Archives available at journals.mriindia.com

International Journal on Research and Development - A Management Review

ISSN: 2319 - 5479

Volume 15 Issue 01, 2026

Consumer Perception With Regards To Frauds in Mobile Banking Reference to Chennai

[1]Ms. D. Vinithra, [2]Dr. G. K.Lavanya

[1]Research Scholar,Shri Shankarlal Sundarbai Shasun Jain college for Women

[2]Research Supervisor,Shri Shankarlal Sundarbai Shasun Jain college for Women

Peer Review Information

Submission: 10 Feb 2026

Revision: 22 Feb 2026

Acceptance: 03 March 2026

Keywords

Mobile banking, frauds, phishing, sim swap, fake apps

Abstract

Mobile banking has transformed financial services by providing ease, rapidity and accessibility. Unauthorized and unlawful activity carried out through mobile application is known as mobile banking frauds. As the technology develops and increase in use of mobiles the consumers are exposed to new risks such as phishing, sim swap, fake apps, or code and malware attacks. The study aims to examine the awareness level of frauds in mobile banking, identify most common frauds in mobile banking, analyse the security satisfaction level in mobile banking, grievances faced by the consumers due to mobile banking frauds and to examine measures taken by banks for prevention of frauds. It is concluded from the study that the majority of respondents are male belonging to the age group 29-44 yrs. Phishing is the most common fraud in mobile banking. Major grievances faced by the consumers is immediate account blocking and authentication measures from banks to prevent frauds is effective.

Introduction

Mobile banking fraud encompasses illicit and unlawful actions executed using mobile banking applications. Unauthorized and unlawful activity carried out via mobile banking applications is known as mobile banking fraud. In order to obtain unauthorized access to bank accounts, steal confidential financial information, or carry out fraudulent transactions, fraud takes advantage of flaws in mobile banking apps, user devices, or behavior. Financial organizations and consumers are increasingly concerned about theft due to the growing reliance on mobile banking.

Banks have implemented many security measures including end-to-end encryption, multi-factor authentication, biometric verification, and AI-driven fraud detection. Consumer confidence in these actions still remains low . While some consumers are relieved, others still have complaints about things like poor chatbot support, delayed fraud alerts, and a dearth of awareness initiatives. Therefore, this study aims to investigate consumer knowledge of mobile banking frauds, the most prevalent fraud types, assess consumer satisfaction with security features, identify complaints, and assess the steps banks have made to prevent fraud.

Statement of Problem

With the simplicity, effectiveness, and accessibility, mobile banking has become an essential part of financial services.Even though banks continue to provide a variety of digital services, many consumers face challenges like lack of awareness, security, technological issues, and exposure to online fraud. The increase in mobile banking fraud cases has brought attention to worries about the security and reliability of digital banking platforms.

Need For Study

The rapid growth in using mobile banking has increased worries about mobile banking frauds. Although digital financial services are convenient, consumers' awareness of various mobile banking frauds and the security measures that banks have put in place is unclear. Evaluating the efficacy of current protections requires identifying frequent scams, measuring security satisfaction levels, and looking into consumers complaints.

Objective of Study

- To examine the awareness level of frauds in mobile banking.
- To identify most common frauds in mobile banking
- To analyse the security satisfaction level in mobile banking
- To bring out grievances faced by the consumers due to mobile banking frauds.
- To examine measures taken by banks for prevention of frauds

Limitation of Study

- The data was collected from the respondents in chennai city therefore the conclusion drawn may not be applicable to other areas.
- It is mainly focused on mobile banking.
- The results are limited based on the number of respondents.

Review of Literature

- **R.Johan Ananth et.al (2024)** examined issue and challenges faced in mobile banking consumer perception.The aim of the study is to examine the issues including security concerns, privacy hazards, usability difficulties, and technological obstacles.The conclusion of the study sheds attention on the many intricate challenges that mobile banking faces, emphasizing issues like security, usability, and technological constraints. Protecting confidential financial data requires putting strong cybersecurity safeguards into place and raising user awareness.
- **G.Sankararaman (2024)** analysed customer awareness on security issues and threats in digital banking in chennai.The purpose of the study is to assess consumers' general awareness of security risks and problems in online banking.According to the conclusion there is a lot of for improvement, especially among specific demographic groups, even if a significant proportion of consumers are aware of cyber security precautions and best practices. Customer education initiatives should be customized to target particular age groups, educational backgrounds, and digital literacy levels.
- **KR Kaojia et.al(2024)** investigated cybercrime in India in the context of the banking industry, a critical analysis of consumer perception.The aim of the study is to find out how Bekasi, Indonesia, commercial bank customers view and trust fraud when utilizing mobile banking services.The results of the study demonstrate that the perception of fraud influences the use of mobile banking services,trust influences the use of mobile banking services,the perception of fraud and trust simultaneously influence the use of mobile banking services.
- **M.Sanjana et.al(2024)** conducted a research on the level of awareness of online banking frauds among middle aged category with special reference to kumbalangi panchayath.The study aims in to determine Kumbalangi Panchayat adults' awareness of e-banking fraud, to learn about the many types of financial fraud and how they affect bank clients and to assess the degree of satisfaction with the banking redressal system.The majority of the respondents were aware of numerous internet banking fraudulent activities, according to the study findings. It is unfortunate that some of them still have a history of banking fraud even though they were aware of it.
- **K.S. Balaji Venkatesh** analysed consumer awareness and perceived risk of ebanking services.The study examines customers' knowledge of e-banking services and the perceived level of risk associated with their use. The results suggest that while the majority of consumers are aware of e-banking services, they typically do not fully understand the risks associated with them. The perceived threat is mostly caused by security concerns, such as the potential for fraud and identity theft.

Conceptual Frame Work

Unauthorized and unlawful activity carried out via mobile banking applications is known as mobile banking fraud. In order to obtain unauthorized access to bank accounts, steal confidential financial information, or carry out fraudulent transactions, this fraud takes advantage of flaws in mobile banking apps, user devices, or behavior.

Types of Mobile Banking Frauds

Phishing-SMS/Whatsapp Scam

Phishing means sending SMS or WhatsApp messages pretending to be banks. These messages frequently contain urgent warnings or alluring offers that deceive users into clicking on harmful links. These links take consumers to

phony websites where they unintentionally divulge private information such card numbers, OTPs, or login credentials, allowing fraudsters to commit identity theft and illegal transactions.

Vishing-Phone Call Scam

Vishing refers to posing as bank employees or regulatory agencies over the phone in order to trick clients into divulging private information such as account numbers, OTPs, or CVV codes. Fraudsters obtain access to accounts and carry out fraudulent transactions, resulting in immediate financial losses, by taking advantage of fear or haste, such as threats of account suspension.

QR Code

In QR scams,fraudsters deceive consumers into scanning harmful QR codes under the disguise of offer, discounts, or cash.The scan is a quick and dishonest approach to steal money straight from mobile banking apps because it authorizes a payment from the victim's account to the fraudster rather than crediting funds.

Sim Swap

SIM swap fraud happens when scammers trick telecom companies into giving them a replica SIM card, which enables them to intercept OTPs and transaction notifications intended for the victim. Large-scale money transfers result from fraudsters gaining unauthorized access to mobile banking accounts and circumventing authentication procedures by controlling the victim's cellphone number.

Fake App

Fake apps are fraudulent applications created to mimic authentic banking apps in order to deceive consumers into downloading them. Once installed, these apps provide fraudsters with direct access to accounts by stealing personal information, OTPs, and login passwords. They take advantage of users' faith in app stores and imitate official branding to look authentic.

Malware Attack

By installing malicious software on a user's phone using fake apps, links, or attachments, fraudsters can monitor behavior, record keystrokes, or obtain private information. Certain malware targets banking apps in particular, giving fraudsters the ability to steal login credentials and carry out illegal activities without the user's awareness.

Data Analysis

Demographic Factors of Respondents

Table 1: Demographic Factors of Respondents

DEMOGRAPHIC FACTORS	PARTICULAR	NO OF RESPONDENTS	PERCENTAGE
Gender	Male	77	73.3
	Female	28	26.7
	Total	105	100.0
Age	18-28yrs	40	38.1
	29-44yrs	44	41.9
	45-60yrs	18	17.1
	above 60 yrs	3	2.9
	Total	105	100.0
Occupation	Upto 12th	3	2.9
	Diploma	6	5.7
	Undergraduate	67	63.8
	Post Graduate	24	22.9
	Professional	5	4.8

	Total	105	100.0
Educational qualification	Student	3	2.9
	Homemaker	3	2.9
	Private employee	77	73.3
	Govt employee	8	7.6
	Business	12	11.4
	others	2	1.9
	Total	105	100.0
Monthly income	Below Rs.10,000	5	4.8
	Rs.10,001-Rs.25,000	30	28.6
	Rs.25,001-Rs.45,000	55	52.4
	Above Rs.45,001	15	14.3
	Total	105	100.0
Marital status	married	58	55.2
	unmarried	47	44.8
	Total	105	100.0

Source:Primary data

Inference

From the above table it is inferred that the majority of the respondents are male with 73.3% and female with 26.7%.

Majority of the respondents belong to age group of 29-44 yrs with 41.9% followed by 18-28 yrs with 38.1%,45-60yrs with 17.1% and above 60 yrs with 2.9%

Most of the respondents belong to categories of under graduates with 63.8% followed by post graduates with 22.9%,diploma with 5.7%,professional with 4.8% and upto 12th 2.9%.

In this study,it is observed that the majority of respondents are private employees with 73.3% followed by business with 11.4%,govt employees with 7.6%,home maker and student with 2.9% and others with 1.9%.

Majority of the respondents monthly income of Rs.25,001-Rs.45,000 with 52.4% followed by Rs.10,001-Rs.25,000 with 28.6%,above Rs.45,0001 with 14.3% and below Rs.10,000 with 4.8%.

Most of the respondents are married with 55.2% and unmarried with 44.8%.

Purchasing Behaviour of Respondents

Table 2: Purchasing Behaviour of Respondents

PURCHASING BEHAVIOUR	PARTICULARS	NO OF RESPONDENTS	PERCENTAGE
	sbi	27	25.7
	iob	29	27.6
	indian bank	13	12.4

Account holding in which bank	hdfc	16	15.2
	citi union	5	4.8
	kvb	13	12.4
	axis	2	1.9
	Total	105	100.0
Type of account	savings account	98	93.3
	current account	7	6.7
	Total	105	100.0
Frequency of using mobile banking	Daily	12	11.4
	Weekly	37	35.2
	Monthly	49	46.7
	Rarely	7	6.7
	Total	105	100.0
Mobile banking services is used	Account Information Services	52	49.5
	Fund Transfer Services	28	26.7
	Payment Services	16	15.2
	Deposit Services	3	2.9
	Loan & Credit Services	2	1.9
	Investment and insurances	1	1.0
	Card Management Services	1	1.0
	Security & Control Services	2	1.9
	Total	105	100.0
Aware of frauds in mobile banking	yes	95	90.5
	no	10	9.5
	Total	105	100.0
	Phishing-SMS Scam/Whatsapp	61	58.1
	Vishing-Phone call scam	22	21.0

Type of frauds faced by consumers	QR scams	9	8.6
	SIM swap	9	8.6
	fake apps	3	2.9
	Malware attack	1	1.0
	Total	105	100.0
Loss in fraud	Less than Rs.500	29	27.6
	Rs.501-Rs.1000	19	18.1
	Rs.1001-Rs.5000	47	44.8
	Rs.5001-Rs.10,000	9	8.6
	Above Rs.10,001	1	1.0
	Total	105	100.0

Source:primary data

Inference

From the above table it is inferred that the majority of the respondents belong to iob with 27.6% followed by sbi with 25.7%,hdfc bank with 15.2%,indian bank and KVB with 15.2%,citi union with 4.8% and axis with 1.9%.

The majority of the respondents have a savings account with 93.3% and current account with 6.7%.

Majority of the respondents use mobile banking monthly with 46.7%,weekly with 11.4% ,daily with 11.4% and rarely with 6.7%.

Most of the respondents use mobile banking for account information services with 49.5%,fund transfer service with 26.7%, payment services with 15.2%, deposit services with 2.9%, loan and credit services with 1.9%, investment,insurance and card management services with 1.0%

The majority of the respondents are aware of mobile banking frauds with 90.5% and are not aware of mobile banking frauds with 9.5%.

The majority of the respondents have experienced phishing with 58.1% followed by vishing with 21.1%,sim swap and qr code with 8.6%,fake app with 2.9%,malware attack with 1.0%.

Majority of the respondents have lost Rs.1001-Rs.5000 with 44.8%,Less than Rs.500 with 27.6%,Rs.501-Rs.1000 with 18.1%.Rs.5000-Rs.10,000 with 8.6% and above Rs.10001 with 1.0%.

Descriptive Statistics

Most Common Frauds in Mobile Banking

The mean and standard deviation has been formed to analyse most common frauds in mobile banking is interpreted in the following table

Table 3: Mean and Standard Deviation of Most Common Frauds in Mobile Banking

Most common frauds in mobile banking	Mean	SD	Rank
Phishing-SMS/Whatsapp Scam	4.51	.761	1
Vishing-phone call scam	4.28	.778	2
QR Scam	4.08	.948	3
sim swap	4.18	.959	4
Fake app	4.19	.982	5
malware attack	3.90	1.070	6

Source:Computed data

Inference

From the above table it is observed that most common frauds are phishing which is ranked first followed by vishing is ranked second,qr scam is ranked third and the malware attack is ranked least.

Thus,the above table clearly states that phishing-sms/whatsapp is the most common fraud and the least common fraud is malware attack.

Grievances Faced By the Consumers Due To Mobile Banking Frauds

The mean and standard deviation has been formed to analyse grievances faced by the consumers due to mobile banking frauds

Table 4: Mean and Standard Deviation of Grievances Faced By the Consumers Due To Mobile Banking Frauds

GRIEVANCES	Mean	SD	Rank
Immediate account blocking	4.43	.732	1
Financial loss	4.25	.794	2
Delay in complaint resolution	4.19	.889	5
Lack of awareness and guidance	4.32	.814	3
Inadequate customer support	4.23	.869	4

Source:Computed data

Inference

From the above table it is observed that immediate account blocking has ranked first followed by financial loss has ranked second,lack of awareness and guidance ranked third and delay in complaint resolution has ranked last.

Thus the above table clearly states that major grievances faced is immediate accounting blocking and least faced is delay in complaint resolution.

Security Satisfaction Level of Mobile Banking

The mean and standard deviation has been formed to analyse the security satisfaction level of mobile banking is interpreted in the following table.

Table 5: Mean and Standard Deviation of Security Satisfaction Level of Mobile Banking

Security satisfaction level of mobile banking	Mean	Std. Deviation	rank
Multi factor authentication	4.57	.633	1
Transaction alerts via sms/email	4.32	.714	2
Fraud alerts/notification	3.74	1.169	6
Card blocking/unblocking	4.26	.809	3
Data privacy and encryption	4.13	.867	4
Ai chat support-Dispute transaction	4.03	1.042	5

Source : Computed data

Inference

From the above table it is observed that multi authentication has ranked first followed by transaction alters,card blocking/unblocking and the least ranked is satisfied with fraud alerts and notification.

Thus,the above table states that security satisfaction level with multi authentication in mobile banking.They are not satisfied with fraud alerts or notification.

Inferential Statistics

Measures Taken By Bank Are Effective In Preventing Mobile Banking Frauds

The Friedman test is used to analyse the difference among mean rank measures taken by banks that are effective in preventing mobile banking frauds.

H_0: There is no significant difference within measures taken by banks that are effective in preventing mobile banking frauds

H_1: There is a significant difference within measures taken by banks that are effective in preventing mobile banking frauds

Table 6: Friedman Test for Measures Taken By Bank Are Effective In Preventing Mobile Banking Frauds

Measures taken by banks are effective in preventing mobile banking frauds	**Mean**	**Rank**	**Chi square**	**Df**	**P value**
Authentication	4.13	1	48.877	5	.000
Transaction safeguard	3.58	3			
Ai fraud detection and chatbots	3.61	2			
End to end encryption	3.45	4			
Awareness through msg, notification	3.24	5			
Grievances Redressal	2.99	6			

Source:Computed data

Inference

There is a significant difference within measures taken by banks that are effective in preventing mobile banking frauds,since p value is less than 0.05.

Authentication is ranked first followed by ai fraud detection and chatbots and transaction safeguard and the last rank is given to grievances redressal.

Hence it is concluded that authentication measures taken by banks are effective in preventing mobile banking frauds and the least effective measure is grievances redressal.

Relationship between Ages With Respect To Grievances Faced By the Consumers Due To Mobile Banking Frauds

ANOVA is used to analyse the relationship between age with respect to grievances faced by the consumers due to mobile banking frauds

H0: There is no significant difference between age and grievances faced by the consumers with regards to fraud.

H1: There is a significant difference between age and grievances faced by the consumers with regards to fraud.

Table 7: ANOVA Showing Relationship between Ages With Respect To Grievances Faced By the Consumers Due To Mobile Banking Frauds

GRIEVANCES		**Sum of Squares**	**df**	**Mean Square**	**F**	**Sig.**
Immediate account blocking	Between Groups	7.183	3	2.394	4.983	.003
	Within Groups	48.532	101	.481		
	Total	55.714	104			
Financial loss	Between Groups	11.753	3	3.918	7.353	.000
	Within Groups	53.809	101	.533		
	Total	65.562	104			
	Between Groups	4.162	3	1.387	1.796	.153

Delay in complaint resolution	Within Groups	78.028	101	.773		
	Total	82.190	104			
Lack of awareness and guidance	Between Groups	6.776	3	2.259	3.667	.015
	Within Groups	62.215	101	.616		
	Total	68.990	104			
Inadequate customer support	Between Groups	8.261	3	2.754	3.959	.010
	Within Groups	70.254	101	.696		
	Total	78.514	104			

Source:Computed data

Inference

Since p value is less than 0.05,the null hypothesis is rejected at 5% level of significance.Hence it is concluded that there is a significant difference between age and grievances faced by the consumers due to mobile banking frauds.

Findings

From the study it is observed that the majority of the respondents are male with 73.3% and female with 26.7%.

It is found from the study that majority of the respondents belong to age group of 29-44 yrs with 41.9% followed by 18-28 yrs with 38.1%,45-60yrs with 17.1% and above 60 yrs with 2.9%

It is observed from the study that most of the respondents belong to categories of under graduates with 63.8% followed by post graduates with 22.9%,diploma with 5.7%,professional with 4.8% and upto 12th 2.9%.

It is found that the majority of respondents are private employees with 73.3% followed by business with 11.4%,govt employees with 7.6%,home maker and student with 2.9% and others with 1.9%.

In this study it is denoted that the majority of the respondents monthly income of Rs.25,001-Rs.45,000 with 52.4% followed by Rs.10,001-Rs.25,000 with 28.6%,above Rs.45,0001 with 14.3% and below Rs.10,000 with 4.8%.

The study indicated that most of the respondents are married with 55.2% and unmarried with 44.8%. It is found from the study that the majority of the respondents belong to iob with 27.6% followed by sbi with 25.7%,hdfc bank with 15.2%,indian b ank and KVB with 15.2%,citi union with 4.8% and axis with 1.9%.

The study found that the majority of the respondents have a savings account with 93.3% and current account with 6.7%.

In this study it is denoted that the majority of the respondents use mobile banking monthly with 46.7%,weekly with 11.4% ,daily with 11.4% and rarely with 6.7%.

It is observed that most of the respondents use mobile banking for account information services with 49.5%,fund transfer service with 26.7%, payment services with 15.2%, deposit services with 2.9%, loan and credit services with 1.9%, investment,insurance and card management services with 1.0%

The study indicated that the majority of the respondents are aware of mobile banking frauds with 90.5% and are not aware of mobile banking frauds with 9.5%.

It is observed from the study that the majority of the respondents have experienced phishing with 58.1% followed by vishing with 21.1%,sim swap and qr code with 8.6%,fake app with 2.9%,malware attack with 1.0%.

It is found that majority of the respondents have lost Rs.1001-Rs.5000 with 44.8%,Less than Rs.500 with 27.6%,Rs.501-Rs.1000 with 18.1%.Rs.5000-Rs.10,000 with 8.6% and above Rs.10001 with 1.0%.

It is observed from the study that most common frauds are phishing which is ranked first followed by vishing,qr scam and the malware attack is ranked least.It is found that phishing-sms/whatsapp is the most common fraud and the least common fraud is malware attack.

It is observed that immediate account blocking has ranked first followed by financial loss,lack of awareness and guidance and delay in complaint resolution has ranked last.It is found that major grievances faced is immediate accounting

blocking and least faced is delay in complaint resolution.

It is observed that multi authentication has ranked first followed by transaction alters,card blocking/unblocking and the least ranked is satisfied with fraud alerts and notification.

It is found that the security satisfaction level with multi authentication in mobile banking.They are not satisfied with fraud alerts or notification.

From the Fried man test it is inferred that there is a significant difference within measures taken by banks that are effective in preventing mobile banking frauds,since p value is less than 0.05.Authentication is ranked first followed by ai fraud detection and chatbots and transaction safeguard and the last rank is given to grievances redressal.Hence it is concluded that authentication measures taken by banks are effective in preventing mobile banking frauds and the least effective measure is grievances redressal.

From the Anova test it is found that Since p value is less than 0.05,the null hypothesis is rejected at 5%level of significance.Hence it is concluded that there is a significant difference between age and grievances faced by the consumers due to mobile banking frauds.

Suggestion

- Banks can provide regular fraud awareness campaigns through sms,email and app notification
- Banks should bring fraud helplines.
- Bank can allow temporary freeze option
- Consumers can use other features like investment,insurance and loan in mobile banking app
- Can bring new features in the app by just one tap for raising complaint registration
- Can use ai to detect and verify the payment person details.
- Consumers to verify senders IDs and avoid clickable links.
- Banks and telecoms can work together in blocking suspicious numbers from calls and sms.
- Regularly update mobile banking app

Conclusion

Mobile banking has grown to be a crucial component of financial transactions, providing accessibility and convenience to a diverse clientele. However, fraud hazards like phishing, vishing, QR frauds, SIM swaps, and fake applications have also increased as mobile banking apps have grown in popularity.Although most consumers are aware of these risks, their confidence in mobile banking is dependent not only on technical security but also on efficient fraud reporting, grievance resolution, and customer service. The study emphasizes that in order to guarantee consumer confidence in digital banking, banks must provide more security features, proactive awareness efforts, and compassionate service.

It is concluded from the study that the majority of respondents are male belonging to the age group 29-44 yrs.Phishing is the most common fraud in mobile banking.Major grievances faced by the consumers is immediate account blocking and authentication measures from banks to prevent frauds is effective.

Reference

Ananth, R & Thandayudhapani, S. (2024). A Study on Issues and Challenges Faced by Mobile Banking with Reference to Customer Perspective. Shanlax International Journal of Management. 11. 64-70. 10.34293/management.v11iS1-May.7838.

Sankararaman, G., & Suresh, S. (2024). A Study on the Customer Awareness on Security Issues and Threats in Digital Banking in Chennai. European Economic Letters, Volume14, (4), 559-574.

Kanojia, K. R., & Singh, R. K. (2024). CYBERCRIME IN INDIA IN THE CONTEXT OF THE BANKING INDUSTRY: A CRITICAL ANALYSIS OF CUSTOMER PERCEPTION. Russian Law Journal, 12(2), 136-141.

SANJANA, M., & FRANCIS, A. S. D. A. (2024). A STUDY ON THE LEVEL OF AWARENESS OF ONLINE BANKING FRAUDS AMONG THE MIDDLE-AGED CATEGORY WITH SPECIAL REFERENCE TO KUMBALANGI PANCHAYATH (Doctoral dissertation, St. Teresa's College (Autonomous) Ernakulam).

Venkatesh, K. B. (2023). Consumer Awareness and Perceived Risk of E-Banking Services: An Examination of Adoption and Usage Behaviour. Center for Development Economic, 10(16), 154-161.