

Digital Arrest & Impersonation Calls: When Someone Official Demands Money

Fake police, CBI, TRAI and courier calls, the relative "in custody", and the boss on WhatsApp: how each works, the one question that exposes them all, and what to do if you have already paid.

30 min read · Content last verified 18 September 2026 · Reviewed by Shravya M

Free awareness guide. Not legal or financial advice. <https://www.shravyadigital.com/guides/impersonation-calls>

CONTENTS

1. Before you start
2. Chapter 1: The one question to ask
3. Chapter 2: "Digital arrest"
4. Chapter 3: "Your SIM will be disconnected"
5. Chapter 4: The parcel, and the relative "in custody"
6. Chapter 5: The boss on WhatsApp
7. Chapter 6: Calls that look local
8. Chapter 7: What to do: Stop, Think, Take action
9. Quick reference card

Before you start

This guide is the reading for **Course 2** of the Digital Safety Pathway. It takes about 30 minutes to read and covers the calls and messages that pretend to come from someone with power over you: the police, the CBI, a regulator, a courier company, or your own boss.

Every chapter follows the same pattern: **what it looks like, why it works, the check, and the rule**. All names, numbers and stories here are made up.

Keep this number: 1930 is the national cybercrime helpline. If you have already paid anyone, call it first, then your bank.

Chapter 1: The one question to ask

Every scam in this course depends on you believing that someone official can demand money, or your details, over a call or a chat. So ask one question: **"Would a real agency do this on a phone or video call?"**

The answer is no.

- The Prime Minister said in *Mann Ki Baat* on 27 October 2024 that no government agency threatens you on the phone like this, questions you, or demands money on a video call.
- The Telecom Regulatory Authority of India (TRAI) said in August 2025 that **no regulatory body conducts investigations or collects payments through phone calls, messaging apps or video platforms.**

Real officials contact you in ways you can check for yourself, and a real case never gets settled by a UPI transfer to a stranger's account.

The rule: Official people don't collect money on calls. Hang up and check it yourself.

Chapter 2: "Digital arrest"

What it looks like

Meera gets a call from "customs": a parcel in her name holds drugs and fake passports. She is put through to a man in police uniform on a video call, in what looks like a police station. He says she is under "digital arrest", must not hang up or tell anyone, and must move her savings to a "verification account" to prove they are clean.

Why it works

The Ministry of Home Affairs described this exact pattern in May 2024: criminals posing as police, CBI, narcotics officers, RBI or the Enforcement Directorate, using studios made to look like police stations and government offices, and keeping victims on video calls until they pay. Fear stops people thinking, and isolation stops anyone else helping them think.

The check

There is no system of "digital arrest" in Indian law; the Prime Minister called it fraud. If you are told you're under one, you already know it's a scam.

The rule: There is no such thing as a digital arrest. Hang up and tell your family.

Our separate guide to the [digital arrest scam](#) goes further into this one scam.

Chapter 3: "Your SIM will be disconnected"

What it looks like

A recorded message says Ravi's mobile number will be disconnected in two hours "as per TRAI order" because of illegal activity. Press 9 to speak to an officer. The "officer" asks for his Aadhaar number, then transfers him to "Mumbai police".

Why it works

A threat to cut off your phone feels urgent, and naming a real regulator makes it sound official. TRAI's August 2025 advisory lists the tricks that misuse its name:

- **"Your SIM will be deactivated"** calls and messages, often blamed on KYC problems.
- **"Digital arrest" calls** from people pretending to be TRAI or police.
- **Mobile tower installation offers** promising high rent in exchange for an upfront "registration fee", sometimes with a forged TRAI approval.
- **Forged letters and emails** carrying TRAI's logo.

The check

TRAI says it **does not contact customers about disconnecting their number**, has not authorised any agency to do so, and **does not ask for Aadhaar, bank, OTP or other personal details**. If something is really wrong with your connection, your own mobile operator will tell you through its official channels.

The rule: A threat to cut off your SIM is a script. Hang up and call your operator's official number.

Chapter 4: The parcel, and the relative "in custody"

What it looks like

"Your mother has been in an accident and is at the police station. Send ₹40,000 now or the case will be registered." The caller is crying, then a "sub-inspector" takes over.

Why it works

The Ministry of Home Affairs says these calls often claim you sent, or are about to receive, a parcel with illegal goods, or that someone close to you has been caught in a crime or an accident and is in custody. A demand for money to "settle" the case follows. Panic about a family member works on everyone.

The check

- **Call the family member yourself**, on the number you already have. A voice alone is not proof: voices can now be copied by software.
- **Call the police station yourself**, using a number you found on your own, not one the caller gave you.
- No real police officer settles a case by UPI.

The rule: Hang up and call your family on the number you already know.

Chapter 5: The boss on WhatsApp

What it looks like

Priya works in accounts. A WhatsApp message from her director says: "In a meeting. Urgent vendor payment of ₹4.8 lakh, process now, I'll explain later." It is his real number and his real photo.

Why it works

In August 2026, the Indian Cyber Crime Coordination Centre (I4C) warned of a campaign in which people receive a **.zip file** over WhatsApp, SMS or email, named like "**Statement of Account**", "**RBI**" or "**MCA**". Opening it on a Windows computer installs malware that takes over the victim's **WhatsApp Web** session. The account then forwards the same file to all its contacts, and fraudsters use the real account of a senior executive to instruct finance staff to send money to mule accounts. I4C calls this the "**Boss Scam**".

The check

- **Confirm any urgent payment instruction by a direct voice call or in person**, whatever number it came from. This is I4C's own advice.
- **Don't open .zip or .exe files** from messages you weren't expecting. I4C notes that regulators such as the RBI **never** send software updates, security fixes or account statements as WhatsApp attachments.
- **Check linked devices** in WhatsApp (Settings, then Linked Devices) and log out of any WhatsApp Web session you don't recognise or no longer use.

The rule: An urgent money instruction on chat gets a voice call before a transfer.

Chapter 6: Calls that look local

What it looks like

The "CBI officer" calls from a +91 number that looks like an ordinary Indian mobile. That makes it feel real.

Why it works

Fraudsters make international calls appear as Indian mobile numbers, because you're more likely to answer and trust them. The government has directed telecom companies to block such spoofed calls, but some still get through.

The check

- **The number on your screen proves nothing**, including one that looks Indian or looks like a real office.
- You can report an international call that showed an Indian number on **Sanchar Saathi** (sancharsaathi.gov.in) for calls **up to 30 days old**, or by calling **1963** or **1800110420**.
- Report fraud calls and messages on **Chakshu**, also on Sanchar Saathi.

The rule: Caller ID can be faked. Judge the request, not the number.

Chapter 7: What to do: Stop, Think, Take action

These three steps come from the Prime Minister's *Mann Ki Baat* address of 27 October 2024.

1. **Stop.** Don't panic, don't act in a hurry, and don't share personal details. If you can, take screenshots and record the call.
2. **Think.** No government agency threatens you on the phone, questions you on a video call, or demands money this way. If you feel scared, something is wrong.
3. **Take action.** Call **1930** or report at **cybercrime.gov.in**, tell your family and the police, and keep the evidence.

If you already paid

- **Call 1930 straight away**, and **tell your bank the same day** using the number on your card, passbook or bank app. Money still in the fraudster's account can sometimes be put on hold.
- From **1 January 2027**, RBI's new rules for banks count a payment you approved **under coercion or duress** from a third party as a fraudulent transaction, which matters for "digital arrest" victims. Compensation for smaller losses depends on reporting to **both** 1930 or cybercrime.gov.in **and** your bank within **5 calendar days**. Our [UPI & Payment Scams guide](#) explains these rules.

Warning: Anyone who calls offering to "recover" your money for a fee is running a second scam.

The rule: Stop, think, take action. And report to both 1930 and your bank.

Quick reference card

1. **No real agency** questions you or collects money on a phone or video call.
2. **"Digital arrest" does not exist.** Hang up and tell your family.
3. **TRAI doesn't call to disconnect your SIM** or ask for Aadhaar, bank details or OTPs.
4. **A relative "in custody"?** Call them on the number you already have.
5. **The boss wants an urgent payment on chat?** Confirm by voice call or in person first.
6. **Don't open .zip or .exe attachments** you weren't expecting.
7. **Caller ID proves nothing.** Report spoofed calls on Sanchar Saathi or 1963.
8. **Paid already?** 1930 and your bank, both, today.

Take the course for what you just read

Take the free 10-question assessment and pass with 8 or more. Every course you pass counts towards a Pathway Certificate issued by Shravya Digital, earned when you pass all five courses in the pathway: <https://digital.shravyaworld.org/courses/impersonation-calls>

Sources

Checked against these primary sources on 18 September 2026. Rules change: if something here looks out of date, trust the source.

- Ministry of Home Affairs, alert on "Digital Arrest" by cyber criminals (PIB, 14 May 2024) (<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2020570>)
- Prime Minister's address, Mann Ki Baat episode 115 (27 Oct 2024) (https://www.pmindia.gov.in/en/news_updates/pms-address-in-the-115th-episode-of-mann-ki-baat/)
- TRAI advisory on fraudulent activities misusing TRAI's name (PIB, 6 Aug 2025) (<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2153153>)
- I4C caution on the "Boss Scam" and WhatsApp account takeover (PIB, 7 Aug 2026) (<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2295889>)
- Ministry of Home Affairs, steps against digital arrest scams incl. spoofed calls (PIB, 12 Mar 2025) (<https://www.pib.gov.in/PressReleasePage.aspx?PRID=2110809>)
- Report incoming international call with Indian number (Sanchar Saathi) (<https://sancharsaathi.gov.in/InternationalCall/ReportIntCall.jsp>)
- RBI (Commercial Banks - Responsible Business Conduct) Third Amendment Directions, 2026 (24 Jun 2026, effective 1 Jan 2027) (<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=13543&Mode=0>)