Based on RBI, NPCI & Government Rules

LATEST 2026 EDITION

UPI Safety Guide

A complete, easy pocket guide for everyday UPI users to stay safe from payment scams

13	100%	4
Detailed Chapters	Verified Rules	Pocket Checklists

Safe Digital Payments • Alert Citizens • Secure India

LEGAL NOTICE • TERMS & LICENSE

Legal Disclaimer & Terms of Use

1. Educational & Public Awareness Purpose

This eBook is an independent educational guide created solely to enhance digital financial literacy and cybersecurity awareness among citizens and merchants. Its goal is to teach safe practices for conducting UPI transactions. It does not constitute legal or financial advice.

2. Non-Affiliation with Official Authorities

This publication is not endorsed, sponsored, authorized, or affiliated with the Reserve Bank of India (RBI), National Payments Corporation of India (NPCI), the Government of India, or any commercial bank or payment app provider (such as PhonePe, Google Pay, or Paytm).

3. Complete Limitation of Liability

While all advice and instructions are compiled from public regulatory frameworks and official circulars of RBI and NPCI, the publisher and author bear no liability for any individual financial transactions, technical failures, cyber fraud, or monetary losses. Readers must verify with their respective bank's official channels.

4. Nominative Fair Use of Trademarks

'UPI', 'BHIM', and 'NPCI' are registered trademarks of NPCI. All other brand names, logos, or app names mentioned (such as Google Pay, PhonePe, Paytm, SBI, HDFC, WhatsApp, etc.) are the property of their respective owners, used solely under nominative fair use for identification and awareness.

5. Fictional Scenarios & Tactics (No Real Names)

All examples and case studies in this guide are illustrative with fictional names to explain scam patterns. No real person, merchant, or institution is depicted as fraudulent; the text focuses exclusively on exposing deceptive techniques.

6. Single-User Digital Product License

This eBook is licensed exclusively for personal use by the individual purchaser. Any unauthorized reproduction, commercial distribution, public re-uploading, resale, or file-sharing of this document, in whole or in part, is strictly prohibited by law.

© 2026 All Rights Reserved • An Independent Guide Based on Official Public Guidelines

EDITORIAL • PREFACE

Why You Need This UPI Safety Guide

Today in India, more than **400 million (40 crore)** UPI transactions take place every single day. From street vendors and local grocery stores to major retail outlets, UPI has transformed everyday commerce into a fast, effortless, and cashless experience.

Yet this unprecedented convenience has brought an aggressive wave of digital deception. Everyday headlines describe seniors losing their hard-earned pension with a single tapped link, or young job seekers being robbed under the illusion of work-from-home tasks and instant cashbacks.

> Cyber fraudsters rarely hack bank mainframe computers. They hack **human psychology** — exploiting urgency, fear, confusion, or greed so that victims hand over their own secret PIN or OTP willingly.

Almost every UPI fraud succeeds because people miss 2 or 3 fundamental rules. The most vital rule remains unknown to millions: *"You NEVER need to enter a UPI PIN or share an OTP to receive money or refunds."*

The Purpose of This Book:

This guide avoids complicated technical jargon. Written in **clear, everyday English**, it walks you through 13 practical chapters featuring real-life case studies, official screenshots, and verified rules established by the Reserve Bank of India (RBI) and the National Payments Corporation of India (NPCI).

> Read this handbook carefully, and share its lessons with your parents, elders, shop staff, and children. Just ten seconds of calm vigilance is your family's strongest shield against cyber crime.

CONTENTS • TABLE OF CONTENTS

Table of Contents

1. **Chapter 1: Understanding UPI & Basics**
   How UPI works, Two-Factor Authentication, and the flow of bank-to-bank money
2. **Chapter 2: UPI & Your Bank Account**
   RBI Zero Liability framework, 3-day reporting deadline, and customer rights
3. **Chapter 3: Protecting Your UPI PIN**
   The Golden Rule: Never enter a PIN to receive funds, and secure reset steps
4. **Chapter 4: Check Before You Pay**
   10-second safety pause, Core Banking (CBS) verified names, and physical QR checks
5. **Chapter 5: Common UPI Scams Exposed**
   Collect Request traps, fake refund lures, and AnyDesk screen-sharing scams
6. **Chapter 6: Daily Shop & Merchant Frauds**
   Tampered QR codes, fake delivery OTPs, and fake electricity disconnection threats
7. **Chapter 7: Dealing with Payment Failures**
   T+1 auto-reversal, ₹100/day bank compensation, and UDIR dispute resolution
8. **Chapter 8: How to Report UPI Fraud**
   The 2-3 hour Golden Hour, cybercrime.gov.in portal, and emergency freeze steps

9 **Chapter 9: AI Voice Cloning & Video Calls**

AI voice synthesis, deepfakes, and the truth behind fake 'Digital Arrests'

10 **Chapter 10: Fake Screenshots & Spoofed Apps**

Prank payment apps, fabricated green ticks, and verifying official 6-character bank SMS

11 **Chapter 11: Malicious Links & Smishing**

Dangerous .apk downloads, lottery messages, and reporting to DoT Chakshu portal

12 **Chapter 12: Securing Your Smartphone**

Device hardening, accessibility service risks, and blocking stolen phones via CEIR

13 **Chapter 13: The Master UPI Safety Checklist**

4 printable pocket cards, official government directory, and safety summary

- **Appendix:** Digital Banking Glossary & Back Cover

CHAPTER 1 • CORE FUNDAMENTALS

Understanding UPI & How It Works

What is UPI, how money travels from one bank account to another in seconds, and why the technology is built to protect everyday users.

What is UPI and Why is It Everywhere?

Walk down any street in India today—from a neighborhood tea stall to a large supermarket—and you will see black-and-white square **QR Codes** displayed on counters. People take out their smartphones, open their camera, scan the code, and payment happens in seconds without handing over cash. The engine powering this daily convenience is **UPI**.

UPI stands for **Unified Payments Interface**. It was designed and built by the **National Payments Corporation of India (NPCI)** under the supervision of the **Reserve Bank of India (RBI)**.

REMEMBER THE PAST

How Difficult Was Sending Money Before UPI?

Before UPI existed, sending money to a friend, family member, or shop required multiple tedious steps:

- You had to ask for their complete 16-digit **Bank Account Number**.
- You had to locate their bank branch's 11-character **IFSC Code**.

• You had to open NetBanking, add them as a new **Beneficiary**, and wait 30 minutes to 2 hours for activation.

• On bank holidays or late nights, **NEFT** transfers remained stuck until the next business morning.

> **UPI eliminated all this friction:** You no longer need to share account numbers, look up IFSC codes, or wait for bank working hours. Money moves directly between bank accounts 24 hours a day, 365 days a year, within 3 to 5 seconds.

Case Study: Mr. Sharma's First UPI Experience

58-year-old Ramesh Sharma had always used cash for his daily groceries. He hesitated to try online banking because he feared that someone glancing at his phone could drain his life savings.

Mr. Sharma: "Priya, if I give the vegetable vendor my mobile number or UPI ID, can he withdraw money from my account?"

Daughter Priya: "Dad, absolutely not! Your UPI ID or mobile number is just your address—not your key. Just like knowing someone's home address doesn't unlock their front door, knowing your UPI ID does not allow anyone to take money. To debit money, someone must enter your secret **UPI PIN**, which stays only in your head."

Mr. Sharma: "What happens if I lose my phone on the bus?"

Daughter Priya: "Even if you lose your phone, your funds remain secure. Your phone has a **Screen Lock**, your payment app requires biometric or passcode entry, and sending money always requires your **UPI PIN**. Furthermore, UPI is bound strictly to your physical SIM card."

That evening, Mr. Sharma made his very first UPI payment of ₹120 for vegetables. When the shopkeeper's **Soundbox** announced clearly—*"Received ₹120 on Paytm"*—Mr. Sharma smiled with genuine relief and confidence.

How Does Money Move? (Behind the Scenes)

Many people mistakenly assume their money is stored inside Google Pay, PhonePe, or Paytm. **That is completely incorrect.**

UPI apps are not wallets; they are secure digital highways. Your money always stays inside your actual **Bank Account**. When you make a payment, the funds travel directly from your bank to the payee's bank.

Step 1

You Scan a QR Code or Enter a UPI ID

Your payment app (BHIM, Google Pay, PhonePe, etc.) identifies the recipient's bank routing address.

↓ Secure Encryption

Step 2

You Enter Your Secret UPI PIN

The PIN is encrypted instantly inside the secure hardware of your phone and sent to your bank. No payment app can ever read or save it.

↓ NPCI Central Switch

Step 3

The NPCI Network Links Both Banks

The government-authorized NPCI network instructs your bank to debit the funds and the recipient's bank to credit the exact amount.

↓ Instant Real-Time Settlement

Step 4

Immediate Credit & Dual Confirmation

The recipient's account receives the money, both parties receive bank SMS alerts, and merchant voice boxes broadcast the payment alert.

What are UPI IDs (VPA) and QR Codes?



UPI ID (VPA - Virtual Payment Address)

This is an email-like alias for your bank account (for example: `rahul@oksbi` or `store@ybl`).

> **Key Benefit:** The other person never sees your sensitive bank account number or branch code, protecting your financial privacy.



QR Code (Quick Response Code)

A QR code is simply a machine-readable graphical picture containing a UPI ID and merchant banking information.

> **Key Benefit:** You don't have to manually type 10-digit mobile numbers or complicated IDs. Scanning reads the verified routing address automatically.

The Two Unbreakable Locks of UPI (Two-Factor Authentication)

Under RBI regulations, UPI is engineered so that a fraudster sitting remotely cannot pull money from your account. Two independent locks must be opened simultaneously:

LOCK 1: SOMETHING YOU HAVE

Your Phone and Registered SIM Card

When you set up UPI, the app sends an encrypted verification SMS from the physical SIM card in your phone. This is called **Device Binding**.

If a cyber thief enters your phone number on their computer or another phone, registration will fail because the physical SIM card is inside your device.

LOCK 2: SOMETHING YOU KNOW

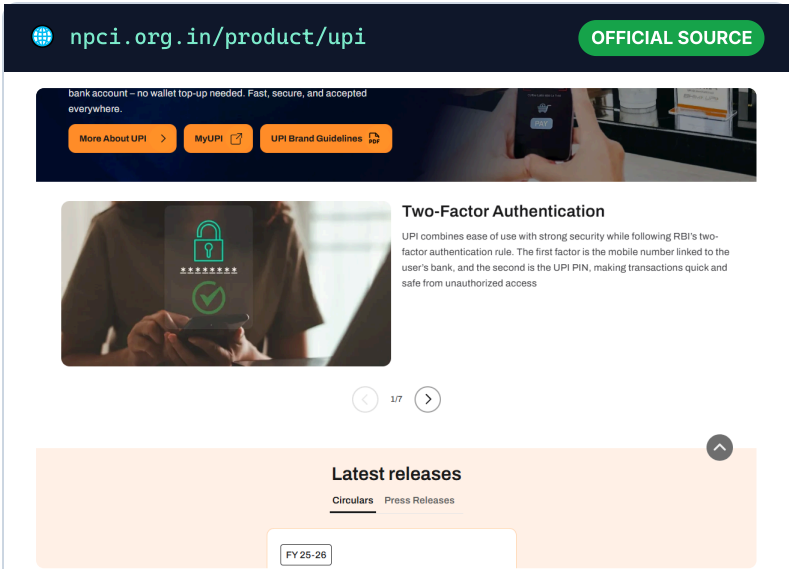
Your Confidential UPI PIN

Every outgoing transaction requires entering your 4-digit or 6-digit UPI PIN. This PIN is never stored on servers in plain text; it exists solely in your memory.

Unless you manually type this PIN on your device, no entity on earth can deduct a single rupee from your bank account via UPI.

Official UPI Information on NPCI's Portal

The **National Payments Corporation of India (NPCI)** maintains public resources and safety guidelines for all UPI users on its official website:



📌 **2 Critical Takeaways from the Official NPCI Portal:**

1. **Verify Official Domains:** Always check that the website URL ends in `npci.org.in` or `.gov.in`. Official government bodies in India never use commercial extensions like `.xyz`, `.top`, or `.site`.

2. **Two-Factor Security Policy:** NPCI explicitly highlights that the SIM-binding layer combined with user UPI PIN authentication forms an unbreakable chain when users protect their PIN.

Chapter 1: Everyday Questions on UPI Basics

(Basics FAQs)

Q1: Can anyone drain my bank account just by knowing my UPI ID or phone number?

Answer: Absolutely not. Your UPI ID or mobile number is only an address for receiving payments. Unless you disclose your UPI PIN, OTP, or approve a debit prompt, no one can withdraw funds from your account.

Q2: Do I need a physical Debit Card (ATM card) to use UPI?

Answer: Historically, a Debit Card was needed for initial PIN setup. Today, NPCI has rolled out **Aadhaar OTP-based authentication** across most major Indian banks, allowing users without an ATM card to set up UPI securely using their Aadhaar details.

Q3: What is the difference between Google Pay, PhonePe, Paytm, and my bank's app?

Answer: These apps are Third-Party Application Providers (TPAPs). They act as convenient interfaces connecting to NPCI's network. Your funds always remain safely parked in your RBI-regulated bank account (such as SBI, HDFC, ICICI, or PNB).

Q4: Is it safe to share my UPI QR code on social media or in my shop?

Answer: Yes, 100% safe. A QR code is strictly a payment reception tool. Displaying it publicly allows people to pay you; it cannot be used by anyone to debit funds from your account.

Q5: Is there a maximum daily transfer limit for UPI payments?

Answer: Yes. As per NPCI guidelines, the standard daily UPI transaction cap is ₹1,00,000 (one lakh rupees) per user per day. Certain categories like educational fees and hospital payments permit higher limits up to ₹5,00,000, while new accounts or reset PINs have temporary 24-hour cooling limits (e.g. ₹5,000) for security.

Chapter 1: Essential Dos and Don'ts for

Beginners (Beginner Checklist)

✅ What to Do (Do's)

- Keep the SIM card registered with your bank in Slot 1 of your phone.
- Always check the receiver's verified bank name on your screen before sending money.
- Download payment apps only from the official Google Play Store or Apple App Store.
- Read bank SMS alerts carefully to confirm whether funds were debited or credited.

❌ What NOT to Do (Don'ts)

- NEVER enter your secret UPI PIN to receive money, cashbacks, or refunds.
- Never write your UPI PIN on your phone cover, diary, or scratchpad.
- Never install remote desktop apps like AnyDesk or TeamViewer at a caller's request.
- Never share one-time bank OTPs or card CVVs over a phone call or chat.

Chapter 1: How to Search Official UPI Information on Google (Safe Search Guide)

Whenever you search online for official information regarding NPCI or UPI rules, follow these 4 essential safety steps:

1. **Step 1: Type the Exact Search Keyword**

   In your browser search bar, type: `NPCI official UPI product overview`

2. **Step 2: Skip Links Marked "Sponsored" or "Ad"**

   Avoid clicking top results displaying **Sponsored** or **Ad** tags. Fraudsters often purchase paid ads to push counterfeit pages to the top of search rankings.

3. **Step 3: Check the Official Website Domain**

   Ensure the small green or grey URL shows `https://www.npci.org.in`. If the domain contains unusual words like `free-upi-cashback.xyz` or `npci-support.online`, close the tab immediately.

4. **Step 4: Never Dial Phone Numbers Found in Search Snippets**

   Do not call mobile or toll-free numbers displayed directly in search result previews. Only trust contact numbers listed on the verified website's internal "Contact Us" page.

🔍 **Official Verification Sources for Chapter 1:**

- **NPCI Official UPI Overview:** `https://www.npci.org.in/product/upi`
- **RBI Digital Payment Security Controls:** `https://www.rbi.org.in`
- **BHIM UPI Official Portal:** `https://www.bhimupi.org.in`

CHAPTER 2 • ACCOUNTS & LIABILITY

UPI & Your Bank Account

How UPI connects to your bank balance, your responsibilities as an account holder, and your legal rights under RBI's 3-day Zero Liability protection framework.

The Real Relationship Between Your Bank and UPI Apps

Many users mistakenly believe that PhonePe, Google Pay, or Paytm are online banks where their money is held. **That is entirely untrue.**

Your money always resides 100% inside your regulated **Bank Account** (such as SBI, HDFC, ICICI, PNB, or Bank of Baroda). A UPI app is simply a digital window on your phone that allows you to transact without physically visiting a bank branch.

SIMPLE ANALOGY

Your Bank Account and Your UPI ID

Think of your bank account as your physical home, and your **UPI ID** (such as `rahul@oksbi`) as the mailbox outside your front door:

- When someone sends money to your UPI ID, it is credited directly into your **Bank Account**.
- When you transfer money, the funds are debited directly from your **Bank Account**.

• Handing someone your UPI ID never reveals your 16-digit account number or branch IFSC code, keeping your core banking information confidential.

Case Study: Sunil's Stolen Phone & The 3-Day Rule

Sunil works at a private logistics company in Pune. While commuting home on a crowded bus, his smartphone was stolen. Upon reaching home and logging into his bank account from his spouse's phone, he froze in shock—₹25,000 had been debited in two unauthorized transactions.

What Immediate Steps Did Sunil Take?

That Same Evening Sunil stayed calm, called his bank's verified 24×7 emergency helpline immediately, and blocked his **UPI, NetBanking, and ATM card**.

Next Morning He visited his home branch, filed a written complaint for **Unauthorized Electronic Banking Transactions**, and obtained an official **Complaint Acknowledgement Number**.

7 Days Later Because Sunil had never shared his **UPI PIN** or **OTP** with anyone and reported the incident **within 3 business days**, the bank restored

the entire ₹25,000 back to his account under **RBI's Zero Liability Policy**!

Core Lesson: If money is debited without your fault, panic and delay are your worst enemies. Immediate formal reporting within 3 days is the legal key to recovering your money.

RBI's 3-Day Zero Liability Framework: Your Legal Shield

To safeguard everyday banking customers, the Reserve Bank of India issued a landmark circular titled *"Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions"*. The rules define three clear liability tiers:

Tier 1: Zero Customer Liability (100% Refund)	Reported within 3 working days

The Rule: If the unauthorized transaction is due to a system glitch or third-party breach where the customer did not share their PIN/OTP, and you report it to the bank **within 3 working days** of receiving the alert:

🎯 **Customer Liability = ₹0 (Zero)!** The bank is legally mandated to reverse and credit the full amount back to your account within 10 working days.

Tier 2: Limited Customer Liability — **Reported within 4 to 7 working days**

The Rule: If there is a delay in reporting between **4 and 7 business days**, your maximum financial loss is legally capped based on your account type:

- Basic Savings Bank Deposit (BSBD/Jan Dhan) Accounts: Maximum liability capped at **₹5,000**.
- Standard Savings and Current Accounts: Maximum liability capped at **₹10,000**.

⚠ **Any amount lost above these statutory caps must be absorbed and refunded by the bank!**

Tier 3: Beyond 7 Working Days — **Reported after 7 days**

The Rule: If reporting is delayed past 7 working days, liability is determined strictly according to the individual bank's board-approved policy.

❌ **Do not wait! Every passing day diminishes your legal protection.**

The Smart 2-Account Strategy for UPI Users

Financial security experts strongly advise against linking your primary life-savings account (holding pensions, fixed deposits, or salary reserves) directly to daily UPI scanning apps. Instead, adopt the **Dual-Account Separation Strategy**:

Account A: Main Savings (Safe Vault)

Keep your emergency funds, salary deposits, and family savings here. **Do not link this account to daily phone UPI apps.**

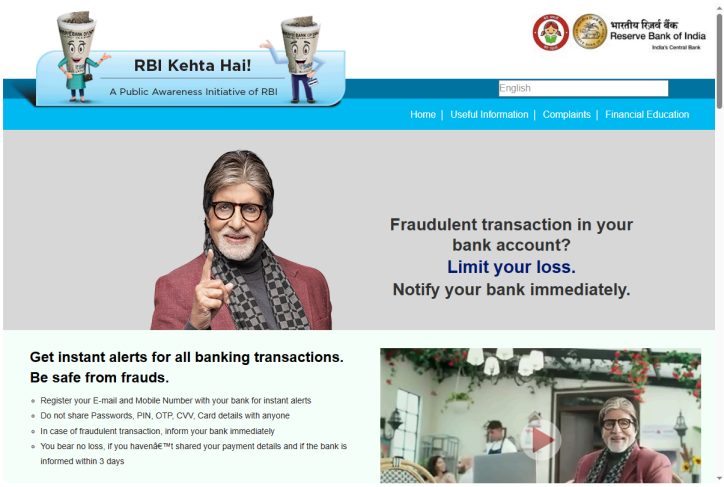
Account B: Daily UPI Spending Account

Maintain a secondary account with a balance of ₹3,000 to ₹10,000 strictly for street shopping, cab fares, and groceries. Even in the worst-case scenario, your life savings remain untouched.

RBI's Official Awareness Guide: Limit Your Liability

The Reserve Bank of India runs its flagship public campaign **"RBI Kehta Hai"** to educate citizens about reporting unauthorized electronic debits:

rbi.org.in / rbikehtahai.rbi.org.in **OFFICIAL RBI GUIDE**



📌 **2 Vital Directives from RBI Regulations:**

1. **Mandatory SMS Alert Registration:** Ensure your current, active mobile number is registered with your bank. RBI mandates that banks provide instant SMS alerts for all electronic transactions.

2. **Reply 'BLOCK' or Call Instantly:** Most bank transaction SMS messages include an emergency reply code or direct phone number to block unauthorized debits instantly.

Chapter 2: Essential Questions on Bank

Accounts & Liability (Bank Liability FAQs)

Q1: If someone tricks me into sharing my OTP over a call, does the Zero Liability rule still apply?

Answer: No. RBI guidelines state that if a loss occurs due to customer negligence (such as voluntarily sharing your UPI PIN, password, or OTP), the customer bears the full loss until the unauthorized transaction is reported to the bank.

Q2: How many bank accounts can I link to a single UPI application?

Answer: You can link multiple bank accounts from different banks to the same UPI app, provided they are all registered with the same mobile phone number. You can select one as your default primary account for receiving payments.

Q3: What should I do if my bank branch refuses to accept my written fraud complaint?

Answer: Request to meet the Branch Manager or the Bank's Branch Grievance Redressal Officer. If the branch does not provide a formal written acknowledgement within 30 days, you can lodge a complaint directly with the **RBI Banking Ombudsman** at `cms.rbi.org.in`.

Q4: Does my bank charge any fee for reporting unauthorized transactions or blocking UPI?

Answer: Absolutely not. Blocking your digital channels and lodging fraud complaints is completely free of charge across all public and private sector banks in India.

Q5: Within how many days must a bank resolve an unauthorized transaction dispute?

Answer: Under RBI mandates, banks must settle and resolve customer liability claims within a maximum of **90 days** from the date of receiving the complaint.

Chapter 2: Bank Account Safety Dos and Don'ts (Account Protection Checklist)

✅ What to Do (Do's)

- Keep a secondary bank account with modest balances for daily street UPI payments.
- Save your bank's official 24×7 emergency helpline number in your phone contacts right now.
- Always demand an official Complaint Acknowledgement Number whenever reporting fraud.
- Immediately notify your bank if you change your mobile phone number.

❌ What NOT to Do (Don'ts)

- Never keep your entire life savings and fixed deposits in the same account linked to daily UPI apps.
- Never ignore bank SMS debit notifications; check unfamiliar debits within minutes.
- Never wait for bank working hours to report cyber fraud—call the emergency 24×7 line immediately.
- Never share your bank account statement or passbook photos on open social media groups.

Chapter 2: How to Search RBI Zero Liability Rules on Google (Safe Search Guide)

To verify your legal consumer rights directly from the Reserve Bank of India, use these search instructions:

1. **Step 1: Use the Exact Official Liability Query**
   Search keyword: `RBI circular limiting liability of customers unauthorized electronic transactions`

2. **Step 2: Verify the Domain Address**
   Make sure the result points directly to `https://www.rbi.org.in` or `https://rbikehtahai.rbi.org.in`.

3. **Step 3: Download the Official PDF Circular**
   Official RBI circulars are published in clean PDF format bearing RBI's department reference numbers. Keep a saved copy for your reference.

4. **Step 4: Beware of Unofficial Legal Blogs**
   Avoid commercial blogs or forums with popup ads providing third-party legal advice. Always rely on primary circulars from RBI.

🔍 Official Verification Sources for Chapter 2:

- **RBI Circular on Customer Liability:**
  `https://www.rbi.org.in/scripts/BS_CircularIndexDisplay.aspx?Id=11040`
- **RBI Kehta Hai Official Portal:**
  `https://rbikehtahai.rbi.org.in`
- **RBI Complaint Management System (CMS):**
  `https://cms.rbi.org.in`

CHAPTER 3 • DIGITAL KEYS & PIN SECURITY

Protecting Your UPI PIN

Your UPI PIN is the digital master key to your bank account. Learn the universal Golden Rule of payments, safe PIN creation, and how to spot fraud traps instantly.

What is a UPI PIN? The Vault Key to Your Savings

When you visit a physical bank branch, you sign a cheque or withdrawal slip. At an ATM, you type your 4-digit card PIN. Similarly, when you transfer money from your phone via **UPI**, you type a confidential 4-digit or 6-digit secret code to prove to your bank that you personally authorized the debit. This code is your **UPI PIN** (Personal Identification Number).

The Single Most Important Golden Rule of UPI

UPI PIN is required ONLY to SEND money.
You NEVER need a UPI PIN to RECEIVE money or refunds!

Burn this one rule into your memory: whenever anyone deposits money into your account, it lands directly in your bank. You do not need to tap your screen, enter a PIN, or approve an OTP to receive even a single rupee.

Case Study: Vikas Selling His Used Sofa on an

Online Marketplace

Vikas listed an old living room sofa for sale on an online marketplace for ₹8,000. Within fifteen minutes, he received a call from an eager buyer.

THE FRAUDSTER'S SCRIPT

"Sir, I am calling from the Army Depot. I want to book your sofa immediately!"

Without bargaining, the caller said: *"Sir, I love the sofa. I am transferring the full advance of ₹8,000 on Google Pay right now. My transport truck will pick up the sofa this evening."*

Two minutes later, Vikas's phone buzzed with an incoming notification: **"Collect Request: Pay ₹8,000 to Army Officer"**. The caller insisted on the phone: *"Sir, I have transferred the amount. Please enter your UPI PIN right now so the ₹8,000 credits to your bank account."*

> Just as Vikas's finger touched the keypad, the Golden Rule flashed in his mind: **"Wait! I never need a PIN to receive money!"** He looked closely at the screen—it read *"Paying ₹8,000"*, not receiving. Vikas immediately tapped Cancel, hung up, and blocked the scammer. His ₹8,000 was saved in that single split second.

Direct Comparison: When Should You Enter Your PIN vs NEVER?

❌ **NEVER Enter PIN (100% Scam Attempt)**

- **When receiving money:** Anyone telling you to enter a PIN to receive funds.
- **Claiming cashbacks or lottery rewards:** Promising free prize money.
- **Unsolicited Collect Requests:** Payment requests sent by unknown parties.
- **Caller claiming to be Bank Customer Care:** Demanding your PIN for KYC.
- **Government scheme benefits:** Falsely claiming subsidies need PIN approval.

✅ **Enter PIN ONLY Here (Legitimate Actions)**

- **When YOU are sending money:** Willingly transferring funds to pay someone.
- **Scanning a merchant QR code:** Buying items at a store.
- **Paying utility bills:** Electricity, water, cooking gas, or mobile recharges.
- **Online shopping checkout:** Paying for an order on trusted websites.
- **Checking your bank balance:** Directly inside your installed UPI app.

How to Change or Reset Your UPI PIN Securely

If you suspect someone saw you type your PIN, or if you are using an obvious sequence like `1234` or your birth year, reset your PIN immediately:

1. **Open Your Payment App & Select Bank Account**
   Tap your profile picture in BHIM, Google Pay, or PhonePe, select your linked bank account, and tap **"Change UPI PIN"** or **"Forgot UPI PIN"**.

2. **Authenticate with Debit Card or Aadhaar**
   Enter the last 6 digits of your ATM card and expiry date, or select Aadhaar verification to receive an official one-time bank OTP.

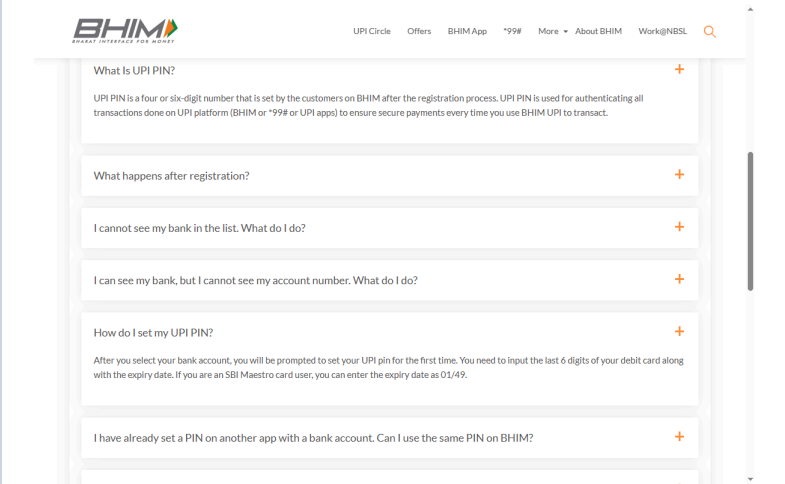
3. **Choose a Strong, Unpredictable New PIN**
   Never choose `1111`, `1234`, `2580`, or your birth year. Pick a random combination that only you can recall.

Official BHIM UPI & NPCI Guidelines on PIN Security

The official **BHIM UPI portal**, operated by NPCI, clearly states the rule regarding UPI PINs:

bhimupi.org.in / npci.org.in

OFFICIAL NPCI GUIDE



📌 **Official NPCI Warning:**

1. **PIN Entry Equals Debit:** Entering your PIN always instructs your bank to release money. It can never result in funds entering your account.

2. **Decline Unknown Collect Requests:** If you receive a payment request notification from an unfamiliar contact, tap 'Decline' or 'Block' immediately.

Chapter 3: Essential Questions on UPI PIN Protection (UPI PIN FAQs)

Q1: Is my UPI PIN the same as my ATM card PIN or NetBanking

password?

Answer: No. Your UPI PIN is a distinct 4 or 6-digit code created specifically for mobile UPI payments. While you can technically set them to match, keeping your UPI PIN completely unique is much safer.

Q2: What happens if I type the wrong UPI PIN three times consecutively?

Answer: Your bank will temporarily freeze UPI transactions on that bank account for **24 hours** as a fraud prevention safeguard. You can reset your PIN after the cooling period using your ATM card or Aadhaar details.

Q3: Can bank employees, police officers, or app support staff ask for my UPI PIN?

Answer: Absolutely NEVER. Under RBI directives, no bank official, RBI officer, police investigator, or app representative is ever authorized to ask for your UPI PIN or OTP under any circumstance.

Q4: Why does my bank balance inquiry require my UPI PIN?

Answer: Checking your account balance accesses sensitive Core Banking data. Entering your UPI PIN validates that you are the genuine account holder before displaying confidential balance information.

Q5: Should I write down my UPI PIN anywhere in my phone notes?

Answer: Never. Storing your PIN in note-taking apps, contact cards (e.g. naming a contact 'PIN'), or drafts exposes your credentials if your phone is lost, repaired, or inspected by others.

Chapter 3: UPI PIN Protection Dos and Don'ts (PIN Security Checklist)

✅ What to Do (Do's)

- Memorize your UPI PIN and shield your phone screen with your hand in public places.
- Decline and report suspicious incoming Collect Requests right away.
- Change your UPI PIN immediately if you ever shared it under pressure or suspicion.
- Use biometrics (fingerprint/face recognition) as an additional app lock layer.

❌ What NOT to Do (Don'ts)

- NEVER enter your UPI PIN after tapping a link sent in WhatsApp or SMS.
- Never use obvious PIN combinations like birthdays, wedding dates, or vehicle numbers.
- Never share your screen over video calls (WhatsApp, Zoom, AnyDesk) while entering a PIN.
- Never trust callers who promise refunds if you enter your PIN on your phone.

Chapter 3: How to Search Official UPI PIN Rules on Google (Safe Search Guide)

When looking for authentic instructions on resetting or securing your UPI PIN, follow these search parameters:

1. **Step 1: Use Clear Official Search Terms**

   Search keyword: `BHIM UPI official safety never enter PIN to receive money`

2. **Step 2: Prioritize NPCI or Bank Domains**

   Verify that URLs originate from `bhimupi.org.in`, `npci.org.in`, or your specific bank's official domain (e.g. `sbi.co.in`, `hdfcbank.com`).

3. **Step 3: Never Click Third-Party "PIN Generator" Links**

   Ignore search ads promising "Instant UPI PIN recovery tools". There is no external tool that can generate a bank UPI PIN.

4. **Step 4: Perform PIN Reset Exclusively In-App**

   Always initiate PIN changes directly from within your authentic mobile banking or UPI application.

🔍 Official Verification Sources for Chapter 3:

- **NPCI BHIM UPI FAQs:** `https://www.bhimupi.org.in/faqs`
- **RBI Cyber Security Framework:** `https://www.rbi.org.in`
- **NPCI Consumer Awareness Hub:** `https://www.npci.org.in`

CHAPTER 4 • PRE-PAYMENT DISCIPLINE

Check Before You Pay

UPI transfers money in less than 2 seconds. Reversing funds sent to the wrong person is notoriously slow and difficult. Master the 10-second safety check before every transaction.

The 10-Second 'Security Pause'

The greatest advantage of UPI is speed—money arrives in the recipient's bank account instantly. However, that very speed becomes a liability when you pay in a rush or under distraction.

Once you type your **UPI PIN** and the payment executes, there is no "Undo" or "Recall" button to stop money in mid-flight. Taking a deliberate **10-second pause** to verify 4 details on your screen is your most dependable financial shield.

MANDATORY NPCI DIRECTIVE

CBS Name Verification: Your Ultimate Safety Check

The National Payments Corporation of India (NPCI) mandates that every UPI app (Google Pay, PhonePe, Paytm, BHIM) must fetch and display the recipient's legal name registered in their bank's Core Banking Solution (**CBS Name**) immediately upon scanning a QR code or entering a UPI ID.

💡 **What this means:** A fraudster can label their display profile as "Electricity Helpline" or "Army Canteen", but the screen will expose their real, bank-registered name (e.g. *"Mohammad Aslam"* or *"Ramesh Kumar"*). If the name doesn't match the merchant, stop immediately!

Case Study: Sonu's Fuel Bill — ₹500 vs. ₹5,000

Sonu was filling petrol in his scooter at a busy city fuel station. Running late for an office presentation, he was eager to pay and rush out. The fuel attendant announced the bill: ₹500.

THE RUSHED MISTAKE

The Extra Zero That Almost Cost ₹4,500

Still sitting on his scooter, Sonu scanned the fuel pump QR stand, hurriedly typed ₹5000 (his finger accidentally tapped zero three times), and pressed Pay.

As his thumb hovered over the PIN pad, the 10-second rule clicked in: **"Pause and check the amount!"** He glanced up at the confirmation screen and caught it—the screen clearly read **₹5,000.00**, ten times the actual bill!

> Sonu immediately tapped the Back button, corrected the amount to ₹500, verified the station name, and completed the payment. That five-second pause saved him weeks of paperwork and disputes over an extra

₹4,500.

What to Check on the Confirmation Screen (Visual Mockup)

Before entering your PIN, your payment app presents a final confirmation screen. Here is what to inspect:

Payment Confirmation Screen Illustrative Example

Recipient's Verified Bank Name (CBS Name)

Ramesh Kumar Kirana ✓ Verified

Check 1: Does this match the business name or person you intend to pay?

UPI ID (VPA)

`rameshkirana@okaxis`

Check 2: Is the merchant ID genuine and free from unusual random strings?

Total Amount to Pay

₹ 350.00

Check 3: Count the zeroes carefully. Ensure no extra digits were tapped.

Debiting From

State Bank of India (••4821)

Check 4: Confirm funds are coming from your intended daily spending account.

Beware of Tampered Physical QR Stickers at

Stores

In busy markets, fraudsters use a low-tech trick called **QR Sticker Overlay**:

How Scammers Hijack Merchant QR Stands:

A scammer prints stickers of their personal UPI QR code and secretly pastes them over a shopkeeper's genuine payment stand during peak rush hours. When customers scan the stand, money goes directly into the thief's account while the shopkeeper receives nothing!

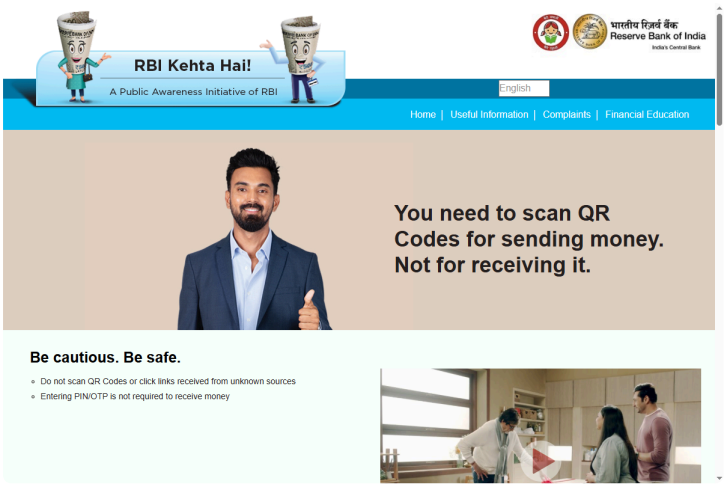
1. **Inspect the QR Plate:** Feel the stand with your finger. If you notice a loose paper sticker pasted over the original acrylic board, alert the shopkeeper.

2. **Voice Soundbox Confirmation:** Always wait until the merchant's soundbox announces the payment aloud before leaving the counter.

RBI's Official QR Code Safety Campaign

The Reserve Bank of India frequently highlights QR code verification in its public alerts:

rbi.org.in / rbikehtahai.rbi.org.in **OFFICIAL RBI GUIDE**



📌 **2 Official Directives from the RBI QR Campaign:**

1. **Read the Displayed Name:** Always verify that the name appearing on your phone screen after scanning belongs to the merchant you are standing before.

2. **QR Codes Only Initiate Debits:** Scanning a QR code is exclusively for paying money out; scanning a QR code can never deposit money into your account.

Chapter 4: Important Questions Before Making a Payment (Payment Checks FAQs)

Q1: What should I do if the name on my screen is different from

the shop's signboard?

Answer: Stop immediately and ask the merchant. Many shops use a proprietor's personal name or a registered legal partnership name rather than their trade brand. Ask the owner: *"Does this name match your bank account?"* Only proceed after verbal confirmation.

Q2: What is the risk of scanning a dynamic QR code on a billing machine screen?

Answer: Dynamic QR codes are actually safer. They have the exact bill amount already embedded inside the code, preventing manual typing errors or extra zeroes. Simply verify the displayed merchant name and approve.

Q3: Can a QR code contain malware or computer viruses?

Answer: Standard UPI QR codes contain only text. However, scanning random QR codes with a generic phone camera (instead of a payment app) can open malicious website URLs. Always scan payment QR codes using trusted UPI apps like BHIM, Google Pay, or PhonePe.

Q4: Why does my payment app sometimes ask for location permissions when paying?

Answer: For fraud detection. Payment apps use device location to identify anomalous transactions—such as a payment occurring in a different state within minutes of a local transaction—flagging potential compromised accounts.

Q5: If I accidentally send money to the wrong person, can my bank cancel it immediately?

Answer: No immediate cancellation exists. Because UPI performs real-time gross settlement, the money is already in the recipient's bank account. You must file a misdirected payment dispute under NPCI guidelines (explained in Chapter 7).

Chapter 4: Pre-Payment Safety Dos and Don'ts (Payment Checklist)

✅ What to Do (Do's)

- Always observe the 10-second pause to read the recipient's verified bank name.
- Double-check digits and decimal points before typing your PIN.
- Verify that the merchant's soundbox announces the exact amount before leaving.
- Touch QR stands in shops to ensure no fake sticker is pasted over the original code.

❌ What NOT to Do (Don'ts)

- Never rush through payment confirmation while walking, riding, or distracted.
- Never scan a QR code sent over WhatsApp by an unknown caller promising lottery winnings.
- Never ignore an unfamiliar name displayed on your confirmation screen.
- Never approve a payment request without inspecting who initiated the request.

Chapter 4: How to Search RBI QR Safety Advice on Google (Safe Search Guide)

To access official guidelines on QR code security from the Reserve Bank of India, use these instructions:

1. **Step 1: Enter the Precise QR Safety Query**
   Search keyword: `RBI Kehta Hai QR code safety guidelines official website`
2. **Step 2: Confirm RBI Official Video Portal**
   Look for links pointing to `https://rbikehtahai.rbi.org.in` or official RBI press releases on `rbi.org.in`.
3. **Step 3: Review Verified Awareness Videos**
   RBI hosts informative 30-second educational clips illustrating QR code precautions for merchants and retail customers.
4. **Step 4: Bookmark Official Educational Material**
   Save official RBI resources to share with older relatives and shop assistants.

🔍 **Official Verification Sources for Chapter 4:**

- **RBI Kehta Hai Awareness Hub:** `https://rbikehtahai.rbi.org.in`
- **NPCI Merchant QR Guidelines:** `https://www.npci.org.in`
- **MeitY Digital Payments Safety Portal:** `https://www.meity.gov.in`

CHAPTER 5 • SCAM TACTICS EXPOSED

Common UPI Scams Exposed

Scammers don't breach banking mainframes; they exploit panic, haste, and curiosity. Learn the anatomy of the 4 most prevalent scams and how to disarm them instantly.

Scammers Hack Human Emotions, Not Bank Servers

Many people assume cybercriminals break through bank encryption using supercomputers. **That is almost never the case.** India's UPI infrastructure is protected by bank-grade security protocols that cannot be penetrated remotely.

Instead, fraudsters target the human operating the phone. By triggering intense panic (e.g., *"Your electricity will be disconnected tonight"* or *"Your account is frozen"*) or irresistible excitement (e.g., *"You won ₹5,000 lottery cashback"*), they manipulate victims into entering their own **UPI PIN** or reading out an **OTP**. In cybersecurity, this is called **Social Engineering**.

Case Study: Anita and the ₹5 Courier Redelivery Trap

Anita ordered clothes online for her daughter's birthday party. The parcel delivery was delayed by one day. That afternoon, she received a call from an unknown mobile number.

THE SCAMMER'S CALL

"Madam, your parcel is on hold. Pay ₹5 to update your address!"

The caller spoke in polite corporate language: *"Madam, I am calling from the courier dispatch hub. Your house number is unclear, so your package cannot be delivered. I am sending a link on WhatsApp. Pay a nominal ₹5 redelivery fee, and our van will deliver it by 5 PM."*

Anita clicked the WhatsApp link, which automatically started downloading a file called **"Support_Quick.apk"**. The caller instructed: *"Madam, install the app, read out the 9-digit session code on your screen, and open your Google Pay app."*

> Anita paused with sudden suspicion: **"Why would a standard ₹5 payment require downloading a third-party application?"** She immediately terminated the call and deleted the downloaded APK file. Two hours later, the regular courier arrived at her door without any fee. Her vigilance saved her entire account balance from being emptied remotely.

The 4 Most Common UPI Frauds in India

SCAM 1 **The Fraudulent Collect Request (Posing as a Payer)**

This remains the single most common trick. Fraudsters pretend they are sending you money, but instead issue a Collect Request to pull money from your account.

The Scammer's Script: *"Sir, I have sent you an advance of ₹10,000. Check your PhonePe notification, tap Accept, and enter your UPI PIN to credit the money."*

The Reality: In UPI, tapping 'Pay' or 'Accept' and entering your PIN initiates an immediate **debit from your account to theirs!**

🛡️ **Defense:** Immediately tap **'Decline'** on any unexpected payment request, and block the user in your app.

SCAM 2 **Fake Cashback & Lottery Links (The Reward Illusion)**

You receive a message: *"Congratulations! You won a ₹3,999 cashback scratch card. Tap here to claim instantly."*

The Scammer's Script: Clicking the link opens a counterfeit web page with a green button: *"Send to Bank"*. It launches your UPI app, prefilling a transfer to the scammer.

The Reality: Genuine rewards and cashbacks deposit automatically into your bank account without requiring you to visit external links or enter your PIN.

Defense: Never click on reward claim links received through WhatsApp, Telegram, or SMS.

SCAM 3

Remote Screen-Sharing Apps (AnyDesk, TeamViewer, RustDesk)

Under the pretext of resolving a pending transaction or fixing KYC errors, the caller instructs you to install an application from the Play Store.

The Scammer's Script: *"Install AnyDesk QuickSupport and tell me the 9-digit code so our technician can verify your banking connection live."*

The Reality: Once connected, the scammer watches your phone screen live, records your UPI PIN as you type it, and views incoming bank OTPs in real time.

Defense: Never install remote desktop or screen-mirroring apps at the direction of any phone caller.

SCAM 4 **Spoofed Customer Care Numbers on Search Engines**

When an online payment gets stuck, anxious users search Google for "GPay customer care number" or "SBI toll-free helpline".

The Scammer's Script: Fraudsters purchase Google Search Ads or edit business listings on Google Maps with their personal mobile numbers.

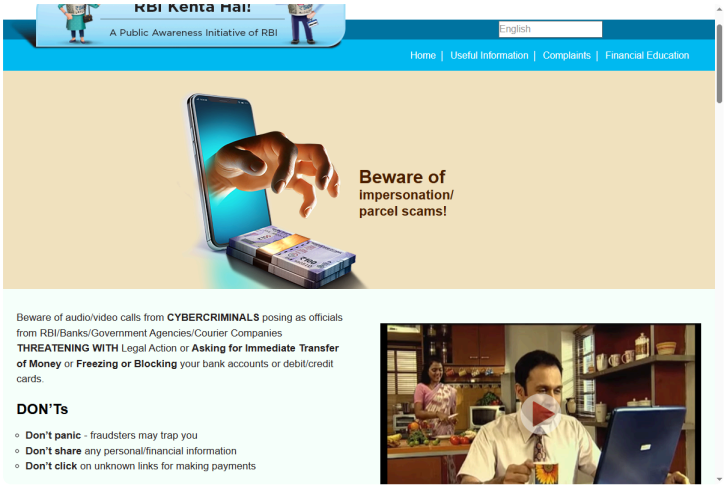
The Reality: When you call, the fake agent offers an immediate refund but asks you to enter your PIN or download a support file.

Defense: Always use the in-app "Help & Support" button inside your payment app. Banks never use personal 10-digit mobile numbers for customer care.

RBI's Public Alert on Impersonation Frauds

The Reserve Bank of India cautions the public against fraudsters impersonating bank officials, couriers, and support desks:

rbi.org.in / rbikehtahai.rbi.org.in OFFICIAL RBI GUIDE



📌 **2 Golden Guidelines from the RBI Awareness Drive:**

1. **Banks Never Request Remote Access:** Legitimate bank staff will never ask you to install screen-sharing software or third-party APKs on your phone.

2. **Beware of Sense of Urgency:** Any call or message insisting you must act "within 15 minutes" or face account suspension is a hallmark of fraud.

Chapter 5: Questions on Recognizing and Stopping Scams (Fraud Defense FAQs)

Q1: If someone sends a Collect Request on my UPI app, can

they deduct money automatically?

Answer: No, never automatically. A Collect Request is simply an invitation to pay. Money cannot leave your account unless you manually click Pay and enter your secret UPI PIN.

Q2: I mistakenly installed AnyDesk during a suspicious call. What should I do right now?

Answer: Act immediately: Turn on Airplane Mode to disconnect internet access. Uninstall the screen sharing app. Turn off your phone, remove the SIM card temporarily, and call your bank from another phone to freeze UPI and NetBanking.

Q3: How do I distinguish an official bank customer care number from a fake one?

Answer: Official bank helplines are found directly on your bank's verified official website or printed on the physical back of your debit card. Banks never conduct customer service via personal 10-digit mobile numbers.

Q4: Can a scammer deduct money if I simply answered their phone call?

Answer: No. Merely answering a voice call cannot initiate a banking transfer. Fraud occurs only when a victim shares an OTP, reveals their UPI PIN, clicks a malicious link, or installs an access tool.

Q5: Why do payment apps show warning alerts for certain Collect Requests?

Answer: UPI apps deploy machine learning algorithms that flag payment requests from unknown numbers, recently registered accounts, or users previously reported for spam. Always heed

these high-risk warning flags.

Chapter 5: Scam Protection Dos and Don'ts (Scam Shield Checklist)

✅ What to Do (Do's)

- Immediately decline and report any Collect Request sent by someone you don't know.
- Initiate customer support only via in-app help menus or numbers on your debit card.
- Verify unexpected delivery charges by checking the official shopping app order status.
- Educate family members about the golden rule: never enter a PIN to receive money.

❌ What NOT to Do (Don'ts)

- Never install remote support tools (AnyDesk, TeamViewer) at the request of a caller.
- Never believe cashback offers that require clicking external web links to claim.
- Never trust phone numbers retrieved from unverified Google search results.
- Never act in haste when a caller creates artificial urgency or threatens legal trouble.

Chapter 5: How to Search RBI Scams Awareness

on Google (Safe Search Guide)

To find verified educational campaigns and booklet resources on common banking frauds, follow this search approach:

1. **Step 1: Use the Exact RBI BE(A)WARE Query**
   Search keyword: `RBI Kehta Hai BE(A)WARE booklet modus operandi financial fraud`

2. **Step 2: Access the RBI BE(A)WARE Publication**
   RBI publishes an exhaustive official handbook titled *BE(A)WARE* documenting common cyber frauds and preventive steps. Download the PDF directly from `rbi.org.in`.

3. **Step 3: Disregard Third-Party Advisory Sites**
   Avoid aggregator websites that repackage safety tips with sponsored loan or credit card advertisements.

4. **Step 4: Check Publication Dates**
   Ensure regulatory publications reflect current UPI and payment ecosystem architectures (2024–2026 guidelines).

🔍 **Official Verification Sources for Chapter 5:**

- **RBI BE(A)WARE Booklet on Modus Operandi of Financial Frauds:** `https://www.rbi.org.in`
- **National Cyber Crime Reporting Portal:** `https://cybercrime.gov.in`
- **NPCI Fraud Prevention Advisories:** `https://www.npci.org.in`

CHAPTER 6 • EVERYDAY SCENARIOS

Daily Shop & Merchant Frauds

From your corner grocery store to your front doorway, cyber fraudsters operate right in your neighborhood. Discover the 3 most common real-world traps and practical safeguards.

Frauds Don't Just Happen Online; They Happen on Your Street

People often think cybercrime only affects corporations or high-tech targets. In reality, street fraudsters exploit everyday moments—visiting a busy grocery shop, receiving a package delivery, or reading a late-night electricity warning text.

Let's examine 3 actual real-world scenarios to see where everyday consumers make mistakes and how 10 seconds of calm awareness protects your money.

CASE STUDY 1

The Replaced QR Code Sticker at the Grocery Store

Sohan visited his local neighborhood grocery store during evening peak rush hours to buy ₹320 worth of household goods. He hurriedly scanned the counter's acrylic QR stand, typed ₹320, entered his **UPI PIN**, and pressed submit.

> **Sohan:** "Bhaiya, I have sent ₹320. Please check."
>
> **Shopkeeper:** "Brother, my voice soundbox didn't make any announcement, and I haven't received any bank SMS."
>
> **Sohan:** "Look, the money was debited from my account!" (He showed his screen: 'Paid ₹320 to Rajesh Kumar').
>
> **Shopkeeper:** "Wait! My name is 'Ramesh Gupta'. Who is this Rajesh Kumar?"

When the shopkeeper inspected his acrylic stand, he discovered that a scammer had discreetly pasted a paper sticker of their own QR code right over the store's original code. Sohan's payment had gone straight into the thief's pocket!

> 💡 **What Was Sohan's Oversight?** Sohan didn't check the recipient's bank-registered name (CBS Name) displayed on his confirmation screen before typing his PIN. Had he asked, *"Bhaiya, the screen says Rajesh Kumar—is that your account?"*, the theft would have been foiled in seconds.

CASE STUDY 2

The Counterfeit Delivery Agent & The Cancellation OTP

Kavita was at home on a Saturday afternoon when her phone rang:

> **Caller:** "Hello Madam, I am calling from Amazon logistics. We have an express parcel for your address, but the house number on the label is smudged. Are you home?"
>
> **Kavita:** "Yes, I am home, but I haven't ordered any parcel recently."
>
> **Caller:** "Madam, perhaps your husband or son ordered it. If you want to decline the delivery, company rules require a 6-digit **Cancellation OTP** sent to your SMS so the system marks it returned without penalties."

Assuming it was a routine cancellation code, Kavita glanced at her notifications and read the 6 digits aloud. Within two minutes of hanging up, her bank sent an alarming notification: **₹20,000 debited** via UPI!

> ⚠ **What Actually Happened?** That OTP was not for parcel cancellation! The scammer had entered Kavita's mobile number into a banking app on their device, and Kavita handed over the bank registration verification OTP.

CASE STUDY 3

The Late-Night Electricity Disconnection Threat SMS

At 8:45 PM while having dinner with his family, Mr. Verma received this alarming text message:

"Dear Consumer, your electricity power will be disconnected tonight at 9:30 PM from the electricity sub-division because your previous month bill was not updated. Immediately contact power officer at: [Personal 10-digit mobile number]"

Worried that the power would be cut off at night, Mr. Verma dialed the mobile number in the SMS immediately.

> **Fraudster:** "Sir, our server shows your bill is pending update. Pay a nominal ₹10 verification charge via this link on Google Pay to keep your line active."

Mr. Verma clicked the link and entered his UPI PIN. But behind the link, the scammer had concealed a **₹35,000 Collect Request**. Entering his PIN immediately deducted ₹35,000 from his account!

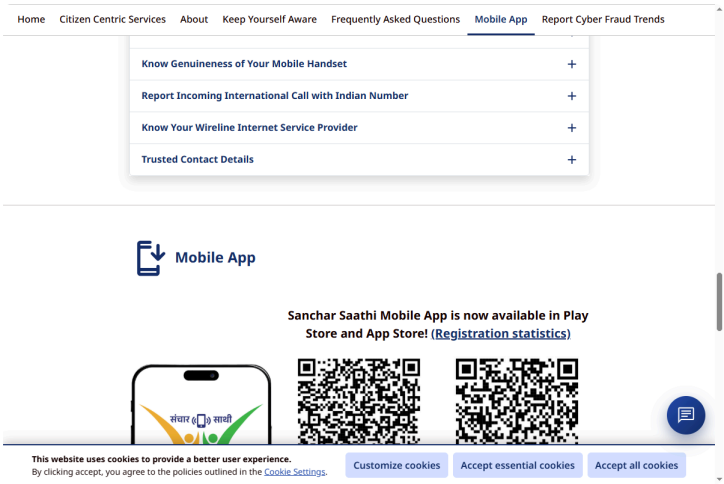
> ⚠️ **The Golden Warning:** State electricity distribution boards never send SMS messages from personal 10-digit mobile numbers, and power is never disconnected at night over an unverified ₹10 fee.

Reporting Fraudulent SMS on DoT's Chakshu Portal

The Department of Telecommunications (DoT) maintains the official **Chakshu** facility on the *Sanchar Saathi* portal to report fraud calls, phishing messages, and lottery scams:

sancharsaathi.gov.in / chakshu

OFFICIAL DOT PORTAL



📌 **Official DoT Directive:**

1. **Report Suspicious Communications:** You can report fake electricity texts, courier OTP scams, and impersonation calls directly on `sancharsaathi.gov.in` to disconnect the fraudster's SIM permanently.

2. **Check SMS Sender ID:** Official utility and bank SMS always arrive under registered 6-character header IDs (e.g. `VK-SBIPAY` or `AD-DISCOM`), never from standard 10-digit mobile numbers.

Chapter 6: Questions on Daily Shop & Street

Frauds (Everyday Safety FAQs)

Q1: For Shopkeepers: How can I protect my shop's QR code from being tampered with?

Answer: Use these 3 merchant safeguards: Install an acrylic encased stand where stickers cannot be easily pasted. Inspect your stand physically every morning. Most importantly, install an official soundbox that speaks payment confirmations aloud.

Q2: Do genuine delivery executives ever need an OTP to cancel an order?

Answer: Never. Delivery personnel only require a Delivery Confirmation OTP when handing a package to you. No legitimate logistics firm generates an OTP to cancel or return an unwanted parcel.

Q3: How can I verify if my electricity or water bill is actually overdue?

Answer: Check the official provider app. Open your electricity board's official website, electricity department app, or check your consumer number directly inside your UPI app's "Bill Pay" section. Never trust phone numbers in SMS warnings.

Q4: What should a merchant do if a customer shows a "Payment Successful" screen but no money arrives?

Answer: Do not release goods based on a phone screenshot. Fraudsters frequently use "prank spoofing apps" that mimic payment screens. Always wait for your official soundbox announcement or verify credits directly in your merchant app.

Q5: If I report a fake electricity threat SMS to Chakshu, what action is taken?

Answer: The Department of Telecommunications investigates the flagged phone number. If verified as fraudulent, the scammer's SIM card and phone IMEI are blacklisted across all Indian telecom operators.

Chapter 6: Everyday Shop & Home Safety Dos

and Don'ts (Daily Defense Checklist)

✅ What to Do (Do's)

- Merchants: Listen for the voice soundbox announcement before handing over items.
- Customers: Confirm the payee's name with the shopkeeper before entering your PIN.
- Verify unexpected parcel deliveries by checking your order history in the shopping app.
- Pay utility bills exclusively via trusted apps or official discom counters.

❌ What NOT to Do (Don'ts)

- Never share an OTP over the phone to cancel or decline an unordered parcel.
- Never dial 10-digit mobile numbers mentioned in urgent electricity disconnection SMS.
- Never accept a customer's phone screenshot as proof of payment in your store.
- Never pay unexpected "reactivation" fees through links sent over WhatsApp.

Chapter 6: How to Report SMS Frauds on Sanchar Saathi (Safe Search Guide)

To report spam and deceptive SMS communications on the government's official platform:

1. **Step 1: Enter the Precise Chakshu Reporting Query**

   Search keyword: `Sanchar Saathi Chakshu report suspected fraud communication`

2. **Step 2: Verify the .gov.in Domain**

   Confirm the portal address is strictly `https://sancharsaathi.gov.in`. Official portals in India must carry `.gov.in`.

3. **Step 3: Select the Chakshu Facility**

   Click on "Citizen Centric Services" and select "Chakshu - Report Suspected Fraud Communication".

4. **Step 4: Attach Screenshot & Submit**

   Provide the scammer's phone number, date/time, and a screenshot of the fraudulent message.

🔍 Official Verification Sources for Chapter 6:

- **DoT Sanchar Saathi Chakshu Portal:** `https://sancharsaathi.gov.in`
- **Ministry of Power Consumer Advisory:** `https://powermin.gov.in`
- **NPCI Merchant Advisory on Soundbox Verification:** `https://www.npci.org.in`

CHAPTER 7 • DISPUTE RESOLUTION

Dealing with Payment Failures

Money debited from your account but didn't reach the payee? Don't panic. Understand where your money is, when it returns, and your legal right to ₹100/day bank compensation for delays.

Money Debited but Payee Didn't Receive It — Why Does This Happen?

Sending a payment via UPI is not instantaneous magic; it is an orchestrated handshake between three independent server systems across the internet:

- **Your Bank (Remitter Bank):** Debits the funds from your account.
- **NPCI's Central Switch:** Verifies the transaction and routes funds securely.
- **The Payee's Bank (Beneficiary Bank):** Credits the funds to the recipient.

If any of these three servers experiences momentary latency, network timeouts, or core maintenance, the handshake pauses mid-flight. In banking terms, this is classified as a **Failed Transaction** or **Deemed Approved Transaction**.

The Core Fact

Your Money Never Disappears into Thin Air!

Remember this fundamental truth: money inside the regulated banking network cannot vanish. If debited without reaching the payee, funds sit safely in an automated settlement pool. The system will either complete the credit to the payee or automatically return (**Auto-Reversal**) the full amount to your bank account.

Case Study: Manoj's Stuck Rent & The ₹300 Compensation

On the 1st of the month, Manoj transferred his monthly room rent of ₹4,500 to his landlord via Google Pay. His bank sent an SMS confirming the debit, but his landlord called: *"Manoj, the money hasn't arrived; my app still shows 'Payment Pending'."*

SMART RESPONSE

Manoj Did NOT Transfer a Second Time

Many people make the costly mistake of immediately sending another payment, doubling their out-of-pocket money. Manoj stayed calm. Inside Google Pay, he tapped on the pending transaction, selected **"Raise Dispute / Check Status"**, and recorded his 12-digit **UTR Number**.

Day 1 (T) Transaction pending; in-app dispute registered automatically via UDIR.

Day 2 (T+1) Subsequent business day ended; reconciliation checks underway between banks.

Day 5 On Day 5, the full ₹4,500 refund was credited back to Manoj's account. In addition, under **RBI's TAT Guidelines**, the bank automatically deposited an extra **₹300 delay compensation** (₹100/day for 3 days of delay beyond T+1) without Manoj even having to ask!

RBI's Turn Around Time (TAT) Framework & Mandatory Compensation

Under official RBI directives (*Circular DPSS.CO.PD No.629/02.01.014/2019-20*), the central bank has established strict resolution timelines:

OFFICIAL RBI DIRECTIVE

The T + 1 Business Day Auto-Reversal Rule

T = Date of Transaction
T + 1 = Next Banking Business Day

If your funds are deducted but fail to reach the beneficiary, banks are legally required to automatically credit the funds back to your account by **T + 1 business day**.

LEGAL CONSUMER RIGHT

₹100 Per Day Delay Compensation

If the bank fails to reverse the amount within T + 1 business days, the remitter bank is legally obligated to compensate the customer **₹100 per day** for every day of delay directly into their bank account.

What is UDIR? (Unified Dispute & Issue Resolution)

NPCI launched an automated settlement framework integrated into all certified UPI apps called **UDIR**:

How UDIR Works in Real Time:

In the past, customers had to visit a branch to complain about stuck payments. With UDIR, tapping "Help" or "Check Status" on a pending payment triggers an automated query directly between both banks' Core Banking Systems. Over 85% of pending transactions resolve within minutes without human intervention.

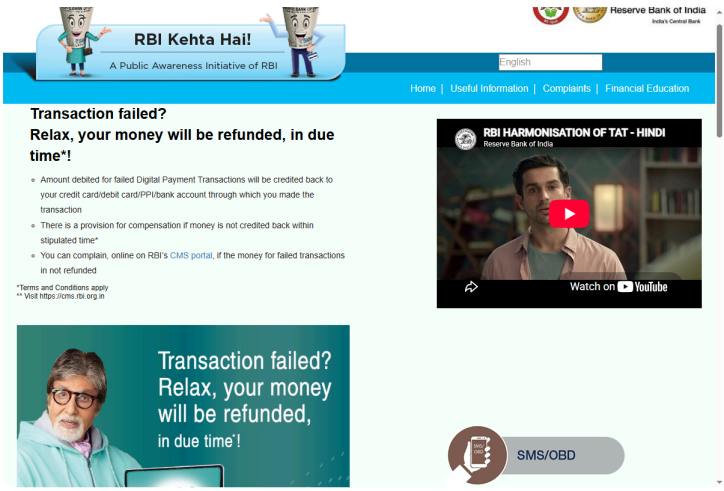
> **The Key Tracking Key:** Always locate your **12-digit UTR Number** (e.g. `4231-XXXX-9812`) on the transaction receipt. This number is your undeniable proof of transaction.

RBI's Official Notification on TAT & Compensation

The Reserve Bank of India transparently publishes its Harmonisation of Turn Around Time (TAT) for failed electronic transactions:

🌐 rbi.org.in / circulars / tat-compensation

OFFICIAL RBI CIRCULAR



📌 **2 Binding Regulatory Mandates from the RBI Circular:**

1. **Automatic Compensation:** Compensation must be credited automatically to the customer's account without requiring a separate claim application.

2. **Applies Across All UPI TPAPs:** This protection applies equally whether you paid via BHIM, Google Pay, PhonePe, Paytm, or direct mobile banking.

Chapter 7: Essential Questions on Failed UPI Transfers (Failed Payment FAQs)

Q1: If my payment status says "Pending", should I pay the store again using cash or another card?

Answer: Wait 3 to 5 minutes first. Most pending transactions either confirm or fail within 180 seconds. If you must leave immediately and choose to pay via cash, take the shopkeeper's phone number and request a refund if the pending UPI transfer later succeeds.

Q2: What should I do if my bank does not credit the ₹100/day compensation for delay?

Answer: File a formal ticket with your bank's Nodal Officer. Quote RBI Circular *DPSS.CO.PD No.629/02.01.014/2019-20*. If unanswered after 30 days, escalate to the **RBI Banking Ombudsman** at `cms.rbi.org.in`.

Q3: What if I transferred money to the wrong phone number by mistake?

Answer: Act immediately: Call your bank with the UTR number, lodge a "Wrong Credit Dispute", and ask the bank to place a lien on the recipient's account. Under RBI guidelines, the beneficiary's bank is required to seek consent from the unintended recipient to reverse funds.

Q4: Does T+1 include bank holidays and Sundays?

Answer: No. 'T' represents the transaction day, while '+1' counts official banking business days. Sundays, 2nd/4th Saturdays, and national holidays are excluded from the business day calculation.

Q5: Can customer care fast-track a stuck transaction on a phone call?

Answer: No. Automated clearing house systems reconcile batches on server schedules. No representative can manually "push" a pending transaction through. Beware of fake agents who claim they can do so for an advance fee.

Chapter 7: Failed Payment Safety Dos and

Don'ts (Payment Failure Checklist)

✅ What to Do (Do's)

- Always note your 12-digit UTR Number for any delayed or failed transaction.
- Use the in-app "Check Status" or "Raise Dispute" button to trigger automated UDIR resolution.
- Allow up to T+1 business days before raising escalations with branch managers.
- Know your statutory right to ₹100/day compensation for delayed reversals.

❌ What NOT to Do (Don'ts)

- Never send a duplicate transfer in a panic without checking your bank passbook/statement.
- Never search for third-party "UPI refund" numbers on social media or search engines.
- Never install remote access tools to claim a pending bank reversal.
- Never share your secret UPI PIN with anyone claiming to represent payment app support.

Chapter 7: How to Search RBI TAT Compensation Rules on Google (Safe Search Guide)

To look up the exact regulatory provisions governing failed electronic transactions:

1. **Step 1: Enter the Precise TAT Framework Query**
   Search keyword: `RBI circular harmonisation of turn around time TAT failed transactions`

2. **Step 2: Check for RBI Domain Origin**
   Verify the link leads to `https://www.rbi.org.in`.

3. **Step 3: Review the Official Framework Table**
   Locate Section 4 of the circular table specifically dedicated to "Unified Payments Interface (UPI)".

4. **Step 4: Keep the Circular Number Handy**
   Quote *Circular DPSS.CO.PD No.629/02.01.014/2019-20* in any written banking escalation.

🔍 Official Verification Sources for Chapter 7:

- **RBI Harmonisation of TAT Circular:** `https://www.rbi.org.in/scripts/FS_Notification.aspx?Id=11693`
- **NPCI Dispute Resolution Portal (UDIR):** `https://www.npci.org.in`
- **RBI Integrated Ombudsman Scheme:** `https://cms.rbi.org.in`

CHAPTER 8 • EMERGENCY PROTOCOL

How to Report UPI Fraud

If defrauded, don't waste time in self-blame or panic. Act decisively. Learn the critical 2-hour 'Golden Hour', the 3 official government reporting channels, and how stolen funds are frozen.

What is the 'Golden Hour' in Cyber Security?

When an unauthorized electronic transaction or online fraud occurs, the initial **2 to 3 hours** immediately following the debit are termed the **'Golden Hour'** by cyber investigation agencies and commercial banks.

Why are these first few hours so decisive? Understanding how cybercriminals launder stolen money explains the urgency:

0 to 15 Minutes	**Initial Credit:** Stolen funds land inside the fraudster's first mule account (a rented or fraudulently opened bank account).
15 to 60 Minutes	**Layering:** To avoid automated tracking, the scammer splits the sum into multiple smaller transfers across 5 to 10 intermediary wallets and accounts.
Within 2 to 3 Hours	**Cash Withdrawal:** An accomplice physically withdraws cash from remote micro-ATMs or rural bank kiosks. Once money turns into

hard paper cash, recovering it becomes exceptionally difficult.

If you report the crime during this **Golden Hour** via official channels, the National Cyber Crime Reporting Portal (CFRMS) triggers instant automated alerts. Banks place an emergency **Lien Mark (temporary freeze)** on the recipient's mule account, locking the funds before they can be withdrawn at an ATM!

Case Study: Rajesh's 25-Minute Alertness & Recovering ₹40,000

Rajesh received a counterfeit SMS stating his electricity would be disconnected by nightfall. In an anxious rush to pay a ₹10 update charge, he clicked a fraudulent link, and **₹45,000** was debited from his savings account.

DECISIVE ACTION

Rajesh Took 3 Immediate Steps in Under 30 Minutes:

> **Rajesh (Thinking):** *"Panicking won't return my money. I must act instantly to freeze the recipient's account!"*

Minute 5 He noted down the 12-digit **UTR Number** from the bank's debit alert SMS.

Minute 12 Inside his UPI app (Google Pay), he flagged the transaction as **"Report Fraudulent Transfer"**.

Minute 25 He accessed the National Cyber Crime Reporting Portal (**cybercrime.gov.in**), lodged a complaint under *"Report Financial Fraud"*, and entered the 12-digit UTR.

> **The Outcome:** The portal immediately transmitted a lien request to the recipient's bank. The fraudster managed to withdraw only ₹5,000, while the remaining **₹40,000 was frozen tight**. Following standard legal procedures, the bank returned the frozen balance back to Rajesh!

4 Critical Pieces of Data to Note on Paper Before Reporting

When filing an emergency complaint, portal forms and helpline officers require exact transaction identifiers. Having these ready saves precious minutes:

🔢

1. 12-Digit UTR Number

The Unique Transaction Reference number printed on the bank SMS and app receipt (e.g. `4231-XXXX-8921`).

⏱️

2. Exact Date and Timestamp

The precise minute when the debit SMS was generated by your bank.



3. Recipient's UPI ID & CBS Name

The VPA or phone number to which funds were routed, along with the recipient's name displayed on the payment receipt.



4. Your Bank Account Number

The specific account from which money was debited, plus the last 4 digits of your debit card.

The 3 Official Channels to Report Financial Fraud

CHANNEL 1 **Inside Your UPI App (Immediate Flagging)**

Open your payment app (Google Pay, PhonePe, Paytm, BHIM) → Navigate to *Transaction History* → Select the fraudulent payment → Tap **"Report a Problem"** or **"Have an Issue with This Payment"** → Select *"Fraudulent Transaction"*.

CHANNEL 2

Your Bank's 24×7 Emergency Helpline & Home Branch

Call your bank's verified emergency card/banking hotline. Demand that your NetBanking, UPI facility, and debit card be blocked immediately. Within 24 hours, visit your home branch and submit a formal written complaint for **Unauthorized Electronic Debit** to preserve your rights under RBI's Zero Liability framework.

CHANNEL 3 (MOST CRITICAL)

National Cyber Crime Reporting Portal (cybercrime.gov.in)

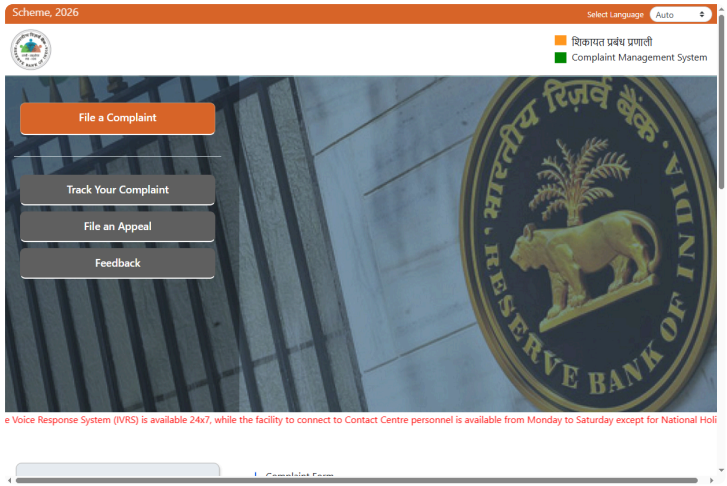
Submit an emergency incident report immediately on **cybercrime.gov.in** under *"Report Financial Fraud"*, or contact the emergency response line listed on the official portal's homepage, operated by the Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs.

RBI's Official Complaint Management System (CMS)

If your bank does not resolve your unauthorized debit complaint within 30 days, escalate directly to the **RBI Banking Ombudsman**:

cms.rbi.org.in

OFFICIAL RBI OMBUDSMAN



📌 **Official Escalation Path under RBI Integrated Ombudsman Scheme:**

1. **30-Day Resolution Window:** Give your bank 30 days to resolve your written grievance. If unsatisfied or unanswered, lodge a case on `cms.rbi.org.in`.

2. **Statutory Authority:** The RBI Ombudsman holds independent legal authority to order full refunds and compensation if banks fail to adhere to security directives.

Chapter 8: Essential Questions on Reporting UPI

Fraud (Cyber Complaint FAQs)

Q1: What is the fastest alternative to register an emergency cyber fraud complaint?

Answer: Go directly to cybercrime.gov.in. Click on *"Report Financial Fraud"* and submit the incident details online. Online reports feed directly into the central Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS).

Q2: Do I have to physically visit a police station to file a cyber complaint?

Answer: Not initially. Lodging an emergency ticket via `cybercrime.gov.in` creates an official digital FIR/complaint acknowledged across all Indian states. You may later be requested to submit bank statements to your local district cyber cell.

Q3: What happens once a scammer's bank account is frozen with a "Lien"?

Answer: The recipient cannot withdraw, transfer, or spend the locked money. After cyber police complete their preliminary verification, the court or magistrate issues an order directing the beneficiary bank to transfer the funds back to the rightful victim.

Q4: Is there any fee to report cyber fraud or access the Banking Ombudsman?

Answer: Completely free. Neither the National Cyber Crime Portal nor the RBI Banking Ombudsman charges any filing fees. Never pay third-party agents who claim to recover lost funds for an upfront commission.

Q5: Should I retain my old phone if I suspect it was infected by malware?

Answer: Yes, keep it as legal evidence. Disconnect Wi-Fi and mobile data (or enable Airplane Mode), but do not wipe or factory reset the device until forensic screenshots and APK logs are examined by investigating officers.

Chapter 8: Fraud Reporting Dos and Don'ts

(Emergency Action Checklist)

✅ What to Do (Do's)

- Note down the 12-digit UTR number from your SMS alert immediately.
- Lodge an online complaint on cybercrime.gov.in within the Golden Hour.
- Block your mobile banking and card facilities via your bank's verified helpline.
- Keep all screenshots of fake SMS, transaction IDs, and call logs safe as evidence.

❌ What NOT to Do (Don'ts)

- Never waste time arguing or pleading with the scammer over phone calls.
- Never hire private "ethical hackers" or recovery agents found on Instagram or Telegram.
- Never delete transaction SMS notifications or format your smartphone immediately.
- Never delay filing a formal written complaint with your home bank branch.

Chapter 8: How to Search cybercrime.gov.in on Google (Safe Search Guide)

To access the legitimate portal of the Ministry of Home Affairs without landing on fake phishing pages:

1 **Step 1: Use the Exact Official Domain**

Search keyword: `National Cyber Crime Reporting Portal official website cybercrime gov in`

2 **Step 2: Confirm the .gov.in Domain**

The URL must strictly be `https://cybercrime.gov.in`. Beware of imitation domains like `cybercrime-portal.in` or `report-fraud.org`.

3 **Step 3: Look for the Government Emblem**

The genuine homepage features the official Ashoka Lion Capital emblem and National Informatics Centre (NIC) security seals.

4 **Step 4: Bookmark the Official Portal**

Bookmark **cybercrime.gov.in** across your household devices for instant access during emergencies.

🔍 **Official Verification Sources for Chapter 8:**

- **National Cyber Crime Reporting Portal:** `https://cybercrime.gov.in`
- **RBI Complaint Management System (CMS):** `https://cms.rbi.org.in`
- **Indian Cyber Crime Coordination Centre (I4C), MHA:** `https://www.mha.gov.in`

CHAPTER 9 • EMERGING THREATS (ARTIFICIAL INTELLIGENCE)

AI Voice Cloning & Video Calls

When you hear your child's exact voice crying for help or see an officer in uniform over video call: learn the reality of AI-generated scams, the truth behind "Digital Arrests", and practical counter-measures.

AI Voice Cloning: The Perfect Digital Imitation

Modern **Artificial Intelligence (AI)** tools can clone anyone's voice using as little as **3 to 5 seconds** of clean audio extracted from public social media videos, reels, or recorded phone calls.

In cybersecurity, this is called **AI Voice Cloning** or synthetic voice generation. Software mimics vocal timbre, pitch, regional accents, and emotional inflections with chilling precision.

⚠ **HOW THE SCAM WORKS IN 3 STEPS:**

The Mechanics of Synthetic Voice Extortion:

- **Voice Harvesting:** Fraudsters download short audio clips from public Instagram reels, YouTube shorts, or Facebook videos posted by your children or relatives.
- **Script Generation:** They input distress scripts into AI voice software: *"Dad, please help me! I met with a terrible car accident, and the police have detained me!"*

- **Targeted Emergency Call:** The cloned audio is played over an incoming phone call to the parents, followed immediately by a fake police officer demanding urgent UPI settlement.

Case Study: Mr. Sharma's Phone Call & The 1-Question Test

58-year-old Ramesh Sharma was at his office when his phone rang from an unknown number. When he answered, the crying, panicked voice of his son Rohit—who works in Bengaluru—shook him to his core:

THE REAL SCENARIO

The Counterfeit AI Emergency Call:

> **Voice (Sounding exactly like Rohit):** *"Papa! I am in severe trouble... my friend's car struck a pedestrian. The police have locked me up in the local station. Please speak to the Inspector and do whatever he says, or they will remand me to central jail!"*
>
> **Fake Police Inspector (Authoritative Tone):** *"Mr. Sharma, your son is in our custody. If you want to settle the matter without an FIR, transfer ₹50,000 immediately to this government verification UPI ID. If you hang up, he goes behind bars!"*

Mr. Sharma's hands trembled. The voice matched Rohit's tone and cries so perfectly that any parent would have transferred money on the spot. But then Mr. Sharma

remembered a simple rule.

> **Mr. Sharma Asked Firmly:** *"Rohit, if that is really you, tell me our pet dog's name."*
>
> **Total Silence from the Scammer:** The caller stuttered, cursed in frustration, and abruptly disconnected the line!

> **The Outcome:** Mr. Sharma dialed Rohit's regular personal mobile number. Rohit answered calmly from his office cafeteria, eating lunch with colleagues—completely safe! That single verification question saved ₹50,000 and immense emotional distress.

Deepfake Video Calls & The 'Digital Arrest' Myth

Fraudsters also employ real-time **Deepfake Video** filters. Posing as law enforcement officers, they dress in counterfeit uniforms and sit in front of artificial police station backdrops during Skype or WhatsApp video calls.

⚖️ Indian Law Does NOT Recognize 'Digital Arrest'!

Under the Constitution of India, the Code of Criminal Procedure (CrPC), and the Bharatiya Nagarik Suraksha Sanhita (BNSS), **there is no legal concept called "Digital Arrest."**

> **1. Police Never Arrest Anyone Over Video Calls:** Legitimate arrests require police officers to be physically present, carry

official identification, and serve written legal warrants.

2. Law Enforcement Never Demands UPI Transfers: Neither the CBI, ED, Income Tax Department, Customs, nor State Police ever ask citizens to transfer money to "secure verification accounts" or private UPI addresses for clearance or bail.

3. Demanding You Stay on Camera is Pure Coercion: Scammers order victims: *"Do not hang up; stay on camera inside a locked room."* They do this solely to prevent you from consulting relatives, lawyers, or local police.

4 Bulletproof Defenses Against AI Frauds

1. **Create a Secret Family 'Safe Word'**

   Agree on a confidential codeword (e.g. a childhood nickname, favorite holiday spot) known only to immediate family. If anyone calls claiming an emergency, ask for the safe word.

2. **Hang Up & Call Back on Their Known Number**

   Never rely on incoming caller ID. Disconnect the call and ring your child, spouse, or friend directly on their saved regular phone number.

3. **Look for Visual Deepfake Artifacts**

   Real-time deepfakes struggle with natural motion. Look for unnatural eye blinking, mouth desynchronization, blurred cheek edges, or robotic

voice delays.

4 **Report to cybercrime.gov.in & Alert Local Police**

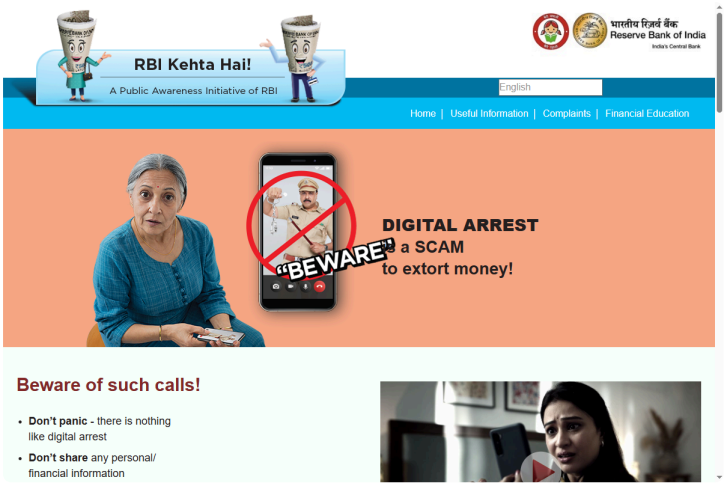
If someone threatens you with "Digital Arrest", hang up immediately. Report the incident directly on **cybercrime.gov.in** or visit your local police station.

RBI & Government Public Warning on Digital Arrests

The Reserve Bank of India, alongside the Ministry of Home Affairs, has issued prominent advisories warning citizens against Digital Arrest scams:

🌐 rbi.org.in / press-releases / digital-arrest-warning

OFFICIAL ADVISORY



📌 **Official Directive from the Central Government:**

1. **Zero Monetary Transfers:** Never transfer funds to any account claiming to be a "Secret RBI Vault" or "Judicial Clearance Escrow". No such accounts exist.

2. **Immediate Disconnect:** Citizens receiving threats of digital arrest are advised to sever the call immediately without engaging in discussion.

Chapter 9: Questions on AI Voice Cloning & Digital Arrest (AI Safety FAQs)

Q1: How can fraudsters clone a voice without having spoken to the person previously?

Answer: Through public social media posts. Videos posted publicly on Instagram, Facebook, LinkedIn, or YouTube provide ample audio samples for AI synthesis models. Setting social media accounts to private helps restrict unauthorized data harvesting.

Q2: What should I do if a caller claims my son is in an ICU and needs immediate hospital payment?

Answer: Call the hospital directly or call your child's friends. Ask the caller for the doctor's registration number and hospital reception landline. Never transfer money to personal UPI accounts based solely on panic-inducing phone calls.

Q3: Can genuine police officers demand bail money via UPI?

Answer: Absolutely never. Bail bonds are legal instruments processed strictly through judicial magistrates and bank challans inside court premises. No police officer accepts bail payments via mobile UPI.

Q4: Why do deepfake callers insist on using Skype or WhatsApp Video?

Answer: Video calls allow them to display counterfeit law enforcement insignia, logos, and forged official documents to create an intimidating sensory atmosphere.

Q5: Is it legal to record phone calls with suspected scammers?

Answer: Yes, and it serves as valuable evidence. Audio recordings and call logs help cyber investigators trace IP telephony gateways and identify synthetic speech models.

Chapter 9: AI Scam Protection Dos and Don'ts (AI Defense Checklist)

✅ What to Do (Do's)

- Establish a secret family codeword for genuine distress emergencies.
- Verify unexpected emergency claims by calling the relative on their known number.
- Know that "Digital Arrest" is 100% fictional under Indian legal statutes.
- Report extortion numbers immediately on cybercrime.gov.in and sancharsaathi.gov.in.

❌ What NOT to Do (Don'ts)

- Never transfer money in response to frantic, high-pressure emergency calls.
- Never stay confined to a room under video surveillance on an unverified call.
- Never believe callers claiming to represent the CBI, ED, or Interpol on WhatsApp.
- Never post high-resolution voice clips and unlisted family numbers on open forums.

Chapter 9: How to Search RBI Advice on Digital Arrest on Google (Safe Search Guide)

To access official advisories regarding AI impersonation and Digital Arrest scams:

1. **Step 1: Enter the Precise Digital Arrest Query**
   Search keyword: `MHA I4C official advisory on digital arrest scam cybercrime`
2. **Step 2: Prioritize Government Domains**
   Check for links originating from `https://www.mha.gov.in`, `https://cybercrime.gov.in`, or `https://pib.gov.in` (Press Information Bureau).
3. **Step 3: Review PIB Fact Check Reports**
   PIB Fact Check issues regular alerts disproving fake arrest warrants and fraudulent government seal documents used by scammers.
4. **Step 4: Share Official Notices**
   Forward verified government advisories to neighborhood WhatsApp and community groups.

🔍 Official Verification Sources for Chapter 9:

- MHA Indian Cyber Crime Coordination Centre (I4C): https://www.mha.gov.in
- Press Information Bureau (PIB) Fact Check: https://factcheck.pib.gov.in
- National Cyber Crime Portal Advisories: https://cybercrime.gov.in

CHAPTER 10 • TECHNICAL SPOOFING

Fake Screenshots & Spoofed Apps

Merchants and everyday users beware: a phone screenshot shown by a customer is never legal proof of payment. Learn how prank spoof apps fabricate success screens and how to verify real credits.

The Illusion of Spoof Apps and Fake Payment Screens

Numerous illicit **Spoof Apps** (often disguised on third-party forums as "Pay Prank" or "Fun Payment Generators") mimic the exact visual interfaces of Google Pay, PhonePe, and Paytm.

In less than 5 seconds, a fraudster types the shopkeeper's business name and bill amount. The app generates an authentic-looking payment screen complete with official fonts, a vibrant green tick, counterfeit UTR numbers, and simulated audio chimes. The scammer thrusts their phone forward: *"Look bhaiya, money sent! Green tick is visible, and screenshot sent on WhatsApp!"*—and attempts to leave with the goods.

⚠ **THE HARSH REALITY: A SCREENSHOT IS JUST PIXELS!**

A screenshot is merely a static graphical image displayed on glass. It has zero cryptographic connection to the banking network (NPCI or Core Banking Systems). Anyone

with basic graphic software or a spoof app can fabricate a "Successful Payment" screen for any amount between ₹10 and ₹10,00,000.

Case Study: Store Owner Mohan Lal & The Fake ₹18,000 Green Tick

Mohan Lal operates a consumer electronics shop in Jaipur. One evening, a well-dressed customer arrived hurriedly, selecting a premium ₹18,000 portable Bluetooth speaker.

MERCHANT VIGILANCE

The "I Am Rushing to the Airport" Ploy

> **Customer (Agitated):** *"Bhaiya, please pack it quickly; my airport cab is waiting outside. I scanned your stand and sent ₹18,000. See, the green checkmark appeared on my PhonePe screen!"*
>
> **Mohan Lal:** *"Sir, please hold on one moment. My merchant soundbox hasn't announced the payment, and my balance has not updated."*
>
> **Customer (Feigning Anger):** *"Look at my phone screen! Do you think I am lying? Your bank server is probably slow. Take a photo of my screen for your records!"*

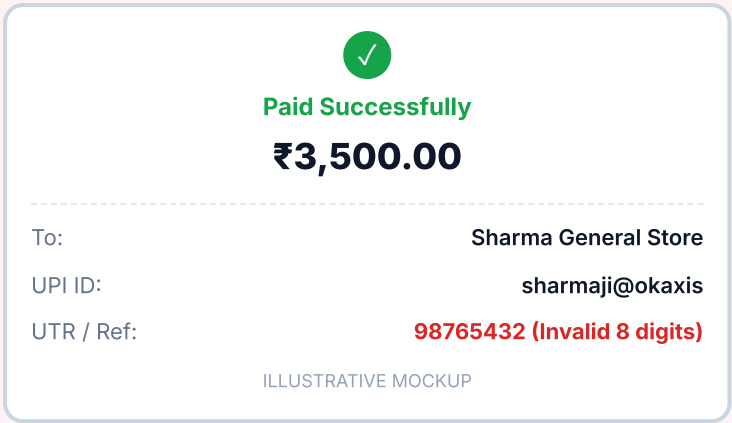
Unfazed by the customer's staged outrage, Mohan Lal opened his official merchant passbook app. His ledger showed no credit entry. When Mohan suggested: *"Sir, no problem—let us walk to the ATM next door to withdraw cash while the network clears,"* the customer slipped his phone into his pocket and quietly disappeared into the crowd!

> **The Takeaway:** By refusing to trust a customer's phone display and relying strictly on his own banking app and soundbox, Mohan Lal saved his business from an ₹18,000 loss.

Comparison: Fake Screenshot vs. Real Bank Confirmation

Notice the telling flaws in counterfeit screens compared to authentic banking alerts:

❌ Fake Spoof App Screenshot



⚠️ **Fatal Flaw:** Valid UPI UTR numbers are always exactly 12 numeric digits (e.g. `4231-XXXX-9812`), never 8 or 10 digits.

✅ Authentic Merchant Soundbox & Bank SMS

Voice Announcement: "Received ₹3,500 on PhonePe Merchant Account"

From: VK-SBIPAY (Official 6-char Alpha Header)

"Your A/c ••4821 is credited by Rs 3,500.00 on 08-Nov-2026 by UPI ref no 4312-XXXX-8912 - SBI"

How to Verify 6-Character Bank SMS Sender IDs

Telecom Regulatory Authority of India (TRAI) regulations require all commercial financial institutions to send SMS only via registered 6-character alphanumeric sender IDs:

GENUINE BANKING HEADER

`VK-SBIPAY`

,

`AD-HDFCBK`

,

`BZ-ICICIB`

The first two letters identify the telecom operator and circle; the remaining characters represent the licensed bank.

COUNTERFEIT / FRAUDULENT SENDER

`+91 98XXX-XXXXX`

,

`+91 76XXX-XXXXX`

Any credit or debit SMS arriving from a standard 10-digit mobile number is 100% fake. Banks NEVER send alerts from personal numbers.

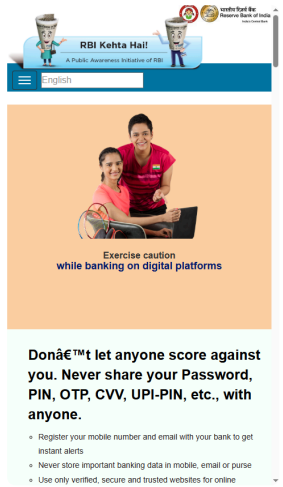
RBI's Official Advisory on Safe Banking Web

Portals

The Reserve Bank of India cautions businesses and citizens regarding cloned banking interfaces:

🌐 rbi.org.in / financial-education / spoofing

OFFICIAL RBI GUIDE



📌 **2 Official Directives for Store Owners:**

1. **Merchant-Side Verification:** Never rely on visual confirmation on customer handsets. Verify credits directly within your business settlement app.

2. **Examine 12-Digit UTR Length:** Authentic banking settlement logs always reflect an unbroken 12-digit numeric sequence.

Chapter 10: Essential Questions on Fake Screenshots & Spoofed Apps (Screenshot Verification FAQs)

Q1: Why do customers claim money was deducted from their account when my soundbox didn't alert?

Answer: Two possibilities exist: Either the customer is deliberately displaying a spoof app screen, or a genuine transaction is temporarily stuck in banking clearing (pending status). Ask the customer to check their official bank SMS or passbook to verify actual debit.

Q2: Can someone forge a bank SMS on my phone?

Answer: They cannot forge an incoming SMS on your phone. Scammers might forward you an SMS or show a text on their device. As long as you examine your own SMS inbox for registered 6-character headers, you are secure.

Q3: Is an audio voice soundbox mandatory for small shops?

Answer: Highly recommended. Soundboxes eliminate payment ambiguity during chaotic store rushes by announcing received amounts loudly in the shopkeeper's preferred language.

Q4: What should a merchant do if a scammer attempts to leave with goods using a spoof screen?

Answer: Politely decline to release merchandise. Explain that store protocol requires soundbox or merchant app confirmation. If the customer becomes aggressive, alert neighboring shopkeepers or call the local police.

Q5: Can WhatsApp payment screenshots be accepted for remote deliveries?

Answer: Never dispatch goods based on WhatsApp images. Log in to your merchant dashboard or check your bank account balance to ensure funds have settled before handing items to couriers.

Chapter 10: Fake Screenshot Defense Dos and Don'ts (Merchant Verification Checklist)

✅ What to Do (Do's)

- Rely exclusively on your own soundbox, merchant app, or bank SMS alerts.
- Verify that the UTR number contains exactly 12 numeric digits.
- Check SMS sender IDs for genuine 6-character alphanumeric bank headers.
- Train retail staff to never release merchandise based solely on customer screen displays.

❌ What NOT to Do (Don'ts)

- Never accept customer phone screenshots or forwarded WhatsApp images as payment proof.
- Never trust credit notifications originating from standard 10-digit mobile numbers.
- Never let rushed or aggressive customer behavior override payment verification protocols.
- Never install third-party APKs promising to "reconcile" unverified payments.

Chapter 10: How to Verify Official Bank Web Portals on Google (Safe Search Guide)

When accessing online banking portals to verify merchant account balances, avoid cloned websites:

1. **Step 1: Type the Official URL Directly**
   Instead of searching Google, type the official address directly into your address bar (e.g. `https://www.onlinesbi.sbi` or `https://www.hdfcbank.com`).

2. **Step 2: Check for Domain Extensions**
   Indian banks predominantly use `.bank.in`, `.co.in`, or brand TLDs like `.sbi`. Avoid lookalike domains like `sbi-netbanking.online`.

3. **Step 3: Verify Secure HTTPS Connection**
   Ensure the browser displays a padlock icon indicating genuine SSL/TLS encryption before entering credentials.

4. **Step 4: Bookmark Official Business Dashboards**
   Save your verified merchant portal to your browser bookmarks for secure one-click access.

🔍 Official Verification Sources for Chapter 10:

- RBI Cyber Security Directions for Commercial Banks: https://www.rbi.org.in
- TRAI SMS Sender ID Registry Framework: https://www.trai.gov.in
- NPCI Merchant Settlement Standards: https://www.npci.org.in

CHAPTER 11 • DECEPTIVE TRAPS (SMISHING & FAKE LINKS)

Malicious Links & Smishing

Fake SMS and WhatsApp messages threatening power cuts, claiming pending courier deliveries, or promising scratch-card jackpots. Discover how malicious links operate and how to protect yourself.

What is Smishing? Fraud Delivered via Text Messages

When cybercriminals dispatch deceptive SMS or WhatsApp texts containing malicious website links, cybersecurity specialists term the attack **Smishing (SMS Phishing)**.

The fraudster's objective is to startle or excite you into tapping a link without thinking. Once clicked, the malicious page attempts to capture your **UPI PIN**, steal one-time bank **OTPs**, or trick you into installing remote control malware.

⚠ The 4 Most Frequent Scam Messages in India:

1. Power Disconnection Threats

"Dear Customer, your Electricity power will be disconnected tonight at 9:30 PM from the electricity office because your previous month

bill was not updated. Immediately pay your bill by clicking here: bit.ly/power-pay-xyz"

The Truth: Electricity boards never issue late-night disconnection warnings from personal 10-digit mobile numbers with shortened links.

2. Bank Account or KYC Suspension Alerts

"SBI/HDFC Alert: Your NetBanking account will be suspended today due to pending PAN KYC. Update immediately to keep your account active: sbi-kyc-verify.online"

The Truth: Banks never send SMS links directing customers to type confidential banking credentials or UPI PINs on external websites.

3. Jackpots, Lotteries & Massive Cashback Lures

"Congratulations! You have received a scratch card worth INR 4,999 on PhonePe/Paytm. Claim your instant cashback directly in your bank account: paytm-reward-claim.site"

The Truth: Legitimate UPI rewards deposit directly into your bank without requiring you to visit external links or enter your PIN.

4. Courier Parcel Re-Delivery Fee

"India Post / Courier: Your parcel cannot be delivered due to wrong house address. Please confirm your details and pay INR 5 re-delivery fee here: indiapost-track.click"

The Truth: India Post and reputable couriers never demand nominal debit payments through unsolicited SMS links to complete deliveries.

The Threat of Malicious .apk Files on Android Handsets

Android smartphones allow sideloading of applications via package files ending in `.apk`. Fraudsters exploit this to distribute spyware disguised as innocent utilities:

How a Rogue APK Compromises Your Bank Account:

- **Disguised Names:** Files are deceptively labeled `Electricity_Update.apk`, `Quick_Support.apk`, or `PM_Yojna_Bonus.apk`.
- **Excessive Permissions:** Upon installation, the malware requests permission to "Read SMS" and "View Screen (Accessibility Service)".
- **Silent OTP Interception:** When your bank sends an OTP for a debit transaction, the malware intercepts the code in the background and forwards it to the scammer's server without displaying a notification to you!

> 🛡️ **Rule of Law:** Never install an app distributed over WhatsApp, Telegram, or SMS links. Only download software directly through the official **Google Play Store**.

Case Study: Suresh & The ₹4,999 Scratch Card Trap

Suresh received a WhatsApp message with an attractive graphic claiming he had won a ₹4,999 festive scratch card.

THE CLICK TRAP

Curiosity Overrides Caution

Suresh tapped the link. A browser window opened displaying a gold coin graphic and a green button labeled: *"Transfer ₹4,999 to Your Bank"*.

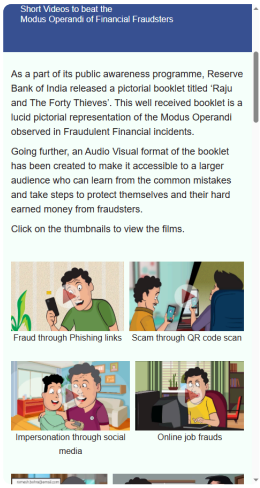
Tapping the button automatically launched his PhonePe app. The screen asked for his 4-digit UPI PIN. Suresh thought: *"Entering my PIN must be the verification needed to credit the money."*

> The instant his PIN was entered, his phone vibrated with an SMS from his bank: **₹4,999 DEBITED** from his savings account. Instead of receiving a reward, Suresh had authorized a direct payment to the scammer's UPI ID!

RBI's Public Awareness Campaign on Phishing Links

The Reserve Bank of India runs prominent public alerts against clicking unverified hyperlinks in electronic communications:

rbi.org.in / rbikehtahai / phishing **OFFICIAL RBI GUIDE**



📌 **2 Official Directives from the RBI Phishing Campaign:**

1. **Inspect Web Domains:** Never input sensitive credentials on websites hosted on suspicious extensions like `.xyz`, `.site`, `.top`, or `.club`.

2. **Banks Never Request PINs:** No legitimate financial institution sends messages asking users to click links to verify PINs or update credentials.

Chapter 11: Essential Questions on Fake Links & Smishing (Smishing Defense FAQs)

Q1: If I accidentally clicked a suspicious link but closed the

page immediately, is my bank account safe?

Answer: Yes, in most cases. Merely opening a web page rarely causes an unauthorized bank debit unless you downloaded an APK file, entered your UPI PIN, or revealed your OTP on that page. As an added precaution, clear your mobile browser's cookies and cached data.

Q2: How do I spot a shortened fake link (like bit.ly or tinyurl) before tapping it?

Answer: Official banks and government departments never use public link shorteners (such as `bit.ly`, `tinyurl.com`, or `is.gd`) for transactional messages. If an SMS uses a shortened link, it is an immediate red flag.

Q3: What should I do if an APK file downloaded automatically on my phone?

Answer: Do not open or install it. Open your phone's File Manager, go to the "Downloads" folder, select the `.apk` file, and delete it permanently.

Q4: Can Truecaller reliably identify scam SMS messages?

Answer: It helps, but cannot be relied on 100%. Truecaller flags numbers previously reported by other users, but cybercriminals purchase fresh bulk SIM cards daily that haven't yet been community-reported.

Q5: Why do fraudsters send messages on WhatsApp instead of regular SMS?

Answer: WhatsApp allows them to display counterfeit corporate logos as profile pictures, bypass telecom operator spam filters, and attach multimedia mockups to appear legitimate.

Chapter 11: Link Safety Dos and Don'ts (Phishing Protection Checklist)

✅ What to Do (Do's)

- Verify unexpected bank alerts by opening your official banking app directly.
- Delete and report suspicious SMS texts immediately on DoT's Chakshu portal.
- Keep Google Play Protect enabled on your Android phone to block rogue apps.
- Check the full domain name in your browser's address bar before interacting.

❌ What NOT to Do (Don'ts)

- Never tap links received in messages warning of imminent power disconnection.
- Never install `.apk` files received through WhatsApp, Telegram, or SMS.
- Never enter your secret UPI PIN on any web browser page.
- Never forward unverified lottery or cashback messages to family groups.

Chapter 11: How to Search RBI Phishing Advisories on Google (Safe Search Guide)

To locate verified advisories on smishing and phishing schemes issued by regulatory authorities:

1. **Step 1: Enter the Precise Phishing Query**

   Search keyword: `RBI Kehta Hai phishing links smishing awareness circular`

2. **Step 2: Confirm Originating Domain**

   Verify that results lead to `https://www.rbi.org.in` or `https://rbikehtahai.rbi.org.in`.

3. **Step 3: Read Specific Case Vignettes**

   RBI's educational portal features illustrated case vignettes demonstrating how deceptive links redirect users to counterfeit payment screens.

4. **Step 4: Educate Older Family Members**

   Share these official illustrations with elderly relatives who may be vulnerable to high-pressure disconnection texts.

🔍 Official Verification Sources for Chapter 11:

- **RBI Cyber Security Awareness Portal:** `https://rbikehtahai.rbi.org.in`
- **Indian Computer Emergency Response Team (CERT-In):** `https://www.cert-in.org.in`
- **DoT Sanchar Saathi Reporting Facility:** `https://sancharsaathi.gov.in`

CHAPTER 12 • DEVICE HARDENING

Securing Your Smartphone

UPI security depends not only on your secret PIN, but on your smartphone's operating system settings. Learn why screen lock and UPI PIN must never match, how to audit app permissions, and how to block a lost phone instantly.

Screen Lock Passcode vs. UPI PIN: Never Make Them Identical

Your smartphone is not merely a communication handset; it is your entire digital banking branch in your pocket. If your physical handset is vulnerable, your bank account cannot remain secure.

Millions of users make one critical mistake for convenience: the 4-digit PIN they use to unlock their phone screen (e.g., `1234`, `2580`, or their birth year `1988`) is the exact same code they use as their **UPI PIN**!



Always Keep Screen Passcode & UPI PIN Distinct

If a stranger on a bus or a coworker glances at your fingers while you unlock your phone, they only see your screen code. But if both codes match, they gain full access to drain your bank balance!

Enable Biometrics (Fingerprint / Face ID)

Use biometrics for daily device unlocking. Biometrics cannot be shoulder-surfed in crowded spaces. Keep your backup alphanumeric passcode complex.

Set Auto Screen-Lock to 30 Seconds

In your phone's Display Settings, set screen timeout to 30 seconds. Leaving an unlocked phone unattended on a restaurant or office table is an open invitation to fraud.

Case Study: Alok's Shared Cab Ride & The Matching PIN Error

28-year-old Alok was commuting home from work in a shared cab in Noida. In the cab, he typed `2580` to unlock his phone. The passenger seated next to him observed the numbers.

THE COST OF CARELESSNESS

Left Behind on the Backseat: An Empty Account

> **Alok (Hurriedly exiting):** *"Bhaiya, stop here; my apartment gate is here!"* (He accidentally left his phone on the back seat).

> **Fellow Passenger (Thinking):** *"His screen passcode was 2580. Let me open PhonePe and test if his UPI PIN is identical..."*

The co-passenger unlocked the handset, opened PhonePe, initiated a ₹25,000 transfer to an accomplice's account, and entered `2580`. The PIN was identical—and the transaction completed instantly!

> **The Essential Lesson:** Had Alok maintained a distinct screen password and a separate secret UPI PIN, the thief would have held a locked brick while his ₹25,000 savings remained 100% safe.

App Permissions Audit: Controlling Sensitive Access

Whenever you install an app, it requests device permissions. Granting sensitive permissions to rogue utilities can expose your banking security:

🚨 **THE MOST DANGEROUS PERMISSION: ACCESSIBILITY SERVICES**

Accessibility Services are designed for users with disabilities to read screen elements aloud. When granted to an unverified app, it allows the app to read everything on your display—including OTPs, passwords, and banking screens—and simulate touch events automatically!

How to Conduct a Quick Monthly Permission Audit:

- **Settings → Apps → Permission Manager:** Inspect which apps have access to *SMS*, *Contacts*, and *Camera*.
- **Revoke SMS Access for Non-Messaging Apps:** Flashlight apps, casual games, and calculators never need SMS permissions.
- **Turn Off "Install Unknown Apps":** Go to Settings → Security → *Install Unknown Apps (Sideloading)* and ensure it is turned OFF for all browsers and file managers.

Lost or Stolen Phone? Block It Nationwide via CEIR

The Department of Telecommunications (DoT) operates the **Central Equipment Identity Register (CEIR)** on `sancharsaathi.gov.in`:

How CEIR Protects Your Identity & Banking:

If your phone is stolen, logging into CEIR and submitting your 15-digit **IMEI number** blacklists the device across all Indian telecom providers (Airtel, Jio, Vi, BSNL). Even if the thief swaps the SIM card or formats the handset, the device cannot connect to any Indian cellular network.

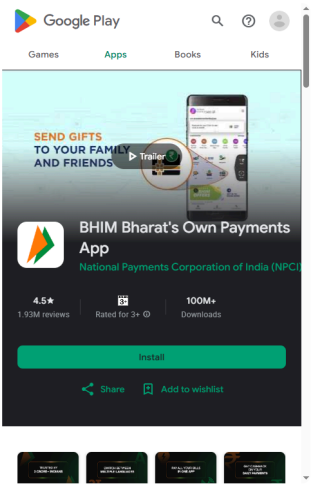
> 💡 **Action Today:** Dial `*#06#` on your phone right now. Note your 15-digit IMEI numbers in a secure home diary.

Official Google Play Store Verification for UPI Apps

Always verify verified publisher badges and download counters before installing payment apps:

play.google.com / store / bhim-official

OFFICIAL STORE BADGE



📌 **2 Verification Marks on Google Play Store:**

1. **Verified Developer Name:** Confirm developer says *"National Payments Corporation of India"* or official bank corporate names.

2. **Download Counts & Ratings:** Official payment apps feature millions of downloads (e.g. 50M+ or 100M+). Clone apps typically display fewer than 10,000 installs.

Chapter 12: Essential Questions on Smartphone & Device Security (Device Security FAQs)

Q1: Is it safe to use UPI apps on public Wi-Fi networks (e.g. at railway stations or cafes)?

Answer: Safe, but mobile data is preferred. UPI traffic is encrypted with bank-grade TLS protocols. However, public Wi-Fi networks are prone to DNS spoofing and man-in-the-middle risks. For financial transactions, cellular mobile data (4G/5G) is always the safer choice.

Q2: What is SIM Swap Fraud, and how can I prevent it?

Answer: Fraudsters pose as you to obtain a duplicate SIM from telecom stores. If your phone suddenly shows "No Service" or loses cellular reception for no obvious reason, contact your mobile operator immediately from another phone. Enable a **SIM Card PIN** in phone settings.

Q3: Should I root (Android) or jailbreak (iPhone) my smartphone?

Answer: Never. Rooting strips away operating system sandboxing, allowing rogue apps to inspect the private memory of other apps, completely defeating UPI and banking security controls.

Q4: How does Google Play Protect safeguard UPI transactions?

Answer: Play Protect automatically scans installed apps daily for known spyware, Trojans, and rogue accessibility service abuse, alerting you to remove hazardous software.

Q5: What should I do immediately if I misplace my phone in a public venue?

Answer: Follow this 3-step sequence: First, call your telecom provider to block your SIM card so OTPs cannot be received. Second, call your bank to freeze UPI and NetBanking. Third, log into `sancharsaathi.gov.in` to blacklist the phone's IMEI.

Chapter 12: Smartphone Hardening Dos and

Don'ts (Phone Defense Checklist)

✅ What to Do (Do's)

- Keep your phone screen passcode completely different from your UPI PIN.
- Set up biometric authentication (fingerprint/face unlock) on your device.
- Dial *#06# today and record your 15-digit IMEI numbers in a home diary.
- Install software updates and security patches promptly when notified.

❌ What NOT to Do (Don'ts)

- Never use predictable screen lock codes like 1234, 0000, 2580, or your birth year.
- Never grant Accessibility Service permissions to unverified utility apps.
- Never enable "Install from Unknown Sources" for browsers or messaging apps.
- Never leave your smartphone unattended and unlocked on public tables.

Chapter 12: How to Verify Official Apps on Google Play (Safe Search Guide)

When searching for and downloading UPI applications, follow these store verification standards:

1. **Step 1: Search Inside Google Play Store Directly**
   Search query: `BHIM Making India Cashless NPCI official app`

2. **Step 2: Inspect Developer Name**
   Ensure the developer name reads **"National Payments Corporation of India"**.

3. **Step 3: Check Reviews and Downloads**
   Legitimate apps possess millions of active reviews. Clones show minimal feedback and suspicious 5-star bot comments.

4. **Step 4: Enable Play Protect**
   Open Play Store → Tap Profile icon → Tap *Play Protect* → Ensure "Scan apps with Play Protect" is turned on.

🔍 Official Verification Sources for Chapter 12:

- **DoT Central Equipment Identity Register (CEIR):** `https://ceir.sancharsaathi.gov.in`
- **CERT-In Smartphone Security Guidelines:** `https://www.cert-in.org.in`
- **NPCI Certified UPI Applications List:** `https://www.npci.org.in`

CHAPTER 13 • MASTER POCKET REFERENCE

The Master UPI Safety Checklist

A comprehensive pocket reference card for daily life. Keep it saved on your phone, print it out, or share it with family. This single checklist encapsulates the entire book's wisdom.

Your Pocket Safety Guide for Daily UPI Payments

UPI has become an essential part of daily life for over 400 million citizens across India. However, pairing convenience with security discipline is your only true shield against monetary theft.

This final chapter condenses the critical practical rules from all previous 12 chapters into **4 distinct color-coded pocket cards** and an **Official Government Directory**. Whenever in doubt, refer back to this master chapter.

1

Before Paying Checklist

Verify these 6 checks before sending any payment

✓ **The 10-Second Security Pause:**

Never enter your UPI PIN in a rush or under external pressure. Inspect the confirmation screen calmly for 10 full seconds.

- **CBS Verified Bank Name Check:**
  Match the legal account name displayed after scanning against the merchant's actual identity. Don't rely solely on shop signboards.

- **Physical QR Code Inspection:**
  Touch shop stands to ensure no fraudster has pasted a loose paper sticker over the genuine merchant QR code.

- **Count Zeroes and Digits:**
  Double-check that ₹500 wasn't mistakenly typed as ₹5,000 or ₹50,000 before pressing Pay.

- **Use Secure Mobile Cellular Data:**
  Avoid initiating financial banking transactions over public open Wi-Fi at railway stations, bus stands, or coffee shops.

- **Confirm "Paying / Sending" Direction:**
  Ensure the screen indicates you are sending funds rather than unwittingly approving an incoming Collect Request.

2 Never Do This — Red Flags Checklist

These 7 mistakes cause over 95% of digital banking crimes

- **NEVER enter your UPI PIN to receive money:**
  Receiving payments or refunds requires ZERO PIN entry or OTP approval. PIN is exclusively for sending money.

NEVER install AnyDesk or TeamViewer on call:
Anyone directing you to download screen sharing apps during a customer care call is a 100% cyber scammer.

NEVER trust customer phone screenshots:
Merchants must verify incoming payments solely through their own soundbox or merchant banking app.

NEVER dial customer care numbers found on Google search:
Search ads often promote fake phone numbers. Only use help links inside the official payment app.

NEVER click electricity disconnection SMS links:
Utility departments never send disconnection threats from personal 10-digit mobile numbers with shortened links.

NEVER keep screen passcode and UPI PIN identical:
Maintain entirely distinct credentials for unlocking your device and authorizing bank transfers.

NEVER panic over "Digital Arrest" threats:
Digital arrest is completely non-existent under Indian law. Law enforcement never demands UPI transfers over video calls.

3

When Payment Problems Arise

What to do if money is debited or stuck

Do not initiate duplicate transfers in a panic:
If funds debited but failed to credit, wait at least 3 to 5 minutes before re-checking your bank statement.

Remember the RBI T+1 Auto-Reversal Mandate:
Banks are legally bound to reverse failed transactions by the subsequent business day (T+1).

Claim ₹100/Day Delay Compensation:
If your refund takes longer than T+1 business days, your bank must compensate you ₹100 per day automatically.

Log In-App UDIR Disputes:
Tap "Raise Dispute" on the payment entry inside your app and preserve the 12-digit
UTR Number
.

Wrong Transfer Disputes:
Submit written applications with your UTR to your branch immediately to place a lien on the recipient's account.

4 Emergency Fraud Protocol

4 immediate actions during the 2-hour Golden Hour

Step 1: Change Your UPI PIN Immediately
Open your official payment app and reset your UPI PIN and NetBanking password without delay.

Step 2: Temporarily Block UPI Services
Call your bank's 24×7 emergency helpline to temporarily freeze digital UPI channels on your account.

Step 3: Lodge Emergency Report on cybercrime.gov.in
Register the fraud with your 12-digit UTR number on the national portal to trigger an emergency lien on the scammer's mule account.

Step 4: Visit Your Branch with Written Grievance
Obtain a written acknowledgement receipt within 3 business days to enforce your rights under RBI's Zero Liability framework.

Official Government & Regulatory Directory

In any case of dispute or cyber fraud, use strictly these verified government and RBI portals:

Portal 1 National Cyber Crime Reporting Portal

Official Website:

`cybercrime.gov.in`

Specific Section:

Report Financial Fraud (Citizen Financial Fraud Facility)

> **Google Search:**
> `"national cyber crime reporting portal official website"`

Portal 2 Chakshu: Reporting Fraud Calls & Messages

🌐 **Official Website:**

`sancharsaathi.gov.in`

📌 **Specific Section:**

Chakshu (Suspected Fraud Communication Reporting)

> 🔍 **Google Search:**
> `"sanchar saathi chakshu report suspected fraud"`

Portal 3 CEIR: Blacklist Lost or Stolen Mobile Handsets

🌐 **Official Website:**

`sancharsaathi.gov.in`

📌 **Specific Section:**

CEIR (Block Stolen/Lost Mobile Devices)

> 🔍 **Google Search:**
> `"sanchar saathi ceir block lost mobile portal"`

Portal 4 RBI Kehta Hai: Digital Safety Hub

🌐 **Official Website:**

`rbikehtahai.rbi.org.in`

📌 **Specific Section:**

Public Awareness Series & Educational Booklets

> 🔍 **Google Search:**
> `"RBI kehta hai official website digital banking awareness"`

Portal 5 RBI Integrated Banking Ombudsman

🌐 **Official Website:**

`cms.rbi.org.in`

📌 **Specific Section:**

File a Complaint against Bank / Payment Service Provider

> 🔍 **Google Search:**
> `"RBI CMS portal banking ombudsman file complaint"`

Chapter 13: Summary Questions & Daily Rules (Checklist FAQs)

Q1: If I remember just one single rule from this entire eBook, what should it be?

Answer: "Entering your UPI PIN ALWAYS debits money from your account." You NEVER need to type a PIN, disclose an OTP, or scan

a code to receive money, refunds, prizes, or subsidies.

Q2: How often should I review my linked UPI bank accounts?

Answer: Every month. Open your payment app, unbind accounts you no longer use, review active auto-debit mandates, and verify registered mobile numbers.

Q3: What is the single best habit for retail shop owners?

Answer: An audio voice soundbox. Never release merchandise based on a customer's phone display. Always wait for your official soundbox or merchant app notification.

Q4: How can I help protect my elderly parents from cyber extortion?

Answer: Teach them the family emergency codeword, explain that "Digital Arrest" is a hoax, set daily UPI spend limits to modest amounts, and advise them to hang up and call you first.

Q5: Where can I obtain physical copies of official banking safety posters for my store?

Answer: Visit your local bank branch or download printable high-resolution collateral from `rbikehtahai.rbi.org.in` and `npci.org.in` free of charge.

Chapter 13: Master Summary Dos and Don'ts

(Final Pocket Checklist)

✅ Master Do's

- Observe the 10-second pause before typing your PIN for every transaction.
- Verify CBS legal bank names against merchant signage.
- Report unauthorized debits within 3 days to invoke RBI Zero Liability.
- Report immediately on cybercrime.gov.in during the Golden Hour if fraud occurs.

❌ Master Don'ts

- Never type your UPI PIN to claim money, refunds, or lottery prizes.
- Never install screen-sharing software (AnyDesk, TeamViewer) at a caller's request.
- Never dial customer care numbers found in Google Search ad results.
- Never share one-time bank OTPs or card CVVs under any circumstance.

Chapter 13: How to Verify All Official Financial Portals on Google (Safe Search Guide)

Bookmark and verify official public infrastructure portals:

1. **Step 1: Check Domain Suffixes Strictly**
   Indian regulatory and government portals strictly end in `.gov.in`, `.nic.in`, `.org.in`, or `.rbi.org.in`.

2. **Step 2: Avoid Commercial Top-Level Domains**
   Government portals never operate on commercial extensions such as `.com`, `.net`, `.xyz`, or `.site`.

3. **Step 3: Bookmark Official Reporting Portal**
   Bookmark the National Cyber Crime Reporting Portal (**cybercrime.gov.in**) across all family handsets.

4. **Step 4: Keep This Guide Saved**
   Maintain an offline PDF copy of this handbook in your phone's documents folder for ready reference.

🔍 Official Verification Sources for Chapter 13:

- **Reserve Bank of India Master Directives:**
  `https://www.rbi.org.in`
- **National Payments Corporation of India (NPCI):**
  `https://www.npci.org.in`
- **Ministry of Home Affairs Cyber Crime Portal:**
  `https://cybercrime.gov.in`
- **Department of Telecommunications Sanchar Saathi:**
  `https://sancharsaathi.gov.in`

APPENDIX • GLOSSARY

Digital Banking & UPI Glossary

VPA (UPI ID)

Virtual Payment Address — A digital alias for your bank account (e.g. name@okhdfcbank). It lets you send and receive money without revealing your account number.

UTR Number

Unique Transaction Reference — A 12-digit tracking number assigned to every UPI payment. It serves as primary legal proof for bank and police inquiries.

2FA

Two-Factor Authentication — A dual-layer security requirement: something you hold (registered physical SIM card) plus something you know (secret 4 or 6-digit UPI PIN).

CBS Name

Core Banking Solution Name — The official, government-verified legal account name stored at the recipient's bank, displayed immediately when you scan a QR code.

UDIR

Unified Dispute and Issue Resolution — NPCI's automated in-app grievance system that settles failed payments directly between banks in real time.

Phishing

A cyber trick where fraudsters create lookalike fake banking pages or websites to lure users into revealing passwords, card details, or credentials.

Smishing

SMS Phishing — Fraudulent text messages threatening electricity disconnection, package delivery failure, or blocked bank accounts to make you click bad links.

Mule Account

A rented bank account opened in someone else's name, used by cyber criminals to launder stolen money across multiple banks before withdrawing cash.

RAT (Screen Sharing)

Remote Access Trojan apps (e.g. AnyDesk, TeamViewer) that allow fraudsters on phone calls to view your screen and capture passwords and OTPs live.

CEIR

Central Equipment Identity Register — The Department of Telecommunications (DoT) official portal to blacklist stolen mobile phones across all Indian telecom networks.

Chakshu Portal

DoT's official reporting platform on sancharsaathi.gov.in where citizens can report suspicious fraud phone calls, SMS, and WhatsApp messages.

TAT (Turn Around Time)

RBI-mandated resolution deadlines (such as T+1 business day) within which banks must automatically refund failed transaction amounts.

💡 Refer to this glossary whenever you encounter unfamiliar digital banking terms.

★ FINAL SECURITY TAKEAWAY

The 4 Unbreakable Golden Rules of UPI

1. **Never enter PIN to receive money:** Receiving funds, cashbacks, or refunds via UPI NEVER requires entering your PIN or sharing an OTP.
2. **Screenshots are just images:** Never trust a customer's phone screen. Trust only your own banking app balance or voice soundbox announcement.
3. **Never download AnyDesk or TeamViewer:** Anyone who asks you to download a screen-sharing app to resolve a payment issue is a 100% cyber scammer.
4. **Never search helpline numbers on Google:** Search engine ads are frequently manipulated with fraudulent numbers. Always use contact links inside your official app.

✓ 13 Detailed Chapters ✓ Real-Life Case Studies

✓ RBI & NPCI Certified ✓ 48+ Practical FAQs

National Security Pledge

The strength of Digital India is at your fingertips. When you stay alert, you protect not only your own money, but help shield the entire nation from cyber crime.

Safe UPI • Safe Family • Safe India

2026 Edition • Published Independently in Public Interest