UPI and Payment Fraud Awareness

Common UPI tricks - fake collect requests, QR code scams and fake refunds - and how to stay safe.

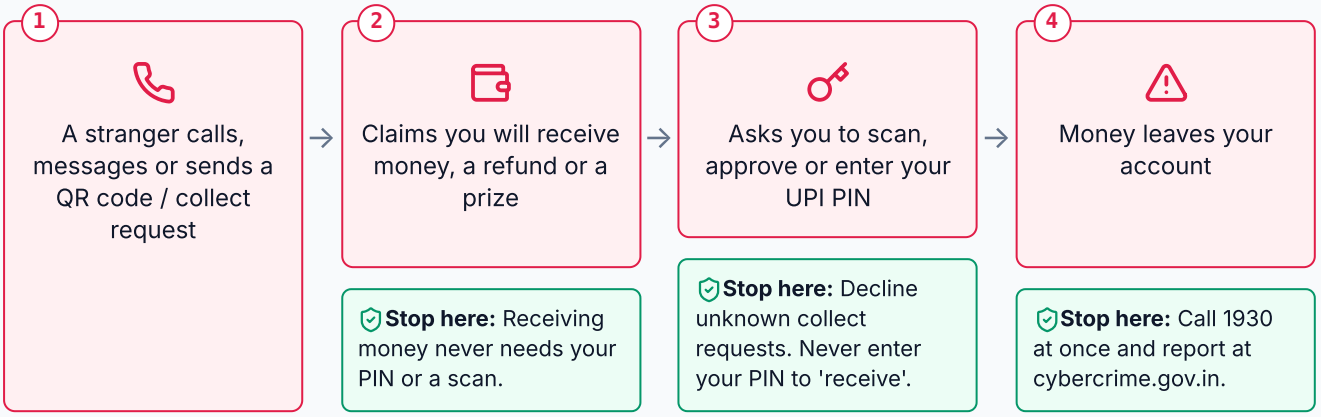
Lost money in an online fraud? Call 1930 right away and report at cybercrime.gov.in.

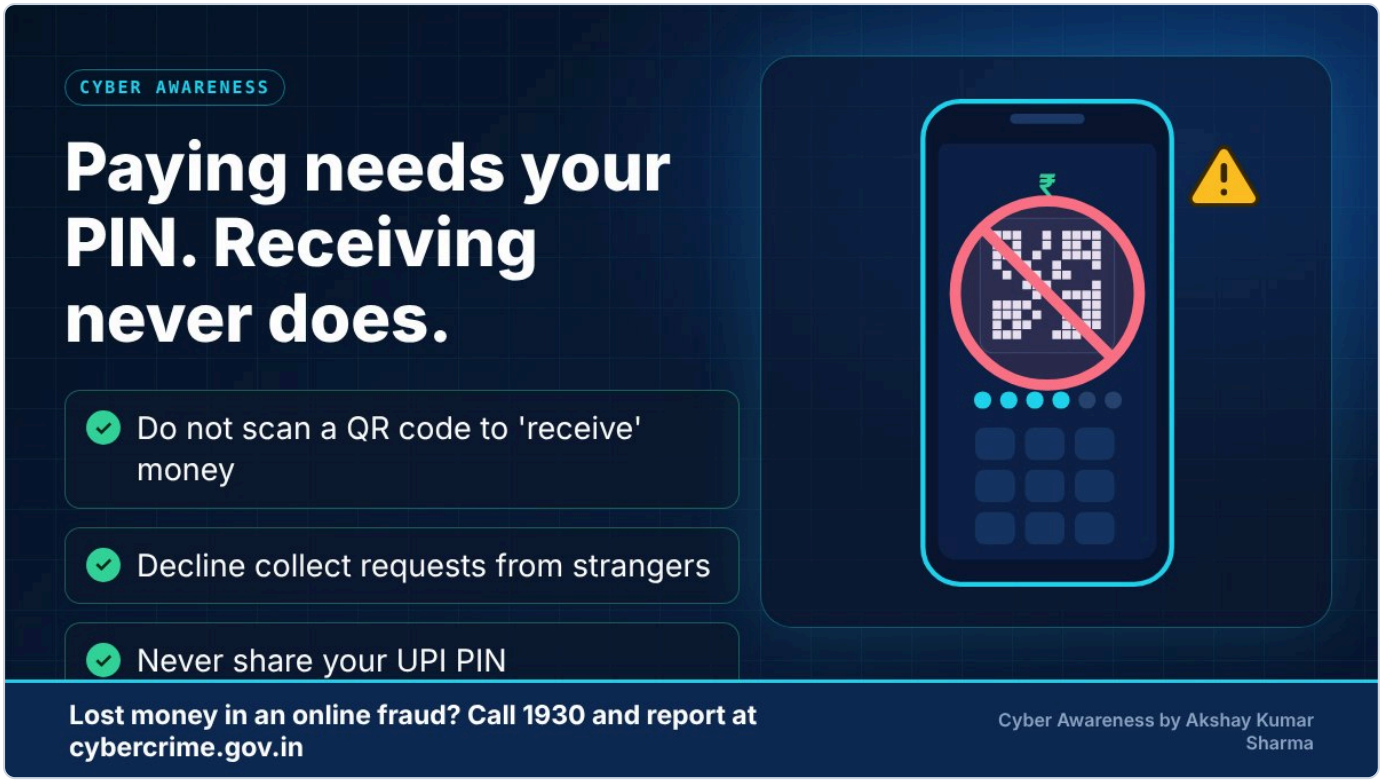
What it is

UPI makes payments fast, which is also why fraudsters like it. A key rule: you enter your UPI PIN only to send money. You never need your PIN to receive money. Scammers rely on confusing people about this, using fake payment requests, QR codes, fake customer-care numbers and 'refund' stories.

How it works - and where you can stop it

Red boxes show what the attacker does. Green boxes show where you can break the chain.





Common warning signs

- ⚠ Someone asks you to scan a QR code or enter your PIN 'to receive' money or a refund.
- ⚠ A 'collect request' appears from an unknown person, or a buyer insists on sending a request instead of paying normally.
- ⚠ A caller claims to be from your bank, a delivery service or a wallet and asks you to install a screen-sharing app.
- ⚠ Customer-care numbers found through search results or social media rather than the official app or website.
- ⚠ Pressure to act immediately, or an offer that is too good to be true.

Practical prevention tips

- Never enter your UPI PIN to receive money. If a screen asks for your PIN, you are sending money.
- Read every payment request carefully and decline requests you did not expect.
- Never install remote-access or screen-sharing apps at someone else's request.
- Get customer-care numbers only from the official app, website or your card.
- Set sensible transaction limits and enable app lock and payment alerts.

Risky habit vs safe habit

RISKY	SAFE
✕ Scan a QR code to 'receive' money	✓ Remember: PIN and scanning are only for paying
✕ Approve a collect request you did not expect	✓ Decline it and report the UPI ID
✕ Call a 'customer care' number found through a search	✓ Use the help section inside the official app
✕ Install a screen-sharing app when 'support' asks	✓ Refuse. Real support does not need remote access to your phone

What to do if it happens

1. Call the cyber crime helpline 1930 immediately - reporting quickly gives the best chance of stopping the transfer.
2. Also file a complaint on the National Cyber Crime Reporting Portal (cybercrime.gov.in).
3. Inform your bank or payment app right away and ask them to block the card, account or UPI ID involved.
4. Keep screenshots, transaction IDs, phone numbers, UPI IDs and chat history. Do not delete anything.
5. Change passwords of affected accounts and do not share OTPs or PINs with anyone who calls you afterwards offering to 'recover' your money.

Official reporting resources

- Cyber crime helpline 1930 (for financial cyber fraud) - 1930
- National Cyber Crime Reporting Portal (cybercrime.gov.in) - https://cybercrime.gov.in/
- NPCI (UPI) - official information - https://www.npci.org.in/
- Reserve Bank of India - public awareness - https://www.rbi.org.in/

Never share your banking password, OTP, UPI PIN, card CVV or full card number with anyone - not even someone claiming to be from your bank, police or a government office. This website will never ask for them.

This website is an educational resource. It is not an official government reporting portal or an emergency response service. If you are a victim of cyber fraud, report it through the official channels listed on each page.
Akshay Kumar Sharma - https://www.youtube.com/@cybersecwithakshay