IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Mobile App Frauds In Maharashtra: A Case Study On Fake Service Apps And Their Impact On Citizens

Author: Rohit Dattatray Kamble

Affiliation: XIT Group of Companies, Pune

Abstract: The rapid adoption of mobile-based financial services in India has created new opportunities for cybercriminals. Maharashtra, being one of the most digitally active states, has seen a surge in mobile app–related frauds where citizens are deceived into installing fake service applications or responding to fraudulent communications. This paper documents real cases from Maharashtra where victims lost significant funds due to fraudulent mobile apps impersonating banks and financial services. The study analyzes four detailed cases; ranging from fake bank KYC apps to trading scams; and categorizes their patterns of deception. Findings reveal that fraudsters exploit trust in banking institutions, use psychological manipulation such as urgency and fear, and leverage SMS, calls, and fake apps to execute scams. This research provides a systematic analysis of fraud patterns and concludes with strong recommendations for awareness, regulation, and institutional safeguards to mitigate such threats.

Keywords*: Mobile app fraud, Fake banking apps, Maharashtra cybercrime, UPI fraud, Financial scams*

1. Introduction

Mobile applications are now at the heart of India’s digital transformation. From UPI transactions to online savings schemes, citizens depend on mobile apps for daily financial activities. This transform has been particularly visible in Maharashtra, home to major financial hubs such as Mumbai and Pune. However, with this progress comes risk: cybercriminals exploit mobile apps to execute highly deceptive financial frauds.

In 2023–2024, Maharashtra Police’s Cybercrime Wing reported that mobile app fraud accounted for a substantial share of online fraud complaints. Victims often lose not just money but also confidence in digital services.

The objective of this study is threefold:

1. To document real-life mobile app fraud cases from Maharashtra.
2. To analyze the fraud techniques and psychological tactics used.
3. To provide actionable recommendations for citizens, institutions, and regulators.

2. Literature Review

Mobile app fraud is a global phenomenon. Studies highlight that fake apps often imitate legitimate banking or financial platforms, tricking users into revealing credentials (Gupta & Shukla, 2021).

In India, RBI and CERT-In advisories have repeatedly warned against fraudulent loan and trading apps (RBI, 2023; CERT-In, 2024). The National Crime Records Bureau also notes that Maharashtra consistently reports among the highest numbers of cyber fraud cases.

While existing literature explains malware design and fraud trends, there remains limited academic work focusing on real citizen experiences in Maharashtra. This study bridges that gap by presenting case-based analysis from actual victims.

3. Methodology

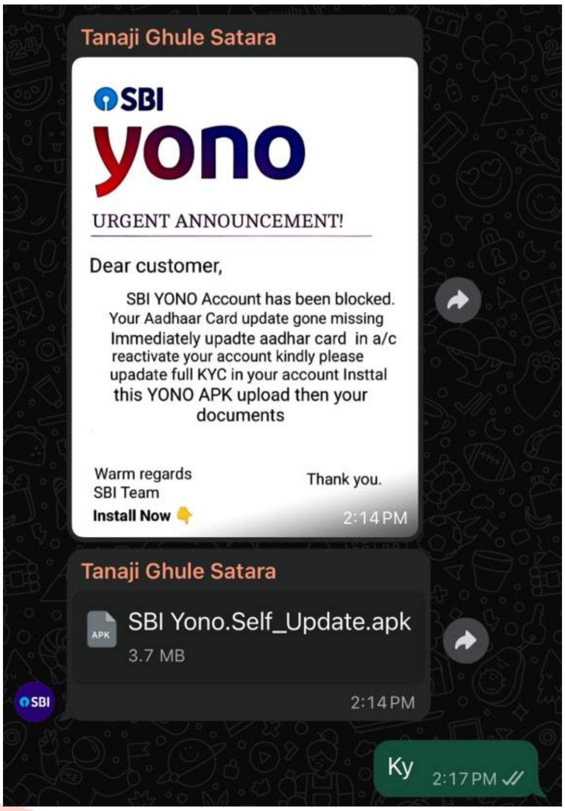
1. **Data Sources:** Over 150 reported cases collected from citizens across Maharashtra (for this paper, four illustrative cases are highlighted).
2. **Verification:** Each case was verified via screenshots, call records, and communication samples shared by victims.
3. **Categorization:** Frauds were grouped into patterns: fake KYC apps, fraudulent fund transfer scams, fake trading apps, and impersonation of bank officials.

Ethical Considerations: No sensitive personal data (like account numbers or personal identifiers) has been shared. All screenshots shown are anonymized. The focus is on fraud patterns, not individuals.

4. Case Studies / Findings

Case 1: Fake SBI KYC Update App

1. **Description:** Victim received an SMS urging them to update KYC or risk account suspension.
2. **Fraud Delivery:** A link led to a fake app mimicking the official SBI application.
3. **Impact:** Victim installed the app and entered credentials. Scammers accessed the account and siphoned off the victim's life savings.
4. **Key Manipulation:** Fear of account suspension and authentic-looking branding.



Tanaji Ghule Satara

SBI yono

URGENT ANNOUNCEMENT!

Dear customer,

SBI YONO Account has been blocked. Your Aadhaar Card update gone missing Immediately upadte aadhar card in a/c reactivate your account kindly please upadate full KYC in your account Insttal this YONO APK upload then your documents

Warm regards
SBI Team
Install Now 👇

Thank you.

2:14 PM

Tanaji Ghule Satara

SBI Yono.Self_Update.apk
3.7 MB

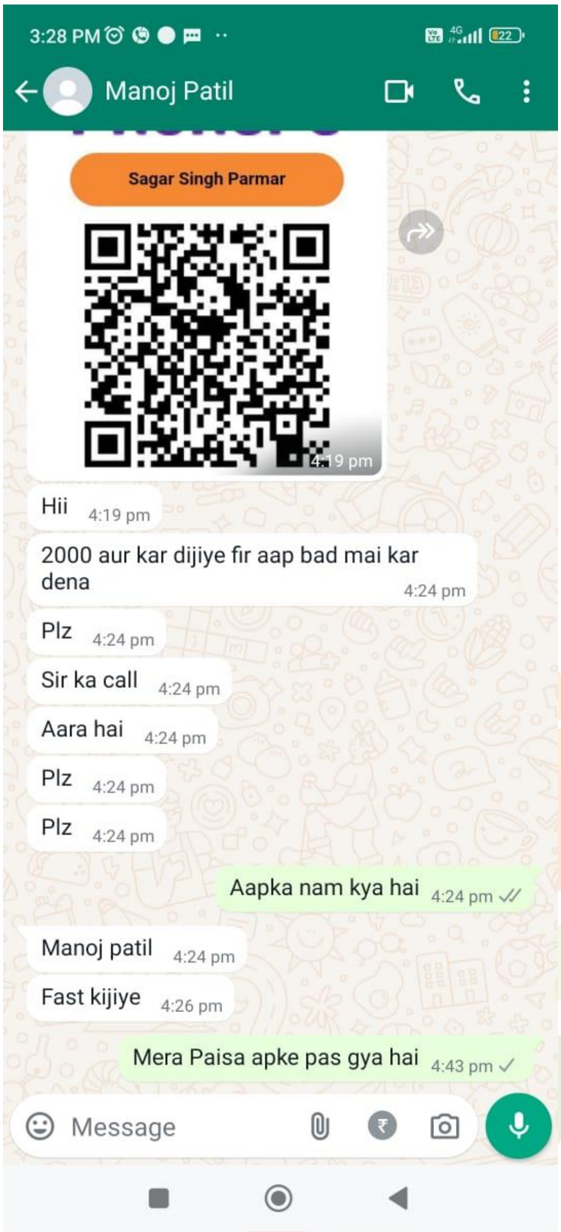
2:14 PM

Ky 2:17 PM

Case 2: "Mistaken Fund Transfer" Scam

1. **Description:** Victim received a phone call claiming funds had been mistakenly transferred to their account. Shortly after, a fraudulent SMS "credit alert" was received.
2. **Fraud Delivery:** Caller convinced victim that returning funds was necessary.
3. **Impact:** Victim transferred a significant amount, later realizing no real funds had been received.

4. **Key Manipulation:** Exploiting honesty and trust; use of fake SMS alerts.



4:19 pm

Hii 4:19 pm

2000 aur kar dijiye fir aap bad mai kar dena 4:24 pm

Plz 4:24 pm

Sir ka call 4:24 pm

Aara hai 4:24 pm

Plz 4:24 pm

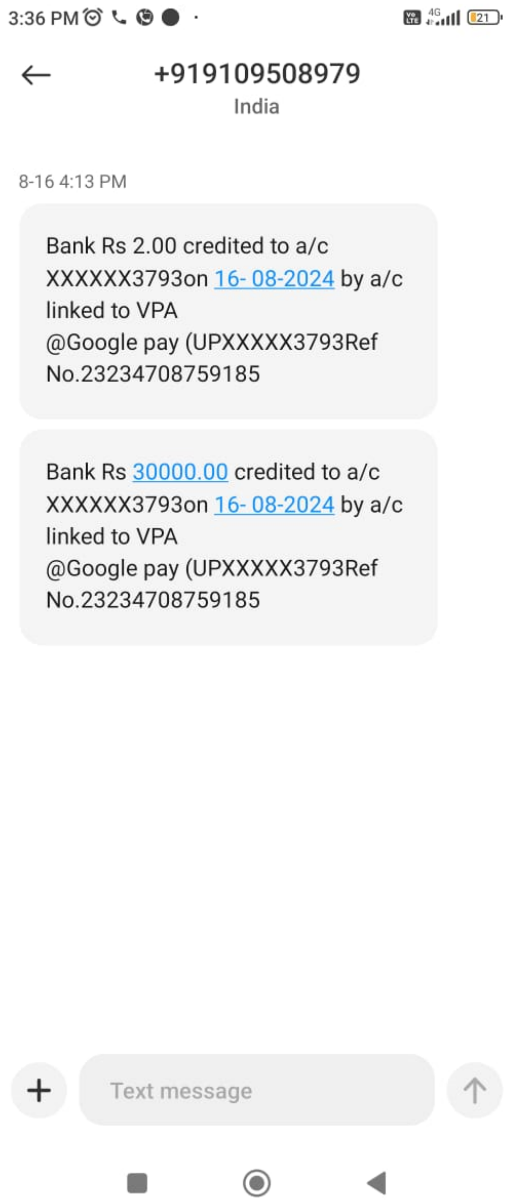
Plz 4:24 pm

Aapka nam kya hai 4:24 pm

Manoj patil 4:24 pm

Fast kijiye 4:26 pm

Mera Paisa apke pas gya hai 4:43 pm



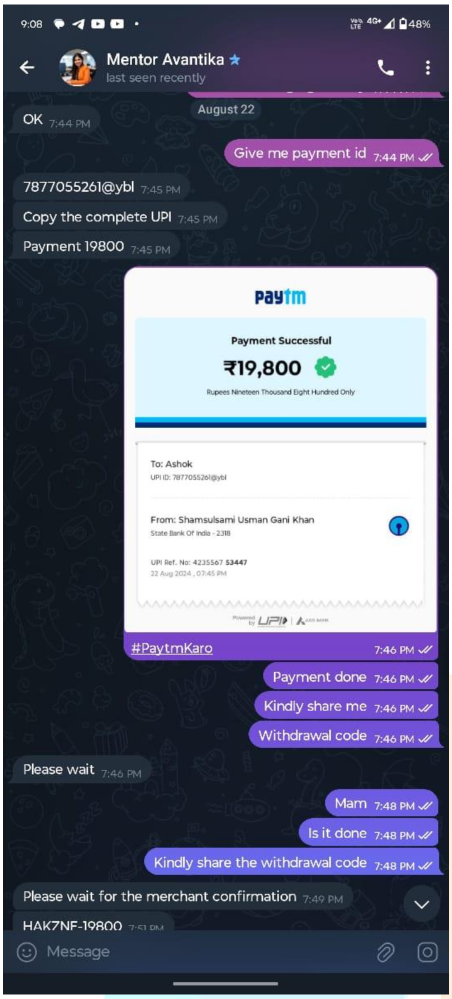
8-16 4:13 PM

Bank Rs 2.00 credited to a/c XXXXXX3793on 16- 08-2024 by a/c linked to VPA @Google pay (UPXXXXX3793Ref No.23234708759185

Bank Rs 30000.00 credited to a/c XXXXXX3793on 16- 08-2024 by a/c linked to VPA @Google pay (UPXXXXX3793Ref No.23234708759185

Case 3: Fake Online Review / Trading App

1. **Description:** Victim was first instructed to provide positive reviews on Google for certain apps and was promised a small payment (around ₹50 per review). Once trust was established, the victim was persuaded to deposit money into a mobile trading app claiming high returns from cryptocurrency and stock investments.
2. **Fraud Delivery:** Social media advertisements and messaging platforms linked to the fraudulent app.
3. **Impact:** The victim deposited substantial funds into the app but could not withdraw any money. The app eventually disappeared after draining the victim's account.
4. **Key Manipulation:** Exploitation of trust through micro-payments, followed by financial greed and aspiration; use of social proof (fake reviews) to gain credibility.



Mentor Avantika
last seen recently

August 22

OK 7:44 PM

Give me payment id 7:44 PM

7877055261@ybl 7:45 PM

Copy the complete UPI 7:45 PM

Payment 19800 7:45 PM

Paytm
Payment Successful
₹19,800
Rupees Nineteen Thousand Eight Hundred Only

To: Ashok
UPI ID: 7877055261@ybl

From: Shamsulsami Usman Gani Khan
State Bank Of India - 2318

UPI Ref. No: 4235567 53447
22 Aug 2024 , 07:45 PM

#PaytmKaro 7:46 PM

Payment done 7:46 PM

Kindly share me 7:46 PM

Withdrawal code 7:46 PM

Please wait 7:46 PM

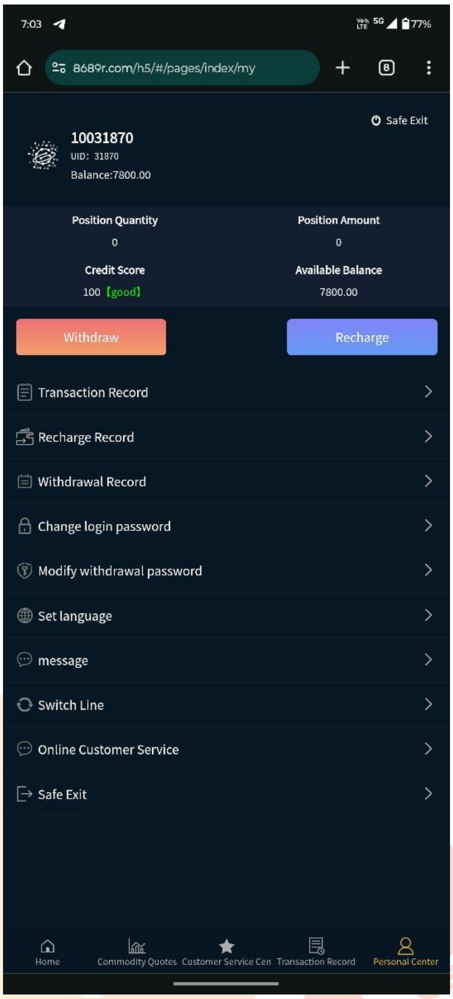
Mam 7:48 PM

Is it done 7:48 PM

Kindly share the withdrawal code 7:48 PM

Please wait for the merchant confirmation 7:49 PM

HAKZNF-19800 7:51 PM

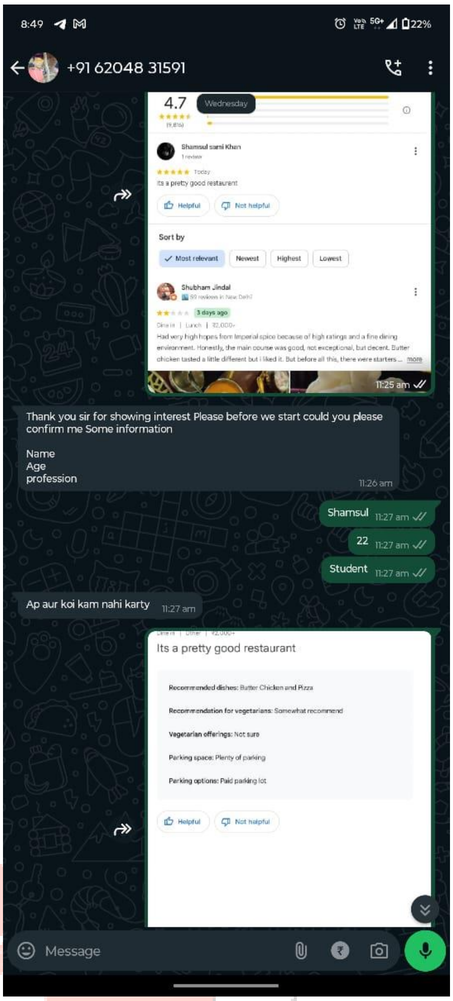


8689r.com/h5/#/pages/index/my

Safe Exit

10031870
UID: 31870
Balance:7800.00

Position Quantity	Position Amount
0	0
Credit Score	**Available Balance**
100 【good】	7800.00



+91 62048 31591

4.7 Wednesday (9,816)

Shamsul sami Khan
1 review
Today
Its a pretty good restaurant

Sort by: Most relevant, Newest, Highest, Lowest

Shubham Jindal
59 reviews in New Delhi
3 days ago
Dine in | Lunch | ₹2,000+
Had very high hopes from Imperial spice because of high ratings and a fine dining environment. Honestly, the main course was good, not exceptional, but decent. Butter chicken tasted a little different but i liked it. But before all this, there were starters ... more

11:25 am

Thank you sir for showing interest Please before we start could you please confirm me Some information

Name
Age
profession
11:26 am

Shamsul 11:27 am

22 11:27 am

Student 11:27 am

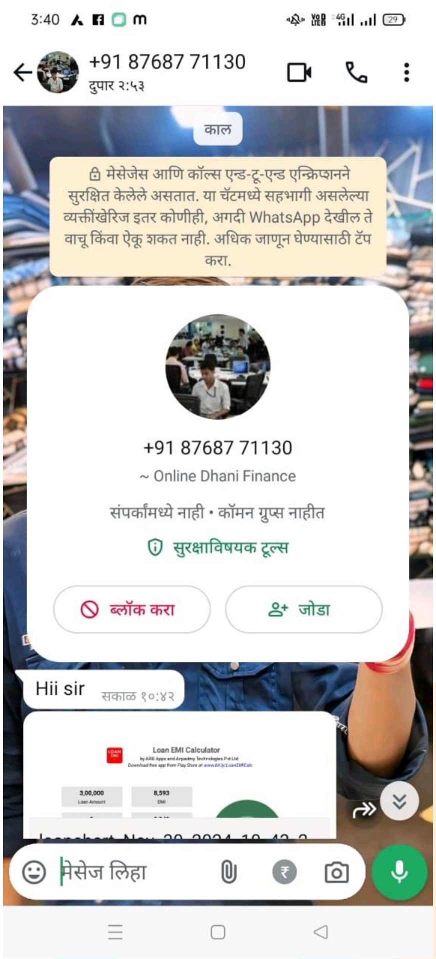
Ap aur koi kam nahi karty 11:27 am

Its a pretty good restaurant

Recommended dishes: Butter Chicken and Pizza
Recommendation for vegetarians: Somewhat recommend
Vegetarian offerings: Not sure
Parking space: Plenty of parking
Parking options: Paid parking lot

Case 4: Axis Bank Employee Impersonation

1. **Description:** Victim received a call from a fraudster posing as an Axis Bank employee offering an “online savings plan.”
2. **Fraud Delivery:** Fake employee ID shared, followed by instructions to transfer funds.
3. **Impact:** Victim transferred money directly to fraudster’s account.
4. **Key Manipulation:** Social engineering, impersonation of authority figures.


3:40

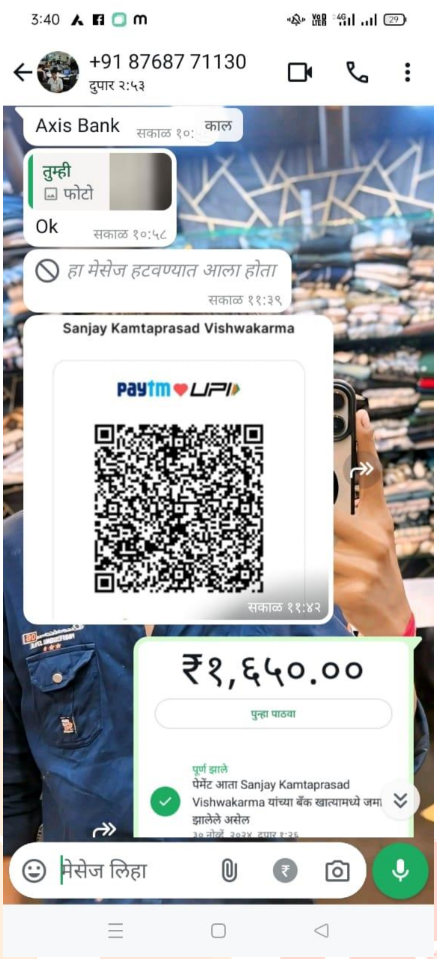
+91 87687 71130
दुपार २:५३

काल

मेसेजेस आणि कॉल्स एन्ड-टू-एन्ड एन्क्रिप्शनने सुरक्षित केलेले असतात. या चॅटमध्ये सहभागी असलेल्या व्यक्तींखेरिज इतर कोणीही, अगदी WhatsApp देखील ते वाचू किंवा ऐकू शकत नाही. अधिक जाणून घेण्यासाठी टॅप करा.

+91 87687 71130
~ Online Dhani Finance
संपर्कांमध्ये नाही • कॉमन ग्रुप्स नाहीत

Hii sir सकाळ १०:४२


3:40

+91 87687 71130
दुपार २:५३

Axis Bank सकाळ १०: काल

तुम्ही
फोटो
Ok सकाळ १०:५८

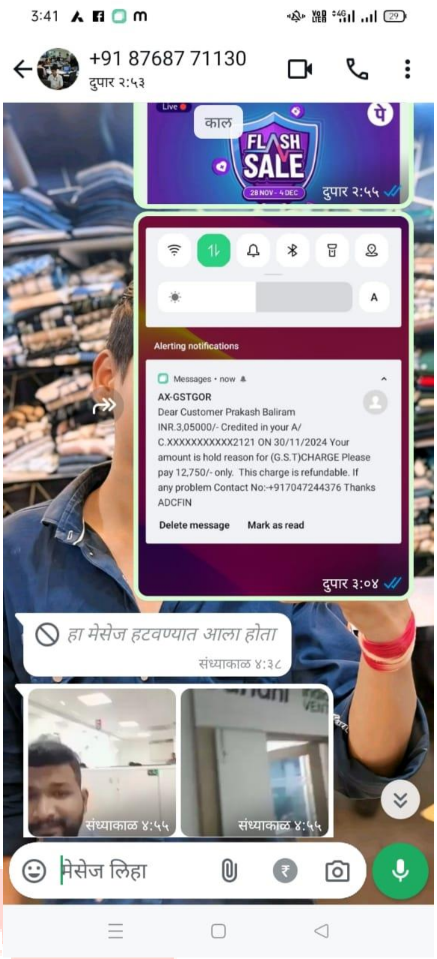
हा मेसेज हटवण्यात आला होता सकाळ ११:३९

Sanjay Kamtaprasad Vishwakarma

सकाळ ११:४२

₹१,६५०.००

पूर्ण झाले
पेमेंट आता Sanjay Kamtaprasad Vishwakarma यांच्या बँक खात्यामध्ये जमा झालेले असेल


3:41

+91 87687 71130
दुपार २:५३

दुपार २:५५

Alerting notifications

Messages • now

AX-GSTGOR
Dear Customer Prakash Baliram INR.3,05000/- Credited in your A/C.XXXXXXXXXXX2121 ON 30/11/2024 Your amount is hold reason for (G.S.T)CHARGE Please pay 12,750/- only. This charge is refundable. If any problem Contact No:-+917047244376 Thanks ADCFIN

दुपार ३:०४

हा मेसेज हटवण्यात आला होता संध्याकाळ ४:३८

संध्याकाळ ४:५५

संध्याकाळ ४:५५

Common Patterns Found:

Scam Type	Delivery Channel	Psychological Trick	Impact
Fake SBI Banking App	SMS / WhatsApp links	Urgency to update account, fear of account lock	Life savings lost
Fake Fund Credit Call / SMS Scam	Phone call + spoofed SMS	Exploitation of trust, urgency, social engineering	Victim sends funds to scammer
Fake Online Review / Trading App	Social media ads / messaging platforms	Micro-payment trust, promise of high profits, social proof	Large fund loss, inability to withdraw
Fake Axis Bank Employee	Phone call / messaging	Impersonation of legitimate bank staff, trust exploitation	Victim sends money thinking it’s for online savings

Summary of Fraud Cases in Maharashtra

Case	Scam Type	Delivery Channel	Psychological Trick	Outcome
1	Fake SBI KYC App	SMS + Fake App	Fear of account suspension	Entire savings lost
2	Mistaken Fund Transfer	Phone Call + Fake SMS	Exploiting honesty & trust	Voluntary transfer of funds
3	Fake Trading App	Social Media + App	Greed (high returns)	Deposited funds unrecoverable
4	Axis Bank Employee Scam	Phone Call + Fake ID	Authority & trust	Direct loss of money

Fraud Delivery Flow

Fraudster → Message/Call → Fake App/Link → Victim Interaction → Credential/Data Entry → Fund Transfer → Financial Loss

5. Discussion:

The cases reveal common themes:

1. **Trust Exploitation**

   Fraudsters exploit citizens' trust in well-known banks and institutions.

2. **Psychological Manipulation**

   Fear (account blocked), urgency (update now), and greed (easy returns) are primary tactics.

3. **Multi-Channel Attacks**

   Scams combine SMS, WhatsApp, phone calls, and apps for maximum impact.

Maharashtra's urban-rural divide also plays a role. Urban victims often fall prey to sophisticated trading apps, while rural users are more vulnerable to SMS-based fake service apps.

6. Recommendations

❖ **For Citizens**

- ➢ Always verify bank messages through official channels.
- ➢ Never download APKs shared via links—use only official app stores.
- ➢ Double-check before transferring funds in "mistaken credit" cases.

- **For Banks & Institutions**
  - ➢ Send regular SMS alerts about fake app scams.
  - ➢ Develop AI-based fraud detection for unusual customer transactions.
  - ➢ Actively monitor misuse of branding/logos.

- **For Regulators & Government**
  - ➢ Strengthen app store verification policies.
  - ➢ Faster takedowns of fraudulent APK hosting sites.
  - ➢ Awareness campaigns in regional languages (Marathi, Hindi).

- **For Cybersecurity Firms**
  - ➢ Build fraud detection dashboards for institutions.
  - ➢ Partner with state police to provide technical intelligence.
  - ➢ Run digital literacy workshops in semi-urban/rural Maharashtra.

7. Conclusion

Mobile app frauds in Maharashtra represent one of the most alarming forms of cybercrime, blending technology with psychological manipulation. Real-life cases demonstrate how citizens, regardless of age or profession, can be deceived into losing life savings.

The study underscores the need for a three-layered approach—citizen awareness, institutional safeguards, and strong regulatory oversight. Only through collaborative action can the growing tide of mobile app frauds in Maharashtra be effectively curbed.

References

1. CERT-In. (2025). *CIAD-2025-0013: Advisory on fake and misleading AI apps and threat actors distributing them via mobile platforms*. Indian Computer Emergency Response Team. https://www.cert-in.org.in/s2cMainServlet?VLCODE=CIAD-2025-0013&pageid=PUBVLNOTES02
 Used in: Literature Review / Discussion — for supporting claims about fake apps exploiting AI demand. CERT-In

2. The Times of India. (2025,). *Maha Cyber police issues advisories to govt depts on online threats, will soon launch "Maha Cyber Safe" app*. Times of India. https://timesofindia.indiatimes.com/city/mumbai/maha-cyber-police-issues-advisories-to-govt-depts-on-online-threats-will-soon-launch-safety-app/articleshow/120216078.cms
 Used in: Literature Review / Recommendations — shows Maharashtra's institutional response to digital frauds. The Times of India

3. Times of India. (2025,). *Maharashtra cyber police arrest key accused in 6 crore cyber fraud case from Nepal border*. Times of India. https://timesofindia.indiatimes.com/city/mumbai/maharashtra-cyber-police-arrest-key-accused-in-6-crore-cyber-fraud-case-from-nepal-border/articleshow/123528420.cms
 Used in: Findings / Case Studies — example of fake trading app fraud with large financial loss. The

Times of India

4. Inc42. (2025,). *CERT-In warns users against vulnerabilities in AI apps*. Inc42. https://inc42.com/buzz/cert-in-warns-users-against-vulnerabilities-in-ai-apps/
 Used in: Literature Review / Methodology — supports the notion of fake/buggy apps being leveraged maliciously. Inc42

5. Economic Times. (2024,). *"Digital arrest" scam: How cybercriminals use fear to empty your bank account*. Economic Times. https://m.economictimes.com/news/india/digital-arrest-scam-how-cybercriminals-use-fear-to-empty-your-bank-account/articleshow/114836839.cms
 Used in: Case Studies / Discussion — example of psychological manipulation (fear, urgency) used in frauds. The Economic Times

6. Hindustan Times. (2024,). *How to avoid digital arrest scams? Centre's advisory as frauds rise across India*. Hindustan Times. https://www.hindustantimes.com/india-news/how-to-avoid-digital-arrest-scams-centres-advisory-as-frauds-rise-across-india-101728216412616.html
 Used in: Recommendations / Discussion — supporting what official guidelines advise citizens to do. Hindustan Times

7. CERT-In. (2025). *Preventing online scams: Advisory for citizens on modus operandi, common tricks and protective measures*. VikasPedia. https://education.vikaspedia.in/viewcontent/education/digital-litercy/information-security/preventing-online-scams-cert-in-advisory?lgn=en
 Used in: General Background / Methodology — describes modes of scams & helps define categories. Vikaspedia Education

8. CERT-In. (2025). *Digital Safety Compass Handbook: Safer Internet Day publication*. CERT-In. https://www.csk.gov.in/documents/CERT-In_Digital_Safety_Compass_Handbook.pdf
 Used in: Literature Review / Methodology — used for definitions and examples of fake banking apps via SMS/WhatsApp or links. Chennai Super Kings

9. Maharashtra Cyber. (n.d.). *About Us*. Government of Maharashtra. https://mhcyber.gov.in/
 Used in: Background / Literature Review — to show Maharashtra Cyber's role & jurisdiction. Maharashtra Cyber

10. CERT-In. (2025,). *CERT-In Issues Advisory on security implications to minimize threats from AI language-based applications*. IndiaAI / CERT-In. https://indiaai.gov.in/news/cert-in-issues-advisory-on-security-implications-to-minimize-threats-from-ai-applications
 Used in: Literature Review / Discussion — about threats from AI-powered fake apps and emerging

vectors. IndiaAI

Disclaimer: This paper is for awareness and educational purposes only. Case details are anonymized, and neither the authors nor the publisher are responsible for any misuse or consequences.