A PRACTICAL FIELD GUIDE / GUJARAT

CYBER SMART GUJARAT

Recognize scams. Protect accounts. Respond quickly.



Participant Handbook

Presented by Nirmal Rabari

Use the pause as a tool

Scams work by rushing us, borrowing trust, or distracting us. This guide gives you a repeatable way to slow the moment down. You do not need technical expertise to use it.

1

STOP

Put the phone down. End the call if needed.

2

THINK

What are they asking me to do, and why now?

3

VERIFY

Use a known app, website or number you open yourself.

4

ACT

Proceed only when the request makes sense. Report and secure if it does not.

If money has moved, contact your bank and call 1930 quickly.

Gujarati reminder: “Roko, socho, jaancho, pachhi karo.” (Pause, think, verify, then act.)

Three pressure tactics

A scam can wear many costumes. Notice the feeling it creates: urgency, excitement or the promise of an easy shortcut.

FEAR

“Do this now or something bad will happen.”

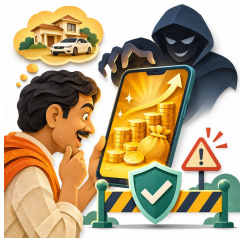
Account closure • police threat • power disconnection • illegal parcel



GREED

“A big reward is guaranteed if you act fast.”

Guaranteed profit • lottery • cashback • easy job • task payout



SHORTCUT

“Skip checking; one tap will fix it.”

Unchecked link • sideloaded app • search-result support number • code sharing • blind approval

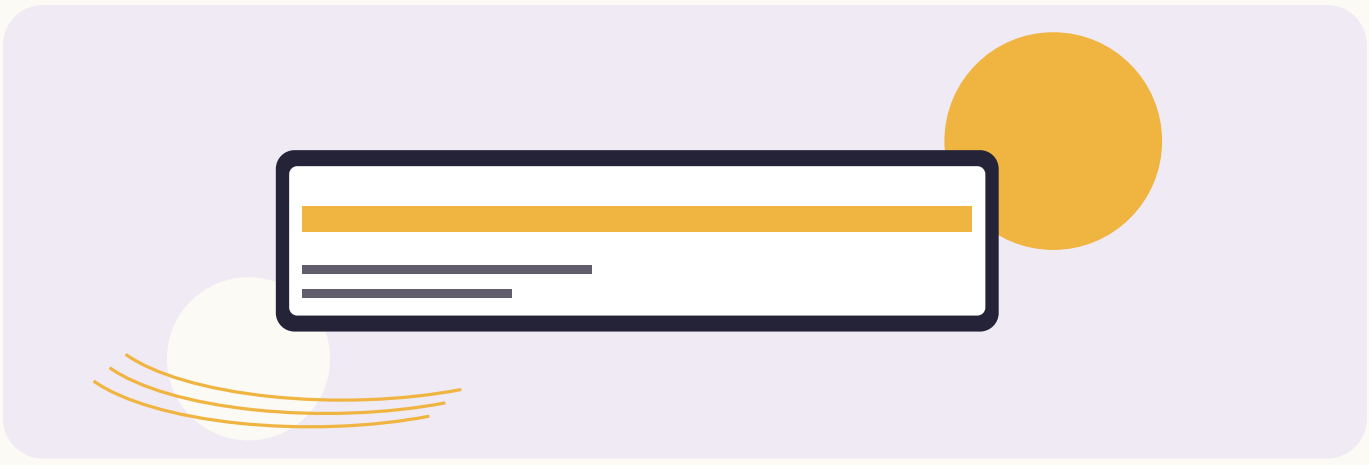


Memory aid: Fear ▫ pause. Greed ▫ think. Shortcut ▫ verify.

A quick self-check

Before you respond, ask yourself:

- [ ] Am I being told to keep this secret?
- [ ] Is there a deadline that prevents a call-back?
- [ ] Would I do this if the message came from a stranger?
- [ ] Can I verify the request using a channel I already trust?
- [ ] Am I being asked to send money, approve a request or reveal a code?



Practice saying: “I will verify independently and call you back.” A real person can wait.

Read the request, not the label

T / G / S / P labels can help sort messages: Transaction, Government, Service and Promotions. A category label or sender name alone does not prove that a message is genuine.

T	**Transaction**	Payment or account activity
G	**Government**	A public service or department
S	**Service**	A service update
P	**Promotions**	Offers and marketing

EXAMPLE ONLY • SUSPICIOUS MESSAGE

“URGENT: service will stop tonight. Install the attached update and share the verification code with our officer.”

- Threat + artificial deadline
- Unrequested app installation
- Request to share a code
- Verify in the official app opened independently

The 25 attack guides

Each guide names the goal, the usual sequence, warning signs and the next safe action. The examples are fictional and deliberately contain no real phone numbers or links.



HOW TO USE THIS INDEX

Start with the situation closest to yours. Page numbers lead to a focused guide; examples are fictional.

- Money and offers • 01-03, 07-12, 20-21, 23
- Threats and identity • 04-06, 13-16, 24
- Devices and accounts • 17-19, 22, 25

01 UPI payment and collect request 8
02 Fake payment screenshot 9
03 QR-code payment and refund scams 10
04 OTP, PIN and verification scams 11
05 Fake KYC and account-block threats 12
06 Digital arrest and fake police calls 13
07 Fake investment, trading and crypto 14
08 Fake jobs and task scams 15
09 Online shopping and fake seller 16
10 Fake customer-care numbers 17
11 Electricity, utility and scheme scams 18
12 Loan-app abuse and fake instant loans 19
13 Romance and matrimonial scams 20
14 Sextortion and intimate-image threats 21
15 SIM swap and number takeover 23
16 Identity-document and credential theft 24
17 Malicious APK and fake bill/KYC apps 25
18 Call-forwarding scams 26
19 Public USB charging and data connections 27
20 Gaming, recharge and in-game purchase scams 28
21 Card and fake bank-support scams 29
22 Social account takeover and fake collaborations 30
23 Money-mule recruitment and suspicious transfers 31
24 Fake courier, customs and illegal parcel 32
25 WhatsApp takeover and impersonation 33

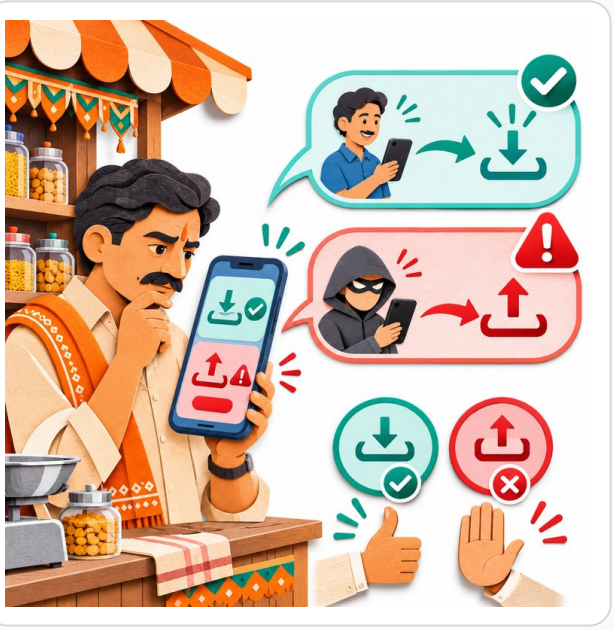
CHAPTER 01 / ATTACK GUIDES 01-14

People, Pressure & Payment

How a conversation, message or payment prompt can turn trust into a rushed decision.

INSIDE THIS CHAPTER

- 01-05 Payment requests, screenshots, QR codes and verification codes
- 06-12 Authority threats, fake offers, shopping, support and utility scams
- 13-14 Romance, matrimonial and intimate-image coercion



A SIMPLE METHOD

Stop. Name the request. Verify it through a channel you open yourself. Act only when the details make sense.

KEEP IN MIND

A caller's urgency does not make a payment request genuine.

01

UPI payment and collect request

CHAPTER 01 / PEOPLE, PRESSURE & PAYMENT

WHAT THE SCAMMER WANTS

Get the victim to authorize money leaving their account.

HOW IT USUALLY UNFOLDS

1. Scammer offers a refund or sale
2. sends a collect request
3. asks the victim to enter a PIN
4. money is debited.

PRESSURE BEING USED

Greed or helpfulness

EXAMPLE ONLY

Example: “Accept this request to receive your refund.”

WARNING SIGNS

- A PIN is requested to receive money
- unknown payer
- rushed collect request.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Open your UPI app yourself. Read whether the screen says pay or collect, check recipient and amount, and decline unexpected requests.

IF IT ALREADY HAPPENED

Tell your bank and payment app; call 1930 promptly. Save the UPI transaction ID and report the request.

TAKEAWAY

A UPI PIN authorizes payment; never enter it to receive money.

02

Fake payment screenshot

CHAPTER 01 / PEOPLE, PRESSURE & PAYMENT

WHAT THE SCAMMER WANTS

Make a seller release goods without receiving funds.

HOW IT USUALLY UNFOLDS

1. Buyer shows an edited screenshot
2. claims a delay
3. pressures the seller to hand over goods.

PRESSURE BEING USED

Urgency and social pressure

EXAMPLE ONLY

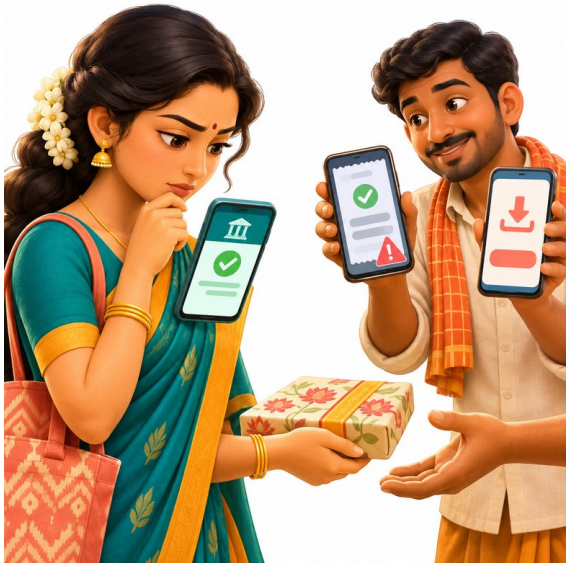
Example: “It is paid; see the screenshot. The bank will update later.”

WARNING SIGNS

- Screenshot instead of account entry
- unusual amount
- buyer hurries collection.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Check your own bank or merchant app, not a screenshot or SMS shown by another person. Wait for credited funds.

IF IT ALREADY HAPPENED

Do not hand over goods. If already released, contact platform, bank and local police; preserve chats and order details.

TAKEAWAY

Trust the balance in your own account, not a picture.

03

QR-code payment and refund scams

CHAPTER 01 / PEOPLE, PRESSURE & PAYMENT

WHAT THE SCAMMER WANTS

Collect money or capture credentials through a deceptive payment prompt.

HOW IT USUALLY UNFOLDS

1. Scammer says scan to receive refund
2. QR opens payment flow
3. victim enters PIN or approves.

PRESSURE BEING USED

Greed and helpfulness

EXAMPLE ONLY

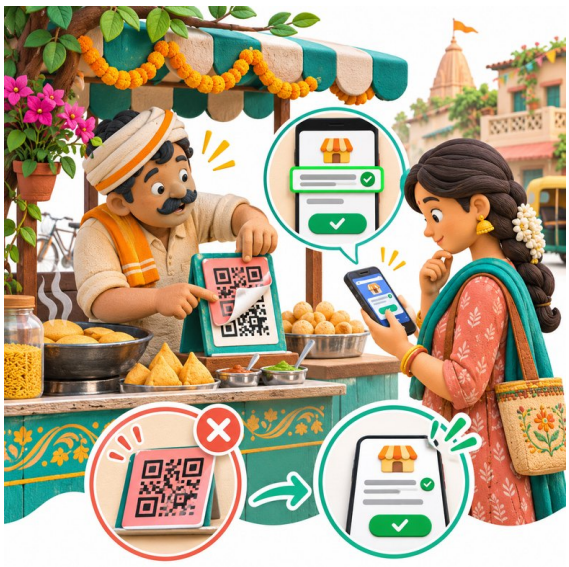
Example: “Scan this code for your delivery refund.”

WARNING SIGNS

- QR code came unsolicited
- refund requires a PIN
- screen says pay
- recipient is unfamiliar.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

A QR code can open a payment request. Read amount and payee on your own screen; use the merchant’s official refund process.

IF IT ALREADY HAPPENED

Contact bank/payment app and 1930. Block further access; keep the QR image, URL and transaction ID.

TAKEAWAY

A scan is not proof of a refund.

04

OTP, PIN and verification scams

CHAPTER 01 / PEOPLE, PRESSURE & PAYMENT

WHAT THE SCAMMER WANTS

Use a one-time code or PIN to access an account or approve a transaction.

HOW IT USUALLY UNFOLDS

1. Impersonator claims to verify identity
2. requests an OTP, PIN or screen share
3. uses it immediately.

PRESSURE BEING USED

Trust and fear

EXAMPLE ONLY

Example: “Read me the code that just arrived so I can secure your account.”

WARNING SIGNS

- Code requested on call
- unexpected login alert
- request for remote access
- caller discourages callback.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Never tell anyone an OTP, UPI PIN, password or card security code. End call; contact the institution via its official app/card.

IF IT ALREADY HAPPENED

Call the bank/provider using a trusted number; change credentials from a clean device; revoke unknown sessions; call 1930 if money moved.

TAKEAWAY

A genuine helper does not need your secret code.

05

Fake KYC and account-block threats

CHAPTER 01 / PEOPLE, PRESSURE & PAYMENT

WHAT THE SCAMMER WANTS

Steal account credentials or money under a fake compliance deadline.

HOW IT USUALLY UNFOLDS

1. SMS or call claims KYC expired
2. link leads to fake page or APK
3. victim enters credentials.

PRESSURE BEING USED

Fear

EXAMPLE ONLY

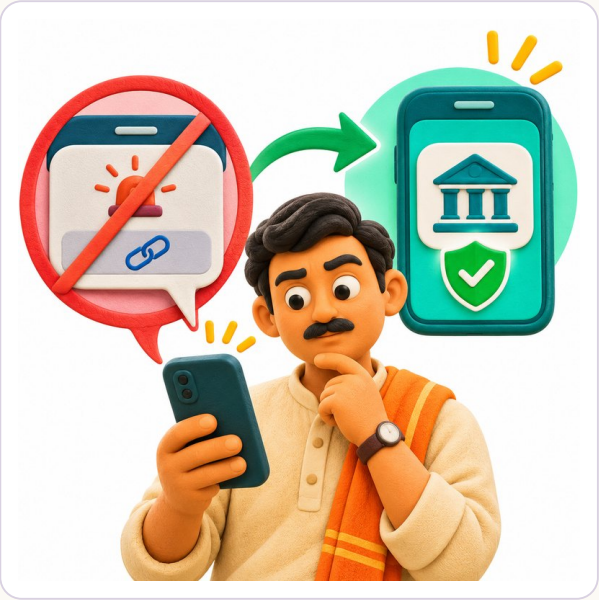
Example: “Update KYC today to avoid account suspension.”

WARNING SIGNS

- Threatening deadline
- shortened or misspelled link
- request for PIN/OTP
- APK attachment.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Open the bank’s official app or type its known address yourself. Ask at a verified branch or contact centre.

IF IT ALREADY HAPPENED

Call the bank to secure the account; remove unknown app safely with expert help; report and call 1930 for financial loss.

TAKEAWAY

KYC is checked through a channel you choose.

06

Digital arrest and fake police calls

CHAPTER 01 / PEOPLE, PRESSURE & PAYMENT

WHAT THE SCAMMER WANTS

Extract money by impersonating police or an agency and isolating the target.

HOW IT USUALLY UNFOLDS

1. Caller alleges a case
2. demands secrecy/video call
3. stages “custody”
4. asks for transfer or verification payment.

PRESSURE BEING USED

Fear and authority

EXAMPLE ONLY

Example: “Stay on video and move your savings for investigation.”

WARNING SIGNS

- No independent contact allowed
- secret investigation
- payment to prove innocence
- threats of arrest.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

End the call. Contact local police using independently found official contact details and tell a trusted person. Authorities do not need you to transfer funds to prove innocence.

IF IT ALREADY HAPPENED

Call your bank and 1930 if paid. Preserve call records and messages; report via cybercrime.gov.in and local police.

TAKEAWAY

No legitimate investigation is settled by a secret transfer.

07

Fake investment, trading and crypto

CHAPTER 01 / PEOPLE, PRESSURE & PAYMENT

WHAT THE SCAMMER WANTS

Take deposits or credentials using fabricated returns and impersonated experts.

HOW IT USUALLY UNFOLDS

1. Victim sees online ad/group
2. gets fake dashboard profits
3. pays fees/tax to withdraw
4. organizer vanishes.

PRESSURE BEING USED

Greed and fear of missing out

EXAMPLE ONLY

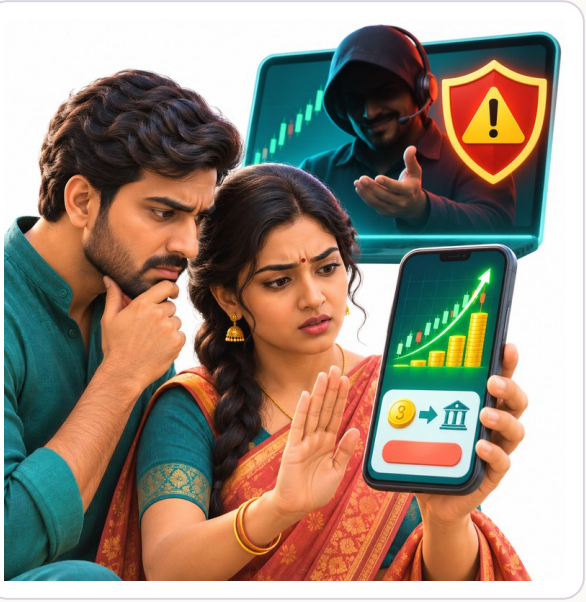
Example: “Guaranteed daily returns; deposit more to unlock withdrawal.”

WARNING SIGNS

- Guaranteed returns
- pressure to recruit
- unregulated platform
- extra withdrawal fee
- crypto transfer.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Check intermediary and warnings through SEBI’s official resources; independently verify registration. Never rely on a group’s screenshots.

IF IT ALREADY HAPPENED

Stop deposits. Contact bank/exchange, preserve wallet addresses and chats, report to cybercrime portal; seek qualified financial/legal help.

TAKEAWAY

A displayed profit is not money you can withdraw.

08

Fake jobs and task scams

CHAPTER 01 / PEOPLE, PRESSURE & PAYMENT

WHAT THE SCAMMER WANTS

Collect registration fees or lure people into transferring funds.

HOW IT USUALLY UNFOLDS

1. Recruiter offers simple remote work
2. initial small payout builds trust
3. asks for deposits to unlock tasks.

PRESSURE BEING USED

Greed and sunk-cost pressure

EXAMPLE ONLY

Example: “Pay a refundable recharge to get the next task.”

WARNING SIGNS

- Pay to get work
- vague employer
- escalating deposits
- tasks involve rating or moving money.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Verify company and recruiter through the company’s official careers channel. Do not pay to unlock wages or handle strangers’ funds.

IF IT ALREADY HAPPENED

Stop paying; call bank/payment provider and 1930 if paid. Save recruiter profile, task messages and transaction details.

TAKEAWAY

Work should not require a secret deposit to release wages.

09

Online shopping and fake seller

CHAPTER 01 / PEOPLE, PRESSURE & PAYMENT

WHAT THE SCAMMER WANTS

Take payment without shipping goods or deliver counterfeit/unsafe goods.

HOW IT USUALLY UNFOLDS

1. Seller uses a cloned shop or social profile
2. offers unusually low price
3. requests off-platform payment.

PRESSURE BEING USED

Greed and scarcity

EXAMPLE ONLY

Example: “Pay by direct transfer for an extra discount.”

WARNING SIGNS

- Price far below usual
- new account
- off-platform payment
- no verifiable return terms.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Check seller history and return policy on the platform. Keep payment inside platform protections; verify independently.

IF IT ALREADY HAPPENED

Raise platform dispute promptly; contact bank for applicable options; preserve listing, messages and proof of payment.

TAKEAWAY

A bargain is not worth losing the payment trail.

10

Fake customer-care numbers

CHAPTER 01 / PEOPLE, PRESSURE & PAYMENT

WHAT THE SCAMMER WANTS

Route a caller to a fraudster posing as support.

HOW IT USUALLY UNFOLDS

1. Victim searches online
2. sponsored/fake number appears
3. agent asks to install app or disclose credentials.

PRESSURE BEING USED

Frustration and urgency

EXAMPLE ONLY

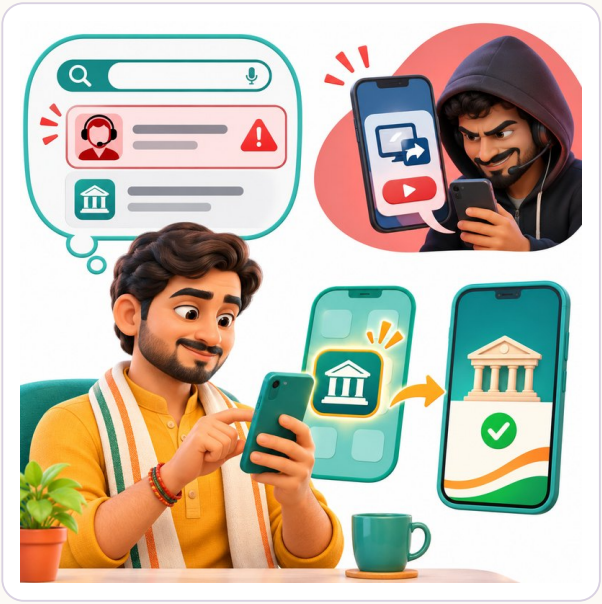
Example: “Support” asks you to install a remote-control tool.

WARNING SIGNS

- Number from comments or search ad
- remote access
- OTP/PIN request
- request to transfer a test amount.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Use contact details printed in the official app, card, bill or website you type yourself. Never give remote control to an unknown caller.

IF IT ALREADY HAPPENED

Disconnect network if remote access is active; contact bank via another device; uninstall suspicious tool with help and call 1930 if needed.

TAKEAWAY

Search ranking does not verify a support number.

11

Electricity, utility and scheme scams

CHAPTER 01 / PEOPLE, PRESSURE & PAYMENT

WHAT THE SCAMMER WANTS

Steal credentials or money with a disconnection or subsidy story.

HOW IT USUALLY UNFOLDS

1. Message threatens cutoff or promises benefit
2. link/app requests payment or identity details.

PRESSURE BEING USED

Fear or greed

EXAMPLE ONLY

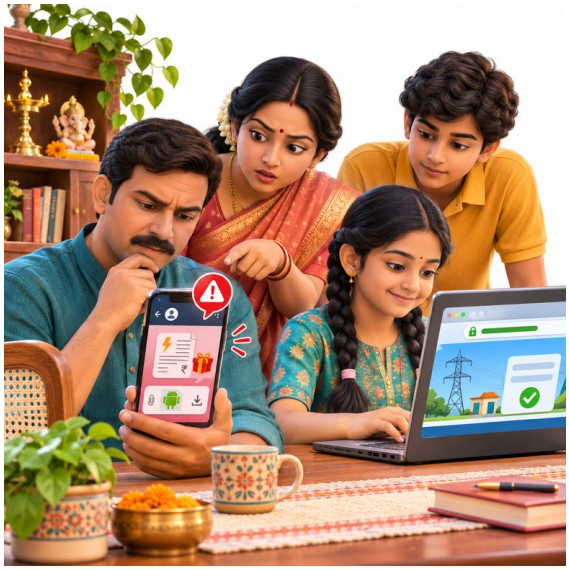
Example: “Power will be disconnected tonight; install bill.apk.”

WARNING SIGNS

- Unexpected urgent bill
- APK attachment
- unknown payment handle
- request for Aadhaar/OTP.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Check bill and scheme only in the official utility or government channel you independently open.

IF IT ALREADY HAPPENED

Call utility using printed bill details; bank and 1930 if paid; remove unauthorized app and secure phone.

TAKEAWAY

Verify the bill with the provider before paying.

12

Loan-app abuse and fake instant loans

CHAPTER 01 / PEOPLE, PRESSURE & PAYMENT

WHAT THE SCAMMER WANTS

Harvest contacts/data, charge hidden fees or coerce repayment.

HOW IT USUALLY UNFOLDS

1. App promises instant loan
2. takes broad permissions
3. demands upfront fee
4. later threatens borrower and contacts.

PRESSURE BEING USED

Desperation and urgency

EXAMPLE ONLY

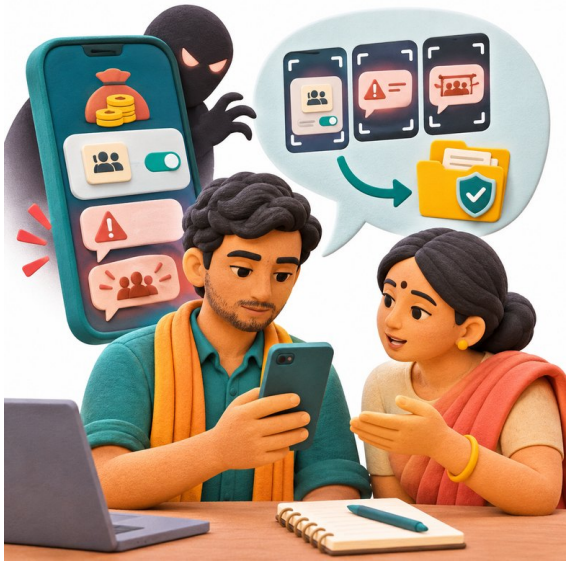
Example: “Pay a processing fee now; approval guaranteed.”

WARNING SIGNS

- Unclear lender
- excessive permissions
- upfront fee
- threats
- unclear interest and grievance contact.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Check the lender and terms independently. Install only from trusted stores and review permissions; do not share contacts unnecessarily.

IF IT ALREADY HAPPENED

Revoke permissions, document threats, contact bank and local police; report app to store and relevant regulator; seek trusted support.

TAKEAWAY

A loan app should explain the lender, cost and permissions.

13

Romance and matrimonial scams

CHAPTER 01 / PEOPLE, PRESSURE & PAYMENT

WHAT THE SCAMMER WANTS

Build intimacy to obtain money, documents or account access.

HOW IT USUALLY UNFOLDS

1. Profile develops relationship quickly
2. crisis or travel story appears
3. requests funds or private details.

PRESSURE BEING USED

Affection, empathy and secrecy

EXAMPLE ONLY

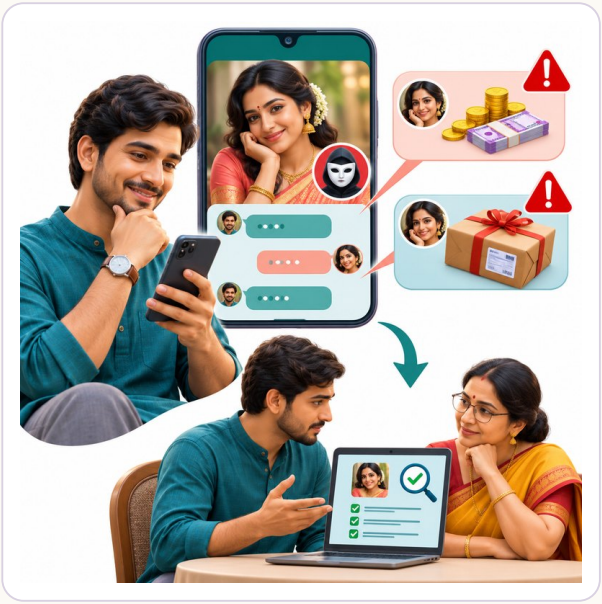
Example: “I am stranded; please transfer money discreetly.”

WARNING SIGNS

- Refuses live verification
- urgent money request
- asks for intimate material
- story changes.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Verify identity through a separate channel and trusted people. Never send money or intimate images under pressure.

IF IT ALREADY HAPPENED

Contact bank if paid; preserve profile and messages; report platform and police; tell a trusted person.

TAKEAWAY

A caring relationship respects a careful boundary.

14

Sextortion and intimate-image threats

CHAPTER 01 / PEOPLE, PRESSURE & PAYMENT

WHAT THE SCAMMER WANTS

Extort money or more images by threatening exposure.

HOW IT USUALLY UNFOLDS

1. Scammer obtains image/video or fabricates one
2. threatens to send it to contacts
3. demands payment.

PRESSURE BEING USED

Shame and panic

EXAMPLE ONLY

Example: “Pay now or I will message your family.”

WARNING SIGNS

- Immediate deadline
- demands secrecy
- repeated escalating payments
- claims every contact has been reached.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Do not pay or send more material. Stop engaging; tighten privacy; tell a trusted person. Preserve evidence before blocking.

IF IT ALREADY HAPPENED

Report account/content to platform and police/cybercrime portal. If a minor is involved, tell a trusted adult immediately. Do not blame the target.

TAKEAWAY

You deserve support; payment rarely ends the demands.

CHAPTER 02 / ATTACK GUIDES 15-25

Identity, Devices & Account Access

How criminals take over a phone number, device, document or online account—and how to contain the damage.

INSIDE THIS CHAPTER

- 15–19 SIM swaps, identity theft, harmful apps, call forwarding and USB risks
- 20–22 Gaming, card support and social-account takeover
- 23–25 Money-mule recruitment, courier threats and messaging impersonation



A SIMPLE METHOD

Stop. Name the request. Verify it through a channel you open yourself. Act only when the details make sense.

KEEP IN MIND

If an app or account may be compromised, use a clean device to get help.

15

SIM swap and number takeover

CHAPTER 02 / IDENTITY, DEVICES & ACCOUNT ACCESS

WHAT THE SCAMMER WANTS

Take control of the phone number to intercept calls or codes.

HOW IT USUALLY UNFOLDS

1. Victim loses network
2. impostor has obtained a replacement SIM
3. attempts password resets.

PRESSURE BEING USED

Confusion and fear

EXAMPLE ONLY

Example: “Your SIM will be upgraded; confirm this code.”

WARNING SIGNS

- Sudden loss of service
- unexpected SIM/eSIM notification
- login resets
- calls no longer arrive.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Contact carrier through a known official channel immediately; add carrier account protections; use app-based MFA where possible.

IF IT ALREADY HAPPENED

Ask carrier to restore/secure SIM; contact banks to block risky access; reset passwords from a clean device; report and call 1930 if loss.

TAKEAWAY

A sudden signal loss deserves a fast carrier check.

16

Identity-document and credential theft

CHAPTER 02 / IDENTITY, DEVICES & ACCOUNT ACCESS

WHAT THE SCAMMER WANTS

Use personal documents or passwords to impersonate the victim.

HOW IT USUALLY UNFOLDS

1. Fake form or recruiter requests ID/password
2. data reused for accounts, loans or targeted fraud.

PRESSURE BEING USED

Opportunity and authority

EXAMPLE ONLY

Example: “Upload Aadhaar, PAN and email password to verify your job.”

WARNING SIGNS

- Unneeded document request
- password asked with ID
- unknown storage destination
- no privacy terms.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Share the minimum necessary through a verified channel. Mask document details where accepted; never send account passwords.

IF IT ALREADY HAPPENED

Change exposed passwords, enable MFA, notify affected institution and monitor accounts; report suspected misuse to the relevant authority.

TAKEAWAY

A document image can unlock real services; share sparingly.

17

Malicious APK and fake bill/KYC apps

CHAPTER 02 / IDENTITY, DEVICES & ACCOUNT ACCESS

WHAT THE SCAMMER WANTS

Install malware that reads messages, captures credentials or controls the device.

HOW IT USUALLY UNFOLDS

1. Scammer sends APK by chat
2. victim enables unknown install
3. app requests accessibility/SMS permissions.

PRESSURE BEING USED

Fear and convenience

EXAMPLE ONLY

Example filename: lightbill.apk. Filenames can change and prove nothing.

WARNING SIGNS

- APK from message
- outside-store install prompt
- broad permissions
- urgent bill/KYC story.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Do not install. Check app publisher in official store and provider channel. Reject unneeded accessibility/SMS/notification access.

IF IT ALREADY HAPPENED

Disconnect phone from network if control suspected; contact bank from another device; get trusted technical help to remove app, reset credentials and call 1930 if money moved.

TAKEAWAY

An app name is not evidence of safety.

18

Call-forwarding scams

CHAPTER 02 / IDENTITY, DEVICES & ACCOUNT ACCESS

WHAT THE SCAMMER WANTS

Redirect calls so the scammer receives calls or verification attempts.

HOW IT USUALLY UNFOLDS

1. Caller requests a code or dialling instruction
2. victim unknowingly changes forwarding
3. calls divert.

PRESSURE BEING USED

Helpfulness and distraction

EXAMPLE ONLY

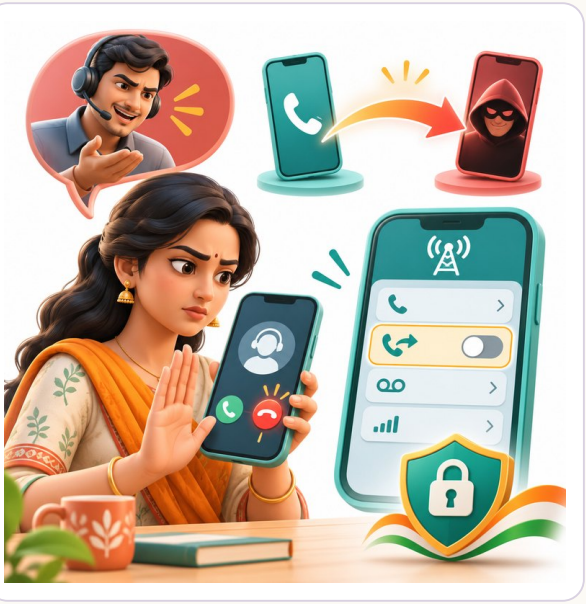
Example: “Enter this code to confirm delivery.”

WARNING SIGNS

- Unsolicited code
- call forwarding suddenly active
- caller asks to dial a sequence.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Do not dial unsolicited USSD codes or follow caller instructions. Inspect call-forwarding settings in phone settings and ask carrier through official channels.

IF IT ALREADY HAPPENED

Disable unexpected forwarding in settings if available; contact carrier and bank using a trusted device; secure accounts.

TAKEAWAY

Never change call settings for an unsolicited caller.

19

Public USB charging and data connections

CHAPTER 02 / IDENTITY, DEVICES & ACCOUNT ACCESS

WHAT THE SCAMMER WANTS

Access device data through an unsafe port or cable.

HOW IT USUALLY UNFOLDS

1. Public port/cable prompts trust or data connection
2. device allows data
3. malicious accessory attempts access.

PRESSURE BEING USED

Convenience

EXAMPLE ONLY

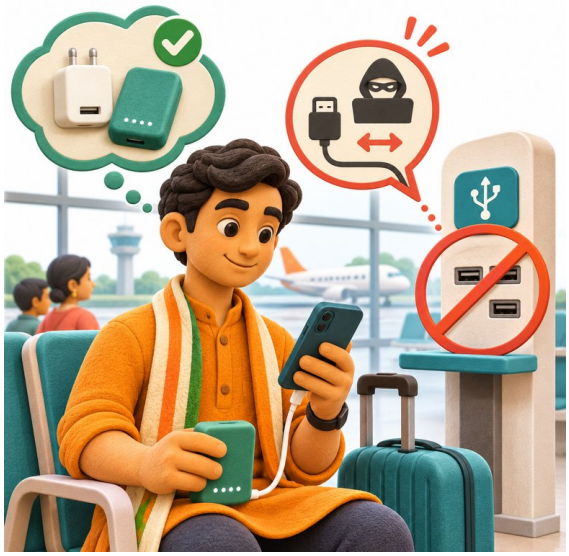
Example: kiosk asks you to “trust” a connected computer.

WARNING SIGNS

- Unknown cable
- data-access prompt
- device unlocked
- no power-only adapter.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Use your own charger and wall socket or a power-only adapter. Choose “charge only”; do not trust unknown computers.

IF IT ALREADY HAPPENED

Disconnect; revoke trusted-computer access if available; change exposed credentials and check device/account activity.

TAKEAWAY

Public power is safer when your data path stays closed.

20

Gaming, recharge and in-game purchase scams

CHAPTER 02 / IDENTITY, DEVICES & ACCOUNT ACCESS

WHAT THE SCAMMER WANTS

Steal game credentials, payment details or funds through fake rewards.

HOW IT USUALLY UNFOLDS

1. Fake moderator promises skins/diamonds
2. asks login code or off-platform payment
3. account is taken.

PRESSURE BEING USED

Greed and belonging

EXAMPLE ONLY

Example: “Free top-up: send your login OTP.”

WARNING SIGNS

- Free premium currency
- fake support DM
- login outside official game
- gift-card payment.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Use the game’s official store and support. Protect account with unique password and MFA; ask a parent before purchases if a minor.

IF IT ALREADY HAPPENED

Recover account through official support; block/report scammer; contact payment provider if charged.

TAKEAWAY

No stranger needs your login code to send a reward.

21

Card and fake bank-support scams

CHAPTER 02 / IDENTITY, DEVICES & ACCOUNT ACCESS

WHAT THE SCAMMER WANTS

Capture card details, PIN, CVV, OTP or remote access.

HOW IT USUALLY UNFOLDS

1. Impersonator claims suspicious charge
2. asks card credentials or “safe account” transfer.

PRESSURE BEING USED

Fear and authority

EXAMPLE ONLY

Example: “Tell me the CVV so I can block your card.”

WARNING SIGNS

- Requests full card details
- asks OTP/PIN
- demands transfer
- caller insists you stay on call.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Hang up. Lock card in official app if appropriate; call number printed on card or official bank app.

IF IT ALREADY HAPPENED

Block card/account through official channel; dispute promptly; call 1930 if cyber fraud; preserve transaction reference.

TAKEAWAY

A bank can secure your card without learning your PIN.

22

Social account takeover and fake collaborations

CHAPTER 02 / IDENTITY, DEVICES & ACCOUNT ACCESS

WHAT THE SCAMMER WANTS

Steal creator credentials or hijack profile to scam followers.

HOW IT USUALLY UNFOLDS

1. Fake brand sends link/document
2. asks login
3. victim enters password and code
4. profile sends money requests.

PRESSURE BEING USED

Opportunity and fear of missing out

EXAMPLE ONLY

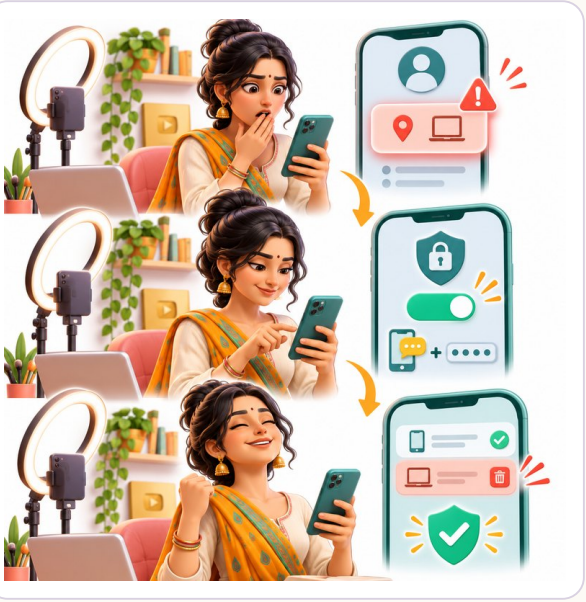
Example: “Brand collab contract—sign in to view.”

WARNING SIGNS

- Unexpected collaboration
- login link
- urgency
- asks for code
- new linked-device alert.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Verify brand through an independently found company contact. Open the platform directly; do not sign in through a sent link.

IF IT ALREADY HAPPENED

Use official recovery flow, revoke unknown sessions/apps, warn followers through another channel and report impersonation.

TAKEAWAY

A collab proposal should survive a separate verification.

23

Money-mule recruitment and suspicious transfers

CHAPTER 02 / IDENTITY, DEVICES & ACCOUNT ACCESS

WHAT THE SCAMMER WANTS

Use another person's account to move or disguise stolen funds.

HOW IT USUALLY UNFOLDS

1. Recruiter asks to receive money and forward it, keeping a fee
2. victim shares account access.

PRESSURE BEING USED

Greed and trust

EXAMPLE ONLY

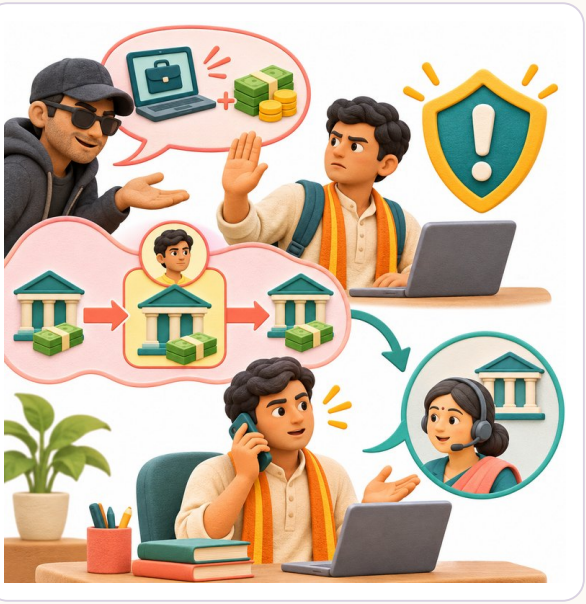
Example: "Let payments pass through your account for commission."

WARNING SIGNS

- Commission for moving funds
- unfamiliar source
- requests account credentials
- secrecy.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Do not receive or forward money for a stranger. Contact your bank and seek legal advice if already involved.

IF IT ALREADY HAPPENED

Stop transfers; preserve records; contact bank and local police promptly. Be truthful and do not delete evidence.

TAKEAWAY

Your account is your responsibility; do not rent it out.

24

Fake courier, customs and illegal parcel

CHAPTER 02 / IDENTITY, DEVICES & ACCOUNT ACCESS

WHAT THE SCAMMER WANTS

Extort money or data by claiming a parcel contains contraband.

HOW IT USUALLY UNFOLDS

1. Caller impersonates courier/police
2. alleges illegal goods
3. sends fake case number or payment link.

PRESSURE BEING USED

Fear and authority

EXAMPLE ONLY

Example: “Your parcel is held; pay clearance before police arrive.”

WARNING SIGNS

- Unexpected parcel
- secrecy
- video interrogation
- payment to clear case
- request for ID/OTP.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Ask for the tracking number and verify with courier via its official site/app. End threats and contact police independently.

IF IT ALREADY HAPPENED

Call bank and 1930 if paid; save parcel ID, call details and payment trail; report the impersonation.

TAKEAWAY

A threatening call does not establish a real parcel or case.

25

WhatsApp takeover and impersonation

CHAPTER 02 / IDENTITY, DEVICES & ACCOUNT ACCESS

WHAT THE SCAMMER WANTS

Take over a messaging account or impersonate a contact to ask for money.

HOW IT USUALLY UNFOLDS

1. Scammer tricks target into sharing login code or linking a device
2. then messages contacts.

PRESSURE BEING USED

Trust and urgency

EXAMPLE ONLY

Example: “I sent you a code by mistake—forward it to me.”

WARNING SIGNS

- Unrequested login code
- unknown linked device
- urgent money request
- changed profile behavior.

PAUSE & MARK IT

What would you verify before responding?



BEFORE YOU ACT

Never share a WhatsApp registration code. Review Linked devices in the app; verify money requests by calling the person on a known number.

IF IT ALREADY HAPPENED

Re-register account through official app; remove unknown linked devices; warn contacts through another channel and report impersonation.

TAKEAWAY

A familiar profile can be controlled by someone else.

CHAPTER 03 / SAFE CLASSROOM DEMOS

Practical Demonstrations

Four safe classroom activities using fictional screens, trusted apps and a training phone.

INSIDE THIS CHAPTER

- DEMO 01 Spot urgency, suspicious requests and unsafe links in a mock message
- DEMO 02 Review APK names, publishers and permissions without installing one
- DEMO 03 Inspect call-forwarding settings through device settings and the carrier
- DEMO 04 Review merchant, amount, frequency and controls in a UPI AutoPay mandate



A SIMPLE METHOD

Stop. Name the request. Verify it through a channel you open yourself. Act only when the details make sense.

KEEP IN MIND

Demonstrate the decision with mock screens and a training phone only.

Demo 1 / Read a suspicious SMS

IN THE ROOM • FICTIONAL MESSAGE ONLY

Notice the ask → Inspect the link → Open known app → Verify separately

MOCK MESSAGE • NOT A REAL ALERT

“Your service is paused. Install update.apk and share the one-time code to restore access.”

- Underline urgency, an unsolicited file and a code request.
- Do not tap. Open the relevant service independently and check status.
- Demonstrate link preview without opening the destination.

Demo 2 / APK filenames

Examples seen in scams include lightbill.apk, gasbill.apk, channel.apk / chnnale.apk, itr.apk and gsr-3b.apk. Names change and never prove an app is genuine. Show a mock download screen; discuss publisher, source and requested permissions. Do not install the files.

Demo 3 / Call forwarding

On a training phone, open the phone app or device settings and inspect call-forwarding options. Menu names vary by device, Android/iOS version and carrier. Ask the carrier through its official app, bill or website if anything is unclear.



Do not dial unsolicited USSD codes. This handbook gives no carrier code.

Demo 4 / UPI AutoPay mandates

OPEN A TRUSTED UPI APP • TRAINING ACCOUNT IF POSSIBLE

Mandates → **Merchant** → **Amount + frequency** → **Next debit** → **Pause / revoke**

Review each mandate in the participant's own trusted app. Confirm merchant, amount, frequency, next debit and the app's pause or revoke controls. Menu names and controls vary. Do not approve an unfamiliar mandate to "cancel" it.

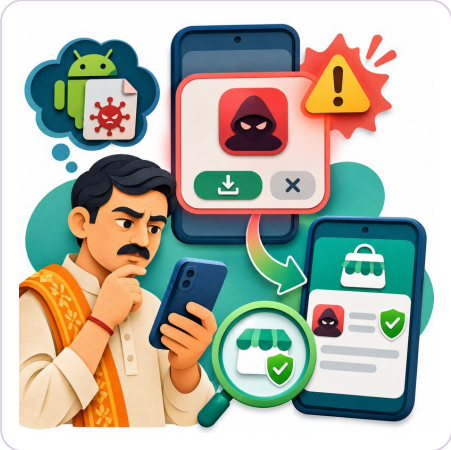
UPI PIN ≠ M-PIN

A UPI PIN authorizes a UPI transaction. Never share it. An mPIN is a device or banking-app access credential; exact meaning and use vary by institution. Neither belongs in a call, chat or form sent by a stranger.

Phone and account toolkit

PHONE SECURITY

- Install system updates from device settings.
- Use a screen lock and a recovery method you control.
- Install apps from trusted official stores; review publisher and permissions.
- Remove apps you no longer need. Review accessibility, SMS and notification access.



ACCOUNTS AND PASSWORDS

- Use a unique, long password for each important account; a password manager can help.
- Turn on two-step verification, preferably with an authenticator or passkey when offered.
- Review active sessions, linked devices and recovery email/phone. Sign out unfamiliar sessions.



IF A PHONE FEELS COMPROMISED

Stop using it for banking. From another trusted device, contact your bank and carrier, secure your primary email, and ask a trusted technician to help inspect the phone before you use it for payments again.

Payments, family and work

PAYMENTS AND UPI

- Read payee and amount on your own screen.
- Decline unexpected collect requests.
- Review AutoPay mandates and disable unknown ones through a trusted app.
- Never pay a fee to receive a refund.



FAMILY VERIFICATION PHRASE

- Agree a private phrase in person, then keep it secret.
- For urgent money requests, call the person on a saved number.
- If unavailable, ask a second trusted family member.



WORKPLACE PAYMENT CHANGES

- Verify changed bank details by calling a known number already on file.
- Separate the person who changes supplier details from the person who approves payment.
- Keep a written trail and require a second approval for exceptions.



UPI PIN REMINDER

A UPI PIN authorizes a payment. Never share it or enter it to receive money.

Back up and recover

A small amount of preparation makes a stressful incident easier to handle.

BACKUP

- Turn on automatic backup for photos and important files.
- Keep a second copy of essential records in a separate, protected place.
- Test that you can restore a file.



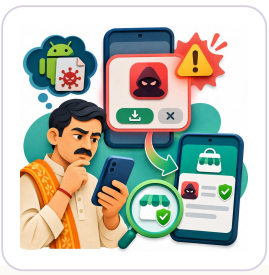
RECOVERY

- Keep account recovery email and phone current.
- Store recovery codes securely, away from the account they unlock.
- Know how to lock a card, report a lost SIM and recover your primary email.



PERMISSIONS

- Allow only what an app needs for its function.
- Recheck location, microphone, camera, contacts, accessibility and SMS permissions.
- Remove access after a temporary need ends.



A TEN-MINUTE MONTHLY RESET

- Check that your backup completed and restore one test file.
- Review recovery email, phone number and linked sessions.
- Remove app permissions you no longer need.



If fraud happens: first five minutes

Breathe. A scam can happen to anyone. You are not at fault for being targeted. Move quickly on containment; do not follow the caller’s directions.

1. Stop further payments. End the call and stop following instructions.
2. Contact your bank or payment provider using the number in its official app, card or website. Ask about blocking and disputes.
3. Call India’s cyber-fraud helpline 1930 promptly. Report at cybercrime.gov.in.
4. Preserve transaction IDs, messages, phone numbers, screenshots, URLs, timestamps and complaint references.
5. From a clean device, secure accounts, revoke unknown sessions or mandates, and alert affected contacts.

KEEP THE RECORD

Write down what happened and when. Save evidence before deleting or resetting. A bank, payment provider, police unit or platform may ask for different information; follow their official instructions.

Worksheet / My device safety

Complete this privately. Do not write passwords, PINs or recovery codes on this page.

- [ ] My phone has a screen lock.
- [ ] My phone and apps are updated.
- [ ] I reviewed app permissions this month.
- [ ] I know where to check linked devices.
- [ ] I know how to contact my carrier through an official channel.
- [ ] I have a backup and know how to restore one.
- [ ] My important accounts have unique passwords.
- [ ] I have enabled two-step verification where available.

Worksheet / Verify before you pay

Pause on every payment, new payee or change of bank details.

- [ ] I opened the app or website myself.
- [ ] I checked the recipient name and account details.
- [ ] I understand whether this action sends money or requests money.
- [ ] The amount and purpose match what I agreed.
- [ ] I verified any changed payment instructions using a known contact.
- [ ] I am not paying to receive a refund, prize, job or loan.
- [ ] I have not shared a PIN, password or OTP.
- [ ] I can wait and verify later if anything feels rushed.

PAYMENT I AM ABOUT TO MAKE

Who receives it? _____

What is it for? _____

How did I verify? _____

Worksheet / Family safety plan

Decide together while everyone is calm.

OUR PRIVATE VERIFICATION PHRASE (DO NOT WRITE THE PHRASE HERE):

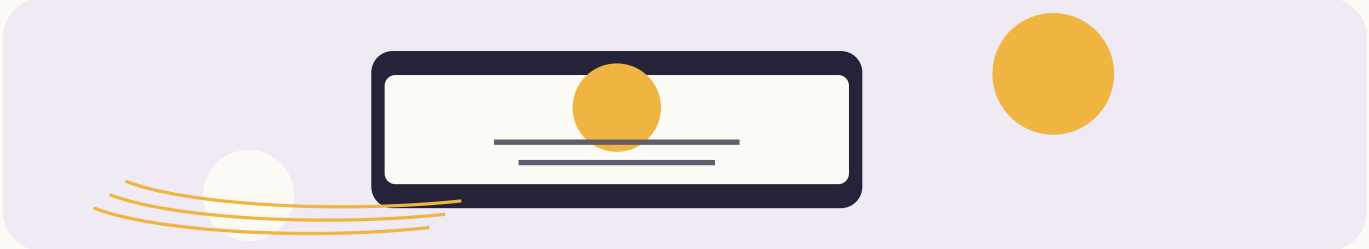
IF SOMEONE ASKS FOR URGENT MONEY, WE WILL CALL:

A SECOND PERSON WHO CAN VERIFY:

WHERE WE KEEP OFFICIAL BANK / CARRIER CONTACT DETAILS:

WHO CAN HELP A CHILD OR OLDER ADULT REPORT A CONCERN:

OUR FAMILY RULE FOR SHARING DOCUMENTS AND CODES:



Practice / Spot the scam

EXERCISE • FICTIONAL MESSAGE

“Your electricity will stop in 20 minutes. Install bill-update.apk and tell our agent the OTP to confirm payment.”

What are the warning signs? What would you do first?

ANSWER KEY

Threat and artificial deadline; unsolicited APK; OTP request. Do not install or share a code. Check the bill in the official utility channel opened independently. If installed, use a clean device to contact your bank and get trusted help to secure the phone.

Notes from the workshop

Ideas, questions and actions I want to remember

TEAR-OUT / SAVE A PHOTO

MONEY MOVED?

1 Stop payment and end the call.

2 Contact your bank using its official app, card or website.

3 Call 1930 promptly.

4 Report at cybercrime.gov.in.

5 Save transaction IDs, messages, numbers and times.

6 Secure accounts from a clean device; alert contacts.

You are not alone. Ask a trusted person to stay with you while you report.

Trusted resources

Open these addresses by typing them yourself or using an official app. Checked on 15 November 2026. Reporting steps and service features may vary by institution and can change; confirm on the official site.

Financial cyber fraud	Call 1930 promptly
National Cyber Crime Reporting Portal	https://cybercrime.gov.in
CERT-In	https://www.cert-in.org.in
Reserve Bank of India	https://www.rbi.org.in
SEBI	https://www.sebi.gov.in
TRAI	https://www.trai.gov.in
Sanchar Saathi (DoT)	https://sancharsaathi.gov.in

Use official channels only. A search result, social post, message label or caller ID does not authenticate a phone number or link. For bank service complaints, first contact the institution and follow RBI’s current grievance process if unresolved.

TAKE THE PAUSE WITH YOU

Safer steps start with a pause.

Stop. Think. Verify. Then choose your next step.

IF MONEY HAS MOVED

Contact your bank and call 1930 promptly. Keep transaction details and messages.

