Based on National Cyber Crime Portal & RBI Safety Rules

Parents & Senior Safety • 2026 Edition

The Parents Shield

A complete, easy pocket guide to protect parents and seniors from Fake Calls, Pension Scams, and UPI Fraud

14	Large Print	100%
Easy Chapters	Senior Friendly	Simple Everyday English

Pension & Life Certificate

Fake Police & Digital Arrest

UPI PIN & QR Scam

AI Voice Clone Scam

WhatsApp Fraud Links

ATM Card Swapping

⚠ **Golden Rule:** You never need to enter any UPI PIN or OTP to receive money. A PIN is only for sending (deducting) money.

Citizen Awareness Cyber Safety Series

Mobile Pocket Size Edition • 120mm × 190mm

LEGAL NOTICE • DISCLAIMER

Legal Terms and Rules of Use

1. Public Awareness Purpose (Awareness Only)

This eBook is an independent guide created solely to raise digital safety awareness among everyday citizens and senior elders. Its goal is to warn readers about fraud phone calls, bank scams, and pension frauds. It is not legal or financial advice.

2. No Affiliation with Any Organization or Government (No Affiliation)

This eBook is not sponsored, endorsed, or approved by the Reserve Bank of India (RBI), Telecom Department, National Cyber Crime Portal, NPCI, Jeevan Pramaan, any bank, or any ministry of the Government of India. It is a fully independent digital guide.

3. Limitation of Liability

Cyber safety rules, government portal links, and procedures can change over time. Neither this eBook nor its author/publisher is legally responsible for any fraud, financial loss, or issue faced by any reader. Always visit the official website of the concerned government department or bank for the latest updates.

4. Trademarks and Brand Names (Fair Use)

'UPI' is a registered trademark of NPCI. 'WhatsApp' is a trademark of Meta Platforms. All other names mentioned in this book (such as PhonePe, Google Pay, SBI, AnyDesk, Airtel, Jio, etc.) belong to their respective owners and are used only for identification and explanation under Fair Use.

5. Methods Only (No Real Names)

All case studies and examples in this guide use fictional names solely to explain ongoing scam methods in society. It does not accuse any real company, organization, or person; only the methods of fraud are exposed.

6. Single-User Digital License

This PDF is licensed strictly for personal and family reading under a Single-User License. Re-uploading it publicly, reselling it, or using it commercially without written permission is prohibited under copyright law.

EDITORIAL • PREFACE

A Digital Shield for Our Parents

In today's fast-changing digital world, our elders (parents and grandparents) are the most trusting and straightforward. Fraudsters take unfair advantage of their innocence, fear, and hesitation with technology.

> “
> Fraudsters never hack the technology itself—they target **human fear (panic)**, **fake emergency dramas**, and **deep trust**.

3 Core Safety Rules for Parents:

1. No PIN Needed to Receive Money: Whenever someone says "I'm sending pension or money to your account, enter your PIN or OTP"—know right away it is 100% fake.

2. There Is No Police on Video Call: Real Police, CBI, or Courts never do "Digital Arrest" on WhatsApp or Skype.

3. Never Transfer Without Calling Your Children: Whenever a call comes claiming an emergency or arrest, call your children's real saved number first to verify.

Purpose of This Pocket Guide: To make elders in every family completely safe and confident against 14 dangerous daily scams, using large print and simple words without confusing jargon.

COMPLETE TABLE OF CONTENTS

The Parents Shield: All 14 Chapters

01 **Why Elders Face Fraud More Often**
How innocence, tech hesitation, and fear are misused

02 **What Is UPI, in Very Simple Words**
Safe way to send money straight from bank to bank

03 **UPI PIN and OTP: Never Tell Anyone**
PIN is only to send money — never to receive it

04 **Fraud Calls: Bank, KYC & Digital Arrest**
The truth behind fake police, CBI, and court threats

05 **WhatsApp Fraud Messages and Links**
Dangers of fake electricity bills, lotteries, and APK files

06 **Fake Payment and QR Scams**
Fake SMS alerts and scanning QR codes to 'receive' money

07 **"Son, I'm in Trouble": AI Voice Scams**
Fake accident and jail dramas in your child's cloned voice

08 **Frauds in the Name of Pension & Govt Schemes**
Life Certificate updates and fear of pension stopping

09 **Asking for Money Pretending to Be a Relative**
Claiming a new number and demanding urgent UPI transfers

10 **Strangers Offering "Let Me Help You"**
Traps at ATMs, bank queues, and AnyDesk on your phone

11 **Always Ask Yourself Before Sending Money**
The 10-second pause and confirming with family by phone

12 **What to Do If Fraud Happens**
Golden 2 Hours, blocking your bank account, and Cyber Crime reporting

13 **For Family Members: How to Teach Parents**
Teaching with patience, phone settings, and daily safety habits

14 **Elders' Master Safety Checklist**
6 golden rules — ready to stick near your phone or cupboard

CHAPTER 1 • DIGITAL SAFETY FOR PARENTS

Why Elders Face Fraud More Often

Human trust, the new world of smartphones, and the full truth about scammer fear tactics.

Phone Rings with Sweet Words: How Scammers Set the Trap

Imagine your father or mother sitting at home when the phone rings. Someone speaks with extreme politeness: *"Namaste Bauji, I'm calling from your Pension Office. Your Life Certificate work is stuck in your bank account. If not fixed in 10 minutes, this month's pension will stop."*

An elderly person gets scared and thinks the caller is telling the truth and trying to help. Scammers target elders at home far more often than young people.

Know the Truth

Why Do Scammers Target Elders?

Our parents worked hard their whole lives to save money, and their bank accounts hold pension or retirement funds. On top of that, elders trust easily and don't know all the hidden tricks of smartphones.

> **Plain truth:** When a stranger on a call shows extra-sweet respect or creates sudden panic, know that something is wrong.

Case Study: Fake Fear of Pension Stopping

See how scammers use sweet respect and fear to trap elders:

📞 PHONE CALL SIMULATION (FAKE PENSION OFFICER)

Scammer (very sweet, respectful voice): "Namaste Uncle ji, I'm calling from the Head Pension Office. There is a technical error in your pension file. If not fixed today, your account will freeze."

Simple Elder: "Oh son, how did that happen? What should I do? Even my medicines depend on this money."

Scammer: "Uncle ji, don't worry at all, I will help you completely. A 6-digit Security Code (OTP) must have arrived on your phone—just tell me that and I'll fix everything from here."

Truth: *(That code was actually the OTP to withdraw money from the bank! The*

moment the elder shared it, their life savings vanished.)

The Scammer's 4-Step Trap Against Elders

1 **Starting with Polite Respect**

The scammer begins with "Pranam Chachaji" or "Namaste Bauji" so the elder thinks they are talking to a kind person.

↓ Suddenly creating a fake crisis

2 **Fear of Pension, Bank, or Power Cut**

They say: "Your SIM will shut tonight", "Your pension will stop", or "Pay your electricity bill right now or power gets cut."

↓ Giving no time to think or ask children

3 **Pressuring for Code (OTP) or App Download**

The scammer pushes: "There is no time to tell anyone—just tell me the code on your phone or tap this link."

↓ Money gone and call cut

4 **Bank Account Emptied and Regret**

The moment you share the code or tap the link, money leaves your bank and the caller disconnects right away.

Real Officer vs Fake Caller: 3 Biggest Differences



1. A Real Bank Never Asks for Codes (OTP)

RBI's clear rule: No real bank staff EVER asks for your OTP, UPI PIN, or the numbers on the back of your ATM card on a phone call.

> **Rule:** Anyone asking for a code or OTP on a call is 100% a scammer.



2. The Pension Office Never Rushes You

Government offices always give proper time for any task. No government service shuts down in 10 minutes over a phone call.



3. Real Companies Never Make You Install Apps

No bank or government department ever asks you to install screen sharing apps like AnyDesk or TeamViewer to fix your phone.

Official Portal: Citizen Safety & Complaint Center

The Ministry of Home Affairs runs the **National Cyber Crime Reporting Portal** so citizens can report any online fraud directly:

cybercrime.gov.in

Official Government Portal



Cyber Crime Related Complaint / Women & Children Related Cybercrime

Cybercrime refers to any unlawful activity carried out using computers, digital devices, or the internet. It includes offenses such as data theft, hacking, online harassment, identity misuse, financial scams, spreading malware, and other acts intended to harm individuals, organizations, or digital infrastructure.

Any victim of financial cyber fraud can dial

📌 **2 Key Facts About the Official Portal:**

1. **Fast Online Complaint:** If any stranger cheats you, you can file a complaint directly on `cybercrime.gov.in`.
2. **Spot the Official Address:** Always check your browser bar to make sure the address ends in `.gov.in`—that is the surest mark of a real government site.

The 3-Step Safe Contact Rule

Never trust unknown numbers shown in SMS, WhatsApp messages, or Google Ads. Always follow this 3-step path:

1. **Open the Real Government Website on Google**

   Type the official URL (like `cybercrime.gov.in`) directly in your browser. Never click unknown message links.

2. **Go to the Official Contact Us Section**

   Open the main menu on the official website and tap 'Contact Us' or 'Helpline'.

3. **Take the Official Number Directly from the Site**

   Call only the verified helpline number displayed right on the official website.

Chapter 1: Do's and Don'ts

✅ Always Do This (DOs)

• The moment you feel fear or pressure on an unknown call, **hang up right away**.

• Before making any decision, talk to your son, daughter, or family members.

• For any bank work, visit your nearest bank branch in person and speak to staff there.

❌ Never Do This (DONTs)

• Never tell anyone the Code (OTP) or UPI PIN shown on your phone screen.

• Never download any new app on your phone just because a stranger on a call told you to.

• Never send money in panic over threats of pension or electricity stopping.

OFFICIAL SOURCES & RULES

• National Cyber Crime Reporting Portal: `cybercrime.gov.in`

• Telecom Department (Sanchar Saathi Portal): `sancharsaathi.gov.in`

• Reserve Bank of India (RBI Senior Citizen Awareness): `rbi.org.in`

CHAPTER 2 • UNDERSTANDING UPI SIMPLY

What Is UPI, in Very Simple Words

No worry about carrying cash: an easy way to send and receive money straight from bank to bank.

How Does Money Move Through a Phone?

Just like a postman delivers your letter to the exact address, **UPI** takes money from your bank and puts it straight into the other person's bank account.

You don't have to stand in bank queues or carry loose cash. Just open a trusted app on your phone like BHIM, Google Pay, PhonePe, or Paytm.

Golden Rule

The Biggest Difference: Receiving vs Sending Money

When you buy fruit or medicines at a shop and pay the shopkeeper, YOU must enter your **UPI PIN**.

But when your son or daughter sends money to your account, you do **NOT have to press any PIN or button**. Money enters your account automatically and your bank sends an SMS.

> **Plain truth:** A PIN is ONLY for money going out. You NEVER enter a PIN to receive money.

Case Study: "I'm Sending Money, Enter Your PIN"

See how scammers try to rob simple elders in the name of sending money:

📞 PHONE CALL SIMULATION (FAKE PAYMENT SENDER)

> **Scammer (acting rushed):** "Oh Chachaji, your son-in-law asked me to send ₹15,000 to your account. I sent a link to your phone—click it and enter your UPI PIN so the money enters your account!"

> **Alert Elder:** "Son, why would I enter a PIN to receive money? My bank taught me that no PIN is needed when money comes in. I won't enter any PIN."

> **Truth:** *(The caller had actually sent a Collect Request to deduct money, not send it! The moment the elder refused, the scammer hung up—and the elder's savings stayed safe.)*

Safe Shopping with UPI: 3 Easy Steps

1 **Scan the Shop's QR Code**

Open your UPI app and hold your phone camera in front of the shopkeeper's QR code.

↓ Check the shop name and amount

2 **Verify Name and Rupees on Screen**

Check that the screen shows the exact amount you owe and the right shopkeeper's name.

↓ Enter your Secret PIN

3 **Type Your UPI PIN to Finish Payment**

Cover the screen with your hand and enter your secret PIN. A green tick (✓) confirms payment.

3 Benefits of UPI & 1 Big Precaution



1. Instant 24-Hour Transfers

Sundays or holidays, UPI works non-stop. Money reaches the other bank account right away.



2. Clear Record of Every Payment

Every payment's date and amount stays recorded inside your app, making it easy to track.



3. Your Bank Details Stay Private

The other person never sees your bank account number or password—only your mobile number or UPI ID.



Biggest Precaution: Never Show Your PIN to Anyone

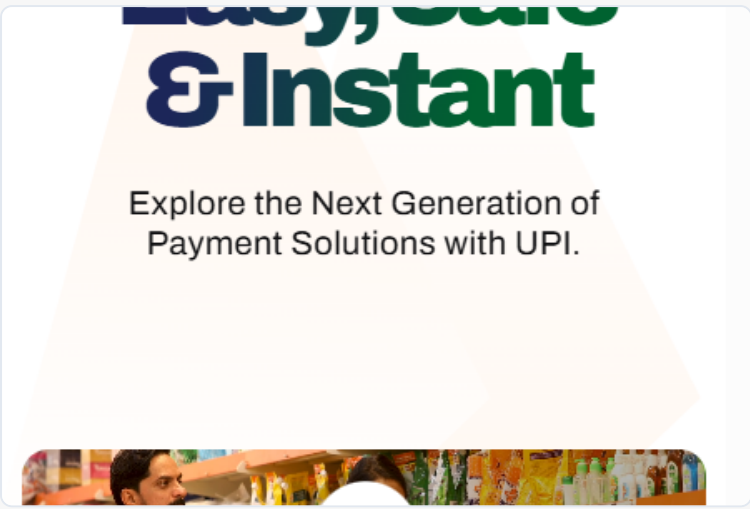
> Just as only you hold the key to your home safe, only you should know your UPI PIN.

Official Portal: Under Government & NPCI Watch

India's entire UPI system runs under the watch of the **National Payments Corporation of India (NPCI)** and the **Reserve Bank of India (RBI)**:

🌐 upichalega.com / npci.org.in (UPI Guide)

Official Organization



📌 **NPCI's Official Advice:**

1. **No PIN to Receive Money:** NPCI clearly states that you never need to enter a UPI PIN when receiving money from anyone.
2. **Use Official Apps Only:** Always download verified bank apps only from Google Play Store or Apple App Store.

The 3-Step Safe Rule to Contact Your Bank

If you ever face a UPI issue, never search Google for customer care numbers. Always follow these 3 steps:

1. **Check the Back of Your ATM Card**
   Your bank's real toll-free number is printed right on every debit card and passbook.
2. **Open Your Bank's Official Website Directly**
   Type your bank's exact official web address directly in your browser bar. Skip ad links.
3. **Take the Number from 'Contact Us'**
   Call only the verified helpline number shown inside your bank's official website.

Chapter 2: Do's and Don'ts

✅ Always Do This (DOs)

• Always double-check the shopkeeper's name and amount on screen before paying.

• Shield the screen with your other hand while typing your UPI PIN.

• Read the SMS from your bank after every payment to confirm it.

❌ Never Do This (DONTs)

• Never enter your UPI PIN to receive money.

• Never unlock your phone or share your PIN just because a stranger asks.

• Never say your UPI PIN or OTP out loud on a phone call.

OFFICIAL SOURCES & RULES

• National Payments Corporation of India (UPI Safety Rules): `npci.org.in`

• Reserve Bank of India (RBI Kehta Hai - UPI Guidelines): `rbi.org.in`

• National Cyber Crime Reporting Portal: `cybercrime.gov.in`

CHAPTER 3 • PROTECTING YOUR DIGITAL KEYS

UPI PIN and OTP: Never Tell Anyone

The key to your safe is in your hands: why telling anyone a code from your phone is the biggest danger.

A Tiny Code That Guards Your Life Savings

Whenever a stranger calls, they speak sweetly and cleverly: *"Uncle ji, a small 6-digit code just came to your phone—just read it out so I can update your pension file."*

Elders wonder what harm one tiny code can do. The truth is, that code is the master lock on your bank account.

Know the Truth

What Is the Difference Between UPI PIN and OTP?

1. UPI PIN: The 4- or 6-digit secret password you create yourself—like the main key to your home safe. It is entered only when sending money.

2. OTP (One Time Password): The temporary 6-digit code your bank sends by SMS. Whenever money is about to leave your account, the bank sends this code to check if it is really you.

> **Plain truth:** Just as you wouldn't hand your house keys to a stranger on the street, never speak your OTP or PIN to anyone.

Case Study: "Your Account Will Be Blocked, Give OTP"

See how scammers use fear to force an OTP out of people:

📞 PHONE CALL SIMULATION (FAKE BANK MANAGER)

> **Scammer (strict, bossy voice):** "I'm calling from State Bank Head Office. Your ATM card will be blocked tonight at 12 AM. Tell me the verification code sent to your phone right now to keep it active!"

> **Alert Parents:** "If there is any issue with my card, I'll visit my bank branch tomorrow morning myself. I will not tell any code on the phone."

> **Scammer (angry):** "If you don't tell me now, a ₹10,000 fine will be charged and your account will never reopen!"

> **Truth:** *(The parents hung up right away. Visiting the bank next morning showed their account was completely safe. The scammer only wanted to steal money using fake fear.)*

The 4-Step OTP Theft Trap

1. **A Sudden Scary Call**

   The scammer claims: "Your debit card stopped", "Power will be cut", or "Money came into your account by mistake."

   ↓ Pretending to help

2. **Saying an SMS Is Coming to Your Phone**

   On their computer, the scammer opens your bank portal and clicks Forgot Password or Money Transfer.

   ↓ Code arrives on your phone screen

3 **Pressuring You in a Rush**

The scammer urges: "Tell me quickly, only 30 seconds left or everything will be shut down!"

↓ Account emptied the moment you share

4 **Money Stolen and Call Cut**

The moment you read out the code, all your money goes to the scammer and their number switches off.

RBI's Clear Rule Every Citizen Must Know



1. No Real Bank Staff Ever Asks for OTP

Under RBI rules, no bank officer has any right to ask a customer for OTP, PIN, or CVV.

> **Rule: Anyone asking for a code or OTP on a call is 100% a fraudster.**



2. The SMS Itself Clearly Prints the Truth

Whenever an OTP arrives, read the full message carefully. It clearly warns: *"Do not share this OTP with anyone for payment of ₹..."*

🤫

3. Always Keep Your PIN Secret

Never write your UPI PIN on your phone cover, inside a diary's first page, or on your passbook.

What to Do If Money Is Deducted or Fraud Happens

If a wrong payment happens by mistake or someone tricks you out of an OTP/PIN, don't panic. Follow these verified steps right away:

🌐 npci.org.in (Official Complaint Guide)

Official Government Body

📌 **3 Easy Actions to Take Immediately:**

1. **Inform Your Bank Fast:** Open your bank's official website, take the real number from Contact Us—or go straight to your nearby branch—and block your account and ATM card immediately.
2. **File a Dispute on NPCI's Official Site:** Type `npci.org.in` directly in your browser. Go to 'UPI Complaint' / 'Dispute' and submit your transaction details.
3. **Report on Cyber Crime Portal:** With a family member's help, file an online complaint at `cybercrime.gov.in` right away so the fraudster's account can be frozen.

The 3-Step Safe Contact Rule

If anyone asks for an OTP on a call, hang up immediately and follow this 3-step path to reach your real bank:

1. **Open the Real Bank Website on Google**
   Type your bank's official URL directly in the browser address bar. Never click links in unknown messages.
2. **Go to the Official Contact Us Section**
   Click 'Contact Us' or 'Customer Care' in the website's main menu.
3. **Take the Official Number Directly from the Site**
   Call only the verified helpline number displayed right on the official website.

Chapter 3: Do's and Don'ts

✅ Always Do This (DOs)

• If anyone asks for any code on a phone call, **hang up immediately** without thinking twice.

• Read every bank SMS calmly and completely.

• If you have any doubt, talk straight to your children or your bank branch staff.

❌ Never Do This (DONTs)

• Never tell anyone your OTP on a phone call, WhatsApp, or SMS.

• Never write down your UPI PIN in a diary or on your phone cover.

• Never follow a stranger's instructions out of rush or fear.

OFFICIAL SOURCES & RULES

• Reserve Bank of India (Customer Protection & OTP Guidelines): `rbi.org.in`

• National Payments Corporation of India (Dispute Redressal): `npci.org.in`

• National Cyber Crime Reporting Portal: `cybercrime.gov.in`

CHAPTER 4 • THE FULL TRUTH ABOUT FAKE CALLS

Fraud Calls: Bank, KYC & Digital Arrest

Fake uniforms, fake courtroom dramas, and threats to lock you in a room: learn how to stay safe.

Police Uniform on Video Call: A Scary Fake Drama

Imagine your father sitting peacefully at home when a video call rings. On screen, a man in a police uniform sits in front of a police station board and an Indian map.

He speaks in a loud, bossy voice: *"A parcel with illegal drugs was found on your Aadhaar card. The Supreme Court issued your arrest warrant. Lock your room door right now, don't talk to anyone, and keep the video call ON!"*

Legal Truth

'Digital Arrest' Is 100% Fake

Under Indian law, there is NO law or rule called **Digital Arrest**. No Police, CBI, or Court in the world ever arrests anyone or runs trials over a video call.

Scammers simply exploit elders' simplicity and fear so they panic and transfer all their bank savings into the fraudster's account.

> **Plain truth:** Whenever someone threatens Police or Court on a video call, don't talk for even 1 second—press the Red Button and hang up right away!

Case Study: Pressure to Lock Yourself in a Room

See how scammers pose as police to trap elders mentally:

📞 VIDEO CALL SIMULATION (FAKE POLICE OFFICER)

> **Scammer (in uniform, harsh voice):** "This is a national security case. If you step outside your room or tell your son, I'll jail your entire family. Transfer all your FDs and bank balance to our RBI Verification Account right now!"

> **Alert Elder:** "If there is an FIR against me, send a written notice to my home address. I will go to the nearest police station myself with my family."

> **Truth:** *(The moment the elder mentioned going to the local police station with family, the scammer cut the video call and vanished. ₹20 lakh of savings stayed safe!)*

The 4-Step Digital Arrest Trap

1 **Courier or SIM Block Excuse**

The scammer claims: "Illegal items were found in a parcel in your name, or your SIM was used in a crime."

↓ Connecting on video call fast

2 **Fake Police Station Studio Set**

The scammer wears a fake uniform, plays wireless radio sounds, and shows stamped fake arrest papers on screen.

↓ Separating you from family

3 **Threatening You to Stay Alone in a Room**

They order: "Keep your camera ON 24 hours; if you tell your children, they'll go to jail too"—leaving zero time to think.

↓ Vanishing once money is sent

4 **Robbing You in the Name of a 'Safe Account'**

They say: "Move all money to this government account until inquiry finishes." Once sent, scammers cut the call.

Real Law vs Fake Call: 3 Biggest Rules

⚖️

1. There Is No Digital Arrest

India's Ministry of Home Affairs has clearly stated: Indian law has zero provision for arrest or inquiry over a video call.

> **Rule:** Listening to "police" on a video call is 100% fake and pointless.



2. Real Police Never Ask for Money

No real police officer ever asks you to transfer money into any account. Anyone asking for money is a criminal.



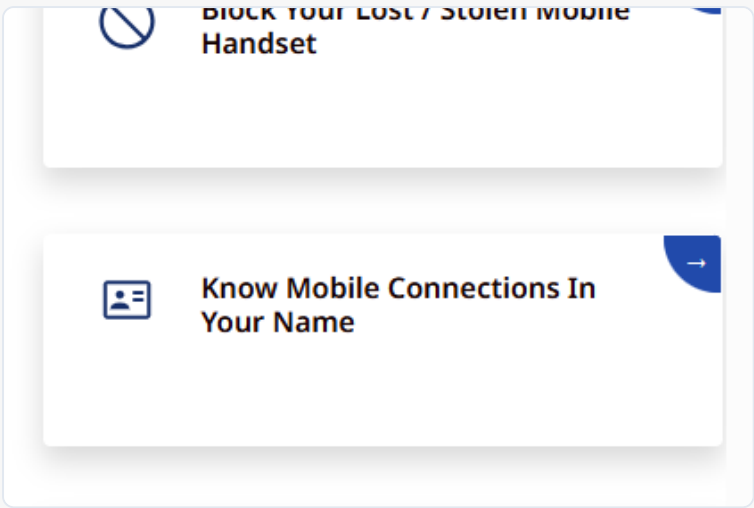
3. A SIM Never Shuts Down in 2 Hours

Telecom Department rules forbid disconnecting any customer's SIM suddenly without proper written notice.

Official Portal: Telecom Department's Citizen Services

The Telecom Department of India built the **Sanchar Saathi** portal to keep citizens safe:

sancharsaathi.gov.in Official Government Portal



📌 **2 Key Facts About the Official Portal:**

1. **Report Fake Calls:** Using the Chakshu option on this portal, you can directly report any fake call or spoofed number.
2. **Check SIMs in Your Name:** Using the TAFCOP option, you can see how many mobile numbers are running on your Aadhaar card.

The 3-Step Safe Contact Rule

If anyone threatens Police or Court on a video call, hang up immediately and follow this 3-step path:

1. **Open the Real Government Website on Google**
   Type the official government portal (like `cybercrime.gov.in` or `sancharsaathi.gov.in`) directly into your browser address bar.
2. **Go to the Official Contact Us Section**
   Open the main menu on the government website and click Contact Us or Help Desk.
3. **Take the Official Number Directly from the Site**
   Call only the verified helpline number shown directly on the official website.

Chapter 4: Do's and Don'ts

✅ Always Do This (DOs)

• Hang up immediately whenever someone threatens Police or Court on a video call.

• Step out of your room right away and tell your son, daughter, or family everything.

• If you still feel scared, go straight to your nearest local police station.

❌ Never Do This (DONTs)

• Never lock yourself alone in a room because a stranger on a call told you to.

• Never transfer even ₹1 to any so-called government or "safe verification" account.

• Never share any code (OTP) on your phone out of fear or rush.

OFFICIAL SOURCES & RULES

• Ministry of Home Affairs (I4C Advisory on Digital Arrest): `cybercrime.gov.in`

• Telecom Department (Sanchar Saathi Portal): `sancharsaathi.gov.in`

• Reserve Bank of India (Caution against Impersonation): `rbi.org.in`

CHAPTER 5 • THE TRUTH ABOUT WHATSAPP MESSAGES

WhatsApp Fraud Messages and Links

Power-cut threats, free gift baits, and dangerous APK files: learn how to spot them easily.

A Blue Link on WhatsApp: A Hidden Trap

Imagine getting a WhatsApp message in the afternoon: *"Electricity Dept Notice: Dear consumer, last month's bill isn't updated. Your home power will be cut tonight at 9:30 PM. Click the link below immediately and pay ₹10!"*

Elders worry that losing power at night in summer will be terrible—and tap the blue link without thinking. That is where the fraud begins.

Spot the Danger

What Happens When You Tap That Link?

Tapping that link does not open the real electricity board—it opens an identical fake website built by scammers.

The moment you enter your bank card or UPI PIN there, all your details go to the scammer—who steals ₹50,000 instead of ₹10.

> **Plain truth:** The electricity board or government offices NEVER send power-cut threats on WhatsApp from an unknown mobile number.

Case Study: The Virus Sent as a Wedding Card (APK Scam)

See how scammers pose as relatives to send dangerous files on WhatsApp:

💬 WHATSAPP CHAT SIMULATION (UNKNOWN NUMBER)

> **Unknown Number (sweetly):** "Pranam Phuphaji, our younger brother's wedding is fixed. Sending the wedding invitation below—please come bless us! 📎 `Wedding_Card.apk`"

> **Alert Elder:** "Wait beta, this is not a photo or PDF—it ends with `.apk`. My son taught me never to install any file like this."

> **Truth:** *(That was no wedding card—it was a dangerous spyware app! Clicking it would have sent all messages and bank OTPs straight to the scammer.)*

The 4-Step WhatsApp Link Scam Trap

1 **Scary or Tempting Message**

A message arrives: "Power will be cut", "You won a ₹25 lakh lottery", or "Get a free ration coupon."

↓ Pressuring you to tap the blue link

2 **Making You Click an Unknown Link**

They urge: "Click this link right away or you'll miss out or face a fine."

↓ Entering bank details in a fake form

3 **Asking for Card Number, PIN, or OTP**

The fake webpage asks for your name, mobile number, debit card, and OTP.

↓ Money stolen and message deleted

4 **Account Emptied and Regret**

The moment you submit details, money vanishes from your bank and the sender blocks you.

3 Biggest Signs of a Fake Message

⚠️

1. Coming from a Normal Mobile Number

Real companies always send SMS from verified sender IDs (like `VM-HDFCBK` or `AD-POWER`), never from a random 10-digit mobile number.

> **Clue:** Any electricity bill message from a 10-digit number is 100% fake.

📎

2. A File Ending in .apk

If a file sent with any message ends in `.apk`, never touch it—it is a dangerous virus.



3. Promises of Free Money and Lotteries

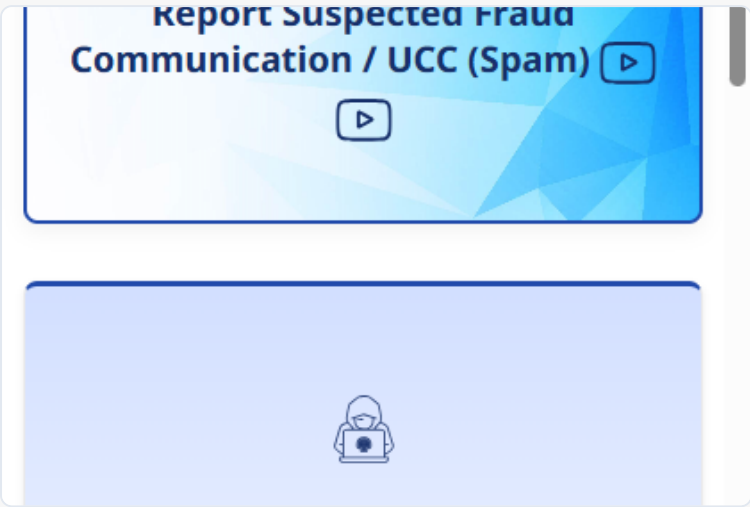
No company or government in the world hands out lotteries or free cash at home for no reason.

Official Portal: Report Fake Messages Directly

If you get a threatening or lottery message on WhatsApp or SMS, report it straight on the government's **Chakshu Portal**:

🌐 sancharsaathi.gov.in/sfc (Chakshu)

Official Government Portal



📌 **2 Big Benefits of Chakshu Portal:**

1. **Blocking the Fraud Number:** Once you report it, the Telecom Department investigates and shuts down the fraudster's number permanently.
2. **Report from Home:** No need to go anywhere—just open the website and submit in 2 minutes.

Checking Electricity Bills or Govt Notices: The 3-Step Rule

Whenever a bill message arrives, never call the number inside the message. Follow this safe path:

1. **Check Your Old Paper Bill**
   Last month's real paper electricity bill at home already prints the correct Consumer Number and Helpline Number.

2. **Open the Electricity Board's Official Website**
   Type the department's official URL directly in your browser address bar—never click unknown links.

3. **Visit the Official Office**
   If you still have any doubt, visit your nearest electricity sub-station or office and confirm face-to-face.

Chapter 5: Do's and Don'ts

✅ Always Do This (DOs)

• Show any bill message to your children at home first.

• Pay electricity or water bills only through trusted official apps.

• Block and report fake WhatsApp messages right away.

❌ Never Do This (DONTs)

• Never click any unknown blue link on WhatsApp.

• Never install any `.apk` file sent by any stranger.

• Never forward any scary or lottery message without checking first.

OFFICIAL SOURCES & RULES

• Telecom Department (Chakshu Suspected Fraud Reporting): `sancharsaathi.gov.in`

• National Cyber Crime Reporting Portal: `cybercrime.gov.in`

• Indian Computer Emergency Response Team (CERT-In Malicious APK Advisory): `cert-in.org.in`

CHAPTER 6 • THE TRUTH ABOUT QR CODES & FAKE PAYMENTS

Fake Payment and QR Scams

The trap of scanning a QR code to 'receive' money, and the truth behind "Sent money by mistake."

"Scan This QR Code to Receive Money" — The Biggest Lie

Imagine posting an old item for sale online, or hearing a relative is sending you some money.

Then a stranger calls, sends a QR code on WhatsApp, and says: *"Uncle ji, I sent you ₹10,000. Scan this QR code with PhonePe or Google Pay and the money will come straight to your account!"*

Golden Rule

Understand the Real Purpose of a QR Code

A QR code does only ONE job—**sending (paying) money out**.

When you buy something at a shop and pay the seller, you scan a QR code and type your PIN. When someone pays YOU, you **neither scan a QR code nor enter a PIN**.

> **Plain truth:** You NEVER have to scan any QR code in the world to receive money. Anyone asking you to scan is 100% a fraudster.

Case Study: "Sent ₹45,000 Extra by Mistake"

See how scammers misuse your kindness to steal money:

📞 PHONE CALL SIMULATION (EMOTIONAL BLACKMAIL)

Scammer (crying, panicked voice): "Uncle ji, I had to send ₹50,000 to someone else, but by mistake it went to your number! You must have got the ₹50,000 SMS too. My mother is in the ICU—please send ₹45,000 back right now or I'm ruined!"

Alert Elder: "Son, first I will open my own bank app and check my real passbook to see if money actually arrived. Without checking my balance, I will not send anything."

Truth: *(When the elder opened his bank app, not even ₹1 had arrived! That SMS was*

> *a fake text generated by scammer software. Being alert saved ₹45,000!)*

The 4-Step QR Scam Trap

1 **Sending a QR Code on WhatsApp**

The scammer says: "I'm sending you advance payment—scan this government QR code."

↓ Pressuring you to scan from gallery

2 **Tapping 'Scan From Gallery'**

The scammer guides: "Open PhonePe or Google Pay and tap 'Upload QR from Gallery'."

↓ Debit amount shows on screen

3 **Tricking You Into Entering Your UPI PIN**

The scammer says: "Yes, now enter your UPI PIN so you can receive the

money."

↓ Money gone the moment PIN is entered

4 **Money Deducted and Call Blocked**

The instant you type your PIN, money leaves your bank to the scammer and their phone shuts off.

The Simple Math of QR Codes: Know When Money Leaves

🛒 **Sending Money (Paying at a Shop):**

Scan shop's QR code → Check amount on screen → **Enter your UPI PIN** → Money leaves your account. (This is normal.)

🛑 **Receiving Money:**

No QR scan → **No PIN needed** → Money arrives straight in your bank. Anyone asking you to scan is trying to **cheat you**!

Fake SMS vs Real Bank Message: 3 Big Differences



1. Check the Sender Header

A real bank message always comes from a 6-letter header (like `AD-SBINB` or `VK-HDFCBK`), never from a normal 10-digit mobile number.



2. Check Balance Inside Your App

Never believe any SMS until you see the money added inside your real bank app or passbook.



3. Refuse Instant Refunds

If someone claims they sent money by mistake, simply say: *"Contact your bank—my bank will handle it automatically."*

The 3-Step Safe Contact Rule

If anyone pressures you to scan a QR code or sends a fake SMS, follow these 3 steps:

1. **Open Your Bank App Immediately**
   Open your phone's official bank app and check 'Account Balance' or 'View Statement'.
2. **Visit Your Bank's Official Website**
   If in doubt, open your bank's official URL directly and check the Contact Us section.

3 **Contact Your Home Bank Branch**

Speak directly to your bank branch manager or trusted staff to confirm your account status.

Chapter 6: Do's and Don'ts

✅ Always Do This (DOs)

• Whenever someone claims they sent money, always check your real balance in your bank app.

• Never trust crying stories from strangers without verifying first.

• Always inform your children at home about any payment dispute.

❌ Never Do This (DONTs)

• Never scan any QR code to receive money.

• Never enter your UPI PIN in PhonePe or Google Pay on anyone's instructions.

• Never send money back just by looking at an SMS on your phone.

OFFICIAL SOURCES & RULES

• National Payments Corporation of India (QR Safety Rules): `npci.org.in`

• Reserve Bank of India (RBI Kehta Hai - QR Code Safety): `rbi.org.in`

• National Cyber Crime Reporting Portal: `cybercrime.gov.in`

CHAPTER 7 • TRUTH ABOUT AI VOICE CLONES

"Son, I'm in Trouble": AI Voice Scams

Fake crying in your loved one's voice, staged accident fears, and sure ways to beat AI voice fraud.

Your Child's Crying Voice on the Phone

Imagine an afternoon call from an unknown number. Picking up, you hear your own son or daughter crying: *"Dad, I made a huge mistake! My car hit someone and police are putting me in lockup. This is the lawyer's number—send ₹60,000 right now or my life is ruined!"*

Hearing their child cry is the hardest moment for any parent. Out of panic, parents get ready to send money right away without checking.

The Tech Truth

What Is AI Voice Cloning?

Computer software (AI) can now listen to just 3 seconds of anyone's voice and build an exact fake clone.

Scammers steal your children's voices from social media (Instagram, Facebook, or YouTube) and make that cloned voice cry and beg.

> **Plain truth:** Never decide it's your child just by the sound of the voice. Before doing anything, call their real saved number back.

Case Study: The Fake "Your Son Is at the Police Station" Call

See how an alert mother exposed the scammer with one secret question:

📞 PHONE CALL SIMULATION (FAKE AI VOICE OF SON)

> **Scammer (exact son's voice + crying):** "Mom, police caught me! My phone broke so I'm calling from a constable's phone. Send ₹40,000 to this UPI right now or they'll take me to court!"

> **Smart Mother (staying calm):** "Beta, first tell me which drawer of your cupboard holds your room key?"

> **Scammer (flustered):** "Mom what nonsense are you asking, I'm in trouble and you're asking about keys!"

> **Truth:** *(Mom realized right away it was a fake voice because her real son knew where the key was. She hung up and called*

her son's real number—he was calmly having lunch at his office!)

The 4-Step AI Voice Scam Trap

1 **Stealing Voice Audio from Social Media**

The scammer saves a voice clip of your son or daughter from Facebook, Instagram, or YouTube.

↓ Creating an identical voice with AI

2 **A Sudden Scary Emergency Call**

They stage an accident, police case, or hospital rush so you get no time to think.

↓ Asking money into a third account

3 **Demanding UPI in a Lawyer's or Doctor's Name**

They claim: "My account isn't working—send money to this lawyer's or policeman's UPI right away."

↓ Number shuts off once paid

4 **Money Stolen and Deep Shock**

The moment money is transferred, the call cuts—and talking to your child later reveals the lie.

3 Sure Ways to Spot an AI Voice Scam



1. Family Secret Code (Secret Question)

Keep a secret question at home whose answer only your family knows (like a childhood nickname or pet's name).



2. Call Back the Real Saved Number Immediately

Hang up on the stranger and call your child's real mobile number directly from your phone's contact list.



3. Never Send Money to Any Third Person

Whenever an unknown "lawyer", "doctor", or "constable" asks for money, never pay without meeting face-to-face.

Official Portal: Report AI & Emergency Frauds

You can report AI voice and emergency frauds directly on India's Cyber Crime Portal:

cybercrime.gov.in

Official Government Portal



Cyber Crime Related Complaint / Women & Children Related Cybercrime

Cybercrime refers to any unlawful activity carried out using computers, digital devices, or the internet. It includes offenses such as data theft, hacking, online harassment, identity misuse, financial scams, spreading malware, and other acts intended to harm individuals, organizations, or digital infrastructure.

Any victim of financial cyber fraud can dial

📌 **2 Key Facts About the Official Portal:**

1. **Golden 2 Hours:** If money was transferred by mistake, report right away on `cybercrime.gov.in` so the scammer's account can be frozen.
2. **Save the Number and Time:** Note down the exact number, date, and time of the fake call.

Checking Emergency Calls: The 3-Step Rule

Whenever someone calls posing as a child or relative in trouble, always follow these 3 steps:

1. **Hang Up Immediately (Don't Panic)**
   The moment you hear scary demands, press the Red Button and end the call.
2. **Call Your Child or Their Friend**
   Open your phone's contact list and call your son, daughter-in-law, or their office colleague directly.
3. **Report the Number on the Government Portal**
   Open your browser, go to `sancharsaathi.gov.in`, and report that fake number on Chakshu.

Chapter 7: Do's and Don'ts

✅ Always Do This (DOs)

• Even if you hear your child crying, stay calm for 10 seconds and take a deep breath.

• Always keep a Family Secret Code or question ready at home.

• Always call back your child's old saved mobile number yourself to check.

❌ Never Do This (DONTs)

• Never transfer money to an unknown UPI ID out of rush or fear.

• Never trust any "lawyer" or "doctor" introduced by an unknown caller.

• Never pay any third person until you speak to your own child directly.

OFFICIAL SOURCES & RULES

• Ministry of Home Affairs (I4C Advisory on AI Voice Cloning Scams): `cybercrime.gov.in`

• Telecom Department (Sanchar Saathi Portal): `sancharsaathi.gov.in`

• Reserve Bank of India (Public Caution on Imposter Scams): `rbi.org.in`

CHAPTER 8 • PROTECTING PENSIONS AND GOVT SCHEMES

Frauds in the Name of Pension & Govt Schemes

Fake Life Certificate excuses, arrears traps, and the truth behind threats to stop your pension over a call.

November Season and Threats to Stop Your Pension

Every November, retired parents submit their Life Certificate (Jeevan Pramaan) so their pension continues smoothly.

Scammers pick this exact season to strike. Someone calls in a serious voice: *"Bauji, I'm calling from the Head Pension Office. Your Life Certificate isn't re-verified. If you don't tell me your Aadhaar OTP by tonight, your pension will stop forever from next month!"*

Government Truth

The Real Rule for Submitting a Life Certificate

The Government of India clearly states that a Life Certificate is NEVER submitted by giving an OTP on an unknown phone call.

There are only 3 legal ways: 1. Biometric thumbprint at your bank branch. 2. Calling your Post Office postman home with a biometric device. 3. Face authentication using the official **Jeevan Pramaan App**.

> **Plain truth:** Anyone calling and asking for a code or OTP to keep your pension running is 100% a scammer.

Case Study: "Your ₹85,000 Arrears Have Been Approved"

See how scammers use fake arrears promises to cheat retired elders:

📞 PHONE CALL SIMULATION (FAKE TREASURY OFFICER)

Scammer (talking like an official clerk): "Pranam Teacher ji, I'm calling from the Finance Treasury. Your ₹85,000 7th Pay Commission arrears have been passed. We'll credit it tomorrow—just deposit ₹1,500 file charge on this government UPI right away!"

Alert Teacher: "Sir, whenever the government pays arrears, it goes straight into the bank account. The government never asks for file charges over a call. I will visit the Treasury Office myself tomorrow."

Truth: *(The moment the teacher mentioned visiting the Treasury Office himself, the scammer hung up! The*

government never asks citizens for advance fees to release pensions or arrears.)

The 4-Step Pension Scam Trap

1 **A Sudden Scary Call**

The scammer claims: "Your PPO number and Aadhaar don't match—your pension will stop."

↓ Offering to fix it from home

2 **Saying an SMS Is Coming to Your Phone**

On their computer, the scammer opens an Aadhaar or bank portal and triggers a login OTP.

↓ Asking for Aadhaar or Bank OTP

3 **Heavy Pressure to Share the Code**

The scammer warns: "Tell me fast, the server is open for only 2 minutes or

you'll lose your pension!"

↓ Account emptied and number blocked

4 **All Pension Savings Stolen**

The moment you share the OTP, your life savings leave the account and the scammer disappears.

Real Govt Rules vs Fake Pension Calls



1. No Government Office Asks for OTP on Phone

India's Pension Department clearly directs that no pensioner will ever be asked for Aadhaar or bank OTPs over a phone call.



2. No Advance Fee for Arrears

All pension and DA arrears go straight into your bank account. There is zero rule for file charges or processing fees.



3. The Postman Comes Home to Help

Under India Post Payments Bank (IPPB), a postman visits your home for a tiny official fee to submit your Digital Life Certificate via biometric machine.

Official Portal: Real Govt Website for Life Certificate

The **Jeevan Pramaan** portal run by India's Ministry of Electronics & IT:

jeevanpramaan.gov.in Official Government Portal



📌 **Key Rules for Jeevan Pramaan Portal:**

1. **Use the Official App Only:** Download the official app or Face App only from `jeevanpramaan.gov.in`.
2. **Check the Government Domain:** Always make sure your browser shows `jeevanpramaan.gov.in`. Never trust private links.

The 3-Step Rule to Solve Any Pension Issue

If anyone threatens over a call that your pension will stop, never panic. Follow these 3 safe steps:

1. **Visit Your Bank Branch Directly**
   Go straight to the bank branch where your pension arrives and talk to the pension desk officer.
2. **Open the Jeevan Pramaan Website**
   Type `jeevanpramaan.gov.in` directly in your browser address bar to check nearby centers.
3. **Use the Postman Service**
   Contact your nearest Post Office to request a postman home visit for biometric Life Certificate.

Chapter 8: Do's and Don'ts

✅ Always Do This (DOs)

• Submit your Life Certificate yourself every November at your bank branch or Post Office.

• Ask any pension or arrears question directly at your Treasury or bank.

• Let your children help store your PPO number and bank passbook details safely.

❌ Never Do This (DONTs)

• Never share any Aadhaar OTP or bank code on a phone call.

• Never send fees to any unknown account to release stuck arrears.

• Never tap any unknown pension scheme link received on WhatsApp.

OFFICIAL SOURCES & RULES

- Department of Pension & Pensioners' Welfare: `pensionersportal.gov.in`
- Jeevan Pramaan Official Portal: `jeevanpramaan.gov.in`
- National Cyber Crime Reporting Portal: `cybercrime.gov.in`

CHAPTER 9 • FRAUDS DISGUISED AS FAMILY TIES

Asking for Money Pretending to Be a Relative

The sweet "Recognized me, Bauji?" trap and safety rules beyond hesitation or politeness.

"Guess Who Is Speaking?" — The Very First Trap

Imagine an unknown number calling with super warm affection: *"Namaste Mamaji, Charan Sparsh! Recognized me? Come on, tell me who is speaking!"*

Out of politeness, elders feel shy saying they don't recognize the voice—and guess from memory: *"Oh Amit beta, is that you?"*

The scammer was waiting for that exact name: *"Yes Mamaji, you guessed right! My phone was stolen, so I'm calling from this new number."*

Understand the Trick

Why Do Scammers Pose as Relatives?

Scammers know elders in our culture feel awkward questioning a son-in-law or nephew tightly about money.

They misuse that warmth—claiming they're stuck at a hospital or police check and asking for ₹25,000 right away on a stranger's UPI.

> **Plain truth:** When a stranger calls without giving their own name and makes you guess, be sure they could be a fraudster.

Case Study: "Your Son-in-Law Is at the Hospital"

See how an alert father-in-law exposed the fraud with one question:

📞 PHONE CALL SIMULATION (FAKE SON-IN-LAW)

Scammer (panicked voice): "Papaji, it's your son-in-law. Police stopped my car and are seizing it. Send ₹15,000 to this constable's UPI right now—I'll pay you back when I get home!"

Smart Father-in-Law: "Okay son, first tell me which city your mother-in-law's parents come from?"

Scammer (irritated): "Papaji, police are catching me here and you're asking about hometowns! Send the money fast!"

Truth: *(He hung up immediately and called his daughter—his son-in-law was peacefully*

> *having tea at home! Being alert saved ₹15,000.)*

The 4-Step Fake Relative Trap

1 **Making You Guess**

The scammer asks: "Guess who I am?" so you yourself speak a relative's name.

↓ Claiming a new number

2 **Excuse of Lost Phone or SIM**

They say: "My old phone fell and broke—this is my new personal number, save it."

↓ Sudden demand for money

3 **Fake Hospital or Police Fear**

They urge: "I'm stuck on the road, don't tell anyone—send ₹20,000 to this UPI right now."

↓ Number shuts off once paid

4

Money Gone and Regret

The moment you pay, that number shuts off forever—and your real relative knows nothing about it.

3 Biggest Rules to Spot Fake Relatives



1. Never Guess a Name Yourself

When someone says "Recognize me?", say plainly: *"I can't place your voice—tell me your full name and your father's name."*

📖

2. Call Back the Old Saved Number Yourself

Don't trust a new-number story. Hang up and call that relative's real number saved in your phonebook.

👨‍👩‍👧

3. Hand the Phone to Someone Else at Home

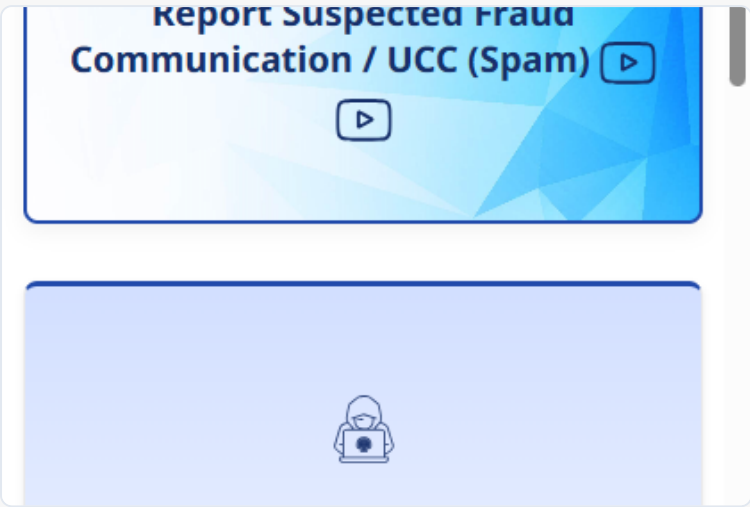
The moment money comes up, say: *"Wait, I'm giving the phone to my son or daughter-in-law—talk to them."* The scammer will hang up instantly.

Official Portal: Report Unknown & Fake Numbers

If any stranger tries to cheat you pretending to be a relative, report them on the Telecom Department's **Chakshu Portal**:

🌐 sancharsaathi.gov.in/sfc (Chakshu)

Official Government Portal



📌 **Benefits of Reporting on Chakshu Portal:**

1. **Nationwide Number Block:** Your single report helps the Telecom Department shut down that fraud number permanently.
2. **Protecting Other Elders:** That fraudster won't be able to target elders in another family.

The 3-Step Relative Verification Rule

Whenever someone on an unknown number claims to be a relative asking for money, follow these 3 steps:

1. **Hang Up Immediately**
   Don't fall for rushed talk—press the Red Button and cut the call.
2. **Call the Old Saved Family Number**
   Call that relative's or their parents' real saved number from your own phone diary.
3. **Tell Your Children Everything**
   Before ever sending money, tell your son or daughter the full story and confirm.

Chapter 9: Do's and Don'ts

✅ Always Do This (DOs)

• Never guess a relative's name on an unknown call.

• Ask the caller an old private family question.

• Always call back that relative's old saved mobile number.

❌ Never Do This (DONTs)

• Never send money to an unknown number out of shyness or politeness.

• Never send money to an unknown shopkeeper's or constable's UPI on someone's call.

• Never promise secret financial help without telling your family.

OFFICIAL SOURCES & RULES

• Telecom Department (Chakshu Suspected Fraud Reporting): `sancharsaathi.gov.in`

• National Cyber Crime Reporting Portal: `cybercrime.gov.in`

• Reserve Bank of India (Advisory on Impersonation Scams): `rbi.org.in`

CHAPTER 10 • SAFETY AT ATMS AND BANKS

Strangers Offering "Let Me Help You"

The truth about helpful strangers outside ATMs, sleight-of-hand card swapping, and PIN theft.

The Polite Young Man Inside the ATM

Imagine your father going to an ATM to withdraw cash. His eyesight is slightly weak and he struggles with the buttons. A well-dressed, sweet-spoken young man standing behind steps up:

"Give it to me Uncle ji, why struggle? Let me insert your card—you just type your PIN and the cash will come right out."

Touched by his polite manners, the elder hands over his card. That's where the entire trap begins.

Sleight of Hand

What Is Card Swapping?

The young man pretends to insert your card —but smoothly pockets your real card and hands you back a useless expired card from the same bank.

When you type your PIN on screen, he watches your fingers from behind and memorizes it. Then he says: *"Uncle ji this machine is out of cash, try the next ATM."*

> **Plain truth:** The moment you step out, he uses your real card and your PIN to withdraw all your cash.

Case Study: Fake Help at the Machine

See how accepting a stranger's help wiped out an account:

🏦 BANK BRANCH SIMULATION (FAKE HELPER)

> **Stranger (respectfully):** "Bauji, this machine keeps rejecting your card. Let me wipe it and insert it properly. Just tell me your 4-digit code, I'll type it in."

> **Simple Elder:** "Yes son, my eyesight is weak—the code is 4-2-8-0."

> **Truth:** *(The boy pocketed the real card, returned a fake one, and withdrew all ₹40,000 of the elder's pension from a nearby ATM within 10 minutes!)*

The 4-Step Card Swapping Trap

1. **Sweet Offer to Help**

   A young man steps forward politely seeing the elder hesitate at the ATM.

   ↓ Taking your card in hand

2 **Swapping the Card by Sleight of Hand**

He hides your real debit card in his palm and hands back a useless card of the same color.

↓ Peeking over your shoulder

3 **Shoulder Surfing (Memorizing Your PIN)**

As the elder presses keys, he watches the finger movement from behind and memorizes the 4-digit PIN.

↓ Blaming a broken machine

4 **Withdrawing Cash with Your Real Card**

Once the elder leaves the ATM, he steals cash immediately using the real card and PIN.

The 3-Point Shield for Safe ATM Use

1. Cover the Keypad with Your Other Hand

Whenever typing your PIN, form a shield over the keypad with your free hand so neither a person nor a hidden camera can see it.

2. Never Let Anyone Touch Your Card

Insert your debit card only with your own hand and put it straight back into your pocket. Never let a stranger touch it.

3. Always Check Your Own Name on the Card

Before leaving the ATM, read your printed name on the card to make sure it is truly yours.

3 Safe Rules When You Need Help



1. Ask Only the Uniformed Security Guard

Never ask another customer inside the ATM cabin—ask only the uniformed bank guard outside.



2. Withdraw Cash at the Bank Counter

If an ATM feels confusing, walk inside the bank branch, fill out a withdrawal slip, and take cash directly from the cashier.



3. Always Take Your Children Along

Whenever elders need to withdraw a large sum, take your son, daughter, or a trusted family member along.

3-Step Rule If Your Card Is Swapped or Stuck

If you ever suspect your card was swapped or got stuck in the machine, act fast:

1. **Block Your Card Immediately**
   Open your bank app and tap 'Block Debit Card' right away so nobody can withdraw money.
2. **Call the Toll-Free Number on Your Passbook**

Immediately call the official helpline printed on the first page of your bank passbook.

3 **Submit a Written Complaint at the Branch**

Visit your bank branch right away and inform the manager so CCTV footage can be checked.

Chapter 10: Do's and Don'ts

✅ Always Do This (DOs)

• Always cover the keypad from above with your other hand while entering your PIN.

• Always read your name on the card before walking out of the ATM.

• Always press the red 'Cancel' button after finishing your transaction.

❌ Never Do This (DONTs)

• Never hand your ATM card to any stranger.

• Never speak your 4-digit secret PIN out loud to anyone.

• Never try to withdraw cash while another stranger is standing inside the ATM cabin.

OFFICIAL SOURCES & RULES

- Reserve Bank of India (Safe ATM Usage Guidelines): `rbi.org.in`
- Indian Banks' Association (ATM Safety Best Practices): `iba.org.in`
- National Cyber Crime Reporting Portal: `cybercrime.gov.in`

CHAPTER 11 • THE 10-SECOND SAFETY PAUSE

Always Ask Yourself Before Sending Money

Never decide in a rush: the 10-second pause and 3 questions that stop every fraud.

A Scammer's Biggest Weapon: Rush and Fear

Notice that whenever a stranger calls, they NEVER say *"Take your time and tell me calmly tomorrow."* They always say: *"You only have 5 minutes—press the button now or pay a huge fine!"*

Scammers do this because they know if you pause calmly for even 1 minute or ask your children, their lie gets caught right away.

Golden Rule

The 10-Second Pause Rule

Whenever someone on a call scares you, tempts you, or demands urgent money, take your finger off the phone screen right away.

Take a deep breath and pause for 10 seconds. Tell the caller clearly: **"I'm busy right now, I'll talk after 10 minutes."** and hang up.

> **Plain truth:** No real work in the world is ruined by pausing 10 seconds—but 10 seconds of panic can wipe out a lifetime of savings.

Case Study: Pausing 10 Seconds Saved Life Savings

See how one tiny pause stopped a ₹2 lakh fraud:

📞 PHONE CALL SIMULATION (HIGH PRESSURE TRAP)

Scammer (shouting): "Bauji, only 2 minutes left before your pension stops! Tell me the 6-digit code on your screen right now or your file closes!"

Alert Elder (stopping his hand, calm voice): "Son, I'm in no rush. If my pension stops, I'll visit my bank branch myself tomorrow. I will not tell any code over the phone."

Truth: *(Frustrated, the scammer hung up. When the elder told his son, they found the pension was completely fine. 10 seconds of patience saved ₹2 lakh!)*

The 4-Step Cycle of the 10-Second Family Shield

1 **Take Your Finger Off the Screen**

The moment you hear urgency, stop tapping any button or typing any code.

↓ Take a deep breath

2 **Press the Red Button and Hang Up**

Don't listen to threats or crying dramas—just cut the call.

↓ Step out of your room

3 **Tell Your Children Everything**

Show your son, daughter, or family what call or message came on your phone.

↓ Safe decision

4 **Your Money and Peace Stay Safe**

With family's help, the truth becomes clear and the fraud number gets blocked.

3 Questions to Ask Yourself Before Sending Money

Question 1: Have I Met This Person Face-to-Face?

If the person is talking only on phone, WhatsApp, or internet—never send even ₹1.

Question 2: Do You Need a PIN to Receive Money?

Answer: Never! Anyone asking you to enter a UPI PIN to receive money is 100% lying.

Question 3: Have I Told My Family About This?

Never pay money to any stranger's account until you have told your children at home.

Haste vs Wisdom



Scammers Always Set Fake Deadlines

They say: "Power cuts in 10 minutes", "Give OTP now", "Offer ends in 2 minutes." That's just a trick to freeze your thinking.



Real Banks & Govt Offices Always Give Time

Every genuine bank, electricity board, or government office gives weeks of notice in writing—never rushing you on a call.

The 3-Step Safe Contact Rule

Whenever anyone pressures you to hurry on a call, follow this 3-step safety rule:

1. **Press the Phone's Red Button**
   Without listening further, cut the call right away and put the phone down.
2. **Call Out to a Family Member**
   Call your son, daughter-in-law, or daughter and tell them what call came.
3. **Get the Number from the Bank's Official Website**
   For any bank matter, talk only on the number printed on your passbook or verified on your bank's official website.

Chapter 11: Do's and Don'ts

✅ Always Do This (DOs)

• Make it a habit to pause 10 seconds on every unknown call.

• Always ask your children before taking any big step.

• Visit your nearest bank branch in person whenever you feel unsure.

❌ Never Do This (DONTs)

• Never tell any code on a phone call out of rush or fear.

• Never send money in haste on any stranger's instructions.

• Never decide alone when someone says "Don't tell anyone."

OFFICIAL SOURCES & RULES

• Reserve Bank of India (Public Awareness on Financial Frauds): `rbi.org.in`

• National Cyber Crime Reporting Portal: `cybercrime.gov.in`

• Telecom Department (Sanchar Saathi Portal): `sancharsaathi.gov.in`

CHAPTER 12 • RIGHT STEPS DURING A CRISIS

What to Do If Fraud Happens

Don't panic if money is cut: understand the Golden 2 Hours and how to save your funds.

Never Blame Yourself or Your Parents If Tricked

Even if money leaves your account due to a scary call or trick, remember first—**do not panic and do not harm your health**.

Scammers are extremely cunning—they even fool senior officers and young engineers. Instead of hiding it out of fear, acting fast gives the best chance of getting money back.

Essential Rule

The Power of the First 2 Hours (Golden Hours)

When money leaves your account, the scammer doesn't pocket it instantly—they bounce it through 3–4 bank accounts to hide it.

If you report to your bank and the government Cyber Crime Portal within the first 2 hours, the law allows officers to **Freeze** that money on the way.

> **Plain truth:** Hiding a fraud never brings money back. Tell your children immediately and file a complaint.

Case Study: Fast Action in 30 Minutes Recovered ₹60,000

See how acting fast saved stuck money:

RECOVERY SIMULATION (QUICK ACTION)

Incident: An elder lost ₹60,000 in a fake electricity bill trick and started trembling seeing the debit SMS.

Smart Choice: Instead of hiding it, he called out to his son immediately. Without scolding, the son opened the bank app and blocked the debit card and Net Banking right away.

Truth: *(Within 25 minutes, the son filed an online complaint on `cybercrime.gov.in`. Cyber Cell froze the receiving account immediately, and all ₹60,000 returned safely in 5 days!)*

Immediate 4-Step Action Plan If Fraud Happens

1 **Freeze Bank Account & Card Immediately**

Use your bank app or official bank helpline to block your debit card, UPI, and Net Banking right away.

↓ Save transaction evidence

2 **Screenshot the SMS and UTR Number**

Save screenshots of the debit message, the 12-digit UTR number, the fraudster's phone number, and the time.

↓ Report on the government portal

3 **Report on Cyber Crime Portal**

Open `cybercrime.gov.in` directly, go to 'Report Financial Fraud', and enter full details.

↓ Visit your local bank branch

4 **Submit Receipt at Your Bank Branch**

Hand in a written letter at your bank branch along with the Cyber Portal complaint (Acknowledgement) number.

RBI's Customer Protection Rule (Zero Liability Rule)



1. Full Protection When Reported Within 3 Days

Under RBI rules, if an online fraud or unauthorized transaction is reported to your bank within 3 days, the customer has Zero Liability.



2. The Faster You Report, the Safer Your Money

Reporting fast lets banks and Cyber Cell stop the money before the scammer withdraws it from an ATM.



3. Family Support Is the Greatest Strength

Your parents' health and dignity matter far more than money. Give them love and courage if a loss ever happens.

Official Portal: Immediate Online Fraud Reporting

The Government of India's **National Cyber Crime Reporting Portal** works 24/7 to protect citizens' money:

cybercrime.gov.in

Official Government Portal



Cyber Crime Related Complaint / Women & Children Related Cybercrime

Cybercrime refers to any unlawful activity carried out using computers, digital devices, or the internet. It includes offenses such as data theft, hacking, online harassment, identity misuse, financial scams, spreading malware, and other acts intended to harm individuals, organizations, or digital infrastructure.

Any victim of financial cyber fraud can dial

📌 **2 Key Points About Reporting on the Portal:**

1. **Citizen Financial Cyber Fraud Reporting System:** Connected directly to all banks and payment apps to hold stolen funds quickly.
2. **Written Complaint Receipt:** You get a complaint number right away to submit at your bank branch.

The 3-Step Rule to Contact Banks & Government

If fraud happens, never call unknown numbers from Google Search. Follow this safe path:

1. **Check the Back of Your Passbook or Debit Card**
   Call the official helpline printed on the back of your bank card to block it immediately.
2. **Go Straight to the Government Website**
   Type `cybercrime.gov.in` directly in your browser address bar and check Contact Us.
3. **Visit Your Nearest Police Cyber Cell**
   Submit a written complaint at your city's main police station and collect an acknowledgment slip.

Chapter 12: Do's and Don'ts

✅ Always Do This (DOs)

• Tell your children at home right away if money is ever deducted.

• Report to your bank and on `cybercrime.gov.in` within the first 2 hours.

• Keep screenshots of the debit SMS and 12-digit UTR number safely.

❌ Never Do This (DONTs)

• Never hide a loss from family out of fear or shame.

• Never fall for "Tell me another OTP to get your refund back."

• Never make the mistake of searching Google for unknown customer care numbers.

OFFICIAL SOURCES & RULES

• Ministry of Home Affairs (National Cyber Crime Reporting Portal): `cybercrime.gov.in`

• Reserve Bank of India (Customer Protection - Limiting Liability): `rbi.org.in`

• Telecom Department (Chakshu Portal): `sancharsaathi.gov.in`

CHAPTER 13 • SPECIAL GUIDE FOR FAMILY & CHILDREN

For Family Members: How to Teach Parents

How to give your parents a digital shield with love and patience—not scolding or irritation.

We Buy Them a New Phone, But Forget to Teach Safety

Most of us gift our parents a new smartphone on birthdays or retirement—forgetting that technology we grew up with feels completely new and strange to them.

When they accidentally tap a link or get stuck in a setting, many children snap: *"You never understand anything—why did you touch the phone!"*

Remember: our anger scares our parents. Next time a scammer threatens them, they hide it out of fear of being scolded—and suffer a huge loss.

The Rule of Empathy

The Art of Teaching with Love and Respect

When we were kids learning to hold a spoon or ride a bicycle, our parents picked us up lovingly even after a hundred falls.

Today, as they learn to ride the new bicycle of technology, they need that exact same patience and warmth from us.

> **Plain truth:** Build such a safe home atmosphere that your parents call you right away after any unknown call—without any fear.

Case Study: 15 Minutes of Kind Talk Instead of Scolding

See how a thoughtful daughter made her mother's phone completely safe:

❤️ **FAMILY SIMULATION (SUPPORTIVE CHILD)**

> **Daughter (holding mom's hand warmly):** "Mom, from tomorrow there's one new rule on your phone. Whenever an unknown call comes or scares you, just do one thing—cut the call and call me. Even if I'm in the office, I will never get angry with you."

> **Mother (relieved):** "Beta, I used to worry you'd get annoyed if I asked small things. Now I'm not scared anymore."

> **Truth:** *(The daughter set a ₹3,000 daily UPI limit on mom's phone and added a Play Store password. Ten days later, when a fake*

electricity call came, mom cut it fearlessly and told her daughter!)

Do These 4 Settings on Your Parents' Phone Today

1 **Lower the Daily UPI Limit**

In their bank app or Google Pay, set the daily transaction limit between ₹2,000 and ₹5,000.

↓ Protection from unknown apps

2 **Put a Password on Play Store**

In Google Play Store Settings, turn on 'Parental Controls' or 'Require Authentication for Purchases'.

↓ Turning on spam call filter

3 **Turn On Spam Call Blocker**

In the phone's Calling Settings, turn on 'Caller ID & Spam Protection' to spot

fake calls early.

↓ Comfort for the eyes

4 **Increase Font Size**

In Display Settings, set Font Size and Display Size to 'Large' so every message is crystal clear.

The 3-Point Family Shield to Keep at Home

1. Promise "You Can Ask Me Anytime"

Remind your parents daily that asking questions about technology is nothing to feel shy about.

2. Avoid Heavy English Jargon

Instead of hard words like Authentication or Phishing, explain simply as "your phone's secret key" or "a fishing bait".

3. Stick the Safety Card on the TV or Fridge

Write the next chapter's Safety Checklist in large print on paper and stick it where they see it daily.

Harm of Scolding vs Benefit of Kind Teaching



What Happens When You Scold?

Elders feel helpless and lonely. Out of fear, they hide future problems from their children —leading to big losses.



What Happens When You Teach Kindly?

Parents gain confidence. The moment any strange call or message arrives, they show it to their children and the scammer fails.

The 3-Step Weekly Rule for Children

Take just 10 minutes every Saturday or Sunday for this 3-step habit:

1. **Check Apps on Your Parents' Phone**
   Check that no unknown screen sharing app (like AnyDesk or QuickSupport) got installed by mistake.

2. **Review Bank Statement & Balance**
   Open the bank app's 1-month Mini Statement to spot any strange small or large deductions.

3. **Ask Lovingly If Anything Bothered Them**
   Ask: "Dad, did any unknown number call with a scary story or pension message this week?"

Chapter 13: Do's and Don'ts

✅ Always Do This (DOs)

• Keep a low daily UPI limit and Spam Protection turned on in your parents' phone.

• Answer every tech question from them calmly and with a smile.

• Sit with them once a week to check their phone's safety together.

❌ Never Do This (DONTs)

• Never yell at or taunt your parents when they make a mistake.

• Never make them feel they are too old to learn technology.

• Never leave them to make big financial decisions alone without safety settings.

OFFICIAL SOURCES & RULES

• Ministry of Home Affairs (Cyber Hygiene Guidelines for Seniors): `cybercrime.gov.in`

• Reserve Bank of India (Financial Literacy for Senior Citizens): `rbi.org.in`

• Telecom Department (Sanchar Saathi Citizen Safety): `sancharsaathi.gov.in`

CHAPTER 14 • 1-PAGE MASTER CHECKLIST

Elders' Safety Checklist

The essence of the entire book: 6 golden rules that keep every parent safe for life.

6 Biggest Rules to Remember

For parents and senior citizens, these 6 rules act like an unbreakable shield. Remember them daily or print and stick them in your room:

✓

1. No PIN Needed to Receive Money

A UPI PIN is ONLY for sending (deducting) money. You never enter any PIN in the world to receive money.

✓

2. Never Give Anyone Any Phone Code (OTP)

No matter how senior an officer or bank manager someone claims to be, never read out a 6-digit code from your phone.

✓

3. Hang Up Immediately If You See Police on Video Call

There is no arrest or inquiry on video call under law. The moment you see a uniform on video call, press the Red Button.

✓

4. Never Touch Unknown Blue Links or Files

Never tap any unknown file or link on WhatsApp disguised as an electricity bill, lottery, or wedding card.

✓

5. Visit Your Bank Branch Directly for Pension or Bank Work

For Life Certificates or any bank work, go straight to your bank branch or Post Office instead of doing it over a call.

6. Pause 10 Seconds and Tell Your Children

No matter how much someone scares or tempts you, pause 10 seconds, step out of your room, and show your son or daughter.

The 3-Step Rule to Contact Bank or Government

If any trouble ever happens, instead of searching Google for unknown numbers, always follow these 3 steps:

1. **Open the Real Government Website on Google**

   Type `cybercrime.gov.in` or `sancharsaathi.gov.in` directly into

your browser address bar.

2. **Go to the Official Contact Us Section**
   Open the website's main menu and click Contact Us or Helpline.

3. **Take the Official Number Directly from the Site**
   Call only the verified helpline number displayed right on the official website.

Final Takeaway: Do's and Don'ts

✅ Always Do This (DOs)

• Stay calm on every unknown call and pause 10 seconds to think.

• Talk to your family before taking any new action.

• Print this checklist and stick it in your room.

❌ Never Do This (DONTs)

• Never enter your UPI PIN or OTP on a stranger's instructions.

• Never transfer money to an unknown account out of fear or rush.

• Never hide any phone incident from your family.

OFFICIAL SOURCES & RULES

- National Cyber Crime Reporting Portal: `cybercrime.gov.in`
- Telecom Department (Sanchar Saathi Portal): `sancharsaathi.gov.in`
- Reserve Bank of India (Senior Citizen Financial Safety): `rbi.org.in`

SENIOR SAFETY GLOSSARY

Essential Digital Words for Elders

UPI PIN (PIN Number)

Your 4- or 6-digit secret password. It is entered **ONLY to send (deduct) money**—never needed to receive money.

OTP (One Time Password) (One Time Password)

A temporary code sent by SMS from your bank. Never share it with anyone on a phone call—even if they claim to be a bank manager or police.

QR Code (QR Code)

A square black-and-white box code. Scanning it always means **sending money**. You never scan a QR code to receive money.

Digital Arrest (Digital Arrest)

A fake police station drama staged by scammers on video call to scare you. **There is NO law called Digital Arrest**.

AI Voice Clone (Fake Voice)

Computer software copying your son's, daughter's, or grandchild's voice to demand accident money. Hang up right away and call their old number.

Screen Share App (AnyDesk / TeamViewer)

An app that lets a stranger watch your entire phone screen live and empty your bank account. Never install it.

Life Certificate (Jeevan Pramaan) (Pension Verification)

The yearly certificate submitted to keep your pension running. Done only at a bank branch, Post Office, or official govt app—never on an unknown call.

Senior Cyber Safety Pledge

4 Unbreakable Safety Rules for Parents

Every elder at home should always remember these 4 points:

1. **No PIN Needed to Receive Money:**
   You never need any PIN or OTP for money to enter your account.
2. **No Arrest on Video Call:**
   Real police never do Digital Arrest over a video call.
3. **Hang Up on Emergency Calls:**
   If told a child or relative had an accident, call their old saved number first.
4. **Never Install Apps on Calls:**
   Never download AnyDesk or screen sharing apps on an unknown call.

✓ 14 Easy Chapters | ✓ Senior-Friendly Large Print | ✓ 100% Free Citizen Protection

Safe Contact Rule: Instead of searching Google for any Bank, Pension Office, or Police number, open their official website directly and take it from the Contact Us section.

National Cyber Safety Awareness Series • 2026 Edition

Mobile Pocket Format (120mm × 190mm)