OTP and Social Engineering

How attackers manipulate people, not computers - and why an OTP is never meant to be shared.

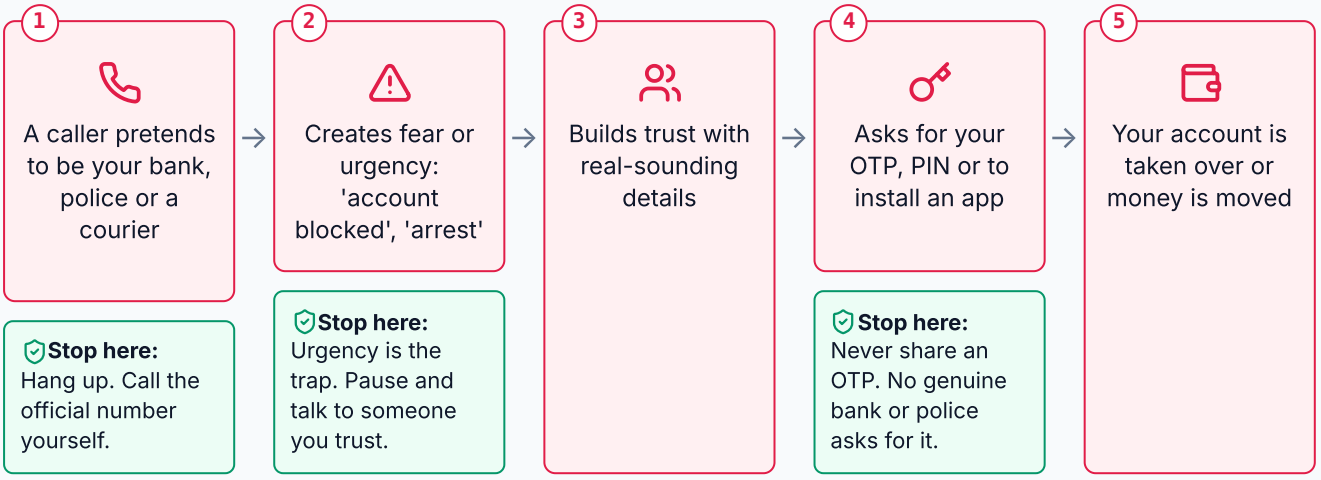
Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.

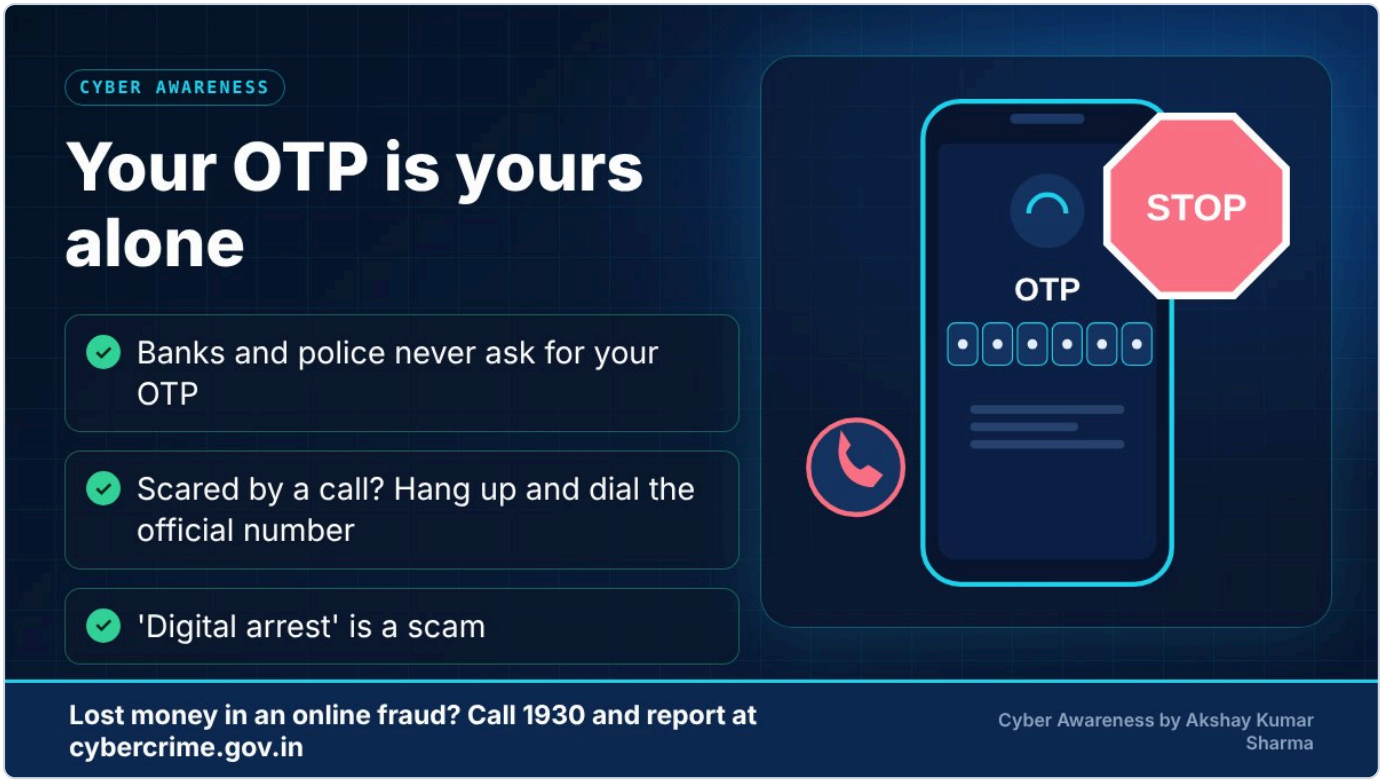
What it is

Social engineering means manipulating a person into giving up information or taking an action, using trust, fear, urgency or greed. An OTP (one-time password) exists to prove that you are the one approving something. If you read it out to a caller, you are approving what the attacker is doing. This includes 'digital arrest' calls, where scammers pose as police or investigation agencies on a call or video call. Authorities have clearly advised that genuine agencies do not arrest people over a video call or demand money to 'settle' a case.

How it works - and where you can stop it

Red boxes show what the attacker does. Green boxes show where you can break the chain.





Common warning signs

- ⚠ A caller claims to be from a bank, police, customs, courier or a government agency and asks for an OTP, PIN or money.
- ⚠ You are told not to disconnect, not to tell family, or to stay on a video call.
- ⚠ Threats such as arrest, account freezing or legal action unless you pay or 'verify' immediately.
- ⚠ A parcel or SIM 'linked to a crime' story that you cannot check independently.
- ⚠ Requests to move money to a 'safe account'.

Practical prevention tips

- Never share an OTP with anyone. A genuine organisation will not ask for it.
- Hang up. Then call the organisation yourself using its official number.
- Do not be rushed. Talk to a family member or friend before acting on any threat.
- Remember: no genuine agency arrests people over video calls or asks for money to close a case.
- Limit what you share publicly - scammers use personal details to sound convincing.

Risky habit vs safe habit

RISKY	SAFE
✕ Share the OTP to 'verify' your account	✓ Keep the OTP private. Only you type it, in the official app
✕ Stay on the line because you are scared	✓ Hang up and call the official number yourself
✕ Believe a 'digital arrest' video call	✓ Know that this is a scam. Call 1930 and report it
✕ Install an app sent on WhatsApp or SMS	✓ Install apps only from the official app store

What to do if it happens

1. Disconnect the call and stop all payments immediately.
2. Report suspected fraudulent calls or messages on Sanchar Saathi (Chakshu).
3. Call the cyber crime helpline 1930 immediately - reporting quickly gives the best chance of stopping the transfer.
4. Also file a complaint on the National Cyber Crime Reporting Portal (cybercrime.gov.in).
5. Inform your bank or payment app right away and ask them to block the card, account or UPI ID involved.
6. Keep screenshots, transaction IDs, phone numbers, UPI IDs and chat history. Do not delete anything.
7. Change passwords of affected accounts and do not share OTPs or PINs with anyone who calls you afterwards offering to 'recover' your money.

Official reporting resources

- Cyber crime helpline 1930 (for financial cyber fraud) - 1930
- National Cyber Crime Reporting Portal (cybercrime.gov.in) - https://cybercrime.gov.in/
- Sanchar Saathi - report suspected fraud calls/messages (Chakshu) - https://sancharsaathi.gov.in/
- Reserve Bank of India - public awareness - https://www.rbi.org.in/

Never share your banking password, OTP, UPI PIN, card CVV or full card number with anyone - not even someone claiming to be from your bank, police or a government office. This website will never ask for them.

This website is an educational resource. It is not an official government reporting portal or an emergency response service. If you are a victim of cyber fraud, report it through the official channels listed on each page.