

# COMMON ONLINE FRAUDS & SCAMS IN INDIA

– By: Mitra Foundation

**Legal Aid • Cyber Awareness • Scam-Free India**

Presented By:  
**SOMITRA JAIN**

Date  
**1/Nov/2025**



# OTP & UPI Fraud

- Fake messages or calls asking for OTP or UPI request approvals.
  - Victims unknowingly authorize transactions.
  - Tip: Never share OTP or click unknown payment links.

**Never Share  
your OTP**

**Don't click unknown  
links or site**

**unknown  
Transaction link**

# FAKE SHOPPING WEBSITES

- Fake e-commerce links with huge discounts.
  - Payment done, product never arrives.
- Tip: Shop only on verified platforms (Amazon, Flipkart, etc.).

**Beware of  
unknown sites**

**APK links or  
Websited**

**unknown merchant  
or seller**

# JOB / INTERNSHIP SCAM

- Offers of high salary or part-time jobs after paying registration fees.
  - Telegram/WhatsApp scams.
  - Tip: Real jobs never demand money upfront.

**TELEGRAM  
GROUPS**

**WHATS UP  
MESSAGES**

**DEMAND MONEY OR  
OFFER LETTER**

# LOAN APP FRAUD

- Fake apps offering instant loans.
- Collect contact data and blackmail users.
- Tip: Use only RBI-registered loan apps.

**QUICK LOAN**

**CHINESE APP**

**NOT REGULATED**

# GAMING & REWARD SCAM

- Free token or diamond pop-ups.
- Malware installation or data theft.
- Tip: Download games only from official stores.

PLAY STORE

APPLE STORE

OFFICIAL STORE

# SEXTORTION / ONLINE BLACKMAIL

- Fake friendship or video call traps victims.
  - Recordings used for extortion.
- Tip: Never share personal photos or videos.

Call starts from  
+92

TURN OFF YOUR  
CAMERA ON CALL

PRIVATE YOUR  
PROFILE

# INVESTMENT & CRYPTO SCAM

- "Double your money" or "Guaranteed 20% return" offers.
  - Telegram or YouTube fake groups.
  - Tip: Verify SEBI/RBI registration before investing.

TRADE ON RBI OR  
SEBI APPROVED

LIKE BINANCE OR  
INDIAN EXCHANGE

STABLE OR NON  
STABLE CRYPTO

# FAKE CUSTOMER CARE / HELPLINE FRAUD

- Fraudsters posing as support staff.
- Ask for OTP or screen share.
- Tip: Use official helpline from verified websites.

**NEVER SHARE  
YOUR SCREEN**

**ASK FOR EMPLOYEE  
ID OR DETAILS**

**TAKE YOUR TIME  
BEFORE MAKE UPI**

# DIGITAL ARREST SCAM

- Fake police or cyber officer call claiming illegal activity.
  - Demands payment to avoid arrest.
  - Tip: Law enforcement never asks for money online.

**DIGITALLY ARREST  
NEVER EXIST**

**DON'T PAY SINGLE  
AMOUNT TO THEM**

**CALL POLICE  
IMMEDIATELY**

# CUSTOM OFFICER / PARCEL SCAM

- Message claiming international parcel with gift or money.
  - Demands "custom duty" to release parcel.
  - Tip: Verify parcel through official courier tracking only.

**INTERNATIONAL  
PARCEL**

**CASH OR JWELLERY  
OR IPHONE**

**LEGAL ACTION**

# LUCKY DRAW / PROMOTION / CASHBACK SCAM

- "You won a car or cash prize" SMS.
  - Fake links steal data or money.
  - Tip: Never click on unverified links.

**LOTTERY MAIL  
INBOX**

**CASH BACK SCAM  
FREEZE ACCOUNT**

**NEVER RESPOND**

# KYC / BANK VERIFICATION FRAUD

- "Your account will be blocked" messages.
  - Fake links to collect bank details.
- Tip: Update KYC only through bank branches or official apps.

**CREDIT CARD  
LIMIT INCREASE**

**KYC UPDATES**

**DEBIT CARD  
BLOCKED**

# FAKE GOOGLE REVIEWS / PROMOTION SCAM

- "Earn ₹50 per review" or "Get money for likes."
  - After few tasks, asks for deposit.
- Tip: Google or YouTube never pay for reviews.

**PAID PACKAGE FOR  
MORE MONEY**

**FAKE REVIEW**

**TELEGRAM GROUP**

# WHATSAPP BUSINESS / TELEGRAM GROUP SCAMS

- Investment groups showing fake profits.
  - Victims invest and lose money.
  - Tip: Never invest via unverified groups.

**FAKE PROFILE**

**FAKE IMAGES OF  
SCREEN SHOTS**

**NOT VERIFIED  
GROUP**

# FAKE POLICE / RBI / INCOME TAX CALLS

- Threat calls claiming illegal transactions.
  - Demand bribe or penalty payment.
- Tip: Government officials never ask for payments online.

**Whats up call**

**Using other country  
code**

**Ask for online  
payment**

# ROMANCE / DATING / MATRIMONY SCAM

- Emotional manipulation for money or blackmail.
- Tip: Verify profiles and never send money to online connections.

**Fake profile**

**Honey Trap**

**Divorcee Soft Target**

# PROPERTY / RENT / OLX SCAM

- Fake buyers send QR code saying “advance payment.”
  - Scanning causes debit instead of credit.
  - Tip: Never scan unknown QR codes.

**Refurbished I  
phones**

**Alto or Hatchback  
Cars**

**Army Person**

# SIM SWAP / MOBILE NUMBER FRAUD

- Duplicate SIM issued to intercept OTPs.
  - Bank accounts drained.
- Tip: Contact telecom operator if network suddenly stops.

**SIM**

**Port**

**Offer or Data**

# FAKE TECH SUPPORT / REMOTE ACCESS SCAM

- Pop-up or call claiming “Your computer has a virus.”
- Installs remote apps (AnyDesk, etc.) to hack system.
- Tip: Never allow remote access to unknown sources.

**Anti Virus Scan**

**Data recover**

**Give permission**

# FAKE RAID / LEGAL THREAT SCAM

- Fraudsters posing as officers, threatening legal action.
  - Demands payment to “settle” case.
- Tip: Report such threats to police or cybercrime portal.

**Fake Order**

**Fake Document**

**Fake Warrant**



**- Stay Alert, Stay Scam-Free!**  
**- Visit: [cybercrime.gov.in](http://cybercrime.gov.in) | Helpline: 1930**

**- Mitra Foundation: Legal Aid • Cyber Awareness • Scam-Free India**