Digital Safety Guide for Shopkeepers & Merchants

RETAIL SAFETY • 2026 EDITION

Merchant UPI Safety Guide

A complete, easy guide for shopkeepers to stay safe from Fake Payments, QR tampering, and Refund Scams

10	5 Seconds	100%
Easy Chapters	Counter Test	Simple Everyday English

Fake Payment Screenshot | QR Sticker Tampering | Overpayment & Cash Refund Scam | Collect Request & PIN Fraud | Fake Advance Order Call | Counter Staff Training

⚡ **Unbreakable Counter Rule:** "No Soundbox alert, no App entry, no Bank SMS = No goods!" A green tick on a customer's phone is never proof of payment.

Merchant Cyber Safety Awareness Series

Mobile Pocket Size Edition • 120mm × 190mm

LEGAL NOTICE • DISCLAIMER

Legal Terms and Rules of Use

1. Awareness Only

This eBook is an independent guide created solely to raise digital payment safety awareness among shopkeepers and retail merchants. Its goal is to warn readers about fake payment screens, QR scams, and overpayment frauds. It is not legal or financial advice.

2. No Affiliation

This eBook is not created, sponsored, or verified by the Reserve Bank of India (RBI), National Payments Corporation of India (NPCI), Telecom Department, National Cyber Crime Reporting Portal, any bank, or any ministry of the Government of India. It is a completely independent digital guide.

3. Limitation of Liability

Digital payment safety rules, government portal addresses, and app rules can change over time. Neither this eBook nor its author is responsible for any fraud, business loss, or issue faced by any reader. Always check the official website of the concerned government department or bank for the latest updates.

4. Trademarks and Brand Names (Fair Use)

'UPI' is a trademark of NPCI. All other names and brands mentioned in this book (such as Paytm, PhonePe, Google Pay, BharatPe, SBI, HDFC, AnyDesk, etc.) belong to their respective owners and are used solely for identification and explanation under Fair Use.

5. Methods Only (No Real Names)

All case studies and examples in this guide use fictional names solely to explain ongoing scam methods in the market. It does not accuse any real person, shop, or organization.

6. Single-User Digital License

This PDF is licensed strictly for personal and your shop/staff use under a Single-User License. Re-uploading it publicly, reselling it, or distributing it without written permission is prohibited under copyright law.

EDITORIAL • PREFACE

Protecting Every Shopkeeper's Cash Counter

Evening rush hours—when your shop is packed with customers—are when scammers strike. One shows a fake Paytm/PhonePe screen and walks out with goods, while another pressures you claiming "money was deducted from my account" even when your Soundbox stays silent.

> “
>
> Scammers exploit your busy counter and rush. A **5-second check** can save your entire day's earnings.

3 Firm Rules for Shopkeepers and Staff:

1. Never Trust a Customer's Phone: A green tick or receipt on a customer's phone is never final. Check only your own Soundbox, Merchant App, or Bank SMS.

2. Zero Cash-Back Rule: If someone claims "I sent extra money by mistake, give me cash back"—never hand over cash on the spot.

3. Morning QR Finger Check: Every morning when opening your shop, run your finger over your QR standee to make sure nobody stuck a fake sticker on top.

Goal of This Pocket Guide: Across 10 short, practical chapters, help every small and big shopkeeper and counter staff stay 100% safe from fake payments, QR scams, and fake advance orders.

COMPLETE TABLE OF CONTENTS

Merchant Master Guide: All 10 Chapters

01 **How UPI Frauds Happen at Shops**
Evening rush tricks, fake screenshots, and counter losses explained

02 **Paid or Not? How to Spot a Real Payment**
Matching Soundbox, Merchant App, and Bank SMS 100% accurately

03 **Fake Payment Screenshots and Spoof Apps**
5 big clues of fake screens and the Spot-the-Fake counter test

04 **QR Code Swapping and Fake QR Stickers**
Sticking a fake QR on your standee and the morning finger check

05 **The "Sent Extra by Mistake, Refund Cash" Trick**
Fake overpayment dramas, emotional stories, and the Zero Cash-Back rule

06 **Collect Requests and Refund Traps**
Tricking you into entering UPI PIN to 'receive' money: "PIN entered = money gone"

07 **Fake Orders and Fake Customer Calls**
Big govt/army camp order claims, fake advance payments, and link scams

08 **What to Train Your Staff and Helpers**
3 strict counter rules for staff when the shop owner steps away

09 **What to Do After Fraud & How to Complain**
Golden 2-hour action, alerting your bank, and reporting on cybercrime.gov.in

10 **Shopkeeper's Daily Safety Checklist**
Master checklist from opening the shutter in the morning to closing at night

CHAPTER 1 • COUNTER AND CASH-BOX SAFETY

How UPI Frauds Happen at Shops

Evening rush tricks, fake screenshot scams, and the full truth behind shopkeeper losses.

Counter Rush: A 5-Second Trick That Wipes Out a Full Day's Profit

Imagine it's 7 PM. Five customers stand at your counter—one wants oil, another wants sugar, and a third is rushing you to pack items fast.

Right then, a fourth customer waves their phone screen in front of you: *"Brother, sent ₹1,800—look at the green tick! Hurry up, my ride is waiting outside."* Caught in the crowd, you nod and hand over the goods. At night, you check your account—and ₹1,800 never arrived!

Case Study

Grocery Store Owner Suresh ji's ₹3,200 Loss

A young man walked into Suresh ji's grocery shop and got ₹3,200 worth of dry fruits and ghee packed. He scanned the counter QR code and showed a Payment Success screen displaying Suresh ji's shop name and ₹3,200.

Suresh ji asked, *"Brother, the Soundbox didn't speak."* The man replied, *"Oh Uncle, Jio network is slow—it cut from my account, it'll announce in 2 minutes."* Suresh ji handed over the bag. Neither the Soundbox spoke nor did any SMS arrive. That screen was generated by a **Fake UPI App**.

> **Plain truth:** A green tick on a customer's phone screen is NEVER proof that money reached your account.

At the Counter: Evening Rush and the Scammer's Play

See how scammers distract shopkeepers in 30 seconds at the counter:

Counter Rush Simulation

The Rush Game

Customer (waving phone in a hurry): "Brother, paid ₹2,400! Look at the screen, green tick is here. Pack fast, my auto's meter is running outside!"

Smart Shopkeeper (staying calm): "Brother, your screen looks fine, but my Soundbox hasn't spoken and no bank SMS came yet. Just wait 1 minute—once confirmed, the goods are yours."

Customer (acting angry): "Are you doubting me? I buy from here every day! Money already left my account, want to see my SMS?"

Rule of truth: A real customer worried about deducted money will happily wait 2 minutes. Only a scammer showing a fake screen tries to pick a fight and run.

The 4-Step Cycle of UPI Fraud at Shops

1 **Waiting for Busy Rush Hours**

Scammers always strike during evening crowds or festivals when the shopkeeper at the counter is busy and tired.

↓ Picking high-value items

2 **Getting Goods Packed Fast**

They pick items easy to carry away fast (groceries, dry fruits, clothes, cigarettes, or pricey electronics).

↓ Showing a fake screen

3 **Generating a Screen via a Fake App**

Typing your shop name and amount into a fake app, they flash an instant green tick and blame a slow network.

↓ Vanishing without paying

4 **Stopped by Shopkeeper Alertness**

Never let goods cross the counter until your Soundbox speaks or your own phone receives confirmation.

Spot-the-Fake: Real vs Fake in 5 Seconds

Any fake screen shown by a scammer has 5 major clues:

🔍 5-Second Screen Test (Real vs Fake)

❌ 4 Clues of a Fake Screenshot

• UTR or UPI Ref Number is missing or has only 10 digits (real ones always have 12 digits).

• Font sizes and letters look slightly blurry or crooked.

• The timestamp is often 5–10 minutes old or altered.

• Your Soundbox stays completely silent and your phone gets zero SMS.

✅ Sure Proof of a Real Payment

• Your Soundbox announces the exact amount clearly.

• Your own mobile receives an instant bank credit SMS.

• Your Merchant App (Business App) History shows the new transaction.

• A full 12-digit UTR number is clearly recorded.

Soundbox 3-Step Verification Ladder

Follow these 3 simple steps right at your counter:

1. **Did the Soundbox Speak?**
   If the Soundbox clearly announced the amount, 100% the money has arrived. Hand over the goods happily.

2 **If Soundbox Is Silent, Check Your Own Phone**

Don't touch the customer's phone. Open your own bank SMS or Merchant App History to check.

3 **If Still Not Visible, Wait 2 Minutes**

Tell the customer politely: *"Brother, please have a seat for 2 minutes—the moment it reflects, take your bag."* Never hand over goods in haste.

3 Strict Rules for Shop Staff & Helpers

If helpers or staff work at your shop, make these rules crystal clear to them:

📌 3 Rules for Counter Staff

Rule 1 Never pack and hand over goods just by looking at a customer's phone screen.

Rule 2 Never let a customer leave until the shop's Soundbox speaks or the counter phone receives a message.

Rule 3 If a customer claims "I sent extra money by mistake, give me cash back", never give ₹1 in cash without asking the owner.

⚡ **5-SECOND COUNTER DECISION**

When a customer says: "Network is down, it'll arrive later"

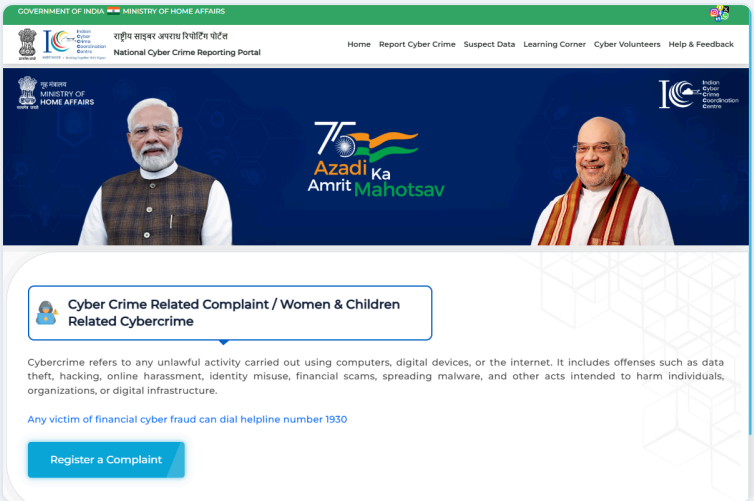
> *"Brother, you may be right, but our shop rule is fixed—until it shows on our phone, we cannot release goods. Please sit 2 minutes and have tea; the moment it rings, take your items."*

Official Portal: Report Online Fraud Immediately

If any shopkeeper faces fake payment or QR fraud, report it right away on India's official portal:

National Cyber Crime Reporting Portal

Government of India



3 Key Things to Check:

1. **Official Website:** Always type `cybercrime.gov.in` directly into your browser address bar. Never open unknown WhatsApp or SMS links.
2. **Financial Fraud Section:** Go to 'Register a Complaint' or 'Cyber Crime Related Complaint' on screen to submit your report fast.
3. **Helpline & Contact:** For help, always follow the verified route in the portal's Official Contact Us / Helpline section. Never call numbers from Google Search Ads.

🔍 Forgot the Website Name? Search This on Google:

Type directly into Google Search: `National Cyber Crime Reporting Portal`

• **Skip 'Ad' / 'Sponsored':** Never click results marked 'Ad' or 'Sponsored' at the top.

• **Verify Govt Domain:** Always check that the address ends with `.gov.in` or `.nic.in`.

• **Official Contact:** Take verified phone numbers or forms only from the portal's 'Contact Us' page.

Shopkeeper's Do's and Don'ts

✅ What to Do (Safe Habits)

• Trust ONLY your shop's Soundbox announcement or your own bank SMS.

• Check your QR standee every morning on opening to be sure nobody pasted another sticker over it.

• Train your staff to check notifications on the shop phone instead of looking at the customer's screen.

• Even during evening rush hours, never release goods without confirmed payment.

❌ What Not to Do (Dangerous Mistakes)

• Never hand over goods just because you saw a green tick on a customer's phone.

• Never hand over cash if someone claims "Sent ₹2,000 extra by mistake" without checking your real bank balance.

• Never enter your UPI PIN or OTP to receive a payment.

• Never download AnyDesk or any screen sharing app on your phone on a stranger's call.

Official Sources:

1. National Cyber Crime Reporting Portal: `cybercrime.gov.in`
2. National Payments Corporation of India (NPCI): `npci.org.in`
3. Reserve Bank of India (RBI Kehta Hai): `rbi.org.in`

CHAPTER 2 • 4 SURE SIGNS OF A REAL PAYMENT

Paid or Not? How to Spot a Real Payment

Stop trusting the customer's phone—verify every payment accurately with your Soundbox, Business App, and SMS.

The Counter Illusion: Is That Green Tick Real or Just a Photo?

During evening rush, customers line up—some weighing lentils, others picking clothes. Suddenly someone thrusts a mobile screen in front of you: *"Brother, look, sent ₹1,200—green tick came!"*

Have you ever stopped to ask whether that green tick came from a real bank or a fake app? Dozens of fake apps online can generate an identical-looking Payment Success screen in 5 seconds.

Case Study

Sweet Shop Owner Ramesh ji's Bitter Lesson

On a busy festival day, Ramesh ji's sweet shop was packed. A young man got two boxes of kaju katli worth ₹1,400 packed, pretended to scan the counter QR, and showed a Payment Success screen.

Ramesh ji asked, *"Brother, why didn't the Soundbox speak?"* The man quickly replied, *"Uncle, server is slow—look, my bank SMS already came showing ₹1,400 deducted!"* Ramesh ji glanced at the SMS and handed over the sweets. That night, ₹1,400 had never arrived. Even the SMS was fake.

> **Plain truth:** A customer's phone is their tool, not your shop's ledger. Money arrives only when YOUR account confirms it.

4 Sure Proofs of a Real Payment

Whenever a customer pays via UPI, truth can be verified only through these 4 checks:

1 **Clear Soundbox Announcement**

Your counter Soundbox clearly speaks out the exact amount (e.g., "₹1,400 received"). This is the fastest and safest proof.

↓ If Soundbox is silent, Step 2

2 **Live Entry in Your Merchant App**

The new transaction appears inside the History of your own Business App (Paytm Business, Google Pay Business, or PhonePe Business).

↓ If App won't open, Step 3

3 **Bank Credited SMS**

An SMS arrives directly from your bank on your registered phone showing money credited along with your account's last 4 digits.

↓ Final proof in case of dispute

4 **12-Digit UPI UTR Number**

Every successful UPI payment has a unique 12-digit reference number. If it is not in your app, no money arrived.

At the Counter: Rush Pressure vs Calm Answer

See how scammers fake urgency and how a smart shopkeeper stays calm:

Counter Conversation (Simulation)

The Rush Game

Customer (waving phone): "Brother, sent ₹1,200! Look at the screen, green tick is here. Give me the bag fast, I'm missing my bus!"

Smart Shopkeeper (calmly): "Brother, your screen looks fine, but my Soundbox hasn't spoken and it's not in my app yet. Please sit 1 minute—the moment it shows, take your items."

Customer (acting annoyed): "Are you suspecting me? I shop here daily! Money left my phone—want to see my bank message?"

Smart Shopkeeper (politely): "Nothing personal brother, it's our shop rule. Money leaving your phone is one thing; reaching our account is another. As soon as it shows on my phone, I'll gladly hand it over."

Rule of truth: Anyone whose money genuinely left will wait 2 minutes and show their UTR number. A scammer picks a fight or leaves the goods and runs.

Spot-the-Fake: Real Bank SMS vs Fake SMS

Sometimes scammers send a fake SMS to your phone or flash one on theirs. Spot it with these 4 checks:

🔍 SMS Check: Real vs Fake

❌ 4 Big Clues of a Fake SMS

- Sent from an ordinary 10-digit personal mobile number.
- Your bank account's last 4 digits are missing or wrong.
- The 12-digit UTR number is missing or incomplete (only 8–10 digits).
- Contains spelling mistakes, grammar errors, or strange wording.

✅ Signs of a Real Bank SMS

- Always arrives from an official 6-letter header (like AD-HDFCBK, VK-SBIINB, CP-ICICIB).
- Clearly prints your bank account's last 4 digits (A/c XX1234).
- Includes the full 12-digit UPI Ref / UTR number.
- Shows your updated total account balance.

The 12-Digit UTR Formula: Ending Every Dispute

Whenever a customer insists *"Money was deducted from my account, why didn't your Soundbox announce it?"*, don't argue.

Use this 3-step formula:

1. **Ask Customer for the 12-Digit UTR**
   Ask them to open Transaction Details in their UPI app and show the 12-digit UPI Reference Number (UTR).

2. **Search It in Your Merchant App**
   Type that exact 12-digit UTR number into the search bar of your own Business App.

3. **Instant Clear Decision**
   If that UTR shows 'Success' in your app, money arrived. If that UTR does not exist in your app, ₹0 reached your shop.

What If the Soundbox Is Silent? (3-Step Ladder)

Sometimes slow network or low battery delays the Soundbox voice. Follow this exact order:

1. **Did Soundbox Speak?**
   If it announced clearly, 100% payment is confirmed. Hand over the goods without worry.

2. **Silent? Refresh Your Merchant App**

Open your Business App on your own phone, pull down History to refresh, and check your new balance.

3 **Not in App? Check Your Bank SMS**

Open SMS on your registered phone. If there is no bank credit SMS, ask the customer to wait 2 minutes.

⚡ **5-SECOND COUNTER DECISION**

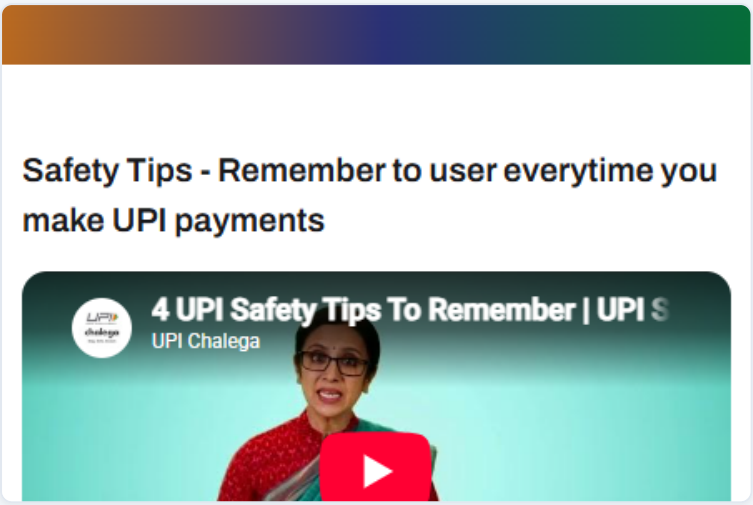
Golden Counter Rule

> *"No Soundbox alert, no App entry, no Bank SMS = No goods! No matter how hard a customer argues or rushes you, nothing leaves the counter until money shows in your account."*

Official Portal: NPCI's UPI Safety Awareness Campaign

NPCI (National Payments Corporation of India) directly advises shopkeepers and citizens to watch out for fake payment messages:

NPCI UPI Safety Campaign (Official Portal) NPCI Verified



3 Key Things to Check:

1. **Official Portal Address:** Always type `upichalega.com` or `npci.org.in` directly in your browser. Never open unknown SMS or WhatsApp links.
2. **Fake Message Warning:** NPCI's official message clearly warns — "If someone sends a fake payment message and asks for money, check your bank account first."
3. **Safe Contact Protocol:** For any UPI issue or fraud, always use the verified Contact Us or Dispute section on the official portal.

Shopkeeper's Do's and Don'ts

✅ What to Do (Safe Habits)

• Always rely only on your Soundbox voice or live entry inside your Business App.

• If Soundbox stays silent, ask for the 12-digit UPI UTR number and match it in your app.

• Always check the Sender ID of bank SMS alerts (like AD-HDFCBK, VK-SBIINB).

• Clearly train your helpers never to hand over goods just by seeing a customer's screen.

❌ What Not to Do (Dangerous Mistakes)

• Never hand over goods after seeing only a green tick or screenshot on a customer's phone.

• Never trust a "Money Credited" SMS arriving from a plain 10-digit mobile number.

• Never give goods on credit just because a customer says "Money got cut, it'll reach later."

• Never share or enter your UPI PIN or OTP to receive a payment.

Official Sources:

1. National Payments Corporation of India (NPCI): `npci.org.in`
2. UPI Safety Campaign (NPCI): `upichalega.com`
3. Reserve Bank of India (RBI Kehta Hai): `rbi.org.in`
4. National Cyber Crime Reporting Portal: `cybercrime.gov.in`

CHAPTER 3 • SPOTTING FAKE SCREENS

Fake Payment Screenshots and Spoof Apps

5 major flaws in fake Paytm, PhonePe, and Google Pay screenshots, and counter rules to stop cheating.

The Counter Trick: How Fake Screens Are Made in 5 Seconds

Imagine a customer buying ₹2,400 worth of dry fruits or clothes. Standing at the counter, they pull out their phone and in 5 seconds show you a screen—displaying your shop name, ₹2,400, and a bright green tick.

You nod and hand over the bag. Did you know that screen never came from a bank? It was generated by a **Spoof App**.

Case Study

Garment Merchant Manoj ji's ₹4,800 Loss

On a Sunday evening, two young men entered Manoj ji's clothes shop and picked two jeans and three shirts totaling ₹4,800. One pulled out his phone and said, *"Brother, paying via GPay."*

He waved his phone in front of Manoj ji—showing a green tick and Manoj ji's shop name. Manoj ji asked, *"Soundbox didn't speak."* The man quickly answered, *"Oh Uncle, it's raining outside, network is jammed. Money left my account—hurry up, we have a train to catch."*

Flustered, Manoj ji handed over the clothes. Checking accounts at night revealed ₹0 had arrived. The man had used a Spoof App.

> **Plain truth:** A green tick on a customer's phone can be just a fake image—not real money in your bank.

Spot-the-Fake: How to Catch 5 Flaws in a Fake Screen

Fake screens built with spoof apps usually have these 5 dead giveaways:

🔍 5-Second Test: Real vs Fake Screen

❌ 5 Clues of a Fake Screenshot

- The UTR number is missing or incomplete (only 8–10 digits).
- Text and fonts look slightly blurry, uneven, or thicker than usual.
- The displayed time is often 5 to 10 minutes old or off.
- Your shop's Soundbox stays completely silent.
- No transaction appears inside your Merchant App History.

✅ Sure Proof of a Real Payment

- A complete 12-digit UPI UTR number is cleanly listed.
- Your Soundbox speaks out the exact amount right away.
- An entry appears immediately inside your own Business App.
- A bank Credited SMS arrives on your registered mobile.
- The time and date match the exact current time.

At the Counter: Rush Pressure vs Calm Reply

See how spoof-app scammers act at the counter and how you should respond:

Counter Conversation (Rush Simulation) The Rush Trick

> **Customer (waving phone):** "Brother, sent ₹2,400! Look at the green tick. Pack fast, my car is idling outside!"

> **Smart Shopkeeper (calmly):** "Brother, screen looks fine, just wait 1 second. Show me the 12-digit UTR number in your app so I can match it in mine."

> **Customer (acting offended):** "Are you doubting me? I buy here regularly! Network is slow, it'll speak in a moment!"

> **Smart Shopkeeper (smiling):** "No doubt at all, brother—it's just our shop rule. No item leaves without an entry on our phone. Please sit for 2 minutes."

> **Rule of truth:** A genuine customer will wait 2 minutes and show their 12-digit UTR. A spoof-app scammer makes excuses and bolts.

The 4-Step Spoof App Scam Trap

1 **Pretending to Scan QR at Counter**

The scammer points their camera at your QR code—but opens a fake spoof app instead of a real UPI app.

↓ Entering your shop name & amount

2 Generating a Fake Screen

Inside the fake app, they type your shop name and amount to produce an instant green tick and 'Payment Successful' screen.

↓ Flashing it in front of your eyes

3 Rushing You to Hand Over Goods

They don't let you inspect closely, making excuses like 'missing my train' or 'auto is waiting'.

↓ Stopped by shopkeeper alertness

4 Exposed by Asking for the 12-Digit UTR

The moment you ask for the 12-digit UTR or wait for the Soundbox, the scammer's lie collapses.

3 Strict Rules for Counter Staff

Teach every helper and staff member at your shop clearly:

📌 3 Rules for Counter Staff

Rule 1 Never treat a green tick on a customer's phone screen as proof of a real payment.

Rule 2 Even if a customer rushes you, never hand over goods until your Soundbox speaks or the shop phone gets an SMS.

Rule 3 In any dispute, ask the customer for the 12-digit UTR number and match it inside your Business App.

⚡ **5-SECOND COUNTER DECISION**

Golden Counter Rule

> *"Customer's screen, MY bank account! Until an entry shows on my phone or the Soundbox speaks, not even ₹1 of goods crosses the counter."*

Official Portal: NPCI's UPI Safety Awareness Campaign

NPCI directly warns shopkeepers to watch out for fake payment screens and spoof messages:

NPCI UPI Safety Campaign (Official Portal) NPCI Verified





UPI Lite

3 Key Things to Check:

1. **Official Website:** Always type `upichalega.com` or `npci.org.in` directly in your browser. Never click unknown links.
2. **Account Verification First:** NPCI clearly states—always check your own bank account before trusting any screen or message shown by a customer.
3. **Safe Contact Protocol:** For any UPI dispute or fraud, always follow the verified helpline section on the official portal.

Shopkeeper's Do's and Don'ts

✅ What to Do (Safe Habits)

• Trust ONLY your Soundbox voice or your Merchant App's live entry.

• Match the 12-digit UTR number from the customer's screen inside your Business App.

• Train shop helpers that trusting a customer's screen is strictly forbidden.

• Stay calm during rush hours and check notifications on your own phone.

❌ What Not to Do (Dangerous Mistakes)

• Never hand over goods after seeing just a green tick on a customer's phone.

• Never release goods when told "Network is jammed, it'll arrive later."

• Never trust fake UTR numbers that have only 8 or 10 digits.

• Never break your shop rules under a customer's anger or rush pressure.

Official Sources:

1. National Payments Corporation of India (NPCI): `npci.org.in`
2. UPI Safety Campaign (NPCI): `upichalega.com`
3. Reserve Bank of India (RBI Kehta Hai): `rbi.org.in`
4. National Cyber Crime Reporting Portal: `cybercrime.gov.in`

CHAPTER 4 • PROTECTING YOUR COUNTER & STANDEE

QR Code Swapping and Fake QR Stickers

The dangerous trick of pasting another QR sticker over your standee, and 4 rules to guard your shop's QR.

Counter Tampering: When Customer Money Goes to a Scammer's Bank

Your shop's QR standee is not just cardboard—it is your digital cash box. Dozens of customers scan it every day.

Have you ever thought what happens if someone pastes their own QR sticker over your standee when you step away? Customers pay properly from their side, yet every rupee lands in the scammer's account!

Case Study

Grocery Owner Harishankar ji's ₹8,500 Loss

Harishankar ji runs a busy grocery store. One crowded Saturday evening, two young men stood near the standee pretending to buy soap and oil. One distracted Harishankar ji with questions while the other quietly slapped a fake QR sticker right over the real standee.

Over the next hour, 6 customers paid ₹8,500 total. Each said, *"Brother paid, look it left my account."* Yet Harishankar ji's Soundbox stayed silent. Looking closely at the standee at night, he discovered a second sticker pasted neatly over his real QR!

> **Plain truth:** Never leave your QR standee unattended. It is the main lock of your cash counter.

How Does the QR Sticker Scam Work? (4-Step Flow)

1. **Standing by the Counter in a Crowd**
   The scammer waits for evening crowds or a distracted owner and moves close to the counter.

↓ Sleight of hand

2 **Pasting a Fake QR Sticker**

They paste a matching-size QR sticker directly over your real standee so it looks invisible at first glance.

↓ Customers unknowingly pay the scammer

3 **All Payments Go to the Scammer**

Customers scan and money leaves their account—but your Soundbox stays silent because money went to the thief.

↓ Stopped by shopkeeper alertness

4 **Daily Morning Finger Check Rule**

Running your finger over the standee and using the QR printed on the Soundbox stops this scam 100%.

4 Rules to Keep Your Shop's QR Code Safe

Build these 4 daily habits to protect your cash box:

1 **Morning Finger Check**

Every morning when opening the shop, run your finger across the QR standee. If anyone pasted a sticker on top, you'll feel the edges immediately.

2 **Keep It Inside a Hard Acrylic Frame**

Never leave a QR printed on loose paper or cardboard. Seal it inside a hard acrylic frame so no sticker goes unnoticed.

3 **Use the QR Printed on Your Soundbox**

If you have a Soundbox, use the permanent QR printed on the Soundbox body itself—it is the safest option.

4 **Do a ₹1 Morning Test Payment**

Right after opening your shop, scan ₹1 from your own phone. When the Soundbox speaks, you know 100% your QR is safe and working.

At the Counter: When a Customer Says "Money Left, Why Didn't It Speak?"

🏪 Counter Conversation (Simulation)

QR Alert

Customer: "Brother, I scanned your standee and sent ₹800. Money left my account—why didn't your Soundbox announce it?"

Smart Shopkeeper (checking standee right away): "Brother, show me in your app what name received the money—is it my shop name or some stranger's name?"

Customer (checking phone): "Whoa, it says 'Rohit Kumar' here, though your shop is 'Gupta Kirana'!"

Rule of truth: If a customer's phone shows a stranger's name instead of your shop name, your standee was tampered with. Pull down the standee right away and check for stickers.

⚡ 5-SECOND COUNTER DECISION

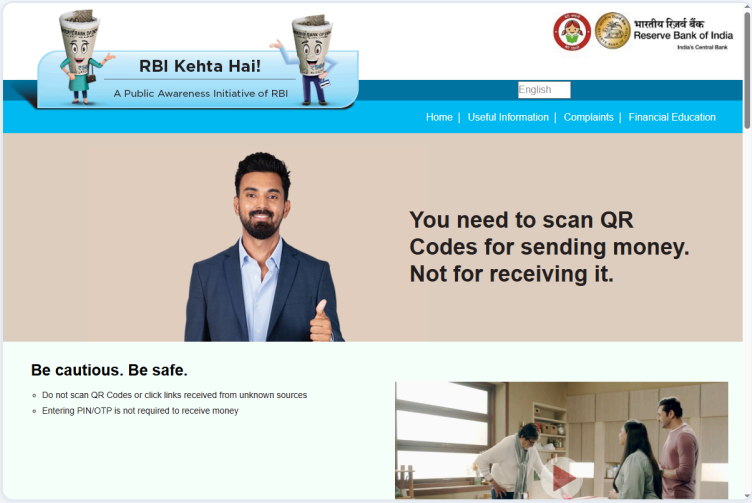
Golden QR Rule

"Your counter QR code is your cash box! Checking it with your finger every morning is just as important as unlocking your shop shutter."

Official Portal: RBI Kehta Hai - Fraud Through UPI QR

The Reserve Bank of India (RBI) clearly warns citizens and merchants about QR code risks:

RBI Kehta Hai (Official Portal) RBI Verified



3 Key Things to Check:

1. **Official Website:** Always type `rbikehtahai.rbi.org.in` or `rbi.org.in` directly in your browser. Never click unknown links.
2. **QR Safety Rules:** RBI clearly states that a QR code is scanned only to send money—never to receive it.
3. **Safe Contact Protocol:** For any unauthorized transaction, alert your bank right away and use only verified routes on official portals.

Shopkeeper's Do's and Don'ts

✅ What to Do (Safe Habits)

• Run your finger over your QR standee every morning to check for extra stickers.

• Always keep your QR code sealed inside a hard acrylic frame or lamination.

• Do a ₹1 test scan from your own phone every morning when opening.

• Always place the standee where it stays in direct sight of the counter.

❌ What Not to Do (Dangerous Mistakes)

• Never leave your QR standee outside the shop or unattended at night.

• Never tape an unframed paper printout of your QR code on the wall.

• Never hand over goods if Soundbox is silent and the customer's phone shows a stranger's name.

• Never leave a helper alone at the counter without teaching them the QR check.

Official Sources:

1. Reserve Bank of India (RBI Kehta Hai): `rbikehtahai.rbi.org.in`
2. National Payments Corporation of India (NPCI): `npci.org.in`

3. UPI Safety Campaign (NPCI): `upichalega.com`
4. National Cyber Crime Reporting Portal: `cybercrime.gov.in`

CHAPTER 5 • THE BIGGEST CASH REFUND TRAP

The "Sent Extra by Mistake, Refund Cash" Trick

Fake overpayment dramas, fake screens, and the unbreakable rule to stop cash being stolen from your till.

Direct Till Robbery: When a ₹300 Purchase Demands ₹3,000 Cash Back

This is the cleverest fraud targeting retail shopkeepers. Here the scammer doesn't just steal goods—they walk away with hard-earned cash straight out of your cash drawer!

Imagine a new customer buying ₹350 worth of medicine or groceries. After scanning the QR, they suddenly grab their head in panic: *"Oh brother, what did I do! I meant to send ₹350, accidentally typed an extra zero, and sent ₹3,350! It left my account—please give me ₹3,000 cash back, I have to rush to the hospital!"*

Case Study

Chemist Jagdish ji's ₹4,500 Loss

Late one night, a young man came to Jagdish ji's medical store and picked ₹500 worth of pain spray and medicines. He scanned PhonePe and showed Jagdish ji a ₹5,000 'Payment Successful' screen.

The man began crying: *"Brother, ₹5,000 went by mistake! That was my last money. Please give me ₹4,500 cash back or how will I buy other medicines!"* Seeing his tears, Jagdish ji pulled ₹4,500 cash from the drawer and handed it over. Soundbox hadn't spoken, yet the man blamed "slow night server."

Next morning, Jagdish ji's bank passbook showed ₹0 had arrived that night. That screen was made by a fake UPI app. Jagdish ji lost both ₹500 of goods and ₹4,500 cash!

> **Plain truth:** Even if someone genuinely sent extra money, NEVER hand over cash from your drawer. Digital money goes back ONLY through digital banking.

The 4-Step Overpayment Scam Cycle

1 **Acting Emotional and Rushed**

The scammer always invents an emotional story —"rushing to hospital", "buying urgent medicine", or "typed an extra zero."

↓ Showing a fake screen or SMS

2 **Fake Screenshot of a Large Amount**

They show a fake ₹3,000 or ₹5,000 screenshot on their phone or send a fake SMS to yours.

↓ Demanding cash from the counter

3 **Pressuring for Real Cash Back**

Notice they never ask "transfer back to my bank"—they always insist on immediate cash from your drawer.

↓ Protected by the shopkeeper's rule

4 **Stopped by the "Zero Cash-Back" Rule**

The shopkeeper refuses firmly: "Zero cash ever leaves the till—refunds happen only via bank reversal."

3 Unbreakable Rules to Beat Overpayment Scams

Whenever a customer claims "I sent extra money by mistake", stick strictly to these 3 rules:

1 **Open Your Own Business App**

Never touch the customer's phone. Open your own Merchant App and check your bank balance. If there's no entry, the talk ends right there.

2 **Zero Cash-Back Rule: Never Give Cash**

Even if money really arrived in your account, never give ₹1 in cash from the till. Say: *"Refunds go only via bank reversal back to the same UPI ID."*

3 **Wait 24 Hours and Note Details**

Tell the customer: *"Brother, write down your name and details. After matching tonight's bank statement, money goes straight back to that same bank account."*

At the Counter: Emotional Drama vs Firm Shopkeeper

Counter Conversation (Simulation) The Cash Refund Trap

Customer (folding hands, looking distressed): "Brother, I needed ₹400 of groceries and accidentally sent ₹4,400! Look at PhonePe's green tick. Please give ₹4,000 cash back—I have to buy mom's medicines!"

Smart Shopkeeper (calmly): "Brother, I understand your trouble. But our strict shop rule is zero cash back from the drawer. Let me check my Business App first."

Customer (getting angry): "What kind of person are you? Money left my account, screen is right here! Are you trying to pocket my ₹4,000 cash?"

Smart Shopkeeper (firmly): "Nothing like that, brother. Zero money has shown in my app yet. Even if it came, it can only reverse back to the exact UPI ID it came from—never in cash."

Rule of truth: A real customer will agree to a bank reversal. A scammer drops the fight and disappears fast.

⚡ **5-SECOND COUNTER DECISION**

Golden Cash Refund Rule

> *"Digital money settles ONLY digitally! No matter how much a customer begs or cries, real cash NEVER leaves the cash drawer."*

💡 **Official RBI Rule: Never Refund Cash from the Counter**

Simple rule: If someone says "Sent extra by mistake, return cash", don't give a single rupee in cash. Under RBI rules, the customer should raise a 'Chargeback / Reversal' dispute in their bank app so both banks settle it directly.

🌐 Official Portal: `rbikehtahai.rbi.org.in` • Google Search: `RBI Kehta Hai`

Shopkeeper's Do's and Don'ts

✅ What to Do (Safe Habits)

• Never decide on any refund claim without checking your real bank balance first.

• Return genuine overpayments only back to the exact same UPI ID via bank reversal.

• Give strict orders to shop staff never to hand over ₹1 in cash refunds from the till.

• Note the customer's name, details, and 12-digit UTR number in a register.

❌ What Not to Do (Dangerous Mistakes)

• Never give real cash out of pity for crying or emotional stories.

• Never believe fake screenshots or SMS alerts shown on a customer's phone.

• Never transfer refund money to a different unknown number or another UPI ID.

• Never allow staff to issue cash refunds when the owner is away.

Official Sources:

1. Reserve Bank of India (RBI Kehta Hai): `rbikehtahai.rbi.org.in`
2. National Payments Corporation of India (NPCI): `npci.org.in`
3. UPI Safety Campaign (NPCI): `upichalega.com`
4. National Cyber Crime Reporting Portal: `cybercrime.gov.in`

CHAPTER 6 • THE BIGGEST UPI PIN TRICK

Collect Requests and Refund Traps

The trick of asking for your UPI PIN to 'receive' money—and how to keep your shop's bank account safe.

UPI's Unbreakable Rule: You Never Need a PIN to Receive Money!

The biggest, unchangeable rule of UPI across India is just one sentence:

⚡ GOLDEN LINE

"You NEVER need a UPI PIN to receive money. Your UPI PIN is entered ONLY and ONLY to deduct (pay) money out of your account."

Yet scammers twist this basic rule to trap shopkeepers. Posing as a buyer, they send a 'Collect Request' to your phone saying: *"Brother, open your app and enter your PIN so the money enters your account."*

Case Study

Hardware Store Owner Balram ji's ₹12,000 Loss

At Balram ji's hardware shop, a customer picked ₹2,500 worth of pipes and taps. At the counter he said, *"Brother, QR scan isn't working—server error. Tell me your PhonePe number, I'll send a direct payment request."*

Balram ji gave his number. Ten seconds later a PhonePe notification popped up. The customer urged: *"Uncle, open it, tap the green 'Pay' button, and enter your 4-digit UPI PIN so the money gets added."* In a rush, Balram ji typed his PIN.

Instead of receiving ₹2,500, ₹12,000 vanished from Balram ji's account! The scammer had sent a ₹12,000 Collect Request—and slipped away right in front of his eyes.

> **Plain truth:** Whenever your phone screen asks for your 4- or 6-digit UPI PIN, money is LEAVING your account—never arriving!

The 4-Step Collect Request Scam Cycle

1 **Fake Excuse That QR Scan Failed**

The scammer claims QR isn't working and asks for the shopkeeper's registered UPI mobile number.

↓ Sending a request to take money instead of pay

2 **Sending a Collect / Pay Request**

Instead of sending money from their phone, they send a payment request asking YOU to pay.

↓ Lying about entering PIN

3 **Saying "Enter PIN to Receive Money"**

They lie that opening the notification and typing your PIN will credit money—the biggest lie of all.

↓ Saved by shopkeeper awareness

4 **Tapping Decline Immediately**

The moment the shopkeeper sees 'Pay' on screen, they tap Decline right away and never enter any PIN.

Spot-the-Difference: 'Pay' vs 'Receive' Truth

🔍 What Shows on Screen? (Real vs Fraud)

❌ When Money Will Leave Your Account (Fraud)

- Screen shows a 'Pay' or 'Accept Request' button.
- Asks you to enter your 4- or 6-digit UPI PIN.
- Top says 'Request by XYZ'.
- The moment you enter PIN, your bank balance drops.

✅ When Money Arrives at Your Shop (Real)

- You never have to enter any PIN.
- Soundbox announces the amount automatically.
- Your Business App shows a 'Credited' notification.
- Your bank balance goes up.

At the Counter: Trying to Confuse You vs Firm Reply

Counter Conversation (Simulation)

The PIN Trap

Customer: "Brother, I sent you a ₹1,800 request. A notification must have come—enter your PIN fast so it credits to your account!"

Smart Shopkeeper (looking at phone): "Brother, my phone says 'Pay ₹1,800'. You never enter a PIN to receive money—entering my PIN will cut money from MY account!"

Customer (rushing): "No Uncle, that's the bank's new system! You have to accept first to receive it. Tap fast!"

Smart Shopkeeper (tapping Decline right away): "There's no such system, brother. UPI's rule is clear: PIN entered = money gone. I'm declining this. Scan our counter QR to pay."

Rule of truth: A scammer panics and bolts the moment you decline their Collect Request.

⚡ 5-SECOND COUNTER DECISION

Golden PIN Rule

> *"PIN entered = Money gone! Whenever a screen asks for your UPI PIN, money is leaving your pocket. NEVER enter a PIN to receive money."*

💡 **Official NPCI Rule: No PIN Needed to Receive Money**

Simple rule: You never enter a PIN to receive UPI money. If a customer says "I sent a Collect Request, enter your PIN to get paid", it is 100% fraud—entering your PIN will deduct money from your account.

🌐 Official Safety Portal: `upichalega.com` • Google Search: `NPCI UPI PIN Safety`

Shopkeeper's Do's and Don'ts

✅ What to Do (Safe Habits)

• Always take payments strictly through the official QR code placed at your counter.

• Immediately tap Decline on any 'Pay' or 'Collect Request' popping up on your phone.

• Train every shop helper that receiving money never requires entering a PIN.

• If money ever gets deducted by mistake, alert your bank right away.

❌ What Not to Do (Dangerous Mistakes)

• Never enter your UPI PIN to receive money on any customer's instructions.

• Never tap 'Pay' on a PhonePe or GPay notification sent by any stranger.

• Never believe excuses like "Entering your PIN deposits money."

• Never write down your UPI PIN on paper near the counter.

Official Sources:

1. National Payments Corporation of India (NPCI): `npci.org.in`
2. UPI Safety Campaign (NPCI): `upichalega.com`
3. Reserve Bank of India (RBI Kehta Hai): `rbi.org.in`
4. National Cyber Crime Reporting Portal: `cybercrime.gov.in`

CHAPTER 7 • BIG ORDER BAIT & SCAM CALLS

Fake Orders and Fake Customer Calls

"It's a big Army camp or govt office order" — protecting your shop from fake advance payments and link scams.

Dream of Big Profits: When a Huge Order Turns Into a Huge Loss

Every shopkeeper loves getting a big wholesale phone order—food for 100 people, 50 kg of sweets, or ₹40,000 of groceries can make any merchant's day.

Scammers exploit that exact excitement. Calling from an unknown number posing as a govt or army officer, they say *"We're sending ₹15,000 advance right now"*—and rob the shopkeeper in the name of sending that advance.

Case Study

Sweet Shop Owner Deendayal ji's ₹28,000 Loss

One afternoon, an unknown call arrived at Deendayal ji's sweet shop: *"We're calling from the nearby Army Cantt. Tomorrow we have a big function for 120 soldiers and need 40 kg of gulab jamun and snacks. We're sending ₹15,000 advance right now."*

Thrilled, Deendayal ji agreed. The caller said: *"Army accounts can't send directly to a regular QR. I sent a barcode on WhatsApp—scan it with PhonePe and enter your 6-digit PIN so the money credits to you."*

Eager for the big order, Deendayal ji scanned and entered his PIN—and ₹15,000 vanished in 5 seconds! The caller phoned right back: *"Oh Uncle, system glitch—sending ₹13,000 more, scan this second barcode."* He lost ₹28,000 total before the number switched off forever.

> **Plain truth:** Any real customer placing a big order will NEVER ask you to scan a barcode or enter a PIN to receive an advance.

The 4-Step Fake Order Scam Cycle

1 **Big Order & Fake Govt Identity**

The scammer poses as an Army, Police, Hospital, or School officer placing a huge order.

↓ Offering instant advance

2 **"Govt Account Rules" Excuse**

They claim a government account cannot pay a normal QR directly—so you must scan their barcode.

↓ Barcode or AnyDesk trap

3 **Tricking You to Scan & Enter PIN**

They send a debit barcode on WhatsApp lying that entering your PIN will deposit the advance.

↓ Protected by shopkeeper's rule

4 **Firm Rule: "Pay Only on Shop's QR"**

The shopkeeper refuses firmly: "Advance comes only to our shop QR—we never scan any barcode."

3 Strict Rules for Phone Orders

Write these 3 rules on your shop wall for every big order received over an unknown call:

Advance Only on Your Shop's Official QR

Tell the caller: *"Sending our official QR on WhatsApp—just scan and pay normally."* Never scan any QR sent by the customer.

2 **Never Install Screen Share Apps**

If a caller says "Download AnyDesk or TeamViewer to activate payment gateway", hang up immediately—it is 100% fraud.

3 **Require Cash Token at the Shop**

For big orders from strangers, ask someone to visit the shop to pay a cash token or pay in full at pickup.

On a Phone Call: Greed Trap vs Smart Shopkeeper

📞 Unknown Call Conversation (Simulation)

The Fake Order Play

Caller: "Namaste, Subedar speaking from Army Cantt. Tomorrow we have dinner for 80 people and need ₹20,000 of supplies. Sending ₹10,000 advance now—check WhatsApp."

Smart Shopkeeper: "Thank you very much sir. Please pay ₹10,000 to our shop QR code—the moment our Soundbox speaks, we'll start preparing."

Caller: "Oh shopkeeper ji, military accounts don't send to regular QR! Scan the barcode I sent on WhatsApp and enter your PIN so ₹10,000 credits right away."

Smart Shopkeeper: "Sir, nobody in the world ever scans a barcode or enters a PIN to receive money. Please send someone to our shop with cash advance—I won't scan any barcode."

Rule of truth: A scammer hangs up or curses immediately. A real buyer sends a token to the shop.

⚡ **5-SECOND COUNTER DECISION**

Golden Order Rule

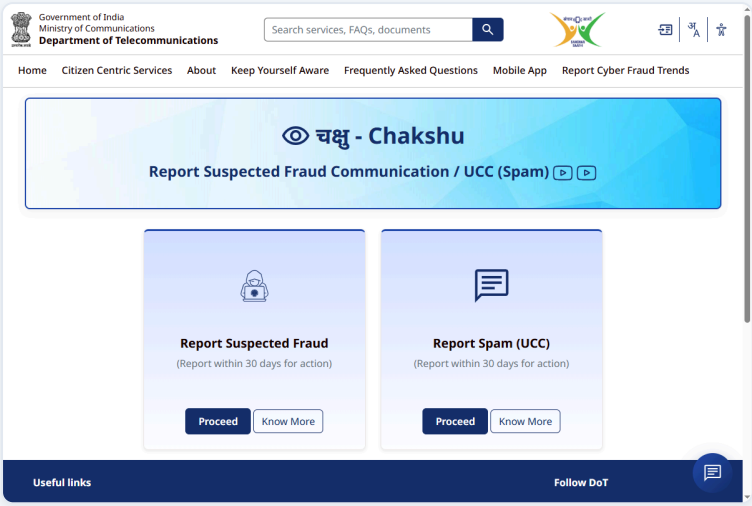
> *"Don't lose your focus seeing a big order! Any buyer asking you to scan a barcode or enter a PIN for an advance is a scammer, not a customer."*

Official Portal: Sanchar Saathi (Chakshu)

If anyone tries to cheat you over a phone call, SMS, or WhatsApp using a fake identity, report them on the Telecom Department's Chakshu Portal:

Sanchar Saathi - Chakshu (Official Portal)

Government of India



3 Key Things to Check:

1. **Official Website:** Always type `sancharsaathi.gov.in` directly in your browser. Never open unknown SMS links.
2. **Report Suspected Fraud:** Report numbers pretending to be govt officers within 30 days on the portal.
3. **Safe Helpline Protocol:** For any financial fraud complaint, go straight to the National Cyber Crime Reporting Portal via official routes.

Shopkeeper's Do's and Don'ts

✅ What to Do (Safe Habits)

• Always require a cash token at the shop for big orders from unknown calls.

• Accept advances strictly on your shop's official standee QR.

• Report suspicious callers right away on Chakshu Portal.

• Train shop staff never to enter a PIN on any customer's instructions.

❌ What Not to Do (Dangerous Mistakes)

• Never scan any barcode or QR sent by a customer on WhatsApp.

• Never trust advance claims blindly just because someone names the Army or govt.

• Never install AnyDesk or TeamViewer on your phone for any customer.

• Never prepare huge stock without confirmed advance payment.

Official Sources:

1. Department of Telecommunications (Sanchar Saathi Chakshu): `sancharsaathi.gov.in`
2. National Payments Corporation of India (NPCI): `npci.org.in`
3. Reserve Bank of India (RBI Kehta Hai): `rbi.org.in`
4. National Cyber Crime Reporting Portal: `cybercrime.gov.in`

CHAPTER 8 • TRAINING YOUR SHOP STAFF

What to Train Your Staff and Helpers

Protecting your counter when the owner steps out—3 strict rules for helpers and running a loss-free shop.

When the Owner Steps Away: A Scammer's Favorite Time

A shopkeeper cannot sit at the counter every second—you step into the godown, visit wholesale markets, or go inside for 15 minutes for lunch.

80% of retail market scams happen the exact moment the owner steps out! Scammers watch outside and walk straight in as soon as a new helper or worker sits at the counter.

Case Study

Grocery Owner Bansilal ji's Helper's ₹3,800 Mistake

Bansilal ji stepped into the back godown to prepare stock bills, leaving 19-year-old helper Rahul at the counter. A sharply dressed man walked up and hurriedly got ₹3,800 of expensive ghee, oil, and almonds packed.

Flashing a green tick on his phone, he said: *"Brother, paid! Bansilal ji knows me well—load it into the rickshaw fast."* Rahul hesitated: *"Brother, Soundbox didn't speak."* The man snapped: *"Are you new here? I pay Bansilal ji online every day! It's raining outside, hurry up!"*

Scared of being scolded, Rahul handed over the bags. When Bansilal ji checked his phone later, ₹0 had arrived—the man had used a fake UPI app screen.

> **Plain truth:** Before blaming staff, teach them one firm rule—no matter how angry or pushy a customer acts, nothing leaves without the Soundbox speaking.

3 Strict Rules for Counter Staff (Counter SOP)

Make every helper and worker at your shop memorize these 3 rules:

📌 3 Unbreakable Staff Rules

Rule 1 **No Screen Trust:** Never treat a green tick on a customer's phone screen as proof of payment. Trust ONLY the shop's Soundbox announcement or bank SMS on the counter phone.

Rule 2 **Zero Cash Refund:** If a customer claims "Sent ₹2,500 instead of ₹500 by mistake, give ₹2,000 cash back", never take even ₹1 cash out of the drawer without the owner present.

Rule 3 **Standee Vigilance:** If any stranger lingers near or touches your QR standee, check right away that no extra sticker was pasted over it.

The Scam Cycle When the Owner Steps Out

1 **Waiting for the Owner to Step Away**

The scammer watches nearby until the shop owner steps away for lunch or into the godown.

↓ **Pressuring the young helper**

2 **Bullying and Faking Urgency**

They boast: "I know your boss personally, I shop here daily—pack my stuff fast."

↓ **Flashing a fake screen**

3 **Scolding While Showing a Green Tick**

If the helper asks to wait, the scammer acts angry to intimidate them.

↓ **Saved by staff training**

4 **Staff's Firm Reply**

Staying calm, the helper replies: "Owner's strict order—nothing goes out until the Soundbox speaks."

At the Counter: Pushy Scammer vs Smart Helper

Counter Conversation (Simulation)

The Bullying Trick

Customer (acting bossy): "Hey kid! Paid ₹2,800, look at the green tick. Load the box in my car fast—your boss knows me well!"

Smart Staff (polite yet firm): "Great that you know Seth ji, brother—but Seth ji's strict rule is that nothing leaves the counter until the Soundbox speaks or our counter phone gets a message."

Customer (glaring angrily): "Teaching me rules? I'll call Seth ji right now and get you fired!"

Smart Staff: "Sure brother, please call Seth ji—he's right inside the godown, let me call him out too."

Rule of truth: The moment the owner's name is called, a scammer drops the bags and runs.

⚡ **5-SECOND COUNTER DECISION**

Golden Staff Rule

> *"Owner away, Staff alert! No matter how loud a customer bullies or shouts, nothing crosses the counter until the Soundbox speaks."*

💡 **Official RBI Rule: What Staff Must Know**

Simple rule: Clearly train every staff member and helper—never let goods leave without hearing the Soundbox under pressure of "I know the owner" or "It's raining, hurry up."

🌐 Official Portal: `rbikehtahai.rbi.org.in` • Google Search: `RBI Kehta Hai Digital Safeguards`

Shopkeeper's Do's and Don'ts

✅ What to Do (Safe Habits)

• Before stepping away from the counter, remind staff not to release goods without Soundbox confirmation.

• Stick a 'Zero Cash Refund' sign clearly near the counter.

• Train staff never to break rules out of fear of a customer's anger.

• Make it a rule for staff to call or summon the owner right away during any dispute.

❌ What Not to Do (Dangerous Mistakes)

• Never leave a new helper at the counter without teaching digital safety first.

• Never allow staff to release goods just by seeing a green tick on a customer's phone.

• Never allow staff to issue cash refunds without the owner's permission.

• Never leave the Soundbox switched off or muted at the counter.

Official Sources:

1. Reserve Bank of India (RBI Kehta Hai): `rbikehtahai.rbi.org.in`
2. National Payments Corporation of India (NPCI): `npci.org.in`
3. UPI Safety Campaign (NPCI): `upichalega.com`
4. National Cyber Crime Reporting Portal: `cybercrime.gov.in`

CHAPTER 9 • EMERGENCY ACTION & COMPLAINTS

What to Do After Fraud & How to Complain

Golden 2-hour action, alerting your bank fast, collecting evidence, and reporting on the official portal.

The First Hour After Fraud: Act Fast Instead of Panicking

Despite being careful, a mistake can still happen during heavy evening crowds, a new helper's slip, or a clever scammer's rush.

But if you are cheated by a fake screenshot, cash refund trick, or wrong transfer, sitting in regret won't bring back ₹1. In online fraud, the first **2 hours (Golden Hours)** matter most.

Case Study

Garment Owner Sudhir ji's Smart Move: Full ₹18,000 Recovered

A scammer took ₹18,000 of sherwanis and kurtas from Sudhir ji's shop using a fake payment screen and vanished. Fifteen minutes later, checking his app showed no money had arrived.

Sudhir ji didn't waste a second. He pulled the scammer's photo from shop CCTV, noted the number shown on the fake screen, called his bank's official helpline to report a fraud transaction, and filed a complaint on `cybercrime.gov.in`.

Because he reported fast, Cyber Cell froze the receiving bank account within 45 minutes—and after 15 days of legal steps, Sudhir ji got all ₹18,000 back!

> **Plain truth:** Reporting within the first 2 hours is what freezes stolen funds before they leave via ATMs.

The 4-Step Golden Action Plan for the First 2 Hours

Take these 4 steps without wasting 1 minute the moment you spot fraud:

1 **Alert Your Bank Immediately**

Call your bank's official helpline directly, share the transaction time and amount, and log a fraud dispute.

↓ Gathering all proof in one place

2 **Keep Evidence Ready**

Write down the screen photo if any, shop CCTV footage, 12-digit UTR number, and exact transaction time.

↓ Online report on govt portal

3 **Complain on Cyber Crime Portal**

Open `cybercrime.gov.in` directly, go to 'Register a Complaint' -> 'Financial Fraud', and submit everything.

↓ Raising a dispute in Merchant App

4 **Log a Dispute in Your Merchant App**

Open Help inside Paytm for Business, Google Pay Business, or PhonePe Business and mark that transaction as fraud.

Safe Contact Protocol

During any crisis, NEVER call unknown numbers from Google Search. Always follow this 3-step safe path:

1. **Open the Official Website Directly**
   Type your bank's official URL or `cybercrime.gov.in` directly into your browser bar—never click ads or links.

2. **Go to 'Contact Us' or 'Helpline'**
   Open the official 'Contact Us' page from the website's main menu.

3. **Follow Only the Verified Route**
   Use only the verified contact details from the official website to file your complaint.

⚡ **5-SECOND COUNTER DECISION**

Golden Complaint Rule

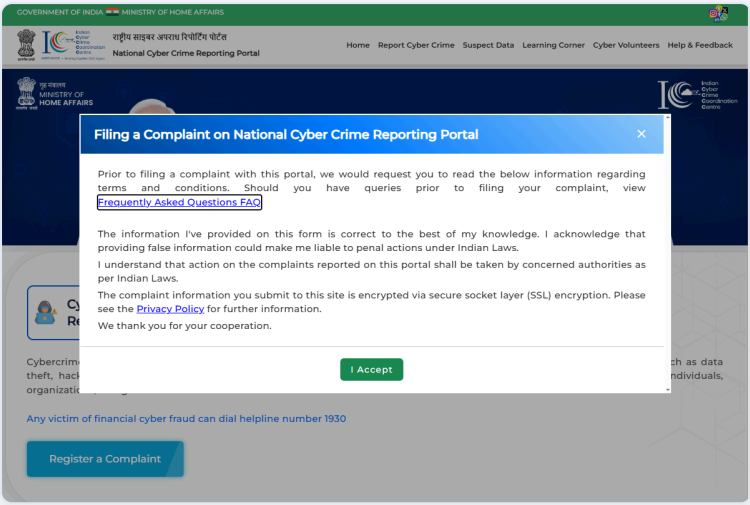
> *"Fear or regret won't bring back ₹1! Reporting to your bank and on cybercrime.gov.in within the first 2 hours is what freezes the scammer's account."*

Official Portal: Filing a Complaint on Cyber Crime Portal

Official page to file a complaint on the National Cyber Crime Reporting Portal:

National Cyber Crime Reporting Portal (Official)

Government of India



3 Key Things to Check:

1. **Official Website:** Always type `cybercrime.gov.in` directly—never visit via unknown SMS or links.
2. **Terms & Instructions:** Read portal instructions carefully and enter accurate transaction details.
3. **Safe Helpline Access:** Use only the portal's official Helpline section for assistance.

🔍 Forgot the Govt Website? Search This on Google:

Search directly on Google: `National Cyber Crime Portal Complaint`

• **Skip 'Ad' / 'Sponsored':** Never click results marked 'Ad' or 'Sponsored' at the top.

• **Check Govt Domain:** Always look for `.gov.in` at the end (like `cybercrime.gov.in`).

• **Official Contact:** Take verified numbers only from the portal's 'Contact Us' page.

Shopkeeper's Do's and Don'ts

✅ What to Do (Safe Habits)

• Complain to your bank and Cyber Crime Portal within 2 hours of spotting any fraud.

• Save shop CCTV footage, transaction UTR numbers, and timestamps safely.

• Raise an immediate dispute inside your Merchant App's Support section.

• Carry copies of all digital evidence when filing a police complaint.

❌ What Not to Do (Dangerous Mistakes)

• Never skip complaining thinking "Let it go, it's a small loss."

• Never search Google for customer care numbers and call strangers.

• Never give your UPI PIN or OTP to anyone in the name of registering a complaint.

• Never post half-baked claims on social media before gathering proper proof.

Official Sources:

1. National Cyber Crime Reporting Portal: `cybercrime.gov.in`
2. Reserve Bank of India (RBI Kehta Hai): `rbi.org.in`
3. National Payments Corporation of India (NPCI): `npci.org.in`
4. Telecom Department (Sanchar Saathi): `sancharsaathi.gov.in`

CHAPTER 10 • MASTER SAFETY CHECKLIST

Shopkeeper's Daily Safety Checklist

Complete counter-side checklist: daily safety habits from opening the shutter in the morning to locking up at night.

Your Cash Box's Shield: A 10-Second Daily Habit

This is the most practical chapter of the entire book. In retail, the biggest loss doesn't come from shoplifting—it comes from 5 seconds of carelessness at the counter.

Stick this checklist on your counter glass, near your cash drawer, or on the first page of your ledger. Review it every morning and evening.

Case Study

Grocery Owner Laxminarayan ji's 100% Safe Counter

Laxminarayan ji pasted a small sign right on his shop counter: *"Goods are handed over ONLY after Soundbox announces payment or bank SMS arrives."*

Every morning upon opening, he runs his finger over the QR standee, checks Soundbox battery, and reminds his helper not to release goods without audio confirmation. In 3 years, dozens of scammers tried fake screenshots and overpayment tricks—and couldn't steal even 1 paisa.

> **Plain truth:** Keep rules strict from Day 1. Honest customers never mind, and scammers won't even dare step inside.

🌞 1. Morning Routine (Opening the Shop)

Do these 4 quick checks right after unlocking your shutter:

📋 4 Morning Checks

Check 1 **QR Standee Finger Check:** Run your finger across your QR code to ensure nobody pasted a fake sticker on top overnight.

Check 2 **Soundbox Battery & Volume:** Switch on your Soundbox, check battery level, and keep volume loud enough to hear over market noise.

Check 3 **₹1 Test Payment:** Scan ₹1 from your own phone. Once Soundbox announces clearly, your system is 100% live.

Check 4 **Staff Briefing:** Remind your counter helper never to release goods without hearing the Soundbox.

2. Business Hours Rules (At the Counter)

Keep these 5 rules unbreakable during daily crowds and payments:

5 Golden Counter Rules

Rule 1 **No Screen Trust:** Never accept a green tick on a customer's phone screen as proof of payment.

Rule 2 **Match 12-Digit UTR:** If Soundbox is silent, ask for the 12-digit UPI UTR number and verify it inside your Merchant App.

Rule 3 **Zero Cash Refund:** Never give even ₹1 cash back from the drawer for "sent extra by mistake" claims—only bank reversals apply.

Rule 4 **No PIN for Receiving:** Never enter a UPI PIN to receive money. Decline incoming Collect Requests right away.

Rule 5 **No Barcode for Orders:** Never scan WhatsApp barcodes or install AnyDesk for big phone orders from strangers.

🌙 3. Closing Routine (Shutting the Shop at Night)

Take 2 minutes before closing every night for these checks:

🌙 Night Tally & Security

Rule 1 **Match Daily Tally:** Open 'Daily Settlements' in your Merchant App and match total digital sales against your cash box and sales register.

Rule 2 **Lock Standee Inside:** Never leave your QR standee or Soundbox outside or unattended—lock them safely inside before heading home.

⚡ **5-SECOND COUNTER DECISION**

Golden Master Rule

> *"Small daily care protects a lifetime of earnings! An alert shopkeeper is the most successful and worry-free merchant."*

💡 **Official Safety Habit: Daily Settlement Check**

Simple rule: Every night while closing your shop, match 'Daily Settlements' in your Merchant App with your sales register. Report any mismatch to your bank that very night within 24 hours.

🌐 Official Portal: `rbikehtahai.rbi.org.in` • Google Search: `RBI Kehta Hai Safety Guidelines`

Shopkeeper's Do's and Don'ts

✅ What to Do (Safe Habits)

• Print this checklist and stick it right on your counter glass.

• Follow the morning Finger Check and ₹1 Test Payment every single day.

• Match your Merchant App digital sales tally every night before closing.

• Remind your staff of the 3 digital safety rules every week.

❌ What Not to Do (Dangerous Mistakes)

• Never compromise shop rules because a customer is angry or in a hurry.

• Never hand over goods without hearing your Soundbox or receiving a bank SMS.

• Never hand over even ₹1 in cash refunds from your cash drawer.

• Never leave your QR standee outside the shop unattended at night.

Official Sources:

1. Reserve Bank of India (RBI Kehta Hai):

`rbikehtahai.rbi.org.in`

2. National Payments Corporation of India (NPCI): `npci.org.in`
3. UPI Safety Campaign (NPCI): `upichalega.com`
4. National Cyber Crime Reporting Portal: `cybercrime.gov.in`

MERCHANT SAFETY GLOSSARY

Essential Digital Terms for Shopkeepers

12-Digit UTR Number (UPI Reference Number)

The 12-digit sure proof of every real UPI payment. If a customer says "money got cut", match their UTR number inside your Merchant App.

Spoof App (Fake Payment App)

Fraud apps built to show fake green-tick receipts identical to Paytm, PhonePe, or GPay—while ₹0 enters your bank.

QR Sticker Swap (QR Sticker Swapping)

Quietly pasting a scammer's own QR sticker over your counter standee so customer payments go straight to the scammer.

Overpayment Scam (Overpayment Drama)

Showing a fake ₹5,000 SMS for a ₹500 purchase and tricking the shopkeeper into handing back ₹4,500 in real cash.

Collect Request (Money-Deducting Request)

A payment request sent by the other person. Accepting it and entering your UPI PIN deducts money from your shop account instead of adding it.

Merchant Soundbox (Soundbox Speaker)

The counter speaker that announces only when money actually reaches your bank. If silent, trust only your Business App and bank SMS.

Official Sender ID (Spotting Real Bank SMS)

Genuine bank SMS alerts always arrive from a 6-letter official ID (like AD-HDFCBK, VK-SBIINB)—never from a 10-digit mobile number.

Merchant Digital Safety Pledge

4 Unbreakable Rules for Your Cash Counter

Every shopkeeper and staff member must remember these 4 points firmly:

1. **No Soundbox, No App Entry = No Goods:**
   Never release goods just by seeing a receipt on a customer's phone.

2. **Zero Cash-Back Rule:**
   Never return cash for "sent extra by mistake" stories.

3. **Morning Finger QR Check:**
   Check your QR standee every morning for pasted fake stickers.

4. **No PIN to Receive Money:**
   Never enter a UPI PIN for advance orders or refunds.

✓ 10 Easy Chapters | ✓ Staff Training Rules | ✓ Counter Print Checklist

Safe Contact Rule: For help with any payment dispute or fraud, always open your Bank's or Cyber Crime Portal's official website directly and take the real number from the Contact Us section.

Merchant Cyber Safety Awareness Series • 2026 Edition

Mobile Pocket Format (120mm × 190mm)