



BEWARE OF UPI FRAUD ALERT

यूपीआई धोखाधड़ी से सावधान रहें

Secure Your Payments. Protect Your Funds Today.

How UPI fraud happens

- **SUSPICIOUS UPI REQUEST**
Scammers send an unexpected payment request or QR code – often saying “pay to receive your refund” – and push you to approve it quickly.
- **LINK OR APP INSTALLATION**
You click a link in an SMS or install an app that asks for access to your UPI account details.
- **ENTERING PIN / OTP**
You enter your UPI PIN or share an OTP. That approves the transaction and gives the fraudster access to your money.
- **UNAUTHORISED TRANSFER**
Fraudsters use your UPI details to send money from your account to unknown accounts.
- **ACCOUNT COMPROMISE**
Your UPI details are misused to drain money from the bank accounts linked to your UPI.
- **REPORT IMMEDIATELY**
Tell your bank at once, then call **1930** or report at **cybercrime.gov.in** so the case can be investigated.



Your UPI PIN is only for **SENDING money.**
You never need it to **RECEIVE money.**

If anyone asks for your PIN or OTP to “send you money” or “refund” – it is a fraud.

Key warning signs

-  Unexpected UPI payment requests
-  Links to unknown apps or websites
-  Unsolicited calls or messages about payments
-  Requests for your UPI PIN or OTP
-  Urgent demands for immediate action

What you should do

VERIFY

Check bank contact details

Verify your bank's details through **Trusted Contact Details** on the Sanchar Saathi portal – not from a call, SMS or link.

REPORT ON CHAKSHU

Suspected fraud call, SMS or WhatsApp?

Report it through **Chakshu** on the Sanchar Saathi portal.

sancharsaathi.gov.in

ALREADY LOST MONEY?

Call the Cyber Helpline

1930

cybercrime.gov.in

Get the Sanchar Saathi mobile app

Scan the QR code for your phone, or search “Sanchar Saathi” – published by the Department of Telecommunications.



Google Play



Apple App Store