



Securing the Future of Finance: Cyber security's Impact on Trust and Usage in Online Banking

Usha*, Ashwini G.C. and Mahantesh K. Chubachi

Department of Studies in Commerce, Davangere University, Davangere, Karnataka, India
ushapoojary123@gmail.com

Available online at: www.isca.in, www.isca.me

Received 26th May 2026, revised 30th June 2026, accepted 1st September 2026

Abstract

Online banking was expanded and has revolutionized the banking industry; however, the Cybersecurity question remains to stimulate the customer confidence and use habits. The paper explores the relationship between customer trust, usage behavior and Cybersecurity awareness among the Indian online banking users and how the awareness of cyber threat and the experienced problems and trust in the security measures of the banks dictates the transaction behavior and willingness. The paper also looked at the primary data of 132 online banking users in terms of descriptive statistics, tests of binomial and tests of Kruskal-Wallis as well as structural equation modeling (SEM). The most significant variables will be self-reported customer Cybersecurity knowledge, personal experience of being a victim of cyber threats, use of preventive measures, and confidence in online security behavior. The review informs that the degree of Cybersecurity awareness and a high degree of trust correlate with the more frequent and confident use of online banking and the past cyber incidents correlate with the higher degree of caution and preparedness. The analysis of SEM shows that the influence of Cybersecurity concerns on customer trust partially depends on customer preparedness and the model shows an adequate fit. The results suggest that increased transparency will be required and that certain aspects of Cybersecurity awareness would be implemented that could allow using online banking platforms safely and sustainably. The paper gives theoretical information and practical proposals to the banking sector with references to that fact that Cybersecurity plays a very important role in generating customer trust.

Keywords: Online Banking, Trust, Cybersecurity, Customer Preparedness, Digital Financial Services.

Introduction

The use of the online banking has transformed the manner in which the financial services are being provided to the customers and its usage has made financial services easier and more accessible to the customers to carry out their daily tasks such as fund transfer, paying bills, making transactions via e-commerce and booking tickets. This shift to online banking has been astonishingly rapid in India, particularly, and has been driven by the widespread use of smart phones, a growing internet connection, and government programs like the Unified Payments Interface (UPI) platform and the India Stack platform¹. These innovations have changed how people and businesses conduct their finances.

Nevertheless, with the rising usage of online banking, the financial services industry is also prone to cyber threats, making it one of the most frequently attacked sectors. In the banking sector, Cybersecurity refers to the adoption of strategies and technologies to protect computer systems, digital infrastructure, and customer information from unauthorized access and fraud, as well as business continuity and confidence among customers².

Phishing, malware, identity theft, and fraudulent websites are

the ways in which the cybercriminals are misusing the weaknesses in banking platforms through creating significant risk for both financial institutions and consumers³.

Recent industry estimates indicate rapid expansion in the digital banking landscape. Precedence Research (2024) reports that the global e-banking sector accounted for nearly US dollars 9.50 trillion in 2024, and is estimated to increase to nearly US dollars 15.59 trillion by the year 2034, showing a compound yearly growth rate of about 5.08 percent during 2025-2034⁴. Despite of this upward trend shows rapid digital uptake, it simultaneously highlights the growing importance of strengthening Cybersecurity structures within online banking systems.

Cybersecurity has evolved as a foundational driver for establishing and maintaining user trust in context of digital financial services⁵. An effective application of Cybersecurity tools safeguards confidential customer information, reduce the risk of unauthorized system access, and ensures the credibility of the online transaction is ensured⁶. Likewise, digital banking solutions are projected to experience tremendously over the coming years with market value increasing from US dollars 111 billion to US dollars 421 billion by 2029 in future, as per IBEF report, suggesting a significant area for technological advancement and operational efficiency⁷.

However, the sustainability of this expansion largely depends on users' perceptions of platform safety. Customer confidence, trust, and satisfaction are key determinants of continued engagement with online banking services, playing a decisive role in their long-term acceptance and usage^{5,8}.

This study explores how Cybersecurity awareness, user experiences with cyber incidents, and trust in banks' security systems influence online banking usage behaviors. It also investigates the role of preparedness such as adopting strong authentication practices in mediating the relationship between Cybersecurity challenges and customer trust.

Literature Review: In a study in Plakkad, Kerala, customers were found to have higher trust in internet banking when more aware of Cybersecurity, and were more likely to use it. The researchers demonstrated that customer perception of online security is more secure and confident, based on the questionnaire responses. The study highlights the importance of banks enlightening users and implementing the use of stronger security to encourage more and safer use of digital banking⁹. A different study results in a higher probability that people trust and use digital payments when they are convenient, have evident advantages, a powerful complaint resolution mechanism, and are influenced by social support. Cybercrime can result in negative exposure that can diminish usage in trustworthy systems. The paper highlights the importance of establishing trust by creating secure and user-friendly technologies to drive more individuals into the digital economy and enhance internet safety, particularly in high-risk settings¹⁰.

The research fills this gap in the academic literature on user perceptions of institutional protection of digital payments, and demonstrates that trust grows in the presence of well-performing public institutions, prompt reactions to Cybersecurity challenges, and consistent security-related actions with user values. It provides Indian policymakers with the insights to develop safer, more trusted digital payment systems that are more indicative of cultural and user interests¹¹. The paper identifies the increasing issue of cyber fraud in e-banking and concludes that more knowledgeable users about Cybersecurity tend to bank safely and develop protective habits. Attitudes towards e-banking are enhanced by ease of use and perceived usefulness, but more studies are required on security-related decisions. It emphasizes that Cybersecurity education, easy-to-use features, and cooperation between banks, policymakers, and governments are important to help train users, improve regulations, and safer digital banking¹².

The researchers discover that security features such as biometrics and SMS notifications are more popular among mobile banking users because of their convenience and reliability, and the use of MFA is not widespread because of the lack of awareness. The use of weak passwords is a threat though they are still being used. The most significant factors that affected the adoption of technology are trust, perceived

usefulness, and usability, which underscore the importance of concerted efforts by banks, developers, and policymakers to enhance awareness, streamline security features, and train users to enhance mobile banking security¹³. The article has conducted a review of 58 articles and has found that identity theft, malware and phishing are significant threats that are slowing down the adoption of digital banking by compromising consumer trust, particularly in the developing markets. It outlines the necessity to invent industry-based and sustainable Cybersecurity lines to address the increasing breaches. Reducing such risks will help banks increase customer trust and promote the efforts toward digital banking even more¹⁴.

The study reveals a growing risk of online transactions and the general ignorance of threats of online fraud, phishing, and identity theft. It involves user education, security-related activities and engagement to vulnerable groups. The suggested framework encourages unremitting evaluation and cooperation among the users, institutions, and platforms to create a safer, more trustworthy, and user-focused digital transaction setting¹⁵. The paper explores the increasing cyber threat in internet banking, investigating the latest cases, financial consequences, and the success of the existing strategies. It demands adaptive methods based on the newest technologies such as AI and Big Data, as well as enhanced regulatory adherence and consumer knowledge. It encourages banks to invest in these fields to secure assets and maintain confidence in the digital age¹⁶. The article focuses on the impact of credibility and security as the two dimensions of E-service quality on the trust of customers in E-banking in Indian banks. The research was carried out among 420 respondents of the public and private sector banks in Delhi/NCR, where the respondents were aged above 18 years and had more than six months of E-banking experience. The results of the FEA, CFA, and SEM analysis, conducted with the help of SPSS 24 and AMOS 21 shows that the credibility and security can contribute to the customer trust significantly, and banks should work on both to build more confidence in their online services¹⁷.

Although past research has investigated Cybersecurity awareness, trust, and security tools in digital banking, there is a shortage of research investigating the combined effects of Cybersecurity incidents, Cybersecurity awareness, and preparedness on trust and usage behavior, particularly in the Indian online banking setting, which is dominated by UPI platforms. Although there has been increased interest in this field, there are limited studies that have used SEM to explore these associations, a gap that the present study is trying to fill.

Objectives of the Study: To assess customer awareness and experiences of Cybersecurity threats in online banking transactions. To evaluate the impact of Cybersecurity on customer trust in banks' security measures. To analyze how Cybersecurity concerns influence customers' online banking usage and preparedness behaviors.

Methodology

The study is based on the descriptive-analytical approach to examine the impact of Cybersecurity on customer trust in online banking practice and customer trust in Karnataka. The descriptive part of the research was aimed at giving an overview of demographic characteristics of groups that responded to the questionnaires, their awareness of Cybersecurity, and experience of online banking transactions. The paper will focus on exploring how Cybersecurity issues, customer readiness, and trust are interconnected using Structural Equation Modeling.

The sample size was composed of individuals that utilize the services of online banking actively and live in Karnataka. Purposive sampling was used since the total population size was not well known so that those respondents who are well versed with online banking could be targeted¹⁸. The analysis of data was conducted on 132 valid respondents. The study conducted online survey as primary data collection method. The questionnaire was constructed in such a way that it should collect data about Cybersecurity awareness, trust in bank security, previous experience of Cybersecurity attacks, internet banking habits, and willingness to respond to possible attacks. The questionnaire comprised of Likert-scale statements and binary (Yes/No) questions pertaining to the online banking problem and Cybersecurity concerns to achieve the best measure of the study variables¹⁹.

Jamovi software (version 2.6.44) was used to check the reliability and validity of the research instrument²⁰⁻²¹. Cronbach alpha was used to assess internal consistency and the scores were 0.940 for all constructs indicating high reliability. Taber suggests that alpha coefficients of 0.70 or higher are considered to be satisfactory as far as internal consistency is concerned, so the measurement tool is considered appropriate to proceed with the analysis²². Both descriptive and inferential statistical analyses, including descriptive statistics, binomial tests, and Kruskal Wallis tests were used to analyze the collected data. Also, Structural Equation Modeling was used to analyze both the direct and indirect relationship between the variables in this study²³⁻²⁹. It was used to examine the impact of Cybersecurity issues on customer trust with customer preparedness acting as a mediator.

Table-1: Data Description for Structural Equation Model

Construct	Code	Items	Response Scale
Cybersecurity Issues Faced by Customers (Cyb_I)	I1–I10	10	5-point Likert (Strongly Disagree–Agree)
Customer Preparedness and Response (Cst_P)	P1–P10	10	5-point Likert (Strongly Disagree–Agree)
Customer Trust in Bank's Security Measures (Cst_T)	T1–T5	5	Dichotomous (Yes/No)

Table-1 shows the variables of the structural equation model: Cybersecurity Issues Faced by Customers (Cyb_I), Customer Preparedness and Response (Cst_P), and Customer Trust in Bank Security Measures (Cst_T). These measures combined investigate the Cybersecurity experiences, protective behaviors, and trust of customers in the security systems of banks and facilitate the structural equation modeling analysis.

Results and Discussion

The demographic data (Table-2) shows that the sample comprised a higher percentage of female respondents (62.1%). The majority of participants were aged 21-30 years (74.2%). Education level is also high in the sample with 48.6 percent being post graduates. A large percentage (58.3) were earning less than 20,000 monthly and a large percentage of the respondents were students (41.7% or 37.1% employed). This implies that the research primarily consists of educated and economically active people that frequently use online resources and possess the corresponding experience connected to the topic of Cybersecurity.

Table-2: Demographic Distribution of the Sample.

Variables		Respondents	%
Gender	Male	50	37.9
	Female	82	62.1
Age	Below 20	7	5.3
	21-30	98	74.2
	31-40	21	15.9
	41-50	5	3.8
	51 and above	1	0.8
Educational Level	Below High school	4	3
	High school	16	12.1
	Graduate	44	33.3
	Post-Graduate	64	48.6
	Others	4	3
Occupation	Student	55	41.7
	Employed	49	37.1
	Business Owner	15	11.4
	Retired	3	2.3
	Others	10	7.5
Monthly Income	Less than 20,000	77	58.3
	20,000-40,000	38	28.8
	40,000-60,000	7	5.3
	60,000-80,000	4	3
	Above 80,000	6	4.5

According to Figure-1 UPI-based applications like Google Pay and PhonePe are the most popular online banking applications, utilizing 53% of the total usage. The second most popular is mobile banking apps, as 24% of respondents use them. Digital wallets such as Paytm and PayPal have 11 percent usage and internet banking via web portals have 10 percent usage. The percentage of respondents who use other platforms is low (2%).

The results indicate that UPI is the most preferred by digital banking, because of its simplicity, instant transfer, and wide acceptance among merchants.

The patterns of online banking usage of respondents are illustrated in Figure-2. Half (48.5) reported that they had been using online banking daily, which means that online banking is well integrated into their financial lives. A quarter (24.2) of them used it at least once a week with smaller percentages saying it was occasionally used monthly (11.4) and occasionally used less frequently (11.4). Only 4.5% of the people were not using online banking. This distribution confirms the fact that the largest part of the respondents are regular users, hence the consumption of the digital financial services is gaining increased importance and the Cybersecurity is critical to the maintenance of trust and stability in further consumption thereof. **H₁:** Customers have a significant level of awareness of Cybersecurity threats in online banking.

The results of the binomial test (Table-3) reveal that the majority of respondents showed significant awareness of various Cybersecurity threats in online banking, with between 72% and 85% answering Yes across all items. The results show that 84.8% were aware that banks would never call or send a message asking sensitive information like OTPs or passwords, and 81.1% understood the significance of a strong and unique password. Even the lowest awareness was still relatively high (72% knowing how to report a fraud incident). Since all items returned $p < .001$, the proportions of Yes responses were significantly higher than 0.5, indicating that customers possess a

strong overall awareness of cyber threats in banking transactions.

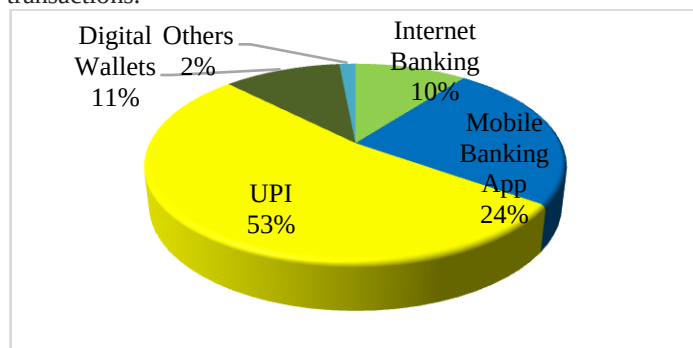


Figure-1: Usage of Online Banking Services.

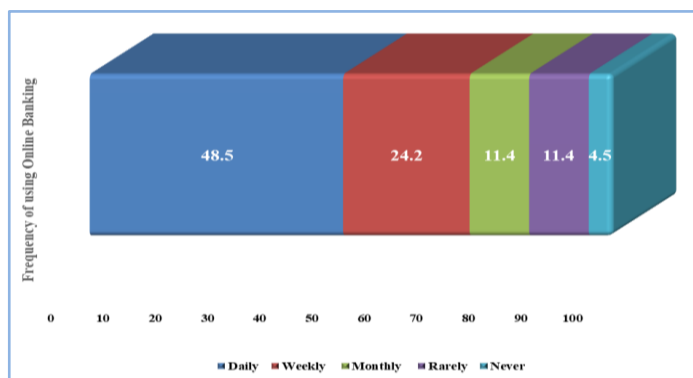


Figure-2: Frequency of using Online Banking.

Table-3: Binomial Test for Customer Awareness of Cyber Threats in Online Banking.

Awareness Statement	Yes (n, %)	No (n, %)	Proportion Yes	p-value <
I am aware of phishing scams targeting online banking users	104 (78.8%)	28 (21.2%)	0.788	.001
I know that cybercriminals can steal banking details through fake websites or apps	102 (77.3%)	30 (22.7%)	0.773	.001
I understand the importance of using strong and unique passwords for online banking	107 (81.1%)	25 (18.9%)	0.811	.001
I am aware that public Wi-Fi can be risky for conducting banking transactions	104 (78.8%)	28 (21.2%)	0.788	.001
I know how to recognize suspicious emails or messages claiming to be from my bank	101 (76.5%)	31 (23.5%)	0.765	.001
I am familiar with the concept of two-factor authentication for securing banking access	107 (81.1%)	25 (18.9%)	0.811	.001
I know that banks never ask for confidential information like OTP or passwords via calls or messages	112 (84.8%)	20 (15.2%)	0.848	.001
I regularly receive Cybersecurity awareness messages or tips from my bank	99 (75.0%)	33 (25.0%)	0.75	.001
I have seen or heard news about recent cyber attacks targeting banking systems	106 (80.3%)	26 (19.7%)	0.803	< .001
I know how to report a suspected cyber fraud incident to my bank	95 (72.0%)	37 (28.0%)	0.72	< .001

The results of the binomial test give solid reasons to accept H_1 since the percentage of the “Yes” answers to all ten statements of awareness were significantly more than the amount of 0.5 which is the neutral value ($p < .001$ for each item). Having a level of awareness of between 72% and 85%, there is statistical evidence that a significant percentage of all respondents were familiar with some of the most common Cybersecurity threats, including phishing, deceptive websites, the dangers of using the Internet in a cafe, and reporting processes. This statistically significant non-randomness of chance demonstrates that customers do not simply have random or partial knowledge but have an informed and structured knowledge, and confirm the

relationship hypothesized. H_2 : Experiences of Cybersecurity issues significantly influence customers’ trust in banks’ security measures.

Table-4 shows the details of fit statistics of the proposed structural equation model. Considering all the result, the obtained values fall within acceptable limits, indicating that the model provides an adequate representation of the relationships among the study variables. Accordingly, the model is considered suitable for further interpretation of the structural paths³⁰.

Table-4: Goodness-of-Fit Measures of the Structural Equation Model.

Fit Index	Value	95% Confidence Interval	Interpretation
Chi-square (χ^2)	410	df = 272, $p < .001$	Significant (common in large models)
Comparative Fit Index (CFI)	0.990	—	Excellent fit (≥ 0.95)
Tucker-Lewis Index (TLI)	0.989	—	Excellent fit
Root Mean Square Error of Approximation (RMSEA)	0.062	0.050 – 0.074	Acceptable fit (< 0.08)
RMSEA p-value	0.055	—	Marginal support
Standardized Root Mean Square Residual (SRMR)	0.105	—	Slightly above ideal (0.08)

Table-5: Structural Path Estimates of SEM.

Dependent Variable	Predictor	Estimate	Std. Error	95% Confidence Interval- Lower	95% Confidence Interval-Upper	Standardized β	z	p-value
Customer_Trust	Customer_Preparedness	0.442	0.105	0.236	0.647	0.618	4.20	<.001
Customer_Trust	Cybersecurity_Issues	-0.146	0.075	-0.293	0.001	-0.210	-1.95	0.052
Customer_Preparedness	Cybersecurity_Issues	0.245	0.043	0.162	0.328	0.373	5.76	<.001

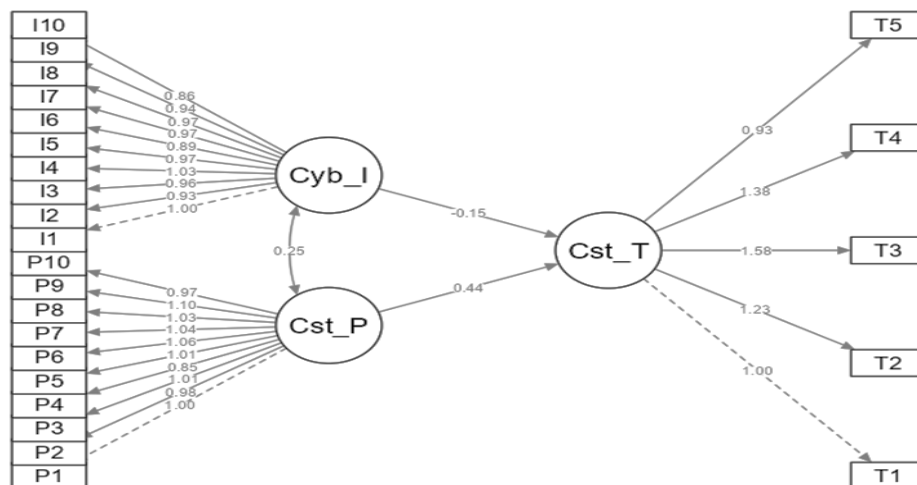


Figure-3: Structural Equation Model of the Influence of Cybersecurity issues on Customer Trust with Customer Preparedness as Mediator.

Table-5 outlines the estimated structural relationships among cybersecurity issues, customer preparedness, and customer trust. The findings indicate that cybersecurity issues significantly influence customer preparedness ($\beta = 0.373$, $p < .001$), pointing to the role of exposure to cybersecurity-related problems encourages customers to adopt more cautious and proactive security behaviors while using online banking services.

The results of the path analysis shows that customer preparedness has a positive relationship with customer trust, whereas cybersecurity issues show a slight negative effect. The indirect influence through preparedness reduces the overall impact of cybersecurity concerns on trust.

As per Figure-3 demonstrate the structural equation model (SEM) for Hypothesis H₂, showing the relationships among Cybersecurity issues (Cyb_I), customer preparedness (Cst_P), and customer trust (Cst_T). The diagram reveals both the direct effect of Cybersecurity issues on customer trust and the indirect effect through the customer preparedness. The path coefficient from Cybersecurity issues to customer preparedness is positive (0.25), indicating that experiencing Cybersecurity incidents tends to increase customers' preparedness measures (e.g., stronger passwords, vigilance in online banking). The path from customer preparedness to customer trust is positive (0.44), showing that greater preparedness significantly enhances customers' trust in banks' security systems. The direct correlation between Cybersecurity problems and customer trust is negative (-0.15), depicts that Cybersecurity problems can reduce trust a bit in the absence of any mitigating variables.

This pattern reflects a partial mediation, even though Cybersecurity incidents affect trust negatively, although to a small extent, their total impact is mediated via the positive indirect effect of high preparedness. That is, as customers grow more ready in reaction to Cybersecurity threats, it counterbalances the trust loss that could result due to such incidents.

As presented in Table-6, all observed items load significantly onto their corresponding latent constructs, with standardized factor loadings above acceptable levels ($p < .001$). This confirms

strong construct validity and indicates that the latent factors of Cybersecurity issues, customer preparedness, and customer trust are reliably measured.

Based on these findings, Hypothesis H₂ is accepted. H₂ states that experiences of Cybersecurity issues influence customers' trust in banks' security measures, and the results confirm this relationship. The influence is primarily indirect, as increased customer preparedness significantly enhances trust, while Cybersecurity issues on their own show a modest weakening influence on trust. This indicates partial mediation. In simple terms, Cybersecurity issues tend to lower trust, but when customers are well-prepared, this negative impact is reduced customer preparedness acts as a shield between issues and trust. **H₃:** Cybersecurity concerns significantly affect customers' online banking usage and preparedness.

According to the Krushal-Wallis test (Table-7) the pattern of use of online banking services (daily, weekly, monthly, rarely, never) had a significant effect on various dimensions of Cybersecurity preparedness. Customers who used online banking more frequently (daily or weekly) demonstrated stronger preparedness practices compared to less frequent users. These included using strong and unique passwords ($\chi^2 = 12.42$, $p = 0.015$), regularly updating banking apps and software ($\chi^2 = 15.26$, $p = 0.004$), enabling two-factor authentication ($\chi^2 = 11.88$, $p = 0.018$), verifying suspicious links or emails ($\chi^2 = 12.80$, $p = 0.012$), knowing how to report fraud ($\chi^2 = 10.09$, $p = 0.039$), staying updated about cyber threats ($\chi^2 = 12.85$, $p = 0.012$), and feeling confident in protecting themselves from fraud ($\chi^2 = 12.74$, $p = 0.013$). These findings indicate that more frequent users tend to adopt stronger Cybersecurity behaviors.

In contrast, avoiding public Wi-Fi showed only marginal significance ($\chi^2 = 9.41$, $p = 0.052$), while receiving Cybersecurity guidance from banks ($\chi^2 = 6.29$, $p = 0.178$) and taking immediate action when suspecting fraud ($\chi^2 = 5.83$, $p = 0.212$) were not significantly influenced by usage frequency. These findings support Hypothesis H₃ partly. Even though the significance of Cybersecurity issues is relevant to most of the preparedness behaviors, not all practices are equally affected.

Table-6: Measurement Model Factor Loadings.

Latent	Observed	Estimate	SE	95% Confidence Intervals Lower	95% Confidence Intervals Upper	B (Beta coefficient)	z (Test Statistic)	p
Cst_P	P1	1.000	0.0000	1.000	1.000	0.799		
	P2	0.983	0.0476	0.890	1.077	0.786	20.64	<.001
	P3	1.007	0.0487	0.912	1.103	0.805	20.70	<.001
	P4	0.853	0.0605	0.734	0.972	0.682	14.10	<.001
	P5	1.009	0.0519	0.908	1.111	0.807	19.46	<.001
	P6	1.056	0.0467	0.964	1.147	0.844	22.62	<.001
	P7	1.044	0.0470	0.952	1.136	0.835	22.21	<.001

	P8	1.031	0.0481	0.937	1.125	0.824	21.44	<.001
	P9	1.104	0.0446	1.016	1.191	0.882	24.72	<.001
	P10	0.969	0.0481	0.874	1.063	0.774	20.12	<.001
Cyb_I	I1	1.000	0.0000	1.000	1.000	0.822		
	I2	0.930	0.0385	0.855	1.006	0.764	24.19	<.001
	I3	0.961	0.0425	0.878	1.044	0.790	22.59	<.001
	I4	1.032	0.0426	0.949	1.116	0.848	24.23	<.001
	I5	0.970	0.0434	0.885	1.055	0.797	22.35	<.001
	I6	0.892	0.0481	0.798	0.986	0.733	18.57	<.001
	I7	0.967	0.0457	0.877	1.056	0.794	21.14	<.001
	I8	0.973	0.0444	0.886	1.060	0.799	21.90	<.001
	I9	0.941	0.0483	0.846	1.035	0.773	19.47	<.001
	I10	0.862	0.0554	0.754	0.971	0.709	15.56	<.001
Cst_T	T1	1.000	0.0000	1.000	1.000	0.571		
	T2	1.235	0.3598	0.530	1.940	0.705	3.43	<.001
	T3	1.581	0.3341	0.926	2.236	0.903	4.73	<.001
	T4	1.384	0.3097	0.777	1.991	0.790	4.47	<.001
	T5	0.928	0.3343	0.273	1.583	0.530	2.78	0.005

Table-7: Kruskal–Wallis Test Results of Cybersecurity Preparedness (DV) by Online Banking Usage Frequency (IV).

Cybersecurity Preparedness Item	χ^2	df	p-value	Decision (at $\alpha = 0.05$)
Use of strong & unique passwords	12.4	4	0.015	Reject H_0
Regularly update app/software	15.3	4	0.004	Reject H_0
Use of two-factor authentication	11.9	4	0.018	Reject H_0
Avoid using public Wi-Fi	9.41	4	0.052	Fail to Reject (marginal)
Verify suspicious links/emails	12.8	4	0.012	Reject H_0
Know how to report fraud	10.1	4	0.039	Reject H_0
Stay updated about cyber threats	12.9	4	0.012	Reject H_0
Received guidance from bank	6.29	4	0.178	Fail to Reject
Immediate action if fraud suspected	5.83	4	0.212	Fail to Reject
Confidence in protecting against fraud	12.7	4	0.013	Reject H_0

Key Findings

Some significant findings about the relationship between Cybersecurity, customer trust, and online banking usage were made in the research.

H₁ confirmed that customers are highly attuned to Cybersecurity with 72-85% of customers demonstrating that they were aware of phishing, strong passwords, two-factor authentication, and reporting policies. The indicators were all statistically significant ($p < .001$), which shows that the awareness campaigns and the digital literacy interventions have reached considerable number of users.

H₂ proved that customer trust is affected by Cybersecurity

incidents in a twofold manner. Direct experiences had a marginally negative impact on trust ($\beta = -0.210$, $p = 0.052$), however the incidents had a strong positive impact on customer preparedness ($\beta = 0.373$, $p < .001$), which in turn had a strong positive impact on trust ($\beta = 0.618$, $p < .001$). This partial mediation underscores preparedness as one of the major mechanisms in ensuring customer confidence although they are exposed to cyber risks.

H₃ concluded that the rate of usage of online banking has a significant impact on Cybersecurity preparedness. Protective actions like regular updates to apps ($p = 0.004$), two-factor authentication ($p = 0.018$) and suspicious links verification ($p = 0.012$) were more frequently adopted by frequent users (daily or weekly) than infrequent users.

The research further established that UPI platforms are the most common when it comes to the use of digital banking (53%), mobile banking apps (24%), and internet banking portal (10%). The demographic profile shows that young (21-30 years), highly educated (48.6% postgraduates) with a majority of female users (62.1%), are the most engaged users, which implies a digitally active and financially conscious population.

Suggestions: Based on the findings, there is a series of strategic recommendations that are needed to enhance customer confidence and Cybersecurity readiness in online banking. The research indicates that even with the high levels of awareness there still exist knowledge and understanding gaps as awareness and implementation are two distinct fields, especially among infrequent users. The mediation effect is added, which implies that the successful management of Cybersecurity incidents, as well as a consistent educational process, can assist in transforming the potential loss of trust into an increase in resilience. It is recommended that these gaps be addressed by the following recommendations to leverage the positive effect of preparedness: Targeted Cybersecurity Education: Financial institutions ought to create segment-wise awareness programs focusing on less frequent users as well as high-risk segments. Creation of more sophisticated security measures: Two-factor authentication, biometrics, and automatic update reminders in the application should be actively encouraged with the help of the user-friendly design. Transparent Risk Communication: Banks are advised to embrace proactive communication approach to discuss new risks that are emerging to counter the loss of trust in the short-run following cyber-attacks. Regulatory Alignment: It is even hinted that policymakers ought to synthesize the demands of digital banking security and achieve inter-institutional collaboration to create resiliency in the sector.

Conclusion

The study confirms that Cybersecurity is a significant consideration when deciding the customer trust and adoption behaviour in online banking. It further points out that awareness, readiness and incident experience are rather interconnected and are joint determinants of user behavior. The levels of awareness of respondents showed that there was high level of awareness (72-85) of phishing and strong password and two factor authentication among the users. But the direct exposure to the instances of Cybersecurity has insignificant negative impact on confidence, which underlines the remaining psychological echo of intrusions and fraudulent activities.

Importantly, the study concludes that preparedness is an effective mediator that transforms negative experiences to positive behavioral changes. This degree of trust in the banking systems ($\beta = 0.618$, $p < .001$) was a resilience effect and was experienced by the better prepared users. Additionally, Cybersecurity behaviour, such as updating their applications in a timely fashion ($p = 0.004$), two-factor authentication ($p = 0.018$), and awareness of phishing attacks ($p = 0.012$) was more

advanced among frequent (daily/weekly) users as compared to occasional users.

These lessons are a pointer to that the future of the digital banking trust any longer refers to the technical perplexity of the security measures, but also to the ability to make the end-users the active agents of the security measures of their own transactions. High-frequency, mobile-first channels have been revealed as a key origin of generating real-time Cybersecurity awareness and reacting to cyber attacks due to the prevalence of UPI (53%).

Policymaking and management lens, banks must find the balance between the quick innovation and user-centered Cybersecurity rules like proactive education, open communication in case of an attack, and the large-scale use of advanced authentication processes.

In addition to these findings, the study also emphasizes the need to have multi-stakeholder cooperation to establish a secure and trustworthy digital banking system. Banks, regulatory bodies, the creators of fintech, and customers will have to collaboratively create a culture of cyber resilience in which threat detection, quick response and constant user attention, functions work together. The introduction of advanced analytics, such as artificial intelligence and machine learning to identify fraud and/or to send custom risk warnings, can also encourage confidentiality among users. In addition to this, the congruency of Cybersecurity with financial inclusion will contribute to providing equal access to safe and financial services by underserved populations, such as rural and first-time users of digital banks. By overcoming these technological and social anomalies, the industry will be able to evolve to a more welcoming, adaptable and sustainable online banking system.

Limitations include the geographically oriented sample and the data were self-reported, which may not be able to represent all user groups, or over-represent awareness. The future should utilize long term studies and cross country studies to be conducted to explore the dynamics of customer preparedness in the long term and whether it may help create long term loyalty in digital banking.

References

1. Singh, S., & Srivastava, R. K. (2018). Predicting the intention to use mobile banking in India. *International Journal of bank marketing*, 36(2), 357-378.
2. B. B. Babu (2018). Cybersecurity in Banks. *J. Indian Inst. Bank. Finance*, 89(1), 26-32.
3. Al-Dosari, K., Fetais, N., & Kucukvar, M. (2024). Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges. *Cybernetics and systems*, 55(2), 302-330.
4. Zoting, S. (2025). Artificial Intelligence (AI) Market Size

- to Hit USD. 3,680.47 Bn by 2034.
5. Mukherjee, A., & Nath, P. (2003). A model of trust in online relationship banking. *International journal of bank marketing*, 21(1), 5-15.
 6. Al-Alawi, A. I., Al-Khaja, N. A., & Mehrotra, A. A. (2023). Women in cybersecurity: a study of the digital banking sector in Bahrain. *Journal of International Women's Studies*, 25(1), 21.
 7. India Brand Equity Foundation (2025). Banking in India: Growth, trends, and opportunities. India Brand Equity Foundation, Industry report.
 8. Arora, P., & Banerji, R. (2024). The impact of digital banking service quality on customer loyalty: An interplay between customer experience and customer satisfaction. *Asian Economic and Financial Review*, 14(9), 712-733.
 9. Shirisha, A. (2026). Impact of Cybersecurity Awareness on user Behaviour in Digital Banking: A Study on Risk Perception, Preparedness and Financial Implications. *International Journal of Creative and Open Research in Engineering and Management*, 2(04).
 10. Aljaradat, A., & Shukla, S. K. (2025). Trust and cybersecurity in digital payment adoption: socioeconomic insights from India. *Journal of Business and Socio-Economic Development*, 5(4), 372-386.
 11. 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.
 12. Afzal, M., Ansari, M. S., Ahmad, N., Shahid, M., & Shoeb, M. (2024). Cyberfraud, usage intention, and cybersecurity awareness among e-banking users in India: an integrated model approach. *Journal of Financial Services Marketing*, 29(4), 1503-1523.
 13. I. Riasat, M. Shah, and M. S. Gonul, "Strengthening Cybersecurity Resilience: An Investigation of Customers' Adoption of Emerging Security Tools in Mobile Banking Apps," *Computers*, vol. 14, no. 4, 2025,
 14. Riasat, I., Shah, M., & Gonul, M. S. (2025). Strengthening cybersecurity resilience: An investigation of customers' adoption of emerging security tools in mobile banking apps.
 15. Aftab, R. S., Emon, M. K. K., Anny, S. F., Sarker, D., & Mazid-Ul-Haque, M. (2024). Security Analysis in Online Transaction Systems: A Proposed Framework. *International Journal of Information Engineering and Electronic Business*, 16(2), 22.
 16. Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies application. *World Journal of Advanced Research and Reviews*, 21(3), 625-643.
 17. Jyoti, Kesharwani, S., & Chaudhry, S. S. (2025). Assessing the Impact of Credibility and Security on Customers E-Trust in the Context of Indian Banks. *Journal of Industrial Integration and Management*, 10(02), 341-362.
 18. Nyimbili, F., & Nyimbili, L. (2024). Types of purposive sampling techniques with their examples and application in qualitative research studies.
 19. R. Acharyya and N. Bhattacharya (2019), Eds., *Research Methodology for Social Sciences*. London: Routledge India, 2019.
 20. Gallucci, M., & Jentschke, S. (2021). *SEMLj: jamovi SEM Analysis*. [jamovi module].
 21. The jamovi project (2018). *Jamovi*. (2024). [Online]. Available: <https://www.jamovi.org>
 22. K. S. Taber (2017). The Use of Cronbach's Alpha When Developing and Reporting Research Instruments in Science Education. *Res. Sci. Educ.*, 48(6), 1273-1296.
 23. R. Shah and S. M. Goldstein, "Use of structural equation modeling in operations management research: Looking back and forward," *J. Oper. Manag.*, vol. 24, no. 2, pp. 148-169, 2005, Shah, R., & Goldstein, S. M. (2006). Use of structural equation modeling in operations management research: Looking back and forward. *Journal of Operations management*, 24(2), 148-169.
 24. Rosseel, Y. (2012). lavaan: An R package for structural equation modeling. *Journal of statistical software*, 48, 1-36.,
 25. R Core Team, R. (2024, January). *R: A language and environment for statistical computing*.
 26. McKight, P. E., & Najab, J. (2010). Kruskal-wallis test. *The corsini encyclopedia of psychology*, 1-1.
 27. Whittaker, T. A., & Schumacker, R. E. (2022). *A beginner's guide to structural equation modeling*. Routledge.
 28. Hutson, A. D. (2006). Modifying the exact test for a binomial proportion and comparisons with other approaches. *Journal of Applied Statistics*, 33(7), 679-690.
 29. S. Epskamp, S. Stuber, J. Nak, M. Veenman, and T. D. Jorgensen, "semPlot: Path Diagrams and Visual Analysis of Various SEM Packages' Output. [R Package]," 2019,
 30. Xia, Y., & Yang, Y. (2019). RMSEA, CFI, and TLI in structural equation modeling with ordered categorical data: The story they tell depends on the estimation methods. *Behavior research methods*, 51(1), 409-428.