



# **100 Top Cyber Frauds in India**

**Sridhar Nallamothu**

## **1. UPI/QR Code Scam – "Scan to receive" trick**

### **How it works:**

Fraudster sends/places a QR saying 'scan to receive' or swaps a merchant QR; scanning actually initiates a debit from your UPI account.

### **Precaution:**

Never scan a QR to receive money; confirm receiver name in your UPI app and pay only if you initiated it.

## **2. Phishing Emails (Bank/UPI lookalikes)**

### **How it works:**

Emails mimic banks/UPI providers with cloned login pages; credentials/OTPs entered there are captured and used to drain accounts.

### **Precaution:**

Don't click email login links; type bank URL or use the official app; keep 2FA enabled.

### **3. Smishing (SMS Phishing)**

#### **How it works:**

Urgent 'KYC expired/SIM blocked' SMS pushes you to a fake site collecting card/UPI/OTP details.

#### **Precaution:**

Ignore SMS links; verify only inside your bank/telecom app.

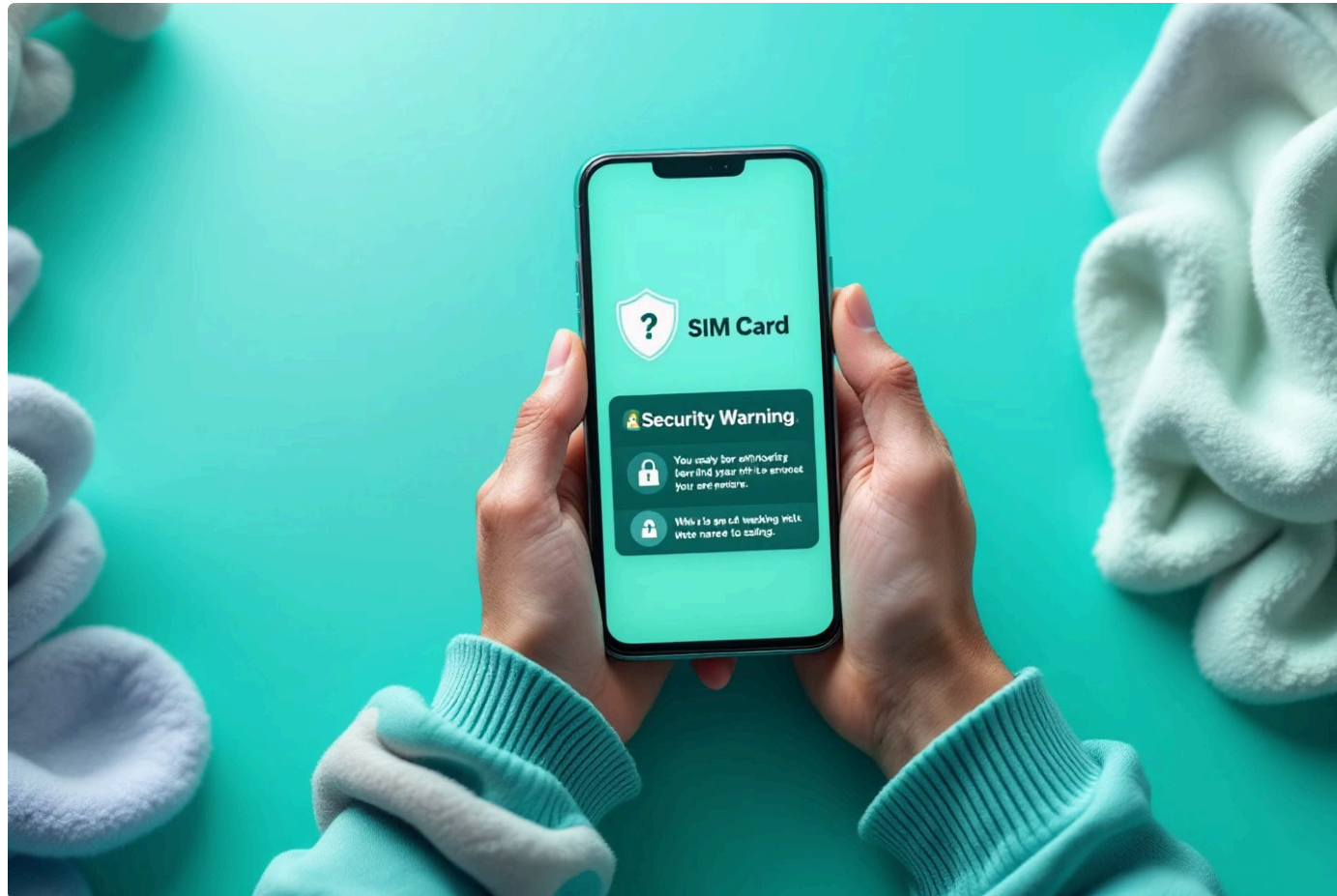
### **4. Vishing (Fake Calls)**

#### **How it works:**

Caller pretends to be bank/insurance staff and demands OTP/CVV 'to unblock/renew'; funds are siphoned.

#### **Precaution:**

Banks never ask OTP/CVV on calls; hang up and dial the official helpline.



## 5. SIM Swap / Number Takeover

### How it works:

Attacker gets a duplicate SIM via fake KYC so OTPs route to them and they access your bank/UPI.

### Precaution:

If your phone shows 'No Signal' without reason, call telco & bank immediately; add SIM change PIN if available.

## 6. Fake KYC Update (Aadhaar/PAN)

### How it works:

Fake forms/bots collect identity, bank, and OTPs under 'KYC update'; data is later abused for fraud/loans.

### Precaution:

Update KYC only via the bank's official app/website; never share OTPs in chats/links.

## **7. Digital Arrest / Fake Police-CBI Extortion**

### **How it works:**

Scammers on WhatsApp/video call threaten arrest for alleged crimes and demand 'penalty' via UPI.

### **Precaution:**

Law enforcement never collects fines on WhatsApp; report at the national cybercrime portal or local police.

## **8. AI Voice Cloning – Family/Boss Impersonation**

### **How it works:**

Attacker clones a known person's voice and urgently asks for money or OTPs.

### **Precaution:**

Verify separately via a known number or video call; never share OTPs.

## 11. Fake Cashback/Offer Pages

### How it works:

Popups mimic Amazon/Paytm and harvest card details for 'rewards/cashback'.

### Precaution:

Avoid popups; enter card details only in trusted, official apps.

## 12. Fake Loan Apps (Data Theft & Blackmail)

### How it works:

'Instant loan' apps grab contacts/gallery, then shame/blackmail on delay.

### Precaution:

Borrow only from RBI-regulated lenders; deny sensitive permissions.

1

## 13. Fake EMI/Insurance Renewal Calls

### How it works:

Scammer sends a payment link for 'due premium/EMI'; money goes to their wallet.

### Precaution:

Pay renewals only inside official insurer/bank portals.

2

## 14. ATM Card Skimming

### How it works:

Hidden skimmers/cameras at ATMs copy card and capture PINs.

### Precaution:

Inspect slot, cover keypad; prefer UPI/cardless withdrawals.





## 15. POS Machine Tampering

### How it works:

Modified POS devices capture card track data and PINs in stores.

### Precaution:

Use contactless/UPI; avoid swiping on suspicious devices.

## 16. Cheque/Auto-Debit Mandate Fraud

### How it works:

Fraudsters activate fake e-mandates or alter cheques to siphon money monthly.

### Precaution:

Review statements and auto-debits; enable SMS/email alerts.



## 17. Fake RBI/Helpline Calls

### How it works:

Threats of freeze/fine coerce transfers or credential sharing.

### Precaution:

RBI/banks never demand payments on calls; disconnect and verify via official numbers.

## 18. Fake Shopping Sites

### How it works:

Cloned e-commerce sites take prepaid orders; goods never arrive.

### Precaution:

Check URL/SSL/company info; buy from verified marketplaces only.

## **19. Refund/Replacement via Remote Apps**

### **How it works:**

'Support' asks to install AnyDesk/QuickSupport and then drains banking apps.

### **Precaution:**

Never install remote apps for refunds; support won't need to see your screen.

## **20. OLX/Marketplace Buyer Fraud**

### **How it works:**

Fake 'payment link' or UPI collect request lures you into entering PIN—money gets deducted.

### **Precaution:**

Never enter UPI PIN to "receive" money; check credit in your own app.



## 21. Courier/Parcel Customs Duty Scam

### How it works:

SMS claims parcel stuck; payment link steals card/UPI details and charges repeatedly.

### Precaution:

Pay only via official courier portals; ignore random payment links.

## 22. Fake Product Reviews & Ratings

### How it works:

Paid/fake 5-star floods mask poor/fake products.

### Precaution:

Read detailed verified reviews; don't trust stars alone.

## 23. Ponzi/MLM Schemes

### How it works:

Early returns are paid from new investors; later the scheme collapses.

### Precaution:

Beware 'guaranteed' or unusually high returns; verify regulator filings.

## 24. Crypto Investment Scam

### How it works:

Fake apps show rising profits; withdrawals blocked or frozen later.

### Precaution:

Use registered exchanges; test with small withdrawals first.

## **25. Pump-and-Dump Stock Tips**

### **How it works:**

Telegram/WhatsApp groups hype a stock; admins sell early, price crashes.

### **Precaution:**

Avoid 'sure shot' tips; invest via research on regulated brokers.

## **26. Pig-Butchering Romance-Investment Hybrid**

### **How it works:**

Long grooming builds trust; victim is guided to invest in a fake platform that later vanishes.

### **Precaution:**

Keep money separate from online relationships; avoid third-party platforms.



## **27. Fake Work-from-Home/Typing Jobs**

### **How it works:**

Victims pay 'registration/training' fees; jobs never exist.

### **Precaution:**

Legit jobs don't charge fees; verify company independently.



## **28. Lottery/Prize Scams**

### **How it works:**

'You won!' messages demand processing/customs fees; no prize follows.

### **Precaution:**

If you didn't enter, it's fake; never pay to claim prizes.

## 29. Fake Missed Call / One-Ring Scam

### How it works:

International missed calls bait you to call back and incur hefty charges.

### Precaution:

Don't return unknown international calls.

## 30. Premium SMS Subscriptions

### How it works:

Silent VAS gets activated; small weekly charges drain balance.

### Precaution:

Review carrier bill/plan; disable unknown subscriptions.



1

## 31. Fake Recharge/Cashback Links

### How it works:

Recharge/cashback links steal card/UPI info.

### Precaution:

Use official telecom apps or verified wallets only.

2

## 32. Caller ID Spoofing

### How it works:

Scammer makes calls appear from 'Bank/Police'.

### Precaution:

Don't trust display name; call back the official number yourself.



### 33. Mobile Tower Installation Scam

#### How it works:

'Rent your land' promises but demands deposits/registration fees.

#### Precaution:

Deal only via telecom operators' official channels; no fees to apply.

### 34. Fake Dating Apps (Extortion/Blackmail)

#### How it works:

Apps harvest chats/photos and later extort money.

#### Precaution:

Avoid unknown apps; never share private images; report promptly.

## 35. Loan Recovery Harassment Apps

### How it works:

Illegal lenders access contacts and shame borrowers to extort.

### Precaution:

Use regulated lenders only; deny contact/gallery permissions.

## 36. QR Sticker Replacement at Shops

### How it works:

Fraud QR pasted over genuine boards diverts payments.

### Precaution:

Merchants should audit QR codes; payers must verify receiver name.

### **37. Malicious Apps (Spyware in 'Free' Tools)**

#### **How it works:**

Free games/utilities steal SMS, contacts, photos.

#### **Precaution:**

Install only from official stores; review permissions carefully.

### **38. Permission Exploits (Flashlight asks mic/camera)**

#### **How it works:**

Over-privileged apps record audio/video or scrape data.

#### **Precaution:**

Grant only necessary permissions; uninstall suspicious apps.



### 39. Fake OTT Subscriptions (₹99/year)

#### How it works:

Phishing pages collect card data; no service provided.

#### Precaution:

Subscribe only via official OTT apps or stores.

### 40. Adware/Click-Fraud Apps

#### How it works:

Apps auto-click ads to earn for scammers, slowing phone and draining data.

#### Precaution:

Remove battery-draining unknown apps; use mobile security tools.

## 41. Remote Access Tool Apps (AnyDesk/TeamViewer misuse)

### How it works:

Under 'support/KYC' pretext, scammers control your phone and transfer money.

### Precaution:

Never allow remote control; banks don't need to see your screen.

## 42. Tech Support Pop-ups ('PC infected')

### How it works:

Fake alerts make you call 'support' that charges fees/installs malware.

### Precaution:

Close the tab; run antivirus from your own tools, not pop-up links.

## **43. Keyloggers & Malware**

### **How it works:**

Malware records keystrokes to steal passwords and IDs.

### **Precaution:**

Keep OS updated, use reputable antivirus, avoid pirated software.

## **44. Screen-Sharing/Remote Desktop Hijack**

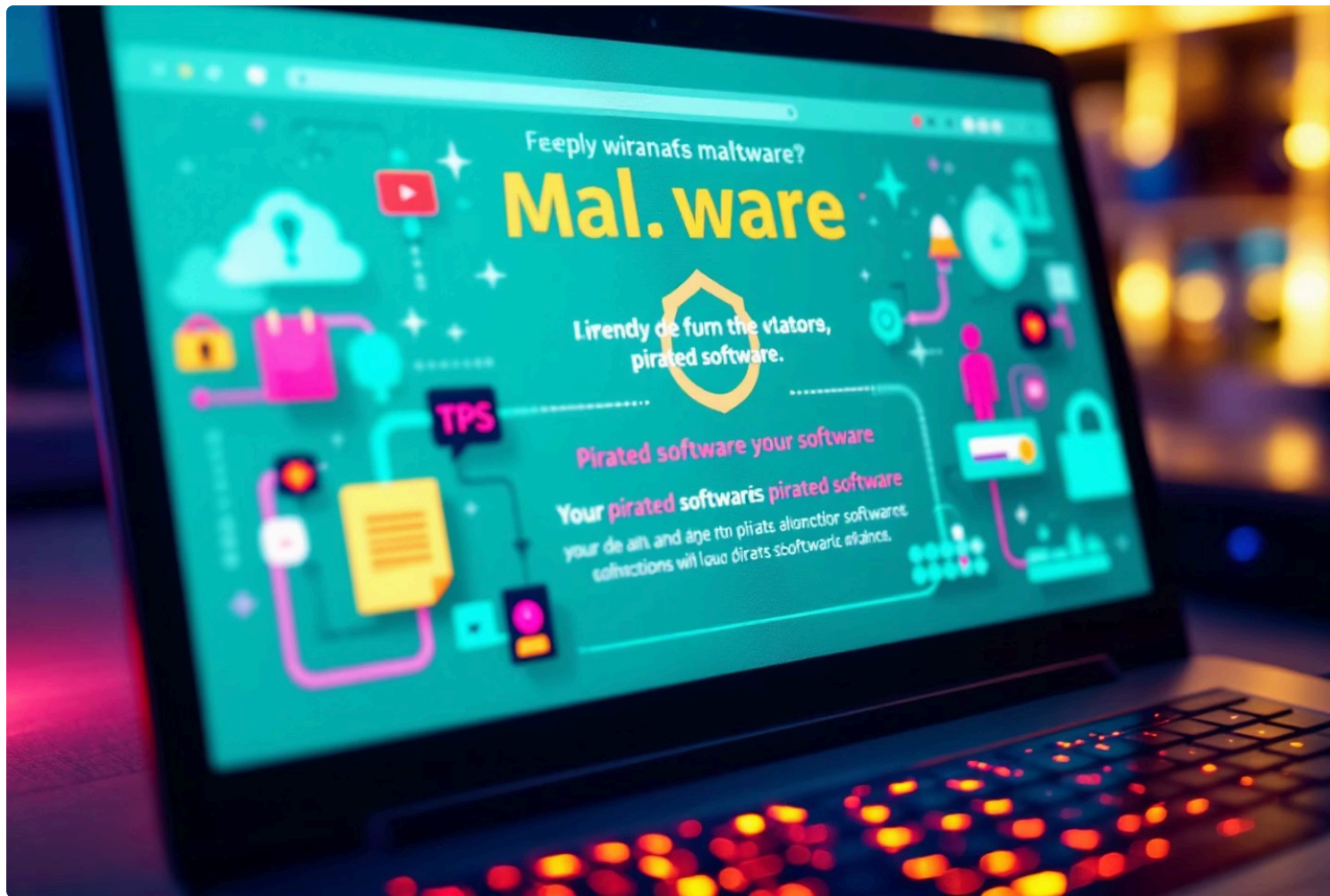
### **How it works:**

Fraudster watches credentials/OTPs during sharing and empties accounts.

### **Precaution:**

Never share screen while banking; cover sensitive info.





## 45. Pirated Software Trojans

### How it works:

Cracked apps carry hidden malware that steals data.

### Precaution:

Use licensed software only; avoid warez sites.



## 46. Fake Browser Updates / Malvertising

### How it works:

Popups/ads push spyware posing as updates.

### Precaution:

Update browsers only via in-app settings; block popups.

## 47. Browser Hijackers / Fake Search Ads

### How it works:

Extensions redirect searches to scam pages mimicking banks.

### Precaution:

Install extensions from trusted publishers; review extension rights.

## 48. Fake Antivirus Software

### How it works:

Pretend scans show fake threats and demand 'upgrade' payment.

### Precaution:

Use well-known security suites from official stores.

1

## 49. Crypto-Mining Malware

### How it works:

Hidden miners hijack CPU/GPU, slow your PC, waste power.

### Precaution:

Avoid shady downloads; run anti-malware scans regularly.

2

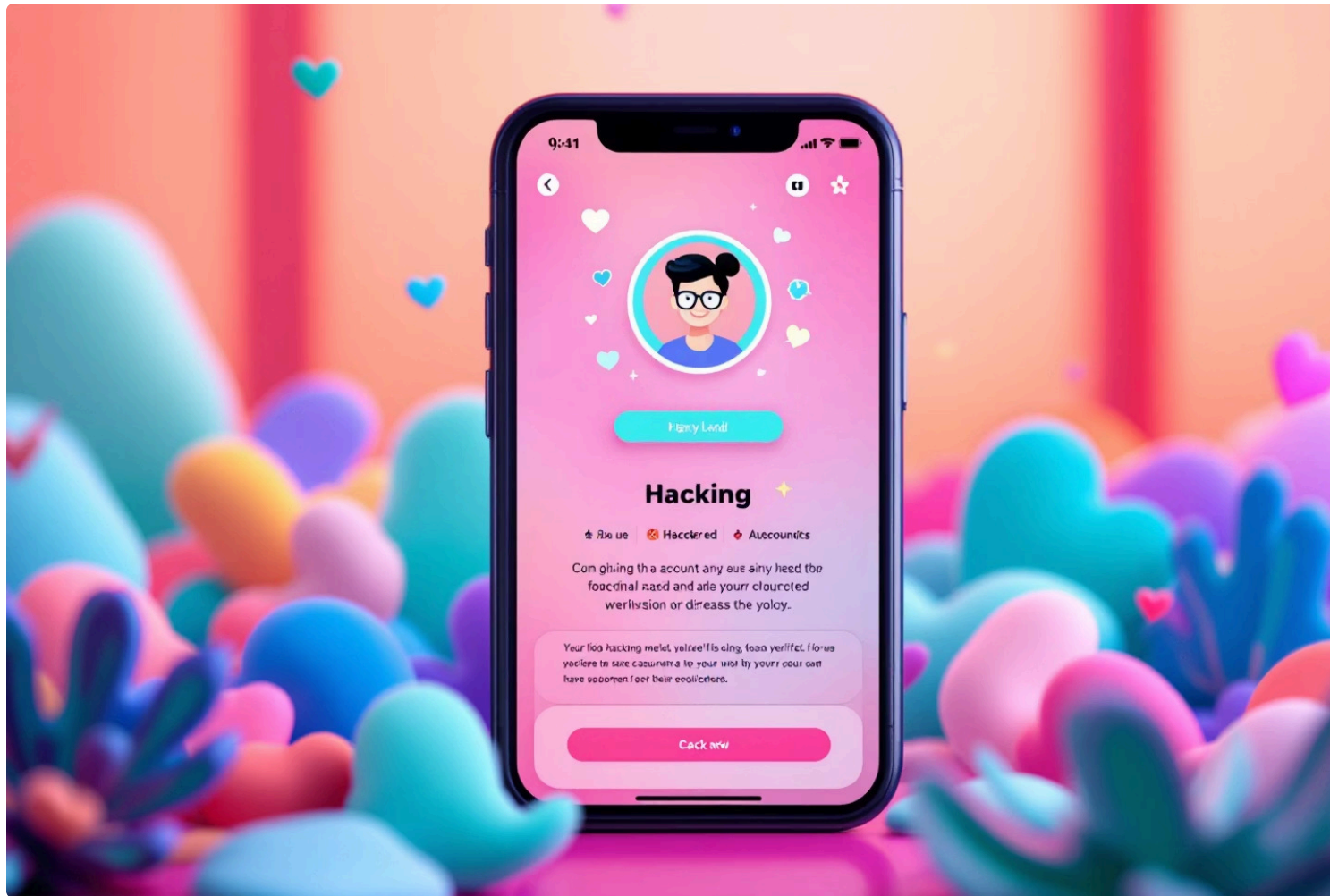
## 50. Ransomware

### How it works:

Malware encrypts files and demands crypto ransom.

### Precaution:

Maintain offline backups; don't open suspicious attachments/links.



## 51. Matrimonial/Romance Blackmail

### How it works:

Offenders gather private content and later extort money.

### Precaution:

Avoid sharing intimate material; report under cybercrime laws immediately.

## 52. Hacked Verified Accounts (Blue-tick)

### How it works:

Compromised celebrity pages push scams that followers trust.

### Precaution:

Verify offers on official websites; treat giveaways/links skeptically.

## 53. Influencer Giveaway Scams

### How it works:

Fake 'brand giveaways' ask delivery fee; no gift arrives.

### Precaution:

Genuine giveaways don't charge; verify brand accounts.

## 54. Quiz/Poll Data Harvesting

### How it works:

DOB/pet-name answers help reset passwords via security Qs.

### Precaution:

Don't share personal data in quizzes; use unique answers.

## **55. Deepfake Celebrity Endorsements**

### **How it works:**

AI videos push crypto/investment schemes.

### **Precaution:**

Verify on official celebrity/brand pages before acting.

## **56. Fake Charity/NGO Relief**

### **How it works:**

Disaster-time donation links collect money then vanish.

### **Precaution:**

Donate only to registered NGOs listed on official portals.





## 57. Fake Govt Subsidy Schemes

### How it works:

Phishing sites using govt logos steal Aadhaar/bank details.

### Precaution:

Use only government portals for schemes; avoid message links.

## 58. Celebrity Impersonation Ads

### How it works:

False endorsements lure buyers to fake e-commerce.

### Precaution:

Check brand collab announcements on official pages.



## 59. Fake Internship Offers

### How it works:

Students pay fees for non-existent internships.

### Precaution:

Verify on company career pages; never pay to apply.

## 60. Friend/Relative Impersonation (Lost Wallet)

### How it works:

WhatsApp/SMS from a cloned number asks urgent cash help.

### Precaution:

Call the real person on a known number to confirm.

## **61. Fake Delivery Agent Extra Charge**

### **How it works:**

Caller sends UPI collect request for '₹20 extra'; money deducted.

### **Precaution:**

Pay only within the delivery app; reject UPI requests.

## **62. WhatsApp/Telegram Investment Groups**

### **How it works:**

Pump groups coordinate buys; admins dump and exit.

### **Precaution:**

Avoid anonymous tip groups; invest via research.



### **63. Fake Social Media Ads (70% off brands)**

#### **How it works:**

Victims prepay; receive fakes or nothing.

#### **Precaution:**

Buy via verified brand stores/marketplaces with buyer protection.



### **64. Business Email Compromise (CEO Fraud)**

#### **How it works:**

Spoofed 'CEO/CFO' emails order urgent transfers to fake vendors.

#### **Precaution:**

Verify via callback or in-person before large transfers.

## 65. Insider Data Selling

### How it works:

Employees exfiltrate sensitive data and sell to criminals.

### Precaution:

Use access controls, monitoring, DLP, and audits.

## 66. Fake Vendor Invoices

### How it works:

Scammers send lookalike invoices; accounts team pays to wrong account.

### Precaution:

Match invoices to PO/vendor records; call vendor to confirm changes.

1

## **67. Industrial Espionage via USB/IoT**

### **How it works:**

Compromised devices spread malware and steal data inside networks.

### **Precaution:**

Block autorun, whitelist USB, segment networks, update IoT firmware.

2

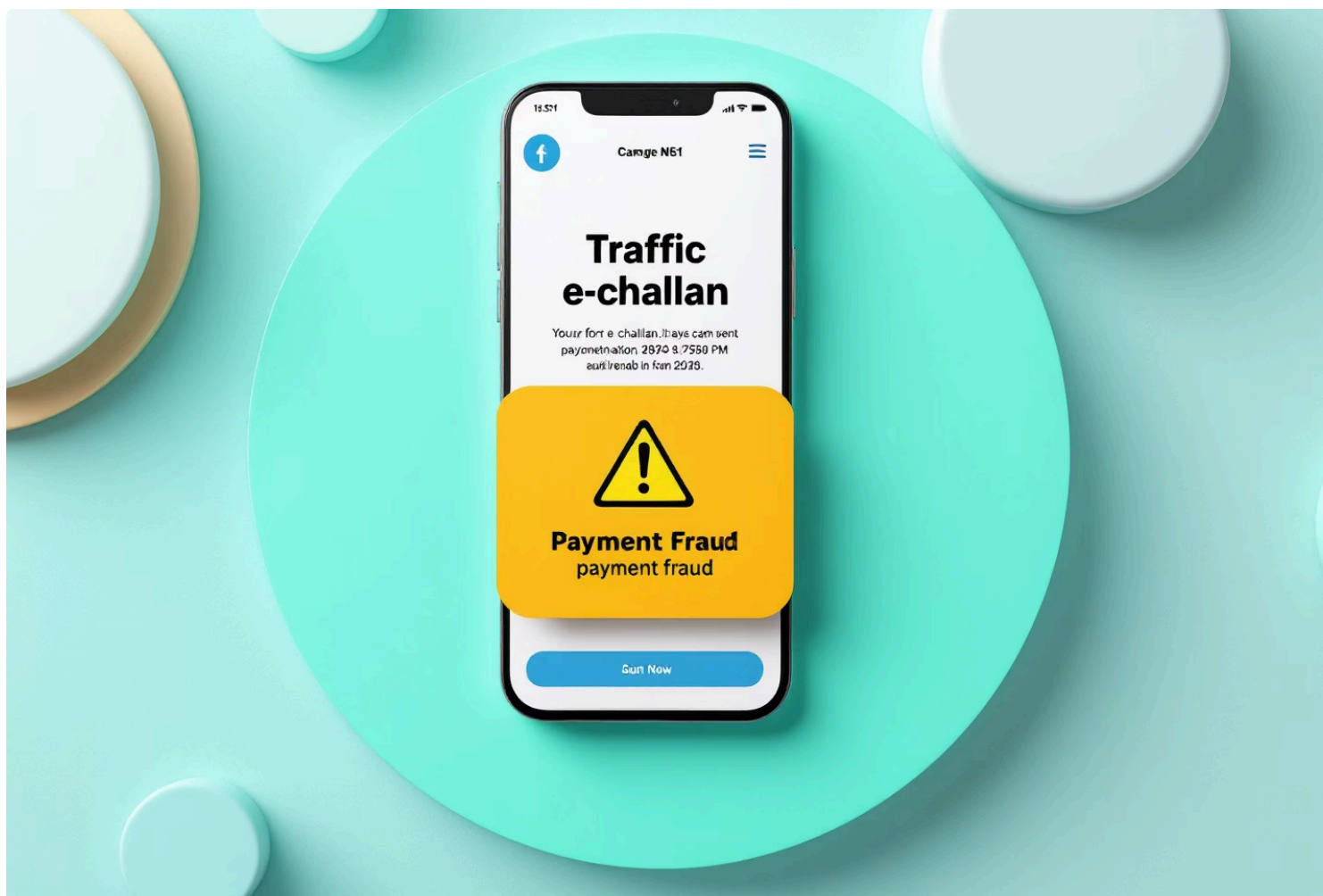
## **68. AI-Generated Voice/Executive Impersonation**

### **How it works:**

AI mimics senior voice ordering transfers or credentials.

### **Precaution:**

Confirm via second channel; never act on voice alone.



## 69. E-Challan / Traffic Violation App Scam

### How it works:

Fake challan links/apps steal banking/UPI info.

### Precaution:

Pay challans only on official transport portals/apps.

## 70. Recruit-and-Sell Bank Accounts (Mule Accounts)

### How it works:

People are paid to open/rent accounts used to launder fraud money.

### Precaution:

Never lend your account/UPI; liability may fall on you.

## 71. Dating/Matrimony App Financial Exploitation

### How it works:

Fake profiles (often AI-generated) solicit money/gifts/investments.

### Precaution:

Verify identity via video; never send money to online-only contacts.

## 72. Fake Electricity Bill Cut-off SMS

### How it works:

'Power cut tonight' links lead to malware/phishing pages.

### Precaution:

Pay only via DISCOM official site/app; ignore scare messages.



## **73. Fake Customer-Care Numbers in Search Ads**

### **How it works:**

Top 'helpline' ads list scam numbers that harvest OTPs or push remote apps.

### **Precaution:**

Get support numbers only inside official apps or verified pages.

## **74. Online Gaming Coin Top-Up Scam**

### **How it works:**

Discounted coin sites steal card details; game account later hijacked.

### **Precaution:**

Buy coins only in-app or via verified partners.



## 75. Fake Scholarship/Education Loan Forms

### How it works:

Students lured to forms asking Aadhaar/bank/card data for 'scholarships'.

### Precaution:

Check schemes on official government portals; avoid third-party forms.

## 76. Freelancer Project 'Security Deposit'

### How it works:

Clients ask for refundable deposits or software fees — then vanish.

### Precaution:

Never pay to get freelance work; verify client/company first.

## 77. Campus Placement / Recruitment Fee Fraud

### How it works:

Fake offers from big brands demand medical/uniform/processing fees.

### Precaution:

Confirm via official HR contact before paying anything.

## 78. Crypto Mining App Scam

### How it works:

Apps show daily returns until you try to withdraw — then freeze.

### Precaution:

Avoid ROI promises; verify registration and try small withdrawals first.

## **79. Insurance Renewal Discount Scam**

### **How it works:**

'Agent' offers renewal discounts via a link to personal wallet.

### **Precaution:**

Renew only on insurer's official portal or app.

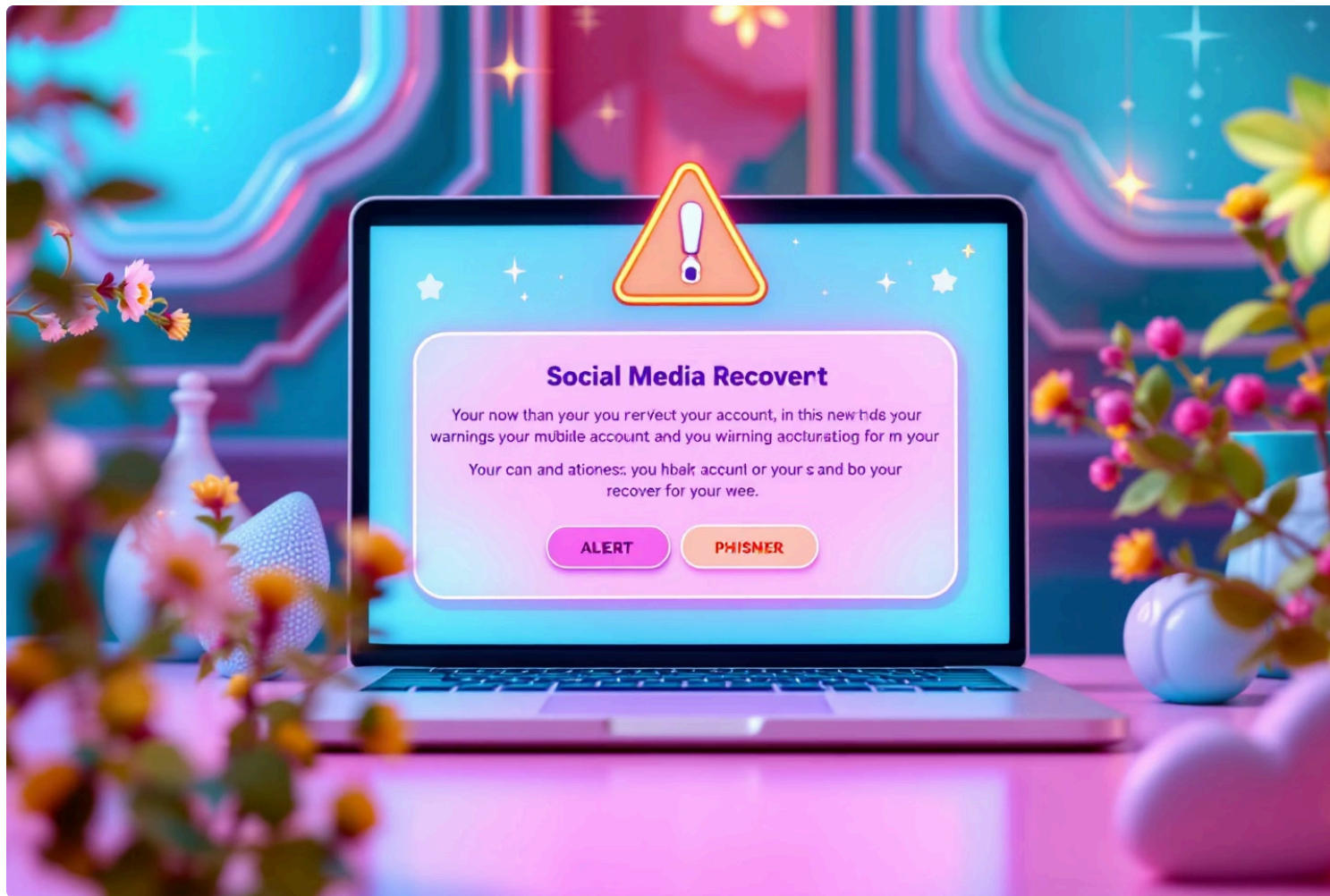
## **80. YouTube Monetization/Violation Phishing**

### **How it works:**

Fake mails claim violations or offer 'monetization boost' to steal Google logins.

### **Precaution:**

Manage YouTube via google.com only; enable 2-step verification.



## 81. Social-Media Account Recovery Phishing

### How it works:

'Policy violation' DMs steal page logs and MFA codes.

### Precaution:

Use Meta Business Suite; ignore non-official domain messages.



## 82. Fake Brand Collaboration (Women Influencers)

### How it works:

Impostor PRs send 'invoice/shipping apps' that steal logs/data.

### Precaution:

Confirm via brand domain emails; never install unknown APKs.

## 83. Instagram Boutique / Beauty Store Scams

### How it works:

Heavy-discount pages take payments; ship fakes or nothing.

### Precaution:

Order from verified accounts/marketplaces with return protection.

## 84. Fake NGO Donation for Disaster

### How it works:

Viral reels/UPI handles solicit donations to non-existent NGOs.

### Precaution:

Donate to registered NGOs only; verify registration numbers.

1

## **85. Mobile-Tower Lease Deposits**

### **How it works:**

Promises of monthly rent but demands 'registration' fees.

### **Precaution:**

Operators don't charge applicants; verify through official operator.

2

## **86. Fake Health Check/Medical Packages**

### **How it works:**

Prepaid 'health packages' with no hospital behind them.

### **Precaution:**

Confirm hospital tie-ups; pay at hospital counters/apps only.





## 87. Loan-App Harassment & Contact Doxxing

### How it works:

Illegal apps spam your contacts to shame you and extort.

### Precaution:

Stick to regulated lenders; report harassment to police/RBI.

## 88. Fake Credit-Card Reward Conversion

### How it works:

Caller 'converts points to cash' and asks for OTP; funds vanish.

### Precaution:

Redeem points only inside your bank's portal/app.

## 89. Subscription Renewal Phishing (Netflix/Prime/Spotify)

### How it works:

'Subscription expired' links mimic services and steal cards.

### Precaution:

Renew subscriptions inside official apps/stores only.

## 90. Fake Police/CBI Video-Call Backdrop

### How it works:

Scammers use office-style backdrops to coerce live 'verification' and payments.

### Precaution:

Police won't interrogate over WhatsApp; report and disconnect.

## **91. Deepfake Job Interview / Joining Kit Fraud**

### **How it works:**

AI 'HR' interviews you, then asks you to buy kits from a fake vendor.

### **Precaution:**

Validate recruiter domain and LinkedIn; never pay vendors suggested by recruiters.

## **92. AI Pornographic Morphing (Women-Targeted)**

### **How it works:**

Faces are morphed into explicit images and victims are extorted.

### **Precaution:**

Collect evidence and file on cybercrime portals; don't pay extortionists.



### 93. Voice-Triggered Payment Assistant Abuse

#### How it works:

Recorded/cloned voices trigger voice UPI assistants near unlocked phones.

#### Precaution:

Disable voice payments/NFC when unused; lock phone consistently.

### 94. Fake PAN-Update WhatsApp Bots

#### How it works:

Bots collect PAN/DOB/OTP claiming to 'update PAN'.

#### Precaution:

Use official tax portals only; never share OTPs in chats.

## 95. Fake AI Investment Bots / Auto-Traders

### How it works:

'AI bots' promise daily trading profits and siphon deposits.

### Precaution:

There's no guaranteed bot; verify registrations; avoid unknown apps.

## 96. Malicious PDF Invoice Links

### How it works:

Invoices contain links/macros that install spyware when opened.

### Precaution:

Scan attachments; don't enable macros; verify sender before opening.

## **97. QR Reprint at Shops/Temples**

### **How it works:**

Fraud QR overlays genuine ones to divert donations/payments.

### **Precaution:**

Verify receiver name; merchants should laminate and audit QRs.

## **98. Fake Cloud Storage Renewal**

### **How it works:**

'Drive full—renew now' prompts Google credentials theft.

### **Precaution:**

Check storage inside the official app; avoid pop-up links.





## 99. Wi-Fi Router Admin Hijack & DNS Poisoning

### How it works:

Default router passwords let attackers redirect banking pages.

### Precaution:

Change admin password; update firmware; use reliable DNS.



## 100. Fake Cyber-Safety Survey (Govt Logos)

### How it works:

Survey links harvest Aadhaar/PAN/bank details under 'awareness program'.

### Precaution:

Govt surveys don't ask financial data; use only .gov.in pages.