SECURING HUMAN FOUNDATION

⚠ Cyber Alert

Awareness is protection

Even without an OTP or a link, your bank account can be emptied!

Fraudsters can now take money from your account without asking for an OTP or sending a link. Learn how they do it — and how to stay safe.



How fraudsters cheat

Aadhaar biometric (AePS) fraud

They copy fingerprints from documents or property papers and withdraw money through Aadhaar-enabled payments (AePS) — no OTP needed.

SIM swap / e-SIM fraud

They get a new SIM or e-SIM issued on your number. Your phone shows "No Network" and every OTP goes to them.

The call-forwarding trick

Posing as a courier or customer care, they get you to dial a code like `*401*`. Your calls and OTPs then go to them.

Fake APK files

They send .apk files on WhatsApp named "Wedding card", "Traffic challan", "PM Kisan" or "Bank KYC". Once installed, your SMS and bank apps are theirs.

Screen-sharing apps

Pretending to help, they get you to install apps like AnyDesk or TeamViewer and control your phone remotely.

Public Wi-Fi and charging points

Banking on public Wi-Fi or at unknown USB charging points puts your phone's data at risk.

Been cheated? Dial immediately 1930 | www.cybercrime.gov.in

SECURING HUMAN FOUNDATION

Stay safe

How to stay safe

- **Lock your Aadhaar biometrics** on myAadhaar (myaadhaar.uidai.gov.in) or the mAadhaar app. Unlock only when needed.
- **Share a "masked Aadhaar".** On any photocopy, write the purpose and date, and sign it.
- **Install apps only from Play Store / App Store.** Never open an .apk file sent on WhatsApp or SMS.
- **Never dial a code a stranger gives you.** Dial `*#21#` to check call forwarding, `##002#` to switch it off.
- **No network for a long time?** Contact your mobile operator and bank immediately.
- **Don't install screen-sharing apps** — no bank or company will ask you to.
- **Keep transaction limits low;** switch off online and international transactions when not needed.
- **Keep SMS and email alerts on** and check your bank statement regularly.
- **Don't bank on public Wi-Fi;** use your own charger and mobile data.
- **Your bank never asks** for your PIN, password, CVV or OTP on a call — never share them.

Been cheated? Do this immediately

National Cyber Crime Helpline

1930

24 × 7 · Free

National Cyber Crime Reporting Portal

www.cybercrime.gov.in

File a complaint online

1. **Call 1930 immediately.** Reporting in the first hour (the "golden hour") can stop the money.
2. **Inform your bank** and block your account, cards and UPI.
3. **Keep the evidence** — transaction IDs, screenshots, messages and call details.
4. **Complain at cybercrime.gov.in** and keep the complaint number safe.

Report suspected fraud calls, SMS or WhatsApp messages on the Sanchar Saathi portal (Chakshu): **www.sancharsaathi.gov.in**

Remember: don't decide in fear or in a hurry — stop, think, then act.