MANTRA
FOR DIGITAL SAFETY

STOP. THINK.
THEN TAKE
ACTION.

Follow
@CyberDost for daily
cyber safety tips.

Report any Cybercrime at
www.cybercrime.gov.in
or
Call Helpline
Number
1930

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Indian
Cyber
Crime
Coordination
Centre
सहवीर्यं करवावहै • Working Together With Vigour

SPOT THE SCAM BEFORE THE SCAM SPOTS YOU

BE CYBER AWARE.
BE CYBER SAFE.

Issued in Public Interest by
the Indian Cyber Crime Coordination Centre (I4C)
Ministry of Home Affairs, Government of India

INVESTMENT SCAM

Scammers lure people online with promises of high returns in shares, crypto, or government schemes via social media ads or unknown WhatsApp/Telegram groups.

- **Beware of 'too good to be true' offers.**
- **Always verify sources on SEBI or official websites**
- **Never install apps shared through social media**

WHATSAPP SCAM

Scammers use handle of someone in your contact list to send an OTP "by mistake" and then ask you to forward it. Sharing it allows them to hijack your WhatsApp account.

- **Never share OTPs even with your known contacts without verifying through phone-call.**

DIGITAL ARREST

You receive calls claiming to be from banks, telecom companies, or police/CBI, saying your SIM or Aadhaar is linked to serious crimes. Fake officials then conduct audio/video interrogations and ask you to transfer money 'for verification'.

- **No government officer conducts inquiries over video calls. Report.**

REFUND SCAM

You receive fake calls or messages claiming you are due a refund. They ask to click a link or for OTP or bank details and drain your account.

- **Refunds never require OTP or PIN.**
- **Verify the offer before sharing any details.**

PART-TIME JOB SCAM

You are offered easy work-from-home jobs through social media groups or ads and asked to pay registration, training, or prepaid task fees. After payment, scammers disappear or ask to pay more.

- **Real jobs never ask for money or pre-paid tasks; Report them.**

CYBER SLAVERY

You are lured overseas with promises of high-paying jobs, only to be forced into cyber-fraud call centres, often held hostage or trafficked on tourist visas.

- **Always go abroad through authorized agents and with a valid visa only.**

SPOT THE SIGNS
BEFORE IT'S TOO LATE

SEXTORTION

Scammers record private photos or video calls and blackmail victims for money. It usually starts with casual online chats on social media or dating sites or unknown video calls.

- **Never share private images or information online.**
- **Do not pay — report without hesitation.**

DATING APP SCAM

Fake profiles gain your trust and then ask for money or personal details or sometimes prompt to invest, often leading to blackmail or investment scam.

- **Never send money or personal data to online contacts.**
- **Report inappropriate messages immediately.**

INSTANT LOAN SCAM

Fraudulent apps or websites offer quick loans at low interest. Later, they charge excessive interest and penalties and harass borrowers.

- **Download/ Use only RBI-approved loan apps.**
- **Never share PAN, OTP, or Aadhaar with unknown sources.**

MONEY TRANSFER FRAUD

Scammers claim they mistakenly sent money to your account and show fake SMS/ screenshots asking you to return it. In reality, no money was received.

- **Check the SMS header and your actual bank balance with your bank.**
- **Never send money based only on screenshots or phone calls.**

FAKE GAMING APPS

These apps look like real games but are designed to steal your data, show fake rewards, or scam money.

- **Download apps only from trusted app stores.**
- **Always check reviews and app permissions.**