KeAi
CHINESE ROOTS
GLOBAL IMPACT

International Journal of Innovation Studies

ANALYSIS ON BANK SCAMS IN THE DIGITAL HUB AND ITS EFFECTS IN GEN - Z AT CHENNAI CORPORATION

Dr.M.MALATHY
Assistant Professor, P.G.& Research Department of Commerce, S.I.V.E.T. College, Chennai, India.

Abstract

There is a rise in bank frauds, especially among the younger population, such as Generation Z, because of greater dependence on online platforms for banking operations. In this research, the prevalence and effects of bank frauds within the digital space, particularly within Chennai Corporation, and how the scams affect the financial security, trust, and behavioral patterns of Gen-Z consumers will be covered. The fraudsters are using new strategies to manipulate customers due to the increased utilization of mobile banking, internet transactions, and digital wallets. This leads to huge monetary losses and undermines user trust. The research methodology used here is a mixed method data collection approach to study Gen-Z bank customers in Chennai by considering both the quantitative survey and qualitative interviewing to gain a better insight into attitudes, vulnerabilities, and coping strategies for the individuals confronted with digital banking frauds. This study further examines how advancements in technology, such as phishing, identity theft, and social engineering, help fraudulent activity. From this study, understandably, an escalating trend has been evidenced towards fraudulent activities where the victims have been younger bank customers; it is a prevalent incident in which fraudulent activity occurs with social network scams, false apps, and phishing emails. With the behavior change changing the usage pattern of Gen Z online banking, belief in these online banking interfaces is lost along with the monetary loss. The research underlines the importance of more powerful cybersecurity controls, more stringent regulation, and more awareness campaigns to secure users, especially the new generations, against online banking frauds. To put everything into context, this research invokes the need to educate Gen Z on online scams and hence invokes a more secure online banking system, where technological advancements would go hand in hand with increased security measures safeguarding the user from threats in the online hub.

Key words : Bank Scams, digital hub, Gen Z

INTRODUCTION

Digital banking has revolutionized the processing of financial transactions, offering customers all over the world convenience, speed, and accessibility. Bank scams, also known as banking frauds, are a collection of deceptive practices aimed at illegally obtaining money, assets, or confidential information from financial institutions or their

clients.

The topic of discussion will be global bank fraud, with an emphasis on the scope of the issue and its effects on financial stability, consumer confidence, and economic expansion as a whole. Furthermore, it will highlight the steps being taken by financial institutions, governments, and global organizations to address and mitigate these risks.

THEORETICAL BACKGROUND

Bank frauds are today one of the most pressing problems for the global financial community, especially considering the rapid growth of digital banking and financial technologies. Bank frauds are of great concern not only to the banks but also to their clients, investors, and the economy in general. A theoretical framework that distinguishes the kind of bank scams, their cause, impact, and mechanisms through which they must be prevented and detected is indispensable for an integral solution to this issue. This Research aims at analyzing the different components of such a framework and presenting a systemic view of the way scams operate in banks, their impact, and how scams can be averted.

BANK – Indian Company Act 1936 has defined Bank as "A Banking Company which accepts deposits in current account or otherwise and satisfies cheques or promissory notes."

BANK SCAM – Banking scam refers to a fraudulent attempt to obtain someone's confidential monetary details such as passwords, credit card number, or banking account numbers.

TYPES OF BANK FRAUD: There are different bank cons that scammers use to get individuals or businesses to lose funds or share private data. Some of the common types follow below:

- Phishing Scams
- Smishing (SMS Phishing)
- Card Skimming
- Money Mule Scams
- Investment Fraud
- Vishing (Voice Phishing)
- Bank Impersonation Scams
- Account Takeover
- Fake Loan Scams

IMPORTANCE OF THE STUDY

The increasing reliance on digital banking in Chennai, particularly among the Gen-Z population, has given rise to significant concerns about online bank scams. As the most digitally active demographic, Gen-Z often lacks comprehensive financial literacy, making them especially vulnerable to fraud. This study is crucial in identifying the types and frequency of scams affecting young users within the Chennai Corporation area. By understanding their awareness levels, behavior patterns, and the psychological and financial impacts they face, the study aims to support the development of effective prevention strategies. It also provides valuable insights for banks, cybersecurity agencies, educational institutions, and policymakers to strengthen security measures, launch targeted awareness

campaigns, and design interventions tailored to this demographic. Furthermore, analyzing these trends within a major urban digital hub like Chennai helps assess the broader socioeconomic impact of such scams on youth and fosters more resilient digital financial ecosystems.

SIGNIFICANCE OF THE STUDY

This study is significant as it focuses on the growing threat of bank scams in the digital space, specifically targeting Gen-Z users within the Chennai Corporation area. As digital banking becomes more widespread, young individuals who are highly active online are increasingly exposed to sophisticated frauds. The research helps in identifying the key vulnerabilities faced by this demographic and provides insights into their awareness, response patterns, and the consequences they endure. By analyzing these factors, the study contributes to the development of more effective digital literacy programs, improved banking security systems, and policy interventions tailored to safeguard young users. Moreover, the findings serve as a valuable resource for banks, educators, cybersecurity professionals, and local authorities to implement targeted strategies that can reduce financial fraud and promote safer digital banking practices in urban regions like Chennai.

RESEARCH GAP

Despite the increasing prevalence of digital banking and the rise in cyber fraud incidents, there is a significant lack of focused research on how bank scams specifically impact Gen-Z in metropolitan areas like Chennai. Most existing studies tend to examine digital fraud in a broad context, often overlooking the unique vulnerabilities, behaviors, and digital habits of Gen-Z users, who are among the most active participants in online banking. Additionally, there is limited literature that explores the psychological, social, and financial consequences of such scams on young urban users. Moreover, the specific context of Chennai as a growing digital hub has not been sufficiently studied in relation to localized scam patterns and response mechanisms. This research aims to address these gaps by providing in-depth, demographic-specific, and region-specific insights that can inform better cybersecurity education, preventive strategies, and policy frameworks targeted at protecting Gen-Z users in Chennai.

RESEARCH METHODOLOGY

The research design employed for this study is descriptive in nature.

COLLECTION OF DATA

The research utilized a combination of primary and secondary data sources. Primary data was gathered using a meticulously designed questionnaire distributed via Google Forms. In contrast, secondary data was sourced from various magazines and academic journals.

STATISTICAL ANALYSIS

The data gathered from the questionnaire is examined using percentage analysis, Descriptive statistics, Inferential statistics, chi-square tests, One way ANOVA and Correlation to interpret the findings.

SAMPLING PROCEDURE

The Sampling Procedure consists of several components as follows:

Population: The Population contained in Chennai Corporation.

Sampling Frame: The Convenience Sampling frame tested for the research.

Sample Size: Sample Size counted as 95 respondents.

Sampling Tools: Questionnaire and Survey method used as a Sampling Tool in this Research.

OBJECTIVES OF THE STUDY:

1. To identify the common types of bank scams and to explore the consequences on economic growth and financial inclusion.
2. To analyse the impact on bank scams on consumer confidence in Digital Banking.
3. To examine the mental trauma caused to human well-being in effect of bank scams.
4. To assess the effectiveness of current fraud prevention measures to provide policy recommendations.

LIMITATIONS OF THE STUDY

Every Coin has two sides. Even though The Study has some advantages. There are some limitations. They are as follows:

- This study was limited by a small sample size, which may affect the generalizability of the findings to a larger population.
- Due to time constraints, the study only examined short-term effects, and long-term impacts were not assessed.
- Uncontrollable external factors, such as economic and political changes, may have influenced participants' responses, potentially affecting the study's conclusions

DATA ANALYSIS AND INTERPRETATION

TABLE – 1 Construct Scale: Awareness of Bank Scams.

Awareness of Bank Scams	N	Mean	Std. Deviation	Variance
Fake loan offers	95	1.48	0.599	0.359
Card skimming or cloning	95	1.47	0.599	0.358
Lottery or Prize scams	95	1.47	0.599	0.358
SMS or text message scams	95	1.49	0.599	0.359
Phishing emails	95	1.47	0.599	0.358
Fake phone calls	95	1.48	0.599	0.359
Fake bank websites	95	1.48	0.599	0.359
Valid N (listwise)	**95**			

Source: Primary Data

INTERPRETATION:

The data presents findings on the awareness levels of different types of bank scams among 95 participants.

The mean awareness scores for all scam types range from 1.47 to 1.49, with a standard deviation of 0.599 and a variance of approximately 0.358–0.359. The mean values for all scam types are quite similar (between 1.47 and 1.49), suggesting that awareness is evenly distributed across different scams. The standard deviation is the same for all scams (0.599), indicating minimal variation in responses and people's awareness levels are very similar across different types of fraud. Variance is Low (≈ 0.358–0.359). This means that the responses are closely clustered around the mean. There is little variation in how people rated their awareness of different scams.

Table No 2: Chi – Square Test on Outcome of the experience with bank scams and extent of the impact caused by bank scams.

Null Hypothesis (H0): There is no association between Outcome of the experience with bank scams and extent of the impact caused by bank scams.

Alternative Hypothesis (H1): There is an association between Outcome of the experience with bank scams and extent of the impact caused by bank scams.

THE OUTCOME OF YOUR EXPERIENCE WITH THE SCAM	**EXTENT OF THE IMPACT CAUSED BY BANK SCAMS.**			**CHI-SQUARE VALUE**	**P VALUE**
	Extreme	**Moderate**	**Low**		
Money was lost	3	3	8		
No financial loss	0	13	9	11.751[a]	0.019
Effect on mental trauma	0	9	5		
TOTAL	3	25	22		

Source: Computed Data

RESULT:

Since p-value (0.019) is less than 0.05, The Null Hypothesis was rejected at 1% of significance. This suggests a statistically significant association between the Outcome of the experience with bank scams and extent of the impact caused by bank scams.

TABLE 3 Correlation between Overall Awareness on Bank Scams and Measures to Prevent the Bank Scams.

Correlations		
PARTICULARS	**OVERALL AWARENESS**	**MEASURES TAKEN TO PREVENT**

OVERALL AWARENESS	Pearson Correlation	1	0.75
	Sig. (2-tailed)		0.00
	N	50	50
MEASURES TAKEN TO PREVENT	Pearson Correlation	0.75	1
	Sig. (2-tailed)	0.00	
	N	50	50

Descriptive Statistics

Particulars	Mean	Std. Deviation	N
OVERALL AWARENESS	9.1800	2.93251	50
MEASURES TAKEN TO PREVENT	22.9000	2.22463	50

Source: Computed Data

INTERPRETATION:

The Pearson correlation between Overall Awareness and Measures Taken to Prevent Bank Scams is 0.75. This indicates a strong positive correlation between the two variables. A higher awareness of bank scams is strongly associated with taking more preventive measures. Since $p < 0.05$, the correlation is statistically significant and there is a strong and meaningful relationship between the Overall Awareness on Bank Scams and Measures to Prevent the Bank Scams.

TABLE 4- ANOVA between Overall Awareness on Bank Scams and Age:

Null Hypothesis: There is no statistically significant difference between Overall awareness on Bank scams and Age.

Alternate Hypothesis: There is a statistically significant difference between Overall awareness on Bank scams and Age.

ANOVA							
Particulars			**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
	(Combined)		64.232	4	16.058	.107	.107
Between Groups		Unweighted	57.252	1	.010	7.214	.010
	Linear Term	Weighted	41.760	1	.027		.027
		Deviation	22.471	3	.427	.944	.427
Within Groups			357.148	45	7.937		

Total			421.380	49			

Source: Computed Data

INTERPRETATION:

ANOVA (Analysis of Variance) tests whether there are statistically significant differences between the means of multiple groups. This tests if there is any significant difference between the groups in Overall Awareness. Since p = 0.107 is greater than 0.05, there is no statistically significant difference among the group.

FINDINGS FROM THE STUDY:

Banking Services Usage:

- Mobile banking is the most preferred service (48.4%).
- Only 3.2% rely solely on traditional in-person banking.
- 24.2% use a combination of banking services.

Awareness & Victimization of Bank Scams:

- 81.1% of respondents are aware of bank scams.
- Despite awareness, 52.6% have been victims of bank scams.
- Phishing emails (40%) and fake websites (28%) are the most common scam tactics.

Response to Scams:

- A majority (64%) ignored the scams, while only 20% reported them to banks.
- Mental trauma was reported by 28% of scam victims.

Impact of Scams:

- 50% of respondents faced moderate effects, while 6% experienced extreme consequences.
- 44% did not suffer financial losses, but 28% lost money.

Perception of Government and Banking Measures:

- 62% believe government measures against bank scams are effective.
- 40% receive frequent bank communication about fraud prevention.
- 44% of respondents agree that regulatory policies are effective, while 30% disagree.

Preventive Measures Taken:

- Most respondents avoid sharing personal details (Mean = 3.98).
- Monitoring bank statements regularly has the lowest variance, indicating strong consensus on its importance.

Statistical Findings:

- No significant association was found between gender and victimization of scams.
- A significant association was found between gender and awareness of bank scams.
- Gender significantly influences banking service usage.
- A strong positive correlation exists between awareness of bank scams

and preventive measures taken.

SUGGESTIONS

1. Strengthen Awareness Campaigns:

Since 81.1% of respondents are aware of bank scams, targeted awareness programs should be conducted for the remaining 18.9% who lack awareness.

2. Focus on Digital Banking Security:

As 48.4% of respondents use mobile banking, banks should strengthen security measures such as biometric authentication and secure OTP verification.

3. Encourage Reporting of Scams:

Since 64% of victims ignored scams, banks and authorities should introduce easier and more confidential reporting mechanisms.

4. Provide Educational Programs for Young Adults:

With 28.4% of respondents aged 18-24, financial literacy programs should be implemented in colleges to educate them on online fraud.

5. Increase Security Communication from Banks:

As 24% of respondents receive fraud prevention messages only once a year or less, banks should increase the frequency of security alerts.

6. Develop AI-Based Fraud Detection:

AI-driven fraud detection should be implemented in banks to identify suspicious transactions and notify customers in real-time.

7. Address Psychological Effects of Fraud:

As 28% of victim's experienced mental distress, banks and consumer protection agencies should provide counseling and financial recovery support.

8. Stricter Verification for Financial Transactions:

Stronger KYC and customer verification processes should be mandated to prevent identity theft and fraud.

9. Enhance Two-Factor Authentication (2FA):

Since mobile banking is widely used, enabling mandatory two-factor authentication for all transactions can reduce unauthorized access.

10. Conduct Fraud Awareness Workshops in High-Risk Zones:

With Zone 12 and Zone 15 having the highest respondents (11.6% each), localized fraud awareness campaigns should be conducted in these areas.

11. Target Working Professionals with Awareness Programs:

As 55.8% of respondents are employed, corporate awareness sessions should be conducted to educate working individuals about phishing emails and cyber fraud.

12. Improve Government Action Against Bank Scams:

Since 22% of respondents are unsure about the effectiveness of government measures, authorities should improve transparency and publicize their anti-fraud initiatives.

13. Strengthen Legal Action Against Scammers:

A fast-track legal process should be implemented to ensure timely punishment for cybercriminals and fraudsters.

14. Ban Unverified Financial Apps:

Stricter regulations should be imposed on financial apps that do not comply with banking

security standards to prevent unauthorized fund transfers.

15. Enhance Fraud Prevention in Retirement Funds:

Since 13.7% of respondents are retired, pension funds and senior citizen banking services should have additional fraud prevention measures.

16. Implement Community-Based Scam Prevention Initiatives:

A peer network system should be developed where victims and experts can share experiences to warn others about scam tactics.

17. Strengthen Anti-Phishing Regulations:

With 40% of scam victims receiving phishing emails, email service providers and banks should collaborate to block scam-related emails.

18. Improve Cybersecurity Training for Bank Employees:

Bank staff should undergo continuous training to identify fraudulent transactions and assist customers in preventing financial fraud.

19. Expand Cybercrime Helplines:

A dedicated 24/7 cybercrime helpline should be introduced to assist scam victims in real-time.

20. Encourage Financial Vigilance Among Consumers:

Customers should be educated on safe banking habits such as not sharing OTPs, regularly updating passwords, and verifying banking communications.

CONCLUSION

This research provides a comprehensive analysis of bank scams and their impact on individuals, focusing on awareness levels, victimization, and preventive measures. The study reveals that while a significant portion of respondents (81.1%) are aware of bank scams, a concerning 52.6% have fallen victim to fraudulent activities. Phishing emails (40%) and fake websites (28%) emerged as the most common tactics used by scammers, highlighting the evolving nature of cyber threats.

One of the critical findings is the lack of active reporting, with 64% of victims choosing to ignore scams rather than report them to banks or authorities. This underscores the need for stronger awareness campaigns and simplified reporting mechanisms to encourage proactive action against fraud. Additionally, the study found that the psychological impact of bank scams is substantial, with 28% of victims experiencing mental distress even if they did not suffer financial losses.

The research also identifies a gap in financial literacy, especially among younger individuals (18- 24 years), who constitute a significant portion (28.4%) of the study's respondents. With mobile banking being the most preferred banking method (48.4%), it is imperative that financial institutions enhance their security protocols, including mandatory two-factor authentication and real-time fraud alerts.

Government measures to combat bank scams were perceived as effective by 62% of respondents, but 22% remained uncertain about their impact. This highlights the need for greater transparency, stronger regulatory frameworks, and stricter legal

actions against cybercriminals.

Overall, this study emphasizes the urgent need for increased financial education, improved banking security, and more proactive consumer protection measures. By implementing the suggested strategies ranging from fraud prevention training to enhanced banking regulations stakeholders can collectively work towards reducing the prevalence of bank scams and ensuring a safer financial environment for all consumers. Further research in this domain can focus on emerging scam tactics and the role of artificial intelligence in fraud detection to develop even more effective prevention mechanisms.

REFERENCES

BOOKS:

- Harris, R. (1999). The Laws of the Ancient Near East: A Critical Study. Cambridge University Press.
- Morris, I. (2012). The Ancient Economy: A History. University of California Press.
- Kearsley, R. (2007). Coinage and Currency in Ancient Rome. Oxford University Press.
- Foxhall, L. (1991). Trade, Traders, and Trade Routes: Ancient Greek Economy in Context. Oxford University Press.
- Cicero, M. T. (1927). On the Duties of the Magistrate. Harvard University Press.'
- Scheidel, W. (2009). The Roman Economy: Studies in the Ancient Economy. Princeton University Press.

JOURNALS:

- Reserve Bank of India (RBI). (2020). Annual Report on Cyberfraud Trends and Cybersecurity Measures in the Banking Sector. RBI Press.
- The Karur Vysya Bank Scam." The Hindu, 1995.
- "Chennai Co-operative Bank Fraud." Business Today, 2003.
- "Tamil Nadu Mercantile Bank Scam." The Economic Times, 2011.
- "Vasantha Bank Fraud." Deccan Chronicle, 2017.