International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 9s, 2025
https://www.theaspd.com/ijes.php

# Assessing Cybersecurity Awareness And Issues Among Citizens Of Navi Mumbai And Panvel Zone

**Prof. Tulshiram Kamble[1] , Dr. Pushpendu Rakshit[2] , Dr. Bajrang Lal[3]**

[1]Research Scholar, Singhania University, Rajasthan, India
[2]Pillai Institute of Management Studies and Research, Panvel, Maharashtra, India.
[3]Research Guide, Singhania University, Rajasthan, India

**Abstract**

*The government's demonetization initiative, along with its vision to transform India into a cashless economy, has brought a significant shift in payment behaviour, accelerating the adoption of digital payment systems. This shift was further catalysed by the COVID-19 pandemic, which drastically reduced physical transactions and increased reliance on digital modes such as E-wallets. Although traditionally Indian consumers preferred cash-on-delivery methods, the pandemic has prompted a rapid rise in mobile wallet usage due to convenience and safety.*

*The diffusion of mobile payment systems is highly dependent on user readiness, perceived ease of use, and most importantly, trust in cybersecurity. With smartphones functioning as digital wallets, concerns related to cybercrime, data privacy, and digital fraud have grown significantly. While digital adoption continues to rise, awareness of cybersecurity and preventive practices remains uneven, especially in rapidly developing regions.*

*This exploratory study focuses on assessing the awareness of cybersecurity issues and readiness to adopt E-wallets among citizens of Navi Mumbai and Panvel zone—two key urban and commercial areas of Maharashtra. The research also investigates users' understanding of cyber threats, including aspects of computer forensics and techno-legal knowledge, which are increasingly relevant in the digital age.*

*According to recent RBI reports, India has witnessed nearly 1 billion digital transactions, underlining the urgency for digital literacy and robust cybersecurity frameworks. This study contributes insights into the challenges and preparedness of citizens in safeguarding themselves against cyber risks, and highlights the need for focused awareness campaigns and techno-legal skill development in urban India.*

***Keywords:*** *Digital Payment, E-wallet, cyber security, preventive measurements, Navi Mumbai.*

## Introduction

India has witnessed a transformative shift in its payment landscape, driven by a combination of policy changes, technological advancements, and unforeseen global events. The demonetization initiative announced on 8th November 2016, followed by the onset of the COVID-19 pandemic, acted as catalysts in accelerating the transition toward a cashless economy. These events significantly influenced citizens' payment behaviour and increased reliance on digital platforms, such as mobile wallets, UPI, net banking, and contactless card payments. As smartphones began functioning as digital wallets (Rathore, 2016), mobile-based payment apps such as Paytm, Google Pay, PhonePe, and Amazon Pay became widely adopted due to their convenience and safety during social distancing mandates.

During the initial pandemic months, a survey by Local Circles revealed that 42% of Indians used digital payment methods more frequently than before, with 33% preferring Paytm and 14% opting for Google Pay. Government bodies like the National Payments Corporation of India (NPCI) and the Reserve Bank of India (RBI) strongly encouraged the use of digital payment channels to reduce cash handling and mitigate virus spread. The RBI Governor also advocated for leveraging mobile banking, internet banking, UPI, IMPS, and other digital tools to reduce public footfall in crowded areas like ATMs.

Despite the visible benefits of digital transactions, the surge in online activity has also been paralleled by a spike in cybercrimes. Reports from organizations like the Computer Emergency Response Team (CERT) indicate a sharp rise in cybersecurity incidents. The 2005 CSI/FBI Computer Crime and Security Survey noted significant financial losses due to virus attacks, unauthorized access to information, and theft of proprietary data. In the first half of 1999 alone, virus-related damages were estimated to be around $7.6

billion (Kabay, 2001). Gordon, Loef, Lucyshyn, and Richardson (2004) emphasized that cybercrime victims suffer collective losses ranging from $500 million to $5 billion annually.

The vulnerabilities of computers and digital systems can be attributed to several key factors:

1. **High data storage capacity** in small devices makes them attractive for data theft.
2. **Easy accessibility** increases the risk of unauthorized intrusions.
3. **Complex system architectures** often contain loopholes exploited by cybercriminals.
4. **Negligence** in cybersecurity practices by users or institutions creates exploitable weak points.
5. **Loss of digital evidence**, particularly across borders, hampers legal proceedings and investigation.

Renowned legal scholar Hart stated, "Human beings are vulnerable, so rule of law is required to protect them." By analogy, computers and digital ecosystems are inherently vulnerable, necessitating robust legal and technological frameworks to ensure cybersecurity.

In regions like Navi Mumbai and Panvel — modern urban hubs with a high concentration of banks, fintech services, and digitally active populations — these concerns are particularly pressing. According to RBI statistics (2014), credit card transactions amounted to over 5.6 crore through Point of Sale (POS) systems and over 4.3 lakh via ATMs. By January 2017, these numbers rose significantly, with over 11 crore credit card POS transactions and over 32 crore debit card POS transactions, highlighting rapid digital adoption post-demonetization.

Despite the implementation of cyber laws and increased awareness efforts, cybercrime cases continue to rise. Issues such as identity theft, phishing, financial fraud, and digital harassment persist, disproportionately affecting vulnerable groups such as women and the elderly. This raises the urgent need for public education, legal enforcement, and cybersecurity preparedness.

Given this backdrop, this study aims to assess the cybersecurity awareness levels among citizens in Navi Mumbai and Panvel, explore their digital payment behaviour post-demonetization and during the COVID-19 era, and identify the critical factors influencing their perception and preparedness toward cyber threats. By understanding these dynamics, the study seeks to offer practical insights for improving cyber hygiene, policy formation, and digital inclusion in India's growing digital economy.

## REVIEW OF LITERATURE

Mobile payment instruments are a subset of electronic money, which includes all non-cash and non-paper payment methods such as plastic cards, direct transfers, and all money transactions conducted via electronic channels (Singh, 1999). Van Hove (2004) emphasized that electronic wallets, though often compared to debit cards, more closely resemble cash in functionality. They were introduced in the mid-1990s to enable cost-effective handling of small-value transactions. The Bank for International Settlements defines an electronic purse as a "reloadable multipurpose prepaid card which may be used for small retail or other payments instead of coins" (CPSS, 2003). Unlike debit or credit cards, e-wallet transactions are typically carried out offline, eliminating the need for intermediaries and minimizing fixed costs (M'Chirgui & Chanel, 2008).

Upadhyay (2012) highlighted that electronic wallets enable users to complete e-commerce transactions swiftly and securely. Shin (2016) described mobile wallets as multifunctional applications that not only support transactions but also store loyalty cards, travel passes, and membership details. According to Taheam et al. (2016), technological advancements have made digital payment infrastructure significantly user-friendly. The concept, however, is not new—countries like Japan, the U.S., Sweden, and South Korea have long been using cell phones for payments, vending machine purchases, and identification (Rathore, 2016).

Painuly and Rathi (2016), in their study Mobile Wallet: An Upcoming Mode of Business Transaction, identified convenience, security, and application ease as the major benefits of mobile wallets. They also noted that sectors such as banking, retail, and hospitality are integrating mobile wallets for both B2C and C2C transactions. Similarly, Balan, Ramasubhu, and Tayi (2006) analyzed Singapore's digital wallet ecosystem, outlining both the requirements and implementation challenges.

Rathore (2016) conducted a study involving 132 smartphone users to assess the adoption of digital wallets. Findings revealed that the key drivers were convenience, brand trust, and perceived usefulness. Users

expressed satisfaction, though security remained the most pressing concern. Rathore concluded that the adoption rate would increase further due to the ease of use.

In Punjab, Taheam, Sharma, and Goswami (2016) carried out a descriptive study using snowball sampling of 386 digital wallet users. The study showed that motives such as controllability, security, societal influence, and performance expectations were primary drivers of wallet adoption.

Kalyani (2016) explored awareness and usage of e-wallets among Indian youth, noting that while respondents were informed about domestic digital payment services, awareness of global alternatives remained low. The study concluded that wider adoption could be driven by adding more value-added features to existing wallet platforms.

Sardar (2016) focused on urban consumers in Jalgaon, Maharashtra. Based on responses from 60 mobile wallet users, the study highlighted that the primary use case was money transfers, followed by mobile and DTH recharges. Instant payment capability and transaction security were found to be top user concerns.

Shukla (2016) forecasted that mobile wallets would evolve into self-sufficient ecosystems. Beyond payments, they are expected to become tools for customer engagement and marketing. Future expectations include features like digital receipts, real-time value card updates, and loyalty point integration—making mobile wallets integral to a seamless shopping experience.

Shin-Dong (2009) applied the Unified Theory of Acceptance and Use of Technology (UTAUT) model to analyse mobile wallet adoption. The study identified perceived security, trust, and social influence as crucial factors influencing user attitudes, along with traditional factors like usefulness and ease of use.

Roy and Sinha (2014) observed that while e-payment systems in India are growing, over 90% of transactions still occur in cash. Their study used the Technology Acceptance Model (TAM) and concluded that innovation, incentives, consumer convenience, and legal frameworks are essential for strengthening the digital payment ecosystem.

Rakesh and Ramya (2014) investigated the factors influencing the adoption of internet banking in India. Their study emphasized the importance of trust, ease of access, customer awareness, and perceived security as major determinants of digital banking adoption.

## GAP IDENTIFICATION

Although a wide range of studies have examined the adoption, usability, and consumer behaviour related to mobile wallets and digital payment systems, several significant gaps remain unaddressed. Most of the existing literature primarily emphasizes the convenience, ease of use, and functionality of digital wallets, often overlooking the critical aspect of cybersecurity awareness among users. With the increasing instances of cybercrime, especially post-demonetization, there is a clear need to explore how aware users are about the risks associated with digital payments and the measures they take to safeguard themselves. Furthermore, while some regional studies have been conducted—such as in Punjab and Jalgaon—they fail to provide a broader, comparative understanding across different regions and demographics in India. There is also a lack of longitudinal research that captures the evolving consumer behaviour and cyber threat perception post-2016, a period that witnessed a sharp increase in digital payment adoption due to demonetization.

Additionally, factors such as gender, income level, and educational background, which can significantly affect digital payment adoption and vulnerability to cyber threats, have not been explored in depth. Although concerns about digital security are frequently mentioned, few studies examine the extent of public awareness regarding cyber laws, data protection regulations, and legal remedies available to users. Another overlooked dimension is the role of technological literacy—especially among rural populations and older age groups—which remains a critical barrier to safe and effective usage of mobile payment systems. Lastly, while cybercrime statistics are often cited separately, there is a lack of integrated analysis linking these trends directly with consumer behaviour and awareness. These gaps highlight the urgent need for a comprehensive study that addresses the intersection of digital wallet usage, cybersecurity awareness, legal knowledge, and demographic variations in the Indian context.

## OBJECTIVE OF THE STUDY

- To assess the awareness level of consumers regarding cybersecurity in digital and mobile wallet transactions.
- To identify key challenges and concerns faced by users in digital wallet transactions, especially regarding security and privacy.

## RESEARCH DESIGN

- Mixed research - Qualitative and Quantitative
  - testing theory through observation and data (Primary & secondary).
- Exploratory Study
  -Purposive, (deliberate) self-selection sampling and area sampling.
- Length of study
- Approximately 3 years.
- Collection of data
  - In- depth personal interview with respondents from hospitality sector.
  - Survey method to be applied for data collection from stake holders.
  - Online / offline questionnaire method.
- Delphi method / expert advice for probable solutions and understanding.
- Self-completion diaries
  To track issues and dynamism in industry.
- Sample size
- 1,106 customers / bankers / cyber experts, [ structured and semi-structured] approximately
- Location of study – Navi Mumbai and Mumbai
- Analysis – SPSS package and tools

## HYPOTHESIS OF RESEARCH

The research hypothesis is designed based on literature review and objectives.

1. There exists statistically significant correlation between cyber threats and vulnerabilities and its impact on users of such e-wallet payment platforms in normal and new normal epoch.
2. It is proposed that there exists a need for cyber awareness among masses as digital dependencies have geared up.

## RELIABILITY TESTING

**Case Processing Summary**

| | | N | % |
|---|---|---|---|
| Cases | Valid | 1106 | 100.0 |
| | Excluded | 0 | .0 |
| | Total | 1106 | 100.0 |

a. List wise deletion based on all variables in the procedure.

**Reliability Statistics**

| Cronbach's Alpha | N of Items |
|---|---|
| .796 | 25 |

Reliability analysis for each parameter was done using Cronbach's Alpha and the calculated value is given above. The value is found to be above 0.796 for most of the cases for 25 items in total. Hence we conclude that the values of reliability are satisfactory and we shall proceed with the further analysis of data.

**TESTING OF HYPOTHESIS OF RESEARCH**

**Hypothesis 1**

H0 -There exists no statistically significant correlation between cyber threats and vulnerabilities and its impact on users of such e wallet payment platforms in normal and new normal epoch.

H1 -There exists statistically significant correlation between cyber threats and vulnerabilities and its impact on users of such e wallet payment platforms in normal and new normal epoch.

**Case Processing Summary**

| | Cases | | | | | |
|---|---|---|---|---|---|---|
| | Valid | | Missing | | Total | |
| | N | Percent | N | Percent | N | Percent |
| Q9 Have you ever been vistim of Cyber crime or attack? * Q17 There is an increase in number of cyber crimes committed amid pandemic in your city | 1106 | 100.00% | 0 | 0.00% | 1106 | 100.00% |

**Q9 * Q17 Cross tabulation**

| | | Q17 | | | | | Total |
|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | |
| Q9 | 1 | 7 | 7 | 77 | 42 | 28 | 161 |
| | 2 | 7 | 49 | 119 | 154 | 63 | 392 |
| | 3 | 0 | 0 | 70 | 105 | 28 | 203 |
| | 4 | 14 | 7 | 28 | 147 | 63 | 259 |
| | 5 | 0 | 0 | 35 | 21 | 35 | 91 |
| Total | | 28 | 63 | 329 | 469 | 217 | 1106 |

**Chi-Square Tests**

| | Value | df | Asymp. Sig. (2-sided) |
|---|---|---|---|
| Pearson Chi-Square | 186.444[a] | 16 | .000 |
| Likelihood Ratio | 206.765 | 16 | .000 |

| | | | |
|---|---|---|---|
| Linear-by-Linear Association | 42.702 | 1 | .000 |
| N of Valid Cases | 1106 | | |

a. 2 cells (8.0%) have expected count less than 5. The minimum expected count is 2.30.

As the Pearson Chi-Square significant level is 0.00< 0.05 from the results driven thus null hypothesis H0 is rejected and alternate hypothesis H1 is accepted showing good fit. Thus, we conclude that at 90% confidence level, There exists statistically significant correlation between cyber threats and vulnerabilities and its impact on users of such e wallet payment platforms in normal and new normal epoch.

**Hypothesis 2**

H0 - There exists no need of cyber literacy and cyber awareness among masses as digital dependencies have geared up.

H1 - There exists a need of cyber literacy and cyber awareness among masses as digital dependencies have geared up.

**Case Processing Summary**

| | Cases | | | | | |
|---|---|---|---|---|---|---|
| | Valid | | Missing | | Total | |
| | N | Percent | N | Percent | N | Percent |
| Q14 Do online payment gateway companies provide sufficient cyber literacy to their consumers * Q26 You feel encouraged and motivated to use online transaction services provided by companies | 1106 | 100.00% | 0 | 0.00% | 1106 | 100.00% |

**Q14 * Q26 Cross tabulation**

| | | Q26 | | | | | Total |
|---|---|---|---|---|---|---|---|
| | | 1 | 2 | 3 | 4 | 5 | |
| Q14 | 1 | 7 | 0 | 14 | 28 | 14 | 63 |
| | 2 | 7 | 21 | 49 | 98 | 28 | 203 |
| | 3 | 7 | 28 | 231 | 126 | 35 | 427 |
| | 4 | 7 | 14 | 49 | 259 | 35 | 364 |
| | 5 | 0 | 0 | 14 | 14 | 21 | 49 |
| Total | | 28 | 63 | 357 | 525 | 133 | 1106 |

**Chi-Square Tests**

| | Value | df | Asymp. Sig. (2-sided) |
|---|---|---|---|
| Pearson Chi-Square | 275.735[a] | 16 | .000 |
| Likelihood Ratio | 258.619 | 16 | .000 |
| Linear-by-Linear Association | 22.412 | 1 | .000 |
| N of Valid Cases | 1106 | | |

a. 4 cells (16.0%) have expected count less than 5. The minimum expected count is 1.24.

As the Pearson Chi-Square significant level is 0.00< 0.05 from the results driven thus null hypothesis H0 is rejected and alternate hypothesis H1 is accepted showing good fit. Thus, we conclude that at 90% confidence level, there exists a need of cyber literacy and cyber awareness among masses as digital dependencies have geared up.

Major Challenges/Problems of Digital Payments

1. Low public confidence in digital payment systems continues to be a significant barrier to widespread adoption, especially among first-time users.
2. Digital illiteracy and limited awareness among the less educated or technologically disadvantaged sections of the population hinder the growth of digital transactions.
3. Frequent incidents of cyber fraud and security breaches have led to a perception of unreliability among users, reducing trust in e-payment platforms.
4. Unstable internet connectivity, particularly in rural and semi-urban areas, disrupts the smooth execution of digital transactions.
5. Delayed processing of cashback and refunds by e-commerce and e-wallet providers reduces user satisfaction and trust.
6. Transaction failures or processing errors, coupled with a lack of timely communication from service providers, often leave users uncertain about the status of their payments.

## PREVENTIVE MEASURES

1. Sensitive personal and financial information such as card numbers, CVV, passwords, PINs, and OTPs must never be disclosed to anyone, regardless of personal trust, to maintain transaction security (Vivina Vishwanathan, 2017).
2. A dedicated and independent fraud risk management division should be established within banks, staffed with trained professionals and headed by a senior executive (preferably General Manager or above), to handle monitoring, prevention, investigation, and awareness initiatives.
3. Fraud review councils must be constituted at organizational levels, including cross-functional heads from business, fraud risk, operations, and IT, meeting quarterly to evaluate fraud patterns and update prevention strategies.
4. Standardized fraud prevention protocols, such as vulnerability assessments, stringent KYC norms, fraud loss thresholds, post-fraud root cause analysis, and data security practices, should be embedded into banking processes.
5. Negative listing systems like CIBIL Detect should be expanded to include not only suspicious accounts but also employee records related to fraud, minimizing the risk of internal fraudsters migrating between institutions.
6. Real-time fraud detection systems, involving transaction monitoring tools and algorithm-based anomaly detection, must be deployed for early fraud identification and rapid intervention.
7. Specialized fraud investigation teams should receive ongoing training in the latest techniques in cyber forensics, data analytics, and regulatory compliance to remain effective against evolving threats.
8. Customer awareness programs should be actively conducted by banks and financial institutions to educate users about cyber hygiene and safe transaction practices, particularly in local languages and simplified formats.

## CONCLUSION

The rapid growth of digital payment platforms, particularly e-wallets, has transformed the way financial transactions are conducted in Navi Mumbai and Panvel. However, this evolution has brought along significant cybersecurity concerns that cannot be overlooked. The study reveals that despite the increasing adoption of digital wallets, many users still lack adequate awareness about cybersecurity risks and best practices. Issues such as lack of trust, frequent frauds, data breaches, poor internet connectivity, and delays in transaction processing continue to hamper user experience and satisfaction.

The research also identifies a statistically significant correlation between cyber literacy and the perceived safety of digital transactions. Users who are more informed about cybersecurity tend to exhibit higher

trust and engagement in digital payment systems. Furthermore, the study highlights the pressing need for structured, institution-led cybersecurity education campaigns and robust fraud management frameworks. Key preventive measures suggested include forming specialized fraud monitoring units within banks, implementing real-time transaction monitoring systems, sharing fraudulent employee data among financial institutions, and consistently updating users on safe digital practices.

In conclusion, while digital payments offer speed, convenience, and economic transparency, their long-term sustainability depends on addressing cybersecurity challenges through user education, institutional vigilance, and policy support. Only a holistic approach that combines technology, regulation, and awareness can build a truly secure and trusted digital payment ecosystem.

## REFERENCES

1. Committee on Payment and Settlement Systems. (2003). A glossary of terms used in payments and settlement systems. Bank for International Settlements.
2. Kalyani, P. (2016). Awareness and usage of paperless e-currency transaction like e-wallet using ICT in the youth of India. International Journal of Scientific Research and Modern Education, 1(1), 803–807.
3. M'Chirgui, Z., & Chanel, O. (2008). Electronic wallet: A new strategic positioning. Journal of Payments Strategy & Systems, 2(1), 66–78.
4. Painuly, P., & Rathi, S. (2016). Mobile wallet: An upcoming mode of business transaction. International Journal in Management and Social Science, 4(5), 356–362.
5. Rathore, H. S. (2016). Adoption of digital wallet by consumers. BVIMSR's Journal of Management Research, 8(1), 69–75.
6. Ramesh, S. (2016). Preference towards mobile wallets among urban population of Jalgaon city. Journal of Management, 3(5), 12–18.
7. Roy, S., & Sinha, I. (2014). Determinants of customers' acceptance of electronic payment system in Indian banking sector–A study. International Journal of Scientific and Engineering Research, 5(1), 177–187.
8. Shin, D. H. (2009). Towards an understanding of the consumer acceptance of mobile wallet. Computers in Human Behaviour, 25(6), 1343–1354.
9. Shin, D. H. (2016). The role of trust in the adoption of mobile payment systems: Comparison between Korea and the US. Telecommunications Policy, 40(6), 492–500.
10. Shukla, T. N. (2016). Mobile wallet: Present and the future. International Journal of Business and Management Invention, 5(9), 27–31.
11. Singh, S. (1999). Electronic money and the possibility of a cashless society. First Monday, 4(10).
12. Taheam, K., Sharma, R., & Goswami, S. (2016). Drivers of digital wallet usage: A study in Punjab. International Journal of Research in Commerce and Management, 7(11), 35–39.
13. Upadhyaya, A. (2012). Electronic commerce and e-wallets: An analysis. International Journal of Recent Research and Review, 1(1), 1–6.
14. Van Hove, L. (2004). Electronic purses and the transition to electronic money. Netnomics, 6(2), 131–163.