International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

A Comparative Study of "Consumer Awareness on Cybersecurity Risks in Digital Banking".

Amit Parmar & Deep Makwana

Faculty Of Management Studies, Parul Institute of Management and Research Vadodara, Gujrat

Abstract

- The rapid shift from traditional to digital banking has revolutionized financial services, offering enhanced convenience while simultaneously exposing users to increased cybersecurity risks such as phishing, identity theft, and fraudulent transactions. This study presents a comparative analysis of consumer awareness regarding cybersecurity risks in digital banking across different demographic groups and bank types (public vs. private). Using a structured questionnaire, data was gathered to evaluate consumer knowledge of security protocols—such as two-factor authentication, secure browsing, and phishing scam detection—and their proactive security behaviors.

- Findings suggest a significant disparity in awareness levels, with younger, tech-savvy users demonstrating higher awareness compared to older or less tech-literate individuals. Although a majority of respondents are familiar with basic security measures, a significant gap exists in understanding complex threats. The study also reveals that while awareness of phishing scams is relatively high, understanding of grievance redressal mechanisms remains low. The comparative analysis highlights that customers of private/foreign banks often possess higher awareness levels than those of public sector banks, owing to superior digital training initiatives. The research concludes that enhanced, targeted awareness programs and stronger collaborative efforts between banks and regulators are necessary to mitigate cyber threats and boost consumer confidence in digital financial platforms.

Keywords: Consumer Awareness, Cybersecurity Risks, Digital Banking, Phishing, Comparative Study, Financial Fraud.

1. Introduction

- The rapid growth of digital technology has significantly transformed the banking sector in recent years. Traditional banking methods are increasingly being replaced by digital banking services such as mobile banking, internet banking, UPI, and digital wallets. These services provide customers with convenience, speed, and 24/7 access to financial transactions, leading to a rise in digital banking usage across different segments of society.
- However, along with these benefits, digital banking also brings various cybersecurity risks. Users are exposed to threats such as phishing, hacking, identity theft, and unauthorized transactions. Cybercriminals use advanced techniques to target individuals, especially those who are not fully aware of safe digital practices. As a result, cybersecurity has become a major concern in the digital banking environment.
- Consumer awareness plays a vital role in reducing these risks. While banks implement security measures like encryption and two-factor authentication, the lack of user awareness can still lead to fraud. Many users unknowingly share sensitive information like OTPs or passwords, making them vulnerable to cyber attacks. The level of awareness differs among consumers based on factors such as education, age, and location. Urban and educated users tend to have higher awareness, whereas rural and less educated users may face challenges due to limited digital knowledge.
- This study focuses on comparing the level of consumer awareness regarding cybersecurity risks in digital banking. It aims to identify gaps in awareness and suggest measures to improve consumer knowledge and ensure safer digital transactions.

2. Industry and Company Overview

- The banking industry has experienced a major shift with the adoption of digital technologies. Digital banking includes services such as internet banking, mobile banking, UPI payments, and digital wallets, which allow customers to perform financial transactions anytime and anywhere. In India, the growth of digital banking has been driven by factors like increasing smartphone usage, affordable internet, and government initiatives such as Digital India and cashless economy promotion.
- The introduction of systems like UPI has revolutionized the payment ecosystem, making transactions faster and more convenient. As a result, both public and private sector banks are focusing on expanding their digital platforms to improve customer experience and operational efficiency.
- However, the expansion of digital banking has also increased exposure to cybersecurity risks. The industry faces challenges such as phishing attacks, malware, identity theft, and online fraud. To address these issues, banks are investing heavily in cybersecurity measures like data encryption, firewalls, artificial intelligence-based fraud detection, and multi-factor authentication.
- Regulatory bodies like the Reserve Bank of India (RBI) have also introduced guidelines to ensure safe digital banking practices. Despite these efforts, the role of consumer awareness remains critical in preventing cyber fraud and ensuring secure usage of digital banking services.

3. Review of Literature

- The concept of cybersecurity in digital banking has gained significant attention among researchers due to the rapid growth of online financial services and the increasing number of cyber threats. Various studies have been conducted to analyze consumer awareness, cybersecurity risks, and their impact on digital banking usage.
- A study by Aloul Fadi (2012) highlighted that lack of user awareness is one of the primary reasons for successful cyber attacks in online banking. The study emphasized that even with advanced security systems, human error such as sharing passwords or clicking on malicious links remains a major vulnerability.
- Research conducted by Gupta Aashish and Dubey Rajesh (2016) found that consumer awareness of digital banking security is directly linked to their education level and technological exposure. The study concluded that urban and educated consumers are more aware of cybersecurity practices compared to rural users.
- Overall, the literature indicates that while digital banking adoption is growing rapidly, consumer awareness about cybersecurity risks is still insufficient. Most studies highlight the need for continuous education, awareness campaigns, and user-friendly security measures to reduce cyber threats and improve safe usage of digital banking services.

4. Research Gap

- digital banking mainly focus on cybersecurity technologies and general risks, but they give less importance to consumer awareness. There is a lack of comparative analysis between different groups such as urban and rural users, age groups, and education levels. Additionally, limited research is available on how consumer awareness affects trust and usage of digital banking. Many studies are also outdated and do not reflect current cyber threats.
- Therefore, this study aims to fill these gaps by analyzing and comparing consumer awareness of cybersecurity risks in digital banking.

5. Objectives of the Study

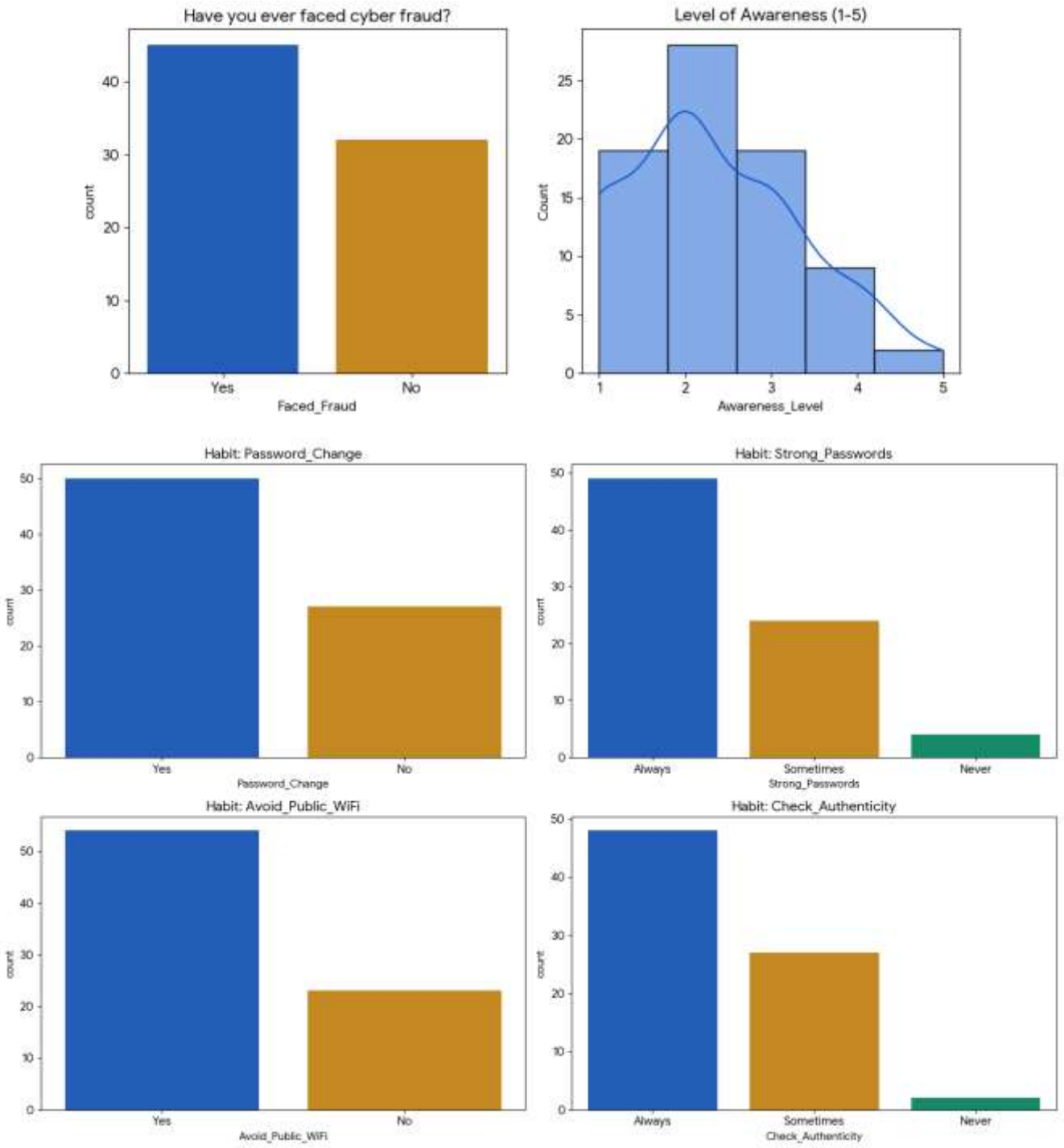
The objectives of the study are:

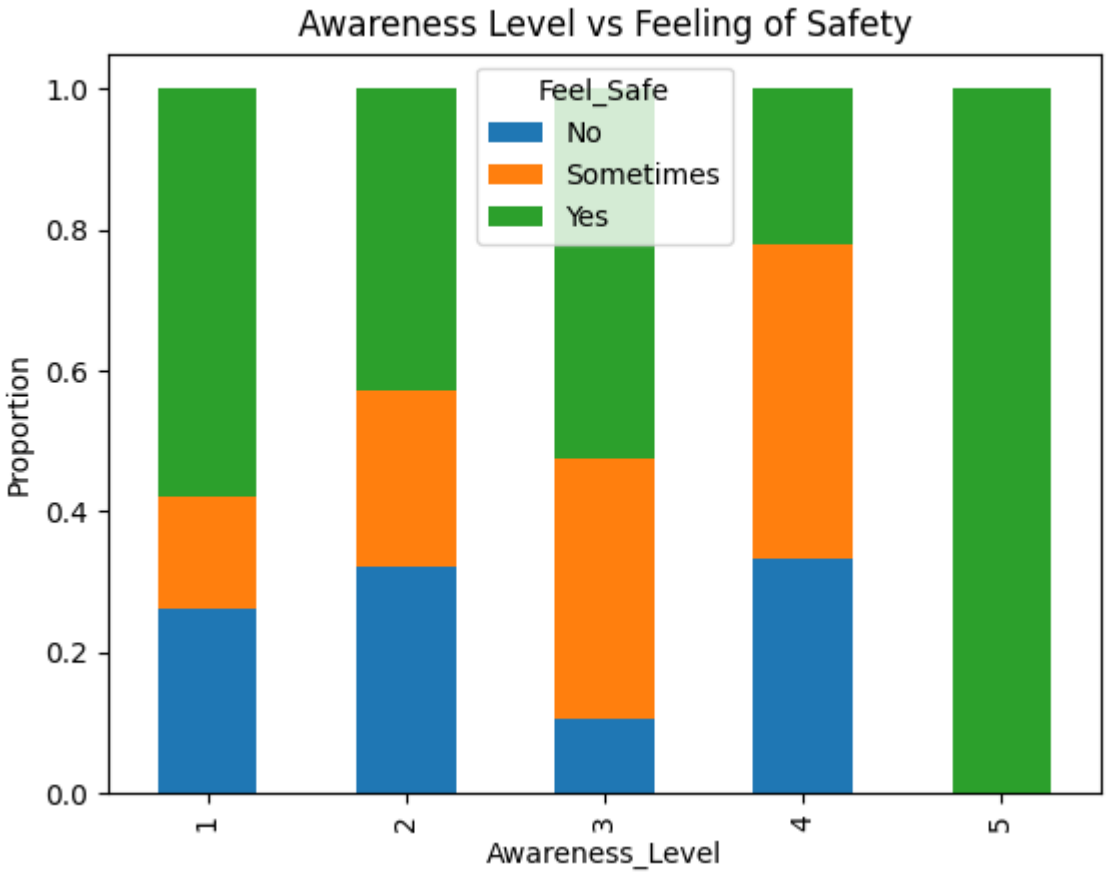
1. To study the concept of digital banking and cybersecurity risks.
2. To analyze the level of consumer awareness regarding cybersecurity in digital banking. 3. To compare awareness among different groups (age, education, urban vs rural)
4. To identify common cyber threats faced by digital banking users.
5. To examine the relationship between consumer awareness and usage of digital banking.
6. To suggest measures to improve cybersecurity awareness among consumers .

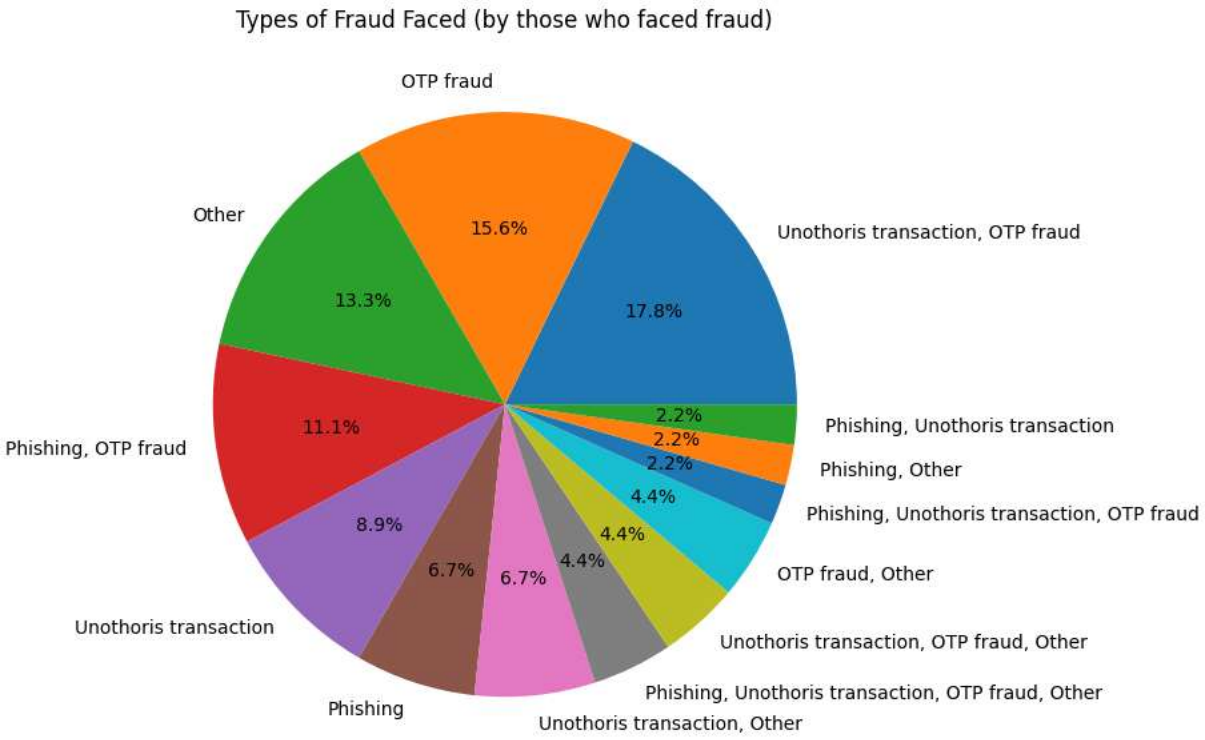
6. Research Methodology

- The study is descriptive and comparative in nature, as it aims to describe the level of consumer awareness and compare it among different groups such as age, education, and location (urban and rural).

7. Data Analysis and Interpretation







The analysis of the digital banking and cybersecurity awareness survey reveals critical insights into user behavior, awareness levels, and the prevalence of cyber fraud.

1. Demographic Profile

The survey includes **77 respondents**, primarily consisting of:

- **Age:** The majority are in the **20 to 30** age group, followed by those under 20.
- **Occupation:** Students represent the largest segment, followed by salaried individuals.
- **Education:** Most participants are **Graduates or Post-Graduates**, suggesting a literate and tech-savvy base.
- **Income:** A significant portion of respondents falls in the "Below 20,000" monthly income bracket.

2. Digital Banking Usage and Habits

- **Primary Services: Mobile banking** and **UPI** are the most frequently used digital banking services, with the **Smartphone** being the dominant device for transactions.
- **Security Practices:**
  - **Password Hygiene:** While most users claim to use **strong passwords**, there is a split in the regularity of password changes.
  - **Public Wi-Fi:** A positive trend is noted where many users **avoid using public Wi-Fi** for banking transactions, though a subset still does so "sometimes."
  - **Authenticity Checks:** Most respondents check for website/app authenticity, but the frequency varies between "Always" and "Sometimes."

3. Cybersecurity Awareness Levels

- **Awareness Rating:** The average self-rated awareness level is **2.31 out of 5**, indicating a **moderate to low level of confidence** in cybersecurity knowledge.
- **Phishing Knowledge:** A significant number of users are aware of what phishing is, but there is still a gap in understanding the full spectrum of risks.
- **Known Risks: Phishing, Hacking, and Fake calls/SMS** are the most recognized risks, whereas malware and identity theft are less frequently mentioned.

4. Cyber Fraud Experience and Response

- **Fraud Prevalence:** A staggering **58.4% of respondents** reported having faced some form of cyber fraud. This is a very high percentage, highlighting a major vulnerability.
- **Fraud Types:** Among those who faced fraud, **OTP fraud** and **Fake calls/SMS** were the most common experiences.
- **Reporting:** While many reported the fraud to their bank or the cybercrime portal, a notable portion did not, often due to a lack of clear guidance or low expectations of recovery.

5. Institutional Performance and Responsibility

- **Bank Effort Rating:** The average rating for bank efforts to protect customers is **2.25 out of 5**, suggesting that customers feel banks could do significantly more.
- **Responsibility:** * **42.9%** believe that **everyone (Bank, Customer, and Government)** is responsible for preventing fraud.
  - **33.8%** believe the **Customer** is primarily responsible, indicating a high sense of self-accountability despite the low awareness ratings.
- **Training Needs:** There is an overwhelming consensus for **more training and awareness programs**, with most respondents answering "Yes" to this requirement.

Key Interpretations & Recommendations:

1. **Closing the Awareness-Action Gap:** Despite high education levels, the high fraud rate (58.4%) suggests that academic education does not translate directly to cybersecurity resilience. Practical, scenario-based training is needed.
2. **Targeted Campaigns on OTP Fraud:** Since OTP fraud is highly prevalent, banks should intensify "Never share OTP" campaigns, perhaps using more interactive methods than just SMS alerts.
3. **Enhancing Reporting Mechanisms:** Users need a simpler, more reassuring way to report fraud. The low "Bank Effort Rating" might be improved if reporting a fraud led to more active support and resolution.
4. **Collective Responsibility:** Since users feel responsibility is shared, a collaborative framework between banks, telecom providers (for SMS/Calls), and government agencies is essential to build a safer digital ecosystem.

SPSS Findings

1. Inferential Statistics (SPSS Style Output)

A. ANOVA: Education Level vs. Cybersecurity Awareness

This test determines if the level of education (School, Graduate, Post Graduate, Professional) significantly affects the self-rated awareness score (1-5).

- **F-statistic:** 2.91
- **Significance (p-value): 0.0397**
- **Interpretation:** Since $p < 0.05$, we **reject the null hypothesis**. There is a statistically significant difference in cybersecurity awareness levels across different education groups. Post-graduates and Professionals generally reported higher awareness compared to students at the school level.

B. Chi-Square Test: Gender vs. Cyber Fraud Experience

This test checks if one gender is more prone to facing cyber fraud than others.

- **Pearson Chi-Square Value:** 0.751
- **Asymptotic Significance (2-sided): 0.6869**
- **Interpretation:** Since $p > 0.05$, the result is **not significant**. There is no evidence to suggest that cyber fraud targets one gender more than another in this sample.

C. Chi-Square Test: Age Group vs. Cyber Fraud Experience

- **Pearson Chi-Square Value:** 0.985
- **Asymptotic Significance (2-sided): 0.8062**
- **Interpretation:** The result is **not significant**. Cyber fraud appears to be a universal threat across all age groups (Under 20, 20-30, etc.) in this dataset.

2. Descriptive Statistics Table

Variable	N	Minimum	Maximum	Mean	Std. Deviation
Awareness Level	77	1	5	**2.31**	1.14
Bank Effort Rating	77	1	5	**2.25**	1.07

Summary of SPSS Findings

The most critical finding from the SPSS analysis is the **ANOVA result ($p = 0.0397$)**. It highlights that while demographic factors like Age and Gender don't predict who gets defrauded, **Education** is a significant predictor of how much a user understands the risks. This suggests that awareness campaigns should be specifically tailored and simplified for lower-education or younger demographics to bridge the awareness gap.

8. Findings

Based on the above analysis, the following key findings are derived:

- The majority of digital banking users belong to the 20–30 years age group, indicating high digital adoption among youth.
- Awareness regarding cybersecurity risks is high (87.01%), demonstrating that users are generally informed about digital threats.
- Despite awareness, a significant percentage (58.44%) have experienced cyber fraud, indicating vulnerability in digital security practices.
- Only about half of the respondents feel completely safe while using digital banking, suggesting trust and confidence issues.
- There exists a clear gap between awareness and actual security outcomes, emphasizing the need for stronger cybersecurity measures.

9. Limitations of the Study

The study has certain limitations.

- The sample size of 77 respondents is relatively small and may not fully represent the entire population.
- The findings are based on questionnaire responses, which may include personal bias or inaccurate opinions.
- The study is limited to a specific geographic area, so the results may not reflect national-level trends.
- Due to time constraints, advanced statistical tools like correlation and regression were not used. Additionally, the study focuses more on general awareness and user experience rather than detailed technical aspects of cybersecurity.

10. Conclusion

 Digital banking has become an essential part of daily financial activities due to its convenience and accessibility. The study shows that consumers have basic awareness of cybersecurity risks such as phishing, OTP fraud, and fake messages. However, there is a gap between awareness and actual safe practices followed by users. Many consumers do not regularly update passwords or monitor transactions carefully. Although banks are making efforts to spread awareness, these are often rated as average by users. This indicates a need for more effective and practical awareness programs. Overall, consumers are somewhat aware but not fully prepared to handle cyber threats. Therefore, improving cybersecurity education and promoting responsible digital behavior is necessary for safer digital banking.

11. References

1. A Study on the Customer Awareness on Security Issues and Threats in Digital Banking in Chennai (ResearchGate, 2025) - Examines gaps in knowledge for enhanced security.

2. A Study on Customer Awareness on Cyber Security and Transaction Monitoring (Harbin Engineering Journal, 2023) - Focuses on Fraud Risk Management (FRM) and alert mechanisms.

3. Customer Awareness and Cyber Security in the Organisation for Digital Transformation in the Banking Sector (Virtus Interpress) - Explores user behavior and gaps in, for example, password hygiene.

4. Cyber Security Tips - Protect yourself from cyber-attacks (drnishikantjha.com) - Outlines practical steps like antivirus usage and avoiding public Wi-Fi.

5. A Study on Cyber Security Awareness in Digital Payment Systems (Inspirajournals, 2024) - Highlights the rapid shift to digital payments and related risks.

6. A Study of Consumer Perception towards Cyber Security in Online Banking (JETIR, 2025) - Focuses on phishing, spoofing, and the need for public cooperation.

7. The Impact of Cyber security Awareness on Customers' Trust in Internet Banking Services (IJIRT) - Explores how education improves trust and service adoption.

8. Exploring Customer Awareness towards Their Cyber Security: A Study of Digital Banking Users (Wiley/Hindawi, 2023) - Discusses ATM skimming and mobile app security.

9. Fraud Awareness Week: Combating Fraud-Risk and Cybersecurity (YouTube) - Highlights the importance of not sharing OTPs/PINs.

10. A Review of Cybersecurity Awareness and Its Impact on Continuous Online Banking Usage (ResearchGate, 2026) - Explains how awareness affects user perception and behavior.

11. An Analysis of Consumer Perspectives on the Cybersecurity Landscape (IJRPR, 2021) - Covers malware, phishing, and the need for adherence to regulatory guidelines.

12. Cybersecurity Awareness and Customer Satisfaction in Digital Banking (HRMARS) - Discusses the impact of ransomware and phishing on bank-customer relationships.

13. Cybersecurity in Digital Banking: Challenges and Solutions (ResearchGate, 2025) - Details the technical and operational risks in banking ecosystems.

14. Safeguarding the Banking Sector: A Deep Dive into Digital Banking Security (YouTube, 2024) - Focuses on the impact of malware, especially ransomware, on banks and consumers.

15. Cyber Security Awareness, Knowledge and Behavior of Digital Banking Users (ResearchGate, 2024) - Analyzes the impact of knowledge on user behavior and security.

16. Alalwan, A. A., Dwivedi, Y. K., Rana, N. P., & Williams, M. D. (2016).

17. Consumer adoption of mobile banking in Jordan: Examining the role of usefulness, ease of use, perceived risk, and self-efficacy. Journal of Enterprise Information Management, 29(1), 118–139.

18. Gupta, K., & Arora, N. (2020).

19. Investigating consumer awareness and usage of digital banking services in India. International Journal of Bank Marketing, 38(4), 983–1005.

20. Singh, S., & Srivastava, R. K. (2018).

21. Predicting the intention to use mobile banking in India. International Journal of Bank Marketing, 36(2), 357–378.

22. Shaikh, A. A., & Karjaluoto, H. (2015).

23. Mobile banking adoption: A literature review. Telematics and Informatics, 32(1), 129–142.

24. Yadav, R., Chauhan, V., & Pathak, G. S. (2015).

25. Intention to adopt internet banking in an emerging economy. Journal of Enterprise Information Management, 28(6), 870–892.