

UPI & Payment Scams: Spot Them Before You Pay

The one rule behind almost every UPI scam, the tricks built on it - fake QR codes, fake payment screens, AutoPay traps - and exactly what to do in the first hour if money has gone.

35 min read · Content last verified 13 September 2026 · Reviewed by Shravya M

Free awareness guide. Not legal or financial advice. <https://www.shravyadigital.com/guides/upi-payment-scams>

CONTENTS

1. Before you start
2. Chapter 1: The one rule
3. Chapter 2: "Scan to receive" and fake requests
4. Chapter 3: Fake proof of payment
5. Chapter 4: Fake support, KYC and bill calls
6. Chapter 5: At the shop
7. Chapter 6: AutoPay mandate traps
8. Chapter 7: Trust traps
9. Chapter 8: If it already happened, the first hour
10. Quick reference card

Before you start

This guide is for anyone in India who pays or gets paid through UPI: first-time users, parents, shopkeepers, students. It takes about 35 minutes to read. You need no prior knowledge.

Every scam chapter follows the same four steps, so the pattern becomes familiar:

1. **What it looks like:** a short, made-up scene
2. **Why it works:** the trick, in a sentence or two
3. **The check:** the one action that exposes it
4. **The rule:** one line to remember

All names, phone numbers and UPI IDs in this guide are invented.

Keep this number: 1930 is the national cybercrime helpline. If money has already gone, call it first. Chapter 8 tells you everything else to do.

Chapter 1: The one rule

If you remember only one page of this guide, make it this one.

Your UPI PIN approves money leaving your account. That is its only job.

- You **never** need your PIN, an OTP, or a QR scan to **receive** money. To receive, you only share your UPI ID or show your own QR code.
- **Scanning a QR code** and **approving a request** are both ways of **paying**.
- Before you confirm, your app shows the **payee's name**. Read it. If it isn't the person or shop you meant to pay, stop.
- If your bank or UPI app **warns that a payment looks like a scam, stop**. Don't tap past the warning.
- No real bank, NPCI, police officer or app support agent will ever ask for your PIN.

To RECEIVE money	To SEND money
Share your UPI ID or show your QR code	Scan a QR, approve a request, or type an amount
No PIN. No OTP. Nothing to approve.	PIN required

The rule: PIN means money leaves. Always.

Chapter 2: "Scan to receive" and fake requests

What it looks like

Priya lists an old study table online for ₹2,500. A buyer replies within minutes and agrees the price without bargaining. He sends a QR code: "Scan this and enter your PIN, the money will come to you." After she scans it, the screen shows ₹2,500.

Why it works

The amount matches what Priya is owed, so it feels like receiving. But a QR code only ever opens a payment. The ₹2,500 on the screen is what will **leave** her account.

The same trick, other ways

- **Fake "cashback" or "reward" requests.** Approving any payment request sends money out, whatever the message says.
- **"I'm sending you money, just approve the popup."** There is no popup to approve when someone pays you.
- **A payment request that seems to come from a person.** Since **1 October 2025**, UPI no longer lets one person send a payment ("collect") request to another. Shops and online merchants can still ask for payment at checkout. **A request that appears to come from an individual is itself a warning sign.**

The check

Ask yourself: *am I receiving money?* If yes, there should be nothing to scan and nothing to approve.

The rule: Nobody needs you to scan or approve anything to pay you.

Chapter 3: Fake proof of payment

What it looks like

Arjun sells his old phone. The buyer shows a "₹12,000 paid successfully" screen, complete with a transaction ID, and asks for the phone. Arjun's own app shows nothing received.

Why it works

A success screen, a transaction ID and a confident buyer all look like proof. None of them are. Only the money arriving in your account is proof.

The same trick, other ways

- **Fake payment apps** that show a realistic success screen without sending anything.
- **Edited screenshots** of a real-looking payment.
- **Fake "credited" SMS messages.** The sender name on an SMS can be faked.
- **"I paid you too much by mistake."** "I sent ₹3,000 instead of ₹300, please return the extra to this QR." Usually no money arrived at all.

The check

Open **your own** bank or UPI app and find the credit in your transaction history **before** you hand anything over. If someone says they overpaid you, check your own app first. If money really did arrive by mistake, contact your bank; don't send it to a new QR code or UPI ID.

The rule: Only your own app proves you've been paid.

Chapter 4: Fake support, KYC and bill calls

What it looks like

Ramesh's payment fails. He searches online for his UPI app's customer care number and calls the first result. A friendly "agent" asks him to install a screen-sharing app so they can "fix it from our side."

Why it works

Ramesh made the call, so he trusts the number. Fraudsters plant fake helpline numbers in search results, ads and social media comments.

The same trick, other ways

- **Screen-sharing (remote access) apps.** Once installed, the caller can see your screen, including every OTP that arrives.
- **"Your KYC expires today"** calls or messages pushing a link or an app download.
- **SMS messages that look like they're from your bank** and contain a short link.
- **"Your electricity will be disconnected tonight"** messages that give a personal mobile number to call.
- **"Read me the OTP so I can cancel the fraud."** The OTP approves whatever the caller has started. Read the OTP message itself: it usually says what it is for.

The check

Find customer support **inside the app itself**, or on an official website whose address you typed yourself. Check bills on the provider's own app or website. Report suspicious calls and messages on **Chakshu**, part of the government's Sanchar Saathi portal (sancharsaathi.gov.in).

The rule: Never install an app, click a link, or read out a code because a caller asked.

Chapter 5: At the shop

For customers

At a busy petrol pump, Neha scans the printed QR code on the counter. The name that comes up is a person's name, not the petrol pump's.

- Fraudsters paste their own QR sticker **over** a shop's real one.
- **The check:** read the payee name before entering your PIN. If it doesn't match the shop, ask the staff before you pay.

For shopkeepers

- Check regularly that your QR code hasn't been covered or replaced.
- Confirm every payment on **your own** soundbox or app, never on the customer's phone screen.
- If your soundbox didn't announce the payment, don't hand over the goods until your app shows the money arrived.

The rule: Read the name before the PIN. Every time.

Chapter 6: AutoPay mandate traps

What it looks like

A website offers Sunil a free trial and asks him to approve "₹1 for verification" through UPI AutoPay. He approves without reading. The mandate lets the merchant take far more, every month.

Why it works

The first charge is tiny, so approving feels harmless. But a mandate is permission for the merchant to take money **again later**.

The check

- Before approving, read what you are really agreeing to: **how much can be taken later, and how often**, not just today's charge.
- Since **31 December 2025**, you can see **all** your active AutoPay mandates in any UPI app you choose, in its AutoPay section, and pause, change or cancel them there. Cancelling needs your UPI PIN.
- Cancel any mandate you don't recognise, then tell your bank.

The rule: Check what it can take later, not just today.

Chapter 7: Trust traps

In these scams the trick is a relationship, not the app.

"It's me, new number"

"Hi Maa, this is my new number, my phone broke. I need ₹15,000 for fees today. Send it to this UPI ID." The message comes from a number she doesn't know.

- **The check:** call your family member on the number you already have for them. A voice note is not proof: voices can now be copied by software.

Part-time "task" jobs

- You are paid small, real amounts (₹150 for "liking videos") to build trust. Then you are asked to deposit money to "unlock" bigger tasks or to withdraw your earnings. The early payouts are bait, and the deposits don't come back.

The "officer" buyer

- A buyer on a marketplace says he is an army or government officer being transferred. He is eager to pay in advance, then asks you to "send ₹1 to verify" or to approve a request. The trusted identity is the trick.

The rule: Urgency, plus a new number, plus money: stop and check another way.

Chapter 8: If it already happened, the first hour

Read this even if nothing has happened to you. In a panic, you won't want to work it out.

Do this, in this order

1. **Call 1930**, the national cybercrime helpline. Do it straight away.
2. **Report it at cybercrime.gov.in**, the National Cyber Crime Reporting Portal.
3. **Tell your bank the same day**, using the number on your card, passbook or bank app. Ask them to block UPI on your account and to register a complaint. Write down the complaint reference number.
4. **Report the number or message** on Chakshu (sancharsaathi.gov.in).
5. **Keep the evidence**: screenshots, the fraudster's phone number and UPI ID, the transaction ID and the time. Don't delete the chat.

Warning: Report to **both** 1930 (or cybercrime.gov.in) **and** your bank. One of them is not enough.

Why speed matters

Money that is still in the fraudster's account can sometimes be put on hold before it is moved on. Every hour you wait lowers that chance.

Will I get my money back? The honest answer

Refunds are **never automatic**. What the Reserve Bank of India's rules say depends on **when** the fraud happened. This is a plain-language summary; your bank decides your individual case.

Frauds up to 31 December 2026

- **You lose nothing** if the fraud happened because of your bank's fault, whenever you report it.
- **You lose nothing** if the fault was somewhere else in the system (neither yours nor the bank's) and you tell your bank within **3 working days**.

- If you **shared your PIN, OTP or payment details**, the bank can treat the loss as your negligence: **you carry the loss up to the moment you report it**. Losses after you report fall on the bank.

Frauds from 1 January 2027

RBI issued new rules on 24 June 2026 that replace the ones above.

- **What counts as fraud:** payments made by a fraudster using details they tricked out of you, and payments you approved yourself **under coercion or duress**, such as during a "digital arrest" call.
- **You lose nothing** if the bank was at fault, or, if the fault was elsewhere in the system, if you report to your bank within **5 calendar days**.
- **Negligence** includes sharing your PIN or OTP, installing a malicious app and ignoring a clear scam warning from your bank. If you were negligent, you carry the loss until you report it, except for any part covered by compensation.
- **New compensation for smaller frauds:** if you are an individual and your total loss is **₹50,000 or less**, you may receive **85% of the net loss, up to ₹25,000, once in your lifetime**. You must have reported it to **both** 1930 or cybercrime.gov.in **and** your bank within **5 calendar days**, and the bank must confirm the fraud is genuine.
- A payment you made **yourself** because you were fooled, with no coercion, does not clearly fit RBI's definition of fraud. Don't count on a refund for it. Report it anyway.

Bottom line: under either set of rules, what most improves your chances is reporting **fast, and to both**.

Warning: Anyone who offers to "recover your money" for an upfront fee is running a second scam. Police and banks do not charge to recover money.

The rule: 1930 and your bank. Both. Today.

Quick reference card

Screenshot this and share it with your family.

1. **PIN means money leaves.** Never enter it to receive money.
2. **Nothing to scan, nothing to approve** when someone is paying you.
3. **Only your own app** proves you've been paid.
4. **Read the name before the PIN**, and stop if your bank warns it's a scam.
5. **AutoPay: check what it can take later**, not just today.
6. **Never install, click or read out a code** because a caller asked.
7. **Money gone? Tell 1930 and your bank: both, today.**

Take the course for what you just read

Take the free 10-question assessment and pass with 8 or more. Every course you pass counts towards a Pathway Certificate issued by Shravya Digital, earned when you pass all five courses in the pathway: <https://digital.shravyaworld.org/courses/upi-payment-scams>

Sources

Checked against these primary sources on 13 September 2026. Rules change: if something here looks out of date, trust the source.

- NPCI circular NPCI/UPI/OC-223/2025-26 (7 Oct 2025): AutoPay mandates in any UPI app (https://www.npci.org.in/uploads/UPI_OC_No_223_FY_2025_26_Enhancement_of_UPI_Autopay_88b38535cb.pdf)
- NPCI circular NPCI/UPI/OC/220/2025-26 (29 Jul 2025): person-to-person collect requests discontinued from 1 Oct 2025 (NPCI has since removed the original)
- RBI (Commercial Banks - Responsible Business Conduct) Directions, 2025, Section D, which consolidates RBI circular DBR.No.Leg.BC.78/09.07.005/2017-18 (6 Jul 2017) on limiting customer liability (https://www.rbi.org.in/Scripts/BS_CircularIndexDisplay.aspx?Id=11040)
- RBI (Commercial Banks - Responsible Business Conduct) Third Amendment Directions, 2026 (24 Jun 2026, effective 1 Jan 2027) (<https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=13543&Mode=0>)
- National Cyber Crime Reporting Portal and helpline 1930 (<https://cybercrime.gov.in/>)
- Chakshu: report suspected fraud communication (DoT) (<https://sancharsaathi.gov.in/sfc/>)