ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 162, Feb 2026
Paper ID: RRJ201489
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-162-february-2026/RRJ201489

CYBERSECURITY RISKS IN DIGITAL BANKING WITH AN EMPIRICAL STUDY ON CUSTOMER AWARENESS THREAT PERCEPTION AND RISK MITIGATION STRATEGIES IN INDIA

Dr. ISHITA RAVAL
Assistant Professor
Sabarmati University, Ahmedabad

ABSTRACT

The rapid expansion of digital banking in India has significantly transformed financial transactions, offering convenience, accessibility, and efficiency. However, this growth has also intensified exposure to various cybersecurity risks, including phishing attacks, malware infections, identity theft, and data breaches. In this context, the present study examines cybersecurity risks in digital banking with a specific focus on customer awareness, threat perception, and risk mitigation strategies in India. The study adopts an empirical approach to assess how users perceive and respond to evolving cyber threats in the digital financial ecosystem. Primary data were collected through a structured questionnaire from 350 respondents across urban and semi-urban regions, ensuring a diverse representation of digital banking users. The study employs descriptive statistics to understand user demographics and usage patterns, factor analysis to identify underlying dimensions of cybersecurity awareness and behavior, and regression modelling to examine the relationship between awareness, threat perception, and adoption of risk mitigation strategies. The findings reveal that while a majority of users are actively engaged in digital banking, there exists a substantial gap in cybersecurity awareness, particularly among older individuals and users from semi-urban backgrounds. Although many respondents demonstrate basic awareness of common threats such as phishing, their understanding of advanced risks and preventive measures remains limited. Furthermore, the study indicates that higher levels of threat perception positively influence the adoption of security practices, such as using strong passwords, enabling two-factor authentication, and avoiding suspicious links. However, inconsistent application of these practices highlights the need for more effective user education. The study concludes that enhancing cybersecurity in digital banking requires a multi-stakeholder approach involving financial institutions, regulatory authorities, and customers. It recommends targeted awareness programs, especially for vulnerable user groups, along with the strengthening of regulatory frameworks and institutional security mechanisms. Additionally, banks and fintech companies should prioritize user-centric security designs and continuous monitoring systems to reduce cyber risks. Overall, the research contributes to understanding behavioral aspects of cybersecurity in digital banking and provides practical insights for improving digital financial safety in India.

Keywords: Cybersecurity, Digital Banking, Customer Awareness, Threat Perception, Risk Mitigation, Phishing, Identity Theft, Data Breach, Online Banking Security, India, Fintech, Cyber Fraud, Information Security, Banking Regulation, Digital Financial Services

Introduction

The proliferation of digital technologies has fundamentally reshaped the global banking landscape, and India stands as one of the fastest-growing digital financial ecosystems in the world. With the rapid expansion of internet penetration, smartphone usage, and government-led initiatives such as Digital India and financial inclusion programs, digital banking has emerged as a cornerstone of modern financial services. Customers increasingly rely on digital platforms including mobile banking

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 162, Feb 2026
Paper ID: RRJ201489
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-162-february-2026/RRJ201489

applications, internet banking portals, and digital wallets for conducting routine financial transactions such as fund transfers, bill payments, and account management. While these advancements have enhanced convenience, efficiency, and financial accessibility, they have simultaneously exposed users and institutions to a wide range of cybersecurity risks.

Cybersecurity has thus become a critical concern in the digital banking environment. As financial transactions move from physical branches to virtual platforms, the threat landscape has evolved significantly. Cybercriminals are employing sophisticated techniques such as phishing, malware attacks, ransomware, identity theft, and social engineering to exploit vulnerabilities in digital systems and human behavior. These threats not only compromise sensitive financial information but also undermine customer trust in digital banking systems. In India, where a large segment of the population is relatively new to digital financial services, the risks are further amplified due to varying levels of digital literacy and cybersecurity awareness.

One of the most pressing challenges in ensuring secure digital banking is the gap in customer awareness. While urban and younger populations tend to demonstrate a higher degree of familiarity with digital platforms, many users particularly those in semi-urban and rural areas lack adequate knowledge of safe online practices. This includes recognizing fraudulent messages, safeguarding personal credentials, and understanding the importance of security features such as two-factor authentication. The lack of awareness often makes users easy targets for cyber fraud, leading to financial losses and psychological distress. Therefore, understanding the level of customer awareness is essential for designing effective cybersecurity interventions.

In addition to awareness, threat perception plays a crucial role in shaping user behavior in digital banking. Threat perception refers to an individual's understanding and evaluation of potential risks associated with digital transactions. Users who perceive higher levels of risk are generally more cautious and likely to adopt preventive measures, whereas those with low threat perception may engage in risky behaviors such as sharing sensitive information or using unsecured networks. However, threat perception is not always aligned with actual risk levels, as it can be influenced by personal experiences, media exposure, and social factors. This mismatch between perceived and actual risks can hinder effective cybersecurity practices.

Risk mitigation strategies are another vital component in addressing cybersecurity challenges in digital banking. These strategies encompass both user-level practices and institutional measures aimed at minimizing the likelihood and impact of cyber threats. At the user level, practices such as creating strong passwords, regularly updating software, avoiding suspicious links, and enabling security alerts are essential. At the institutional level, banks and financial service providers implement advanced technologies such as encryption, intrusion detection systems, artificial intelligence-based fraud detection, and secure authentication mechanisms. Despite these measures, the effectiveness of risk mitigation largely depends on user compliance and awareness.

The Indian context presents unique challenges and opportunities in the domain of digital banking cybersecurity. On one hand, initiatives such as the Unified Payments Interface (UPI), Aadhaar-based authentication, and the rapid growth of fintech companies have significantly accelerated digital financial adoption. On the other hand, the diversity of users in terms of education, income, language, and technological exposure creates disparities in cybersecurity preparedness. Reports of increasing cyber fraud cases in India highlight the urgent need for comprehensive strategies that address both technological vulnerabilities and human factors.

The regulatory environment plays a significant role in shaping cybersecurity practices in digital banking. Regulatory bodies such as the Reserve Bank of India (RBI) have introduced guidelines and frameworks to enhance the security of digital transactions and protect customer interests. These include

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 162, Feb 2026
Paper ID: RRJ201489
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-162-february-2026/RRJ201489

mandates on data protection, customer authentication, and fraud reporting mechanisms. However, the dynamic nature of cyber threats requires continuous updates to regulatory frameworks and proactive collaboration between regulators, financial institutions, and technology providers.

The present study seeks to examine cybersecurity risks in digital banking through an empirical analysis of customer awareness, threat perception, and risk mitigation strategies in India. By focusing on these three interconnected dimensions, the study aims to provide a comprehensive understanding of how users interact with digital banking systems in the context of cybersecurity. The research is particularly relevant in identifying gaps in awareness and behavior that may contribute to increased vulnerability among users. The study also contributes to the existing literature by integrating behavioral and technological perspectives on cybersecurity. While previous research has often focused on technical aspects of cyber threats, there is a growing recognition of the importance of human factors in cybersecurity. User behavior, decision-making, and perception significantly influence the effectiveness of security measures. Therefore, examining these aspects in the context of digital banking can provide valuable insights for policymakers, financial institutions, and researchers. While digital banking has revolutionized the financial sector in India, it has also introduced complex cybersecurity challenges that require a multidimensional approach. Addressing these challenges necessitates not only technological advancements but also a deep understanding of user behavior and perception. By exploring the interplay between customer awareness, threat perception, and risk mitigation strategies, this study aims to contribute to the development of a secure and resilient digital banking ecosystem in India.

Review of Literature

The rapid evolution of digital banking has attracted significant scholarly attention, particularly in the context of cybersecurity risks, customer awareness, and behavioral responses to emerging threats. Existing literature highlights that while technological advancements have improved the efficiency and accessibility of banking services, they have also introduced complex security challenges that require both institutional safeguards and informed user behavior. This section reviews key studies related to cybersecurity risks in digital banking, focusing on customer awareness, threat perception, and risk mitigation strategies, with an emphasis on empirical findings and their implications. Early research in the domain of digital banking primarily emphasized technological infrastructure and system vulnerabilities. However, more recent studies have shifted toward understanding the human element in cybersecurity. For instance, studies by Aloul Fadi (2012) highlighted that human error remains one of the most significant contributors to cybersecurity breaches. The research demonstrated that even well-designed security systems can fail if users lack awareness or fail to follow secure practices. This perspective has been reinforced by subsequent studies, which argue that cybersecurity is not solely a technical issue but also a behavioral one.

Empirical studies conducted in the Indian context further reveal significant gaps in cybersecurity awareness among digital banking users. Research by Gupta Priya and Sharma Anil (2018) found that although users were familiar with basic digital banking operations, their understanding of cybersecurity threats such as phishing and malware was limited. The study observed that users often underestimated the risks associated with sharing personal information online, making them vulnerable to cyber fraud. Similarly, a study by Kumar Rajesh (2020) reported that awareness levels were significantly lower among older adults and individuals from semi-urban and rural areas, indicating a digital divide in cybersecurity preparedness. Threat perception has emerged as a critical determinant of user behavior in digital environments. According to research by Liang Huigang and Xue Yajiong (2010), individuals who perceive higher levels of risk are more likely to adopt protective behaviors, such as using strong passwords and avoiding suspicious links. Their study, based on Protection Motivation Theory (PMT),

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 162, Feb 2026
Paper ID: RRJ201489
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-162-february-2026/RRJ201489

demonstrated that perceived severity and vulnerability significantly influence security-related decision-making. This theoretical framework has been widely applied in subsequent studies to explain variations in user behavior across different contexts.

Singh Ritu (2021) found that while many users were aware of common threats like phishing, their perception of risk was often inconsistent with actual threat levels. The study suggested that media reports and personal experiences played a significant role in shaping threat perception. Users who had previously encountered cyber fraud were more cautious and proactive in adopting security measures, whereas others exhibited a sense of complacency. This finding aligns with global research, which indicates that experiential learning significantly influences cybersecurity behavior. Another important dimension explored in the literature is the adoption of risk mitigation strategies. Studies indicate that while users may be aware of certain security practices, consistent implementation remains a challenge. Research by Anderson Ross (2016) emphasized that usability issues often discourage users from adopting security measures. For example, complex authentication procedures may lead users to bypass security protocols for convenience. This trade-off between security and usability is a recurring theme in digital banking research.

Verma Neha (2022) examined the effectiveness of risk mitigation strategies among digital banking users. The findings revealed that while a majority of users reported using basic security measures such as passwords and OTP-based authentication, fewer users adopted advanced practices like regularly updating software or monitoring account activity. The study also highlighted the role of banks in promoting secure behavior through awareness campaigns and user-friendly security features. Institutional efforts and regulatory frameworks have also been extensively discussed in the literature. The role of central banks and regulatory authorities in ensuring cybersecurity has gained prominence, particularly in emerging economies. In India, the Reserve Bank of India (RBI) has introduced several guidelines to enhance the security of digital transactions. Studies suggest that regulatory interventions, such as mandatory two-factor authentication and customer liability frameworks, have contributed to reducing fraud incidents. However, researchers argue that regulations alone are insufficient without active user participation and awareness.

The rise of fintech has added another layer of complexity to the cybersecurity landscape. Fintech platforms often operate with innovative technologies and business models, which may not always align with traditional regulatory frameworks. Research by Arner Douglas et al. (2017) highlighted that while fintech enhances financial inclusion, it also introduces new vulnerabilities that need to be addressed through adaptive regulatory approaches. In India, the widespread adoption of platforms like UPI has increased transaction volumes, thereby attracting cybercriminals and necessitating stronger security measures. Cross-country studies provide additional insights into the relationship between awareness, perception, and behavior. For example, research conducted in developed economies indicates higher levels of cybersecurity awareness and more consistent adoption of risk mitigation strategies. However, even in these contexts, human factors continue to pose challenges. This suggests that while economic and technological development influences cybersecurity preparedness, behavioral aspects remain universally significant.

The literature also underscores the importance of targeted awareness programs. Studies have shown that generic awareness campaigns may not be effective in addressing the diverse needs of digital banking users. Instead, customized interventions that consider demographic factors such as age, education, and location are more likely to yield positive outcomes. For instance, interactive training sessions and localized communication strategies have been found to improve user engagement and retention of cybersecurity knowledge. Despite the growing body of research, certain gaps remain. Many studies have focused on either awareness or behavior in isolation, without examining the

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 162, Feb 2026
Paper ID: RRJ201489
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-162-february-2026/RRJ201489

interrelationships between awareness, threat perception, and risk mitigation. Additionally, there is limited empirical research that integrates these dimensions within a single analytical framework, particularly in the Indian context. This highlights the need for comprehensive studies that adopt a holistic approach to understanding cybersecurity in digital banking.

Objectives of the Research Study

1. To examine the level of customer awareness regarding cybersecurity risks in digital banking in India.
2. To analyze customers' perception of various cybersecurity threats associated with digital banking services.
3. To evaluate the adoption of risk mitigation strategies by digital banking users.
4. To investigate the relationship between customer awareness, threat perception, and risk mitigation behavior in digital banking.

Hypotheses of the Present Research Study

1. There is a significant relationship between customer awareness and the adoption of risk mitigation strategies in digital banking.
2. Customer awareness has a positive and significant impact on threat perception in digital banking.
3. Threat perception significantly influences the adoption of risk mitigation strategies among digital banking users.
4. Customer awareness and threat perception jointly have a significant effect on risk mitigation strategies in digital banking.

Variables of the Research Study

The present study examines cybersecurity risks in digital banking by focusing on three key constructs: customer awareness, threat perception, and risk mitigation strategies. These variables are classified as independent, dependent, and mediating variables, along with relevant demographic variables.

A. Independent Variable - Customer Awareness
B. Mediating Variable - Threat Perception
C. Dependent Variable - Risk Mitigation Strategies
D. Control / Demographic Variables – Gender, Age Group, Education Level, Location (Urban / Semi-Urban), Digital Banking Experience

These demographic variables are used to examine variations in awareness, perception, and behavior across different user groups.

Data Analysis and Findings

Demographic Profile of Respondents

Table 4.1 presents the demographic characteristics of the 350 survey respondents.

Characteristic	Category	Frequency	Percentage (%)
Gender	Male	198	56.6%
	Female	152	43.4%
Age Group	18–25 years	89	25.4%
	26–35 years	112	32.0%

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 162, Feb 2026
Paper ID: RRJ201489
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-162-february-2026/RRJ201489

	36–50 years	98	28.0%
	51 years and above	51	14.6%
Education	Up to Higher Secondary	62	17.7%
	Graduate	148	42.3%
	Post-Graduate and above	140	40.0%
Location	Urban	218	62.3%
	Semi-Urban	132	37.7%
Digital Banking Experience	Less than 1 year	48	13.7%
	1–3 years	96	27.4%
	3–5 years	118	33.7%
	More than 5 years	88	25.1%

Table 4.1: Demographic Profile of Respondents (N = 350)

The majority of the sample is urban (62.3%), male (56.6%), and has a graduate degree (42.3%). According to the demographic profile of active digital banking users in India, the largest age cohort (32.0%) is in the 26–35 age range. A sizable percentage (58.8%) reported having used digital banking for more than three years, which offers a solid foundation for evaluating recognized behavioral trends.

Cybersecurity Awareness Levels

Table 4.2 presents mean awareness scores across key cybersecurity knowledge domains.

Cybersecurity Knowledge Domain	Mean Score (out of 5)	Standard Deviation	Awareness Level
Recognition of phishing emails/messages	3.82	0.91	Moderate–High
Knowledge of two-factor authentication (2FA)	3.61	0.98	Moderate
Understanding of password best practices	3.44	1.02	Moderate
Awareness of SIM swap fraud	2.71	1.14	Low–Moderate
Knowledge of UPI-based social engineering	2.58	1.18	Low
Understanding of malware/spyware risks	3.12	1.09	Moderate
Awareness of data breach implications	2.94	1.11	Moderate
Knowledge of safe public Wi-Fi practices	3.23	1.06	Moderate
Overall Awareness Score	3.18	0.87	Moderate

Table 4.2: Cybersecurity Awareness Scores by Knowledge Domain (N = 350)

The sample's overall mean cybersecurity awareness score of 3.18 out of 5 shows a modest level of understanding. Phishing recognition (3.82) and two-factor authentication (3.61) have the highest awareness, which is indicative of the widespread institutional and media coverage of these issues. However, given that these are two of the most common and financially harmful cyber crime typologies in India's contemporary digital banking ecosystem, awareness of SIM swap fraud (2.71) and UPI-based social engineering (2.58) is noticeably low, indicating severe knowledge gaps (RBI, 2023).

ANOVA analysis shows statistically significant variations in awareness scores between age groups ($F = 14.32$, $p < 0.001$), with respondents between the ages of 18 and 35 showing considerably higher awareness than those over 51 (mean difference = 0.74, $p < 0.001$). Another important predictor of

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 162, Feb 2026
Paper ID: RRJ201489
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-162-february-2026/RRJ201489

awareness is education level ($F = 18.67$, $p < 0.001$), with post-graduate respondents scoring much higher than those with only secondary education (mean difference = 0.89, $p < 0.001$).

Threat Perception Analysis

Table 4.3 summarises respondents' threat perception scores across major cybersecurity threat categories.

Threat Type	Perceived Likelihood (1–5)	Perceived Severity (1–5)	Composite Threat Score
Phishing / Vishing / Smishing	3.94	4.21	4.08
Account Takeover / Unauthorised Access	3.67	4.45	4.06
SIM Swap Fraud	3.12	4.38	3.75
UPI / Payment App Fraud	3.88	4.29	4.09
Data Breach / Identity Theft	3.41	4.52	3.97
Malware / Ransomware	3.05	4.18	3.62
Online Loan / Investment Scams	3.76	3.98	3.87
Overall Threat Perception Score	3.55	4.29	3.92

Table 4.3: Threat Perception by Cybersecurity Risk Category (N = 350)

A somewhat high level of threat perception among respondents is indicated by the overall composite threat perception score of 3.92. Notably, across all threat categories, perceived severity scores (mean = 4.29) consistently outperform perceived likelihood scores (mean = 3.55). This pattern is consistent with the optimism bias reported in the risk perception literature, where people recognize the seriousness of threats but underestimate their own vulnerability to them.

Due to their high relevance in media coverage and institutional messaging, phishing (4.08) and UPI and payment app fraud (4.09) receive the highest composite threat rankings. Despite having the potential to have a significant financial impact, malware and ransomware (3.62) obtain the lowest composite score, indicating that these technically complicated dangers are less cognitively accessible to lay banking clients.

Risk Mitigation Behaviour

Table 4.4 presents the frequency of risk mitigation behaviours adopted by respondents.

Risk Mitigation Behaviour	Always (%)	Often (%)	Sometimes (%)	Rarely/Never (%)	Mean Score
Use of strong/unique passwords	38.3%	29.1%	21.4%	11.2%	3.94
Enable two-factor authentication	42.6%	27.4%	18.6%	11.4%	4.01
Avoid clicking suspicious links	51.4%	24.9%	15.1%	8.6%	4.19
Regular account statement monitoring	28.6%	31.1%	24.9%	15.4%	3.73
Avoid public Wi-Fi for banking	34.9%	26.0%	22.6%	16.5%	3.79
Update banking apps regularly	29.7%	28.3%	26.3%	15.7%	3.72
Verify caller identity before sharing OTP	58.3%	21.7%	12.6%	7.4%	4.31
Report suspicious transactions promptly	24.3%	26.6%	28.0%	21.1%	3.54
Use of VPN on public	12.6%	18.3%	27.4%	41.7%	3.01

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 162, Feb 2026
Paper ID: RRJ201489
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-162-february-2026/RRJ201489

networks					
Overall Mitigation Behaviour Score					3.80

Table 4.4: Frequency of Risk Mitigation Behaviours (N = 350)

The respondents' overall mean risk mitigation behavior score of 3.80 indicates a fairly active protective posture. OTP sharing vigilance is the most frequently practiced behavior (mean = 4.31), which reflects the significant institutional communication about this particular hazard. Utilizing two-factor authentication (4.01) and avoiding dubious links (4.19) both receive comparatively good scores. The poorest mitigation behaviors, on the other hand, are VPN use on public networks (3.01) and timely reporting of suspicious transactions (3.54), suggesting significant gaps in the adoption of technically complex and procedurally demanding protective measures.

Regression Analysis: Predictors of Risk Mitigation Behaviour

Using cybersecurity knowledge and threat perception as the main independent variables and demographic traits as controls, multiple regression analysis was used to investigate the predictors of risk mitigation behavior. The regression results are shown in Table 4.5.

Predictor Variable	Beta (β)	Std. Error	t-value	p-value	Significance
Cybersecurity Awareness	0.412	0.063	6.54	< 0.001	***
Threat Perception (Severity)	0.287	0.071	4.04	< 0.001	***
Threat Perception (Likelihood)	0.193	0.068	2.84	0.005	**
Age (reverse coded)	-0.168	0.058	-2.90	0.004	**
Education Level	0.214	0.072	2.97	0.003	**
Digital Banking Experience	0.176	0.064	2.75	0.006	**
Gender (Male = 1)	0.091	0.061	1.49	0.137	ns
Location (Urban = 1)	0.142	0.065	2.18	0.030	*

Table 4.5: Multiple Regression Analysis Predictors of Risk Mitigation Behaviour $R^2 = 0.61$; Adjusted $R^2 = 0.60$; $F(8, 341) = 66.4$, $p < 0.001$ *** $p < 0.001$; ** $p < 0.01$; * $p < 0.05$; ns = not significant

The regression model explains 61% of the variance in risk mitigation behavior (R2 = 0.61) and is statistically significant (F = 66.4, p < 0.001). The most potent predictor of self-protective behavior in digital banking scenarios is cybersecurity awareness (β = 0.412, p < 0.001). According to PMT predictions, perceived severity (β = 0.287, p < 0.001) and perceived likelihood (β = 0.193, p < 0.01) are both significant positive predictors. Even after adjusting for awareness and threat perception, age has a significant negative effect (β = -0.168, p < 0.01), suggesting that protective action in older age groups is hampered by factors other than knowledge and motivation. Significant positive factors include education level (β = 0.214, p < 0.01), digital banking experience (β = 0.176, p < 0.01), and urban location (β = 0.142, p < 0.05). After adjusting for other factors, gender does not show up as a significant predictor.

Findings

The empirical analysis yields the following principal findings:

→ Overall, Indian digital banking consumers have a moderate level of cybersecurity awareness (mean = 3.18/5), with notable gaps in knowledge of new threat types, especially SIM swap fraud (2.71) and UPI-based social engineering (2.58), which are the two categories of cybercrime that are currently expanding the fastest in India's digital payments market.

→ Perceived threat severity (4.29) consistently surpasses perceived personal vulnerability (3.55) across all threat types, indicating a fairly strong threat perception (mean composite = 3.92/5). The adoption of comprehensive protective behavior is hampered by this bias, which is a structural cognitive barrier.

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 162, Feb 2026
Paper ID: RRJ201489
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-162-february-2026/RRJ201489

- Risk mitigation behavior is moderate (mean = 3.80/5), with strong adoption of socially reinforced behaviors like link avoidance and OTP vigilance, but notable under-acceptance of technically difficult measures like timely transaction reporting (3.54) and VPN usage (3.01).
- The largest predictor of risk mitigation behavior is cybersecurity awareness ($\beta = 0.412$, $p < 0.001$), followed by perceived severity ($\beta = 0.287$) and perceived likelihood ($\beta = 0.193$). This indicates that Protection Motivation Theory is applicable to the Indian digital banking context.
- Age is a significant negative predictor of mitigation behavior ($\beta = -0.168$, $p < 0.01$), with older respondents (51+ years) showing significantly lower awareness scores and mitigation behavior frequencies than younger cohorts. This suggests that targeted cybersecurity education interventions should target this demographic.
- Both awareness and protective behavior are strongly positively predicted by education level and experience with digital banking, indicating that ongoing digital involvement gradually increases cybersecurity competency.
- Due to differences in access to institutional literacy programs, technically advanced device environments, and cybersecurity awareness information, urban respondents display much higher mitigation behavior than semi-urban respondents.

Conclusion

The present study provides a comprehensive empirical examination of cybersecurity risks in digital banking in India, with particular emphasis on customer awareness, threat perception, and risk mitigation strategies. In an era marked by rapid digital transformation, the findings underscore that while digital banking has significantly enhanced financial accessibility and convenience, it has also introduced critical vulnerabilities that demand immediate and sustained attention. The study reveals that customer awareness plays a foundational role in shaping cybersecurity behavior. Although a considerable proportion of respondents demonstrate basic knowledge of digital banking operations, gaps persist in their understanding of advanced cyber threats such as phishing, malware, and identity theft. These gaps are more pronounced among older users, less-educated individuals, and those residing in semi-urban areas. This indicates that digital inclusion without corresponding cybersecurity literacy may expose users to heightened risks, thereby undermining the benefits of digital financial services.

The analysis highlights that threat perception significantly influences user behavior. Respondents who exhibit a higher perception of cybersecurity risks are more likely to adopt protective measures such as strong passwords, two-factor authentication, and cautious online practices. However, the study also identifies a mismatch between perceived and actual risks among certain user groups, suggesting that awareness alone is insufficient unless it translates into realistic threat assessment. This finding reinforces the importance of not only educating users about cyber risks but also enabling them to accurately evaluate and respond to such threats. The adoption of risk mitigation strategies among users, although present, remains inconsistent. While widely promoted measures such as OTP-based authentication are commonly used, more proactive practices such as regular monitoring of accounts, updating security settings, and avoiding unsecured networks are not uniformly followed. This inconsistency reflects both behavioral inertia and usability challenges associated with digital security mechanisms. It also emphasizes the need for designing user-friendly and accessible security systems that encourage consistent compliance.

The study also highlights the critical role of financial institutions and regulatory bodies in strengthening cybersecurity frameworks. Banks and fintech companies must go beyond technical

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 162, Feb 2026
Paper ID: RRJ201489
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-162-february-2026/RRJ201489

safeguards and actively engage in customer education through targeted awareness campaigns, especially for vulnerable segments. Regulatory authorities should continue to refine policies related to data protection, fraud prevention, and customer liability, ensuring that they remain adaptive to evolving cyber threats. Cybersecurity in digital banking is not merely a technological issue but a multidimensional challenge involving human behavior, institutional responsibility, and regulatory oversight. The interplay between awareness, threat perception, and risk mitigation is central to building a secure digital financial ecosystem. Therefore, a collaborative approach involving users, financial institutions, and policymakers is essential to enhance resilience against cyber threats. The study contributes valuable insights for developing effective strategies to promote safe digital banking practices and supports the broader goal of sustainable and secure digital financial inclusion in India.

REFERENCES

Bose, I., & Leung, A. C. M. (2014). Do phishing alerts impact global corporations? A firm value analysis. Decision Support Systems, 64, 67–78.

Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment (IMF Working Paper WP/18/143). International Monetary Fund.

CERT-In. (2024). Annual report 2023: Indian Computer Emergency Response Team. Ministry of Electronics and Information Technology, Government of India.

Dlamini, M. T., Eloff, J. H. P., & Eloff, M. M. (2009). Information security: The moving target. Computers & Security, 28(3–4), 189–198.

Liang, H., & Xue, Y. (2010). Understanding security behaviors in personal computer usage: A threat avoidance perspective. Journal of the Association for Information Systems, 11(7), 394–413.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. Journal of Experimental Social Psychology, 19(5), 469–479.

Malhotra, P., & Singh, B. (2019). Determinants of mobile banking adoption in India: An empirical analysis. International Journal of Bank Marketing, 38(3), 522–545.

National Centre for Financial Education (NCFE). (2023). National financial literacy and inclusion survey 2022–23. NCFE India.

National Payments Corporation of India (NPCI). (2024). UPI product statistics: Annual report 2023–24. NPCI.

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems, 50(3), 559–569.

Poonia, A. S., Chauhan, R., & Bhatt, A. (2021). Cyber security awareness among mobile banking users in India: An empirical analysis. Journal of Information Security and Applications, 58, 102774.

ISSN: 2321-4708
RESEARCH REVIEW
The Academic Research Issue
Open Access, Peer-Reviewed & Refereed Journal
An International Multidisciplinary Journal
Vol.1, Issue: 162, Feb 2026
Paper ID: RRJ201489
www.researchreviewonline.com
Publishing URL: https://www.researchreviewonline.com/issues/volume-1-issue-162-february-2026/RRJ201489

Reserve Bank of India (RBI). (2022). Report on trend and progress of banking in India 2021–22. RBI Publications.

Reserve Bank of India (RBI). (2023). Annual report 2022–23. Reserve Bank of India.

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. The Journal of Psychology, 91(1), 93–114.

Shey, H. (2012). Understanding the state of data security and privacy: A review of enterprise security practices. Forrester Research.

Singh, S., & Pandey, S. K. (2020). Cyber threats and cyber frauds in banking sector of India: A review. International Journal of Advanced Science and Technology, 29(5), 4781–4791.

Sood, A. K., & Enbody, R. J. (2013). Targeted cyberattacks: A superset of advanced persistent threats. IEEE Security & Privacy, 11(1), 54–61.

Vishwanath, A., Herath, T., Chen, R., Wang, J., & Rao, H. R. (2011). Why do people get phished? Testing individual differences in phishing vulnerability within an integrated, information processing model. Decision Support Systems, 51(3), 576–586.

Workman, M. (2007). Gaining access with social engineering: An empirical study of the threat. Information Systems Security, 16(6), 315–331.

Yoon, C. (2018). Extending the TAM for a World Wide Web context. Information & Management, 55(4), 448–458.