Based on DoT, TRAI, RBI & Cyber Crime Portal

LATEST 2026 EDITION

How to Stay Safe from Fraud Calls

A complete, easy pocket guide to stay safe from Bank, KYC, Screen Sharing, and Digital Arrest scams

16	100%	0
Easy Chapters	Verified Rules	Fear & Panic

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

Alert Voice • Safe Family • Strong India

2026 Mobile Pocket Edition • Published in Public Interest

LEGAL NOTICE • DISCLAIMER

Legal Terms and Rules of Use

1. Public Awareness Purpose

This eBook is an independent guide created solely to raise cyber safety awareness among everyday citizens. Its goal is to warn readers about fraud phone calls, bank scams, and Digital Arrest tricks. It is not legal or financial advice.

2. No Affiliation with Any Organization or Government

This eBook is not sponsored, endorsed, or approved by the Reserve Bank of India (RBI), Telecom Regulatory Authority of India (TRAI), DoT, National Cyber Crime Portal, NPCI, any bank, or any agency of the Government of India. It is an independent digital product.

3. Limitation of Liability

Cyber safety rules, app settings, and government website addresses can change over time. Neither this eBook nor its author is responsible for any phone fraud, technical issue, or financial loss faced by any reader. Always check the official website of the concerned authority for the latest updates.

4. Trademarks and Brand Names

'UPI' is a registered trademark of NPCI. 'WhatsApp' is a trademark of Meta Platforms. All other names mentioned in this book (such as Google Pay, PhonePe, AnyDesk, TeamViewer, Airtel, Jio, FedEx, etc.) belong to their respective owners and are used only for identification under Fair Use.

5. Description of Methods (No Real Names)

All examples and case studies in this book use fictional names solely to explain common scam methods. No real person, company, or organization is called a fraudster; only the methods of crime are exposed.

6. Single-User Digital License

This eBook is strictly for the buyer's personal reading. Unauthorized printing, re-uploading on the internet, or reselling of this eBook is strictly prohibited.

© 2026 All Rights Reserved • Independent Guide Based 100% on DoT, TRAI & Cyber Crime Portal Rules

EDITORIAL • PREFACE

Preface: Why Do You Need This Guide?

Today in India, every smartphone user receives 3 to 4 calls a day from unknown numbers—someone pretending to be a bank manager, threatening that drugs were found in a courier parcel, or video-calling in a police or CBI uniform.

This is called today's most dangerous fraud—**Digital Arrest and Voice Scams**. Even senior officers, doctors, retired employees, and educated youth transfer their life savings to scammers out of sheer fear and panic.

> “ **No real Police, CBI, or Court in India EVER arrests or questions anyone on a WhatsApp video call.** Digital Arrest is purely a fake drama staged to steal your money.

Most people fall into this trap simply because they don't know 2–3 basic phone call rules: *"No matter how big the threat on a call, never install a screen*

sharing app—hang up right away and confirm at your local police station or on the Cyber Crime Portal."

Purpose of This eBook:

This eBook is written in **simple, everyday language**, not heavy words. Across 16 chapters, it exposes how phone scams work so you don't panic on unknown calls—and hang up with full confidence.

Read this guide yourself and make sure every member of your home—especially your parents and elders—reads it too. One smart decision from you can protect your whole family from a huge loss.

TABLE OF CONTENTS

Complete Chapter List

1. **Chapter 1: How Fraud Calls Happen**
   Call spoofing, telecom data leaks, and the first-ring trap
2. **Chapter 2: Fake Bank Calls and Asking for OTP**
   Fear of card blocking and stealing OTPs in the bank's name
3. **Chapter 3: Fake KYC Calls**
   The new trap of SIM, electricity, and wallet KYC expiry
4. **Chapter 4: Digital Arrest: Fake Police or CBI Calls**
   Fake uniforms, fake courtrooms, and extorting money through fear
5. **Chapter 5: Fake Customer Care Calls**
   Fake numbers on Google Search and refund scams
6. **Chapter 6: Loan, Credit Card, and Government Scheme Calls**
   Zero-interest loans, reward points, and fake scheme traps
7. **Chapter 7: Screen Sharing and Remote App Scams**
   Taking full control of your phone via AnyDesk, TeamViewer, and QuickSupport
8. **Chapter 8: AI Voice Clone: Calls in a Loved One's Voice**
   Using AI to copy a child's voice and demand emergency money
9. **Chapter 9: Missed Calls and Unknown Number Traps**
   Foreign codes like +92, +84 and the fear of one-ring calls
10. **Chapter 10: Fake Course and Financial Freedom Calls**
    Stock market courses, trading tips, and get-rich-quick traps
11. **Chapter 11: Fake Memberships and Big Promises**
    Credit card billing in the name of club, hotel, and travel coupons

12 **Chapter 12: Loan Fraud and Recovery Agent Threats**
Fake loan apps, photo blackmail, and illegal recovery threats

13 **Chapter 13: Calls Pretending to Be a Relative Asking for Money**
"Guess who I am", sudden hospital emergencies, and money demands

14 **Chapter 14: Prize, Lottery, Courier, and SIM Block Calls**
KBC lottery, parcels stuck in customs, and threatening IVR calls

15 **Chapter 15: What to Do After Fraud & How to Complain**
Golden 2 Hours, Cyber Crime Portal, and freezing the bank account

16 **Chapter 16: Fraud Call Safety Checklist**
10 things never to say on a call and master pocket checklist

• **Appendix:** Printable Safety Card, Cyber Safety Glossary & Back Cover

CHAPTER 1 • UNDERSTANDING PHONE FRAUD

How Fraud Calls Happen

The truth about data leaks, caller ID spoofing, and spotting IVR robocalls.

Your Phone Rings: How Does the Scammer Know Your Name and Bank?

Imagine picking up a normal phone call. A serious, authoritative voice says: *"Hello, am I speaking to Rahul? You have an HDFC Bank account, right? ₹25,000 is about to be deducted from your debit card right now—stop it immediately!"*

When the caller gets your real name, father's name, or bank name right, you naturally think: *"This really is from the bank—how else would they know my name?"*

The Real Danger

Where Do Scammers Get Your Data?

A scammer is no detective. Whenever you write your name and mobile number for a mall lucky draw, on an unknown website, or at a hotel, that data leaks and is sold cheaply on the dark web.

> **Plain truth:** Just knowing your name or bank name never proves someone is a real officer.

Case Study: The Scary Trick of Caller ID Spoofing

See how scammers display the real bank's number on your screen to fool you:

📞 PHONE CALL SIMULATION (FAKE BANK EXECUTIVE)

> **Scammer (serious voice + office noise in background):** "Sir, I'm calling as a Senior Security Manager from Head Office. You can check—our official number is showing right on your screen."

> **Ordinary User:** *(Looks at the screen and sees the bank's real official number!)* "Yes sir, it does show the bank's number. Tell me what happened?"

> **Scammer:** "Sir, your card has been hacked. A cancellation code (OTP) just arrived on your phone—tell me quickly or all your money will be gone!"

> **Truth:** *(The real number appeared on screen only because of **Caller ID Spoofing**. The moment the user shared the OTP, ₹50,000 vanished from the account!)*

The 4-Step Trap of Phone Call Scams

1 **Auto-Dialing by Computer**

Scammers use computer software to blast IVR robocalls or live calls to 10,000 numbers at once.

↓ Creating fear and panic

2 **A Fake Big Crisis Drama**

They claim: "Your SIM will be shut off tonight", "A police FIR is filed against you", or "Money is leaving your bank account."

↓ Leaving you no time to think

3 **Demanding OTP, PIN, or Screen Sharing**

The scammer says: "Tell me the OTP now", "Download AnyDesk app", or "Move your money to a safe account."

↓ Money gone and call cut

4 **Account Emptied and Number Switched Off**

The moment you obey, your account is wiped clean and the scammer cuts the call and disappears.

Real Call vs Fraud Call: 3 Biggest Differences



1. A Real Bank Never Asks for Your OTP

RBI's clear rule: No genuine bank staff will EVER ask for your OTP, UPI PIN, or the 3-digit CVV on the back of your ATM card on a call.

> **Rule:** Anyone asking for an OTP on a call is 100% a scammer.



2. Police Never Arrest Anyone on Video Call

Under Indian law, courts do not run on video calls, and there is no legal rule called "Digital Arrest."



3. A SIM Never Shuts Down in 2 Hours

Telecom Department rules require proper written notice and verification before disconnecting a SIM. No SIM is blocked by an IVR call.

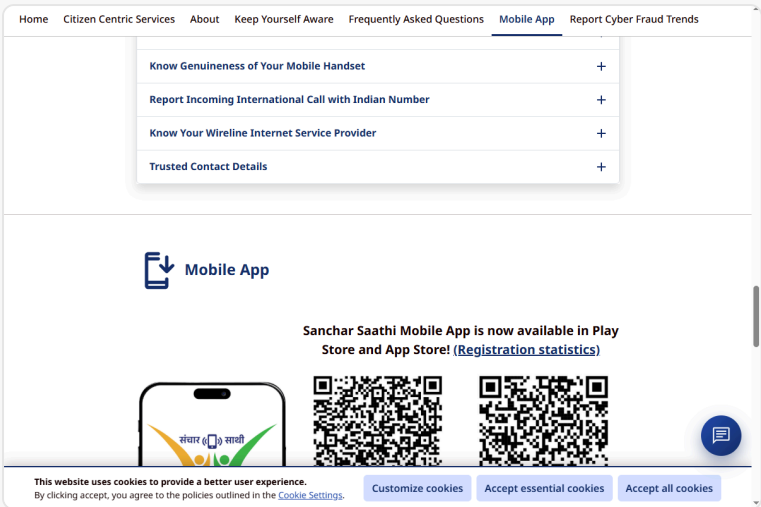
Official Portal: Report Fraud Calls Directly

to the Government

The Telecom Department of India built the **Chakshu Portal** for citizens to report any fake call or spoofed number directly:

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

Official Government Portal



📌 2 Key Facts About Chakshu Portal:

1. **Report the Number Fast:** If an unknown number called pretending to be your bank, KYC team, or police, report it here so it can be blocked nationwide.
2. **Check the Official Address:** Always make sure the browser address bar says `sancharsaathi.gov.in`. Real government portals always end in `.gov.in`.

Chapter 1: Do's and Don'ts

✅ Always Do This (DOs)

• The moment you feel fear or pressure on an unknown call, **hang up immediately**.

• If someone claims to be from your bank, call back yourself on the official number printed on the back of your ATM card.

• Report fake calls on the official **Chakshu** portal (`sancharsaathi.gov.in`).

❌ Never Do This (DONTs)

• Never trust a caller blindly just by looking at the Caller ID on your phone screen.

• Never share your OTP, PIN, or password with anyone on a call.

• Never download apps like AnyDesk or TeamViewer because someone on a call told you to.

OFFICIAL VERIFICATION & COMPLAINT SOURCES

• 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`

CHAPTER 2 • BANK AND CARD SECURITY TRUTH

Fake Bank Calls and Asking for OTP

Fear of card blocking, reward point traps, and how OTPs are stolen.

Your Phone Rings with a "Bank Manager's" Authority

Imagine receiving an afternoon call. Someone speaks in a very polished, serious tone: *"Hello, I'm a Senior Officer from your bank's Card Security Division. Your debit card will be blocked tonight at 12 AM because a new chip card has been issued."*

When you hesitate, they calmly recite your bank name, your city, and the last 4 digits of your card accurately. Hearing that, 90% of people get scared and believe the caller is a real bank officer.

Know the Truth

How Did the Scammer Know Your Card's Last 4 Digits?

Whenever you swipe your card at a petrol pump, restaurant, or grocery shop, the paper slip prints the last 4 digits of your card. Scammers collect such slips or buy leaked online data.

> **Plain truth:** Simply knowing the last 4 digits does not make anyone a bank officer. As long as your **OTP** and **PIN** stay secret, nobody can take even ₹1 from your account.

Case Study: The Dangerous "Cancellation Code" Trick

See how scammers twist words to get you to read out a payment OTP:

📞 PHONE CALL SIMULATION (FAKE SECURITY OFFICER)

> **Scammer (urgent voice):** "Sir, a ₹45,000 transaction just started on your HDFC card in Dubai. Did you make this payment?"

> **User (panicked):** "No! I didn't make any payment! I'm at home."

> **Scammer:** "Don't worry sir, I'm cancelling this fraud transaction right away. Head Office sent a **Cancellation Code** to your phone. Tell me quickly before the money gets deducted!"

> **User (reading only the 6 numbers in the SMS):** "Yes, the code came... 482910."

> **Truth:** *(In reality, the scammer had started a ₹45,000 purchase on a shopping site using the user's card. The moment the user read out the OTP, the money was gone and the call disconnected!)*

The Real SMS Truth vs The Scammer's Lie

The scammer will always rush you: *"Don't bother reading the SMS, just tell me the code."* See what a real bank SMS actually says:

VK-HDFCBK Official Bank SMS

Today • 11:42 AM

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

❌ **SCAMMER'S LIE**

"This is a verification code to cancel the transaction."

✅ **THE REAL SMS TRUTH**

It clearly states: OTP to debit **INR 45,000**! There is NO such thing as a cancellation OTP.

The 4-Step Trap of Bank Call Scams

1 **The Fear or Greed Hook**

The caller claims: "Your card is getting blocked", "Your reward points are expiring", or "A wrong payment is cutting."

↓ Winning your trust

2 **Fooling You with Old Data**

They tell you your name, city, birth date, or card's last 4 digits so you believe the call is really from your bank.

↓ Leaving you no time to think

3 **Asking for OTP as a "Cancellation Code"**

The scammer starts a payment on their computer and tells you: "Quickly tell me the code sent to cancel it."

↓ Account wiped and call cut

4 **Money Gone and Number Switched Off**

The moment you share the OTP, your account is drained and the scammer hangs up and disappears.

3 Golden Rules Always to Remember

🚫

1. There Is No OTP to Cancel a Transaction

No bank in the world ever uses an OTP to cancel a payment. An OTP is sent ONLY to approve money

leaving or transferring out.

> **Rule:** Anyone asking for a "Cancellation Code" on a call is 100% a scammer.



2. A Real Bank Never Asks for Your OTP

Reserve Bank of India (RBI) has a strict rule: no genuine bank employee can ever ask for your OTP, UPI PIN, card CVV, or password on the phone.



3. Always Check the Back of Your Card

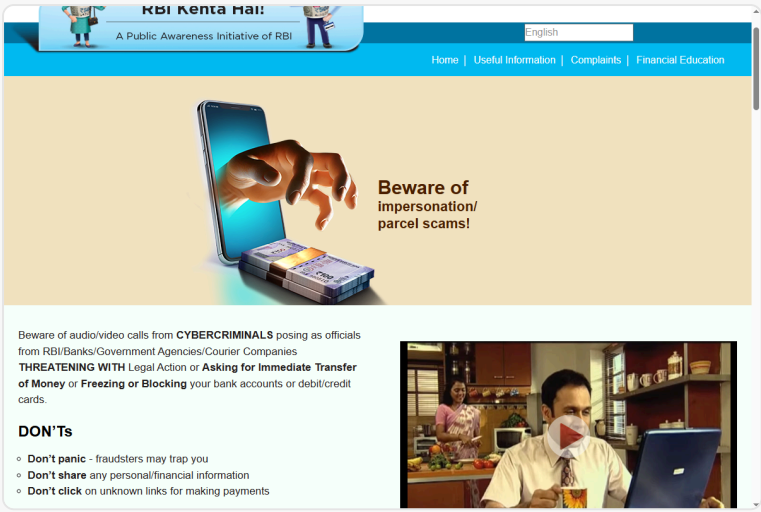
If you have even 1% doubt, hang up right away. Flip your debit or credit card over and call the official customer care number printed on the back.

RBI Kehta Hai: The Truth About Fake Bank Officer Calls

In its public awareness campaign **RBI Kehta Hai**, the Reserve Bank of India warns every citizen against fake calls made in a bank's name:

rbikehtahai.rbi.org.in

RBI Official Public Message



📌 2 Biggest Rules from RBI's Official Message:

1. **Banks Never Ask for OTP:** RBI clearly states that no bank staff or officer will ever ask for your OTP, PIN, password, or card CVV on a phone call.
2. **Hang Up Instead of Panicking:** "Your card will be blocked" or "Your account will be closed" are pure scare tactics. Hang up immediately.

Chapter 2: Do's and Don'ts

✅ Always Do This (DOs)

• Immediately **hang up** on any suspicious call claiming to be from your bank.

• Whenever an OTP SMS arrives, always read the first line to see how much money is being debited.

• For any card issue, call ONLY the **official number** printed on the back of your card.

❌ Never Do This (DONTs)

• Never tell anyone your OTP, card CVV, expiry date, or PIN on a call.

• Never share any code in panic after hearing "Your card will be blocked."

• Never open any link sent by SMS just because someone on a call asks you to.

OFFICIAL & VERIFIED COMPLAINT SOURCES

• 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`

CHAPTER 3 • KYC UPDATES AND THE SIM BLOCK FEAR

Fake KYC Call

The ₹10 trap in the name of SIM and bank KYC, remote app tricks, and official government KYC rules.

"Your SIM Will Shut Down at 12 Tonight": Is That Even True?

Imagine getting a call in the afternoon: *"Sir, I'm calling from Jio / Airtel's KYC Department. Your Aadhaar is not linked to your SIM. Under TRAI orders, your number will be blocked tonight."*

Hearing that makes anyone's heart race. Today our bank, UPI, WhatsApp, and Aadhaar OTPs all depend on that single number. Once fear sets in, people themselves ask the scammer: *"Sir, please tell me what I should do?"*

Legal Truth

Strict Rules of TRAI and the Telecom Department

Under **Telecom Department** rules, no active SIM card can ever be shut down within 24 hours over a single phone call. Real SIM verification happens only in person at the company's official store using your biometric fingerprint.

> **Plain truth:** Anyone saying on a call "Complete your KYC in 2 minutes from home" is 100% a scammer.

Case Study: The Dangerous "Just Pay ₹10" Trap

See how scammers use a tiny ₹10 excuse to empty an entire bank account:

📞 PHONE CALL SIMULATION (FAKE TELECOM AGENT)

> **Scammer (serious tone):** "Sir, your KYC form was rejected in our system. To keep your SIM

active, I sent a link to your phone. Just pay a ₹10 verification fee there."

User: "Only ₹10? Okay, I'll pay it right now."

Scammer: "Yes sir, open the link and enter your net banking or debit card PIN to pay ₹10. Once paid, your KYC will be updated for life."

Truth: *(That link was NOT from the telecom company—it was a **Fake Phishing Page** built by the scammer. The moment the user entered card details and PIN, ₹65,000 was stolen instead of ₹10!)*

The 4-Step Trap of Fake KYC Calls

1. **Threatening SIM or Bank Block**
   The scammer claims: "Aadhaar isn't linked—if you don't update KYC by tonight, your phone will stop working."

↓ Pretending to help from home

2 **Making You Open a Fake Link or Download an App**

The scammer says: "No need to visit a store—click the link below or download the 'Quick Support' app."

↓ Stealing your screen and PIN

3 **Watching Your PIN and OTP via Screen Share**

Once you install that app, the scammer sees your entire phone screen live—and notes down every PIN you type.

↓ Account emptied and number shut

4 **All Money Gone**

The scammer quickly transfers all your money out of your bank account and disconnects.

Real KYC vs Fake KYC Call: 3 Biggest Differences



1. Real SIM KYC Happens Only at an Official Store

Airtel, Jio, or Vi never ask for your Aadhaar or PAN on a phone call. They always invite you to an official store for biometric verification.

> **Rule:** SIM KYC is NEVER done over a phone call.



2. Bank KYC Happens Only in the Official App or Branch

Bank re-KYC can be done only by logging into your bank's official app or visiting your bank branch in person.



3. KYC Never Costs Any Money

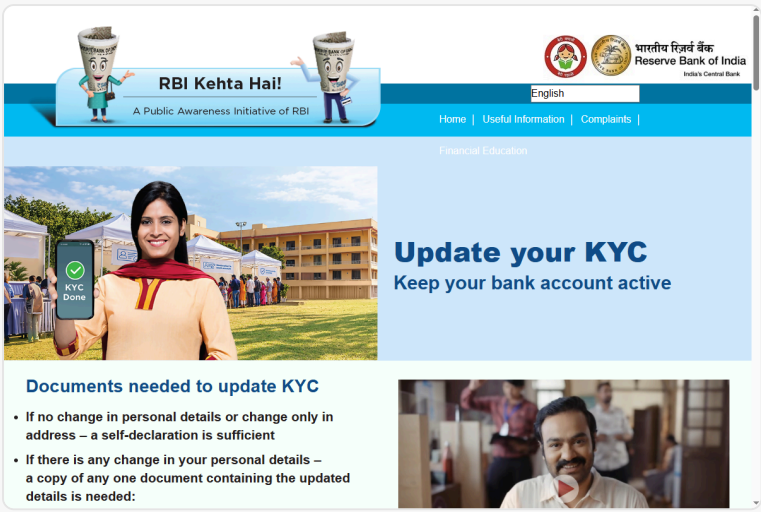
All forms of KYC in India (SIM, Bank, Wallet) are 100% free. Anywhere someone asks for ₹10 or ₹1, it is 100% fraud.

RBI Advisory: Protection from Fake KYC Links and Phishing

The Reserve Bank of India (RBI) has issued clear instructions never to trust fake KYC links sent by scammers:

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

Official RBI Warning



📌 **2 Key Lessons from RBI's Phishing Advisory:**

1. **Don't Open Links Sent via SMS or Call:** No real telecom company or bank ever sends a link by SMS or call asking you to fill out a KYC form.
2. **KYC Is 100% Free:** Updating KYC never costs ₹10 or even ₹1. Anyone asking for money is 100% a fraudster.

Chapter 3: Do's and Don'ts

✅ Always Do This (DOs)

• Hang up immediately if anyone threatens on a call that your SIM will be blocked.

• Visit the company's official store directly to check your SIM status.

• Report fake calls on the official **Chakshu** portal (`sancharsaathi.gov.in`).

❌ Never Do This (DONTs)

• Never click any link on a stranger's instructions during a call.

• Never download AnyDesk, TeamViewer, or QuickSupport in the name of KYC.

• Never make any ₹10 or ₹1 online payment for KYC verification.

OFFICIAL VERIFICATION & COMPLAINT SOURCES

• 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`

CHAPTER 4 • TRUTH ABOUT DIGITAL ARREST AND FAKE POLICE

Digital Arrest: Fake Police, CBI, or Court Calls

Fake police station sets on video calls, fake arrest warrants, and crore-rupee extortion in the name of proving innocence.

"You Are Under Digital Arrest": Does Indian Law Even Have This?

Imagine getting a call saying drugs and fake passports were found in a parcel sent abroad in your name. Next, they tell you to join a video call on Skype or WhatsApp.

On the video call, men in khaki police uniforms sit in front of a police station board with wireless radio sounds in the background. They hold up a paper with a fake Supreme Court seal and arrest warrant: *"You are under Digital Arrest—keep your camera ON 24 hours!"*

PM & Supreme Court Warning

The Biggest Truth of Indian Law

India's Prime Minister and the Supreme Court have clearly warned the whole country: **"There is NO such thing as 'Digital Arrest' under Indian law. No government agency or police ever arrests anyone over a phone or video call."**

> **Plain truth:** Every "police station" shown on a video call is just a fake studio set built by scammers inside a rented room.

Case Study: Fake Police Station Drama on Video Call

See how scammers use fear and atmosphere to hold victims hostage mentally:

☎ VIDEO CALL SIMULATION (FAKE CRIME BRANCH STUDIO)

> **Fake Inspector (in uniform + wireless sound behind):** "Sunita ji, 16 bank accounts were

opened with your Aadhaar and ₹38 crore was laundered. The Supreme Court has issued your non-bailable arrest warrant."

Sunita ji (trembling): "Sir, I have never committed any crime in my life! I have nothing to do with these accounts."

Fake Inspector: "If you are innocent, cooperate with our probe. Lock your room door from inside right now. Tell any relative or lawyer and we'll add a treason case. Now transfer all your money to our Secret Verification Account so we can check it isn't black money."

Truth: *(Terrified, she broke ₹45 lakh of Fixed Deposits and sent it to the scammer's account. The moment the money landed, the video call cut off!)*

The 4-Step Trap of Digital Arrest Scams

1 **Fake Customs or Courier Call**

They claim: "Drugs were found in a parcel sent to Taiwan using your Aadhaar—connecting you to Mumbai Police."

↓ Fake studio set on video call

2 **Skype / WhatsApp Video Call**

Scammers wear uniforms and show fake CBI ID cards, FIR copies, and arrest warrants on screen.

↓ Locking you alone in a room (Isolation)

3 **Digital Arrest and Isolation Pressure**

Victims are ordered to stay locked in a room for 24 to 72 hours with the camera always on so they can't ask anyone for advice.

↓ Extortion in the name of innocence

4 **Transferring Money to an "RBI Verification Account"**

They claim: "Transfer all funds to a government account; it'll be returned in 30 minutes after checking." Once sent, it's gone forever!

Real Law vs Fake Digital Arrest: 3 Biggest Truths



1. Nobody Is Ever Arrested on a Video Call

Under Indian law, to make an arrest, police must appear physically in front of you and hand over a formal arrest memo. Video-call arrests are impossible.

> **Rule:** Anyone talking about arrest on a video call is 100% a fraudster.



2. "RBI Verification Account" Is a Complete Lie

The Reserve Bank of India (RBI) never collects money from citizens to prove innocence. No government agency has any such verification account.



3. Police Never Take Statements on Video Call

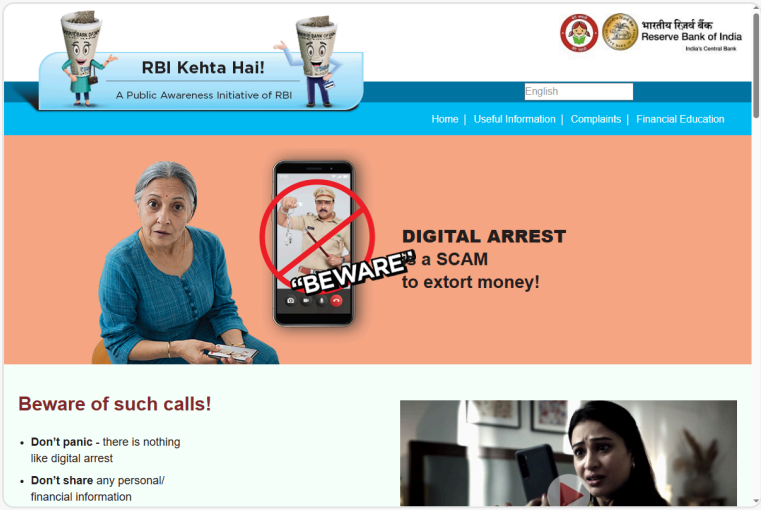
CBI, ED, or Police send official summons for any inquiry. They never interrogate people on Skype or WhatsApp video calls.

Official Advisory: The Truth About Digital Arrest Frauds

The Reserve Bank of India (RBI) and the Ministry of Home Affairs (Cyber Dost) issued this strict official alert against Digital Arrest scams:

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

Official RBI & MHA Warning



📌 **2 Essential Facts from the Official Alert:**

1. **No Law Called Digital Arrest Exists:** No Indian agency (Police, CBI, ED, Court) has any power to detain or arrest people on a video call.
2. **Verification Accounts Are 100% Fake:** Neither the government nor police ever ask citizens to deposit money for "checking." Anyone asking for money is 100% a criminal.

Chapter 4: Do's and Don'ts

✅ Always Do This (DOs)

• Hang up immediately the moment someone threatens "Digital Arrest" on a video call.

• Tell your family, children, or visit your local police station right away.

• Report such fake calls immediately on the official Cyber Portal `cybercrime.gov.in`.

❌ Never Do This (DONTs)

• Never lock your room door and sit alone out of fear.

• Never transfer your money to any unknown account to prove your innocence.

• Never trust any warrant or paper flashed on a video call.

OFFICIAL VERIFICATION & COMPLAINT SOURCES

• 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`

CHAPTER 5 • GOOGLE SEARCH AND HELPLINE FRAUD

Fake Customer Care Call

The full truth about fake helpline numbers on Google Search, remote screen sharing apps, and refund scams.

The Biggest Mistake When Searching Numbers on Google

Suppose you ordered food or bought something online. The order got cancelled, yet ₹450 was deducted from your bank account. Naturally, you get anxious about when your refund will come.

In a hurry, you open Google and type: *"Zomato Customer Care Number"* or *"Courier Refund Helpline"*. A 10-digit mobile number appears right at the top—and you call it without thinking.

Be Careful

Google Search Is Not a Verified Phone Book!

The top result on Google is not always the real company. Scammers pay Google to run **Sponsored Ads** showing their fake number at the top—or even add their mobile number onto real shop listings on Google Maps.

> **Plain truth:** A number at the top of Google Search doesn't have to be real. Scammers can pay for fake ads.

Case Study: Lost ₹60,000 While Chasing a ₹350 Refund

See how polite scammers talk people into handing over full control of their phone:

📞 PHONE CALL SIMULATION (FAKE SUPPORT EXECUTIVE)

> **User:** "Sir, I cancelled an online order, but my ₹350 refund hasn't arrived yet."

> **Scammer (very polite voice):** "Hello sir! We're very sorry for the trouble. Your money is stuck on our server. I'm releasing your refund right now."

> **User:** "Yes, please tell me what I need to do."

> **Scammer:** "Sir, to connect directly with the bank server, download **'QuickSupport'** or **'AnyDesk'** from the Play Store. Open it and tell me the 9-digit code shown on screen."

> **User (reading the code):** "Yes, the code is 739-102-845."

> **Scammer:** "Great sir! Now open Google Pay or PhonePe and transfer just ₹1 for verification."

> **Truth:** *(The moment the user shared that 9-digit code, the scammer saw the phone screen live. When the user typed their secret UPI PIN for ₹1, the scammer saw the PIN—and wiped ₹60,000 in the next 5 minutes!)*

The 4-Step Trap of Fake Customer Care

1 **Fake Ads on Google Search**

Scammers pay Google to display their 10-digit fake mobile numbers at the very top of search results.

↓ Sweet-talking "help" drama

2 **Making You Download a Remote App**

Under the excuse of releasing a refund, the scammer gets you to install AnyDesk, TeamViewer, or QuickSupport.

↓ Stealing the 9-digit code

3 **Getting the Screen Share Code**

The moment you read out the code, your phone screen runs live on the scammer's laptop or phone.

↓ Seeing UPI PIN and emptying bank

4 **Watching Your PIN and Stealing Money**

The scammer tells you to open your UPI app, sees your PIN on screen, and quietly transfers out all your money.

3 Biggest Differences Always to Remember



1. Official Companies Never Make You Download AnyDesk

No genuine company (Amazon, Flipkart, any Bank, Zomato, Swiggy) ever asks customers to install screen sharing apps like AnyDesk or TeamViewer.

> **Rule:** Anyone asking for a screen sharing app is 100% a scammer.



2. A Normal 10-Digit Mobile Number Is Never a Corporate Helpline

Official helplines of big companies and banks are always listed on the Contact page of their verified website. Never trust a random 10-digit mobile number.



3. You Never Enter a PIN to Get a Refund

When a refund arrives, the bank credits your account automatically. If someone says *"Enter your PIN to receive your money"*, they are robbing you.

Official Advisory: Staying Safe from Fake Support & Impersonation

On its awareness portal **RBI Kehta Hai**, the Reserve Bank of India warns strongly against frauds done by posing as company or bank staff:

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

Official RBI Public Message



📌 **2 Essential Lessons from RBI's Official Advisory:**

1. **Never Panic, Never Share Details:** Scammers trap you by creating fear or urgency. Never share personal details, OTPs, or PINs on a call.
2. **Report on Official Portals:** If you spoke to a fake number or lost money, go straight to `cybercrime.gov.in` and file an urgent complaint.

4 Precautions When Finding Customer Care

on Google

Whenever you need to contact any company, strictly follow these 4 checks:

1. **Step 1: Open "Help & Support" Inside the Official App**
   Instead of searching Google for a number, open "Contact Us" or "Chat Support" directly inside the Swiggy, Amazon, or Bank app.
2. **Step 2: Skip Any Link Marked "Sponsored" or "Ad"**
   If a link at the top of Google results says **Sponsored** or **Ad**, never click it.
3. **Step 3: Never Call a Plain 10-Digit Mobile Number**
   If a search result shows a normal 10-digit mobile number next to a big company's name, it is 100% fake.
4. **Step 4: Use the Number Printed on the Back of Your Card**
   For any bank issue, always flip your debit or credit card over and call only the official helpline printed there.

Chapter 5: Do's and Don'ts

✅ Always Do This (DOs)

• Always use the built-in chat or Help Support inside the official app to reach customer care.

• For bank issues, call ONLY the **official number** printed on the back of your debit or credit card.

• Report fake helpline numbers on the **Chakshu Portal** (`sancharsaathi.gov.in`).

❌ Never Do This (DONTs)

• Never blindly call any unknown mobile number found on Google Search.

• Never download AnyDesk, TeamViewer, or QuickSupport on anyone's support instructions.

• Never enter your UPI PIN on your phone in the name of receiving a refund.

OFFICIAL VERIFICATION & COMPLAINT SOURCES

- 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`

CHAPTER 6 • TRUTH ABOUT FAKE LOANS & ADVANCE FEES

Loan, Credit Card, and Government Scheme Calls

Protection from processing fee scams in the name of zero-interest loans, pre-approved credit cards, and government schemes.

Lakhs in Loans Over a Call: A Blessing or a Deadly Trap?

Imagine badly needing money to grow your shop, repair your home, or pay school fees. Suddenly, in the afternoon, your phone rings:

"Congratulations sir! A ₹5,00,000 business loan under the PM Mudra Loan scheme has been sanctioned on your Aadhaar and PAN. No CIBIL score, no ITR, and no guarantor needed—at just 1% yearly interest!"

The Greed Game

Why Can't You Get Lakhs in Loans Without Documents?

The basic rule of banking is that no real bank lends even ₹10,000 to a stranger without verifying identity and CIBIL score. Scammers know a person in financial need easily trusts an "easy loan" offer.

> **Plain truth:** Real banks never ask you to pay ₹1 upfront out of your pocket before giving a loan. Any charges are always deducted from the approved loan amount itself.

Case Study: Lost ₹28,000 Chasing a ₹5 Lakh Loan

See how scammers use fake government letters to extract money bit by bit:

📞 PHONE CALL SIMULATION (FAKE LOAN EXECUTIVE)

> **Scammer (serious, professional voice):**
> "Suresh ji, your ₹5,00,000 loan is approved. I

sent the Sanction Letter on WhatsApp—please check."

Suresh ji: *(Opens WhatsApp and sees a fake Government of India logo, fake RBI stamp, and his own name and photo!)* "Yes sir, got the letter. When will I get the money?"

Scammer: "Sir, the file is at final approval. You must pay ₹2,500 for government GST and file charges to this UPI right away. The loan will reach your account in 15 minutes."

Suresh ji: *(Sends ₹2,500. Twenty minutes later, the phone rings again!)*

Scammer: "Suresh ji, per Finance Ministry rules, a ₹6,500 loan insurance is mandatory for such a big amount. It's refundable—pay quickly or the file gets cancelled!"

Truth: *(Thinking he's already paid ₹2,500 and can't back out now, Suresh ji ends up sending ₹28,000*

> *for insurance, NOC, and tax. Then the scammer switches off the phone and vanishes!)*

The 4-Step Trap of Fake Loan Calls

1. **Baiting with Big Document-Free Loans**

   The scammer calls and promises: "No CIBIL needed, no salary slip—₹5 lakh loan approved in 10 minutes."

   ↓ Fake government papers

2. **Fake Sanction Letter on WhatsApp**

   They send forged letters with government seals and RBI logos so you believe it 100%.

   ↓ Demanding advance fees

3. **Demanding File Charge, GST, or Insurance**

   The scammer says: "Pay ₹2,500 to ₹5,000 advance fee first so we can release your loan."

   ↓ Draining money and blocking number

4 **Stealing in Installments and Vanishing**

Once you pay once, they invent new fees and keep looting—without ever giving even ₹1 in loan.

3 Biggest Truths Always to Remember

🚫

1. Real Banks Never Ask for Advance Processing Fees

RBI's clear rule: No genuine bank or NBFC asks customers to pay advance fees out of pocket. All charges are automatically cut from the sanctioned loan amount.

> **Rule:** Anyone asking for money before giving a loan is 100% a scammer.

📋

2. No Loan Comes Without CIBIL or Income Checks

No bank in the world hands out lakhs without checking your identity and ability to repay. Anyone promising "no-document loans" is only out to cheat you.

🏛️

3. Government Scheme Money Never Goes via Personal UPI

Demanding money into a person's private UPI or bank account for PM Mudra or any government scheme is illegal. The government never asks for UPI transfers on calls.

Official Portal: Check Fake Schemes and Illegal Loans

The Reserve Bank of India (RBI), SEBI, and partner regulators launched the **Sachet Portal** to protect citizens from fake financial schemes and illegal loans:

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

Official RBI & SEBI Joint Portal



📌 **2 Essential Lessons from Sachet Portal:**

1. **Report Fake Loan Calls:** If someone on a call asks for money in the name of no-paper loans, big returns, or government schemes, report it right on Sachet Portal.
2. **Verify Registered NBFCs:** Before borrowing from any unknown company or app, check here if it is an RBI-registered bank or NBFC.

Chapter 6: Do's and Don'ts

✅ Always Do This (DOs)

• Always visit your nearest bank branch directly when you need a loan.

• Always verify any unknown loan company on the **Sachet Portal** (`sachet.rbi.org.in`).

• Report fake loan calls on the government **Chakshu** portal (`sancharsaathi.gov.in`).

❌ Never Do This (DONTs)

• Never pay even ₹1 upfront for loan approval or file processing.

• Never trust any sanction letter or stamped paper sent on WhatsApp.

• Never send photos of your Aadhaar, PAN, or bank passbook to anyone on a call.

OFFICIAL VERIFICATION & COMPLAINT SOURCES

- 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`

CHAPTER 7 • TRUTH ABOUT REMOTE ACCESS & PHONE HACKING

Screen Sharing and Remote App Scams

How AnyDesk, TeamViewer, and QuickSupport hand over full control of your phone—and how to stop it right away.

When Your Phone Falls Into Someone Else's Control

Imagine getting a call with a very serious voice: *"Sir, your last electricity bill payment isn't showing in our system. Your home power will be cut at 9:30 PM tonight."*

When you nervously say you don't know how to fix it online, the scammer acts super helpful: *"Don't worry sir, you don't have to do anything. Just open Google Play Store and download 'AnyDesk' or 'QuickSupport'. Our support team will fix it from here."*

Serious Danger

A Screen Sharing App Is No Ordinary App!

Apps like AnyDesk, TeamViewer, and RustDesk are built for IT engineers to fix computers remotely. When you install them on your phone, the other person sees every screen, every photo, and every incoming OTP live.

> **Plain truth:** Giving an AnyDesk or TeamViewer 9-digit code to a stranger is like handing your house keys to a thief.

Case Study: ₹1.2 Lakh Wiped Over an Electricity Bill

See how scammers watch your entire phone screen using a 9-digit code:

📞 PHONE CALL SIMULATION (FAKE SUPPORT EXECUTIVE)

> **Scammer (helpful voice):** "Satish ji, only ₹110 of your bill is pending. I'm not sending any link

—just install 'AnyDesk' from Play Store so the bill server can connect to your phone."

Satish ji: "Okay, I installed it. A 9-digit number is showing on screen."

Scammer: "Just tell me that 9-digit code, sir, I'll secure the connection."

Satish ji (reading the code): "The code is 842-195-307."

Scammer: "Great sir! Now open Google Pay or PhonePe and pay the ₹110 bill."

Truth: *(The moment Satish ji shared that 9-digit code, his screen appeared live for the scammer. When he typed his secret 6-digit UPI PIN to pay ₹110, the scammer saw it clearly—and stole ₹1,20,000 in 3 transfers over the next 10 minutes!)*

The 4-Step Trap of Remote App Scams

1 **Fake Fear of Power Cut, SIM, or KYC**

The scammer threatens power disconnection, SIM blocking, or stuck parcels to leave you no time to think.

↓ Installing an app from Play Store

2 **Getting You to Install AnyDesk / TeamViewer**

Pretending to help, they guide you to download AnyDesk, TeamViewer, or QuickSupport from Play Store.

↓ Stealing the 9-digit access code

3 **Getting the Screen Share Code**

The moment you read out the code, your phone screen runs live on the scammer's laptop or phone.

↓ Seeing UPI PIN and emptying bank

4 **Seeing Your PIN on Screen and Stealing Money**

The scammer asks you to open your banking app, watches your PIN live on screen, and empties your account in minutes.

3 Biggest Truths Always to Remember



1. The 9-Digit Code Is the Key to Your House

Sharing your AnyDesk or TeamViewer 9-digit code is just like giving your house keys to a burglar.

> **Rule:** Never share this code with anyone on a phone call.



2. Real Banks Never Ask for Remote Access

No genuine bank, electricity board, or telecom company ever asks customers to download AnyDesk or any screen sharing app.



3. Turn Off Internet Immediately If Screen Is Shared

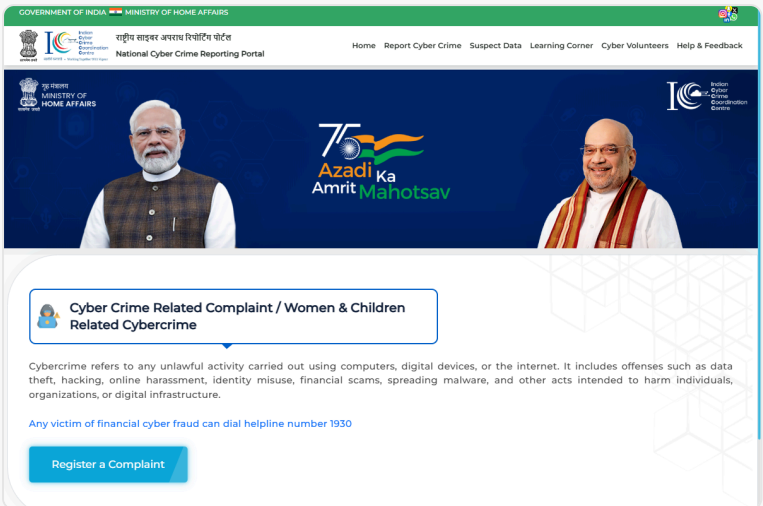
Even if you shared the code by mistake, without wasting 1 second turn off Mobile Data and Wi-Fi or turn on Flight Mode right away.

Official Portal: What to Do Immediately If Remote Fraud Happens

The Ministry of Home Affairs' **National Cyber Crime Reporting Portal** runs 24-hour reporting against cyber fraud and financial theft:

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

Official MHA Portal



📌 2 Essential Facts About Cyber Crime Portal:

1. **Visit the National Portal Immediately:** If money is stolen via a remote app, don't waste a single minute—go straight to `cybercrime.gov.in` and file an urgent complaint.
2. **Report Within the Golden Hours:** Filing within the first 2 hours allows nodal officers to freeze the stolen funds in transit inside bank accounts.

What to Do Right Away If You Downloaded a Remote App by Mistake

If you installed AnyDesk or shared the code on someone's instructions, take these 4 steps immediately:

1. **Step 1: Turn On Flight Mode Immediately**
   Swipe down your phone's top bar and switch on **Flight Mode**. This cuts the internet right away and breaks the scammer's connection.

2. **Step 2: Uninstall the Remote App Immediately**
   Press and hold AnyDesk, TeamViewer, or QuickSupport and **Uninstall (Delete)** it from your phone right away.

3. **Step 3: Alert Your Bank from Another Phone**
   Use a family member's phone to call your bank's official number right away and block your Net Banking and UPI ID.

4. **Step 4: Report Immediately on the Cyber Crime Portal**
   File an immediate complaint at `cybercrime.gov.in` and contact your bank's nodal officer through the official helpline listed on the portal.

Chapter 7: Do's and Don'ts

✅ Always Do This (DOs)

• Always use your electricity board's or bank's official office or app for bill or KYC issues.

• Turn off your phone's internet (Mobile Data & Wi-Fi) the moment you feel suspicious.

• Report fraud immediately on `cybercrime.gov.in`.

❌ Never Do This (DONTs)

• Never download AnyDesk or TeamViewer on any stranger's phone call.

• Never tell anyone the 9- or 10-digit code shown on your screen.

• Never open any banking or UPI app while screen sharing is active.

OFFICIAL VERIFICATION & COMPLAINT SOURCES

• 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`

CHAPTER 8 • AI VOICE CLONING SCAMS

AI Voice Clone: Calls in a Loved One's Voice

Fake accident dramas, police arrest lies, and how AI mimics your loved ones' voices.

Crying Voice: "Dad, I Had a Terrible Accident!"

Imagine your phone ringing in the afternoon from an unknown number. The moment you answer, someone cries and screams:

"Dad... it's Rohan! I had a terrible accident. Someone got hurt and a crowd is beating me. I need ₹40,000 right now for hospital and settlement—I'm calling from my friend's phone, send money to this number!"

The voice sounds exactly like your son—the same tone, the same crying, the same fear. Any parent would shake hearing such a call.

The Real Danger

But What Was the Real Truth?

Rohan was calmly studying in his college library. There had been no accident at all. That crying voice was not Rohan—it was a **Fake AI Voice** created using Artificial Intelligence!

> **Plain truth:** Never trust a call just by how the voice sounds. Scammers can steal 5 seconds of audio from the internet and build an identical fake voice.

Case Study: ₹45,000 Stolen Pretending to Be a Nephew

See how scammers use crying dramas to scare family members into paying fast:

📞 PHONE CALL SIMULATION (FAKE NEPHEW & POLICE)

> **Fake Nephew (crying & screaming):** "Uncle, it's your nephew Amit... Police caught me in a case and took my phone. The inspector is talking—please save me!"

> **Fake Inspector (harsh, heavy voice):** "Hello, Sub-Inspector speaking. An FIR is being filed against your nephew. If you want to save him from court and jail, transfer ₹45,000 to this UPI ID right now—you only have 15 minutes!"

> **Uncle (terrified):** *(The voice truly sounded like Amit—out of fear, he transferred the money immediately without thinking!)*

> **Truth:** Amit was working safely at his office all day. The scammer had simply taken 5 seconds of audio from Amit's Instagram Reel and fed it into AI software.

How Scammers Build an AI Voice Clone

1 **Stealing Audio from Social Media**

Scammers download 5–10 seconds of clear audio from your Instagram Reels, Facebook videos, or YouTube Shorts.

↓ Uploading to voice cloning software

2 **AI Copies the Voice**

AI voice cloning tools learn the person's pitch, tone, and speaking style completely.

↓ Making the voice say anything

3 **Fake Accident or Police Drama**

The scammer types whatever words they want, and the AI speaks them on the call in a crying or panicking voice.

↓ Panicked money transfer

4 **Money Lost via Urgent UPI**

The panicked family transfers money without checking, and the scammer switches off the phone.

3 Most Effective Ways to Catch a Fake AI Voice Call



1. Family Secret Code

Decide a secret word or question with your family members (like a childhood pet name or a special

date).

> **Golden tip:** Whenever an emergency call arrives, ask for that secret code first. AI can never know it.



2. Hang Up Immediately and Call the Real Number

Never trust a call from an unknown number. Hang up right away and call your child's or relative's real saved mobile number.

> **If their phone doesn't connect:** Call their friend, roommate, or college/office colleague to verify.



3. Ask a Personal Question Only They Know

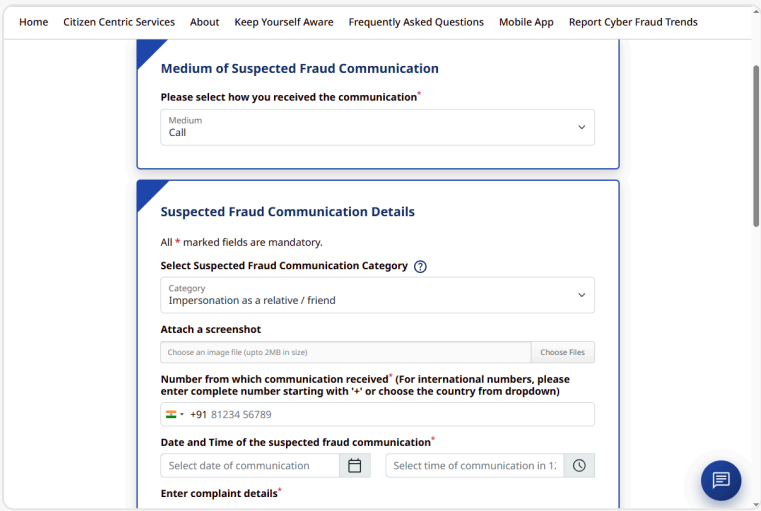
Scammers only have a copy of the voice, not your personal memories.

> **Ask right away:** "What did we eat for dinner last night?" or "What was our old car's number?"

Report Fake Calls Immediately on the Official Portal

The Telecom Department launched **Chakshu** on the Sanchar Saathi portal, where you can report fake calls made by pretending to be a relative:

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



Report on Chakshu Portal in 3 Easy Steps:

1. **Choose Medium:** Open the Chakshu Reporting page and pick `Call`.
2. **Select Category:** Choose `Impersonation as a relative / friend` from the list.
3. **Enter Number & Details:** Fill in the caller's number and time, and submit the form with OTP.

Do's and Don'ts (Golden Rules)

✓ Do's

✓ Hang up right away and call your family member's real saved number.

✓ Keep a Family Secret Code known only to your household.

✓ Ask personal questions that no scammer could ever know.

✓ If money was deducted, go to cybercrime.gov.in within 15 minutes.

✕ Don'ts

✕ Don't panic just because you hear crying or screaming.

✕ Never send money to any new UPI ID or account given by a stranger.

✕ Don't keep your voice clips and daily routine completely public on social media.

✕ Never pay immediately out of fear of any 'Inspector' or 'Doctor'.

VERIFIED OFFICIAL 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

CHAPTER 9 • ONE-RING & INTERNATIONAL MISSED CALL SCAMS

Missed Calls and Unknown Number Traps

1-second missed calls from foreign country codes, huge bills on calling back, and the truth about Wangiri fraud.

A 1-Second Ring at 2 AM: One-Ring Scam (Wangiri Fraud)

Suppose you wake up, check your phone, and see a missed call from an unknown number like `+882 13...`, `+232 21...`, or `+247....`

Human curiosity naturally kicks in: *"Who called? Maybe an old friend or relative from abroad!"*

The moment you call back that unknown number, nobody talks on the other side. Instead, strange music plays or a computer voice says: *"Please stay on the line, your call is being connected..."*

The Real Danger

Calling Back Empties Your Wallet

You wait 2 or 3 minutes and hang up thinking nothing happened—until you check your prepaid balance or get your postpaid bill and discover ₹500 was charged for just 2 minutes!

> **Plain truth:** Around the world, this is called the **Wangiri Scam** or **One-Ring Scam**. Never call back unknown foreign numbers.

Case Study: ₹1,400 Vanished from Mobile Balance

See how calling back a 1-second missed call creates a massive bill:

📞 PHONE CALL SIMULATION (ONE-RING WANGIRI TRAP)

> **Mohit ji:** *(Sees a missed call from a +882 number)* "Maybe it's a friend's new number from abroad—let me call back once."

> **Recorded Audio (sweet, tempting voice):** "Congrats! Your mobile number was picked for an International Lucky Draw. Press 1 and stay on the line to claim your ₹25 lakh prize..."

> **Mohit ji:** *(Presses 1 and waits 4 minutes while music plays and nobody speaks)*

> **Truth:** As soon as the call ended, ₹1,400 was wiped from Mohit ji's balance! It was a premium-rate international line whose fee went straight to the scammer's foreign company.

The 4-Step Cycle of One-Ring Scams

1. **1-Ring Call by Computer**
   Scammers use auto-dialers to ring millions of numbers for just 1 second and hang up.

   ↓ Exploiting human curiosity

2 **User Calls Back**

People assume they missed an important call and call back the unknown foreign number without checking.

↓ Connecting to a premium line

3 **Keeping You Holding on the Line**

Recorded music or fake lottery announcements keep you stuck on the line for 3 to 5 minutes.

↓ Heavy ISD bill deduction

4 **Shocking ₹100 to ₹300 Per Minute Charge**

Huge charges get deducted from your balance or postpaid bill, paying a commission to the scammer.

3 Big Rules: How to Stay Safe from Unknown Missed Calls

🚫

1. Never Call Back Unknown Numbers Outside +91

India's country code is +91. If a number starts with strange codes like +882, +232, +247, or +685, never call back.

> **Simple rule:** If you don't know the person, ignore or block foreign missed calls right away.



2. Important Calls Always Call Again

If a relative or colleague truly has urgent work, they won't ring for 1 second and vanish.

> **Remember:** They will call again or send an SMS/WhatsApp message.



3. Turn On TRAI DND (Do Not Disturb)

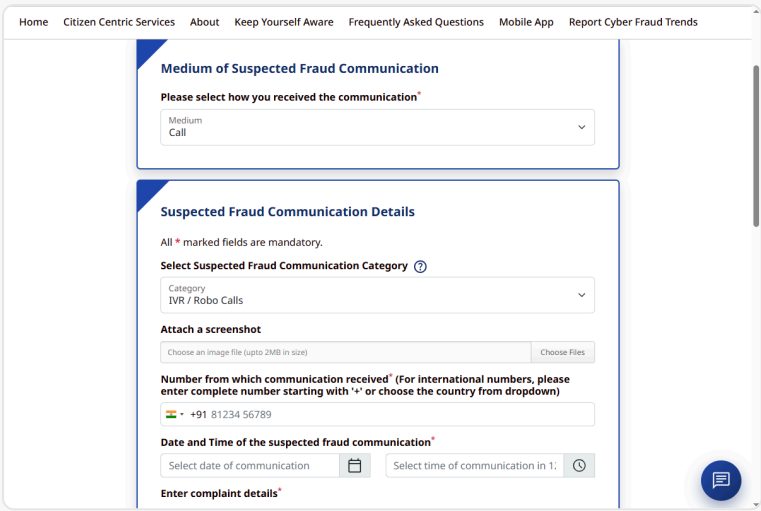
Activate DND using TRAI's official website (`trai.gov.in`) or the official TRAI DND app.

> **Benefit:** Unwanted commercial and spam calls get blocked automatically.

Report Spam Calls on Sanchar Saathi Chakshu Portal

If you keep getting unknown foreign calls, robocalls, or 1-ring spam, report them on the government's Chakshu Portal:

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



Report Spam Calls on Chakshu Portal in 3 Easy Steps:

1. **Choose Medium:** Open the Chakshu Reporting page and choose `Call`.
2. **Select Category:** Pick `IVR / Robo Calls` from the dropdown menu.
3. **Enter Unknown Number:** Fill in the spam/foreign number and call time, then submit.

Do's and Don'ts (Golden Rules)

✓ Do's

✓ Ignore or block 1-ring missed calls from unknown foreign numbers right away.

✓ Keep DND active on your number via the official TRAI DND app or website.

✓ Report repeated spam calls on Chakshu Portal (`sancharsaathi.gov.in`).

✓ If you pick up by mistake, hang up within 1 second.

✗ Don'ts

✗ Never call back an unknown foreign number out of curiosity.

✗ Never stay on hold listening to music or a computer voice on an unknown call.

✗ Never press any keypad button during a recorded spam call.

✗ Never click any link sent from an unknown number.

VERIFIED OFFICIAL 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`

CHAPTER 10 • FAKE STOCK TRADING COURSES

Fake Course and Financial Freedom Calls

False promises of guaranteed stock profits, ₹35,000 courses, and 'Secret Strategy' scams.

The Phone Dream to Get Rich: "Earn ₹2 Lakh Every Month Guaranteed!"

Imagine your phone ringing in the afternoon. A super confident young man or woman speaks:

"Hello sir! Tired of your regular job? Want financial freedom from home? Our research team built a Secret Strategy where clients earn ₹10,000 to ₹25,000 every day. We have a special webinar tonight—shall I book your seat?"

They speak in polished corporate style and send WhatsApp screenshots of luxury cars, expensive hotels, and lakh-rupee profits.

Legal Truth **SEBI's Strict Rule**

India's market regulator SEBI (Securities and Exchange Board of India) has a strict rule: **Nobody in the stock market can EVER promise guaranteed returns or sure profits.**

> **Plain truth:** Whoever promises you guaranteed profits is not making money from trading—they are making money from your course fee.

Case Study: Lost ₹35,000 on a "No-Loss Course"

See how false dreams sold on calls steal people's money:

📞 PHONE CALL SIMULATION (FAKE STOCK MARKET GURU)

> **Course Executive:** "Sir, only 5 seats left! In our 3-day VIP Masterclass we teach a Secret

Strategy that never fails. The fee is ₹35,000, which you'll recover in 1 week of trading."

User: "But is there a risk of loss? I don't know much about stocks."

Course Executive: "0% risk sir! Our team sends 3 sure-shot tips on WhatsApp daily. Just buy and sell blindly—book your seat today."

Truth: As soon as he paid, they only sent links to old ordinary YouTube videos. When the user invested in their stock tips, he lost ₹80,000 more—and when he asked for help, they blocked his number!

The 4-Step Cycle of Fake Course Scams

1 **Showing Off Fake Wealth on Social Media**

They lure people using rented luxury cars and Photoshopped profit screenshots.

↓ Cold calling unknown numbers

2 **Selling "Financial Freedom" on Calls**

They pull numbers from leaked databases and pitch easy side income from home.

↓ Collecting heavy fees

3 **₹15,000 to ₹50,000 Course Fees**

Using pressure like "limited seats" and "today-only discount", they collect huge course fees via UPI.

↓ Blocking you after losses

4 **Old Free Content and Disappearing**

They hand over basic 10-minute internet videos and kick students out of the group once losses happen.

3 Biggest Rules: Avoiding Fake Stock Market Calls

🔍

1. Check SEBI Registration

Anyone giving stock market advice in India must be registered with SEBI.

> **Simple rule:** Always verify their registration number on SEBI's official website (`sebi.gov.in`) before paying.

⚠️

2. "Guaranteed Return" Means Pure Fraud

Nobody in the stock market can give 100% guaranteed profits.

> **Remember:** Anyone claiming "No Risk" is the biggest scammer.

📜

3. Watch Out for the "Educational Purpose" Excuse

Scammers cleverly say "This is only for education" while selling buy/sell stock tips inside.

> **Legal truth:** Giving stock tips without registration is illegal under SEBI rules.

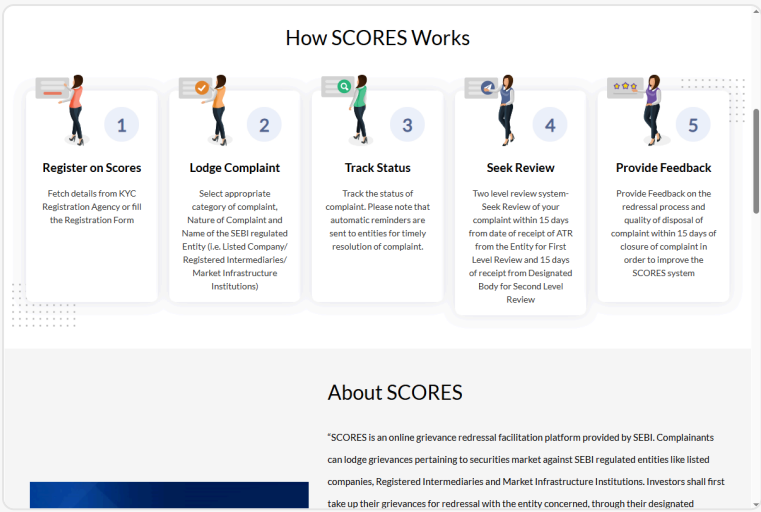
Report Illegal Courses on SEBI's SCORES

Portal

If someone cheated you with false stock promises or unregistered tips, file a complaint on SEBI's official SCORES portal:

scores.sebi.gov.in • SEBI SCORES Portal

Official Portal



Complain on SCORES Portal in 3 Easy Steps:

1. **Register on SCORES:** Type `scores.sebi.gov.in` directly in Google/browser and finish registration.
2. **Lodge Complaint:** Pick the right complaint category and enter details of the fake firm or person.
3. **Track Status:** Track your complaint status online and see SEBI's action.

Do's and Don'ts (Golden Rules)

✓ Do's

✓ Always check any advisor's name on SEBI's official website before paying.

✓ Learn and invest in the stock market using your own understanding.

✓ Report fake claims directly on SEBI SCORES Portal (`scores.sebi.gov.in`).

✓ Always verify any stranger's claims independently.

✗ Don'ts

✗ Never send money for "get-rich-quick" promises on a phone call.

✗ Never give your trading account or Demat password to any stranger.

✗ Never borrow money via loan or credit card to buy a trading course.

✗ Never trust car photos and profit screenshots shown on social media.

VERIFIED OFFICIAL 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`

CHAPTER 11 • FAKE MEMBERSHIP & HOLIDAY CLUB FRAUD

Fake Memberships and Big Promises

Free 5-star hotel stay traps, 25-year VIP club memberships, and lakh-rupee credit card bills.

The Free Bait: "Congrats, You Won a 5-Star Hotel Stay!"

Imagine your phone ringing one day. A very polite young woman says:

"Congratulations sir! Your name was picked among the top 10 winners in the mall lucky draw you filled last month. You and your family won a 3-night, 4-day 5-star hotel stay and a VIP Welcome Voucher!"

She tells you there is zero cost—just drop by a big hotel's banquet hall this evening to collect your gift voucher.

The Real Danger

The Social Pressure Trap at the Hotel

Inside, they pitch a 25-year 'Holiday Club Membership': *"Sir, it actually costs ₹2 lakh, but as a lucky draw winner you only pay ₹55,000. This offer ends tonight at 9 PM—give your credit card right now!"*

> **Plain truth:** No real company hands out lakh-rupee luxury stays free to strangers. "Free Voucher" is just bait to get you to swipe your card.

Case Study: ₹55,000 Lost on a Fake Goa Trip Promise

See how high-pressure hotel presentations push people to swipe credit cards:

📞 HOTEL SALES SIMULATION (FAKE HOLIDAY MEMBERSHIP)

> **Club Executive:** "Sir, 6 nights a year for 10 years at 50+ 5-star hotels across India are 100% free! Just swipe ₹55,000 today for activation."

> **User:** "Will I have to pay extra when booking rooms later?"

> **Club Executive:** "Not at all sir, everything is 100% free. But this special offer is valid only for the next 10 minutes."

> **Truth:** 4 months later when he called to book Goa, they said "No rooms are available that week, plus there's a ₹15,000 maintenance charge." When he asked for a refund, they said the agreement is non-refundable!

The 4-Step Cycle of Club Membership Scams

1. **Collecting Data via Mall Lucky Draws**
   Under the excuse of free coupons or movie tickets, they collect your name, number, and salary details.

↓ Inviting you to a hotel banquet hall

2 **2-Hour Heavy Presentation & Pressure**

Amidst loud music and clapping, families are seated separately with no time to think or talk to relatives.

↓ Instant credit card swipe

3 **₹30,000 to ₹1,00,000 Deducted Immediately**

Pressuring you with "today-only discount", they swipe your card and get forms signed right away.

↓ No rooms available at booking time

4 **Hidden Charges and Non-Refundable Excuses**

You never get the promised hotel later, and refund requests are rejected citing tiny fine print.

3 Biggest Rules: Avoiding Fake

Memberships



1. Nothing Is Truly Free

Free hotel stays, club memberships, or gift vouchers are simply bait.

> **Simple rule:** If a company invites you to a hotel saying you won a "free lucky draw", never go.



2. Never Swipe Your Credit Card on the Spot

No matter how huge a discount the salesman promises, never hand over your card right there.

> **Say clearly:** "I will take a copy of the agreement home and decide only after reading the rules calmly."



3. Spoken Promises Have Zero Legal Value

Any sweet promise the salesman makes means nothing unless it is clearly written in the signed

agreement.

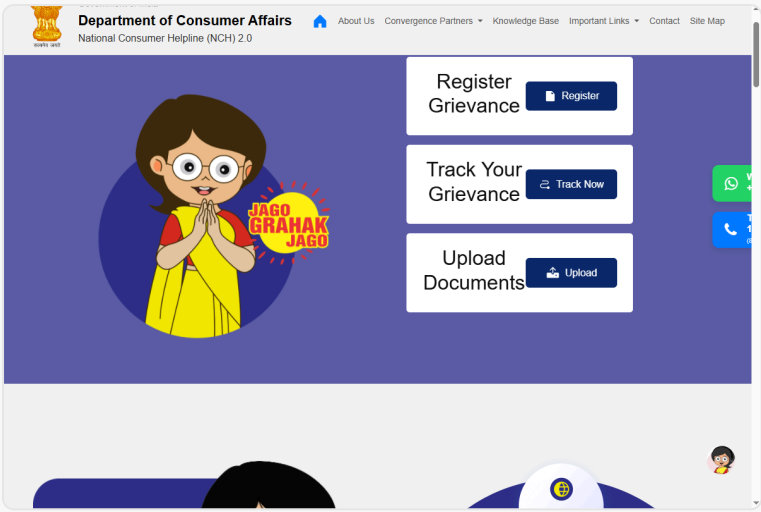
> **Check:** Read the refund and cancellation rules yourself before signing any form.

Complain on the National Consumer Helpline Portal

If a holiday club or company trapped your money with false promises, file an online complaint on the Government of India's Consumer Affairs portal:

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

Official Government Portal



Complain on NCH Portal in 3 Easy Steps:

1. **Open Official Portal:** Type `consumerhelpline.gov.in` directly in Google/browser.
2. **Register Grievance:** Click 'Register Grievance' on the portal and file your complaint against the company.
3. **Upload Documents:** Attach your payment slip, card statement, and membership agreement copy.

Do's and Don'ts (Golden Rules)

✓ Do's

✓ Always read online reviews and complaints about any company before joining.

✓ Immediately file a chargeback request with your bank for unwanted card deductions.

✓ File a complaint on National Consumer Helpline Portal (`consumerhelpline.gov.in`) if cheated.

✓ Always check the refund policy on the written copy of the agreement.

✕ Don'ts

✕ Never attend hotel presentations after a "Free Holiday Voucher" phone call.

✕ Never swipe your credit card on the spot under presentation hall pressure.

✕ Never trust a salesman's spoken promises without written proof.

✕ Never sign any long agreement or form without reading it first.

VERIFIED OFFICIAL 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`

CHAPTER 12 • FAKE LOAN APPS & RECOVERY AGENT THREATS

Loan Fraud and Recovery Agent Threats

The 7-day fake loan app trap, gallery theft, morphed photos, and legal rules against recovery harassment.

Instant Loan Bait: "₹50,000 Loan in 2 Minutes Without Salary Slip!"

You often see tempting ads on social media, SMS, or WhatsApp:

"Get ₹50,000 instant loan with NO salary slip and NO CIBIL score! Just upload Aadhaar and get money in your bank in 2 minutes!"

Needing money urgently, people click the link and install an unknown app.

The Real Danger

Blackmail Starts the Moment Contacts & Gallery Are Stolen

Right after installing, the app asks permission for Contacts, Gallery Photos, and SMS. The moment you tap 'Allow', all your phone data goes to the fraudster's server. Seven days later, they threaten to send morphed obscene photos to your relatives.

> **Plain truth:** RBI strictly forbids any legal bank or lender from accessing your phone contacts or personal photo gallery. Any app asking for them is 100% illegal.

Case Study: ₹80,000 Extorted & Threatened Over a ₹5,000 Loan

See how 7-day fake loan apps mentally terrorize victims:

📞 PHONE CALL SIMULATION (FAKE RECOVERY AGENT)

> **Recovery Agent (angry and abusive):**

"Amit speaking? Today is the due date for your ₹5,000 loan. Transfer ₹9,000 to this UPI ID right now, or I'll ruin your life!"

Amit (scared):
"Sir, the loan was for 3 months and it's only been 6 days! And I only received ₹3,500 in my bank!"

Recovery Agent:
"Don't teach me rules! I have your entire contact list and your sister's photo. If you don't send the payment screenshot in 15 minutes, I'm writing 'THIEF' on your photo and WhatsApping every relative!"

Amit:
"Sir, please don't do that! I'm borrowing from someone right now to send ₹9,000."

Truth: Amit paid ₹9,000 out of fear. The very next day, another number called saying *"₹15,000 system penalty is still pending—pay now!"* Amit lost ₹80,000 in 1 month, yet the blackmail never

> stopped until he filed a legal complaint with Cyber Crime Cell.

How the 7-Day Fake Loan App Trap Works

This illegal syndicate traps people in 4 steps:

1. **Social Media Ads & Unknown APK Links**

   Ads on Facebook, Instagram, or SMS promise "No CIBIL, Instant ₹50,000" and push you to install a third-party APK file.

   ↓ Stealing phone permissions

2. **Uploading Contacts and Gallery to Their Server**

   Upon opening, the app takes Contacts, Camera, Photos, and Storage access and copies all your private data.

   ↓ Heavy fee cuts and 7-day deadline

3. **Cutting High Fees and Sending Less Cash**

   On a ₹10,000 loan, they cut ₹4,000 and send only ₹6,000—then demand double money on day 6.

↓ Morphed photos and blackmail

4 **Sending Morphed Photos & Abusing Relatives**

They paste your face onto obscene images and threaten to send them on WhatsApp to your family and office colleagues.

3 Biggest Rules: Avoiding Fake Loan Apps & Threats

🚫

1. Never Install 7-Day Unknown Loan Apps

Never install any app from Play Store or links claiming to give no-document loans in 2 minutes.

> **Simple rule:** Always apply for loans only through official apps of RBI-registered banks or NBFCs.

🛡️

2. Never Pay Extra Out of Fear (Blackmail Never Stops)

Once you pay a blackmailer out of fear, they know you are scared and will keep inventing new penalties.

> **Simple rule:** Stop paying right away. Not repaying a loan is a civil matter—nobody can send you to jail.



3. Delete the App Immediately and Warn Your Contacts

Revoke app permissions in Phone Settings, delete the app, and inform your relatives upfront.

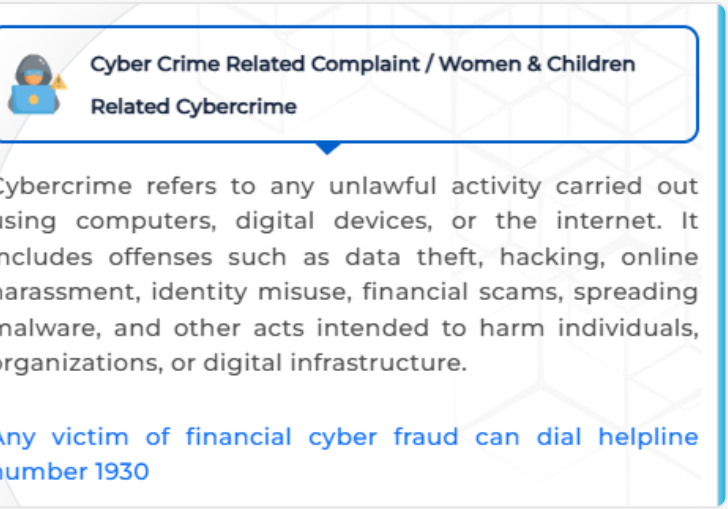
> **Put a WhatsApp Status:** "My phone was hacked. If any fraud number sends fake or morphed photos of me, please report and block it immediately."

File a Complaint Immediately on Cyber Crime Portal

If a fake loan app or recovery agent threatens you with morphed photos or abusive calls, report online on the government portal:

cybercrime.gov.in • National Cyber Crime Reporting Portal

Official Government Portal



File a Complaint on Cyber Crime Portal in 3 Easy Steps:

1. **Open Official Portal:** Type `cybercrime.gov.in` directly in Google/browser.
2. **Report Other Cyber Crime:** Click 'Report Other Cyber Crime' or 'Financial Fraud' on the portal.
3. **Attach Evidence:** Upload screenshots of threatening WhatsApp chats, call recordings, and the app name, then submit.

Do's and Don'ts (Golden Rules)

✓ Do's

✓ Apply for loans only from RBI-registered banks and NBFCs.

✓ Never grant Contacts and Storage permissions to any loan app.

✓ Save recordings of threatening calls and screenshots of WhatsApp chats.

✓ Warn family and friends early that a fraud app stole your contact data.

✕ Don'ts

✕ Never install loan apps from social media ads or SMS links.

✕ Never fall into the trap of any 7-day quick loan app.

✕ Never keep transferring extra money out of fear of blackmailers.

✕ Don't suffer mental stress silently—file a legal complaint with Cyber Cell right away.

VERIFIED OFFICIAL 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

CHAPTER 13 • FAKE RELATIVE & FRIEND IMPERSONATION

Calls Pretending to Be a Relative Asking for Money

The trick of posing as an uncle, old friend, or relative in an emergency—and how to catch it.

"Recognize Me? It's Me!" — The Voice & Relationship Trick

Imagine getting a call early morning from an unknown number. A warm, friendly voice says:

"Hello! Recognized me? Come on, don't you know my voice?"

Out of politeness, people hesitate to say they don't know—thinking the other person will feel bad. So you guess yourself: *"Oh... is that Ramesh bhai?"*

The Real Danger

The Guessing Game: Making You Say the Name

The fraudster instantly plays along: *"Yes, yes, Ramesh! How is everyone at home? I lost my old phone, so I'm calling from a new number."* Two minutes later, the fake emergency drama begins.

> **Plain truth:** When a stranger says "Recognize me?", never guess a name. Ask plainly: "Who is speaking? Please tell me your full name."

Case Study: "Uncle, It's Your Nephew Rahul Speaking"

See how fake emergencies and panic pressure steal people's money:

PHONE CALL SIMULATION (FAKE NEPHEW)

> **Caller (panicked voice):**
> "Hello Uncle! Recognize me? It's Rahul calling from Pune."

Suresh ji (58 years old):

"Oh Rahul beta! What happened to your voice? Is everything okay?"

Caller:

"Uncle, I'm in huge trouble! My car hit a bike rider. Police are catching me. I need to pay ₹30,000 at the hospital right now or police will file an FIR!"

Suresh ji (worried):

"Beta, did you call your father?"

Caller:

"No Uncle, Dad has a heart condition—he'll get an attack if he hears! Please don't tell anyone. I'm having my friend send ₹30,000 to your Google Pay—just transfer it to this QR code right away."

Truth: Suresh ji got a fake SMS saying ₹30,000 'Received'. Without checking his bank balance, he sent ₹30,000 from his own account. That evening,

> calling his brother revealed Rahul was calmly sitting in his office and had never called!

How Fake Relative Scams Work (The 4-Step Trap)

This scam exploits your trust in 4 planned steps:

1. **Making You Guess (Guessing Game)**

   The scammer never gives a name first—they chat warmly until you yourself guess a relative's name.

   ↓ Fake emergency story

2. **Hospital or Police Fear**

   They use road accidents, hospital bills, or police threats so you have zero time to think.

   ↓ Fake SMS or transaction trick

3. **"I Already Sent Money to Your Account"**

   Blaming bank server issues, they send a fake SMS claiming money was deposited in your account.

   ↓ Instant drain from your account

4 **Asking for Money on a Third QR or UPI**

The moment you transfer money from your bank, the scammer's number shuts down forever.

3 Biggest Rules: Staying Safe from Fake Relative Calls



1. Never Say a Name First (Test Their Identity)

When a stranger asks "Recognize me?", never guess.

> **Direct question:** Ask "Who is speaking? Tell me your full name." Then ask a personal question only the real relative knows.



2. Call the Old Saved Number to Confirm

Never trust anyone simply because they say they have a new number.

> **Do this right away:** Hang up and call their old number saved in your phone, or call someone else in their house.



3. Never Send Money Just by Seeing an SMS (Check Passbook)

A credit alert SMS can be just an ordinary fake text message.

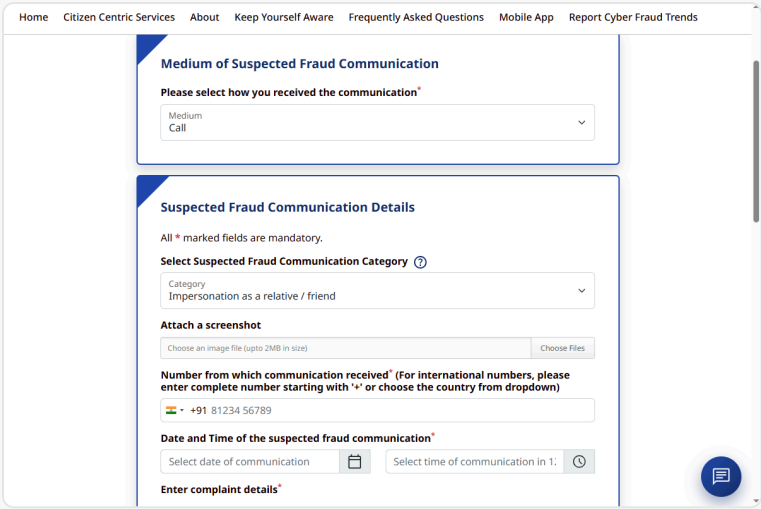
> **Check first:** Open your bank app or Google Pay and check your real account balance yourself. Until money shows in your bank, don't send ₹1.

Report Such Fake Calls on Chakshu Portal

If a stranger tried to cheat you by posing as a relative, report it right away on the government's Sanchar Saathi portal:

sancharsaathi.gov.in • Chakshu Fraud Reporting

Official Government Portal



Report on Chakshu Portal in 3 Easy Steps:

1. **Open Official Portal:** Open `sancharsaathi.gov.in` directly in Google/browser and select Chakshu.
2. **Select Category:** Choose 'Impersonation / Fake Relative or Friend'.
3. **Submit Details:** Enter the fraud caller's mobile number, call time, and short details.

Do's and Don'ts (Golden Rules)

✓ Do's

✓ Always ask unknown callers for their full name and purpose first.

✓ Whenever someone asks for money, call their old saved number to verify.

✓ Always check your real balance in your bank app before sending money forward.

✓ Report the fraud number right away on Chakshu Portal.

✕ Don'ts

✕ Never guess a name when someone asks "Recognize me?"

✕ Never transfer money in panic on hearing "emergency" or "police".

✕ Never send money forward based only on an SMS or WhatsApp screenshot.

✕ Never act alone if told a family member had an accident or fell sick.

VERIFIED OFFICIAL 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

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

Prize, Lottery, Courier, and SIM Block Calls

The truth about winning a car, drugs found in FedEx parcels, and threats to cut your SIM in 2 hours.

"Your SIM Will Shut Down in 2 Hours!" — Twin Weapons of Fear and Greed

Phone scammers rely most on two traps:

1. Greed: *"Congrats! You won a ₹25 lakh KBC Lottery or a brand-new car!"*

2. Fear: *"Notice from Telecom Department: Your mobile SIM will be blocked in 2 hours—press 9 now!"* or *"Your FedEx parcel was caught with illegal drugs inside!"*

The Real Danger

Giving You Zero Time to Think Is Their Main Trick

Whether using greed or police fear, scammers never give you 1 minute to think or talk to family. They push you to transfer money immediately for GST, Customs Clearance, or Penalty.

> **Plain truth:** No Indian telecom operator or Customs Department ever uses IVR calls to block numbers or collect fines via UPI.

Case Study: "Drugs Caught in Your FedEx Courier"

See how everyday citizens are terrified using Customs and Narcotics threats:

PHONE CALL SIMULATION (FAKE COURIER & CUSTOMS)

> **Caller (serious tone):**
> "Hello, calling from FedEx Courier Head Office. Is this Rohit Verma?"

Rohit:
"Yes, but I didn't send any courier!"

Caller:
"Sir, a parcel was being shipped abroad from Mumbai using your Aadhaar card. Airport Customs found 150 grams of drugs and 3 fake passports inside. An FIR has been filed in your name!"

Rohit (terrified):
"Sir, that parcel isn't mine! Someone misused my Aadhaar!"

Caller:
"If you are innocent, I'm transferring your call to Narcotics Department. Send ₹75,000 to this bank account right now as clearance fee for investigation, or police are coming to your home!"

Truth: Terrified, Rohit transferred ₹75,000. He later learned that neither FedEx nor Customs ever

> registers cases or asks for bank transfers over the phone. The entire gang ran out of a fake call center.

How Fake Lottery, Courier & SIM Block Traps Work

This syndicate traps victims in 4 steps:

1. **Computerized IVR Call or Flashy SMS**

   A robotic voice warns of "SIM blocking" or an SMS claims you won a car in a lucky draw.

   ↓ Pressing 9 connects to a fake call center

2. **Posing as Customs or Telecom Officer**

   The caller claims to be a senior DoT or Customs officer and creates heavy fear of legal action.

   ↓ Urgent money demand

3. **GST, RTO Fee, or Clearance Excuses**

   They demand money as lottery registration fee or 'Anti-Terror Clearance' for the parcel.

   ↓ Vanishing once paid

4 **Demanding New Taxes & Blocking Numbers**

After the first payment, they invent fresh fees and eventually switch off all numbers forever.

3 Biggest Rules: Staying Safe from These Calls



1. Hang Up Immediately on "SIM Blocking" IVR Calls

The Telecom Department never calls saying "Your number will be blocked in 2 hours."

> **Simple rule:** Never press 9—hang up right away. If unsure, check at your operator's official store.



2. Don't Fear Fake Illegal-Parcel Claims

Customs or Police never record statements over the phone or demand money via UPI.

> **Simple rule:** If you never sent any parcel, hang up. No real police case works like that.



3. Never Pay Advance Fees to Claim Any Prize

You can never win a lottery you didn't even buy a ticket for.

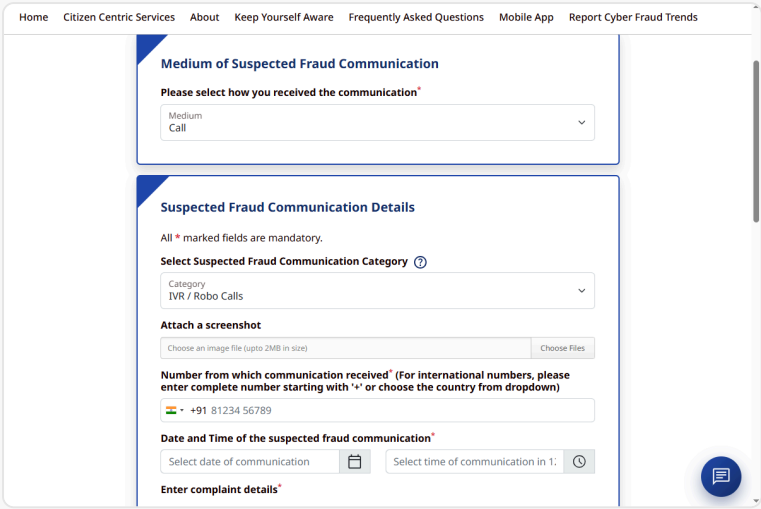
> **Golden rule:** Real prizes deduct tax from the winnings—winners are never asked to pay advance fees.

Report IVR & Robocalls on Chakshu Portal

If you received a SIM block threat, fake lottery, or courier fraud call, report it right away on the Sanchar Saathi portal:

sancharsaathi.gov.in • Chakshu Robocall Reporting

Official Government Portal



Report on Chakshu Portal in 3 Easy Steps:

1. **Open Official Portal:** Open `sancharsaathi.gov.in` directly in Google/browser and tap Chakshu Service.
2. **Select Category:** Choose 'Fake Telecom Notice / SIM Disconnection' or 'Lottery Fraud'.
3. **Submit Details:** Enter the fraud number, call time, and details, then submit.

Do's and Don'ts (Golden Rules)

✓ Do's

✓ Hang up right away on IVR calls threatening SIM disconnection.

✓ Before believing any prize call, ask yourself if you ever bought a lottery ticket.

✓ Disconnect without fear if told illegal items were found in a courier.

✓ Report fraud numbers immediately on Chakshu Portal.

✗ Don'ts

✗ Never press 9 on an IVR call to talk to "customer support".

✗ Never pay advance registration fees to claim a prize or gift.

✗ Never share bank account or Aadhaar details out of fear.

✗ Never transfer money to any bank account on an unknown caller's instructions.

VERIFIED OFFICIAL 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`

CHAPTER 15 • EMERGENCY RESPONSE & CYBER COMPLAINT

What to Do After Fraud & How to Complain

Golden 2 Hours strategy, freezing bank accounts, Cyber Crime Portal reporting, and RBI Zero Liability rules.

Golden 2 Hours: What to Do in the First 120 Minutes After Losing Money

If money is deducted from your bank account due to a fraud call or fake bank call, don't waste time panicking or blaming yourself.

In cyber crime cases, the first 2 hours are called the **"Golden Hours"**. Scammers quickly move stolen money across fake accounts in multiple states. Acting fast lets your bank and Cyber Police put a Lien Freeze (hold) on those funds.

Legal Protection

RBI's Zero Liability Rule: Your Shield

The Reserve Bank of India (RBI) clearly states that if a customer informs their bank within 3 working days of an unauthorized transaction, the customer's liability is Zero and the bank bears the loss.

> **Plain truth:** Delay lets scammers withdraw the cash from ATMs. The faster you report, the closer to 100% your chance of safe recovery.

Case Study: Action in 30 Minutes Saved ₹1,20,000

See how reporting on time helps bring money back:

EMERGENCY ACTION TIMELINE (SUCCESS STORY)

> **Incident (11:15 AM):**
> Sunil ji got a fake KYC call, and the moment screen sharing started, ₹1,20,000 was

deducted from his account.

Sunil ji's Daughter (11:25 AM):

Without panicking, she immediately took the official number from the bank's portal and permanently blocked the debit card, Net Banking, and UPI.

Online Action (11:40 AM):

She visited the National Cyber Crime Portal (`cybercrime.gov.in`) and submitted the transaction's UTR number and the fraudster's UPI ID.

Truth & Result: Because she reported fast, the portal traced the destination account and froze it immediately. The scammer couldn't withdraw cash from an ATM. After 14 days of legal process, Sunil ji got all ₹1,20,000 back in his account.

4 Emergency Steps the Moment Money Is Deducted

This 4-step process is your surest path to recovering lost funds:

1. **Freeze Your Bank Account and UPI Immediately**

   Open your bank app to block your card or get the helpline from your bank's official portal to stop Net Banking so no more money leaves.

   ↓ Online report within 30 minutes

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

   Go to 'Report Financial Fraud' and enter the Transaction Reference Number (UTR) and the fraudster's account details.

   ↓ Getting the fraud caller's number blocked

3. **Report the Fraud Call on Chakshu Portal**

   Submit the fraud caller's number on Sanchar Saathi's Chakshu portal so their SIM gets blocked fast.

↓ Written receipt at local police

4 **Written Complaint & Receipt at Nearest Cyber Cell**

Submit a written letter with your bank statement and SMS screenshots, and collect your Acknowledgment Number.

3 Biggest Rules: Safe Contact Protocol



1. Never Call Numbers from Google Ads

Scammers put fake customer care numbers inside Google Search Ads.

> **Simple rule:** Type `cybercrime.gov.in` or your bank's official URL directly into the browser address bar yourself.



2. Remember the 3 Working Days Limit

Per RBI rules, informing your bank within 3 days protects you under Zero Liability.

> **Simple rule:** Visit your bank branch right away, hand in a written letter, and take a stamped receipt.



3. Never Format Your Phone (Save All Evidence)

Out of panic, people reset their phones and wipe out all digital proof.

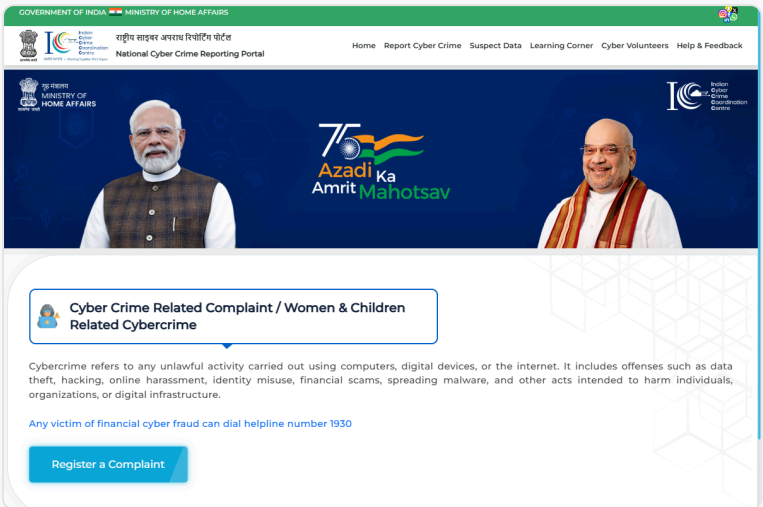
> **Simple rule:** Save call logs, messages, and WhatsApp chat screenshots somewhere safe first.

Report on the National Cyber Crime Reporting Portal

How to file an online complaint on the official portal run by the Ministry of Home Affairs:

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

Official Government Portal



3 Easy Steps to File a Portal Complaint:

1. **Open Official Portal:** Open `cybercrime.gov.in` directly in Google/browser.
2. **Report Financial Fraud:** Click 'Report Financial Fraud' and fill in short details of what happened.
3. **Submit Bank Details & UTR:** Enter your bank name, Transaction ID, and the fraudster's account details.

Do's and Don'ts (Golden Rules)

✓ Do's

✓ Complain to your bank and Cyber Crime Portal within the first 2 hours of losing money.

✓ Always save the transaction's UTR number and SMS screenshots safely.

✓ Submit a written complaint at your home bank branch within 3 days and take a receipt.

✓ Report the fraudulent call right away on Chakshu Portal.

✕ Don'ts

✕ Don't sit silent out of fear or shame if fraud happens.

✕ Never call unknown helpline numbers shown in Google Search Ads.

✕ Never pay any advance fee to a "recovery agent" or "private hacker" promising to get your money back.

✕ Never format your phone after fraud—digital evidence will be destroyed.

VERIFIED OFFICIAL 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

CHAPTER 16 • MASTER POCKET CHECKLIST

Fraud Call Safety Checklist

What Never to Share on a Phone Call — 10 Golden Safety Rules and Complete Pocket Checklist.

Phone Call Master Safety Checklist: What Never to Tell Anyone

This chapter is the most important takeaway of the entire book. Save it on your phone or print and stick it where everyone in your family sees it daily.

95% of phone scams can be stopped completely just by remembering these 10 points:

The Core Rule of Safety

Rule #1: No Government Officer Ever Asks for Money on a Phone Call

Whether someone claims to be a Bank Manager, Police Commissioner, CBI Officer, Supreme Court Judge, or Telecom Officer—Indian law gives NO government department the right to ask for money over a phone or video call.

> **Plain truth:** The moment anyone on a phone asks you to transfer money or share an OTP, know they are 100% a fraudster. Hang up right away!

10 Golden Checklist Rules (Tick Box Summary)

Check These 10 Rules in Daily Life:

- ☑ **1. Never tell anyone your OTP:**
  Even if the caller claims to be a bank manager or police, never share any OTP sent to your phone.

☑ **2. UPI PIN is only for sending money:**
You never need to enter a PIN to receive money, win a lottery, or get a refund.

☑ **3. Never download any screen sharing app:**
Never install AnyDesk, TeamViewer, or QuickSupport and give a 9-digit code to any stranger.

☑ **4. There is no law called "Digital Arrest":**
No Police, CBI, or Court in India ever arrests anyone over a video call.

☑ **5. Never take customer care numbers from Google Search:**
Always get numbers from your bank passbook, the back of your card, or the official website.

☑ **6. Never install 7-day instant loan apps:**
Any app asking for Contacts and Gallery permissions is an illegal blackmail syndicate.

☑ **7. Never press 9 on "SIM blocking" IVR calls:**
The Telecom Department never uses automated calls threatening to cut your number in 2 hours.

☑ **8. Never guess a name when asked "Recognize me?":**
Ask the caller for their full name and purpose first, then confirm on their old saved number.

☑ **9. Beware of AI Voice Scams:**
If someone calls in your child's or relative's voice claiming an accident and asking for money, never transfer right away.

☑ **10. Act within the Golden 2 Hours if money is cut:**
Freeze your bank account immediately and file a complaint on the official Cyber Crime Portal.

What Never to Tell on a Phone Call (Never

Share List)

Private Detail	Caller's Excuse	Your Firm Answer ❌
OTP	"Tell me the 6-digit code to verify your account"	**Refuse clearly!** Real banks never ask for OTPs.
UPI PIN	"Enter your 6-digit PIN to get your refund"	**Never!** Entering a PIN sends money out, never in.
Card CVV	"Give the 3-digit CVV on the back to activate your new card"	**Strictly forbidden!** Never share CVV with anyone.
Screen Share	"Read out the 9-digit code on screen to fix the error"	**Hang up right away!** This hacks your entire phone.
Aadhaar / PAN Photo	"Send your KYC form and ID proof on WhatsApp right now"	**Never!** Never send private documents to strangers.

3-Step Verified Safety Protocol



1. Take a 5-Minute Break When Faced with Fear or Greed

Whenever someone on a call pressures you to pay fast, threatens arrest, or offers a lottery, hang up immediately.

> **Golden rule:** Drink water and think calmly for 5 minutes. Rush is a scammer's biggest weapon.



2. Ask Family or Friends for Advice

Never make a big money decision alone.

> **Simple rule:** Tell sensible family members or friends what happened—the scammer's lie will be caught right away.



3. Trust Only Official Portals

Always go straight to official Government of India portals for any complaint or help.

> **Safe URLs:** `cybercrime.gov.in` and `sancharsaathi.gov.in`

VERIFIED OFFICIAL 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`

APPENDIX

Call Safety Glossary

Digital Arrest

A fake drama where scammers pose as Police/CBI on video call to hold victims trapped in a room for hours until they pay out of fear.

Caller ID Spoofing

Using technology to display a real police station or bank number on your screen while the call actually comes from a fraudster.

Screen Sharing App

Apps like AnyDesk or TeamViewer that let scammers watch your entire phone screen and incoming OTPs live.

AI Voice Cloning

A fraud where AI copies someone's voice from a few seconds of audio to demand ransom or emergency help.

Golden 2 Hours

The first 2 hours right after money is transferred—reporting on Cyber Crime Portal lets banks freeze the fraudster's account fast.

Mule Account

A rented bank account opened in a poor person's name for commission so scammers can quickly pull out stolen money.

140 / 160 Calling Header

Official number series set under TRAI rules for bank and telemarketing calls to tell promotional and service calls apart.

Chakshu Portal

The Telecom Department's official portal where suspicious fraud calls and WhatsApp fraud numbers are reported and blocked nationwide.

Sim Swap Fraud

Issuing a duplicate SIM in your name using fake documents, cutting your phone's signal so all bank OTPs go to the scammer.

Recovery Harassment

Harassing and abusing family members by phone over illegal loans—strictly banned as illegal by RBI.

💡 Keep this glossary handy whenever any phone call feels suspicious.

★ FINAL SECURITY RULES

4 Golden Rules of Call Safety

1. **Digital Arrest Is Fake:** Police, CBI, or Courts never arrest or question anyone on video call. Hang up on any threat.
2. **Never Share Your Screen:** Never install AnyDesk, TeamViewer, or similar apps for bank or KYC work.
3. **Never Share OTP or PIN:** No real bank officer ever asks for your password, card details, or 6-digit OTP on a phone call.
4. **Don't Panic at a Familiar Voice:** If a call in your child's or relative's voice asks for urgent money, hang up and call their old saved number first.

✓ 16 Detailed Chapters ✓ Real-Life Case Studies

✓ DoT & Cyber Portal Verified ✓ Master Pocket Checklist

🤝 Pledge for a Safe Digital India

When you stay calm and hang up smartly instead of panicking on unknown calls, you protect both your family's savings and dignity.

Safe Calls • Safe Family • Safe India

2026 Edition • Independently Published in Public Interest