CYBER CENTRE OF EXCELLENCE

Gujarat Police

WITHOUT OTP FRAUD

When Your Money Leaves Without a Code

■ *If no OTP came, you are still the target.*

A Public Awareness Guide

Cyber Crime Helpline: 1930 | cybercrime.gov.in

What Is Without OTP Fraud?

Most people believe their bank account is safe as long as they never share an OTP. **This is no longer true.** A growing share of digital banking fraud in India now happens through channels that do not require — or that silently capture — the One-Time Password. The victim never reads out a code, never approves a transaction, and yet money leaves the account.

These attacks exploit a different weak link: a screen-sharing app installed on your phone, a duplicate SIM issued to a fraudster, a fake banking APK that quietly forwards your SMS, an e-mandate authorised once but renewed forever, or a UPI "collect request" disguised as a refund. In every case, the OTP either never travels through you — or you approve a payment thinking you are receiving one.

The single most important fact:
An OTP is just one layer of defence. **The real defence is recognising the trick before any code is ever needed** — never install an app a stranger asks you to install, never approve a UPI request you didn't initiate, never give your phone to anyone offering "help" with your bank, and always lock SIM-swap and e-mandate channels through your bank's app.

The Scale of the Problem

11.3 L
Cyber-financial fraud complaints registered on NCRP in 2023 (I4C)

₹7,488 Cr
Reported losses across cyber-financial frauds in India, 2023 (MHA / I4C)

1930
Report cyber crime 24×7 All India, toll-free

RBI and NPCI advisories have repeatedly flagged screen-sharing apps, SIM-swap requests, malicious APKs, and unsolicited UPI "collect" requests as the fastest-growing attack vectors in India. Banks have responded with cooling-off periods, mandatory app vetting, and SIM-swap pause windows — but every protection works only when the customer recognises the trick early enough to refuse it.

Five Ways Money Leaves Without an OTP

Each of these attacks reaches your money through a different door — but none of them requires you to read out a code over the phone. Knowing the door is the first step to closing it.

1

Screen-Sharing & Remote-Access Apps

A "bank support" caller asks you to install AnyDesk, TeamViewer, QuickSupport, or RustDesk to "fix" a problem. The moment the app is installed and the 9-digit code is shared, the fraudster sees your screen live and can operate your phone. They open your banking app, read OTPs as they arrive, and transfer money — you watched it happen.

2

SIM Swap

The attacker collects your KYC details (Aadhaar, PAN, address) from leaks, walks into a telecom store, and requests a duplicate SIM. Once activated, your number goes dark and every OTP from that point lands on the attacker's phone — including high-value banking and UPI approvals.

3

Malicious APK Files

You receive a WhatsApp message with an APK file labelled "Wedding Invitation", "Electricity Bill", "Income Tax Refund", or a bank's name. Installing it grants SMS and accessibility permissions; the malware silently reads incoming OTPs and forwards them to a server. You never see the code — but the transaction goes through.

4

UPI "Collect Request" Trick

The fraudster, posing as a buyer for your OLX listing or a refund processor, sends a UPI collect request. The screen says "Pay ₹X" — but they call it a "test credit" or "cashback" and insist you must "approve to receive". Entering your UPI PIN debits — not credits — your account.

5

E-Mandates & Auto-Debits

A one-time approval for a "free trial" sets up a recurring debit (NACH or UPI AutoPay) that pulls money every month or every week without further OTP. Forgotten subscriptions, lottery scams, and "lucky-draw insurance" schemes use this mechanism — silent, recurring, and difficult to revoke for users unaware of the e-mandate page in their UPI app.

How To Protect Yourself

✔ DO THIS

✔ **Uninstall every screen-sharing app** (AnyDesk, TeamViewer, QuickSupport, RustDesk) from your personal phone. You almost certainly do not need them.

✔ Open your UPI app monthly → **Autopay / Mandates** and cancel anything you don't recognise or no longer use.

✔ Set up **SMS & email alerts** for every debit on every account — even ₹1.

✔ Lock the SIM-swap window with your telecom — many operators now offer a 24-hour cooling-off setting.

✔ Read every UPI screen carefully. If it says "**Pay**" — you are paying. A genuine refund **never** needs your UPI PIN.

✔ Install apps **only from the Play Store or App Store**. Block APK installs in your phone's security settings.

✔ If a transaction you didn't make appears, call **1930** and your bank within the golden hour.

✘ NEVER DO THIS

✘ Never install an app a phone caller asks you to install — no bank, no government office, no courier company makes such a request.

✘ Never grant **Accessibility** or **SMS** permission to an app you didn't actively choose to install for a clear reason.

✘ Never enter your UPI PIN to "receive" money. Receiving is automatic; PIN means paying.

✘ Never share an OTP, CVV, card PIN, or screen-share code — even with someone who "already knows your account number" or quotes your last transaction.

✘ Never open APK attachments on WhatsApp, even from known contacts — their accounts may be compromised.

✘ Never ignore a "SIM has gone blank" sudden loss of signal — that is the first sign of an active SIM swap.

Remember:

An OTP-free fraud does not mean you were careless with an OTP. It means the attacker found a different door — usually one you didn't know existed. Closing those doors (no screen-share apps, no APKs from outside the store, no auto-pay you didn't review, no UPI PIN for "refunds") is more powerful than guarding a single OTP. Take fifteen minutes this week to audit your phone — it is the cheapest insurance available.

How to Report — Step by Step

1930

Toll-free | 24×7 | All India

The Reporting Process

1

Call 1930 Immediately

The first hour after the debit is the **golden hour**. The operator records the transaction reference, the beneficiary account, and any phone number involved, and pushes a hold request to the recipient bank to freeze the funds before the mule withdraws them.

2

Inform Your Bank in Writing

Email the bank's fraud helpdesk and visit the branch the same day. Under the RBI's "Limited Liability of Customers" circular, if you report unauthorised electronic transactions **within 3 working days**, your liability is zero for third-party breaches.

3

File at cybercrime.gov.in

Log in and file a complaint under 'Financial Fraud → UPI / Banking Fraud'. Upload bank SMS screenshots, your account statement, screenshots of any screen-share or APK install messages, and the phone number / UPI ID of the fraudster.

4

Cut Off the Attack Channel

Uninstall any screen-sharing or unknown app on your phone. Revoke all suspicious app permissions. If you suspect SIM swap, visit your telecom store and demand a SIM reissue with full ID verification. Cancel any unrecognised e-mandate or UPI AutoPay.

5

Follow Up With Your Complaint Number

After filing, you receive an acknowledgement number. Track progress at cybercrime.gov.in. Visit your local cyber police station with printed evidence and request an FIR if one has not already been registered.

Family Safety Checklist

First-time smartphone users, senior citizens, and those who handle large UPI volumes (small traders, OLX sellers) are the most heavily targeted. Walk through this checklist with every member of your household:

- **Audit every phone in the house** — uninstall AnyDesk, TeamViewer, QuickSupport, RustDesk and any app whose origin you cannot explain.
- Enable **"Block installation from unknown sources"** in Android security settings on every device.
- Open the UPI app → Autopay / Mandates and review every active recurring debit. Cancel anything unrecognised.
- Enable **SMS & email alerts** on every linked bank account, including the dormant ones.
- Teach every family member: a UPI PIN is **always** for paying, never for receiving.
- Save **1930**, your bank's fraud helpline, and your telecom's SIM-swap helpline on every phone in the house.
- Agree on a rule: **no APK file** is ever installed from WhatsApp, SMS, or email — no matter who sent it.
- If a family member suddenly loses mobile signal for hours, treat it as a possible SIM-swap attack and check banking activity immediately.

Real Cases Reported in India

Maharashtra — AnyDesk Screen-Share, ₹3.4 lakh (2024)
A 54-year-old businessman in Pune received a call from a "credit card support team" about an unblock request. He was guided through installing AnyDesk and reading out the 9-digit code. Within ten minutes the fraudsters had operated his banking app from their end, transferred funds across three beneficiary accounts, and read the OTPs aloud from his own screen.

Delhi — SIM Swap of a Senior Citizen (2023)
A retired government official's mobile went blank on a Saturday morning. By Monday his savings account had been drained of ₹7.8 lakh — every OTP from Saturday onward had landed on a duplicate SIM issued at a small telecom outlet. Police arrested the outlet operator. The victim's prompt FIR and bank report within 48 hours preserved his right to limited liability.

Gujarat — APK File via WhatsApp, ₹46,000 (2025)
An Ahmedabad homemaker received a WhatsApp message from a known contact whose account had been hacked, containing an APK labelled "Wedding Invitation Card". After installing, the malware quietly read every banking SMS for two days before triggering a transfer. She reported within the golden hour to 1930; ₹31,000 of the ₹46,000 was successfully frozen by the recipient bank.

Important Contacts & Resources

Service	Contact
National Cyber Crime Helpline	1930 (24×7, toll-free)
National Cyber Crime Reporting Portal	cybercrime.gov.in
Report fraudulent SMS / call (Chakshu)	sancharsaathi.gov.in
Check / disconnect mobile numbers in your name	tafcop.sancharsaathi.gov.in
RBI Sachet (unauthorised entities)	sachet.rbi.org.in
Banking Ombudsman (RBI)	cms.rbi.org.in
NPCI Dispute Redressal (UPI)	npci.org.in/disputes
Police Emergency	112
CERT-In (incident reporting)	incident@cert-in.org.in

Five Things to Remember

1. **No bank ever asks you to install an app.**
   If a caller asks you to install AnyDesk, TeamViewer, or any "support" app, the call is a fraud — hang up immediately, no exceptions.

2. **UPI PIN is always for paying.**
   You never need a PIN to receive money. If anyone tells you to "enter PIN to receive" — they are debiting your account.

3. **APKs from WhatsApp install malware.**
   Never open .apk attachments — wedding cards, bill PDFs, refund forms. Install only from the official Play Store or App Store.

4. **A sudden loss of signal is a warning.**
   If your phone goes blank for hours without reason, suspect SIM swap. Call your telecom from another phone and check your bank balance.

5. **The first hour after fraud is decisive.**
   Call 1930 immediately. Money frozen within the golden hour is recovered far more often than money reported even a day later.

If you remember only one number: **1930**.
If you remember only one app to delete: **any screen-sharing app on your personal phone.**
If you remember only one rule: **UPI PIN is always for paying, never for receiving.**