DoT, TRAI, RBI व Cyber Crime Portal पर आधारित

नवीनतम 2026 EDITION

Fraud Call से कैसे बचें

Bank, KYC, Screen Sharing और Digital Arrest वाले Phone Scams से बचने की पूरी और आसान Pocket Guide

16	100%	0
आसान अध्याय	Verified नियम	डर और Panic

Digital Arrest • Fake KYC • Screen Share • AI Voice Clone

सचेत आवाज़ • सुरक्षित परिवार • सशक्त भारत

2026 Mobile Pocket Edition • जनहित में प्रकाशित

कानूनी सूचना • LEGAL NOTICE

कानूनी बातें और इस्तेमाल के नियम

1. जन-जागरूकता उद्देश्य

यह eBook केवल आम नागरिकों में Cyber Safety जागरूकता बढ़ाने के उद्देश्य से तैयार की गई एक स्वतंत्र Guide है। इसका उद्देश्य पाठकों को Phone Calls, Bank Scams और Digital Arrest के तरीकों से सावधान करना है। यह कोई कानूनी (Legal) या Financial सलाह नहीं है।

2. किसी भी संस्था या सरकार से कोई संबंध नहीं

यह eBook Reserve Bank of India (RBI), Telecom Regulatory Authority of India (TRAI), DoT, National Cyber Crime Portal, NPCI, किसी भी Bank या भारत सरकार की किसी भी एजेंसी द्वारा प्रायोजित, समर्थित या Approved नहीं है। यह एक स्वतंत्र Digital उत्पाद है।

3. ज़िम्मेदारी की सीमा (Limitation of Liability)

Cyber Safety के नियम, App Settings और सरकारी Websites के पते समय के साथ बदल सकते हैं। किसी भी पाठक के साथ होने वाले Phone Fraud, तकनीकी समस्या या आर्थिक नुकसान के लिए यह eBook या इसके लेखक किसी भी रूप में ज़िम्मेदार नहीं होंगे। ताज़ा जानकारी के लिए हमेशा संबंधित संस्था की Official Website देखें।

4. Trademarks और Brand Names

'UPI' NPCI का पंजीकृत Trademark है। 'WhatsApp' Meta Platforms का Trademark है। पुस्तक में उल्लिखित अन्य सभी नाम (जैसे Google Pay, PhonePe, AnyDesk, TeamViewer, Airtel, Jio, FedEx आदि) उनके संबंधित मालिकों की संपत्ति हैं। इनका इस्तेमाल केवल पहचान और Fair Use के तहत किया गया है।

5. तरीकों का विवरण (No Real Names)

इस किताब में दिए गए सभी उदाहरण और Case Studies केवल समाज में प्रचलित ठगी के तौर-तरीकों को समझाने के लिए काल्पनिक नामों से दिए गए हैं। किसी भी असली व्यक्ति, कंपनी या संस्था को ठग नहीं कहा गया है; केवल अपराध के तरीकों को उजागर किया गया है।

6. Single-User Digital License

यह eBook केवल खरीदार के व्यक्तिगत पढ़ने के लिए है। इस eBook का अनधिकृत मुद्रण, Internet पर दोबारा Upload करना या Resale करना पूर्णतः प्रतिबंधित है।

© 2026 सर्वाधिकार सुरक्षित • 100% DoT, TRAI व Cyber Crime Portal के नियमों पर आधारित स्वतंत्र Guide

संपादकीय • EDITORIAL PREFACE

प्रस्तावना: यह गाइड आपके लिए क्यों आवश्यक है?

आज भारत में हर SmartPhone User को दिन भर में 3 से 4 अनजान Numbers से Calls आती हैं। कभी Bank Manager बनकर, कभी कूरियर में नशीली दवाइयाँ मिलने का डर दिखाकर, तो कभी Police या CBI की वर्दी में Video Call करके।

इसे आज की सबसे ख़तरनाक ठगी कहा जाता है—**Digital Arrest और Voice Scams**। बड़े-बड़े अफ़सर, डॉक्टर, रिटायर्ड कर्मचारी और पढ़े-लिखे युवा भी डर और Panic में अपने जीवन की सारी जमा-पूँजी Scammers के खातों में Transfer कर देते हैं।

> “ **भारत में कोई भी असली Police, CBI या Court कभी भी WhatsApp Video Call पर किसी को Arrest या पूछताछ नहीं करती।** Digital Arrest केवल एक नाटक है जो आपका पैसा लूटने के लिए रचा जाता है।

ज़्यादातर लोग केवल इसलिए फँस जाते हैं क्योंकि उन्हें Phone Call पर बात करने के 2-3 Basic नियम नहीं पता होते: *"Call पर कोई कितनी भी बड़ी धमकी दे, कभी Phone पर Screen Sharing App Install न करें और तुरंत Call काटकर पास के थाने या Cyber Crime Portal पर Confirm करें।"*

इस ई-बुक का उद्देश्य:

यह ई-बुक भारी शब्दों में नहीं, बल्कि **साधारण बोलचाल की हिंदी** में लिखी गई है। इसमें 16 अध्यायों के माध्यम से Phone Scams की पूरी पोल खोली गई है, ताकि आप किसी भी अनजान Call पर घबराएँ नहीं, बल्कि आत्मविश्वास के साथ Call काट सकें।

इस गाइड को स्वयं पढ़ें और अपने घर के हर सदस्य, विशेषकर माता-पिता और बुज़ुर्गों को ज़रूर पढ़ाएँ। आपकी एक समझदारी पूरे परिवार को बड़े नुकसान से बचा सकती है।

विषय सूची • TABLE OF CONTENTS

अध्यायों की विस्तृत सूची

1 **अध्याय 1: Fraud Call कैसे आते हैं**
कॉल स्पूफिंग, टेलीकॉम डाटा लीक और पहली घंटी का खेल

2 **अध्याय 2: Fake Bank Call और OTP माँगना**
कार्ड ब्लॉक होने का डर और बैंक के नाम पर ओटीपी की चोरी

3 **अध्याय 3: Fake KYC Call**
सिम, बिजली और वॉलेट केवाईसी एक्सपायरी का नया जाल

4 **अध्याय 4: Digital Arrest: Fake Police या CBI Call**
वर्दी, फर्जी कोर्ट रूम और डर दिखाकर पैसे ऐंठने का पूरा सच

5 **अध्याय 5: Fake Customer Care Call**
गूगल सर्च के फर्जी नंबर और रिफंड के नाम पर ठगी

6 **अध्याय 6: Loan, Credit Card और सरकारी Scheme Call**
बिना ब्याज का लोन, रिवॉर्ड पॉइंट और योजनाओं के नाम पर लूट

7 **अध्याय 7: Screen Sharing और Remote App Scam**
AnyDesk, TeamViewer और QuickSupport से फोन का कंट्रोल छीनना

8 **अध्याय 8: AI Voice Clone: अपनों की आवाज़ में Call**
आर्टिफिशियल इंटेलिजेंस से बच्चों की आवाज़ बनाकर फिरौती माँगना

9 **अध्याय 9: Missed Call और अनजान Number के जाल**
+92, +84 जैसे विदेशी कोड और वन-रिंग कॉल का खौफ

10 **अध्याय 10: Course और Financial Freedom के Fake Call**
शेयर बाजार के कोर्स, ट्रेडिंग टिप्स और रातों-रात अमीर बनने का झांसा

11 **अध्याय 11: Fake Membership और बड़े वादे**
क्लब, होटल और ट्रैवल कूपन के नाम पर क्रेडिट कार्ड बिलिंग

12 **अध्याय 12: Loan Fraud और Recovery Agent की धमकी**
फर्जी लोन ऐप्स, फोटो ब्लैकमेलिंग और कानून के दायरे से बाहर वसूली

13 **अध्याय 13: रिश्तेदार बनकर पैसे माँगने वाले Call**
पहचानो मुझे, अचानक अस्पताल की इमरजेंसी और पैसे की मांग

14 **अध्याय 14: Prize, Lottery, Courier और SIM Block Call**
केबीसी लॉटरी, कस्टम में फंसा पार्सल और धमकी भरे कॉल

15 **अध्याय 15: Fraud हो जाए तो क्या करें और Complaint कैसे करें**
गोल्डन 2 घंटे, साइबर क्राइम पोर्टल और बैंक खाता सीज कराना

16 **अध्याय 16: Fraud Call Safety Checklist**
कॉल पर कभी न बोलने वाली 10 बातें और मास्टर पॉकेट चेकलिस्ट

- **अंतिम भाग:** Printable Safety Card, पारिभाषिक शब्दकोश एवं बैक कवर

अध्याय 1 • PHONE FRAUD की शुरुआती समझ

Fraud Call कैसे आते हैं

Data Leaks का सच, Caller ID Spoofing का खेल और IVR Robocalls की असली पहचान।

Phone की घंटी बजी: आपका नाम और Bank कैसे जानता है Scammer?

सोचिए, आपके Phone पर एक सामान्य Call आती है। सामने से बहुत ही गंभीर और भारी आवाज़ में कोई बोलता है: *"नमस्ते, क्या मैं राहुल जी से बात कर रहा हूँ? आपका HDFC Bank में खाता है ना? आपके Debit Card से अभी ₹25,000 कटने वाले हैं, तुरंत रोकें!"*

जब सामने वाला आपका असली नाम, आपके पिता का नाम या आपके Bank का नाम सही-सही बता देता है, तो आप सोचते हैं: *"यह तो सच में Bank से ही Call है, क्योंकि इसे मेरा नाम कैसे पता चला?"*

खतरे की सच्चाई

Scammers के पास आपका Data कहाँ से आता है?

Scammer कोई जासूस नहीं है। जब भी आप किसी Shopping Mall में Lucky Draw के नाम पर, किसी अनजान Website पर, या किसी Hotel में अपना Mobile Number और नाम लिखते हैं, तो वह Data लीक होकर Dark Web पर कौड़ियों के भाव बिक जाता है।

> **सीधी बात:** केवल आपका नाम या Bank का नाम बता देने से कोई व्यक्ति असली अधिकारी साबित नहीं हो जाता।

Case Study: Caller ID Spoofing का भयानक खेल

देखें कैसे Scammer अपनी Screen पर असली Bank का Number दिखाकर लोगों को चकमा देता है:

📞 PHONE CALL SIMULATION (FAKE BANK EXECUTIVE)

> **Scammer (गंभीर आवाज़ + पीछे Office का शोर):** "सर, मैं Head Office से Senior Security Manager बोल रहा हूँ। आपके Phone की Screen पर हमारा Official Number दिख रहा होगा, आप Check कर सकते हैं।"

> **साधारण User:** *(Screen देखता है तो सच में Bank का असली Official Number दिखाई दे रहा होता है!)* "हाँ सर, Number तो Bank का ही है। बताइए क्या बात है?"

> **Scammer:** "सर, आपका Card Hack हो गया है। अभी आपके Phone पर एक Cancel Code (OTP) आया है, जल्दी बताइए वरना सारा पैसा कट जाएगा!"

> **सच्चाई:** *(Screen पर असली Number दिख रहा था, लेकिन वह केवल **Caller ID Spoofing** थी। जैसे ही User ने OTP बताया, खाते से ₹50,000 कट गए!)*

Phone Call Scam का 4-Step Trap

1 **Computer द्वारा Auto-Dialing**

Scammers Computer Software से एक साथ 10,000 Numbers पर IVR Robocalls या सामान्य Calls लगाते हैं।

↓ डर और हड़बड़ी पैदा करना

2 **बड़ी मुसीबत का झूठा नाटक**

कहा जाता है: "आज रात SIM बंद हो जाएगा", "Police FIR हो चुकी है", या "आपके Bank खाते से पैसे कट रहे हैं।"

↓ सोचने का समय न देना

3 **OTP, PIN या Screen Sharing की माँग**

Scammer कहता है: "तुरंत OTP बताएँ", "AnyDesk App Download करें", या "पैसे सुरक्षित खाते में Transfer करें।"

↓ पैसा गायब और Call Cut

4 **खाता खाली और Number Switch Off**

जैसे ही आपने बात मानी, खाते से सारा पैसा साफ़ हो जाता है और Scammer तुरंत Call काटकर गायब हो जाता है।

असली Call vs Fraud Call: 3 सबसे बड़े फर्क



1. असली Bank कभी OTP नहीं माँगता

RBI का साफ़ नियम है: कोई भी असली Bank कर्मचारी कभी भी Call पर आपसे OTP, UPI PIN, या ATM Card के पीछे का 3-Digit CVV नहीं माँगता।

> **नियम:** जो भी Call पर OTP माँगे, वह 100% Scammer है।

👮

2. Police कभी Video Call पर गिरफ़्तारी नहीं करती

भारत में कानून के तहत Video Call पर न तो कोई अदालत चलती है, न ही "Digital Arrest" नाम की कोई कानूनी नियम होती है।

📱

3. SIM कभी 2 घंटे में बंद नहीं होता

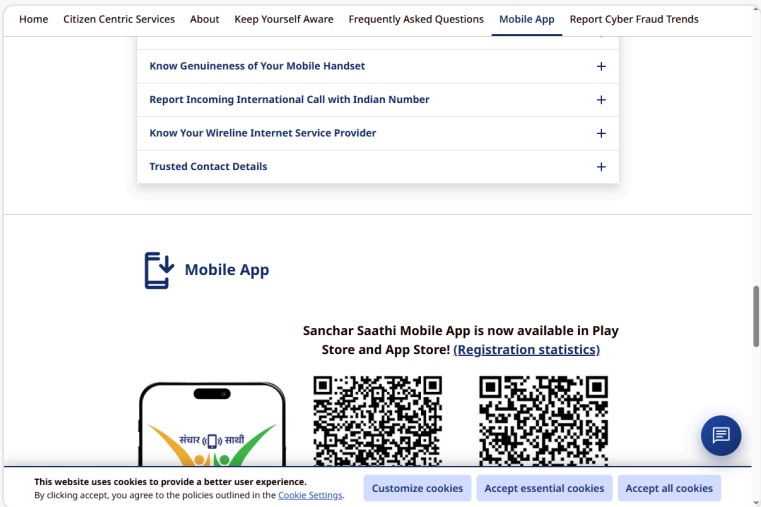
Telecom Department का नियम है कि किसी भी SIM को बंद करने से पहले लिखित नोटिस और सही नियम होती है। IVR Call पर कोई SIM बंद नहीं होता।

Official Portal: Fraud Call की सीधे सरकार से शिकायत

भारत सरकार के Telecom Department ने आम नागरिकों के लिए **Chakshu Portal** बनाया है, जहाँ आप किसी भी Fake Call या Spoofed Number की सीधे Report कर सकते हैं:

🌐 `sancharsaathi.gov.in (Chakshu Portal)`

Official सरकारी Portal



📌 Chakshu Portal से 2 ज़रूरी बातें:

1. **तुरंत Number Report:** अगर किसी अनजान Number से Bank, KYC या Police के नाम पर Fake Call आई है, तो उसे यहाँ Report करें ताकि वह Number पूरे देश में Block हो सके।
2. **Official Address Check:** हमेशा Browser में देखें कि Website का पता `sancharsaathi.gov.in` ही हो। सरकारी पते के अंत में हमेशा `.gov.in` होता है।

अध्याय 1: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• अनजान Call पर डर या हड़बड़ी महसूस होते ही सीधे **Call काट दें**।

• Bank का दावा करने पर अपने ATM Card के पीछे लिखे Official Number पर खुद Callback करें।

• Fake Calls की Report सरकारी Portal **Chakshu** (`sancharsaathi.gov.in`) पर करें।

❌ यह कभी न करें (DONTs)

• Phone की Screen पर दिखने वाले Caller ID Number पर आँख मूँदकर भरोसा न करें।

• Call पर किसी भी व्यक्ति को अपना OTP, PIN या Password कभी न बताएँ।

• Call पर किसी के कहने पर AnyDesk या TeamViewer जैसा कोई App Download न करें।

OFFICIAL सत्यापन व शिकायत स्रोत

• Telecom Regulatory Authority of India (TRAI Caller ID Guidelines): `trai.gov.in`

• Chakshu Fraud Reporting Portal (Telecom Department): `sancharsaathi.gov.in`

• National Cyber Crime Reporting Portal: `cybercrime.gov.in`

• Reserve Bank of India (RBI Phone Fraud Warnings): `rbi.org.in`

अध्याय 2 • BANK और CARD SECURITY की सच्चाई

Fake Bank Call और OTP माँगना

Card Block होने का डर, Reward Points का लालच और OTP चुराने का पूरा खेल।

Phone की घंटी और Bank Manager का रुआब

सोचिए, दोपहर के समय आपके Phone पर एक Call आती है। सामने से कोई बहुत ही गंभीर और Professional आवाज़ में बोलता है: *"नमस्ते, मैं आपके Bank के Card Security Division से Senior Officer बात कर रहा हूँ। आपका Debit Card आज रात 12 बजे Block हो जाएगा क्योंकि नया Chip Card जारी हुआ है।"*

जब आप थोड़ा हिचकिचाते हैं, तो वह आपके Bank का नाम, आपके शहर का नाम और आपके Card के आखिरी 4 अंक सही-सही बता देता है। यह सुनकर 90% लोग डर जाते हैं और सोचने लगते हैं कि सामने वाला सच में Bank का असली अधिकारी है।

सच्चाई समझें

Card के आखिरी 4 अंक Scammer को कैसे पता चले?

जब भी आप किसी Petrol Pump, Restaurant या Grocery Store पर Card से Payment करते हैं, तो मिलने वाली Slip पर Card के आखिरी 4 अंक छपे होते हैं। Scammers ऐसी पर्चियों या Online Data Leaks से यह जानकारी चुराते हैं।

> **सीधी बात:** केवल आखिरी 4 अंक बता देने से कोई Bank अधिकारी नहीं बन जाता। जब तक आपके पास **OTP** और **PIN** सुरक्षित है, कोई आपके खाते से ₹1 भी नहीं निकाल सकता।

Case Study: "Cancellation Code" का खतरनाक खेल

देखें कैसे Scammer शब्दों का जाल बुनकर User से पैसे काटने का OTP निकलवा लेता है:

📞 PHONE CALL SIMULATION (FAKE SECURITY OFFICER)

> **Scammer (गंभीर आवाज़ में):** "सर, आपके HDFC Card से अभी Dubai में ₹45,000 का Transaction शुरू हुआ है। क्या यह Payment आपने किया है?"

> **User (डरकर):** "नहीं! मैंने कोई Payment नहीं किया! मैं तो घर पर हूँ।"

> **Scammer:** "चिंता मत कीजिए सर, मैं इस Fraud Transaction को तुरंत Cancel कर रहा हूँ। Head Office से एक **Cancellation Code** आपके Phone पर भेजा है। जल्दी बताइए वरना पैसा कट जाएगा!"

> **User (SMS की केवल 6 संख्याएँ देखकर):** "हाँ, Code आया है... 482910।"

> **सच्चाई:** *(वास्तव में Scammer ने Shopping Website पर User के Card से ₹45,000 का Payment शुरू किया था। जैसे ही User ने OTP बताया, पैसे कट गए और Scammer ने Call काट दी!)*

SMS का असली सच vs Scammer का झूठ

Scammer हमेशा कहेगा कि *"SMS मत पढ़िए, बस तुरंत Code बोल दीजिए।"* आइए देखें असली Bank SMS कैसा दिखता है:

VK-HDFCBK
आज • 11:42 AM

Official Bank SMS

`OTP is 482910 for txn of INR 45,000.00 at AMAZON INDIA. Do not share OTP with anyone including Bank staff.`

❌ **SCAMMER का झूठ**

"यह Transaction Cancel करने का Verification Code है।"

✅ **SMS का असली सच**

साफ़ लिखा है: **INR 45,000** कटने का OTP है! Cancel करने का कोई OTP नहीं होता।

Bank Call Scam का 4-Step Trap

1 **डर या लालच का जाल**

Call करके कहा जाता है: "Card Block होने वाला है", "Reward Points Expire हो रहे हैं", या "गलत Payment कट रहा है।"

↓ विश्वास जीतना

2 **पुराना Data बताकर भरमाना**

आपका नाम, शहर, जन्मतिथि या Card के आखिरी 4 अंक बोलकर भरोसा दिलाया जाता है कि Call असली Bank से ही है।

↓ सोचने का समय न देना

3 **Cancellation Code के नाम पर OTP माँगना**

Scammer अपने Computer पर Payment शुरू करता है और User से कहता है: "Cancel करने के लिए आया हुआ Code तुरंत बताएँ।"

↓ खाता साफ़ और Call Disconnect

4 **पैसे गायब और Number Switch Off**

OTP मिलते ही खाते से सारा पैसा निकल जाता है और Scammer तुरंत Call काटकर गायब हो जाता है।

3 Golden Rules जो हमेशा याद रखें

🚫

1. Cancel करने का कोई OTP नहीं होता

दुनिया के किसी भी Bank में Transaction Cancel करने के लिए OTP की ज़रूरत नहीं होती। OTP केवल पैसे निकालने या Transfer करने के लिए ही भेजा जाता है।

> **नियम:** जो भी Call पर Cancel Code माँगे, वह 100% Scammer है।



2. असली Bank कभी OTP नहीं माँगता

Reserve Bank of India (RBI) का कड़ा नियम है: कोई भी असली Bank कर्मचारी Phone पर आपसे OTP, UPI PIN, Card CVV या Password नहीं माँग सकता।



3. हमेशा Card के पीछे देखें

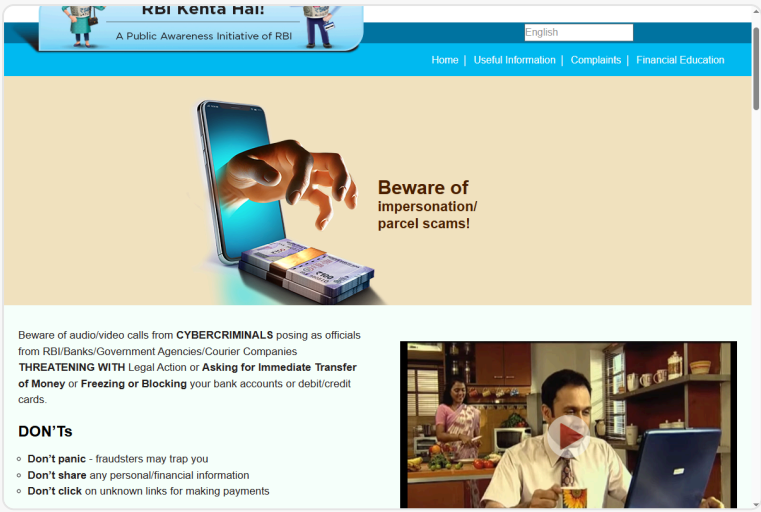
अगर मन में ज़रा भी शक हो, तो तुरंत Call काटें। अपने Debit या Credit Card को पलटें और उसके पीछे छपे Official Customer Care Number पर खुद Callback करें।

RBI Kehta Hai: Bank अधिकारी बनकर Call करने वालों का सच

भारतीय रिज़र्व Bank (RBI) अपने जन-जागरूकता अभियान **RBI Kehta Hai** में देश के हर नागरिक को Bank के नाम पर आने वाली Fake Calls से सतर्क करता है:

rbikehtahai.rbi.org.in

RBI Official जनहित संदेश



📌 **RBI के Official संदेश से 2 सबसे बड़े नियम:**

1. **Bank कभी OTP नहीं माँगता:** RBI साफ कहता है कि कोई भी Bank कर्मचारी या अधिकारी कभी Phone Call पर आपसे OTP, PIN, Password या Card का CVV नहीं माँगता।
2. **डरने के बजाय Call काटें:** "Card Block हो जाएगा" या "खाता बंद हो जाएगा" केवल Scammers का डराने का पैंतरा है। ऐसी Call आते ही तुरंत Phone काटें।

अध्याय 2: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• Bank के नाम पर आने वाली किसी भी शक वाली Call को तुरंत **काट दें**।

• OTP का SMS आने पर हमेशा पहली लाइन पढ़ें कि कितना पैसा कट (Debit) रहा है।

• Card से जुड़ी किसी भी समस्या के लिए केवल Card के पीछे लिखे **Official Number** पर ही Call करें।

❌ यह कभी न करें (DONTs)

• Call पर किसी को भी अपना OTP, Card CVV, Expiry Date या PIN कभी न बताएँ।

• "Card Block हो जाएगा" की धमकी सुनकर हड़बड़ी में कोई Code Share न करें।

• Call पर किसी के कहने पर SMS में आया कोई Link कभी न खोलें।

OFFICIAL व VERIFIED शिकायत स्रोत

• Reserve Bank of India (RBI Customer Protection Guidelines): `rbi.org.in`

• National Cyber Crime Reporting Portal: `cybercrime.gov.in`

• Chakshu Fraud Reporting Portal (Telecom Department): `sancharsaathi.gov.in`

अध्याय 3 • KYC UPDATE और SIM BLOCK का डर

Fake KYC Call

SIM और Bank KYC के नाम पर ₹10 का लालच, Remote App का खेल और असली KYC के सरकारी नियम।

"आज रात 12 बजे आपका SIM बंद हो जाएगा": क्या सच में?

सोचिए, दोपहर के समय आपके Phone पर एक Call आती है। सामने से कोई कहता है: *"सर, मैं Jio / Airtel के KYC Department से बोल रहा हूँ। आपका Aadhaar Card आपके SIM से Link नहीं है। TRAI के आदेशानुसार आज रात आपका Number बंद कर दिया जाएगा।"*

यह सुनते ही इंसान की धड़कनें बढ़ जाती हैं। आज हमारा Bank, UPI, WhatsApp, आधार OTP—सब कुछ उसी एक Number से जुड़ा है। जैसे ही SIM बंद होने का डर बैठता है, इंसान Scammer से खुद पूछता है: *"सर, कृपया बताइए मैं क्या करूँ?"*

कानूनी सच

TRAI और Telecom Department का कड़ा नियम

भारत सरकार के **Telecom Department** के अनुसार, किसी भी चालू SIM Card को इस तरह एक Phone Call करके 24 घंटे में कभी बंद नहीं किया जा सकता। किसी भी SIM का Verification केवल कंपनी के Official Store पर जाकर Biometric (अँगूठा लगाकर) ही होता है।

> **सीधी बात:** जो भी व्यक्ति Call पर कहे कि "घर बैठे 2 मिनट में KYC करा लो", वह 100% Scammer है।

Case Study: "बस ₹10 का Recharge करें" वाला खतरनाक जाल

देखें कैसे Scammer ₹10 का बहाना बनाकर Bank खाता खाली कर देता है:

📞 PHONE CALL SIMULATION (FAKE TELECOM AGENT)

> **Scammer (गंभीर आवाज़ में):** "सर, आपका KYC Form हमारे System में Reject हो गया है। इसे चालू रखने के लिए आपके Phone पर एक Link भेजा है। उस पर जाकर केवल ₹10 का Verification Charge जमा करें।"

> **User:** "सिर्फ ₹10? ठीक है, मैं अभी भर देता हूँ।"

> **Scammer:** "हाँ सर, Link खोलें और अपने Net Banking या Debit Card का PIN डालकर ₹10 का Payment करें। जैसे ही Payment होगा, आपकी KYC Life-Time के लिए Update हो जाएगी।"

> **सच्चाई:** *(वह Link असली Telecom Company का नहीं, बल्कि Scammer का बनाया हुआ **Fake Phishing Page** था। जैसे ही User ने Card Details और PIN डाला, खाते से ₹10 के बजाय सीधे ₹65,000 कट गए!)*

Fake KYC Call का 4-Step Trap

1. **SIM या Bank Block होने की धमकी**
   Scammer कहता है: "Aadhaar Card Link नहीं है, आज रात तक KYC Update नहीं किया तो Phone बंद हो जाएगा।"

↓ घर बैठे मदद का दिखावा

2 **Fake Link या App Download करवाना**

Scammer कहता है: "Store जाने की ज़रूरत नहीं, नीचे दिए Link पर Click करें या 'Quick Support' App Download करें।"

↓ Screen और Password चोरी

3 **Screen Share करके PIN और OTP देखना**

अगर आपने App Download किया, तो आपके Phone की पूरी Screen Scammer को दिखने लगती है। आप जो भी PIN डालते हैं, वह Scammer नोट कर लेता है।

↓ खाता साफ़ और Number बंद

4 **सारे पैसे गायब**

Scammer तुरंत आपके Bank से पूरा पैसा Transfer कर लेता है और Phone काट देता है।

असली KYC vs Fake KYC Call: 3 सबसे बड़े फर्क



1. असली SIM KYC हमेशा Official Store पर होती है

Airtel, Jio या Vi कभी Phone Call पर आधार Card या पैन Card नहीं माँगते। वे हमेशा अपने Official Store पर Biometric के लिए बुलाते हैं।

> **नियम:** Phone Call पर कभी भी SIM KYC नहीं होती।



2. Bank KYC केवल Official App या शाखा में होती है

Bank खाते की Re-KYC केवल Bank की Official Net Banking App में Login करके या अपनी Bank शाखा में जाकर ही की जा सकती है।



3. KYC के लिए कभी पैसे नहीं देने पड़ते

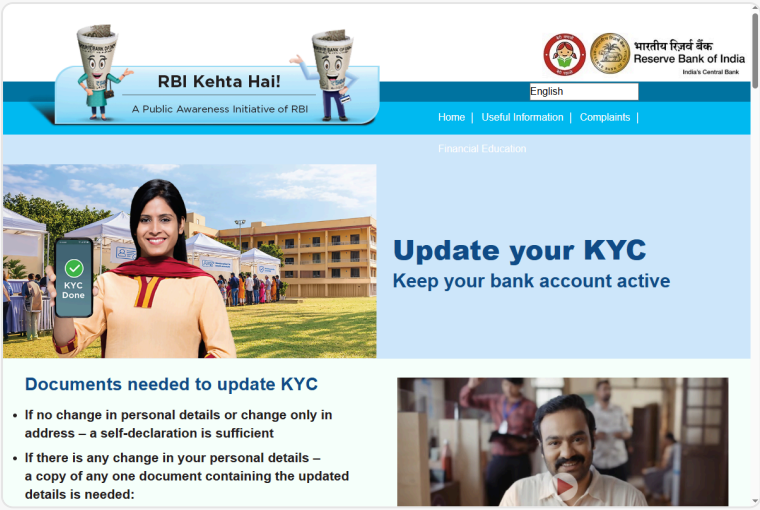
भारत में किसी भी प्रकार की KYC (SIM, Bank, Wallet) पूरी तरह मुफ़्त होती है। जहाँ भी ₹10 या ₹1 माँगा जाए, वह 100% Fraud है।

RBI Advisory: Fake KYC Links और Phishing से सुरक्षा

भारतीय रिज़र्व Bank (RBI) ने साफ निर्देश जारी किए हैं कि Scammers द्वारा भेजे गए Fake KYC Links पर कभी भरोसा न करें:

🌐 rbi.org.in (RBI Cyber Security Advisory)

Official RBI चेतावनी



📌 **RBI Phishing Advisory से 2 मुख्य सबक:**

1. **SMS या Call पर आया Link न खोलें:** कोई भी असली Telecom Company या Bank कभी SMS या Call पर KYC Form भरने का Link नहीं भेजती।
2. **KYC पूरी तरह मुफ़्त है:** KYC Update करने के लिए ₹10 या ₹1 भी नहीं लगता। अगर कोई पैसे माँगे, तो वह 100% Fraud है।

अध्याय 3: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• SIM बंद होने की धमकी वाली Call आते ही तुरंत **Call काट दें**।

• SIM की स्थिति जानने के लिए सीधे कंपनी के Official Store पर जाएँ।

• Fake Calls की Report सरकारी Portal **Chakshu** (`sancharsaathi.gov.in`) पर करें।

❌ यह कभी न करें (DONTs)

• Call पर किसी अनजान व्यक्ति के कहने पर कोई Link कभी न खोलें।

• KYC के नाम पर अपने Phone में AnyDesk, TeamViewer या QuickSupport Download न करें।

• KYC Verification के नाम पर ₹10 या ₹1 का भी कोई Online Payment न करें।

OFFICIAL सत्यापन व शिकायत स्रोत

• Chakshu Fraud Reporting Portal (Telecom Department): `sancharsaathi.gov.in`

• Telecom Regulatory Authority of India (TRAI Guidelines): `trai.gov.in`

• Reserve Bank of India (RBI KYC Master Direction): `rbi.org.in`

• National Cyber Crime Reporting Portal: `cybercrime.gov.in`

अध्याय 4 • DIGITAL ARREST और FAKE POLICE का सच

Digital Arrest: Fake Police, CBI या Court Call

Video Call पर नकली Police Station का सेट, Fake Arrest Warrant और बेगुनाही के नाम पर करोड़ों की ठगी।

"आप Digital Arrest हैं": क्या भारतीय कानून में ऐसा कुछ होता है?

सोचिए, आपको एक Call आती है कि आपके नाम से विदेश भेजे गए Parcel में नशीली दवाइयाँ और जाली Passports मिले हैं। फिर आपको एक Video Call (Skype या WhatsApp) पर जुड़ने को कहा जाता है।

Video Call पर सामने खाकी Uniform पहने Police अधिकारी बैठे दिखते हैं, पीछे Police Station का बोर्ड और वायरलेस सेट की आवाज़ें आ रही होती हैं। वे एक कागज़ दिखाते हैं जिस पर Supreme Court की Fake Seal और Arrest Warrant लिखा होता है: *"आपको Digital Arrest किया जाता है, Camera 24 घंटे On रहेगा!"*

प्रधानमंत्री व सुप्रीम कोर्ट की चेतावनी

भारतीय कानून का सबसे बड़ा सच

भारत के प्रधानमंत्री और सुप्रीम कोर्ट ने पूरे देश को साफ़-साफ़ चेताया है: **"भारतीय कानून में 'Digital Arrest' नाम की कोई व्यवस्था ही नहीं है। कोई भी सरकारी एजेंसी या Police कभी भी Phone या Video Call पर किसी नागरिक को Arrest नहीं करती।"**

> **सीधी बात:** Video Call पर दिखने वाला हर "Police Station" केवल Scammers द्वारा किराए के कमरे में बनाया गया नकली स्टूडियो (Set) होता है।

Case Study: Video Call पर Fake Police Station का ड्रामा

देखें कैसे Scammer डर और माहौल बनाकर पीड़ित को मानसिक रूप से बंधक बना लेता है:

☎️ VIDEO CALL SIMULATION (FAKE CRIME BRANCH STUDIO)

> **नकली Inspector (Uniform में + पीछे वायरलेस की आवाज़):** "सुनीता जी, आपके आधार Card से 16 Bank

खाते खुले हैं और उनमें ₹38 करोड़ का Money Laundering हुआ है। Supreme Court ने आपका गैर-जमानती Arrest Warrant जारी किया है।"

सुनीता जी (काँपते हुए): "सर, मैंने तो ज़िंदगी में कभी कोई अपराध नहीं किया! मेरा इन खातों से कोई लेना-देना नहीं है।"

नकली Inspector: "अगर आप बेगुनाह हैं, तो जाँच में सहयोग करें। तुरंत कमरे का दरवाज़ा अंदर से बंद करें। किसी रिश्तेदार या वकील को बताया तो देशद्रोह का Case लगेगा। अब आपको हमारे Secret Verification Account में सारे पैसे Transfer करने होंगे ताकि हम Check कर सकें कि यह काला धन नहीं है।"

सच्चाई: *(डर के मारे महिला ने अपने ₹45 लाख के Fixed Deposits तोड़कर Scammer के बताए खाते में भेज दिए। पैसे मिलते ही Scammer ने Video Call बंद कर दिया!)*

Digital Arrest Scam का 4-Step Trap

1. **Customs या Courier का Fake Call**
   कहा जाता है: "आपके आधार से ताइवान भेजे गए सामान में Drugs मिले हैं, आपको Mumbai Police से Connect किया जा रहा है।"

↓ Video Call पर नकली सेट

2 **Skype / WhatsApp Video Call**

Scammers Uniform पहनकर बैठते हैं और Fake CBI ID Card, FIR की कॉपी और Arrest Warrant Screen पर दिखाते हैं।

↓ कमरे में बंद करना (Isolation)

3 **Digital Arrest और अकेलेपन का दबाव**

पीड़ित को 24 से 72 घंटे तक कमरे में बंद रहने को कहा जाता है। Camera हमेशा On रखने का आदेश दिया जाता है ताकि वह किसी से सलाह न ले सके।

↓ बेगुनाही के नाम पर वसूली

4 **"RBI Verification Account" में पैसा Transfer**

कहा जाता है: "सारे पैसे सरकारी खाते में Transfer करें, जाँच के बाद 30 मिनट में वापस आ जाएँगे।" पैसा जाते ही सब गायब!

असली कानून vs Fake Digital Arrest: 3 सबसे बड़े सच

⚖️

1. Video Call पर कोई Arrest नहीं होता

भारत में कानून के तहत गिरफ्तारी के लिए Police को भौतिक रूप से आपके सामने आना पड़ता है और औपचारिक गिरफ्तारी मेमो देना होता है। Video Call पर कोई गिरफ़्तारी संभव नहीं है।

> **नियम:** Video Call पर Arrest की बात करने वाला 100% Fraud है।



2. "RBI Verification Account" एक सफेद झूठ है

Reserve Bank of India (RBI) किसी भी नागरिक से बेगुनाही साबित करने के लिए अपने पास पैसे जमा नहीं करवाता। सरकारी एजेंसियों का कोई भी ऐसा खाता नहीं होता।



3. Police कभी Video Call पर बयान नहीं लेती

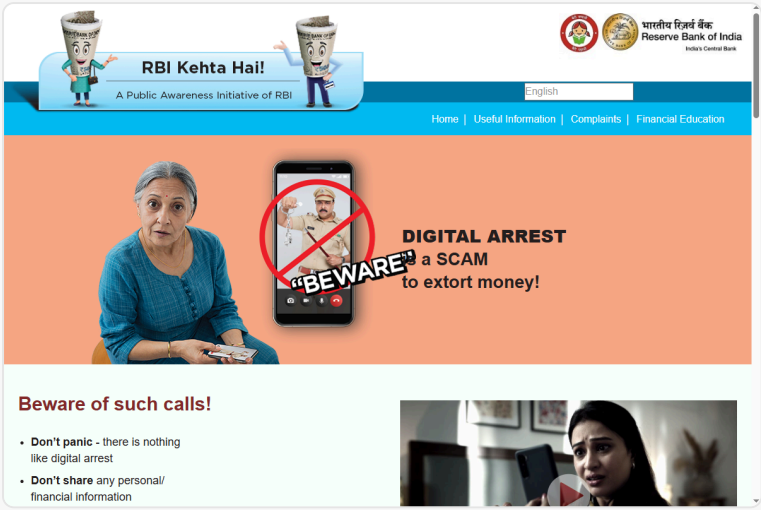
CBI, ED या Police किसी भी जाँच के लिए अधिकृत समन भेजती है। वे कभी Skype या WhatsApp पर Video Call करके पूछताछ नहीं करते।

Official Advisory: Digital Arrest के नाम पर होने वाले Fraud का सच

भारतीय रिज़र्व Bank (RBI) और गृह मंत्रालय (Cyber Dost) ने देश भर में फैले "Digital Arrest" Scam के खिलाफ यह कड़ा Official Alert जारी किया है:

🌐 rbikehtahai.rbi.org.in (Digital Arrest Alert)

Official RBI व गृह मंत्रालय चेतावनी



📌 **Official Alert से 2 सबसे बहुत ज़रूरी बातें:**

1. **Digital Arrest नाम का कोई कानून नहीं:** भारत में किसी भी एजेंसी (Police, CBI, ED, Court) को Video Call पर लोगों को बंधक बनाने या गिरफ़्तार करने का कोई अधिकार नहीं है।
2. **Verification Account पूरी तरह Fake है:** सरकार या Police कभी किसी नागरिक से पैसा जमा कराकर "जाँच" नहीं करती। जो पैसे माँगे, वह 100% अपराधी है।

अध्याय 4: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• Video Call पर "Digital Arrest" की धमकी मिलते ही सीधे **Call काट दें**।

• तुरंत अपने परिवार, बच्चों या स्थानीय Police थाने जाकर पूरी बात बताएँ।

• ऐसी Fake Calls की तुरंत सरकारी Cyber Portal `cybercrime.gov.in` पर Report करें।

❌ यह कभी न करें (DONTs)

• डर के मारे कमरे का दरवाज़ा बंद करके अकेले न बैठें।

• बेगुनाही साबित करने के लिए किसी भी अनजान खाते में अपने पैसे Transfer न करें।

• Video Call पर दिखाए जाने वाले किसी भी Warrant या कागज़ पर विश्वास न करें।

OFFICIAL सत्यापन व शिकायत स्रोत

• Prime Minister's Advisory on Digital Arrest (Mann Ki Baat Episode 115)

• Ministry of Home Affairs (I4C Cyber Dost Advisory): `cybercrime.gov.in`

• Chakshu Fraud Reporting Portal: `sancharsaathi.gov.in`

अध्याय 5 • GOOGLE SEARCH और HELPLINE FRAUD

Fake Customer Care Call

Google Search पर Fake Helpline Numbers, Remote Screen Sharing Apps और Refund Scam की पूरी सच्चाई।

Google पर Number ढूँढने की सबसे बड़ी भूल

सोचिए, आपने Online खाना Order किया था या कोई सामान मँगवाया था। Order Cancel हो गया लेकिन आपके Bank खाते से ₹450 कट गए। अब आप बेचैन हो जाते हैं कि मेरा पैसा कब वापस आएगा?

हड़बड़ी में आप सीधे Google खोलते हैं और Search बार में Type करते हैं: *"Zomato Customer Care Number"* या *"Courier Refund Helpline"*। Screen पर सबसे ऊपर एक 10-अंकों का Mobile Number दिखता है। आप बिना सोचे तुरंत Call लगा देते हैं।

सावधान रहें

Google Search कोई जाँची हुई Phone Book नहीं है!

Google पर जो भी Search Result सबसे ऊपर दिखता है, ज़रूरी नहीं कि वह असली कंपनी का ही हो। Scammers Google को पैसे देकर **Sponsored Ads** चलाते हैं और अपना Fake Number ऊपर लगवा देते हैं। इसके अलावा वे Google Maps पर भी असली दुकान या कंपनी के पते में अपना Mobile Number जोड़ देते हैं।

> **सीधी बात:** Google Search में सबसे ऊपर दिख रहा Number किसी असली कंपनी का होना ज़रूरी नहीं है। Scammers पैसे देकर Fake Ad लगा सकते हैं।

Case Study: ₹350 के Refund के चक्कर में ₹60,000 साफ़

देखें कैसे Scammer मीठी बातों में फँसाकर Phone का पूरा Control अपने हाथ में ले लेता है:

📞 PHONE CALL SIMULATION (FAKE SUPPORT EXECUTIVE)

User: "सर, मैंने Online Order Cancel किया था, लेकिन मेरा ₹350 का Refund अभी तक नहीं आया।"

Scammer (बहुत विनम्र आवाज़ में): "नमस्ते सर! आपकी असुविधा के लिए हमें बेहद खेद है। हमारे Server में आपका पैसा अटका हुआ है। मैं अभी आपका Refund तुरंत Release कर रहा हूँ।"

User: "हाँ, बताइए मुझे क्या करना होगा?"

Scammer: "सर, Bank Server से Direct Connect करने के लिए Play Store से **'QuickSupport'** या **'AnyDesk'** App Download करें। App खोलते ही Screen पर 9 अंकों का Code आएगा, बस वह Code मुझे बता दें।"

User (Code देखकर): "हाँ, Code है 739-102-845।"

Scammer: "बहुत बढ़िया सर! अब अपना Google Pay या PhonePe App खोलें और Verification के लिए केवल ₹1 का Transfer करें।"

सच्चाई: *(जैसे ही User ने 9-Digit Code बताया, Scammer को User के Phone की पूरी Screen लाइव दिखने लगी। जैसे ही*

> *User ने ₹1 भेजने के लिए गुप्त UPI PIN डाला, Scammer ने वह PIN देख लिया। अगले 5 मिनट में User के खाते से ₹60,000 साफ़ हो गए!)*

Fake Customer Care का 4-Step Trap

1 **Google Search पर Fake Ads**

Scammers Google पर पैसे देकर अपने 10-अंकों के Fake Mobile Numbers को Search Results में सबसे ऊपर दिखाते हैं।

↓ मदद का मीठा नाटक

2 **Remote App Download करवाना**

Refund Release करने के बहाने Scammer आपसे AnyDesk, TeamViewer या QuickSupport Download करवाता है।

↓ 9-Digit Code की चोरी

3 **Screen Share Code हासिल करना**

जैसे ही आप Code बताते हैं, आपके Phone की पूरी Screen Scammer के Laptop या Phone पर Live चलने लगती है।

↓ UPI PIN देखकर खाता खाली

4 **Screen पर PIN देखना और पैसा गायब**

Scammer आपसे UPI App खुलवाता है, PIN देख लेता है और बैकग्राउंड में तुरंत सारा पैसा ट्रांसफर कर लेता है।

3 सबसे बड़े फर्क जो हमेशा याद रखें

🚫

1. Official Companies कभी AnyDesk Download नहीं करवातीं

कोई भी असली Company (Amazon, Flipkart, Bank, Zomato, Swiggy) कभी भी ग्राहक से AnyDesk या TeamViewer जैसा Screen Sharing App Download नहीं करवाती।

> **नियम:** जो भी Screen Sharing App कहे, वह 100% Scammer है।

📱

2. साधारण 10-अंकों का Mobile Number कभी Corporate Helpline नहीं होता

बड़ी कंपनियों और Bankों के Official Helpline Numbers हमेशा उनकी Verified Website के Contact Page पर मिलते

हैं। किसी भी साधारण 10-अंकों के अनजान Mobile Number पर कभी भरोसा न करें।

💳

3. Refund पाने के लिए कभी PIN नहीं डालना पड़ता

पैसा मिलने या Refund आने पर Bank सीधे खाते में पैसा जोड़ता है। अगर कोई कहे कि *"पैसे पाने के लिए अपना PIN दर्ज करें"*, तो समझ जाएँ कि वह ठग रहा है।

Official Advisory: Fake Support और Impersonation से बचाव

भारतीय रिज़र्व Bank (RBI) अपने जन-जागरूकता Portal **RBI Kehta Hai** पर कंपनी या Bank का अधिकारी बनकर होने वाली ठगी के खिलाफ यह कड़ा निर्देश देता है:

🌐 rbikehtahai.rbi.org.in (RBI Cautions)

Official RBI जनहित संदेश



📌 **RBI के Official Advisory से 2 सबसे बहुत ज़रूरी सबक:**

1. **Never Panic, Never Share Details:** Scammers डर या हड़बड़ी बनाकर जाल में फँसाते हैं। Call पर कभी भी अपनी निजी जानकारी, OTP या PIN Share न करें।
2. **Official Portal पर Report करें:** अगर किसी Fake Number पर बात हो गई हो या पैसा कट गया हो, तो तुरंत सीधे `cybercrime.gov.in` Portal पर जाकर Emergency ीन Report दर्ज करें।

Google पर Customer Care ढूँढते समय 4

सावधानियाँ

जब भी आपको किसी Company से संपर्क करना हो, तो इन 4 बातों का कड़ाई से पालन करें:

1. **चरण 1: App के भीतर "Help & Support" खोलें**
   Google पर Number ढूँढने के बजाय सीधे Swiggy, Amazon या Bank App के अंदर दिए गए "Contact Us" या "Chat Support" पर जाएँ।

2. **चरण 2: "Sponsored" या "Ad" लिखे Link को छोड़ दें**
   Google Search Result में सबसे ऊपर अगर किसी Link के आगे **Sponsored** या **Ad** लिखा हो, तो उस पर कभी Click न करें।

3. **चरण 3: साधारण 10-अंकों के Mobile Number पर Call न करें**
   अगर Search Result में किसी Company के नाम के आगे कोई साधारण Mobile Number दिख रहा हो, तो वह 100% Fake है।

4. **चरण 4: Card के पीछे लिखे Number का इस्तेमाल करें**
   अगर Bank से जुड़ा कोई मामला हो, तो हमेशा अपने Debit या Credit Card को पलटें और उस पर लिखे Official Helpline Number पर ही Call करें।

अध्याय 5: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• Customer Care से संपर्क के लिए हमेशा Official App के इन-बिल्ट Chat या Help Support का इस्तेमाल करें।

• Bank का मामला होने पर Debit या Credit Card के पीछे लिखे **Official Number** पर ही Call करें।

• Fake Helpline Numbers की Report **Chakshu Portal** (`sancharsaathi.gov.in`) पर करें।

❌ यह कभी न करें (DONTs)

• Google Search में दिखने वाले किसी भी अनजान Mobile Number पर आँख मूँदकर Call न करें।

• Customer Support के कहने पर AnyDesk, TeamViewer या QuickSupport App Download न करें।

• Refund लेने के नाम पर अपने Phone पर UPI PIN कभी दर्ज न करें।

OFFICIAL सत्यापन व शिकायत स्रोत

• Reserve Bank of India (RBI Impersonation Advisory): `rbikehtahai.rbi.org.in`

• National Cyber Crime Reporting Portal: `cybercrime.gov.in`

• Chakshu Fraud Reporting Portal: `sancharsaathi.gov.in`

• Telecom Regulatory Authority of India: `trai.gov.in`

अध्याय 6 • FAKE LOANS और ADVANCE FEES का सच

Loan, Credit Card और सरकारी Scheme के Call

बिना ब्याज Loan, Pre-Approved Credit Card और सरकारी योजना के नाम पर Processing Fees की ठगी से सुरक्षा।

Phone पर लाखों का Loan: वरदान या भयानक जाल?

सोचिए, आपको अपनी दुकान बढ़ाने, मकान की मरम्मत या बच्चों की पढ़ाई के लिए पैसों की सख्त ज़रूरत है। अचानक दोपहर में आपके Phone पर एक Call आती है:

"बधाई हो सर! आपके Aadhaar और PAN Card पर PM Mudra Loan योजना के तहत ₹5,00,000 का Business Loan Sanction हो चुका है। न कोई CIBIL Score चाहिए, न ITR और न ही कोई Guarantor। ब्याज केवल 1% सालाना है।"

लालच का खेल

बिना कागज़ात के लाखों का Loan क्यों नहीं मिलता?

Bankिंग का Basic नियम है कि कोई भी असली Bank किसी अनजान व्यक्ति को बिना पहचान और बिना CIBIL Score देखे ₹10,000 भी नहीं देता। Scammers जानते हैं कि मजबूरी में फँसा व्यक्ति आसान Loan के नाम पर तुरंत भरोसा कर लेता है।

> **सीधी बात:** असली Bank कभी Loan देने से पहले आपकी जेब से ₹1 भी Advance नहीं माँगता। सारे Charges हमेशा पास हुए Loan की रकम में से ही काटे जाते हैं।

Case Study: ₹5 लाख के Loan के चक्कर में ₹28,000 गँवाए

देखें कैसे Scammer नकली सरकारी लेटर दिखाकर किश्तों में पैसे ठगता है:

📞 PHONE CALL SIMULATION (FAKE LOAN EXECUTIVE)

> **Scammer (गंभीर और Professional आवाज़):** "सुरेश जी, आपका ₹5,00,000 का Loan Approved है। मैंने WhatsApp पर Sanction Letter भेजा है, Check कर लीजिए।"

सुरेश जी: *(WhatsApp खोलते हैं तो उस पर भारत सरकार का नकली लोगो, RBI की नकली मुहर और उनका नाम व Photo साफ दिखती है!)* "हाँ सर, लेटर तो मिल गया। पैसा कब मिलेगा?"

Scammer: "सर, File Final Approval पर है। सरकारी GST और File Charge के ₹2,500 आपको तुरंत नीचे दिए गए UPI Number पर भेजने होंगे। 15 मिनट में पैसा आपके खाते में आ जाएगा।"

सुरेश जी: *(₹2,500 भेज देते हैं। 20 मिनट बाद फिर Call आती है!)*

Scammer: "सुरेश जी, Finance Ministry के नियम के अनुसार इतनी बड़ी रकम के लिए ₹6,500 का Loan Insurance कराना बहुत ज़रूरी है। यह पैसा Refundable है, जल्दी जमा करें वरना File Cancel हो जाएगी!"

सच्चाई: *(सुरेश जी सोचते हैं कि ₹2,500 तो दे ही दिए हैं, अब पीछे नहीं हट सकते। वे Insurance, NOC और Tax के नाम पर कुल ₹28,000 भेज देते हैं। इसके बाद Scammer Phone Switch Off करके गायब हो जाता है!)*

Fake Loan Call का 4-Step Trap

1 **बिना कागज़ात के बड़े Loan का लालच**

Scammer Call करके कहता है: "न CIBIL चाहिए, न Salary Slip, 10 मिनट में ₹5 लाख का Loan तुरंत Pass।"

↓ नकली सरकारी कागज़

2 **WhatsApp पर Fake Sanction Letter**

सरकारी मुहर और RBI का Logo लगाकर नकली कागज़ात भेजे जाते हैं ताकि आपको 100% पक्का यकीन हो जाए।

↓ Advance Fees की माँग

3 **File Charge, GST या Insurance की माँग**

Scammer कहता है: "Loan की रकम भेजने के लिए पहले ₹2,500 से ₹5,000 Advance Fees जमा करें।"

↓ पैसे ऐंठना और Number Block

4 **किश्तों में पैसे लूटना और फरार होना**

एक बार पैसा मिलने के बाद वह नए-नए बहानों से और पैसे माँगता है और कभी ₹1 का Loan नहीं देता।

3 सबसे बड़े सच जो हमेशा याद रखें



1. असली Bank कभी Advance Processing Fee नहीं माँगता

RBI का साफ नियम है: कोई भी असली Bank या NBFC कभी ग्राहक से अपनी जेब से Advance पैसे जमा करने को नहीं कहता। सारे Charges हमेशा पास हुए Loan की रकम में से अपने आप काटे जाते हैं।

> **नियम:** जो भी Loan के लिए पहले पैसे माँगे, वह 100% Scammer है।



2. बिना CIBIL या Income Proof के कोई Loan नहीं मिलता

दुनिया का कोई भी Bank बिना आपकी पहचान और बिना Repayment क्षमता जाँचे लाखों रुपये नहीं बाँटता। जो भी बिना कागज़ के Loan का वादा करे, वह केवल ठग रहा है।



3. सरकारी योजना का पैसा Personal UPI पर नहीं जाता

PM Mudra Loan या अन्य सरकारी योजनाओं के नाम पर किसी व्यक्ति के Personal UPI या Bank Account में पैसे मँगवाना कानूनी अपराध है। सरकार कभी Call पर UPI से पैसे नहीं मँगवाती।

Official Portal: Fake Schemes और अवैध Loan की जाँच

भारतीय रिज़र्व Bank (RBI), SEBI और अन्य संस्थाओं ने देश के नागरिकों को Fake Financial Schemes और अवैध Loan से बचाने के लिए **Sachet Portal** शुरू किया है:

🌐 sachet.rbi.org.in (RBI Sachet Portal)

Official RBI व SEBI संयुक्त Portal



📌 **Sachet Portal से 2 सबसे बहुत ज़रूरी सबक:**

1. **Report Fictitious Phone Calls:** अगर किसी Phone Call पर बिना कागज़ के Loan, भारी Return या सरकारी योजना के नाम पर पैसे माँगे जा रहे हैं, तो सीधे Sachet Portal पर Report करें।
2. **Check Registered NBFCs:** किसी भी अनजान कंपनी या App से Loan लेने से पहले यहाँ Check करें कि वह RBI Registered Bank या NBFC है या नहीं।

अध्याय 6: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• Loan की ज़रूरत होने पर हमेशा सीधे अपने नज़दीकी Bank की शाखा में जाकर बात करें।

• अनजान Loan कंपनी की सत्यता हमेशा **Sachet Portal** (`sachet.rbi.org.in`) पर Check करें।

• Fake Loan Calls की Report सरकारी Portal **Chakshu** (`sancharsaathi.gov.in`) पर करें।

❌ यह कभी न करें (DONTs)

• Loan पास कराने या File Processing के नाम पर ₹1 भी Advance कभी न दें।

• WhatsApp पर आए किसी भी Sanction Letter या सरकारी मुहर वाले कागज़ पर भरोसा न करें।

• Phone Call पर किसी को भी अपने आधार, पैन या Bank Passbook की Photo न भेजें।

OFFICIAL सत्यापन व शिकायत स्रोत

• Sachet Multi-Regulator Portal (RBI, SEBI, IRDAI): `sachet.rbi.org.in`

• Reserve Bank of India (Digital Lending Framework): `rbi.org.in`

• National Cyber Crime Reporting Portal: `cybercrime.gov.in`

• Chakshu Fraud Reporting Portal: `sancharsaathi.gov.in`

अध्याय 7 • REMOTE ACCESS और PHONE HACKING का सच

Screen Sharing और Remote App Scam

AnyDesk, TeamViewer और QuickSupport से पूरा Phone Hack होने का सच और तुरंत बचने के तरीके।

जब आपका Phone किसी और के Control में चला जाता है

सोचिए, आपके Phone पर एक Call आती है। सामने वाला बहुत ही गंभीर आवाज़ में बोलता है: *"सर, आपके बिजली Bill का पिछला Payment System में नहीं दिख रहा है। आज रात 9:30 बजे आपके घर का बिजली कनेक्शन काट दिया जाएगा।"*

जब आप घबराकर कहते हैं कि मुझे Online यह सब ठीक करना नहीं आता, तो Scammer बहुत ही मददगार बनकर कहता है: *"कोई चिंता मत कीजिए सर, आपको कुछ नहीं करना। आप सीधे Google Play Store खोलिए और वहाँ से 'AnyDesk' या 'QuickSupport' App Download कर लीजिए। हमारी Support Team यहीं से बैठकर सब ठीक कर देगी।"*

गंभीर खतरा

Screen Sharing App कोई साधारण App नहीं है!

AnyDesk, TeamViewer और RustDesk जैसे Apps दुनिया भर में IT Engineers के काम के लिए बनाए गए हैं ताकि वे दूर बैठकर किसी Computer को ठीक कर सकें। लेकिन जब आप इसे अपने Phone में Download करते हैं, तो सामने वाला आपके Phone की हर एक Screen, हर एक Photo और आने वाले सभी OTPs को Live देख सकता है।

> **सीधी बात:** AnyDesk या TeamViewer का 9-Digit Code किसी अनजान व्यक्ति को बताना अपने घर की चाबी चोर के हाथ में सौंपने जैसा है।

Case Study: बिजली बिल के नाम पर ₹1.2 लाख साफ़

देखें कैसे Scammer 9-अंकों का Code लेकर Phone की पूरी Screen देख लेता है:

📞 PHONE CALL SIMULATION (FAKE SUPPORT EXECUTIVE)

> **Scammer (मददगार आवाज़ में):** "सतीश जी, बिल का केवल ₹110 बाकी है। मैं कोई Link नहीं भेज रहा, आप सीधे

Play Store से 'AnyDesk' App Download करें ताकि बिल का Server आपके Phone से Connect हो सके।"

सतीश जी: "हाँ, मैंने App Install कर लिया। Screen पर कुछ 9 अंकों का Number दिख रहा है।"

Scammer: "बस वही 9 अंकों का Code मुझे बता दीजिए सर, मैं कनेक्शन सुरक्षित कर रहा हूँ।"

सतीश जी (Code देखकर): "Code है 842-195-307।"

Scammer: "बहुत बढ़िया सर! अब अपना Google Pay या PhonePe खोलें और ₹110 का बिल Payment करें।"

सच्चाई: *(जैसे ही सतीश जी ने 9 अंकों का Code बताया, Scammer को सतीश जी के Phone की पूरी Screen लाइव दिखने लगी। जैसे ही सतीश जी ने ₹110 भेजने के लिए अपना 6 अंकों का गुप्त UPI PIN डाला, Scammer ने अपनी Screen पर वह PIN देख लिया। अगले 10 मिनट में सतीश जी के खाते से तीन बार में ₹1,20,000 साफ़ हो गए!)*

Remote App Scam का 4-Step Trap

1 **बिजली बिल, SIM या KYC का झूठा डर**

Scammer बिजली कटने, SIM बंद होने या Courier अटकने का डर दिखाकर आपको सोचने का मौका नहीं देता।

↓ Play Store से App Download

2 **Remote App (AnyDesk/TeamViewer) Install करवाना**

मदद का नाटक करके Play Store से AnyDesk, TeamViewer या QuickSupport Download करवाया जाता है।

↓ 9-Digit Access Code की चोरी

3 **Screen Share Code हासिल करना**

जैसे ही आप Code बताते हैं, आपके Phone की पूरी Screen Scammer के Laptop या Phone पर Live चलने लगती है।

↓ UPI PIN देखकर खाता खाली

4 **Screen पर PIN देखना और पैसे उड़ाना**

Scammer आपसे Banking App खुलवाता है, Screen पर PIN देख लेता है और मिनटों में पूरा खाता खाली कर देता है।

3 सबसे बड़े सच जो हमेशा याद रखें



1. 9-Digit Code आपके घर की चाबी है

AnyDesk या TeamViewer का 9-Digit Code किसी को बताना ऐसा ही है जैसे अपने घर की चाबी किसी चोर के हाथ में सौंप देना।

> **नियम:** Phone Call पर किसी भी व्यक्ति को यह Code कभी न बताएँ।



2. असली Bank कभी Remote Access नहीं माँगता

कोई भी असली Bank, बिजली विभाग या Telecom Company कभी भी ग्राहक से AnyDesk या Screen Sharing App Download करने को नहीं कहती।



3. Screen Share होते ही तुरंत Internet बंद करें

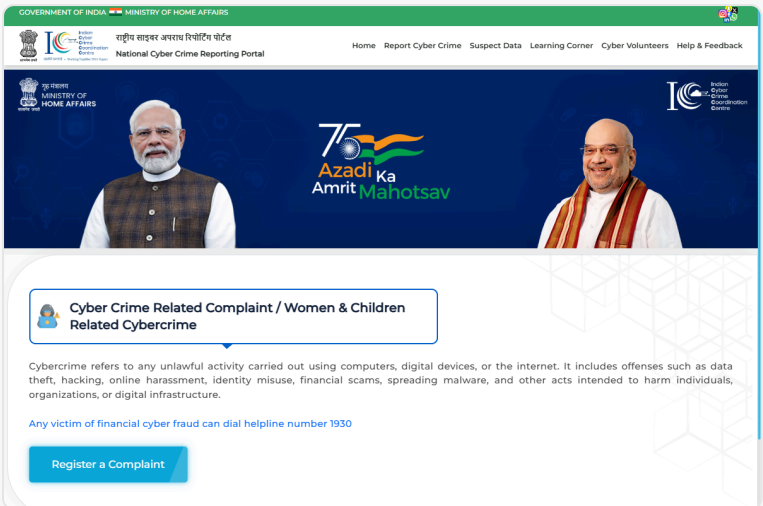
अगर गलती से Code बता भी दिया हो, तो 1 सेकंड भी गँवाए बिना तुरंत Phone का Mobile Data और Wi-Fi बंद करें या Flight Mode चालू कर दें।

Official Portal: Remote Fraud होने पर तुरंत क्या करें?

भारत सरकार के गृह मंत्रालय का **National Cyber Crime Reporting Portal** Cyber Fraud और पैसे की ठगी के खिलाफ 24 घंटे हेल्पलाइन चलाता है:

🌐 cybercrime.gov.in (National Cyber Crime Portal)

Official गृह मंत्रालय Portal



📌 **Cyber Crime Portal से 2 सबसे बहुत ज़रूरी बातें:**

1. **National Portal पर तुरंत जाएँ:** अगर किसी Remote App के ज़रिए खाते से पैसे कट जाएँ, तो बिना 1 मिनट गँवाए सीधे `cybercrime.gov.in` Portal पर जाकर Emergency ीन शिकायत दर्ज करें।
2. **Golden Hours में शिकायत:** शुरुआती 2 घंटे के भीतर Portal पर शिकायत दर्ज कराने से नोडल अधिकारी Bank खातों में पैसे को रास्ते में ही Freeze करवा देते हैं।

अगर गलती से Remote App Download हो जाए तो

तुरंत क्या करें?

अगर आपने किसी के कहने पर AnyDesk या Code बता दिया है, तो तुरंत इन 4 कदमों का पालन करें:

1. **कदम 1: तुरंत Flight Mode चालू करें**
   Phone की Screen ऊपर से नीचे खींचे और **Flight Mode** चालू कर दें। इससे Internet तुरंत बंद हो जाएगा और Scammer का कनेक्शन कट जाएगा।

2. **कदम 2: Remote App को तुरंत Uninstall करें**
   AnyDesk, TeamViewer या QuickSupport App पर उंगली दबाकर रखें और उसे तुरंत अपने Phone से **Uninstall (Delete)** कर दें।

3. **कदम 3: दूसरे Phone से Bank को सूचित करें**
   परिवार के किसी सदस्य के Phone से तुरंत अपने Bank के Official Number पर Call करके अपनी Net Banking और UPI ID को तुरंत Block करवाएँ।

4. **कदम 4: Cyber Crime Portal पर तुरंत Report करें**
   घटना की तुरंत शिकायत सीधे `cybercrime.gov.in` Portal पर दर्ज करवाएँ और Portal पर दिए Emergency Helpline से Bank नोडल अधिकारी से संपर्क करें।

अध्याय 7: क्या करें और क्या न करें

✅ हमेशा यह करें (DOs)

• बिजली बिल या KYC के लिए हमेशा संबंधित विभाग के Official Office या App का इस्तेमाल करें।

• शक होते ही Phone का Internet (Mobile Data व Wi-Fi) तुरंत बंद कर दें।

• Fraud की तुरंत शिकायत `cybercrime.gov.in` Portal पर दर्ज करें।

❌ यह कभी न करें (DONTs)

• Phone Call पर किसी अनजान व्यक्ति के कहने पर AnyDesk या TeamViewer Download न करें।

• Screen पर दिखने वाला 9 या 10 अंकों का Code किसी को भी कभी न बताएँ।

• Screen Sharing चालू रहने के दौरान कोई भी Banking या UPI App कभी न खोलें।

OFFICIAL सत्यापन व शिकायत स्रोत

• National Cyber Crime Reporting Portal (MHA): `cybercrime.gov.in`

• Indian Computer Emergency Response Team: `cert-in.org.in`

• Reserve Bank of India (Cyber Security Framework): `rbi.org.in`

• Chakshu Fraud Reporting Portal: `sancharsaathi.gov.in`

अध्याय 8 • AI VOICE CLONING SCAM

AI Voice Clone: अपनों की आवाज़ में Call

Accident, Police पकड़ने का नाटक और AI से बनाई अपनों की असली जैसी आवाज़ का सच।

रोती हुई आवाज़: "पापा, मेरा भयानक Accident हो गया है!"

सोचिए, दोपहर के समय आपके Phone की घंटी बजती है। Screen पर एक अनजान Number दिखता है। जैसे ही आप Call उठाते हैं, दूसरी तरफ से रोने और चीखने की आवाज़ आती है:

"पापा... मैं रोहन बोल रहा हूँ! मेरा बहुत बुरा Accident हो गया है। एक आदमी को चोट लग गई है और भीड़ मुझे मार रही है। मुझे तुरंत अस्पताल और समझौते के लिए ₹40,000 चाहिए। मैं अपने दोस्त के Phone से Call कर रहा हूँ, तुरंत इस Number पर पैसे भेज दीजिए!"

आवाज़ बिल्कुल आपके बेटे की है। वही आवाज़, वही रोने का अंदाज़ और वही डर। कोई भी माता-पिता ऐसी Call सुनकर काँप उठेंगे।

खतरे की सच्चाई **लेकिन असली सच क्या था?**

रोहन अपनी Call ेज की लाइब्रेरी में शांति से पढ़ाई कर रहा था। उसके साथ कोई Accident नहीं हुआ था। वह रोती हुई आवाज़ रोहन की नहीं, बल्कि AI (Artificial Intelligence) से तैयार की गई एक Fake Voice थी!

> **सीधी बात:** केवल कानों से आवाज़ सुनकर विश्वास न करें। Scammers Internet से 5 सेकंड की आवाज़ चुराकर बिल्कुल हूबहू नकली आवाज़ बना सकते हैं।

Case Study: भतीजा बनकर ₹45,000 की ठगी

देखें कैसे Scammer रोने का नाटक करके परिवार के लोगों को डराता है:

📞 PHONE CALL SIMULATION (FAKE NEPHEW & POLICE)

> **Fake Nephew (रोने और चीखने की आवाज़):** "चाचा जी, मैं आपका भतीजा अमित बोल रहा हूँ... Police ने मुझे एक केस में पकड़ लिया है, मेरा Phone ज़ब्त है। इंस्पेक्टर साहब बात कर रहे हैं, कृपया मुझे बचा लीजिए!"

> **Fake Inspector (कड़क और भारी आवाज़):** "हेलो, मैं Sub-Inspector बोल रहा हूँ। आपके भतीजे पर FIR दर्ज हो

रही है। अगर कोर्ट और जेल जाने से बचाना है, तो तुरंत ₹45,000 इस UPI ID पर Transfer करें। आपके पास केवल 15 मिनट हैं!"

चाचा जी (डरकर): *(आवाज़ सचमुच अमित की ही लग रही थी, डर के मारे उन्होंने बिना सोचे-समझे तुरंत पैसे Transfer कर दिए!)*

सच्चाई: अमित पूरे दिन अपने Office में काम कर रहा था। Scammer ने अमित के Instagram Reel Video से केवल 5 सेकंड का Audio उठाकर AI Software में डाला था।

Scammers AI Voice Clone कैसे तैयार करते हैं?

1. **Social Media से Audio चुराना**
   Scammers आपके Instagram Reels, Facebook Videos या YouTube Shorts से 5–10 सेकंड का साफ़ Audio Sample Download करते हैं।

   ↓ मशीन लर्निंग Software में Upload

2. **AI द्वारा आवाज़ की नकल**
   AI Voice Cloning Tools आवाज़ की पिच, टोन और बोलने की शैली को पूरी तरह सीख लेते हैं।

↓ कोई भी नया वाक्य बुलवाना

3 **Accident या Police का झूठा नाटक**

Scammer AI Tool में मनचाहे शब्द टाइप करता है और वह रोने या चिल्लाने की आवाज़ में Call पर बोलकर सुना देता है।

↓ डर और हड़बड़ी में पैसे ट्रांसफर

4 **हड़बड़ी में UPI द्वारा पैसे गायब**

पीड़ित परिवार घबराकर बिना सोचे-समझे तुरंत पैसे Transfer कर देता है और Scammer Phone बंद कर लेता है।

3 सबसे असरदार तरीके: Fake Voice Call को कैसे पकड़ें



1. Family Secret Code (पारिवारिक Secret Code)

अपने परिवार के सदस्यों के साथ एक गुप्त शब्द या सवाल तय करें (जैसे बचपन का कोई पालतू नाम या कोई खास तारीख)।

> **Golden टिप:** जब भी कोई मुसीबत की Call आए, सबसे पहले वह Secret Code पूछें। AI यह कभी नहीं बता सकता।



2. तुरंत Call काटें और असली Number पर मिलाएँ

अनजान Number से आई Call पर कभी भरोसा न करें। तुरंत Call काटें और अपने बच्चे या रिश्तेदार के असली Mobile Number पर Call मिलाएँ।

> **अगर Phone न लगे:** उसके दोस्त, रूममेट, Colleज या Office के साथी को Call करके सच्चाई पता करें।



3. निजी सवाल पूछें जिसका जवाब सिर्फ वही जानता हो

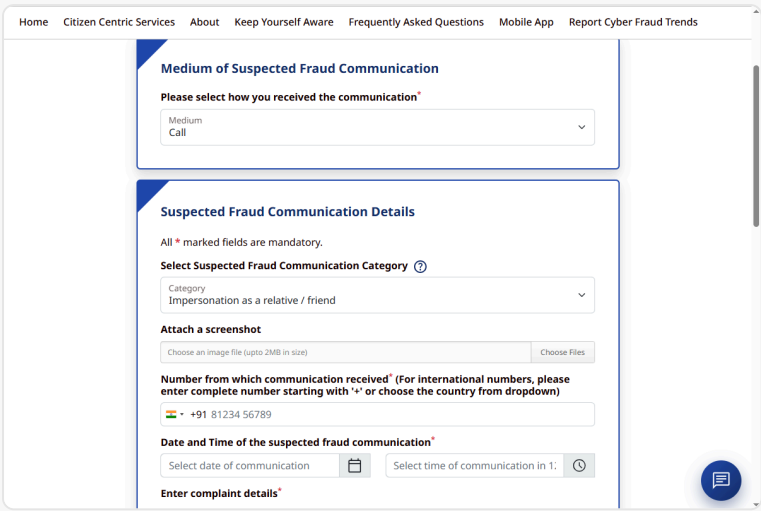
Scammer के पास सिर्फ आवाज़ की नकल होती है, आपकी निजी बातें नहीं।

> **तुरंत पूछें:** "कल रात घर में क्या खाना बना था?" या "हमारी पुरानी कार का Number क्या था?"

Official Portal पर Fake Call की तुरंत शिकायत करें

भारत सरकार के Telecom Department ने Sanchar Saathi Portal पर **Chakshu (चक्षु)** सुविधा शुरू की है, जहाँ आप रिश्तेदार बनकर आई Fake Calls की Report कर सकते हैं:

sancharsaathi.gov.in/sfc • Chakshu Portal **Official Portal**



Chakshu Portal पर 3 आसान Steps में Report करें:

1. **Medium चुनें:** Chakshu Reporting Page पर जाकर `Call` का विकल्प चुनें।
2. **Category चुनें:** सूची में से `Impersonation as a relative / friend` चुनें।
3. **अनजान Number व विवरण भरें:** जिस Number से Fake Call आई थी, उसका समय लिखकर OTP से Form Submit कर दें।

क्या करें और क्या न करें (Golden Rules)

✓ क्या करें (Do's)

✓ Call को तुरंत काटें और परिवार के असली Number पर Call करें।

✓ परिवार में एक Secret Code रखें जो सिर्फ आप लोगों को पता हो।

✓ अनजान व्यक्ति से निजी बातें और ऐसा सवाल पूछें जो Scammer न जानता हो।

✓ यदि पैसे कट गए हों तो 15 मिनट के अंदर cybercrime.gov.in Portal पर जाएँ।

✗ क्या न करें (Don'ts)

✗ रोने या चीखने की आवाज़ सुनकर घबराएँ नहीं।

✗ अनजान व्यक्ति के कहे किसी नए UPI ID या खाते में पैसे न भेजें।

✗ Social Media पर अपनी आवाज़ और पूरी निजी दिनचर्या Public न रखें।

✗ किसी भी 'Inspector' या 'Doctor' की धमकी में आकर तुरंत Payment न करें।

जाँचे गए OFFICIAL स्रोत (VERIFIED SOURCES)

National Cyber Crime Reporting Portal: `cybercrime.gov.in`

DoT Sanchar Saathi Chakshu Facility: `sancharsaathi.gov.in/sfc/`

Indian Cybercrime Coordination Centre (I4C) & Cyber Dost Advisory on Deepfake & AI Voice Cloning

अध्याय 9 • ONE-RING व INTERNATIONAL MISSED CALL SCAM

Missed Call और अनजान Number के जाल

विदेशी Country Code से 1 सेकंड की Missed Call, Call Back करने पर भारी Bill और Wangiri Fraud का सच।

रात के 2 बजे 1 सेकंड की घंटी: One-Ring Scam (Wangiri Fraud)

सोचिए, सुबह उठकर जब आप अपना Phone देखते हैं, तो Screen पर एक अनजान Number से Missed Call दिखती है। Number कुछ ऐसा होता है: `+882 13...`, `+232 21...` या `+247...`।

इंसान के मन में स्वाभाविक रूप से जानने की इच्छा होती है: *"अरे! किसका Phone था? शायद विदेश से किसी रिश्तेदार या पुराने दोस्त ने किया हो!"*

जैसे ही आप उस अनजान Number पर Call Back करते हैं, दूसरी तरफ कोई बात नहीं करता। बस एक अजीब सा संगीत बजता रहता है या Computer की आवाज़ बोलती है: *"लाइन पर बने रहें, आपकी Call जोड़ी जा रही है..."*

खतरे की सच्चाई **Call Back करते ही जेब पर डाका**

आप 2 या 3 मिनट इंतज़ार करते हैं और फिर Phone काट देते हैं। आपको लगता है कि कोई बात नहीं हुई, लेकिन जब आपके Mobile का Prepaid Balance Check होता है या Postpaid Bill आता है, तो पता चलता है कि केवल 2 मिनट के ₹500 कट चुके हैं!

> **सीधी बात:** इसे दुनिया भर में **Wangiri Scam** या **One-Ring Scam** कहा जाता है। अनजान विदेशी Number पर कभी भी पलटकर Call न करें।

Case Study: Phone Balance से ₹1,400 उड़ गए

देखें कैसे 1 सेकंड की Missed Call पर Call Back करने से भारी बिल बनता है:

📞 PHONE CALL SIMULATION (ONE-RING WANGIRI TRAP)

> **मोहित जी:** *(Screen पर +882 Number से Missed Call देखकर)* "शायद विदेश में रहने वाले किसी दोस्त का नया Number होगा, एक बार मिलाकर देख लेता हूँ।"

> **Recorded Audio (मीठी व लुभावनी आवाज़):** "बधाई हो! आपका Mobile Number इंटरनेशनल Lucky Draw के लिए चुना गया है। अपने ₹25 लाख के इनाम की जानकारी सुनने के लिए 1 दबाएँ और लाइन पर बने रहें..."

> **मोहित जी:** *(1 दबाकर 4 मिनट तक लाइन पर इंतज़ार करते रहे, बस एक धुन बजती रही और कोई बात नहीं हुई)*

> **सच्चाई:** जैसे ही Call कटी, मोहित जी के Main Balance से ₹1,400 कट गए! यह एक Premium-Rate International Number था, जिसका पैसा सीधे Scammer की विदेशी कंपनी के पास गया।

One-Ring Scam का 4-Step चक्र

1 **Computer द्वारा 1-Ring Call**

Scammers Auto-Dialer Software से एक साथ लाखों लोगों के Numbers पर केवल 1 सेकंड की घंटी बजाकर Call काट देते हैं।

↓ जानने की इच्छा का फायदा

2 **User द्वारा Call Back**

लोग सोचते हैं कि कोई ज़रूरी Call छूट गई है और वे बिना सोचे-समझे उस अनजान विदेशी Number पर Call मिला देते हैं।

↓ Premium Line से कनेक्ट होना

3 **Line पर जान-बूझकर रोके रखना**

रिकॉर्डेड धुन या लॉटरी का लालच देकर User को 3 से 5 मिनट तक Phone पर उलझाए रखा जाता है।

↓ भारी ISD बिल की कटौती

4 **₹100 से ₹300 प्रति मिनट का झटका**

User के Balance या Postpaid बिल से मोटी रकम कटती है, जिसका कमीशन विदेशी ऑपरेटर से Scammer को मिलता है।

3 बड़े नियम: अनजान Missed Call से कैसे बचें

🚫

1. +91 के अलावा अनजान Numbers पर Call Back न करें

भारत का Country Code +91 है। अगर Number के आगे कोई अजीब Code जैसे +882, +232, +247 या +685 लगा है, तो

कभी भी Call Back न करें।

> **सीधा नियम:** जिस व्यक्ति को आप नहीं जानते, उसकी विदेशी Missed Call को तुरंत Ignore या Block करें।



2. ज़रूरी Call हमेशा दोबारा आएगी

अगर किसी रिश्तेदार या Office वाले को सच में कोई ज़रूरी काम है, तो वह केवल 1 सेकंड की घंटी बजाकर नहीं छोड़ेगा।

> **याद रखें:** वह दोबारा Call करेगा या SMS/WhatsApp भेजेगा।



3. TRAI DND (Do Not Disturb) सेवा सक्रिय करें

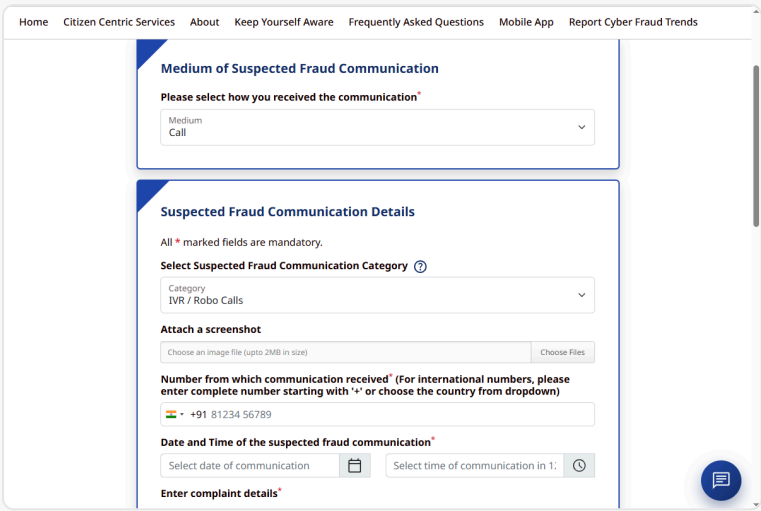
TRAI की Official Website (`trai.gov.in`) या Official TRAI DND App का उपयोग करके DND सक्रिय करें।

> **फायदा:** अनचाहे कमर्शियल और Spam Calls पर तुरंत रोक लगती है।

Sanchar Saathi Chakshu Portal पर Spam Call की शिकायत करें

यदि आपके Phone पर बार-बार अनजान विदेशी Calls, रोबोट Calls या 1-Ring स्पैम आ रहे हैं, तो भारत सरकार के Chakshu Portal पर Report करें:

sancharsaathi.gov.in/sfc • Chakshu Portal **Official Portal**



Chakshu Portal पर 3 आसान Steps में Spam Call Report करें:

1. **Medium चुनें:** Chakshu Reporting Page पर जाकर `Call` विकल्प चुनें।
2. **Category चुनें:** Drawपडाउन मेनू से `IVR / Robo Calls` विकल्प चुनें।
3. **अनजान Number दर्ज करें:** उस अनजान विदेशी या स्पैम Number की जानकारी और समय लिखकर Submit करें।

क्या करें और क्या न करें (Golden Rules)

✓ क्या करें (Do's)

✓ अनजान विदेशी Number से आई 1-Ring Missed Call को तुरंत Ignore या Block करें।

✓ TRAI DND App या Official Website के ज़रिए अपने Number पर DND सेवा सक्रिय रखें।

✓ बार-बार आने वाली Spam Calls को Chakshu Portal (`sancharsaathi.gov.in`) पर Report करें।

✓ अगर गलती से Call मिल जाए, तो 1 सेकंड में तुरंत Phone काट दें।

× क्या न करें (Don'ts)

× जानने की इच्छा में कभी भी अनजान विदेशी Number पर Call Back न करें।

× Call पर बज रहे संगीत या Computer की आवाज़ को सुनने के लिए Line पर न रुके रहें।

× रिकॉर्डेड Call पर कभी कोई Button न दबाएँ।

× अनजान Number से आए किसी Link पर Click न करें।

जाँचे गए OFFICIAL स्रोत (VERIFIED SOURCES)

Telecom Department (DoT) Advisory on International Missed Call & Wangiri Frauds

TRAI Telecom Commercial Communications Customer Preference Regulations & Official DND Registry

DoT Sanchar Saathi Chakshu Facility: `sancharsaathi.gov.in/sfc/`

National Cyber Crime Reporting Portal: `cybercrime.gov.in`

अध्याय 10 • FAKE STOCK TRADING COURSES

Course और Financial Freedom के Fake Call

शेयर बाज़ार में पक्का मुनाफा, ₹35,000 का कोर्स और 'Secret Strategy' के नाम पर होने वाली ठगी का सच।

Phone पर अमीर बनने का सपना: "महीने का ₹2 लाख पक्का कमाएँ!"

सोचिए, दोपहर के समय आपके Phone की घंटी बजती है। सामने से एक बहुत ही आत्मविश्वास से भरा लड़का या लड़की बोलती है:

"नमस्ते सर! क्या आप अपनी सामान्य नौकरी से परेशान हैं? क्या आप घर बैठे Financial Freedom पाना चाहते हैं? हमारी रिसर्च टीम ने शेयर बाज़ार की एक ऐसी Secret Strategy तैयार की है, जिससे हमारे क्लाइंट्स रोज़ाना ₹10,000 से ₹25,000 कमा रहे हैं। आज शाम को हमारा Special Webinar है, क्या मैं आपकी Seat Book कर दूँ?"

सामने वाला बहुत ही प्रोफेशनल भाषा में बात करता है। वह आपको WhatsApp पर बड़ी-बड़ी लक्ज़री गाड़ियों, महँगे Hotels और लाखों के मुनाफे वाले Fake Profit Screenshots भेजता है।

कानूनी सच्चाई **SEBI का कड़ा नियम**

भारत के बाज़ार की संस्था SEBI (Securities and Exchange Board of India) का सख्त नियम है: **शेयर बाज़ार में कोई भी व्यक्ति कभी Guaranteed Return या पक्के मुनाफे का वादा नहीं कर सकता।**

> **सीधी बात:** जो व्यक्ति आपको पक्के मुनाफे का वादा कर रहा है, वह खुद ट्रेडिंग से नहीं, बल्कि आपके Course की Fees से पैसे कमा रहा है।

Case Study: "No-Loss Course" के नाम पर ₹35,000 की चपत

देखें कैसे Phone Call पर झूठे सपने दिखाकर पैसे ठगे जाते हैं:

📞 PHONE CALL SIMULATION (FAKE STOCK MARKET GURU)

> **Course Executive:** "सर, केवल 5 सीटें बची हैं! हमारी 3-दिन की 'VIP Masterclass' में हम ऐसी Secret Strategy सिखाएँगे जो कभी फेल नहीं होती। Course की Fees ₹35,000 है, जो आप 1 हफ्ते की Trading में वापस निकाल लेंगे।"

> **User:** "लेकिन क्या इसमें नुकसान का कोई रिस्क है? मुझे शेयर बाज़ार की ज़्यादा समझ नहीं है।"

> **Course Executive:** "बिल्कुल 0% रिस्क सर! हमारी टीम रोज़ WhatsApp पर 3 पक्की Tips देगी। आँख मूँदकर Buy और Sell करना, बस आज ही Seat Book कर लीजिए।"

> **सच्चाई:** पैसे भेजते ही YouTube के कुछ पुराने और साधारण Videos के Link थमा दिए गए। जब User ने बाज़ार में बताए गए शेयरों में पैसे लगाए, तो ₹80,000 और डूब गए। मदद माँगने पर Scammer ने उसका Number Block कर दिया!

Fake Course Scam का 4-Step चक्र

1. **Social Media पर दौलत का झूठा दिखावा**
   किराए की लक्ज़री कारों और Photoshop से बने लाखों के मुनाफे के Fake Screenshots दिखाकर लोगों को लुभाया जाता है।

   ↓ अनजान Numbers पर Cold Calling

2. **Phone पर "Financial Freedom" का लालच**
   डेटाबेस से Number निकालकर लोगों को Call किया जाता है और "घर बैठे Side Income" का लालच दिया जाता है।

↓ भारी Fees की वसूली

3 **₹15,000 से ₹50,000 की Fees**

"सीमित सीटें" और "आज ही डिस्काउंट" का दबाव बनाकर तुरंत UPI द्वारा महँगी कोर्स Fees ऐंठ ली जाती है।

↓ नुकसान होने पर Number Block

4 **मुफ्त का पुराना Content और गायब**

Internet से चुराए गए 10 मिनट के साधारण Videos देकर पल्ला झाड़ लिया जाता है और छात्र को Group से निकाल दिया जाता है।

3 सबसे बड़े नियम: Fake Stock Market Calls से कैसे बचें

🔍

1. SEBI Registration की जाँच करें

भारत में शेयर बाज़ार की सलाह देने के लिए SEBI Registered होना बहुत ज़रूरी है।

> **सीधा नियम:** पैसे देने से पहले SEBI की Official Website (`sebi.gov.in`) पर उसका Registration Number ज़रूर जाँचे।

⚠️

2. "Guaranteed Return" का मतलब है सिर्फ Fraud

शेयर बाज़ार में कोई भी व्यक्ति कभी 100% पक्का मुनाफा नहीं दे सकता।

> **याद रखें:** अगर कोई व्यक्ति No-Risk का दावा कर रहा है, तो वह सबसे बड़ा Scammer है।

📜

3. "Educational Purpose" वाले बहाने से सावधान रहें

Scammers चालाकी से कहते हैं कि "यह सिर्फ पढ़ाई के लिए है", लेकिन अंदर शेयर खरीदने की टिप्स देते हैं।

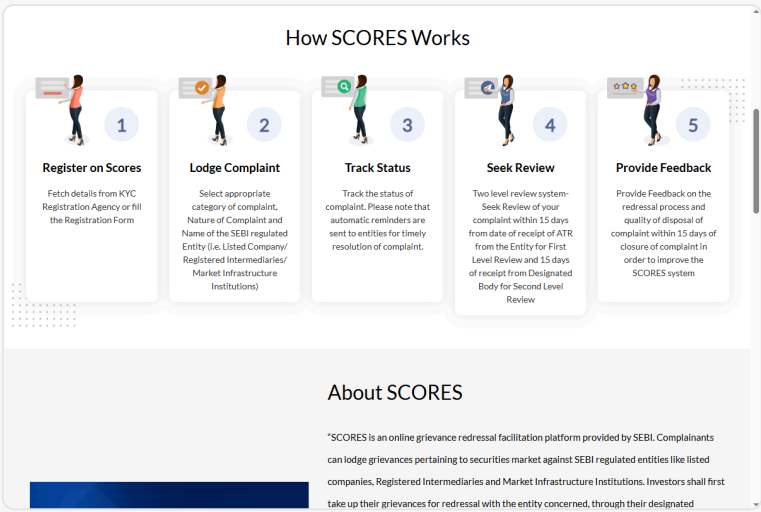
> **कानूनी सच:** बिना रजिस्ट्रेशन टिप्स देना SEBI के तहत गैर-कानूनी अपराध है।

SEBI के SCORES Portal पर अवैध कोर्स की शिकायत करें

अगर किसी व्यक्ति या संस्था ने शेयर बाज़ार के झूठे वादे या बिना रजिस्ट्रेशन के टिप्स देकर ठगी की है, तो SEBI के Official SCORES Portal पर शिकायत दर्ज करें:

scores.sebi.gov.in • SEBI SCORES Portal

Official Portal



SCORES Portal पर 3 आसान Steps में शिकायत करें:

1. **Register on Scores:** Google पर जाकर सीधे `scores.sebi.gov.in` खोलें और अपना रजिस्ट्रेशन पूरा करें।
2. **Lodge Complaint:** शिकायत की सही Category चुनें और उस फर्जी संस्था या व्यक्ति का विवरण दर्ज करें।
3. **Track Status:** अपनी शिकायत का स्टेटस Online ट्रैक करें और SEBI के एक्शन की जानकारी लें।

क्या करें और क्या न करें (Golden Rules)

✓ क्या करें (Do's)

✓ किसी भी एडवाइजर को पैसे देने से पहले SEBI की Official Website पर उसका नाम जाँचे।

✓ शेयर बाज़ार में खुद पढ़ाई करके और अपनी समझ से निवेश करें।

✓ फर्जी दावों की शिकायत सीधे SEBI SCORES Portal (`scores.sebi.gov.in`) पर करें।

✓ किसी भी अनजान व्यक्ति के दावों को हमेशा स्वतंत्र रूप से Verify करें।

× क्या न करें (Don'ts)

× Phone Call पर "रातों-रात अमीर बनने" के झाँसे में आकर कभी पैसे न भेजें।

× किसी भी अनजान व्यक्ति को अपना Trading Account या Demat Password न दें।

× Loan या Credit Card से पैसे उधार लेकर कोई Trading Course न खरीदें।

× Social Media पर दिखाए जाने वाले कारों और मुनाफे के Fake Screenshots पर भरोसा न करें।

जाँचे गए OFFICIAL स्रोत (VERIFIED SOURCES)

Securities and Exchange Board of India (SEBI): `sebi.gov.in`

SEBI Complaints Redress System (SCORES): `scores.sebi.gov.in`

National Stock Exchange (NSE) & BSE Investor Protection Guidelines

National Cyber Crime Reporting Portal: `cybercrime.gov.in`

अध्याय 11 • FAKE MEMBERSHIP & HOLIDAY CLUB FRAUD

Fake Membership और बड़े वादे

मुफ्त 5-Star Hotel Stay का लालच, 25 साल की VIP Club Membership और Credit Card से लाखों की चपत का सच।

मुफ्त का झाँसा: "बधाई हो, आपको 5-Star Hotel Stay मिला है!"

सोचिए, एक दिन आपके Phone की घंटी बजती है। सामने से एक बहुत ही विनम्र आवाज़ में लड़की बोलती है:

"बधाई हो सर! आपने पिछले महीने Mall में जो Lucky Draw Coupon भरा था, उसमें आपका Number पहले 10 लकी विजेताओं में चुना गया है। आपको और आपके परिवार को 3 रात और 4 दिन का 5-Star Hotel Stay और लक्ज़री Club का VIP Welcome Voucher मिला है!"

Caller आपसे कहता है कि आपको कोई पैसा नहीं देना है। बस आज शाम को किसी बड़े Hotel के Banquet Hall में आकर अपना Lucky Coupon और Gift Voucher Collect करना है।

खतरे की सच्चाई **Hotel पहुँचते ही सामाजिक दबाव का जाल**

वहाँ आपको 25 साल की 'Holiday Club Membership' बेची जाती है। आपसे कहा जाता है: *"सर, इसकी असली कीमत ₹2 लाख है, लेकिन Lucky Draw विनर होने के नाते आपको केवल ₹55,000 देने हैं। यह मौका केवल आज रात 9 बजे तक है, तुरंत अपना Credit Card दीजिए!"*

> **सीधी बात:** दुनिया में कोई भी असली कंपनी किसी अनजान व्यक्ति को लाखों का लक्ज़री Stay मुफ्त में नहीं बाँटती। "Free Voucher" केवल Card Swipe करवाने का बहाना है।

Case Study: गोवा ट्रिप के नाम पर ₹55,000 की चपत

देखें कैसे Hotel Presentation में दबाव बनाकर Credit Card से पैसे कटवाए जाते हैं:

📞 HOTEL SALES SIMULATION (FAKE HOLIDAY MEMBERSHIP)

> **Club Executive:** "सर, पूरे देश के 50 से ज़्यादा 5-Star Hotels में 10 साल तक हर साल 6 रात का Stay बिल्कुल फ्री

है! बस एक्टिवेशन के लिए आज ही ₹55,000 का Card Swipe करना होगा।"

User: "क्या मुझे बाद में कमरे Book करते समय कोई Extra पैसा देना होगा?"

Club Executive: "बिल्कुल नहीं सर, सब कुछ 100% फ्री है। बस यह स्पेशल ऑफर सिर्फ अभी 10 मिनट के लिए मान्य है।"

सच्चाई: 4 महीने बाद जब User ने परिवार के साथ गोवा जाने के लिए Call किया, तो कहा गया कि "उस हफ्ते कोई कमरा खाली नहीं है और ₹15,000 का Maintenance Charge अलग से लगेगा।" पैसे वापस माँगने पर कहा गया कि Agreement Non-Refundable है!

Club Membership Scam का 4-Step चक्र

1 **Mall में Lucky Draw के नाम पर डेटा**

मुफ्त गिफ्ट Coupon या मूवी टिकट के बहाने आपका नाम, Mobile Number और सैलरी का डेटा जुटाया जाता है।

↓ Hotel Banquet Hall में बुलावा

2 **2 घंटे का भारी Presentation और दबाव**

तेज़ संगीत और तालियों के बीच परिवार को अकेले बिठाकर सोचने या घर वालों से बात करने का मौका नहीं दिया जाता।

↓ Credit Card से तुरंत Swipe

3 **₹30,000 से ₹1,00,000 की कटौती**

"सिर्फ आज के लिए Discount" का दबाव बनाकर तुरंत Card Swipe करवा लिया जाता है और Form पर साइन करा लिया जाता है।

↓ Booking के समय कमरे गायब

4 **Hidden Charges और Non-Refundable का बहाना**

बाद में कभी Hotel नहीं मिलता और पैसे वापस माँगने पर Agreement के बारीक नियमों का हवाला देकर टरका दिया जाता है।

3 सबसे बड़े नियम: Fake Membership से कैसे बचें

🎁

1. मुफ्त कुछ नहीं होता

Hotel Stay, Club Membership या Gift Voucher केवल एक चारा होता है।

> **सीधा नियम:** अगर कोई कंपनी "फ्री Lucky Draw" कहकर Hotel में बुलाए, तो वहाँ कभी न जाएँ।



2. मौके पर कभी Credit Card Swipe न करें

चाहे Salesman कितना भी बड़ा Discount क्यों न दे, कभी भी उसी समय Card न दें।

> **साफ बोलें:** "मैं Agreement की Copy घर ले जाऊँगा और शांति से नियम पढ़ने के बाद ही फैसला लूँगा।"



3. मौखिक बातों की कोई कानूनी कीमत नहीं

Salesman जो भी मीठे वादे करे, अगर वह लिखित Agreement में दर्ज नहीं है, तो वह पूरी तरह बेबुनियाद है।

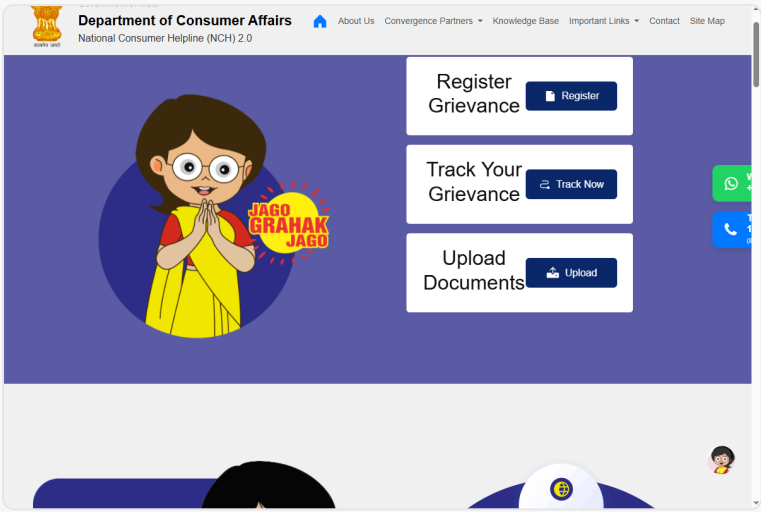
> **Check करें:** Form साइन करने से पहले Refund और Cancellation के नियम खुद पढ़ें।

National Consumer Helpline Portal पर शिकायत करें

यदि किसी Holiday Club या कंपनी ने झूठे वादे करके आपके पैसे फँसा दिए हैं, तो भारत सरकार के उपभोक्ता मामलों के विभाग के Official Portal पर Online शिकायत दर्ज करें:

`consumerhelpline.gov.in` • National Consumer Helpline (NCH 2.0)

Official Government Portal



NCH Portal पर 3 आसान Steps में शिकायत दर्ज करें:

1. **Official Portal खोलें:** Google पर जाकर सीधे `consumerhelpline.gov.in` खोलें।
2. **Register Grievance:** Portal पर 'Register Grievance' पर Click करें और कंपनी के खिलाफ शिकायत दर्ज करें।
3. **दस्तावेज़ Upload करें:** Payment Slip, Card Statement और Membership Agreement की Copy Upload करें।

क्या करें और क्या न करें (Golden Rules)

✓ क्या करें (Do's)

✓ किसी भी कंपनी से जुड़ने से पहले Internet पर उसके Reviews और शिकायतें ज़रूर पढ़ें।

✓ Card से अनचाहे पैसे कटने पर Bank में तुरंत Chargeback की अर्जी लगाएँ।

✓ ठगी होने पर National Consumer Helpline Portal (`consumerhelpline.gov.in`) पर शिकायत दर्ज करें।

✓ Agreement की लिखित Copy पर Refund Policy ज़रूर Check करें।

× क्या न करें (Don'ts)

× "Free Holiday Voucher" के Phone पर कभी किसी Hotel Presentation में न जाएँ।

× Presentation Hall के सामाजिक दबाव में आकर कभी तुरंत Credit Card Swipe न करें।

× Salesman के मौखिक वादों पर बिना लिखित सबूत के भरोसा न करें।

× बिना पढ़े किसी भी लंबे Agreement या Form पर कभी साइन न करें।

जाँचे गए OFFICIAL स्रोत (VERIFIED SOURCES)

Department of Consumer Affairs, Government of India: `consumerhelpline.gov.in`

Central Consumer Protection Authority (CCPA) Guidelines on Misleading Advertisements & Unfair Contracts

Reserve Bank of India (RBI) Regulations on Credit Card Chargeback & Disputed Transactions

National Cyber Crime Reporting Portal: `cybercrime.gov.in`

अध्याय 12 • FAKE LOAN APPS & RECOVERY AGENT THREATS

Loan Fraud और Recovery Agent की धमकी

7-दिन वाले Fake Loan Apps का जाल, Gallery Hack, Morphed Photos और Recovery Agent की धमकी से बचाव के कानूनी नियम।

Instant Loan का झाँसा: "बिना सैलरी स्लिप 2 मिनट में ₹50,000 Loan!"

अक्सर Social Media, SMS या WhatsApp पर ऐसे लुभावने Message आते हैं:

"बिना किसी Salary Slip और CIBIL Score के तुरंत ₹50,000 का Instant Loan पाएँ! केवल आधार Card Upload करें और 2 मिनट में पैसा सीधे Bank खाते में!"

पैसे की ज़रूरत में लोग ऐसे Ads के झाँसे में आ जाते हैं और दिए गए Link पर Click करके एक अनजान App Download कर लेते हैं।

खतरे की सच्चाई

Contacts और Gallery चोरी होते ही शुरू होता है Blackmail

App Install होते ही यह आपसे Contacts, Gallery Photos और SMS की Permission माँगता है। जैसे ही आप 'Allow' करते हैं, आपके Phone का पूरा Data Fraudster के Server पर पहुँच जाता है। 7 दिन बाद शुरू होता है गंदी Photos बनाकर रिश्तेदारों को भेजने का खौफनाक खेल।

> **सीधी बात:** RBI का सख्त नियम है कि कोई भी लीगल Bank या लोन कंपनी आपके Phone Contacts और निजी Gallery की Permission नहीं माँग सकती। जो App यह माँगे, वह 100% गैर-कानूनी है।

Case Study: ₹5,000 के Loan पर ₹80,000 की वसूली और धमकी

देखें कैसे 7-दिन वाले Fake Loan Apps लोगों को मानसिक रूप से डराते हैं:

📞 PHONE CALL SIMULATION (FAKE RECOVERY AGENT)

Recovery Agent (गुस्से और गाली-गलौज में):

"अमित बात कर रहा है? तूने जो ₹5,000 का Loan लिया था, आज उसकी आखिरी तारीख है। तुरंत ₹9,000 इस UPI ID पर Transfer कर, नहीं तो तेरी ज़िंदगी बर्बाद कर दूंगा!"

अमित (डरते हुए):
"सर, Loan तो 3 महीने के लिए था और आज सिर्फ 6 दिन हुए हैं। मुझे तो केवल ₹3,500 ही अपने खाते में Receive हुए थे!"

Recovery Agent:
"नियम मत सिखा मुझे! तेरे Phone की पूरी Contact List और तेरी बहन की Photo मेरे पास है। अगर 15 मिनट में Payment का Screenshot नहीं भेजा, तो तेरी Photo पर 'चोर' लिखकर तेरे सारे रिश्तेदारों को WhatsApp पर भेज रहा हूँ!"

अमित:
"सर, ऐसा मत कीजिए! मैं अभी किसी से उधार लेकर ₹9,000 भेज रहा हूँ।"

सच्चाई: अमित ने डरकर ₹9,000 भर दिए। लेकिन अगले ही दिन दूसरे Number से Call आ गया कि *"System में Penalty ₹15,000 बाकी है, वो भी तुरंत भरो!"* अमित 1 महीने में ₹80,000 गँवा चुका था, फिर भी Blackmail नहीं रुका। जब उसने Cyber

> Crime Cell में कानूनी Complaint की, तब जाकर यह मामला शांत हुआ।

Fake Loan Apps का 7-Day Trap कैसे काम करता है?

यह गैर-कानूनी सिंडिकेट 4 चरणों में लोगों को अपने शिकंजे में कसता है:

1. **Social Media Ad और अनजान APK Link**

   Facebook, Instagram या SMS पर "No CIBIL, Instant ₹50,000" का लालच देकर थर्ड-पार्टी APK File Download कराई जाती है।

   ↓ Permissions की चोरी

2. **Contacts और Gallery का Data Server पर Upload**

   App खुलते ही Contacts, Camera, Photos और Storage की Permission लेकर सारा निजी Data अपने Server पर Copy कर लेते हैं।

   ↓ भारी कटौती और 7-दिन की मियाद

3. **Processing Fee काटकर कम पैसे भेजना**

   ₹10,000 के लोन पर ₹4,000 काटकर केवल ₹6,000 भेजे जाते हैं और 6वें दिन ही दोगुने पैसे की मांग शुरू हो जाती है।

↓ Morphed Photos और Blackmail

4 **रिश्तेदारों को Morphed Photos और गाली-गलौज**

आपकी तस्वीरों को अश्लील तस्वीरों के साथ जोड़कर आपके पूरे परिवार और Office के दोस्तों को WhatsApp पर भेजकर डराया जाता है।

3 सबसे बड़े नियम: Fake Loan App और धमकियों से कैसे बचें



1. 7-दिन वाले अनजान Loan App कभी Install न करें

Google Play Store या किसी Link से ऐसा कोई App Install न करें जो बिना कागज़ के 2 मिनट में लोन देने का दावा करे।

> **सीधा नियम:** हमेशा केवल RBI-Registered Banks या NBFCs के Official Apps से ही Loan के लिए आवेदन करें।



2. डरकर कभी Extra पैसा न दें (Blackmail रुकता नहीं)

Blackmailer को अगर आपने एक बार डरकर पैसा दे दिया, तो वह समझ जाता है कि आप डर चुके हैं और नई Penalty बनाकर माँगता रहेगा।

> **सीधा नियम:** पैसे देना तुरंत बंद करें। लोन न चुकाना एक Civil मामला है, कोई आपको जेल नहीं भेज सकता।

📱

3. तुरंत App Delete करें और जान-पहचान वालों को Alert करें

Phone की Settings में जाकर Permissions Revoke करें, App Delete करें और अपने रिश्तेदारों को पहले ही सच बता दें।

> **WhatsApp Status लगाएँ:** "मेरा Phone Hack हुआ है। किसी भी Fraud Number से मेरी Fake या Morphed Photo आए, तो उसे तुरंत Report और Block करें।"

Cyber Crime Portal पर तुरंत Complaint दर्ज करें

यदि कोई Fake Loan App या Recovery Agent आपको Morphed Photos या Call करके Blackmail कर रहा है, तो भारत सरकार के Official Portal पर Online शिकायत दर्ज करें:

`cybercrime.gov.in` • National Cyber Crime Reporting Portal

Official Government Portal



Cyber Crime Related Complaint / Women & Children Related Cybercrime

Cybercrime refers to any unlawful activity carried out using computers, digital devices, or the internet. It includes offenses such as data theft, hacking, online harassment, identity misuse, financial scams, spreading malware, and other acts intended to harm individuals, organizations, or digital infrastructure.

Any victim of financial cyber fraud can dial helpline number 1930

Cyber Crime Portal पर 3 आसान Steps में शिकायत दर्ज करें:

1. **Official Portal खोलें:** Google पर जाकर सीधे `cybercrime.gov.in` टाइप करें और खोलें।
2. **Report Other Cyber Crime:** Portal पर 'Report Other Cyber Crime' या 'Financial Fraud' पर Click करें।
3. **सबूत Attach करें:** धमकियों वाले WhatsApp Chat के Screenshot, Call Recording और App का नाम Upload करके Complaint Submit करें।

क्या करें और क्या न करें (Golden Rules)

✓ क्या करें (Do's)

✓ केवल RBI-Registered Banks व NBFCs से ही लोन के लिए आवेदन करें।

✓ App Download करते समय Contacts और Storage की Permission कभी न दें।

✓ धमकी वाले Call और WhatsApp Chat की Call Recording व Screenshot सुरक्षित रखें।

✓ अपने परिवार व दोस्तों को पहले ही बता दें कि आपका Data Fraud App ने चुराया है।

✕ क्या न करें (Don'ts)

✕ Social Media के Ads या SMS Link से कोई भी Loan App Install न करें।

✕ 7 दिन वाले किसी भी Quick Loan App के झाँसे में कभी न आएँ।

✕ Blackmailers की धमकी से डरकर बार-बार Extra पैसे Transfer न करें।

✕ चुपचाप अकेले मानसिक तनाव न सहें; तुरंत Cyber Cell में कानूनी Complaint दर्ज कराएँ।

जाँचे गए OFFICIAL स्रोत (VERIFIED SOURCES)

Reserve Bank of India (RBI) Digital Lending Guidelines: `rbi.org.in`

RBI Sachet Portal for Illegal Deposit Schemes & Unregistered Entities: `sachet.rbi.org.in`

Ministry of Home Affairs - National Cyber Crime Reporting Portal: `cybercrime.gov.in`

Department of Financial Services Advisory on Illegal Digital Lending Apps

अध्याय 13 • FAKE RELATIVE & FRIEND IMPERSONATION

रिश्तेदार बनकर पैसे माँगने वाले Call

मामा, चाचा, पुराना दोस्त या दामाद बनकर Emergency में पैसे माँगने की चाल और बचने का तरीका।

"पहचाना मुझे? मैं बोल रहा हूँ!" — आवाज़ और रिश्ते का झाँसा

सोचिए, सुबह-सुबह आपके Phone पर एक अनजान Number से Call आता है। सामने से कोई बहुत अपनेपन और गर्मजोशी से बोलता है:

"नमस्ते जी! पहचाना मुझे? अरे आवाज़ नहीं पहचान पाए क्या?"

इंसान स्वभाव से संकोच में पड़ जाता है। उसे लगता है कि अगर उसने मना किया, तो सामने वाले को बुरा लग जाएगा। इसलिए वह खुद ही अंदाज़ा लगाकर बोल पड़ता है: *"अरे... रमेश भाई बोल रहे हो क्या?"*

खतरे की सच्चाई

Guessing Game: आपसे ही नाम उगलवाना

Fraudster तुरंत कहता है: *"हाँ-हाँ रमेश ही! और बताओ घर में सब कैसे हैं? मेरा पुराना Phone खो गया था, इसलिए नए Number से Call कर रहा हूँ।"* हाल-चाल पूछने के दो मिनट बाद शुरू होता है झूठी Emergency का नाटक।

> **सीधी बात:** जब कोई अनजान Number से कहे "पहचाना मुझे?", तो कभी खुद अंदाज़ा लगाकर नाम न बोलें। सीधे पूछें: "आप कौन बोल रहे हैं, पूरा नाम बताइए।"

Case Study: "चाचाजी, मैं आपका भतीजा राहुल बोल रहा हूँ"

देखें कैसे झूठी Emergency और डर का माहौल बनाकर पैसे ठगे जाते हैं:

PHONE CALL SIMULATION (FAKE NEPHEW)

Caller (घबराई हुई आवाज़ में):
"नमस्ते चाचाजी! पहचाना मुझे? मैं राहुल बोल रहा हूँ पुणे से।"

सुरेश जी (58 वर्ष):

"अरे राहुल बेटा! तेरी आवाज़ को क्या हुआ? सब ठीक तो है ना?"

Caller:
"चाचाजी, बहुत बड़ी मुसीबत में हूँ। मेरी गाड़ी से एक बाइक वाले की टक्कर हो गई है। Police मुझे पकड़ रही है। मुझे तुरंत Hospital में ₹30,000 जमा करने हैं, नहीं तो Police FIR कर देगी!"

सुरेश जी (डरते हुए):
"अरे बेटा, तेरे पापा को Phone किया क्या?"

Caller:
"नहीं चाचाजी, पापा को हार्ट की बीमारी है, उन्हें पता चला तो अटैक आ जाएगा! प्लीज़ आप किसी को मत बताइए। मैं आपके Google Pay पर अपने दोस्त से ₹30,000 डलवा रहा हूँ, आप तुरंत मुझे इस QR Code पर Transfer कर दीजिए।"

सच्चाई: सुरेश जी के Phone पर ₹30,000 'Received' का एक Fake SMS आया। सुरेश जी ने Bank Balance Check किए बिना तुरंत अपने खाते से ₹30,000 भेज दिए। शाम को जब भाई को Phone किया, तो पता चला कि राहुल तो आराम से Office में बैठा था और उसने कोई Call नहीं किया था।

Fake Relative Scam कैसे काम करता है? (4-Step Trap)

यह जालसाज़ी 4 सुनियोजित चरणों में आपके भरोसे का फायदा उठाती है:

1. **अंदाज़ा लगवाना (Guessing Game)**
   Scammer कभी खुद नाम नहीं बताता। वह बहुत गर्मजोशी से बात करके आपसे ही किसी रिश्तेदार का नाम बुलवा लेता है।

   ↓ झूठी Emergency की कहानी

2. **Hospital या Police का डर**
   गाड़ी का Accident, Hospital का बिल या Police केस का डर दिखाकर सोचने-समझने का बिल्कुल समय नहीं दिया जाता।

   ↓ Fake SMS या Transaction का झाँसा

3. **"मैंने आपके खाते में पैसे भेज दिए हैं"**
   Bank Server खराब होने का बहाना बनाकर आपके खाते में पैसे भेजने का Fake SMS भेजा जाता है।

   ↓ आपके खाते से तुरंत निकासी

4 **तीसरे QR Code या UPI पर पैसे मँगवाना**

जैसे ही आप अपने Bank खाते से पैसे भेजते हैं, Scammer का Number हमेशा के लिए बंद हो जाता है।

3 सबसे बड़े नियम: रिश्तेदार वाले Fake Call से कैसे बचें

❓

1. खुद कभी नाम न लें (पहचान का Test लें)

जब कोई अनजान व्यक्ति कहे "पहचाना मुझे?", तो कभी अंदाज़ा न लगाएँ।

> **सीधा सवाल:** "आप कौन बोल रहे हैं, अपना पूरा नाम बताइए?" कोई ऐसा निजी सवाल पूछें जो सिर्फ असली रिश्तेदार जानता हो।

📞

2. पुराने Save Number पर Call करके पक्का करें

नया Number बताने पर उसकी बात पर कभी तुरंत भरोसा न करें।

> **तुरंत करें:** Call काटें और अपने Phone में पहले से Save उसके पुराने Number पर Call लगाएँ या उसके घर वालों से बात करें।



3. SMS देखकर कभी पैसे न भेजें (Passbook Check करें)

पैसे आने का SMS केवल एक साधारण Text Message हो सकता है।

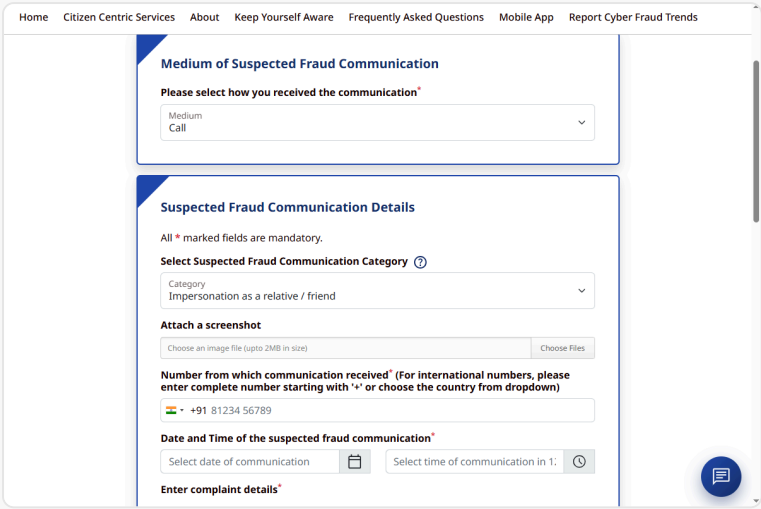
> **Check करें:** अपने Bank App या Google Pay में जाकर Account Balance खुद Check करें। जब तक Bank खाते में पैसा न दिखे, ₹1 भी न भेजें।

Chakshu Portal पर ऐसे Fake Call की Report करें

यदि किसी अनजान व्यक्ति ने रिश्तेदार बनकर आपसे पैसे ठगने की कोशिश की है, तो भारत सरकार के Sanchar Saathi Portal पर तुरंत Report दर्ज करें:

`sancharsaathi.gov.in` • Chakshu Fraud Reporting

Official Government Portal



Chakshu Portal पर 3 आसान Steps में Report करें:

1. **Official Portal खोलें:** Google पर सीधे `sancharsaathi.gov.in` खोलें और Chakshu विकल्प चुनें।
2. **Category चुनें:** 'Impersonation / Fake Relative or Friend' विकल्प सेलेक्ट करें।
3. **Details सबमिट करें:** Fraud Caller का Mobile Number, Call का समय और घटना का संक्षिप्त विवरण दर्ज करें।

क्या करें और क्या न करें (Golden Rules)

✓ क्या करें (Do's)

✓ अनजान Number से Call आने पर हमेशा Caller से उसका पूरा नाम और काम पूछें।

✓ पैसे माँगने पर उसके पुराने Save Number पर Call करके सच्चाई जाँचे।

✓ पैसे भेजने से पहले अपने Bank App में असली Balance खुद Check करें।

✓ Fraud Number की Report तुरंत Chakshu Portal पर दर्ज कराएँ।

✗ क्या न करें (Don'ts)

✗ "पहचाना मुझे" कहने पर कभी खुद अंदाज़ा लगाकर किसी का नाम न बोलें।

✗ Emergency या Police का नाम सुनकर डर में आकर तुरंत पैसे Transfer न करें।

✗ केवल SMS या WhatsApp Screenshot देखकर पैसे आगे कभी न भेजें।

✗ परिवार के किसी सदस्य के Accident या बीमारी की बात पर अकेले फैसला न लें।

जाँचे गए OFFICIAL स्रोत (VERIFIED SOURCES)

Department of Telecommunications (DoT) Sanchar Saathi Portal: `sancharsaathi.gov.in`

Chakshu Facility for Reporting Suspected Fraud Communications

National Cyber Crime Reporting Portal: `cybercrime.gov.in`

Reserve Bank of India (RBI) Public Awareness on Social Engineering & Impersonation Frauds

अध्याय 14 • PRIZE, LOTTERY, COURIER & SIM BLOCK CALLS

Prize, Lottery, Courier और SIM Block Call

गाड़ी जीतने का झाँसा, FedEx Parcel में Drugs का डर और 2 घंटे में SIM बंद होने की धमकी का सच।

"आपका SIM 2 घंटे में बंद हो जाएगा!" — डर और लालच का दोहरा वार

Phone पर आने वाले Fraud Calls में दो तरह के हथियार सबसे ज़्यादा इस्तेमाल होते हैं:

1. लालच: *"बधाई हो! आपने ₹25 लाख की KBC Lottery या चमचमाती नई कार जीती है!"*

2. डर: *"Telecom Department से सूचना: आपका Mobile SIM अगले 2 घंटे में बंद कर दिया जाएगा, तुरंत 9 दबाएँ!"* या *"FedEx Courier में आपका Parcel पकड़ा गया है जिसमें नशीली दवाइयाँ मिली हैं!"*

खतरे की सच्चाई

सोचने का समय न देना ही इनकी सबसे बड़ी चाल है

चाहे लालच हो या Police का डर, जालसाज आपको सोचने या परिवार से बात करने का 1 मिनट भी समय नहीं देते। वे तुरंत GST, Customs Clearance या Penalty के नाम पर पैसे Transfer करने का दबाव बनाते हैं।

> **सीधी बात:** भारत का कोई भी Telecom Operator या Customs Department कभी IVR Call करके Number बंद करने या UPI पर चालान भरने को नहीं कहता।

Case Study: "FedEx Courier में Drugs पकड़े गए हैं"

देखें कैसे Customs और Narcotics के नाम पर आम नागरिक को डराया जाता है:

PHONE CALL SIMULATION (FAKE COURIER & CUSTOMS)

> **Caller (गंभीर आवाज़ में):**

"नमस्ते, FedEx Courier Head Office से बोल रहा हूँ। क्या आप रोहित वर्मा बोल रहे हैं?"

रोहित:
"हाँ, पर मैंने तो कोई Courier नहीं भेजा!"

Caller:
"सर, आपके आधार Card का इस्तेमाल करके मुंबई से विदेश के लिए एक Parcel भेजा जा रहा था। एयरपोर्ट Customs Checking में इसमें 150 ग्राम नशीली दवाइयाँ और 3 Fake Passports मिले हैं। आपके नाम पर FIR दर्ज हो गई है!"

रोहित (डरते हुए):
"सर, यह Parcel मेरा नहीं है! किसी ने मेरे आधार का गलत इस्तेमाल किया है!"

Caller:
"अगर आप निर्दोष हैं, तो अपनी Call Narcotics Department को Transfer कर रहा हूँ। तुरंत अपनी जांच के लिए Clearance Fee के ₹75,000 इस Bank Account में Transfer करें, नहीं तो Police आपके घर आ रही है!"

> **सच्चाई:** रोहित ने डरकर ₹75,000 Transfer कर दिए। बाद में पता चला कि FedEx या सरकारी Customs कभी Phone पर केस दर्ज करने या निजी Bank Account में पैसे Transfer करने को नहीं कहते। यह पूरा गिरोह एक Fake Call Center से चल रहा था।

Fake Lottery, Courier और SIM Block Trap कैसे काम करता है?

यह सिंडिकेट 4 चरणों में लोगों को अपने जाल में फँसाता है:

1. **Computerized IVR Call या शानदार SMS**
   रोबोटिक आवाज़ में "SIM Block होने" की चेतावनी दी जाती है या Lucky Draw में कार जीतने का Message भेजा जाता है।

   ↓ 9 दबाते ही नकली Call Center से जुड़ाव

2. **Customs या Telecom Officer का नाटक**
   सामने से Caller खुद को DoT या Customs का वरिष्ठ अधिकारी बताकर कानूनी कार्रवाई का भारी डर बनाता है।

   ↓ तुरंत पैसों की मांग

3. **GST, RTO Fee या Clearance का झाँसा**
   Lottery के लिए Registration Fee या Parcel के लिए 'Anti-Terror Clearance' के नाम पर पैसे माँगे जाते हैं।

↓ पैसे मिलते ही गायब

4 **नए टैक्स की मांग और Number Block**

एक बार पैसे भेजने के बाद नई-नई Fees माँगी जाती है और अंत में सभी Numbers हमेशा के लिए बंद कर दिए जाते हैं।

3 सबसे बड़े नियम: ऐसे Calls से कैसे बचें



1. "SIM बंद होने" की IVR Call तुरंत काटें

Telecom Department कभी Phone करके यह नहीं कहता कि "आपका Number 2 घंटे में बंद हो जाएगा।"

> **सीधा नियम:** कभी 9 न दबाएँ, तुरंत Call काटें। कोई संदेह हो तो अपने Operator के Official Store पर जाकर पता करें।



2. Courier में गैर-कानूनी सामान का डर न लें

Customs या Police कभी Phone पर बयान दर्ज नहीं करती और न ही UPI पर पैसे माँगती है।

> **सीधा नियम:** अगर आपने कोई Parcel नहीं भेजा, तो Phone काट दें। कोई असली केस ऐसे नहीं बनता।

🎁

3. Prize पाने के लिए कभी Advance न दें

जिस Lottery में आपने हिस्सा नहीं लिया, उसमें आप कभी विजेता नहीं बन सकते।

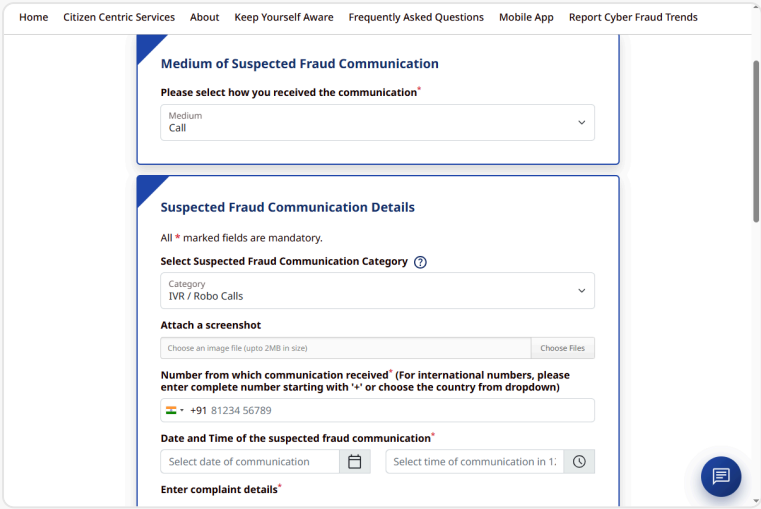
> **Golden रूल:** असली इनाम में टैक्स काटकर बचा हुआ पैसा दिया जाता है, कभी विजेता से Advance Fee नहीं ली जाती।

Chakshu Portal पर IVR व Robocall की Report करें

यदि आपको SIM Block होने की धमकी, Fake Lottery या Courier Fraud का कोई Call आया है, तो भारत सरकार के Sanchar Saathi Portal पर तुरंत Report करें:

sancharsaathi.gov.in • Chakshu Robocall Reporting

Official Government Portal



Chakshu Portal पर 3 आसान Steps में Report करें:

1. **Official Portal खोलें:** Google पर सीधे `sancharsaathi.gov.in` खोलें और Chakshu Service पर Click करें।
2. **Category सेलेक्ट करें:** 'Fake Telecom Notice / SIM Disconnection' या 'Lottery Fraud' चुनें।
3. **Details Submit करें:** Fraud Number, Call आने का समय और विवरण दर्ज करके Submit करें।

क्या करें और क्या न करें (Golden Rules)

✓ क्या करें (Do's)

✓ SIM बंद होने की धमकी वाली IVR Call तुरंत काट दें।

✓ किसी भी इनाम की बात सुनने से पहले खुद से पूछें कि क्या आपने कोई Lottery Ticket लिया था।

✓ Courier में अवैध सामान की बात पर बिना डरे Call Disconnect करें।

✓ Fraud Numbers की Report तुरंत Chakshu Portal पर दर्ज कराएँ।

✕ क्या न करें (Don'ts)

✕ IVR Call में Customer Support से बात करने के लिए 9 कभी न दबाएँ।

✕ Prize या Gift पाने के लिए कभी भी Advance Registration Fee न दें।

✕ डर के मारे अपने Bank खाते या आधार Card की जानकारी किसी को न दें।

✕ अनजान Caller के कहने पर किसी भी Bank खाते में पैसे Transfer न करें।

जाँचे गए OFFICIAL स्रोत (VERIFIED SOURCES)

Telecom Regulatory Authority of India (TRAI) Advisories on Fake Disconnection Calls

Department of Telecommunications (DoT) Sanchar Saathi: `sancharsaathi.gov.in`

Central Board of Indirect Taxes and Customs (CBIC) Public Advisory on Courier Frauds

National Cyber Crime Reporting Portal: `cybercrime.gov.in`

अध्याय 15 • EMERGENCY RESPONSE & CYBER COMPLAINT

Fraud हो जाए तो क्या करें और Complaint कैसे करें

Golden 2 Hours की रणनीति, Bank Account Freeze कराना, Cyber Crime Portal पर FIR और RBI Zero Liability के नियम।

Golden 2 Hours: पैसे कटते ही पहले 120 मिनट में क्या करें?

यदि किसी Fraud Call या Fake Bank Call के चक्कर में आपके Bank खाते से पैसे कट जाएँ, तो डरने या पछताने में समय बर्बाद न करें।

Cyber अपराध के मामलों में पहले 2 घंटों को **"Golden Hours"** कहा जाता है। जालसाज चुराए हुए पैसे को तुरंत कई राज्यों के अलग-अलग Fake Accounts में घुमाते हैं। अगर आप तुरंत सही Action लेते हैं, तो Bank और Cyber Police उस पैसे पर Lien Freeze (रोक) लगा देती है।

कानूनी सुरक्षा

RBI का Zero Liability नियम: ग्राहक की ढाल

Reserve Bank of India (RBI) का स्पष्ट नियम है कि अगर अनधिकृत Transaction होने पर ग्राहक 3 कार्य दिवसों के भीतर अपने Bank को सूचित कर देता है, तो ग्राहक की देनदारी Zero (शून्य) होती है और पूरा नुकसान Bank को वहन करना पड़ता है।

> **सीधी बात:** देर करने से जालसाज पैसा ATM से निकाल लेता है। जितनी जल्दी सूचना देंगे, पैसे की सुरक्षित वापसी की संभावना उतनी ही 100% पक्की होगी।

Case Study: 30 मिनट में Action और ₹1,20,000 की सुरक्षित वापसी

देखें कैसे सही समय पर की गई शिकायत से पैसे वापस मिलते हैं:

EMERGENCY ACTION TIMELINE (SUCCESS STORY)

> **घटना (11:15 AM):**
> सुनील जी के Phone पर Fake KYC Call आया और बातों-बातों में Screen Share होते ही उनके खाते से ₹1,20,000 कट गए।

सुनील जी की बेटी (11:25 AM):
बिना घबराए तुरंत Bank के Official Portal से Number लेकर Debit Card, Net Banking और UPI को हमेशा के लिए Block करवाया।

Online Action (11:40 AM):
National Cyber Crime Portal (`cybercrime.gov.in`) पर जाकर Transaction का UTR Number और Fraudster की UPI ID Submit की।

सच्चाई व परिणाम: तुरंत शिकायत से Portal ने तुरंत उस गंतव्य खाते को ट्रेस किया और उस पर Freeze लगा दिया। जालसाज पैसा ATM से नहीं निकाल पाया। 14 दिनों की कानूनी नियम के बाद सुनील जी के पूरे ₹1,20,000 उनके मूल Bank खाते में वापस आ गए।

पैसे कटते ही 4 Emergency Steps (तुरंत करें)

यह 4-चरणीय तरीका आपके पैसे की वसूली का सबसे पक्का रास्ता है:

1 **Bank Account और UPI तुरंत Freeze कराएँ**

Bank App खोलकर Card Block करें या Official Portal से Helpline लेकर Net Banking बंद करवाएँ ताकि आगे पैसे न कटें।

↓ 30 मिनट के भीतर Online Report

2 **Cyber Crime Portal (cybercrime.gov.in) पर Report**

'Report Financial Fraud' पर जाकर Transaction Reference Number (UTR) और जालसाज के खाते की जानकारी दर्ज करें।

↓ Fraud Caller का Number Block करवाना

3 **Chakshu Portal पर Fraud Call की Report**

Sanchar Saathi Portal के Chakshu माध्यम पर उस Fraud Caller का Number दर्ज करें ताकि उसका SIM तुरंत Block हो सके।

↓ नजदीकी Police में कानूनी पावती

4 **नजदीकी Cyber Cell में लिखित शिकायत और Receipt**

Bank Statement और SMS के Screenshot के साथ लिखित अर्जी देकर Acknowledgment Number लें।

3 सबसे बड़े नियम: Safe Contact Protocol



1. Google Ads के Number पर कभी Call न करें

जालसाज Google Search Ads में अपने फर्जी Customer Care Numbers डाल देते हैं।

> **सीधा नियम:** सीधे Google एड्रेस बार में `cybercrime.gov.in` या अपने Bank का URL खुद Type करें।



2. 3 Working Days की समय सीमा याद रखें

RBI के अनुसार 3 दिनों के भीतर Bank को सूचना देने पर नुकसान Bank को वहन करना पड़ता है।

> **सीधा नियम:** तुरंत अपनी Bank शाखा में जाकर लिखित अर्जी दें और उस पर Bank की मुहर व पावती लें।



3. Phone कभी Format न करें (सबूत सुरक्षित रखें)

डर या हड़बड़ी में लोग Phone Reset कर देते हैं, जिससे सारे Digital सबूत मिट जाते हैं।

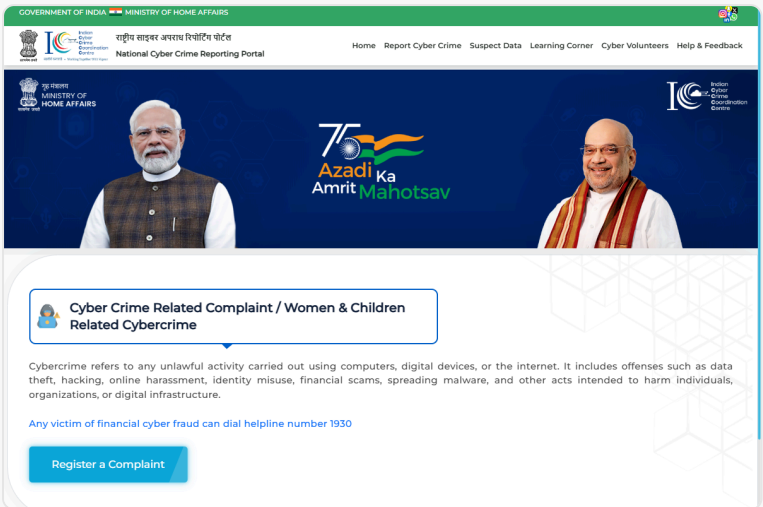
> **सीधा नियम:** Call Logs, Messages और WhatsApp Chat के Screenshots पहले किसी सुरक्षित जगह Save करें।

National Cyber Crime Reporting Portal पर शिकायत करें

भारत सरकार के गृह मंत्रालय द्वारा संचालित Official Portal पर Online शिकायत दर्ज करने का तरीका:

`cybercrime.gov.in` • National Cyber Crime Portal

Official Government Portal



Portal पर शिकायत दर्ज करने के 3 आसान Steps:

1. **Official Portal खोलें:** Google पर सीधे `cybercrime.gov.in` खोलें।
2. **Report Financial Fraud:** 'Report Financial Fraud' पर Click करें और घटना का संक्षिप्त विवरण भरें।
3. **Bank Details व UTR Submit करें:** अपने Bank का नाम, Transaction ID और जालसाज के खाते की जानकारी दर्ज करें।

क्या करें और क्या न करें (Golden Rules)

✓ क्या करें (Do's)

✓ पैसे कटते ही पहले 2 घंटे के भीतर Bank और Cyber Crime Portal पर शिकायत करें।

✓ Transaction का UTR Number और SMS Screenshot हमेशा सुरक्षित रखें।

✓ 3 दिनों के भीतर अपने Bank की होम ब्रांच में लिखित अर्जी देकर Receipt लें।

✓ Fraudulent Call की शिकायत तुरंत Chakshu Portal पर दर्ज कराएँ।

× क्या न करें (Don'ts)

× Fraud होने पर डरकर या शर्म के मारे चुपचाप न बैठें।

× Google Search Ads में दिखने वाले अनजान Helpline Numbers पर Call न करें।

× किसी भी Recovery Agent या Private Hacker को पैसे वापस दिलाने के नाम पर Advance न दें।

× Fraud के बाद अपने Phone को Formेट न करें, Digital सबूत नष्ट हो सकते हैं।

जाँचे गए OFFICIAL स्रोत (VERIFIED SOURCES)

Ministry of Home Affairs - National Cyber Crime Reporting Portal: `cybercrime.gov.in`

Reserve Bank of India (RBI) Circular on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions

Department of Telecommunications (DoT) Sanchar Saathi Portal: `sancharsaathi.gov.in`

Indian Cyber Crime Coordination Centre (I4C) Citizen Financial Cyber Fraud Reporting Guidelines

अध्याय 16 • MASTER POCKET CHECKLIST

Fraud Call Safety Checklist

Phone पर कभी क्या न बताएँ — 10 Golden सुरक्षा नियम और पूरी Pocket Checklist।

Phone Call Master Safety Checklist: क्या कभी किसी को न बताएँ

यह अध्याय इस पूरी किताब का सबसे बहुत ज़रूरी निचोड़ है। इसे अपने पास Save रखें या Print करके घर में ऐसी जगह लगाएँ जहाँ परिवार के सभी सदस्य इसे रोज़ देख सकें।

Phone पर होने वाली 95% ठगी केवल इन 10 बातों को याद रखने से पूरी तरह रोकी जा सकती हैं:

सुरक्षा का मूलमंत्र

पहला नियम: Phone पर कोई भी सरकारी अधिकारी पैसे नहीं माँगता

चाहे कोई खुद को Bank Manager, Police Commissioner, CBI Officer, Supreme Court का जज या Telecom अधिकारी बताए—भारत के कानून में किसी भी सरकारी विभाग को Phone या Video Call पर पैसे माँगने का अधिकार नहीं है।

> **सीधी बात:** जब भी कोई Phone पर पैसे Transfer करने या OTP माँगने की बात करे, समझ जाइए कि सामने वाला 100% Fraudster है। तुरंत Call काटें!

10 Golden Checklist Rules (Tick Box Summary)

रोज़मर्रा के जीवन में इन 10 नियमों की जाँच ज़रूर करें:

☑ **1. OTP कभी किसी को न बताएँ:**
चाहे Caller खुद को Bank Manager या Police बताए, Phone पर आया OTP कभी Share न करें।

☑ **2. UPI PIN केवल पैसे भेजने के लिए होता है:**

पैसे Receive करने, Lottery जीतने या Refund पाने के लिए कभी PIN डालने की ज़रूरत नहीं होती।

☑ **3. Screen Sharing App कभी Download न करें:**
AnyDesk, TeamViewer या QuickSupport App Install करके किसी अनजान को 9-Digit Code न दें।

☑ **4. "Digital Arrest" नाम का कोई कानून नहीं होता:**
भारत में कोई भी Police, CBI या Court Video Call पर किसी को Arrest नहीं करती।

☑ **5. Google Search से Customer Care Number कभी न लें:**
हमेशा Bank की Passbook, Card के पीछे या Official Website पर जाकर ही Number लें।

☑ **6. 7-दिन वाले Instant Loan Apps कभी Install न करें:**
जो App Contacts और Gallery की Permission माँगे, वह गैर-कानूनी Blackmailing सिंडिकेट है।

☑ **7. "SIM बंद होने" की IVR Call पर कभी 9 न दबाएँ:**
Telecom Department कभी Automated Call करके 2 घंटे में Number काटने की धमकी नहीं देता।

☑ **8. "पहचाना मुझे" कहने पर कभी खुद नाम न बोलें:**
पहले Caller से उसका पूरा नाम और काम पूछें, फिर उसके पुराने Save Number पर Call करके पक्का करें।

☑ **9. AI Voice Scam से सावधान रहें:**
अगर कोई अपने बच्चे या रिश्तेदार की आवाज़ में Accident का डर दिखाकर पैसे माँगे, तो तुरंत पैसे Transfer न करें।

☑ **10. पैसे कटते ही Golden 2 Hours में Action लें:**
तुरंत Bank Account Freeze कराएँ और Official Cyber Crime Portal पर शिकायत दर्ज करें।

Phone Call पर कभी क्या न बताएँ (Never Share List)

Private जानकारी	Caller का बहाना	आपका अटल जवाब ❌
OTP	"Account Verify करने के लिए 6 अंकों का Code	**साफ मना करें!** असली Bank कभी

Private जानकारी	Caller का बहाना	आपका अटल जवाब ❌
	बताइए"	OTP नहीं माँगता।
UPI PIN	"Refund पाने के लिए अपना 6 अंकों का PIN डालें"	**कभी नहीं!** PIN डालने से पैसे कटते हैं, आते नहीं।
Card CVV	"नया Card Activate करने के लिए पीछे का 3-अंकों का CVV दें"	**सख्त मना है!** CVV कभी किसी को न बताएं।
Screen Share	"Error ठीक करने के लिए 9-अंकों का Code Screen से पढ़ें"	**तुरंत Call काटें!** इससे Phone Hack हो जाता है।
आधार / PAN Photo	"WhatsApp पर तुरंत KYC Form और ID Proof भेजें"	**कभी नहीं!** अनजान व्यक्ति को निजी दस्तावेज न भेजें।

3-Step Verified Safety Protocol

⏸

1. डर और लालच के सामने 5 मिनट का Break लें

जब भी कोई Phone पर आपको तुरंत पैसे भेजने, Arrest करने या Lottery देने की बात कहे, तुरंत Phone काटें।

> **Golden रूल:** 5 मिनट शांति से पानी पिएँ और सोचें। जल्दीबाज़ी ही जालसाज का सबसे बड़ा हथियार है।



2. परिवार या दोस्तों से राय लें

अकेले में कभी पैसे से जुड़ा कोई बड़ा फैसला न लें।

> **सीधा नियम:** अपने घर के समझदार सदस्यों या दोस्तों को पूरी बात बताएँ। जालसाज का झूठ तुरंत पकड़ा जाएगा।



3. Official Portals पर ही भरोसा करें

किसी भी शिकायत या सहायता के लिए हमेशा भारत सरकार के Official Portals पर सीधे जाएँ।

> **सुरक्षित URL:** `cybercrime.gov.in` और `sancharsaathi.gov.in`

जाँचे गए OFFICIAL स्रोत (VERIFIED SOURCES)

Ministry of Home Affairs - National Cyber Crime Reporting Portal: `cybercrime.gov.in`

Department of Telecommunications (DoT) Sanchar Saathi Portal: `sancharsaathi.gov.in`

Reserve Bank of India (RBI) Financial Education & Awareness: `rbi.org.in`

Telecom Regulatory Authority of India (TRAI): `trai.gov.in`

परिशिष्ट • APPENDIX

कॉल सुरक्षा शब्दकोश (Glossary)

Digital Arrest

वीडियो कॉल पर नकली पुलिस/CBI बनकर घंटों तक कमरे में डिजिटल रूप से कैद रखने का नाटक, जिससे पीड़ित डरकर पैसे भेज दे।

Caller ID Spoofing

तकनीक से असली पुलिस स्टेशन या बैंक का नंबर स्क्रीन पर दिखाना, जबकि कॉल वास्तव में किसी साइबर अपराधी के फोन से आ रही होती है।

Screen Sharing App

AnyDesk या TeamViewer जैसे ऐप्स जिन्हें डाउनलोड करवाकर ठग आपके फोन की पूरी स्क्रीन और आने वाले OTP लाइव देख लेते हैं।

AI Voice Cloning

आर्टिफिशियल इंटेलिजेंस की मदद से कुछ सेकंड के ऑडियो से किसी की भी हूबहू आवाज बनाकर फिरौती या मदद माँगने का फ्रॉड।

Golden 2 Hours

पैसे ट्रांसफर होने के तुरंत बाद के 2 घंटे, जब साइबर क्राइम पोर्टल पर शिकायत दर्ज होने से बैंक ठग के खाते को तुरंत होल्ड कर सकता है।

Mule Account

किराये का बैंक खाता, जिसे ठग कमीशन देकर गरीबों के नाम पर खुलवाते हैं और अपराध का पैसा तुरंत निकालने के लिए इस्तेमाल करते हैं।

140 / 160 Calling Header

TRAI के नियमानुसार बैंक और टेलीमार्केटिंग कॉल्स के लिए तय Official नंबर सीरीज, जिससे प्रमोशनल और सर्विस कॉल पहचानी जाती हैं।

Chakshu Portal

Telecom Department (DoT) का Official Portal जहाँ शक वाले (Fake) कॉल्स और WhatsApp Fraud नंबर्स को Report करके देश भर में ब्लॉक कराया जाता है।

Sim Swap Fraud

आपके नाम पर फर्जी दस्तावेज देकर नया सिम निकलवाना, जिससे पुराने फोन का सिग्नल बंद हो जाता है और सारे बैंक OTP ठग के पास जाने लगते हैं।

Recovery Harassment

गैर-कानूनी लोन ऐप्स द्वारा परिजनों को फोन करके गंदी धमकियाँ देना, जिसे RBI ने गैर-कानूनी घोषित कर रखा है।

💡 किसी भी फोन कॉल पर शक होने पर इस शब्दकोश को संदर्भ के रूप में देखें।

★ FINAL SECURITY RULES

कॉल सुरक्षा के 4 सुनहरे नियम

1. **Digital Arrest एक धोखा है:** पुलिस, CBI या कोर्ट कभी वीडियो कॉल पर गिरफ़्तारी या जाँच नहीं करती। धमकी मिलते ही कॉल काटें।
2. **Screen Sharing कभी न करें:** बैंक या KYC के नाम पर AnyDesk, TeamViewer या कोई अन्य ऐप कभी फोन में Install न करें।
3. **OTP और PIN कभी न बताएँ:** कोई भी असली बैंक अधिकारी आपसे फोन पर पासवर्ड, कार्ड नंबर या 6-अंकों का OTP कभी नहीं माँगता।
4. **आवाज़ सुनकर घबराएँ नहीं:** बेटे या रिश्तेदार की आवाज़ में मदद की कॉल आने पर पहले पुराने नंबर पर सामान्य फोन करके सच्चाई परखें।

✓ 16 विस्तृत अध्याय ✓ Real-Life Case Studies

✓ DoT व Cyber Portal Verified ✓ Master Pocket Checklist

🤝 सुरक्षित डिजिटल भारत का संकल्प

जब आप किसी अनजान कॉल पर घबराते नहीं बल्कि समझदारी से कॉल काटते हैं, तो आप अपने परिवार की पूँजी और सम्मान दोनों की रक्षा करते हैं।

Safe Calls • Safe Family • Safe India

2026 Edition • जनहित में स्वतंत्र रूप से प्रकाशित