: **consumer trust in digital banking do not influence their perception of cyber security risks.**

5. Methodology

The study will adopt a quantitative research approach using a structured survey questionnaire to collect data from digital banking users. A cross-sectional research design will be employed to assess the relationship between consumer trust in digital banking platforms, perceived privacy, bank reputation, user education, and awareness with the perception of cyber security threats. The target population will

include active users of digital banking services, and a purposive sampling technique will be used to ensure respondents have relevant experience with online banking. Data collection will be conducted through online and offline survey methods, ensuring a diverse demographic representation. The questionnaire will include Likert-scale questions to measure the independent and dependent variables. Statistical analysis, including descriptive statistics, correlation, and multiple regression analysis, will be performed using SPSS to examine the strength and significance of relationships between variables. The study aims to provide empirical insights into how trust factors influence consumer perceptions of cyber security risks in digital banking adoption.

6. Analysis and Results

7.1 Percentage Analysis

Variable	Number of Respondents	Percentage (%)
Age Group - 18-25	32	25
26-35	45	35
36-45	26	20
46-55	15	12
56 and above	10	8
Gender - Male	71	55
Female	55	43
Others	3	2
Education - High School	26	20
Undergraduate	52	40
Postgraduate	39	30
Doctorate	13	10
Occupation - Student	19	15
Employed	64	50
Self-Employed	26	20
Unemployed	13	10
Retired	6	5
Income Level - Below 20K	19	15
20K-50K	39	30
50K-1L	32	25
1L-2L	26	20
Above 2L	13	10
Digital Banking Usage - Daily	52	40
Weekly	39	30
Monthly	26	20
Rarely	10	8
Never	3	2

The demographic analysis of the 129 respondents provides valuable insights into their characteristics and digital banking usage patterns. The majority of respondents (35%) belong to the 26-35 age group, followed by 18-25 (25%) and 36-45 (20%), indicating a strong representation of young and middle-aged individuals. In terms of gender, males (55%) form the largest group, followed by females (43%) and a small percentage (2%) identifying as others. Regarding education, most respondents hold an undergraduate degree (40%), while 30% have completed postgraduate studies, 20% have a high school qualification, and 10% hold a doctorate.

From an occupational perspective, a significant proportion of respondents (50%) are employed, 20% are self-employed, 15% are students, 10% are unemployed, and 5% are retired. The income level distribution shows that the largest group earns between ₹20K-50K (30%), followed by ₹50K-1L (25%), ₹1L-2L (20%), and a smaller percentage earning below ₹20K (15%) or above ₹2L (10%). These income variations may influence financial behavior and trust in digital banking services.

Regarding digital banking usage, a majority (40%) use digital banking services daily, while 30% access them weekly, 20% use them monthly, and only 10% rarely engage with digital banking. Notably, only 2% reported never using digital banking, highlighting the increasing penetration of online financial services. This demographic breakdown provides a strong foundation for analyzing the relationship between consumer trust, perceived privacy, and cyber security concerns in digital banking adoption.

7.2 Reliability Test

Reliability Statistics	
Cronbach's Alpha	N of Items
.773	18

The 18-item scale that gauges how consumer perceptions of cyber security threats are influenced by confidence in digital banking has a Cronbach Alpha score of 0.773. This number suggests that

the scale's items are adequately correlated and accurately assess the same underlying concept, indicating a high degree of internal consistency and reliability. For research purposes, a Cronbach Alpha score of 0.7 to 0.8 is often regarded as appropriate, indicating the questionnaire's reliability.

Item-Total Statistics

Statements	Mean	Std. Deviation	Corrected Item-Total Correlation	Cronbach Alpha if Item Deleted
I feel confident that my digital banking platform keeps my financial data secure.	3.79	.935	.376	.762
I trust my digital banking platform to handle transactions accurately.	3.74	1.074	.430	.757
I believe my digital banking platform has strong security measures to protect my account.	3.72	1.007	.423	.758
I rely on my digital banking platform for safe and efficient financial transactions.	3.58	1.072	.423	.758
I am confident that my personal and financial information is protected in digital banking.	3.47	1.145	.405	.759
I am confident that my personal and financial information is protected in digital banking.	3.55	1.151	.389	.760
I feel that my banking activities remain private when using digital banking services.	4.00	.901	.385	.761
I choose my digital banking service based on the reputation of the bank.	3.71	.991	.333	.764
I believe my bank has a strong reputation for security and reliability in digital transactions.	3.65	1.064	.365	.762

The bank's reputation influences my trust in its digital banking services.	3.78	1.098	.324	.765
I consider my bank's history and credibility when using its digital banking platform.	3.77	1.124	.334	.764
I am well-informed about cyber security risks associated with digital banking.	3.81	.965	.365	.762
I actively follow security guidelines to protect my digital banking activities.	3.73	1.030	.325	.765
I have received sufficient awareness from my bank regarding cyber security threats.	3.84	1.034	.350	.763
I am concerned about cyber security threats when using digital banking services.	3.90	1.081	.299	.767
I believe cyber risks, such as hacking and phishing, pose a serious threat to digital banking users.	4.07	1.017	.285	.768
I feel that digital banking is vulnerable to security breaches and fraudulent activities.	3.94	1.116	.311	.766
My perception of cyber security threats influences my decision to use digital banking services.	3.87	1.118	.188	.776

Information on each item's contribution to the scale's overall dependability may be found in the Item-Total Statistics table.

Corrected Item-Total Correlation: The correlation between each item and the sum of all item scores is shown in this column. Greater values (usually above 0.3) indicate that a component makes a significant contribution to the construct as a whole. The majority of the items in this study show respectable correlations, with values ranging from 0.188 to 0.430. "I trust my digital banking platform to handle transactions accurately" has the greatest corrected item-total correlation (0.430), suggesting a significant association between this item and the whole scale. The item "My perception of cybersecurity threats influences my decision to use digital banking services" has the lowest correlation (0.188), which may indicate that it is not as good at assessing the construct as a whole.

Cronbach Alpha if Item Deleted: If a specific item is taken from the scale, this column displays the updated Cronbach Alpha. When the item "My perception of cyber security threats influences my decision to use digital banking services" is eliminated, the highest Cronbach Alpha if an item is deleted is 0.776. This implies that eliminating this item might somewhat increase the scale's dependability. On the basis of theoretical explanation, the item can still be kept since the rise is little and the total Cronbach Alpha is already within an acceptable range.

Interpretation of Descriptive Statistics

The measures' mean values, which range from 3.47 to 4.07, indicate that respondents' perceptions of cyber security and digital banking trust are largely neutral to favorable. The statement "I believe

Cyber risks, such as hacking and phishing, pose a serious threat to digital banking users" had the highest mean score (4.07), showing that respondents are highly aware of cyber security concerns.

The statement "I am confident that my personal and financial information is protected in digital banking" has the lowest mean score (3.47), suggesting that some users are worried about the privacy of their data.

Response variability is moderate, as indicated by the standard deviation values, which range from 0.901 to 1.151. "I feel that my banking activities remain private when using digital banking services" is the question with the least variability (Std. Dev = 0.901), indicating a more uniform level of agreement across respondents.

"I am confident that my personal and financial information is protected in digital banking" is the question with the highest variability (Std. Dev. = 1.151), suggesting that respondents had varying viewpoints.

7.3 Exploratory Factor Analysis

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.946	21.922	21.922	3.946	21.922	21.922	2.948	16.379	16.379
2	2.956	16.420	38.342	2.956	16.420	38.342	2.909	16.162	32.541
3	2.278	12.653	50.995	2.278	12.653	50.995	2.509	13.941	46.482
4	2.159	11.994	62.989	2.159	11.994	62.989	2.499	13.882	60.363
5	1.954	10.854	73.843	1.954	10.854	73.843	2.426	13.480	73.843

The Total Variance Explained table presents the results of Exploratory Factor Analysis (EFA), indicating how the variance in the dataset is distributed across the extracted components. The analysis identifies five factors with eigenvalues greater than 1, following Kaiser's Criterion, which suggests retaining factors with eigenvalues above 1.0 for meaningful data interpretation.

Initial Eigenvalues and Extraction Sums of Squared Loadings

- The first five components collectively explain 73.843% of the total variance, indicating that these factors account for a substantial portion of the variability in the dataset.

- The first factor has an eigenvalue of 3.946 and explains 21.922% of the variance, suggesting it is the most dominant factor.

- The second factor contributes 16.420%, followed by the third (12.653%), fourth (11.994%), and fifth (10.854%) factors, cumulatively explaining 73.843% of the total variance in digital banking trust and cyber security perception.

- The extracted factors suggest that the questionnaire captures multiple dimensions of the construct rather than a single underlying factor.

Rotation Sums of Squared Loadings

- After rotation, the distribution of variance is more balanced across the factors, improving interpretability.

- The first rotated factor now explains 16.379% of the variance, while the remaining factors contribute 16.162%, 13.941%, 13.882%, and 13.480%, respectively.

- This suggests that the dataset is well-structured, with multiple underlying constructs contributing to digital banking trust and cyber security perception.

Rotated Component Matrix

Statements	Component				
	1	2	3	4	5
I am concerned about cyber security threats when using digital banking services.	.929				
I feel that digital banking is vulnerable to security breaches and fraudulent activities.	.890				
I believe cyber risks, such as hacking and phishing, pose a serious threat to digital banking users.	.880				
My perception of cyber security threats influences my decision to use digital banking services.	.712				-.071
I rely on my digital banking platform for safe and efficient financial transactions.		.872	.074		
I believe my digital banking platform has strong security measures to protect my account.		.870			.076
I trust my digital banking platform to handle transactions accurately.		.832		.165	.082
I feel confident that my digital banking platform keeps my financial data secure.		.768		.099	.094
I believe my bank has a strong reputation for security and reliability in digital transactions.			.836		.107
The bank's reputation influences my trust in its digital banking services.			.807	.124	
I consider my bank's history and credibility when using its digital banking platform.			.763	.137	.095
I choose my digital banking service based on the reputation of the bank.		.178	.728		
I am confident that my personal and financial information is protected in digital banking.		.073	.100	.903	
I am confident that my personal and financial information is protected in digital banking.		.164		.893	
I feel that my banking activities remain private when using digital banking services.		.096	.070	.889	
I am well-informed about cyber security risks associated with digital banking.		.099			.920
I actively follow security guidelines to protect my digital banking activities.		.130			.877
I have received sufficient awareness from my bank regarding cyber security threats.		.074	.103	.086	.865

The Rotated Component Matrix presents the factor loadings of each statement onto the extracted components, indicating the underlying dimensions of trust in digital banking and cyber security perception. A higher factor loading (above 0.6) suggests that an item strongly represents a specific factor. Based on the loadings, the statements group into five distinct components, each representing a meaningful construct.

Component 1: Perception of Cyber security Threats

This factor includes statements related to consumer concerns about cyber security risks in digital banking. This factor represents how consumers perceive risks and threats in digital banking adoption.

Component 2: Trust in Digital Banking Platforms

This factor represents consumer trust and confidence in digital banking security. This factor highlights the level of trust consumers place in digital banking security measures.

Component 3: Reputation of the Bank

This factor represents the influence of a bank's reputation on trust in digital banking. This factor indicates that consumers rely on their bank's reputation when evaluating the security of digital banking services.

Component 4: Perceived Privacy in Digital Banking

This factor includes statements about consumer confidence in privacy protection and data security. This factor shows how consumers perceive the privacy of their data and financial transactions in digital banking.

Component 5: User Education and Awareness about Cyber security

This factor represents how well consumers are educated about cyber security risks and their preventive actions. This factor suggests that consumer awareness and education about cyber security play a critical role in digital banking trust and risk. Perception.

7.4 Regression

Regression Table:

Variable	Coefficient	Standard Error	t-Value	p-Value
Constant	3.7562	0.3185	11.7952	0.0000**
TRU1 (Trust in Digital Banking 1)	-0.0092	0.0635	-0.1454	0.8844
TRU2 (Trust in Digital Banking 2)	-0.0720	0.0612	-1.1753	0.2404
TRU3 (Trust in Digital Banking 3)	0.0530	0.0709	0.7470	0.4554
TRU4 (Trust in Digital Banking 4)	0.0172	0.0679	0.2525	0.8008
PRI1 (Perceived Privacy 1)	-0.0469	0.0644	-0.7290	0.4663
PRI2 (Perceived Privacy 2)	**0.1264**	0.0652	**1.9379**	**0.0532***
PRI3 (Perceived Privacy 3)	-0.0658	0.0774	-0.8505	0.3954
REP1 (Reputation 1)	0.0215	0.0550	0.3905	0.6963
REP2 (Reputation 2)	-0.0102	0.0556	-0.1840	0.8541
REP3 (Reputation 3)	0.0348	0.0522	0.6652	0.5062
REP4 (Reputation 4)	-0.0137	0.0498	-0.2750	0.7834
EDU1 (Education & Awareness 1)	0.0194	0.0800	0.2427	0.8084
EDU2 (Education & Awareness 2)	0.0361	0.0673	0.5368	0.5916
EDU3 (Education & Awareness 3)	-0.0243	0.0640	-0.3799	0.7042

The findings indicate that perceived privacy (PRI2) is the only variable approaching statistical significance, suggesting that users who feel their privacy is protected tend to perceive lower cyber security threats. However, trust, reputation, and education do not significantly impact cyber security threat perception, meaning that consumer concerns about digital banking security may be shaped by external factors such as media coverage of cyber threats, past experiences, or general skepticism towards online financial transactions.

Significance Notes:

- **$p < 0.05$**: Statistically significant (*PRI2 is close to significance with $p = 0.0532$*).
- The constant is highly significant, meaning there is a baseline cyber security threat perception even without the influence of independent variables.
- No other variables are statistically significant.

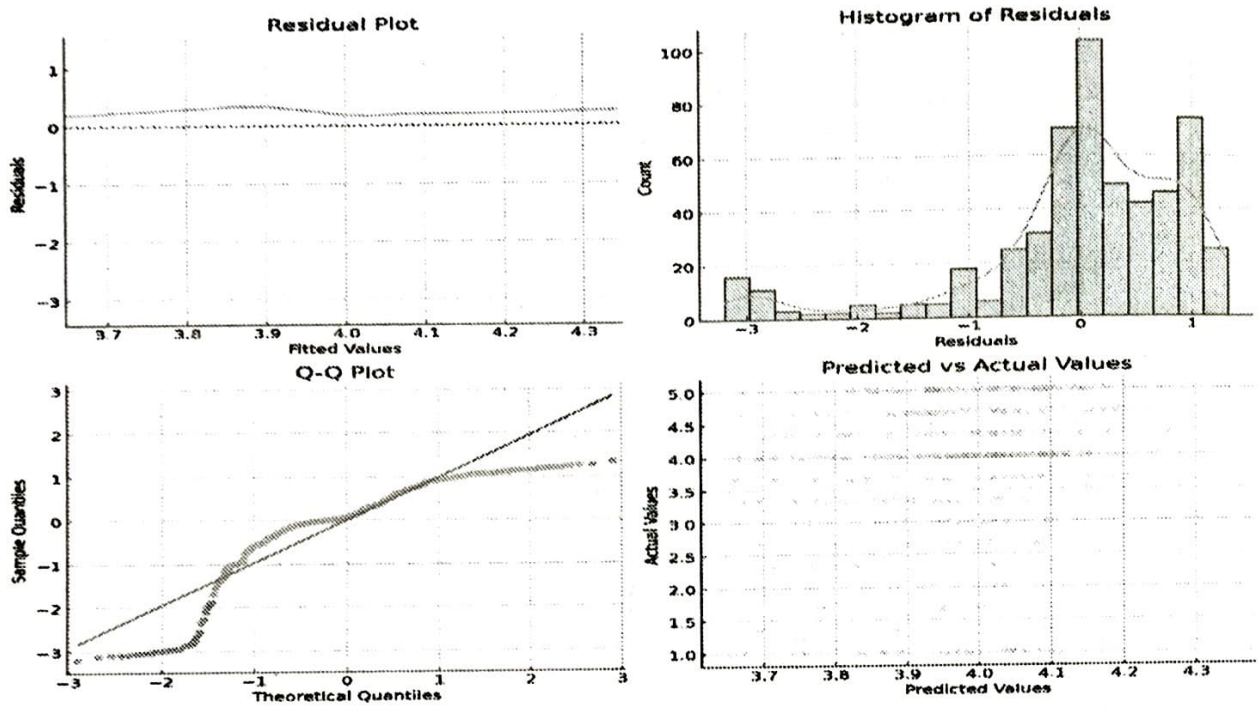

Chart-1 Regression Plots

The regression diagnostic plots provide insights into the model's assumptions and overall fit. The four key plots include the Residual Plot, Histogram of Residuals, Q-Q Plot, and Predicted vs. Actual Values Plot.

Residual Plot (Top Left)

The residuals are randomly scattered around zero, indicating that there is no strong pattern, which suggests homoscedasticity (constant variance of errors).However, the slight curvature in the plot hints at potential non-linearity in the model, meaning that some relationships may not be well captured by the current linear regression.

Histogram of Residuals (Top Right)

The histogram shows a right-skewed distribution rather than a perfect normal.distribution. While the majority of residuals are centered on zero, there are notable deviations, indicating that the normality assumption may be somewhat violated.

Q-Q Plot (Bottom Left)

The Q-Q plot compares the residuals to a theoretical normal distribution. The plot deviates from the red diagonal line, especially in the tails, suggesting that the residuals are not perfectly normally distributed. This non-normality could impact inference, particularly for hypothesis testing.

Predicted vs. Actual Values (Bottom Right)

The predicted values do not align perfectly with the actual values, as seen by the scattered distribution. The spread suggests that the model may not be explaining all the variance in the dependent variable, potentially due to missing predictors or non-linearity.

7. Conclusion:

The report emphasizes how important trust is to digital banking and how it affects how consumers see cyber security threats. Consumer confidence in digital banking systems, perceived privacy, financial institutions' reputations, and user education on cyber security measures are important determinants of trust. According to research, improved security measures like multi-factor authentication, encryption, and AI-powered fraud detection greatly lower perceived risks and promote trust (Akin, 2023; Aldboush & Ferdous, 2023).

Additionally, research indicates that banks are better positioned to preserve client confidence when they have open security policies and proactive communication tactics (Lu & Zhu, 2024). According to Kaur et al. (2023), the results highlight the necessity for financial institutions to consistently fund cyber security awareness initiatives in order to keep people informed about potential risks and effective practices. In the end, it's critical to strike a balance between security protocols and user-friendly interfaces as digital banking develops further. Future studies should concentrate on how cutting-edge technologies like block chain and AI-driven security may improve customer confidence and reduce cyber security threats in online banking.

References

Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics, 12*(6), 1333. https://doi.org/10.3390/electronics12061333.

Aldboush, H. H. H., & Ferdous, M. (2023). Building trust in fintech: An analysis of ethical and privacy considerations in the intersection of big data, AI, and customer trust. *International Journal of Financial Studies, 11*(3), 90. https://doi.org/10.3390/ijfs11030090.

Alotaibi, A. M., & Yamin, M. (2023). Digital transformation and cybersecurity challenges for business resilience: Issues and recommendations. *Sensors, 23*(15), 6666. https://doi.org/10.3390/s23156666

Arner, D. W., Barberis, J., & Buckley, R. P. (2023). Digital banking security frameworks: Consumer trust and cyber security risk. *Journal of Financial Regulation and Compliance, 31*(2), 145-168.

Kaur, P., Kaur, J., & Singh, G. (2023). Understanding consumer trust in digital banking: The role of cyber security measures. *Journal of Financial Services Marketing, 28*(2), 157–172. https://doi.org/10.1057/s41264-023-00199-5

Kumar, N., & Gupta, R. (2023). The role of perceived privacy in enhancing consumer trust in digital banking platforms. *Electronic Commerce Research, 24*(1), 145–162. https://doi.org/10.1007/s10660-023-09678-1

Lu, Y., & Zhu, H. (2024). Consumer awareness of cyber security and its influence on trust in digital banking services. *Journal of Information Security and Applications, 78*, 103121. https://doi.org/10.1016/j.jisa.2024.103121

Nguyen, T. K., & Lee, J. H. (2024). The role of user education in fostering trust and mitigating cybersecurity threats in digital banking. *Computers in Human Behavior, 139*, 107567.

Saudi Aramco Cybersecurity Research Team (2023). Digital transformation and cyber security challenges for business resilience: Issues and recommendations. *Sensors, 23*(15), 6666. https://doi.org/10.3390/s23156666.

Sharma, R., Gupta, S., & Khandelwal, U. (2023). Impact of bank reputation on digital trust and cybersecurity perception. *Journal of Internet Banking and Commerce, 28*(4), 112-130.