InSight Bulletin: A Multidisciplinary Interlink International Research Journal
Peer Reviewed International, Open Access Journal.
ISSN : 3065-7857 / Website: https://ibrj.us / Volume-3, Issue-1 / January - 2026

Original Article

An Empirical Study on Cybersecurity Awareness of UPI Users

Vinayak E. Midgule[1], Dr. Archana Tukaram Bhise[2]
[1,2]Asst. Prof., Shri Jagdishprasad Jhabarmal Tibrewala University (SJJTU)

Manuscript ID:
IBMIIRJ -2026-030128

Submitted: 08 Dec. 2025

Revised: 12 Dec. 2025

Accepted: 07 Jan. 2026

Published: 31 Jan. 2026

ISSN: 3065-7857

Volume-3

Issue-1

Pp. 144-148

January 2026

Correspondence Address:
Vinayak E. Midgule
Asst.Prof., Shri Jagdishprasad Jhabarmal Tibrewala University (SJJTU)
Email: vinayak.midgule@rediffmail.com

OPEN ACCESS

Quick Response Code:

Web. https://ibrj.us

DOI: 10.5281/zenodo.18953971

DOI Link:
https://doi.org/10.5281/zenodo.18953971

Abstract

The rapid growth of digital payment systems in India, particularly the Unified Payments Interface (UPI), has transformed the way financial transactions are conducted. While UPI offers convenience, speed, and accessibility, it has also increased users' exposure to cyber threats such as phishing, social engineering attacks, fake QR codes, and unauthorized access. This empirical study aims to assess the level of cybersecurity awareness among UPI users, analyze their security practices, and examine the relationship between awareness and vulnerability to cyber fraud. Primary data was collected through a structured questionnaire from 200 UPI users across different demographic groups. The findings reveal moderate awareness levels but poor security practices among users, highlighting the urgent need for targeted awareness programs and improved digital literacy initiatives.

Keywords: *UPI, Cybersecurity Awareness, Digital Payments, Cyber Fraud, User Behavior*

Introduction

The rapid advancement of digital technology has significantly transformed the financial services sector, leading to the widespread adoption of electronic payment systems across the globe. In India, one of the most notable innovations in this domain is the Unified Payments Interface (UPI), developed by the National Payments Corporation of India (NPCI). UPI enables instant, secure, and seamless fund transfers between bank accounts through mobile applications, making it one of the most popular digital payment platforms in the country. Its ease of use, low transaction cost, and interoperability across banks have contributed to its massive adoption among individuals, businesses, and government institutions.

Despite its numerous advantages, the exponential growth of UPI usage has also led to a corresponding increase in cybersecurity threats. Cybercriminals exploit user vulnerabilities through various techniques such as phishing, vishing, smishing, fake QR codes, malware attacks, and social engineering scams. These threats often target users' lack of awareness rather than technical flaws in the UPI system itself. As a result, many UPI users become victims of fraud due to unsafe practices such as sharing PINs or OTPs, clicking on malicious links, or trusting fraudulent payment requests.

Cybersecurity awareness plays a crucial role in ensuring the safe usage of UPI services. Awareness includes users' understanding of potential cyber threats, knowledge of secure transaction practices, and familiarity with reporting mechanisms in case of fraud. However, a significant portion of UPI users, especially first-time digital users, elderly individuals, and users from rural or semi-urban areas, lack adequate cybersecurity knowledge. This gap between widespread adoption and security awareness increases the risk of financial loss and undermines user confidence in digital payment systems.

An empirical study on cybersecurity awareness of UPI users is therefore essential to evaluate the current level of user awareness, identify gaps in knowledge and behavior, and assess how awareness influences vulnerability to cyber fraud. Such a study can provide valuable insights for policymakers, financial institutions, and technology providers to design effective awareness programs, strengthen user education initiatives, and enhance the overall security of the digital payment ecosystem. Understanding user behavior and awareness is a key step toward building a secure, inclusive, and resilient digital financial environment in India.

How to cite this article:
Midgule, V. E., & Bhise, A. T. (2026). An Empirical Study on Cybersecurity Awareness of UPI Users. InSight Bulletin: A Multidisciplinary Interlink International Research Journal, 3(1), 144–148. https://doi.org/10.5281/zenodo.18953971

Literature Review

This study focuses on evaluating the cybersecurity awareness of UPI users and understanding how awareness influences safe usage behavior. Balambal [1] This study examines the level of cybersecurity awareness and threat perception among users of digital payment systems, with particular emphasis on semi-urban regions in India. The author highlights that although digital payments such as UPI, mobile wallets, and internet banking have enhanced convenience and efficiency, they have simultaneously increased users' exposure to cyber threats including phishing, malware, identity theft, and data breaches. Using primary data collected through structured questionnaires, the study analyses user behaviour, security practices, and perception of online threats. The findings reveal a significant awareness gap among users, where many fail to adopt basic security measures such as strong password practices, software updates, and verification of digital platforms. The study concludes that technological safeguards alone are insufficient unless supported by strong user education and regulatory enforcement. It emphasizes the need for proactive awareness campaigns and user-centric security designs to strengthen the overall digital payment ecosystem.

Kavita & Yadav [2] This paper focuses on assessing cybersecurity awareness among users of digital payment systems in an academic environment. The study adopts a quantitative research approach using a self-structured questionnaire, with data analysed through correlation and regression techniques using SPSS. The findings indicate that although most respondents are educated and actively use digital payment services, their awareness of cyber threats and protective measures remains low. Educated users were found to make comparatively better security decisions, yet overall awareness regarding cyberattacks such as malware, phishing, and data breaches was inadequate. The study concludes that cybersecurity concerns continue to demotivate users from fully trusting digital financial services. The authors strongly recommend integrating cybersecurity education into institutional learning frameworks to enhance digital safety awareness.

Reddy & Swathi [3] This research addresses the growing incidence of UPI-related frauds in India by proposing an AI-based fraud detection and awareness framework. The study recognizes that UPI users are increasingly targeted by phishing links, QR code tampering, screen-sharing scams, and social engineering attacks. A mixed-method research design was employed, combining surveys from UPI users and interviews with banking and cybersecurity professionals. Based on the findings, the authors developed a conceptual framework where AI systems detect anomalous transaction patterns in real time while simultaneously alerting users through multilingual warnings and educational prompts. The study demonstrates that combining AI-driven detection with user education significantly enhances fraud prevention, builds trust, and promotes secure adoption of digital payments in India. Nair [4] This study explores cybersecurity awareness, perceived threats, and user perception among college students. The research is motivated by the increasing dependence on digital platforms for education and communication, which has amplified exposure to cyber risks. Using a questionnaire-based survey of students in Thiruvananthapuram district, the study finds that while students are frequent internet users, their cybersecurity awareness is weak. Even when basic knowledge exists, it is often insufficient to protect against real-world cyberattacks. The study highlights malware and online scams as the most common threats faced by students. It emphasizes the importance of continuous cybersecurity education and awareness programs to help young users navigate digital environments safely.

Khandal [5] This exploratory study investigates customer awareness, usage behaviour, and challenges related to UPI and mobile banking services in Delhi. Based on data collected from 300 respondents, the study analyses reasons for adopting digital banking over traditional banking methods. The findings reveal high awareness and adoption of UPI and mobile banking due to convenience, cost-effectiveness, and smartphone penetration. However, the study also identifies issues such as transaction failures, cybersecurity concerns, and limited technical knowledge among users. The author concludes that while UPI has become a preferred payment method, improving cybersecurity awareness and user support mechanisms is essential for sustained growth and trust. Wadkar & Mundhe [6] This paper examines the cybersecurity challenges associated with UPI payment frauds in India. The study analyses how social engineering techniques such as phishing, vishing, smishing, and QR-code manipulation are exploited to deceive users. The authors identify design-level vulnerabilities in UPI's authentication mechanisms and emphasize that most frauds occur due to user manipulation rather than system failure. The study highlights that age, occupation, or education do not significantly influence susceptibility to cyber fraud. It concludes that strengthening protocol-level security along with large-scale user awareness initiatives is essential to reduce UPI-related cybercrimes.

Kaur, Mishra & Goyal [7] This research provides a technical security analysis of the UPI protocol by reverse-engineering multiple UPI applications. The study identifies previously unreported design-level flaws in the multi-factor authentication framework of UPI 1.0. The findings reveal that attackers can exploit installed malicious applications to conduct scalable and remote attacks, potentially draining bank accounts without user interaction. The authors emphasize that social engineering remains the dominant cause of fraud, as users often blindly follow fraudulent instructions. The study calls for stronger authentication protocols, improved app-level security, and enhanced user education. Shreenivas & Basavaraj [8] This study examines usage patterns, awareness levels, and challenges within India's digital payment ecosystem, focusing on users in Sindhanur Taluk. Using structured questionnaires, the study identifies UPI as the dominant payment platform, particularly for small-value transactions. While users demonstrate moderate awareness of cybersecurity practices, challenges such as poor network connectivity, transaction failures, and limited infrastructure persist. The study also highlights emerging trends like voice-based and vernacular payment interfaces. The authors conclude that strengthening digital infrastructure and cybersecurity awareness is crucial for ensuring inclusive and sustainable growth of digital payments.

UPI is a secure and widely used digital payment system supported by encryption, device binding, and multi-factor authentication. However, existing studies show that most UPI frauds occur due to user-centric issues such as phishing, fake collect requests, QR-code scams, and social engineering rather than technical failures. Research also highlights risks from malware-infected or rooted mobile devices. The literature suggests that effective remediation requires a multi-layered approach, combining AI-based fraud detection, stronger authentication, regular security audits, and increased user awareness. Rashmi [15] The study

focuses on understanding students' awareness, perception, and adoption of UPI. Existing literature shows that ease of use, convenience, peer influence, and promotional offers are the main factors encouraging UPI adoption among young consumers. Previous studies also indicate that students prefer UPI over traditional payment methods due to its speed and cashless nature. However, concerns related to security and trust still influence usage frequency. Overall, the literature supports that UPI usage among undergraduate students is largely behavior-driven, shaped by awareness levels, social influence, and perceived usefulness.

Objectives of the Study

The main objectives of this study are:

1. To assess the level of cybersecurity awareness among UPI users.
2. To analyze users' cybersecurity practices while using UPI.
3. To examine the relationship between awareness and experience of cyber fraud.
4. To suggest measures for improving cybersecurity awareness among UPI users.

Research Methodology

Step 1: Selection of Research Design

A descriptive and empirical research design is adopted to study real-life behaviour and awareness of UPI users using primary data.

Step 2: Identification of Population and Sample

The population consists of individuals using UPI applications such as Google Pay, PhonePe, Paytm, and BHIM. A suitable sample size is selected using convenience sampling**.**

Step 3: Questionnaire Design

A structured questionnaire is developed focusing on:

- UPI usage frequency
- Awareness of cyber threats (phishing, fake QR codes, fraud calls)
- Security practices (PIN sharing, OTP handling)
- Experience with UPI-related fraud
- Knowledge of reporting procedures

Step 4: Data Collection

Primary data is collected through online and offline surveys from UPI users while ensuring confidentiality and voluntary participation

Step 5: Data Tabulation

Collected responses are coded and tabulated to enable systematic analysis of cybersecurity awareness and user behavior.

Step 6: Data Analysis

Simple statistical tools such as percentage analysis and frequency distribution are used to assess awareness levels, security practices, and fraud experiences of UPI users.

Step 7: Interpretation of Results

Results are interpreted to identify gaps between awareness and actual cybersecurity practices among UPI users.

Cybersecurity Awareness among UPI Users

Cybersecurity awareness among Unified Payments Interface (UPI) users refers to the level of understanding and knowledge individuals possess regarding digital payment risks, secure transaction practices, and preventive measures against cyber fraud. As UPI transactions are conducted through smartphones and internet connectivity, users become a crucial component of the security ecosystem. Even though UPI is supported by strong technical safeguards, lack of user awareness remains a major cause of cybercrime incidents.

UPI platforms implement security mechanisms such as multi-factor authentication (MPIN), device binding, encrypted communication, and secure APIs**.** However, attackers often bypass these controls by exploiting human behavior rather than technical vulnerabilities. Many UPI users are unaware of evolving threats such as phishing links, fake collect requests, QR code scams, and impersonation frauds, which significantly increases their exposure to financial loss.

Studies indicate that cybersecurity awareness varies widely among UPI users based on factors such as age, education level, digital literacy, and prior experience with cyber fraud. Users with limited awareness may unknowingly share sensitive information like OTPs or approve fraudulent payment requests. In contrast, users with higher awareness tend to verify transaction details, recognize suspicious activity, and follow recommended safety practices.

Another important aspect of cybersecurity awareness is knowledge of safe usage guidelines issued by banks and regulatory bodies. Many users remain unaware that UPI transactions cannot be reversed once authorized or that banks never ask for MPINs or OTPs. This lack of awareness makes users vulnerable to social engineering attacks, where fraudsters manipulate victims into authorizing transactions themselves.

Cybersecurity awareness also includes understanding the importance of secure device usage**,** such as keeping applications updated, avoiding public Wi-Fi networks for financial transactions, and using screen locks or biometric authentication. Poor digital hygiene increases the risk of malware infections and unauthorized access to UPI applications.

The literature emphasizes that improving cybersecurity awareness among UPI users is as critical as strengthening technical security measures. Awareness-driven security enables users to act as the first line of defense against cyber threats. Therefore, continuous education through awareness campaigns, in-app alerts, digital literacy programs, and simplified security guidelines is essential to ensure safe and sustainable use of UPI.

Cybersecurity Practices in UPI Usage

Cybersecurity practices in Unified Payments Interface (UPI) usage refer to the precautionary actions and responsible behaviors adopted by users to ensure safe and secure digital transactions. Although UPI platforms are designed with robust security mechanisms, the effectiveness of these systems largely depends on how carefully users follow safe usage practices. One of the most important cybersecurity practices is the protection of authentication credentials**,** such as MPINs and OTPs. Users are advised never to share these credentials with anyone, as banks and UPI service providers do not request such information. Regularly changing MPINs and avoiding predictable number combinations further enhance account security.

Another critical practice involves verifying transaction details before approving payments. Users should carefully check the recipient's name, amount, and transaction type (pay or collect request) to prevent fraudulent transfers. Many UPI-related frauds occur when users unknowingly approve fake or misleading payment requests. Safe device usage is also an essential cybersecurity practice. Users should ensure that their smartphones are protected with screen locks or biometric authentication and that UPI applications are downloaded only from official app stores. Keeping the operating system and payment applications updated helps protect against malware and known vulnerabilities.

Avoiding suspicious links, QR codes, and unknown messages is another key practice. Fraudsters often use phishing techniques through SMS, emails, or social media to trick users into clicking malicious links. Users should understand that scanning a QR code is meant only for making payments and not for receiving money. Additionally, users should refrain from conducting financial transactions over public or unsecured Wi-Fi networks**,** as such networks increase the risk of data interception. Logging out of UPI applications after use and monitoring transaction history regularly also help in early detection of unauthorized activities. Overall, cybersecurity practices in UPI usage emphasize the role of users as active participants in maintaining digital payment security. Consistent adherence to safe practices significantly reduces the risk of cyber fraud and enhances trust in UPI-based payment systems.

Relationship between Awareness and Cyber Fraud Experience

The relationship between cybersecurity awareness and cyber fraud experience among UPI users is a critical aspect of digital payment security. Cybersecurity awareness refers to a user's understanding of potential threats, safe usage practices, and preventive measures, while cyber fraud experience reflects incidents of financial loss or attempted fraud during UPI transactions. Existing studies and theoretical models suggest a strong inverse relationship between cybersecurity awareness and cyber fraud experience. Users with low awareness levels are more likely to fall victim to fraud due to unsafe practices such as sharing OTPs or MPINs, clicking on suspicious links, or approving fake collect requests. Fraudsters commonly exploit these knowledge gaps through social engineering techniques rather than technical attacks.

Conversely, users with higher cybersecurity awareness are better equipped to identify fraudulent attempts. Such users tend to verify transaction details carefully, recognize phishing messages, and follow official safety guidelines issued by banks and UPI service providers. As a result, they experience fewer fraud incidents and are more likely to report suspicious activity promptly. Cyber fraud experiences themselves can also influence awareness. Users who have previously encountered fraud often become more cautious and develop safer transaction habits. However, the literature indicates that preventive awareness is more effective than post-fraud learning**,** as financial losses and emotional stress can be significant.

Overall, the relationship between awareness and cyber fraud experience highlights that improving cybersecurity awareness among UPI users can substantially reduce fraud occurrences. Strengthening user educatio education, therefore, plays a vital role in enhancing the security and reliability of UPI transactions.

Measures to Improve Cybersecurity Awareness

Improving cybersecurity awareness among UPI users is essential to reduce cyber fraud and ensure secure digital transactions. Since most UPI-related frauds arise due to user negligence and lack of knowledge rather than technical failures, awareness-focused measures play a vital role in strengthening the overall security ecosystem. One effective measure is the implementation of continuous awareness campaigns by banks, UPI service providers, and regulatory bodies. These campaigns should educate users about common fraud techniques such as phishing, fake collect requests, QR-code scams, and impersonation frauds. Simple and clear messages delivered through SMS alerts, mobile notifications, and social media platforms can significantly improve user awareness.

In-app security alerts and warnings can further enhance awareness. UPI applications should display real-time alerts when users receive suspicious payment requests or attempt risky actions. Periodic reminders about not sharing MPINs or OTPs can reinforce safe behavior. Promoting digital literacy programs at educational institutions, workplaces, and community centers is another important measure. Such programs can help users understand basic cybersecurity concepts, safe transaction practices, and the consequences of cyber fraud.

Banks and service providers should also simplify and widely publicize official safety guidelines for UPI usage. Easy-to-understand instructions on verifying transactions, reporting fraud, and securing mobile devices can empower users to protect themselves. Lastly, encouraging users to regularly update their applications, use strong authentication methods, and monitor transaction history can foster responsible digital behavior. Collectively, these measures can significantly enhance cybersecurity awareness and reduce cyber fraud incidents among UPI users.

Conclusion

Cybersecurity awareness plays a crucial role in ensuring the safe and reliable use of Unified Payments Interface (UPI) services. Although UPI systems are supported by strong technical security mechanisms, the effectiveness of these safeguards

largely depends on user awareness and responsible practices. Lack of knowledge about cyber threats, unsafe transaction behaviour, and negligence significantly increase the risk of cyber fraud.

The study highlights that users with higher cybersecurity awareness are better equipped to identify and avoid fraudulent activities, while those with limited awareness are more vulnerable to cyberattacks. Therefore, enhancing user awareness through continuous education, in-app alerts, digital literacy programs, and clear safety guidelines is essential. Strengthening cybersecurity awareness among UPI users not only reduces fraud incidents but also builds greater trust in digital payment systems, ensuring sustainable growth of cashless transactions.

Acknowledgment
The author expresses sincere gratitude to the Department of Computer Science, RJSPM's Arts, Commerce & Science College, Landewadi, Bhosari, Pune, for providing a supportive academic environment and continuous encouragement throughout this study.

Financial support and sponsorship
Nil.

Conflicts of interest
The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. Balambal, S. (2025). A study on user awareness and threat perception in digital payment.
2. Kavita, & Yadav, R. (2024). A study on cyber security awareness in digital payment system with special reference to Banasthali Vidyapith.
3. Reddy, T., & Swathi, G. (2025). A study on developing AI-powered fraud detection awareness for UPI transactions in India.
4. Nair, A. (2025). Awareness, threats and perception of cyber security.
5. Khandal, S. (2022). Customer awareness on UPI and mobile banking: An exploratory study.
6. Wadkar, P., & Mundhe, S. (2023). Cyber security challenges in UPI payment frauds in India.
7. Kaur, J., Mishra, P., & Goyal, R. (2023). Cyber-security in UPI payments.
8. Shreenivas, S., & Basavaraj, K. (2025). Digital payment ecosystem in India: Usage pattern, challenges and trends.
9. Anand, D. R., Rane, S., & Waikar, A. (2023). Unlocking the future: Exploring the societal shifts catalyzed by UPI in Indian payments. Journal of Digital Finance Studies.
10. Bhatia, D. R. (2024). Usage of UPI transactions and its challenges: A study on Gen Z and Millennials. International Journal of Commerce and Management Research.
11. Dam, S., & George, B. (2024). Customer perceptions about UPI-based mobile payment apps in India. SSRN Electronic Journal.
12. Edburg, B. F., Umadevi, K., Vidya, M., & Kumar, P. M. R. (2024). Role of UPI application usage and mitigation of payment transaction frauds. MDIM Journal of Management Review and Practice.
13. Harshini, A. L. (2021). A comparative study of UPI and traditional payment methods: Efficiency, accessibility, and user adoption. International Journal of Financial Studies.
14. Kumar, A., Sharma, V., & Singh, R. (2020). Security analysis of UPI payment systems. International Journal of Computer Applications.
15. Rashmi, & Anusha. (2025). UPI in the minds of young consumers: Awareness and usage intention among undergraduate students of Mangalore University. International Journal of Science and Management Studies.
16. Sakhiya, K., Lakhtariya, D., & Vidani, J. (2024). A study on consumer preference of UPI with reference to Ahmedabad City. International Journal of Integrative Sciences.
17. Thirupathi, K., & Akula, R. (2022). Perceptions of postgraduate students towards UPI transactions. Asian Journal of Economics, Business and Accounting.
18. Zohmingthanga, H. (2024). Adoption of Unified Payments Interface (UPI) in Mizoram: Understanding user behaviour and personal finance. Journal of Digital Banking.
19. Reserve Bank of India (RBI). (2023). Guidelines on digital payment security and customer protection. RBI Publications.
20. National Payments Corporation of India (NPCI). (2024). UPI product and safety guidelines. NPCI Reports.