CYBER SMART INDIA

Complete Cybersecurity Awareness Masterclass

India Edition · Practical awareness for everyday digital life

Recognize scams · Protect accounts
Respond with confidence



AI Educator · Cybersecurity Awareness · Digital Safety

PRESENTED BY NIRMAL RABARI

01 · LEARN TO PAUSE

A scam succeeds when urgency beats verification

Today’s goal is practical: recognize the pattern, stop the transfer, verify independently, and report quickly.

01

STOP

Pause the call, click or payment.

02

THINK

What is the person asking me to do?

03

VERIFY

Use a separate, official channel.

04

ACT

Continue only when the request checks out.

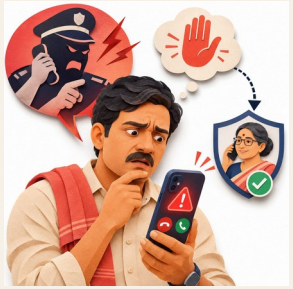
EMERGENCY ACTION

If money has moved: contact your bank using an official channel and call 1930 quickly. Preserve messages and transaction details.

02 · THE PRESSURE BEHIND SCAMS

Fear, greed and laziness are the scammer’s tools

A scammer often tries to influence your decision before trying to compromise your device.



DAR · FEAR

“Your account will be blocked.”
“Police case against you.”

Pause. End the call. Verify independently.



LALACH · GREED

“Guaranteed profit.”
“Pay a fee to unlock rewards.”

Question the promise. Verify the company.



AALAS · LAZINESS

“Click now.”
“Install this APK.”

Slow down. Check the source and permissions.

03 · READ THE SIGNAL, VERIFY THE REQUEST

SMS labels help classify messages; they do not prove authenticity

T = Transaction · G = Government · S = Service · P = Promotion

T TRANSACTION

Payment or account activity

G GOVERNMENT

Government communication

S SERVICE

A service you use

P PROMOTION

Offers and marketing

SAFE HABIT

A sender label can be spoofed. Do not use the message link or phone number to verify it. Open the official app or website yourself.

ATTACK 01 / 25

UPI Payment Fraud



HOW IT WORKS

A collect request can take money from you when you approve it and enter your UPI PIN. A PIN is never needed to receive money.

WARNING SIGNS

- Unexpected collect request framed as a refund
- Caller asks for UPI PIN, OTP or screen access
- Payment is confirmed by screenshot only

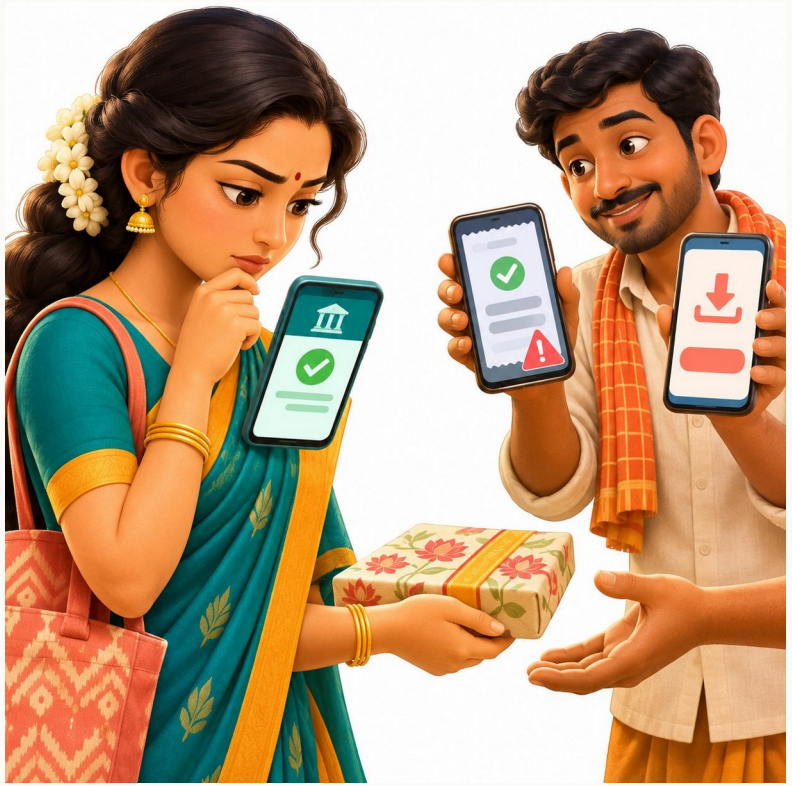
PROTECT YOURSELF

- Read the payee and amount before approving.
- Decline requests you did not initiate.
- Check the actual credit in your bank app.

STOP · THINK · VERIFY · ACT

ATTACK 02 / 25

Fake Payment Screenshot



HOW IT WORKS

A fabricated or edited receipt is used to make a seller release goods before money reaches the account.

WARNING SIGNS

- Buyer rushes you to hand over goods
- Receipt is shown instead of your bank ledger
- Payment account name or amount does not match

PROTECT YOURSELF

- Verify the credit in your own banking app.
- Wait for settlement before handing over goods.
- Never trust a screenshot as proof of payment.

STOP · THINK · VERIFY · ACT

ATTACK 03 / 25

QR Code Scam



HOW IT WORKS

A QR code may initiate a payment or open a fake page. Scanning a QR is not a way to receive money.

WARNING SIGNS

- Asked to scan a code to receive a refund
- UPI PIN requested after scanning
- QR sticker may cover the genuine one

PROTECT YOURSELF

- Use the official app and check the payee.
- Never enter a PIN to receive money.
- Confirm the amount before authorizing.

STOP · THINK · VERIFY · ACT

ATTACK 04 / 25

OTP Fraud



HOW IT WORKS

A one-time password can approve a login, reset or transaction. The scammer tries to make you share it.

WARNING SIGNS

- Unexpected OTP or login alert
- Caller claims to be bank or government support
- Pressure to read a code aloud

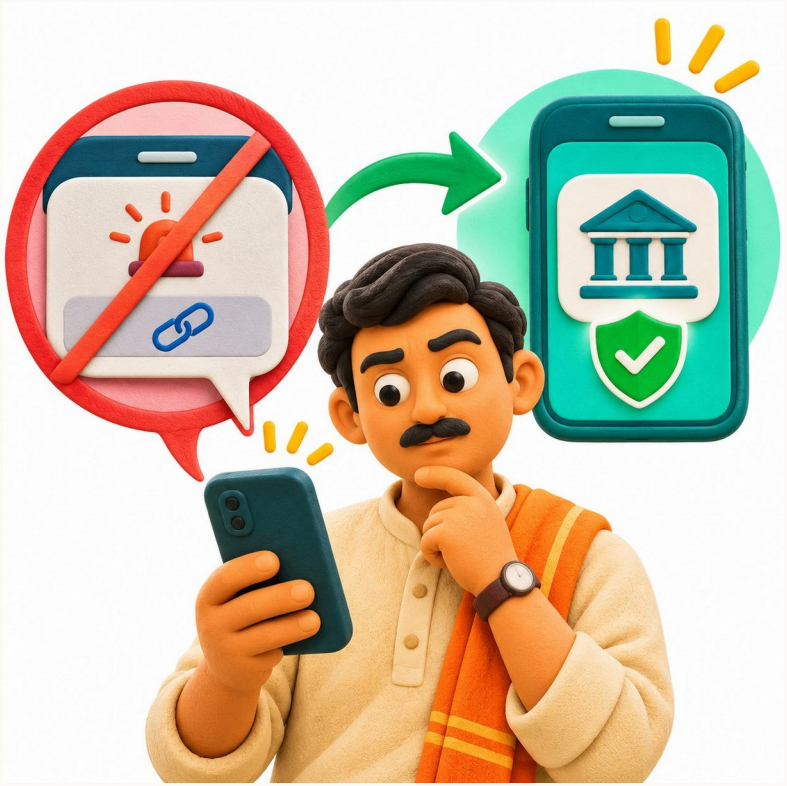
PROTECT YOURSELF

- Never share an OTP with anyone.
- Stop if a caller asks for a code or PIN.
- Contact the institution using its official app.

STOP · THINK · VERIFY · ACT

ATTACK 05 / 25

Fake KYC Update



HOW IT WORKS

A threat of account suspension pushes you to a fake KYC link, form or APK.

WARNING SIGNS

- Urgent “account blocked today” message
- Link shortener or unknown website
- Request for OTP, PIN or APK installation

PROTECT YOURSELF

- Open the bank app yourself or visit a branch.
- Do not update KYC through an unsolicited link.
- Never install an attached APK.

STOP · THINK · VERIFY · ACT

ATTACK 06 / 25

Digital Arrest Scam



HOW IT WORKS

A caller impersonates police or another agency, isolates the victim and demands money to avoid arrest.

WARNING SIGNS

- Continuous video call and secrecy
- Arrest threat or “verification” transfer
- Documents shown on an unsolicited call

PROTECT YOURSELF

- End the call and contact a trusted person.
- Do not transfer money to prove innocence.
- Verify through official police channels.

STOP · THINK · VERIFY · ACT

ATTACK 07 / 25

Investment and Trading Fraud



HOW IT WORKS

Fake experts and dashboards promise high returns, then demand more deposits or a fee to withdraw.

WARNING SIGNS

- Guaranteed daily profit
- Unverified trading group or app
- Tax or unlock fee demanded before withdrawal

PROTECT YOURSELF

- Verify registration through the regulator’s official site.
- Do not pay to unlock supposed profits.
- Avoid tips sent by unknown groups.

STOP · THINK · VERIFY · ACT

ATTACK 08 / 25

Job and Task Scam



HOW IT WORKS

A small task or payout builds trust before the scammer asks for a fee or larger deposit.

WARNING SIGNS

- Advance registration or training fee
- Unverified employer identity
- Pressure to invest to unlock earnings

PROTECT YOURSELF

- Verify the company using its own website.
- Never pay to receive wages.
- Stop when a task requires deposits.

STOP · THINK · VERIFY · ACT

ATTACK 09 / 25

Online Shopping Fraud



HOW IT WORKS

A fake store uses low prices, prepaid-only payment or a fake refund process to steal money or credentials.

WARNING SIGNS

- Unusually low price and urgency
- No verifiable seller contact details
- Payment goes to an unrelated account

PROTECT YOURSELF

- Check seller history and return terms.
- Use protected payment methods.
- Open the shop’s official app yourself.

STOP · THINK · VERIFY · ACT

ATTACK 10 / 25

Fake Customer Care



HOW IT WORKS

A fake support number, often found in search or social media, leads to requests for OTPs or remote access.

WARNING SIGNS

- Number appears only in a search result
- Agent asks for OTP or screen sharing
- “Refund” requires a payment or PIN

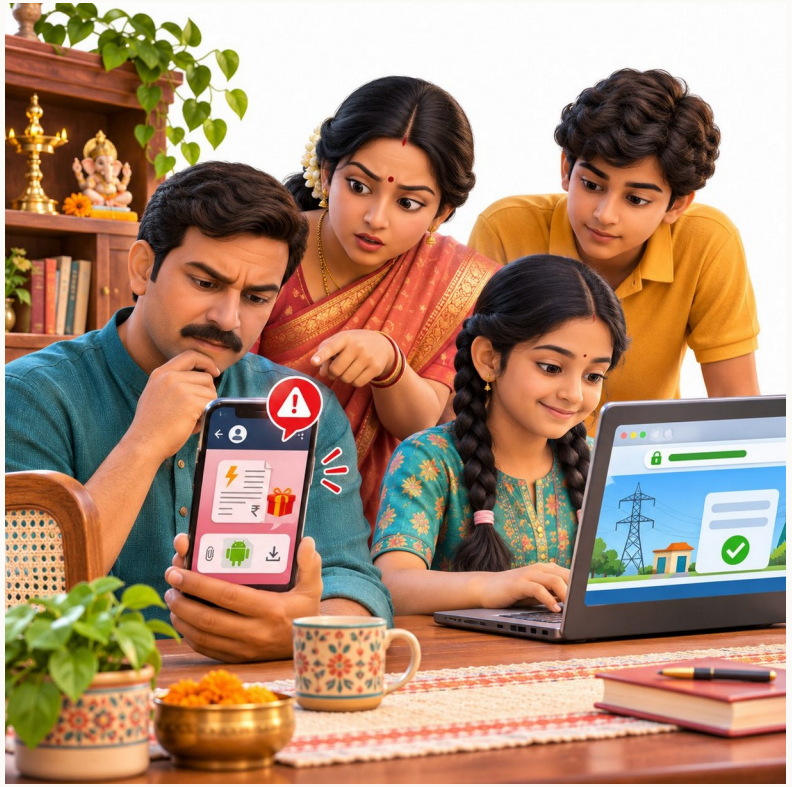
PROTECT YOURSELF

- Find support in the official app or website.
- Never install remote-access apps for support.
- Do not reveal credentials to a caller.

STOP · THINK · VERIFY · ACT

ATTACK 11 / 25

Electricity Bill and Scheme Scam



HOW IT WORKS

A disconnection threat or subsidy offer leads to a fake payment link or malicious app.

WARNING SIGNS

- Urgent disconnection SMS
- APK presented as a bill update
- Unsolicited request for bank details

PROTECT YOURSELF

- Check the bill in the provider’s official app.
- Do not install bill APKs.
- Verify benefits through government portals you open yourself.

STOP · THINK · VERIFY · ACT

ATTACK 12 / 25

Loan App Fraud



HOW IT WORKS

A fake or abusive loan app may hide fees and misuse contacts, photos or accessibility access.

WARNING SIGNS

- Lender identity or terms are unclear
- Excessive phone permissions
- Threats or harassment after applying

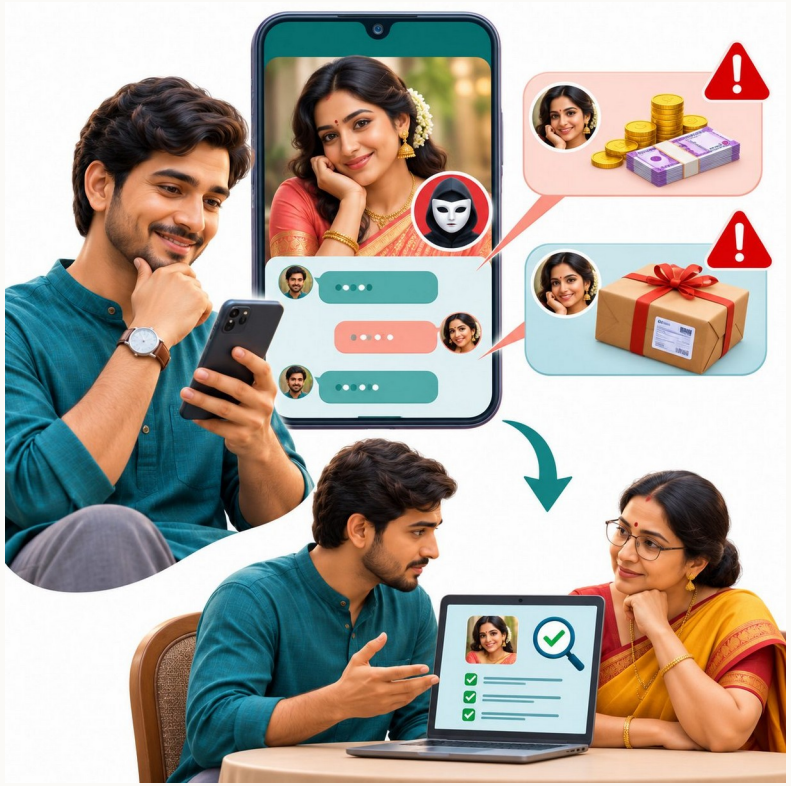
PROTECT YOURSELF

- Verify the regulated lender and agreement.
- Review permissions before installing.
- Keep evidence and report threats.

STOP · THINK · VERIFY · ACT

ATTACK 13 / 25

Romance and Matrimonial Fraud



HOW IT WORKS

A fake profile builds trust, then invents an emergency or asks for money, gifts or private documents.

WARNING SIGNS

- Fast intimacy and secrecy
- Repeated financial emergencies
- Avoids independent identity checks

PROTECT YOURSELF

- Verify identity through another channel.
- Do not send money or intimate material.
- Tell someone you trust before acting.

STOP · THINK · VERIFY · ACT

ATTACK 14 / 25

Sextortion and Blackmail



HOW IT WORKS

The scammer threatens to publish private images or recordings and demands money.

WARNING SIGNS

- Threat to expose private content
- Payment demand grows after first transfer
- Scammer insists you remain isolated

PROTECT YOURSELF

- Do not pay or negotiate further.
- Save evidence and report the account.
- Seek trusted support; do not blame the victim.

STOP · THINK · VERIFY · ACT

ATTACK 15 / 25

SIM Swap Fraud



HOW IT WORKS

A criminal takes control of a mobile number to intercept calls and messages and access accounts.

WARNING SIGNS

- Sudden loss of mobile service
- Unexpected password reset alerts
- Bank alerts arrive through another channel

PROTECT YOURSELF

- Contact your carrier from another phone.
- Secure email and banking accounts.
- Use app-based authentication where available.

STOP · THINK · VERIFY · ACT

ATTACK 16 / 25

Identity and Credential Theft



HOW IT WORKS

Personal documents, passwords or login codes are collected for account takeover or impersonation.

WARNING SIGNS

- Unexpected request for Aadhaar, PAN or OTP
- Fake verification page
- Document requested without a clear purpose

PROTECT YOURSELF

- Share only what is necessary.
- Use unique passwords and two-step verification.
- Watermark document copies with purpose and date.

STOP · THINK · VERIFY · ACT

ATTACK 17 / 25

Malicious APK Fraud



HOW IT WORKS

An APK sent through chat or SMS may steal data or give an attacker control of the phone.

WARNING SIGNS

- Fake bill, tax or KYC app file
- Requests for SMS or Accessibility access
- App comes from an unknown link

PROTECT YOURSELF

- Install apps only from trusted official stores.
- Do not allow unnecessary sensitive permissions.
- If installed, disconnect and secure accounts from a clean device.

STOP · THINK · VERIFY · ACT

ATTACK 18 / 25

Call Forwarding Scam



HOW IT WORKS

A caller tricks you into entering a code or number that redirects calls, including some account-verification calls.

WARNING SIGNS

- Stranger asks you to dial a code
- Delivery or network issue used as an excuse
- Calls or verification messages stop arriving

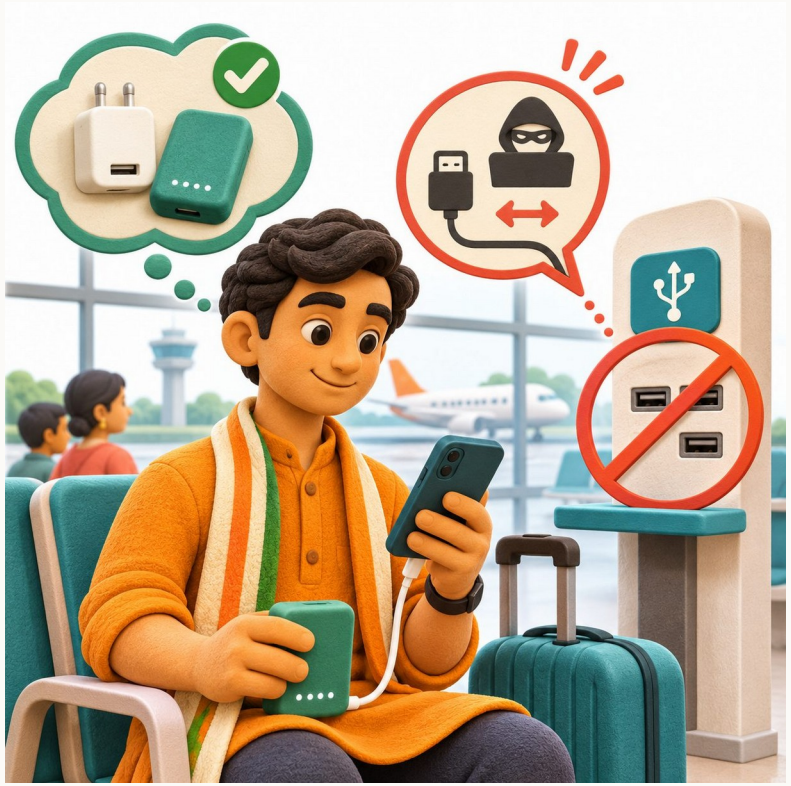
PROTECT YOURSELF

- Never dial a code given by an unsolicited caller.
- Review forwarding settings in phone settings.
- Contact your carrier through its official channel.

STOP · THINK · VERIFY · ACT

ATTACK 19 / 25

Public USB Charging Risk



HOW IT WORKS

A compromised charging port or cable may attempt data access. Risk is reduced by charging-only equipment.

WARNING SIGNS

- Public port prompts data access
- Unknown cable or adapter
- Phone requests trust or file transfer

PROTECT YOURSELF

- Use your own charger and a wall outlet.
- Choose charge-only mode if offered.
- Keep the phone locked while charging.

STOP · THINK · VERIFY · ACT

ATTACK 20 / 25

Gaming and Recharge Scam



HOW IT WORKS

Fake top-ups, free rewards or gaming currency links steal payment or login information.

WARNING SIGNS

- Free reward requires a login link
- Seller asks for OTP or game password
- Payment is outside the official store

PROTECT YOURSELF

- Buy only through the official game or store.
- Never share login codes.
- Report fake accounts and preserve receipts.

STOP · THINK · VERIFY · ACT

ATTACK 21 / 25

Credit and Debit Card Fraud



HOW IT WORKS

A fake bank or merchant call collects card details, CVV or OTP for unauthorized transactions.

WARNING SIGNS

- Caller asks for CVV, PIN or OTP
- Unexpected card-not-present alert
- Urgent “card verification” request

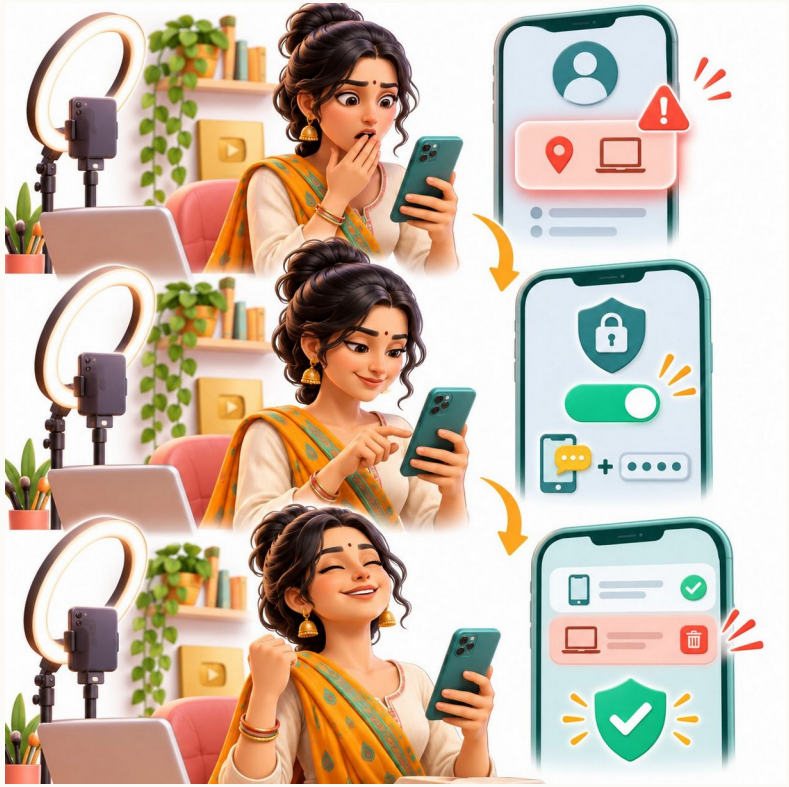
PROTECT YOURSELF

- Never share card PIN, CVV or OTP.
- Freeze or block a card through the official bank app.
- Report unauthorized transactions promptly.

STOP · THINK · VERIFY · ACT

ATTACK 22 / 25

Social Media Account Takeover



HOW IT WORKS

A fake login or collaboration offer steals a password or session and uses the account to scam contacts.

WARNING SIGNS

- Unexpected login link or brand offer
- Unknown device or password reset alert
- Friends receive unusual money requests

PROTECT YOURSELF

- Open the platform directly, not through the link.
- Enable two-step verification and review sessions.
- Warn contacts from a trusted channel.

STOP · THINK · VERIFY · ACT

ATTACK 23 / 25

Money Mule Fraud



HOW IT WORKS

A recruiter offers commission to receive and forward money through a personal bank account.

WARNING SIGNS

- Commission for moving money
- Asked to lend or rent an account
- Unfamiliar funds followed by pressure to forward

PROTECT YOURSELF

- Never receive or move money for strangers.
- Contact your bank if unexpected funds arrive.
- Preserve messages and report the approach.

STOP · THINK · VERIFY · ACT

ATTACK 24 / 25

Fake Courier and Customs Scam



HOW IT WORKS

A caller claims a parcel contains illegal goods and demands money while posing as police or customs.

WARNING SIGNS

- Parcel you never sent or ordered
- Threats, secrecy and video-call pressure
- Demand to transfer money to clear your name

PROTECT YOURSELF

- Do not transfer money or share documents.
- End the call and contact the courier independently.
- Tell family and report threats.

STOP · THINK · VERIFY · ACT

ATTACK 25 / 25

WhatsApp Account Takeover



HOW IT WORKS

A scammer tricks you into sharing a registration code or approving a device link, then impersonates you.

WARNING SIGNS

- Unexpected verification code
- Unknown linked device
- Friend asks for money from a new account

PROTECT YOURSELF

- Never share the six-digit registration code.
- Review linked devices and enable two-step verification.
- If locked out, use WhatsApp's official recovery process.

STOP · THINK · VERIFY · ACT

PRACTICAL LAB 1

Spot the fake website



USE THIS CHECKLIST

- Check the exact domain, not just the logo.
- Look for unexpected redirects, misspellings and pressure.
- Do not enter credentials from a message link.
- Open the official site yourself and compare.

TRAINER NOTE

Use a training screenshot. Never enter real passwords.

PRACTICAL LAB 2

APK safety check



USE THIS CHECKLIST

- Examples used in scams: lightbill.apk, gasbill.apk, channel/chnnale.apk, itr.apk and gsr-3b.apk.
- Filenames can change; the name does not prove what the app is.
- Avoid unsolicited APKs and unknown-source installs.
- Review SMS, Accessibility and notification access.

TRAINER NOTE

If installed: disconnect if remote control is suspected; secure accounts from a clean device.

PRACTICAL LAB 3

Call forwarding: inspect safely



USE THIS CHECKLIST

- A caller may use a delivery or network story to persuade you to dial a code.
- Never dial a code supplied by an unsolicited caller.
- Review forwarding settings in phone settings.
- Contact the carrier through its official app or website.

TRAINER NOTE

Carrier procedures vary. Do not rely on universal USSD codes.

PRACTICAL LAB 4

UPI AutoPay and PIN safety



USE THIS CHECKLIST

- Review merchant, amount or limit, frequency, validity and next debit.
- Pause or revoke mandates you no longer recognize.
- UPI PIN authorizes a payment; it is not needed to receive money.
- mPIN is generally used for bank-app access; details vary by bank.

TRAINER NOTE

Review mandates and transactions in your own trusted UPI app.

INCIDENT RESPONSE

The first five minutes after fraud



USE THIS CHECKLIST

- Stop following the caller’s instructions and make no further payments.
- Call your bank or payment provider using an official channel.
- Call 1930 quickly for financial cyber fraud.
- Report at cybercrime.gov.in and note the acknowledgement number.

TRAINER NOTE

Preserve transaction IDs, numbers, messages, screenshots and timestamps.

SECURE YOUR ACCOUNTS

Protect access after compromise



USE THIS CHECKLIST

- From a clean device, change compromised passwords.
- Revoke unknown sessions, linked devices and payment mandates.
- Review call forwarding and SIM status.
- Warn contacts if your account may be impersonated.

TRAINER NOTE

Do not delete evidence before saving it.

FAMILY AND WORK

Make verification a shared habit



USE THIS CHECKLIST

- Agree on a family verification phrase and callback process.
- Confirm payment or bank-detail changes on a second channel.
- Use unique passwords and two-step verification.
- Back up important files and test recovery.

TRAINER NOTE

Ask for help without blame; pressure and impersonation can fool anyone.

TRUSTED INDIA RESOURCES

Use official reporting and help channels



USE THIS CHECKLIST

- 1930 — financial cyber-fraud helpline.
- cybercrime.gov.in — National Cyber Crime Reporting Portal.
- Use official RBI, SEBI, CERT-In, TRAI and Sanchar Saathi websites for relevant guidance.
- Do not trust contact numbers supplied by an unsolicited caller.

TRAINER NOTE

Check current procedures on the official site before acting.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Andhra Pradesh

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake farmer-benefit and subsidy messages.
- Electricity-bill disconnection links.
- UPI collect-request and QR payment traps.
- Fake investment and trading groups.

EXAMPLE

A person receives a message claiming that a government subsidy is pending and must be claimed through a link.

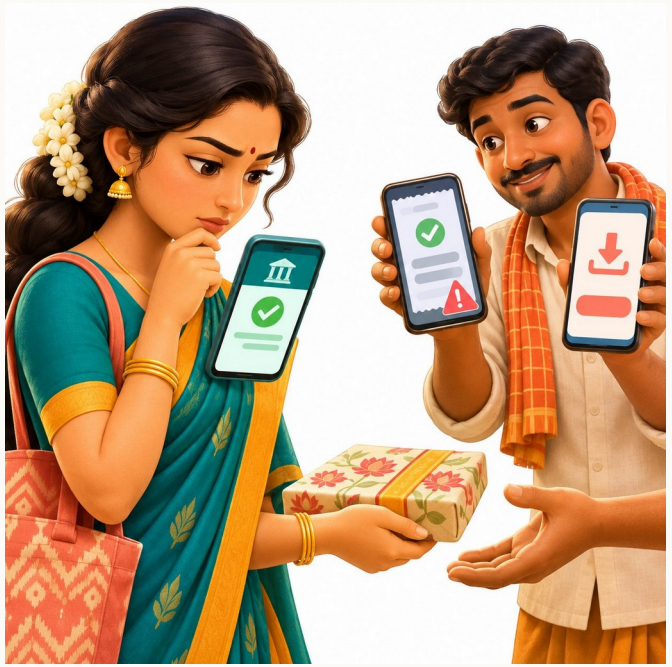
PROTECTION

Verify the scheme on the official government portal. Never install an application from an unsolicited message.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Arunachal Pradesh

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake government recruitment and scholarship notices.
- Social-media impersonation.
- Fraudulent travel and accommodation bookings.
- Fake online-shopping pages.

EXAMPLE

A fake recruiter requests a registration fee for a government job.

PROTECTION

Verify recruitment notices through the relevant official department or recruitment portal.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Assam

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake recruitment and work-from-home offers.
- Task and investment schemes promoted through messaging groups.
- Fake loan offers.
- Social-account takeover attempts.

EXAMPLE

A task group initially shows small earnings and later demands a large deposit.

PROTECTION

Do not pay money to unlock tasks or withdraw supposed earnings.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Bihar

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake pension and welfare-benefit messages.
- Scholarship and admission impersonation.
- Fake job and placement offers.
- UPI collect requests.
- Fake customer-care numbers.

EXAMPLE

A student receives a scholarship approval message requesting an application fee through a personal UPI ID.

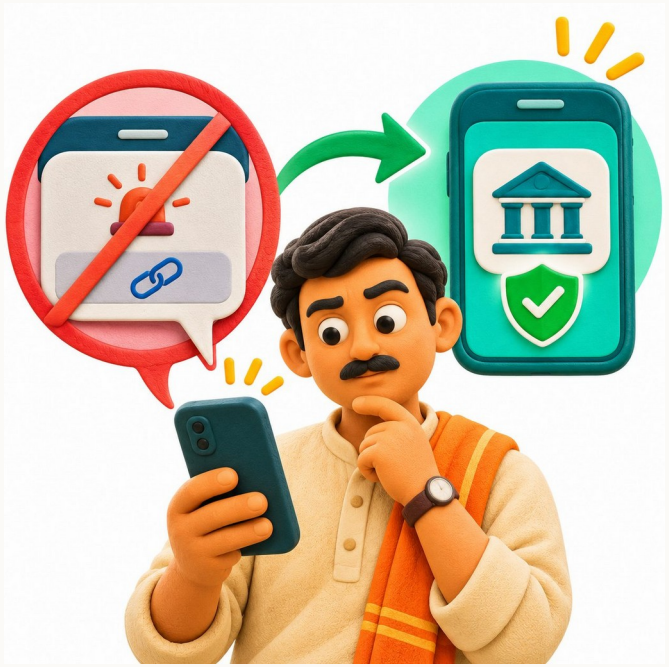
PROTECTION

Verify scholarship information through the official institution or government portal.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Chhattisgarh

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake government-scheme and farmer-support links.
- Loan-app permission abuse.
- QR-code payment deception.
- Social-media impersonation.

EXAMPLE

A person is asked to install an APK to receive a government benefit.

PROTECTION

Use official app stores and independently verify government services.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Goa

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake hotel and villa bookings.
- Fake holiday packages.
- Impersonated taxi and tour operators.
- Fake booking confirmations.

EXAMPLE

A traveller pays an advance to a fake accommodation account and discovers that the booking does not exist.

PROTECTION

Confirm bookings directly with the property through independently verified contact details.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Haryana

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake recruitment and overseas-job offers.
- Investment and trading groups.
- Fake e-Challan links.
- Property and rental listing fraud.
- Digital-arrest impersonation.

EXAMPLE

A person receives a message claiming an urgent traffic fine must be paid through an unfamiliar link.

PROTECTION

Check challans through official government services, not message links.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Himachal Pradesh

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake hotel and homestay bookings.
- Trekking and tour-package fraud.
- Recruitment impersonation.
- Online-shopping fraud.

EXAMPLE

A fake trekking operator requests advance payment for a package that does not exist.

PROTECTION

Independently verify the operator, accommodation and payment recipient.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Jharkhand

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake job and placement offers.
- Government-benefit impersonation.
- Money-mule recruitment.
- UPI transfer requests.

EXAMPLE

A person is offered commission for receiving money into a personal bank account and transferring it elsewhere.

PROTECTION

Never allow your bank account to be used for unknown third-party transactions.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Karnataka

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake technology jobs and internships.
- Fake training and placement offers.
- Business Email Compromise.
- Fake IT support.
- Investment impersonation.

EXAMPLE

An employee receives an email that appears to come from a company director, requesting an urgent vendor payment to a changed bank account.

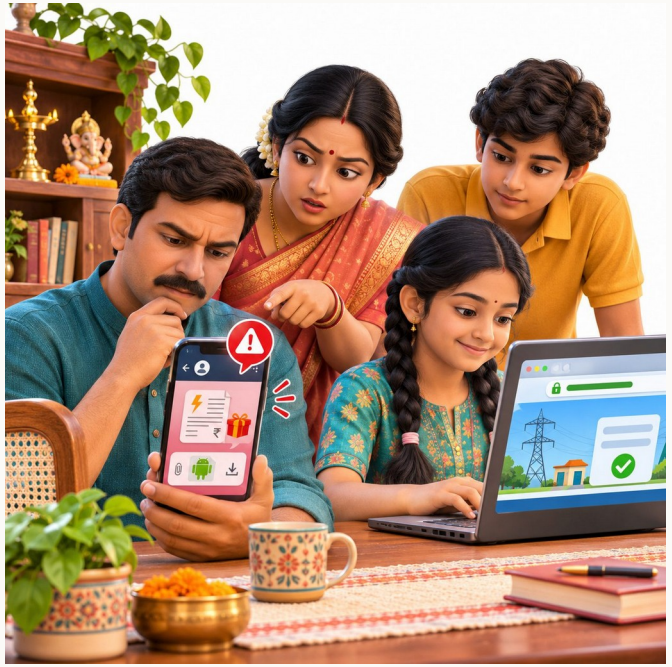
PROTECTION

Verify payment changes through a known, previously recorded phone number and require a second approval.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Kerala

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake bank and KYC messages.
- Digital-arrest impersonation.
- Courier and customs scams.
- Investment and matrimonial fraud.

EXAMPLE

A caller claims to represent a bank and threatens to block an account unless the recipient shares an OTP.

PROTECTION

Never disclose OTPs, passwords or UPI PINs to callers.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Madhya Pradesh

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake government schemes.
- Property and land-listing impersonation.
- Recruitment fraud.
- UPI and customer-care scams.

EXAMPLE

A fake property seller requests a token payment before allowing a site visit.

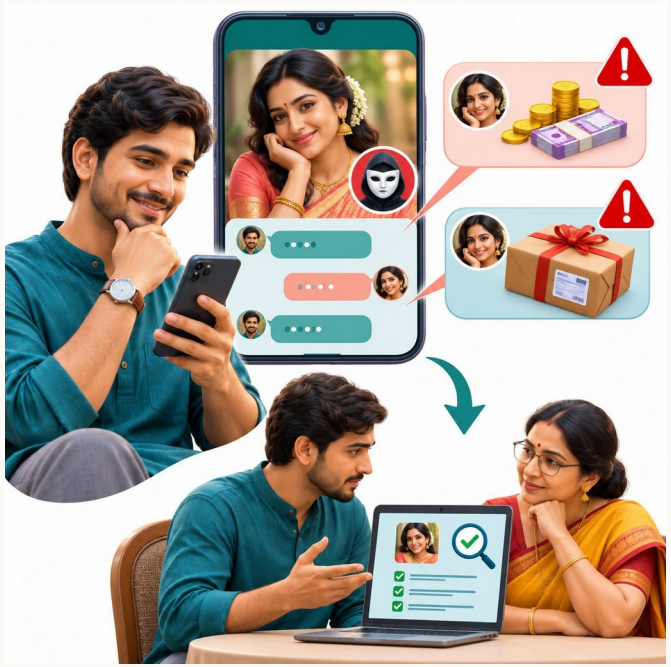
PROTECTION

Verify ownership, identity and property documentation through appropriate channels before transferring money.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Maharashtra

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Investment and trading impersonation.
- Digital-arrest scams.
- Business Email Compromise.
- Invoice and vendor-payment diversion.
- Property fraud.

EXAMPLE

A business receives a fake supplier email requesting payment to a different bank account.

PROTECTION

Verify bank-detail changes independently and use dual approval for payments.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Manipur

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake social profiles.
- Account impersonation.
- Recruitment and scholarship phishing.
- Online-shopping fraud.
- Fake payment screenshots.

EXAMPLE

An impersonator creates an account using another person's profile picture and asks their contacts for emergency money.

PROTECTION

Verify urgent requests using a separate communication channel.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Meghalaya

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake homestay and tourism bookings.
- Tour-package impersonation.
- Online-shopping fraud.
- Recruitment scams.
- Social-media impersonation.

EXAMPLE

A fake travel page offers an unusually cheap package and demands immediate payment.

PROTECTION

Verify the operator and booking details before paying.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Mizoram

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake employment offers.
- Scholarship impersonation.
- Social-account takeover.
- Online-shopping fraud.
- Phishing messages.

EXAMPLE

A fake scholarship page asks for personal documents and a processing fee.

PROTECTION

Verify the scholarship through the institution or official portal.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Nagaland

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake recruitment and education offers.
- Online-shopping scams.
- Social-media impersonation.
- Fake payment confirmations.
- Phishing messages.

EXAMPLE

A seller receives a screenshot showing payment, but no money appears in the bank account.

PROTECTION

Confirm actual credit in the official banking app before handing over goods.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Odisha

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake government-benefit messages.
- Electricity and utility links.
- Fake recruitment.
- UPI fraud.
- Online-shopping impersonation.

EXAMPLE

A message claims that an electricity connection will be disconnected unless an APK is installed.

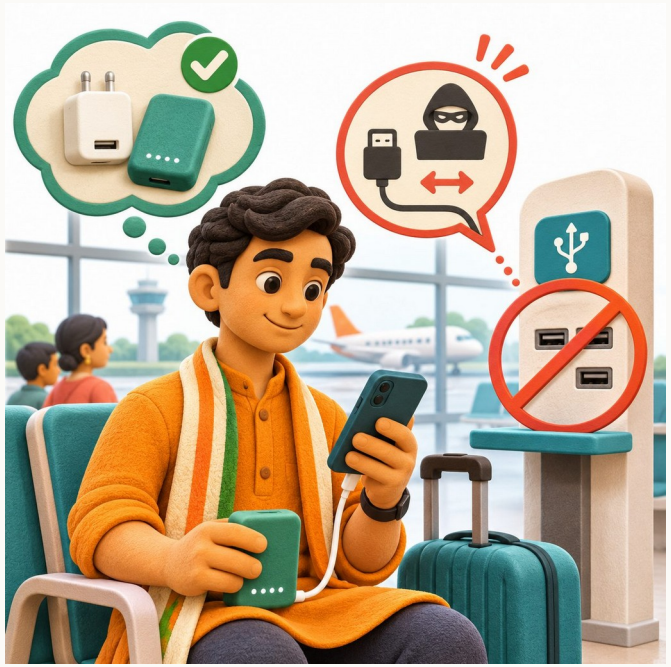
PROTECTION

Never install applications from unexpected utility messages.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Punjab

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake overseas employment and immigration services.
- Loan-app harassment.
- Investment impersonation.
- Social-media account fraud.
- OTP and UPI scams.

EXAMPLE

A fake overseas recruiter demands money for a guaranteed job or visa.

PROTECTION

Verify the agency, employer and applicable registration before paying.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Rajasthan

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Tourism and accommodation booking fraud.
- Property impersonation.
- Recruitment scams.
- Investment fraud.
- UPI payment deception.

EXAMPLE

A fake tour operator requests full advance payment through a personal account.

PROTECTION

Confirm the service provider and payment beneficiary independently.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Sikkim

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake hotel and trekking bookings.
- Travel-service impersonation.
- Online-shopping scams.
- Recruitment fraud.
- Social-account impersonation.

EXAMPLE

A fake trekking page offers a limited-time discount and requests an immediate deposit.

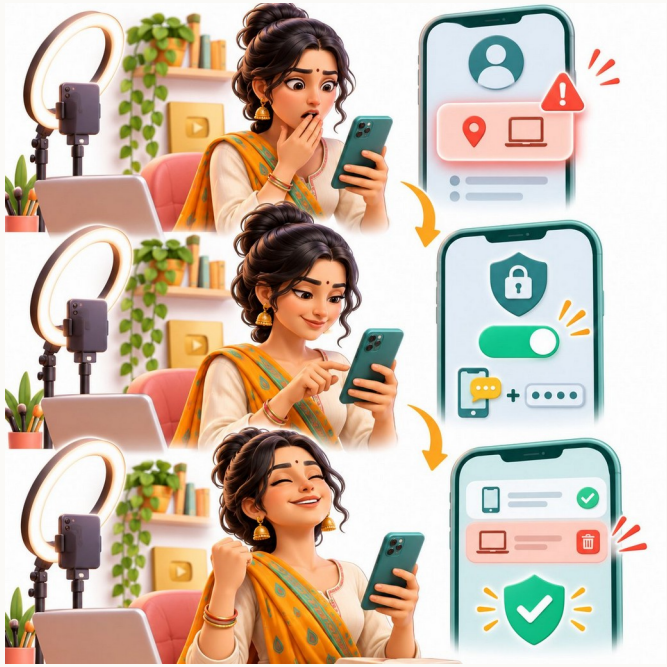
PROTECTION

Verify the operator, itinerary and accommodation before payment.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Tamil Nadu

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Investment and trading impersonation.
- Fake jobs and internships.
- Business Email Compromise.
- Loan-app misuse.
- Delivery and customer-care scams.

EXAMPLE

An employee receives a fake invoice from an impersonated supplier.

PROTECTION

Verify supplier bank details and invoice changes through a separate trusted channel.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Telangana

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Investment and trading impersonation.
- Technology recruitment scams.
- Digital-arrest calls.
- Fake IT support.
- Social-account takeover.

EXAMPLE

A fake investment expert shares screenshots of supposed profits and asks participants to deposit more money.

PROTECTION

Verify financial intermediaries independently and avoid guaranteed-return promises.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Tripura

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Scholarship and recruitment phishing.
- Online-shopping impersonation.
- Social-media account fraud.
- OTP scams.

EXAMPLE

A fake scholarship message asks the student to provide login credentials.

PROTECTION

Access the institution's official website independently.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Uttar Pradesh

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake government-service messages.
- Police impersonation and digital-arrest threats.
- Recruitment scams.
- UPI and QR fraud.
- Property and loan-app scams.

EXAMPLE

A caller claims that a family member is involved in a criminal case and demands money.

PROTECTION

Disconnect, verify independently and contact the relevant official authority.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Uttarakhand

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Pilgrimage and travel booking fraud.
- Fake hotel and homestay listings.
- Donation-link impersonation.
- Recruitment and shopping scams.

EXAMPLE

A fake accommodation provider requests advance payment for a pilgrimage stay.

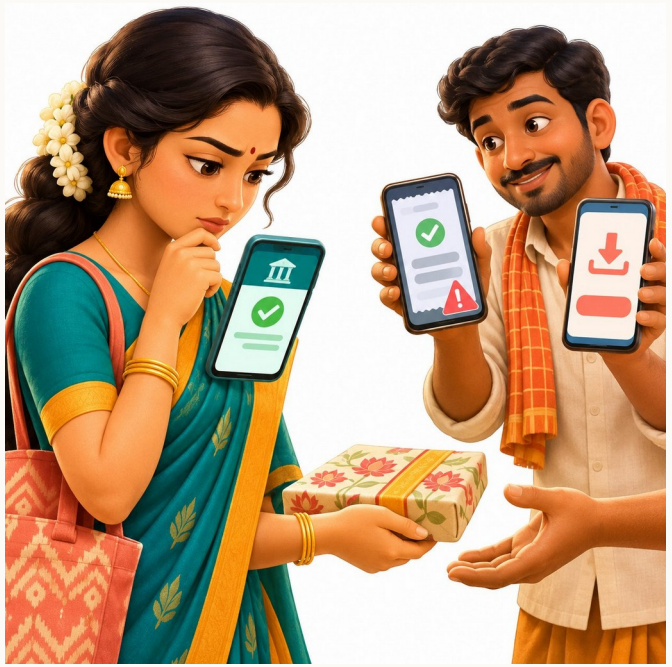
PROTECTION

Confirm the accommodation and payment recipient through independently verified details.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

West Bengal

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Investment and shopping impersonation.
- Fake job offers.
- Banking phishing.
- Social-account takeover.

EXAMPLE

A fake job offer requests payment for document verification.

PROTECTION

Verify the employer and never pay an unverified recruiter for a guaranteed job.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Andaman & Nicobar Islands

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake tourism and accommodation bookings.

EXAMPLE

An unsolicited message asks for money or personal details using a local service or benefit as a pretext.

PROTECTION

Use the official department, provider or recruitment portal. Do not install apps sent in unsolicited messages.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Chandigarh

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Government and police impersonation.

EXAMPLE

An unsolicited message asks for money or personal details using a local service or benefit as a pretext.

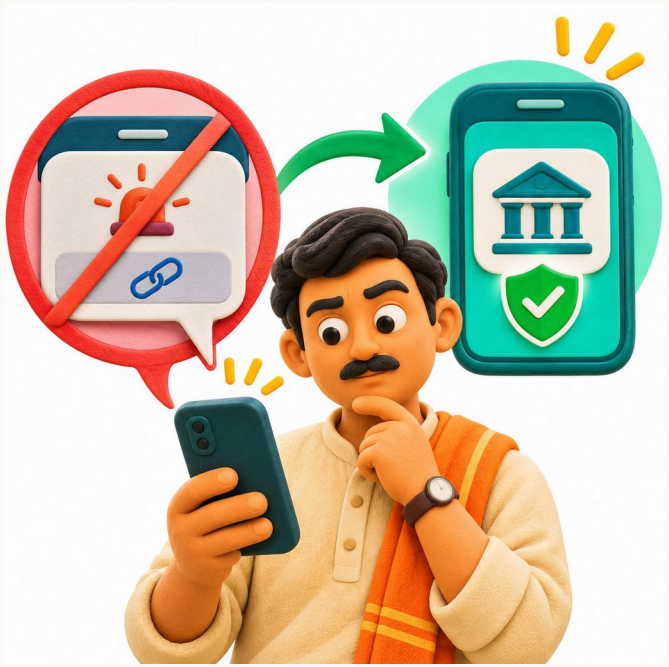
PROTECTION

Use the official department, provider or recruitment portal. Do not install apps sent in unsolicited messages.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Dadra & Nagar Haveli and Daman & Diu

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Business payment and QR deception.

EXAMPLE

An unsolicited message asks for money or personal details using a local service or benefit as a pretext.

PROTECTION

Use the official department, provider or recruitment portal. Do not install apps sent in unsolicited messages.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Delhi

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Digital-arrest and courier/customs impersonation.

EXAMPLE

An unsolicited message asks for money or personal details using a local service or benefit as a pretext.

PROTECTION

Use the official department, provider or recruitment portal. Do not install apps sent in unsolicited messages.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Jammu & Kashmir

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake recruitment and education notices.

EXAMPLE

An unsolicited message asks for money or personal details using a local service or benefit as a pretext.

PROTECTION

Use the official department, provider or recruitment portal. Do not install apps sent in unsolicited messages.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Ladakh

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Fake travel and accommodation services.

EXAMPLE

An unsolicited message asks for money or personal details using a local service or benefit as a pretext.

PROTECTION

Use the official department, provider or recruitment portal. Do not install apps sent in unsolicited messages.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Lakshadweep

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Tourism and accommodation booking impersonation.

EXAMPLE

An unsolicited message asks for money or personal details using a local service or benefit as a pretext.

PROTECTION

Use the official department, provider or recruitment portal. Do not install apps sent in unsolicited messages.

INDIA-WIDE AWARENESS · ILLUSTRATIVE, NOT RANKINGS

Puducherry

Use local examples to teach the same habit: verify the sender, website, payment recipient and organisation independently.



SCENARIOS TO DISCUSS

- Tourism and accommodation scams.

EXAMPLE

An unsolicited message asks for money or personal details using a local service or benefit as a pretext.

PROTECTION

Use the official department, provider or recruitment portal. Do not install apps sent in unsolicited messages.

NCRB · 2024

Cybercrime cases registered across India



INDIA SNAPSHOT

101,928 registered cybercrime cases · 101,118 in States · 810 in Union Territories · rate 7.3 per lakh population.

HOW TO EXPLAIN THIS DATA

Police-registered cases are not the same as financial-fraud complaints submitted through the National Cyber Crime Reporting Portal.

NCRB · SELECTED STATES

Reported cases need context



INDIA SNAPSHOT

Telangana 27,230 · Karnataka 21,993 · Uttar Pradesh 11,073 · Maharashtra 9,922 · Bihar 6,380 · Tamil Nadu 5,793 · Kerala 2,962 · Gujarat 1,592.

HOW TO EXPLAIN THIS DATA

Population, awareness, reporting behaviour, police registration and classification affect these numbers. Counts are not a ranking of prevalence for every fraud type.

MHA / PIB · 2021–2025

Financial cyber-fraud complaints rose sharply



INDIA SNAPSHOT

Complaints: 2.63 lakh (2021) · 6.94 lakh (2022) · 13.10 lakh (2023) · 19.19 lakh (2024) · 24.03 lakh (2025).

HOW TO EXPLAIN THIS DATA

Amounts reported: ₹551 cr · ₹2,290 cr · ₹7,465 cr · ₹22,848 cr · ₹22,495 cr. Report counts and reported amounts are different measures; amounts are not necessarily final verified losses.

MHA / PIB · AS OF 31 DEC 2025

Fast reporting can help stop fund movement



INDIA SNAPSHOT

More than ₹8,189 crore saved across more than 23.61 lakh complaints through the Citizen Financial Cyber Fraud Reporting and Management System.

HOW TO EXPLAIN THIS DATA

Early reporting lets authorities and financial institutions attempt to hold funds. It does not guarantee recovery in every case. Call 1930 promptly.

ADDITIONAL ATTACK 1 / 10

Fake Traffic Challan / e-Challan



HOW IT WORKS

A message claims an urgent fine is due and sends the user to a fake payment page.

WARNING SIGNS

- Unfamiliar link or short deadline
- APK attached as a challan
- Recipient or domain does not match official service

PROTECTION

- Check challans through the official government service you open yourself.
- Do not install an APK from a message.

ADDITIONAL ATTACK 2 / 10

Fake FASTag / Toll Payment



HOW IT WORKS

A fake low-balance or toll notice leads to a credential-stealing payment page.

WARNING SIGNS

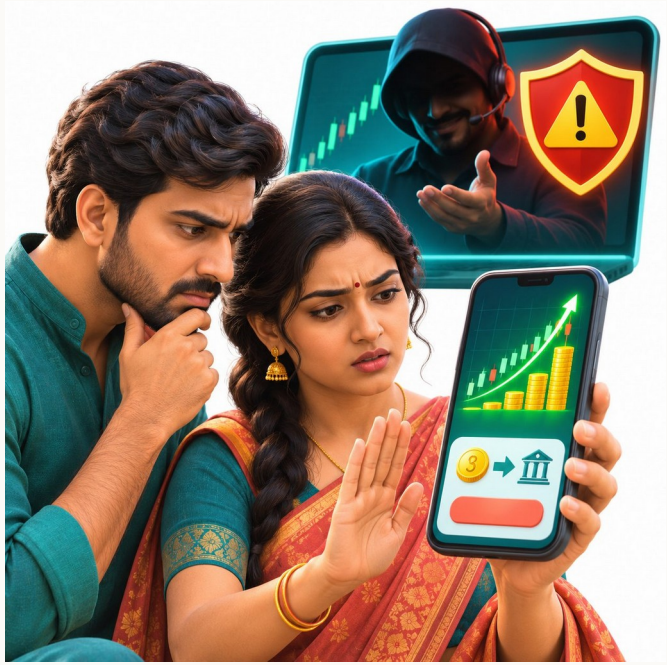
- Urgent recharge or account-block warning
- Link asks for card, OTP or UPI PIN
- Unknown payment recipient

PROTECTION

- Use the issuer’s official app/site.
- Never share OTPs or PINs with support callers.

ADDITIONAL ATTACK 3 / 10

Business Email Compromise



HOW IT WORKS

A criminal impersonates a supplier or executive and changes payment instructions.

WARNING SIGNS

- Unexpected bank-detail change
- Urgent secrecy or pressure
- Email domain differs slightly

PROTECTION

- Confirm changes on a known phone number.
- Use two-person approval for payments.

ADDITIONAL ATTACK 4 / 10

Fake QR Donation / Charity



HOW IT WORKS

A fake cause or altered QR code diverts donations to a scammer.

WARNING SIGNS

- Emotional urgency
- Personal UPI ID for an organisation
- QR name differs from the stated charity

PROTECTION

- Verify the organisation and recipient independently.
- Keep the payment receipt.

ADDITIONAL ATTACK 5 / 10

Fake Insurance / Financial Service



HOW IT WORKS

An impersonator promises policy benefits or refunds to collect fees and sensitive details.

WARNING SIGNS

- Unsolicited refund or bonus
- Processing fee requested
- OTP or policy credentials demanded

PROTECTION

- Call the insurer using policy documents or its official site.
- Do not pay a fee to receive a refund.

ADDITIONAL ATTACK 6 / 10

Digital Lending and Recovery Abuse



HOW IT WORKS

A deceptive app hides charges or uses personal data to threaten borrowers.

WARNING SIGNS

- Unclear lender or repayment terms
- Excessive contacts/photos permissions
- Threats to contact family

PROTECTION

- Check the regulated lender and loan agreement.
- Save abusive messages and report them.

ADDITIONAL ATTACK 7 / 10

Child Online Safety and Grooming



HOW IT WORKS

An adult builds private contact with a child and may ask for secrecy, images or meetings.

WARNING SIGNS

- Requests to move to private chat
- Gifts or threats tied to secrecy
- Requests for images or location

PROTECTION

- Keep communication open and non-judgmental.
- Report threats and seek trusted safeguarding help.

ADDITIONAL ATTACK 8 / 10

Fake Social-Media Customer Support



HOW IT WORKS

An impersonated support account replies to a public complaint and requests codes or remote access.

WARNING SIGNS

- Support account contacts you first
- Requests OTP or screen sharing
- Moves conversation to an unknown link

PROTECTION

- Use support inside the verified app/site.
- Never share authentication codes.

ADDITIONAL ATTACK 9 / 10

SIM, OTP and Account-Recovery Fraud



HOW IT WORKS

A fraudster exploits a lost number or fake recovery process to take over accounts.

WARNING SIGNS

- Unexpected recovery codes
- SIM suddenly loses service
- Caller asks to forward a code

PROTECTION

- Contact your carrier and bank through official channels.
- Secure recovery email and sessions.

ADDITIONAL ATTACK 10 / 10

Fake AI Apps and Browser Extensions



HOW IT WORKS

A fake AI tool may steal logins, files or business data.

WARNING SIGNS

- Unknown publisher or copied branding
- Broad permissions unrelated to function
- Requests confidential data upload

PROTECTION

- Install from trusted stores and verify the publisher.
- Do not upload sensitive data without approval.

PRACTICAL LAB 1 / 6

Lab 1 · Identify a fake website



TRY IT SAFELY

- Inspect the exact domain, not just the logo.
- Look for spelling differences, redirects and unusual payment requests.
- Never enter credentials from an unsolicited link.

REMEMBER

Open the official site independently and compare.

PRACTICAL LAB 2 / 6

Lab 2 · Smartphone security check



TRY IT SAFELY

- Review screen lock, system updates and app permissions.
- Remove apps you do not recognize.
- Keep device-finding and backup options current.

REMEMBER

Use a participant’s own device only with their consent.

PRACTICAL LAB 3 / 6

Lab 3 · WhatsApp security



TRY IT SAFELY

- Review linked devices.
- Turn on two-step verification.
- Check privacy and group-invitation settings.

REMEMBER

Never share a registration code.

PRACTICAL LAB 4 / 6

Lab 4 · Google account security



TRY IT SAFELY

- Review signed-in devices and recent activity.
- Use a unique password and a recovery method you control.
- Enable two-step verification.

REMEMBER

Use the official account security page opened directly.

PRACTICAL LAB 5 / 6

Lab 5 · UPI safety



TRY IT SAFELY

- Read payee, amount and request type before approving.
- Review AutoPay mandates and revoke unknown ones.
- Confirm receipt in the bank app, not a screenshot.

REMEMBER

Never enter a UPI PIN to receive money.

PRACTICAL LAB 6 / 6

Lab 6 · Verify official websites



TRY IT SAFELY

- Check the exact government or financial domain.
- Navigate from a trusted official portal.
- Do not trust search ads or forwarded URLs alone.

REMEMBER

Never enter real credentials in a classroom demo.

WHEN SOMETHING GOES WRONG

First five minutes after financial fraud



ACTION CHECKLIST

- Stop further payments.
- Call your bank or UPI provider through its official channel.
- Call 1930 promptly.
- Report at cybercrime.gov.in.

IMPORTANT

Write down transaction IDs and acknowledgement numbers.

WHEN SOMETHING GOES WRONG

First 30 minutes after account compromise



ACTION CHECKLIST

- Use a clean device to change compromised passwords.
- Revoke unknown sessions and linked devices.
- Tell your bank if payment access may be at risk.
- Warn contacts through a trusted channel.

IMPORTANT

Keep original evidence; do not edit messages or files.

WHEN SOMETHING GOES WRONG

First 24 hours after suspicious APK installation



ACTION CHECKLIST

- Disconnect from the internet if remote control is suspected.
- From a clean device, contact your bank and secure accounts.
- Revoke Accessibility, SMS and notification access; remove the app.
- Seek trusted technical support about safe reset options.

IMPORTANT

Do not sign into sensitive accounts on a potentially compromised phone.

WHEN SOMETHING GOES WRONG

Preserve evidence and understand recovery



ACTION CHECKLIST

- Keep numbers, SMS headers, emails, URLs, app names and timestamps.
- Save transaction references and bank complaint records.
- Report quickly; record each reference number.
- Follow bank, police and portal instructions.

IMPORTANT

A report does not guarantee recovery, but prompt action may help.

PRINT · REVIEW · DISCUSS

Family digital safety checklist

CHECKLIST

- Agree on a private verification phrase.
- Call back using a saved number.
- Review linked devices and mandates monthly.
- Ask for help without blame.



PRINT · REVIEW · DISCUSS

Student digital safety checklist

CHECKLIST

- Keep profiles private and location sharing limited.
- Tell a trusted adult about threats or blackmail.
- Do not share OTPs, passwords or intimate images.
- Report impersonation and suspicious links.



PRINT · REVIEW · DISCUSS

Small-business security checklist

CHECKLIST

- Confirm bank-detail changes on a second channel.
- Separate payment approval from payment release.
- Use unique accounts and MFA.
- Back up files and test recovery.



REPORT · VERIFY · GET HELP

Official Indian cyber safety resources

REPORT FINANCIAL CYBER FRAUD

1930 · cybercrime.gov.in · Contact your bank or UPI provider through its official app, website or card.

SAFETY NOTE

Never rely on a phone number or link provided by an unsolicited caller. Open the official website yourself.

OFFICIAL GUIDANCE

CERT-In · cert-in.org.in
Sanchar Saathi · sancharsaathi.gov.in
RBI · rbi.org.in
SEBI · sebi.gov.in
TRAI · trai.gov.in

PAUSE FOR DISCUSSION

What would you do next?

SCENARIO 1

A “bill APK” arrives with a same-day disconnection threat. What is the pressure tactic? Where will you verify the bill?

SCENARIO 2

A trading group shows profit screenshots and asks for a withdrawal fee. What evidence would you trust?

SCENARIO 3

A familiar voice asks for an urgent transfer and secrecy. What second channel will you use?

GROUP TASK

Name the trigger, the warning sign and one safe next step. Give each group 60 seconds.

TAKE THIS WITH YOU

25 golden cybersecurity rules

RULES 1–9

1. Pause before urgency.
2. Never share OTPs or PINs.
3. Use unique passwords and MFA.
4. Verify links and callers independently.
5. Install apps from trusted stores only.
6. Review app permissions.
7. Check UPI payee and amount.
8. Never scan a QR to receive money.
9. Verify payment in your own account.

RULES 10–18

10. Avoid unknown screen sharing.
11. Do not dial codes from unsolicited callers.
12. Use official support channels.
13. Check AutoPay mandates.
14. Keep devices updated.
15. Back up important data.
16. Protect identity documents.
17. Verify job and investment offers.
18. Do not pay to unlock profits.

RULES 19–25

19. Confirm family emergencies.
20. Teach children safe reporting.
21. Use privacy settings.
22. Report impersonation quickly.
23. Save evidence.
24. Call 1930 promptly after financial fraud.
25. Share safety habits without blame.

CYBER SMART INDIA

BE DIGITAL SMART

Be cyber safe, every day

Recognize the pressure. Protect your accounts. Report quickly.

REMEMBER

STOP · THINK · VERIFY · ACT



THANK YOU

Stay alert. Stay secure. Help others stay safe.

STOP · THINK · VERIFY · ACT

