PREVIEW | FREE SAMPLE

CyberWithMadhav

2026 EDITION

PREVIEW



INDIA'S CYBER SAFETY PLAYBOOK

Scam-Proof Family Kit

15 scams explained in simple words. What to do in the first 60 minutes. Checklists and a fridge card for your parents.

Madhav Pandya
CyberWithMadhav | cyberwithmadhav.com

$ stop. think. verify.

15 common Indian scams | First 60 minutes guide | Printable fridge card | Kids' safety

CyberWithMadhav

START HERE

How to use this kit

Namaste. This kit is written for families: parents, students and anyone who uses a phone, UPI or WhatsApp. It uses simple English with a few Hinglish lines, so you can read it with your family.

THE ONE RULE BEHIND EVERYTHING

Ruko. Socho. Verify karo.

Stop. Think. Verify. Every scam in this kit tries to make you act **fast**, **scared**, **greedy** or **secretive**. NPCI notes that people fall for frauds mostly because of greed, fear or ignorance. A pause breaks the spell.

Use it in three steps

STEP 1: READ

Read the **15 scams** (Part 1). Each one has how it works, red flags and what to do. Start with the ones you or your parents are most likely to meet.

STEP 2: SET UP

Sit with your family for one hour and tick off the **security and WhatsApp checklists** on each phone.

STEP 3: PREPARE

Print the **fridge card** and keep the **First 60 minutes** page ready. In a scam, you will not have time to search.

How each scam page is laid out

- **How it works**: the story the scammer tells, in plain words.
- **Red flags**: the signs you can spot in the moment.
- **What to do**: the safe steps, and where to report.
- **Hinglish line**: a short line you can remember and tell your parents.

If you are being scammed right now

GO STRAIGHT TO THE FIRST 60 MINUTES PAGE

Do not finish this section first. Turn to **First 60 minutes**, call your bank, then call **1930**. Come back and read the rest later.

Printing tips

The inner pages are light so they print well in black and white. For the fridge card, print that page at 100 percent scale (no "fit to page") and cut along the dotted line.

Menu names in apps can differ a little between phone models and app versions. If a menu looks different, look for the closest option or use the app's search.

CyberWithMadhav

1 Digital arrest

Fake police, CBI, customs or ED video call

HOOK: FEAR

How it works. A caller, an IVR message or a video call says you are linked to a crime: a parcel with drugs or fake passports, money laundering, or misuse of your Aadhaar or SIM. Sometimes they say a relative is in custody. You are told to stay on a video call (the so-called digital arrest), often in front of a fake police-station setup, and to pay money to "settle" the case.

RED FLAGS

- Threat of arrest, jail or a bank freeze within hours
- You are told to stay on camera and not tell anyone
- Uniforms and an office background on a video call
- Caller IDs that can be spoofed to look official
- Demand to move money to a "safe" or "verification" account

WHAT TO DO

- Hang up. I4C says CBI, police, customs, ED and judges do not arrest anyone on a video call
- There is no concept of digital arrest under any Indian law
- Call the nearest police station yourself on a number you look up, to verify
- Speak to family before you move any money
- Report at 1930 or cybercrime.gov.in

Digital arrest jaisi koi cheez nahi hoti. Call kaato, phir 1930 lagao.

2 UPI collect request

"Enter your PIN to receive money"

HOOK: GREED AND TRUST

How it works. You get a payment request in your UPI app, or a caller asks you to approve one, saying it is a refund, a reward, or payment for something you are selling. The scammer says you must enter your UPI PIN to receive the money. But a PIN is only ever needed to send money out of your account.

RED FLAGS

- Anyone asking for your PIN so you can "receive" money
- A request from a name or ID you do not know
- A refund, cashback or prize story you did not expect
- Pressure to approve quickly while they are still on the phone
- The screen says you will pay, but the caller says you will receive

WHAT TO DO

- Remember the NPCI rule: enter the UPI PIN only to pay, never to receive
- Read the app screen. If it says Pay, money is leaving your account
- Decline or ignore unknown collect requests
- If you already paid, call your bank, then 1930
- Never share your PIN with anyone, including "bank staff"

Paisa lena hai to PIN nahi daalna. PIN sirf paisa dene ke liye hota hai.

CyberWithMadhav

IF YOU ARE SCAMMED

The first 60 minutes

The first hour is often called the golden hour. The sooner a fraud is reported, the better the chance that the money can be traced and frozen. If more time has passed, still report. Do not wait and do not feel ashamed.

MINUTE 0 TO 5

Stop. Breathe. Do not pay anything more.

Stop the call or chat. Do not send "one last payment", and do not try to get the money back by talking to the scammer. Do not delete chats, messages or call history. Tell a family member, so you are not alone.

MINUTE 5 TO 15

Call your bank on its official number

Use the number on your card, on the bank's official app or website. Ask them to block the card, UPI or net banking, and to raise a fraud complaint on the transaction. Keep the complaint reference they give you.

MINUTE 10 TO 20

Call 1930, the National Cyber Crime Helpline

For financial fraud, dial **1930** without delay. Keep these ready: your mobile number, the bank, wallet or merchant name, your account or UPI ID, the transaction ID (UTR), the date and time, the amount, and the scammer's phone number, UPI ID or account number. Screenshots help.

You will get an acknowledgement number by SMS or email. Note it down. You are then expected to complete your complaint on cybercrime.gov.in within 24 hours.

MINUTE 20 TO 40

File the complaint on cybercrime.gov.in

Choose the right type of complaint (financial fraud or other cyber crime), enter the transaction details, and upload your evidence. After submission you get an acknowledgement number. Log in later with the same details to check the status.

MINUTE 40 TO 60

Lock down your accounts

- Change the passwords of email, banking and UPI apps, starting with your email
- Log out of all devices, and turn on 2FA
- Uninstall any remote-access app (after taking screenshots)
- If the SIM looks dead or you get no signal, call your operator at once
- If a social media or WhatsApp account was taken, warn your contacts

NOT A MONEY LOSS? (SEXTORTION, FAKE PROFILE, THREATS)

Report at **cybercrime.gov.in** under *Report Other Cyber Crime*. For suspicious calls and messages where nothing was lost, use **Chakshu** on sancharsaathi.gov.in. For sextortion, do not pay. If someone is in danger, call **112**.

CyberWithMadhav