



A STUDY ON PUBLIC AWARENESS AND PERCEPTION OF BANKING SCAMS IN INDIA

Mr. Pawan Vakil Gupta

Student Researcher, M. Com Banking And Finance Semester III.

PTVA's Mulund College of Commerce (Autonomous),
Mulund west, Mumbai, Maharashtra.

Dr. Abhilasha N

Assistant Professor, Department of Management Studies,
PTVA's Mulund College of Commerce (Autonomous),
Mulund Vanijya Mahavidyalaya Road, Mulund (West),
Mumbai - 400080, Maharashtra, India

Email id: abhilasha.n@mccmulund.ac.in

ABSTRACT

This study explores how aware people in India are about banking scams and how they perceive the safety of digital banking. As online banking, UPI, and mobile payment services grow, scams such as phishing, vishing, OTP fraud, and ATM skimming have also increased. Findings from 110 respondents show that although many people use digital banking regularly, their understanding of scam techniques and safe practices is still limited. Some users feel confident using digital services but remain unaware of common risks. The study also reveals that awareness campaigns by banks and the RBI do not reach all customers effectively. Demographic factors like age and education influence how people view digital banking security. Overall, the research highlights the need for stronger awareness programs, better communication, and improved safety measures. Strengthening digital literacy is essential for building trust and reducing fraud in India's growing digital banking ecosystem.

Keywords: Public Awareness, Public Perception, Banking Scams, Digital Banking Frauds, Phishing

INTRODUCTION

Over the last few years, the Indian banking sector has changed dramatically. With the rise of internet banking, UPI payments, mobile apps, and card transactions, banking has become faster, simpler, and more convenient than ever before. Today, people can transfer money, pay bills, and manage accounts within seconds from their phones. While this digital revolution has made life easier, it has also opened the door to a growing number of banking scams and cyber frauds.

Banking scams such as phishing emails, fake customer-care calls, UPI frauds, ATM skimming, SIM swaps, and identity theft have become increasingly common. Fraudsters use convincing messages, links, and calls to trick people into sharing sensitive information like OTPs, PINs, and passwords. Even with repeated warnings from the Reserve Bank of India (RBI) and commercial banks, many people still fall victim because they are unaware of how these scams work or how to protect themselves online.

Public awareness, therefore, becomes extremely important. When customers know how scams happen and what red flags to look for, they are far less likely to be cheated. However, awareness is not the same for everyone. Younger people who frequently use digital services may understand online risks better, while older individuals or those with limited digital skills may find it harder to identify fraud. Public perception also shapes how people use digital banking. Some customers feel confident and trust online systems, while others feel unsafe because of the rising number of fraud cases highlighted in the news. In this context, it becomes necessary to study what people actually know about banking scams and how they perceive the

safety of the banking system. Understanding their awareness levels helps identify which groups are more vulnerable, what knowledge gaps exist, and which areas need stronger awareness campaigns. It also helps banks and policymakers design better communication strategies to protect customers from fraud.

This research aims to explore these issues by analysing public awareness, attitudes, and experiences related to banking scams in India. By doing so, it hopes to contribute to safer digital banking practices, improved financial literacy, and greater trust in India's rapidly growing digital financial ecosystem.

The rapid shift toward digital payments after initiatives like UPI has made online banking a routine part of daily life for millions of Indians. However, this convenience has also increased people's exposure to cyber threats, making it essential to understand how well customers can protect themselves. As fraudsters continue to adopt more innovative and convincing methods, the gap between digital usage and digital awareness becomes more visible. Many users rely heavily on online transactions without fully understanding the risks involved or the safety measures they should follow. Therefore, studying public awareness and perception becomes crucial for building a safer and more trustworthy digital banking environment.

2. REVIEW OF LITERATURE

Aravind Sueya R. (2022) found that most customers know about e-banking, especially ATMs, and many recently started using online services. People like e-banking because it's easy access, but network issues and security concerns stop them from using it fully. The study suggests banks improve usability, fix network problems, build trust, and promote online services better.

Khanna & Arora (2009) studied why bank frauds happen in India and how security measures can be improved. Their research, based on responses from bank employees, showed that most frauds occur due to overworked staff, lack of proper training, low compliance, and high competition. They found that current security practices in banks are not meeting expectations. The study highlights that better employee training and stronger internal systems are essential to prevent fraud effectively.

Aysha Shabbir, Maryam Shabir, Abdul Rehman Javed et.al (2021) focused on detecting suspicious banking transactions and preventing fraud. Their study introduces a fast, reliable, and advanced fraud-detection method for modern banking systems. Using quantum and cognitive computing within the Banking Cyber-Physical System (BCPS), they propose a smarter way to identify suspicious entities and strengthen fraud detection in the post-quantum era.

Priyanka Datta, Sarvesh Tanwar, Surya Narayan Panda, and Ajay Rana (2020) reviewed the major security issues in mobile and online banking. Their report highlights how online fraud cases are rising rapidly and explains the different scams happening in the banking sector. The authors stress that stronger customer awareness programs are needed so users can protect themselves and avoid falling victim to these online frauds.

Charan Singh, Divyesh Satishkumar Dixit et.al (2016) examined various types of banking frauds and the rise in credit card debt in India. Using secondary data, case studies, and interviews with stakeholders, the report highlights the increase in non-performing assets (NPAs), especially in public sector banks. The study also offers practical suggestions to reduce future frauds and strengthen the Indian banking system.

Mohammed Afzal et al. (2024) found that Indian e-banking users' awareness of cyberfraud and cybersecurity knowledge positively influences their intention to use e-banking services. The study integrated cybersecurity awareness into the Technology Acceptance Model and showed that increased knowledge helps users protect themselves and encourages safer usage of online banking platforms. However, it also highlighted that emerging cyberfraud remains a significant challenge to full adoption of digital banking, suggesting that more education on fraud identification and prevention is needed to build user confidence and reduce vulnerability to scams.

Sreethi Rebeka R. and Jaikala L. (2023) examined customer awareness of cyber security and digital payment frauds in the context of Indian nationalized banks, finding that increased online transactions have led to a rise in fraud attempts and hacking. Their research indicated that many customers fall victim to online fraud due to lack of awareness about cyberattack techniques like phishing and hacking; they stressed that improving customer knowledge about security practices and strengthening cyber defenses is essential to prevent banking scams.

Ramesh Kumar (2025) investigated awareness and perception of digital banking frauds among rural customers in Sonipat and found varying levels of awareness across different demographic groups. The research showed that younger, more educated, and employed individuals tended to be more aware of digital banking scams, while others remained less informed. The study emphasized the need for targeted awareness programs to enhance understanding of fraud risks and improve preventive behaviours among less aware segments of the population.

3.RESEARCH OBJECTIVES

The specific objectives of the study are as follows:

1. To assess the current level of public awareness concerning various forms of banking in India
2. To examine the perception of individuals regarding the security and trustworthiness of banking institutions, particularly in the context of scam prevention and response.
3. To investigate the primary channels and sources through which the public acquires information related to banking scams and fraud prevention
4. To analyse the influence of socio demographic factors such as age, education, income level and digital literacy on public awareness and perception of banking scams.
5. To provide suggestions on how the awareness can be increased and how the perception can be changed.

4.RESEARCH HYPOTHESIS

H01: There is no significant relationship between individual's awareness level and their exposure to information about banking scams through digital media

H1: There is a significant relationship between individual's awareness level and their exposure to information about banking scams through digital media

H02: Individuals who perceive bank as secure are less likely to take preventive actions against banking scams.

H2: Individuals who perceive bank as less secure are more likely to take preventive actions against banking scams.

H03: There is no significant influence of socio-demographic factors on public perception of banking security and scam vulnerability

H3: There is significant of socio-demographic factors on public perception of banking security and scam vulnerability

5.RESEARCH METHODOLOGY

5.1 Research Design: This research is primarily descriptive in nature. The study uses a quantitative and qualitative mixed approach. Quantitative research involves collecting numerical data through surveys and analysing them using statistical methods. Qualitative elements are included to interpret people's opinions, experiences, and attitudes toward banking safety and fraud prevention.**5.2 Sources of Data:** The study uses both primary and secondary data:

- **Primary Data:** Collected directly from respondents through structured questionnaires.
- **Secondary Data:** Gathered from existing sources such as RBI reports, published research papers, financial journals, books, government publications, and credible online sources on banking scams and digital fraud.

5.3 Sampling Design

- a) **Sampling Unit:** Individuals who use banking services — such as account holders, credit/debit card users, and digital payment users — across different age groups and occupations.
- b) **Sample Size:** Depending on feasibility, around 110 respondents are selected to ensure a representative sample.
- c) **Sampling Technique:** Convenience sampling is used, as respondents are chosen based on accessibility and willingness to participate.
- d) **Tools used for analysis:** The collected data from primary sources has been analyzed by using percentage using excel and also graphs have been adopted for graphical representation of the data.

6.DATAS ANALYSIS

6.1 Showing the Demographic Distribution of the respondents

DEMOGRAPHICS	CATEGORIES	NO. OF RESPONSES	PERCENTAGE (%)
AGE	18-20	14	12.70
	20-30	90	81.80
	30-40	3	2.70
	40 AND ABOVE	3	2.70
MONTHLY INCOME	BELOW 20,000	65	59.10
	20,000 – 30,000	24	21.80
	30,000 – 40,000	7	6.40
	40,000 ABOVE	14	12.70
	STUDENT	42	38.20
OCCUPATION	PRIVATE SECTOR	49	44.50
	GOVERNMENT	3	2.70
	SELF-EMPLOYED	10	9.10
	OTHER	6	5.50

INTERPRETATION:

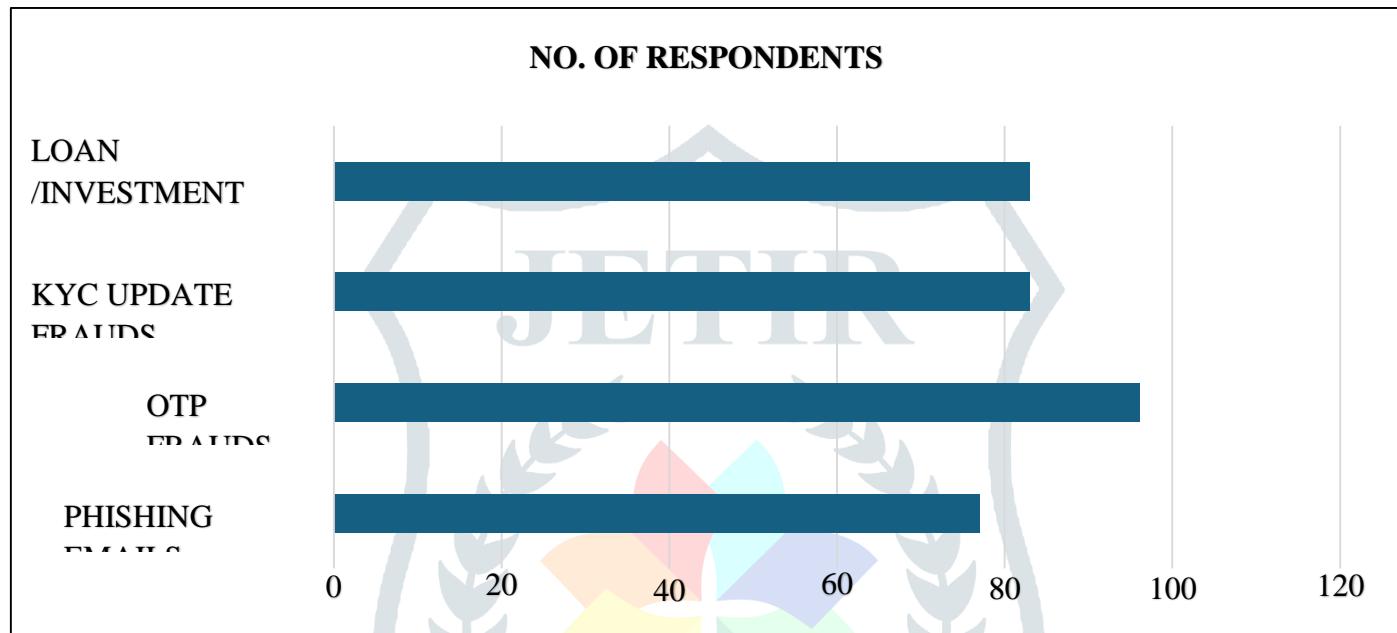
The sample is largely dominated by young adults, especially those aged 20–30. Most respondents fall in the lower-income category, earning below ₹20,000 per month. A significant portion of participants are students and private sector employees, indicating a young and digitally active population. Very few respondents belong to older age groups or higher income brackets.

This suggests that the study mainly reflects the experiences of youth and early-career individuals. Their familiarity with digital platforms may influence their awareness and perception of banking scams. Overall, the demographic profile shows a tech-savvy group that is frequently exposed to online banking services.

6.2 Showing the Analysis of Awareness of Different Types of Banking Scams

BANKING SCAMS	NO. OF RESPONDENTS	RESPONSES (IN %)
PHISHING EMAILS	77	70.00
OTP FRAUDS	96	87.30
KYC UPDATE FRAUDS	83	75.50
LOAN / INVESTMENT	83	75.50

6.1 Showing the Analysis of Awareness of Different Types of Banking Scams



Interpretation

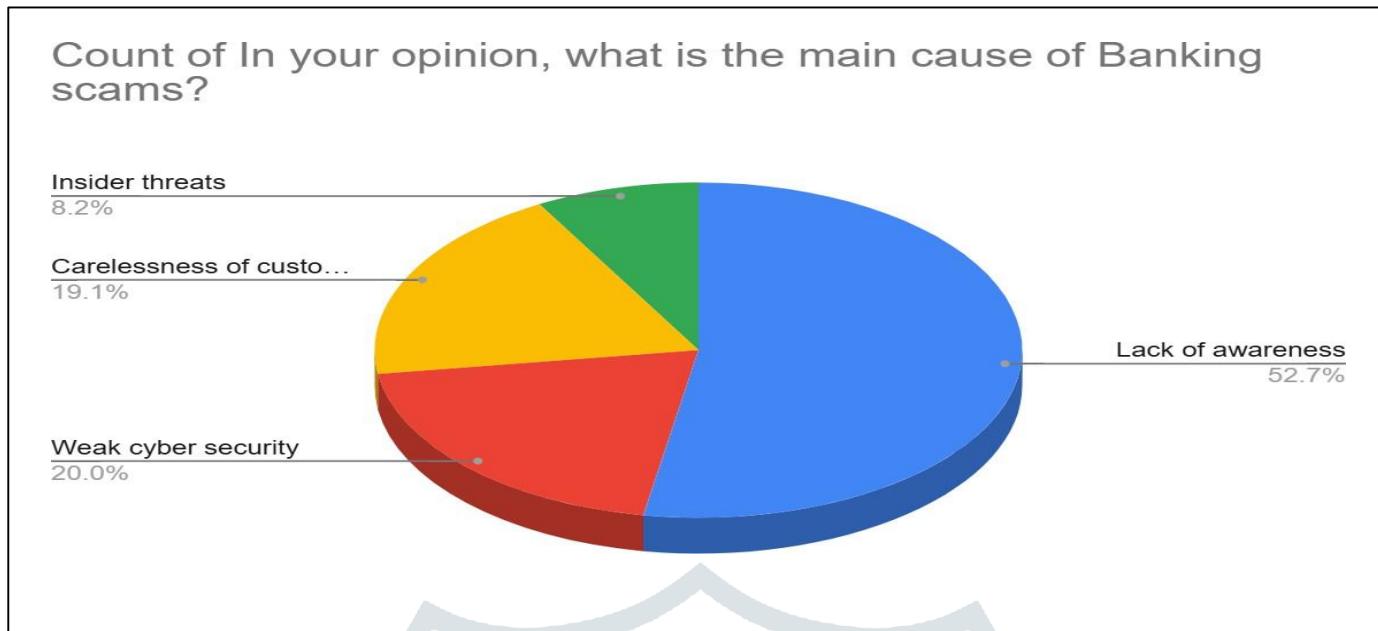
The chart shows that respondents are most aware of OTP frauds, with 96% recognizing this as a major scam, likely because it is widely discussed by banks. Awareness of phishing emails stands at 77%, meaning some people still fail to identify suspicious links or messages. Knowledge about KYC update frauds and loan/investment scams is also fairly high at 83%, indicating that many respondents understand these common financial risks.

Overall, the results suggest that people have a strong general awareness of banking scams, especially those involving OTP misuse.

6.3 Analysis of the Main Cause of Banking Scams

CAUSE OF SCAM	NO. OF RESPONDENTS	RESPONSES (%)
LACK OF AWARENESS	58	52.70
WEAK CYBER SECURITY	22	20.00
CARELESSNESS	21	19.10
INSIDER THREATS	9	8.20
TOTAL	110	100.00

6.2 Showing the main causes of banking scams



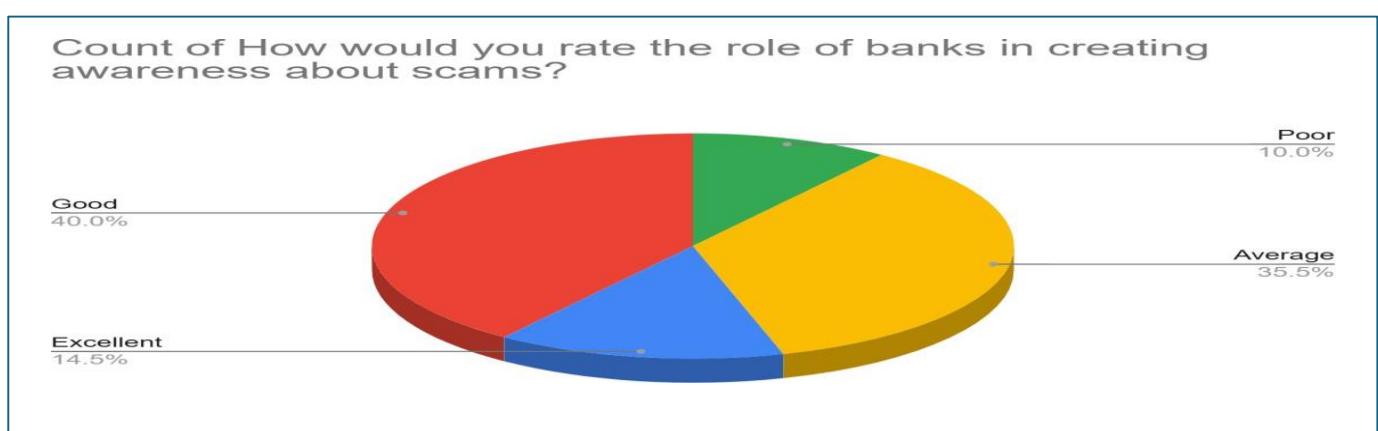
Interpretation

The data shows that over half of the respondents (52.7%) believe banking scams mainly happen because customers lack awareness, highlighting a major gap in financial literacy. Around 20% feel weak cybersecurity systems are to blame, while 19.1% think customer carelessness also plays a big role. Only a small percentage (8.2%) believe insider involvement is a cause. Overall, the results point to both user-related and system-related issues, stressing the need for stronger awareness programs, better digital security, and tighter monitoring to reduce banking scams.

6.4 Analysis of Role of Banks in Creating Awareness about Scams

ROLE OF BANKS	NO. OF RESPONDENTS	RESPONSES (IN %)
EXCELLENT	16	14.50
GOOD	44	40.00
AVERAGE	39	35.50
POOR	11	10.00
TOTAL	110	100.00

6.3 Showing the main causes of banking scams



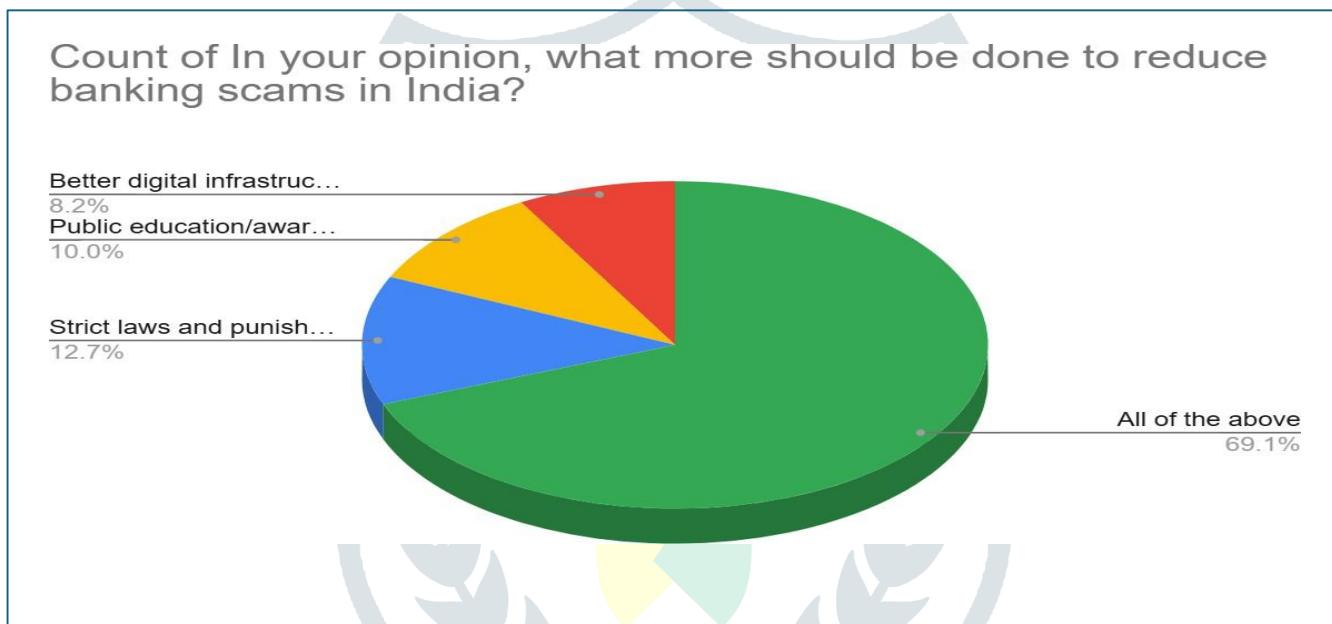
Interpretation: The chart shows that 40% of respondents feel banks are doing a “Good” job in creating scam awareness, while 35.5% think their efforts are only “Average.” About 14.5% believe the awareness initiatives are “Excellent,” and just 10% rate them as “Poor.” This means most customers appreciate the steps taken by

banks but still see space for better communication. Overall, the results suggest that although banks are making meaningful efforts, they need to strengthen and expand their awareness programs to reach a wider audience more effectively

6.5 Analysis to reduce the banking scams

REDUCTION MEASURES	NO. OF RESPONDENTS	RESPONSES (IN %)
BETTER DIGITAL INFRASTRUCTURE	9	8.20
PUBLIC EDUCATION / AWARENESS DRIVE	11	10.00
STRICT LAWS & PUNISHMENTS	14	12.70
ALL OF THE ABOVE	76	69.10
TOTAL	110	100.00

6.4 Showing the ways to reduce banking scams in India



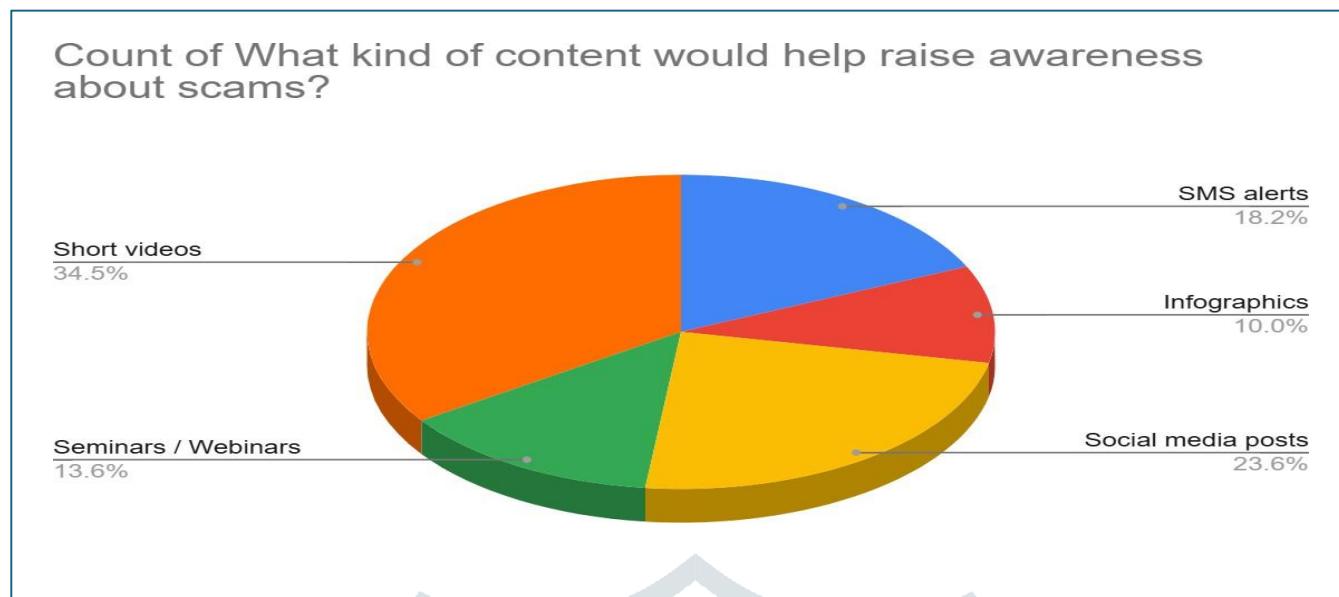
Interpretation:

The chart shows that 69.1% of respondents believe that reducing banking scams requires a mix of solutions—stronger digital systems, better public awareness, and stricter laws. Only 12.7% think strict legal action alone is enough, while 10% highlight the importance of customer education, and 8.2% focus mainly on improving digital infrastructure. This suggests that most people see scam prevention as a shared responsibility involving technology, law, and awareness. Overall, respondents clearly support a combined, multi-layered approach to effectively tackle banking fraud in India.

6.6 Analysis of Preferred Mediums for Banking Scam Awareness

PREFERRED MEDIUMS	NO. OF RESPONDENTS	RESPONSES (IN %)
SMS ALERTS	20	18.20
INFOGRAPHICS	11	10.00
SOCIAL MEDIA POSTS	26	23.60
SHORT VIDEOS	38	34.50
SEMINARS / WEBINARS	15	13.60
TOTAL	110	100.00

6.5 Showing the kind of content that would help to raise awareness about scams



Interpretation

The data shows that short videos are the most preferred way to learn about banking scams (34.5%), followed by social media posts (23.6%), indicating that people respond best to fast, engaging content. Traditional methods like seminars and infographics are less popular, suggesting a clear shift toward digital learning. This trend highlights the strong influence of online platforms in spreading awareness. Overall, the results suggest that future awareness campaigns should focus on quick, visual, and mobile-friendly content to reach the public more effectively.

7.FINDINGS

The study reveals that most respondents are well aware of common banking scams, especially OTP frauds, phishing emails, and KYC-related frauds. Lack of customer awareness emerged as the leading cause of banking scams, followed by weak cybersecurity and customer carelessness. The demographic analysis shows that young adults and working individuals form the majority of digital banking users, making them more exposed to online risks. Respondents also believe that banks are playing a reasonably good role in spreading awareness, though their efforts still fall short for many customers. Overall, the findings suggest that people understand the risks but still need more guidance and support to confidently navigate digital banking safely.

8.SUGGESTIONS

Based on the results, it is clear that banks must focus on stronger and more consistent awareness campaigns, especially targeting young users who rely heavily on digital banking. Short videos, social media content, and mobile-friendly formats should be used, as these are the preferred learning channels of most respondents. Banks should also improve their digital infrastructure, strengthen cybersecurity systems, and reduce network-related issues that create vulnerabilities. Regular training programs for both customers and bank staff can help reduce carelessness and improve response to suspicious activity. Additionally, stricter regulations and faster action against fraudsters will help build trust and protect the public more effectively.

9. COCLUSION

The study concludes that while digital banking has become an essential part of everyday life, it also brings significant risks that customers must be prepared to handle. Most people are aware of major scams but still lack complete understanding of how to avoid them. Banking frauds in India stem from a mix of low awareness, weak security, and user negligence, making a combined approach essential for effective prevention. Banks, customers, and regulatory bodies must work together to strengthen security, promote financial literacy, and create a safer digital environment. Ultimately, increasing awareness and improving digital safeguards will play a key role in reducing banking scams and building greater trust in the digital banking system.

REFERENCES

1. Aravind Sueya, R. (2020). *A study on customer issues and recommendations for improving e-banking services*. International Journal of Management Studies, 7(2), 45–52.
2. Khanna, A., & Arora, B. (2009). Investigation into the causes of bank frauds and the application of security measures in the Indian banking sector. *International Journal of Business Science and Applied Management*, 4(1), 1–21.
3. Shabbir, A., Shabir, M., Javed, A. R., Chakraborty, C., & Rizwan, M. (2021). Suspicious transaction detection in banking cyber-physical systems using quantum and cognitive computing. *IEEE Transactions on Computational Social Systems*, 8(6), 1475–1486.
4. Datta, P., Tanwar, S., Panda, S. N., & Rana, A. (2020). Security and issues of mobile banking: A technical review. *International Journal of Information Security Science*, 9(3), 317–328.
5. Sood, P., & Bhushan, P. (2019). Factors impacting banking frauds in India: A conceptual framework. *International Journal of Banking, Risk and Insurance*, 7(2), 12–21.
6. Afzal, M., Siddiqui, S. H., & Khan, M. S. (2024). Cybersecurity awareness and cyber fraud influence on e-banking adoption: An extension of the technology acceptance model. *Journal of Financial Services Marketing*, 29(4), 1–15.
7. Rebeka, R. S., & Jaikala, L. (2023). A study on customer awareness of cyber security and digital payment frauds with special reference to nationalized banks. *Harbin Engineering Journal*, 44(6), 897–904.
8. Kumar, R. (2025). A study on digital banking frauds and safety awareness in rural areas of Sonipat district. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, 13(1), 1023–1029.
9. Barla, S., & Reddy, G. N. (2023). *Customer perceptions of bank frauds: An analytical study*. *Journal of Informatics Education and Research*.
10. Upadhyay, D. (2019). *Banking scams in India*. *Journal of Banking and Insurance Law*, 1(2), 7–13.
11. Jadhav, A. N., & Others. (2021). *Need for Banking Ombudsman in the era of bank related scams in India*. *Psychology and Education Journal*, 58(3), 1–9.
12. Singh, G., & Kaur, S. (2023). *Bank frauds reported in India: A case study*. *Journal of Pharmaceutical Negative Results*, 14(S2), 304–309.

