Agri Articles
(e-Magazine for Agricultural Articles)
Volume: 06, Issue: 05 (SEP-OCT, 2026)
Available online at http://www.agriarticles.com

The Call That Could Empty Your Bank Account: Inside India's Cyber Fraud Epidemic and The Habits That Could Actually Protect You and Your Family

*Dr. Ekta[1], Dr. Preeti Sharma[2] and Dr. Sukhdeep Kaur[3]
[1]YP-II, ATARI-Ludhiana, Punjab, India
[2]Associate Professor, Department of Extension Education and Communication Management, PAU, Ludhiana, Punjab, India
[3]Assistant Professor, Department of Extension Education and Communication Management, PAU, Ludhiana, Punjab, India
*Corresponding Author's email: ektamachra9510@gmail.com

It usually starts small. A text about a parcel stuck in customs. A call saying your Aadhaar is linked to a crime. Someone friendly on the phone who says they're from the bank and just needs a minute of your time. Then, within minutes, the panic sets in, and by the time it lifts, the money is gone. Cyber fraud in India isn't the occasional bad-luck story anymore. It's one of the fastest-growing crimes in the country, and it doesn't much care how old you are, what you do for a living, or how careful you think you are.

A Crisis Measured in Crores

The numbers are staggering, honestly. UPI and mobile banking spread through the country faster than digital literacy could keep up, and fraud followed right behind. The National Human Rights Commission puts total losses at around ₹52,976 crore over six years, and "digital arrest" scams alone accounted for close to ₹3,000 crore of cases reported to the Supreme Court in 2025. Cybercrime complaints more than doubled between 2022 and 2024, from about 1.03 million cases to 2.27 million.

"These frauds don't just hit people's wallets," the NHRC said at a discussion on digital arrest scams in June 2026. "They hit their sense of safety and dignity too."

Why People Fall For It

Here's the thing about most scams today: they don't need to be technically clever. They just need to move faster than you can think. Fear works best. Tell someone they're being investigated for money laundering or drug trafficking, and the panic that follows makes it hard to think straight. Scammers know this, so they immediately demand secrecy, cutting the person off from the one thing that could stop it: a call to a family member or friend. Sometimes it works the other way. A lottery win. A grandchild supposedly in trouble. AI voice cloning has gotten good enough now that a scammer can fake a grandchild's voice convincingly enough to talk a grandparent into an emergency wire transfer. Older adults do carry extra risk, mostly because of circumstance. A lot of them live alone while their children work in another city or abroad, so there's no one nearby to ask, does this actually sound right to you? But it would be a mistake to treat this as only an elderly problem. Plenty of victims are in their twenties and thirties, busy and distracted, and just as capable of being caught off guard.

The Scams Worth Knowing

Most fraud in India today falls into a few recognisable patterns. Once you've seen the shape of one, the others get a lot easier to spot.

- **Digital Arrest: A Fake Courtroom on Your Screen**

This has become India's most elaborate scam, and it usually plays out in stages. First, someone calls claiming to be from a courier company or telecom provider, saying there's a problem, an illegal parcel maybe, or a mismatch in your Aadhaar details. They transfer you to someone else. That person shows up on a WhatsApp or Skype video call in a police uniform, sitting in front of what looks like a courtroom, and accuses you of a serious crime. Then a third voice, sounding senior and official, declares you're under "digital arrest" and tells you to move money to a government "safety vault."

It sounds almost too theatrical to work, but the losses say otherwise. Once the money moves, it doesn't sit still for long. It gets routed through a string of "mule" accounts and converted to crypto before it disappears abroad.

- **UPI, Phishing, and Fake Investments**

Away from these elaborate setups, most of the damage is done by scams that don't need a script at all. A fake SMS about your account being suspended or your KYC expiring sends people straight to a cloned banking website, or talks them into installing a remote-access app like AnyDesk. UPI has a blind spot too: a lot of people assume you need to enter your PIN to receive money. You don't. Scammers rely on this, sending a "Request Money" notification or a QR code, and the moment you enter your PIN to "accept" it, money leaves your account instead.

Then there's investment fraud, which causes more financial damage worldwide than almost anything else on this list. AI-generated deepfake videos, often of recognisable business leaders, promote trading platforms that show fake profits on your screen while quietly blocking every withdrawal, usually followed by a demand for one more "clearance fee."

The common scams and their warning signs

Scam	What It Preys On	Warning Signs
Digital Arrest	Fear of arrest or legal trouble	"Police" on a video call, forged court orders, demands for total secrecy
KYC / Account Freeze	Fear of losing bank access	Urgent SMS with a link; asked to install a remote-access app like AnyDesk
UPI "Request Money"	Trying to receive a payment	Told to scan a QR code or enter your PIN to "accept" money, which always debits you, never credits
Deepfake Investment	Hope of high, quick returns	AI video of a famous businessperson promising guaranteed profits on an unknown app
Romance / Loneliness	Companionship, connection	An online partner you've never met asks for money, gifts, or crypto

The One Habit That Actually Works

Software helps, but the biggest difference comes down to a habit: treat every unexpected call, message, or video call from a "bank," a "government office," or the "police" as suspicious until proven otherwise. If something feels off, hang up. Call back using a number from your bank's website or the back of your card, never a number the caller gives you. Two things are worth remembering, because scammers count on people not knowing them. No court, police officer, or government office will ever investigate you, issue a warrant, or ask for money over a phone or video call. And no bank will ever ask for your OTP or password. Not to verify you, not to reverse a transaction, not for any reason.

Looking Out for Family

If your parents or grandparents live on their own, a few small changes make a real difference. Turn on real-time SMS and email alerts for their accounts so a large transfer or an early FD closure doesn't go unnoticed. Set a low daily UPI transaction limit, just in case. And agree, as a family, that any big or unexpected money request gets a phone call to someone else in the family before anything moves. It's a small rule, but it directly undercuts the isolation scammers depend on.

Regular check-in calls help too, not just to catch a scam mid-flight but to notice if something feels off, like unusual secrecy or stress. If you can't visit often, a neighbour you trust or a professional check-in service can fill that gap.

Everyday Digital Hygiene

- Use a different, complex password for each account, and turn on multi-factor authentication wherever you can.
- Skip banking or shopping over public Wi-Fi.
- Bookmark your bank's website instead of clicking links in messages or search results.
- Let your phone and security apps update automatically.
- At an ATM, cover the keypad, don't share your PIN, and call your bank right away if the machine keeps your card.

If It Happens to You: The Golden Hour

The first two hours after a fraudulent transaction matter more than people realise. Stolen money usually sits in a chain of "mule" accounts for a while before it's converted to crypto and gone for good, so acting fast can genuinely bring it back. If you or someone in your family gets scammed:

- Call your bank right away to freeze your cards, block net banking, and ask for a transaction recall.
- Call 1930, the national cybercrime helpline, and file a complaint at cybercrime.gov.in.
- Hold onto everything: transaction IDs, screenshots, SMS alerts, call logs.
- If you installed any remote-access software, get off the internet immediately, uninstall it, and consider a factory reset.

Know Your Rights

The RBI has rules for exactly this situation. If the fraud happened because of a problem on the bank's end, or if you report it within three working days and you're not at fault, you owe nothing. Even if you shared an OTP by mistake, you're only responsible for what was taken before you reported it; anything after that becomes the bank's problem, not yours. Banks are supposed to resolve these complaints within 90 days. If they drag their feet, you can escalate to the RBI's Integrated Ombudsman Scheme at cms.rbi.org.in, or call 14440. There's also a lesser-known tool worth bookmarking: the Chakshu facility on the Sanchar Saathi portal (sancharsaathi.gov.in), where you can report a suspicious call or message before any money changes hands. It's already helped disconnect more than 39 lakh mobile connections and blacklist over two lakh handsets tied to scam operations.

What Needs to Change

Staying alert helps, but it isn't the whole answer. A lot of people who study this problem say India also needs stricter rules: clear legal provisions to criminalise digital arrest scams and the misuse of police or government identity, real penalties for anyone renting or selling bank accounts as mule conduits, automatic checks on unusually large transfers, and compensation funds for people who've already lost money. Until that happens, the best protection is still the boring kind: slow down, call someone you trust, and don't be afraid to hang up on anyone who wants secrecy or an instant payment. It isn't much, but it's usually enough

Reference

1. National Human Rights Commission. (2026). NHRC flags ₹52,976 crore cyber fraud losses, seeks urgent action against 'digital arrest' scams. The Hindu. https://www.thehindu.com/sci-tech/technology/nhrc-flags-52976-crore-cyber-fraud-losses-seeks-urgent-action-against-digital-arrest-scams/article71081619.ece