



Gurukul Technicals Institute

Computer education · Robotics · Science projects · Delhi

FREE EBOOK

COMPUTER AND OFFICE SKILLS

Safe UPI and Digital Payments

Pay and receive money online, and recognise the tricks fraudsters use

INSIDE THIS BOOK

- What UPI is and how it works
- Setting up a UPI app safely
- UPI IDs and QR codes
- Paying and receiving: the golden rule
- Cards and net banking basics
- ...and 6 more chapters, practice questions and a glossary

Beginner

Families, students, shopkeepers and senior citizens

engineergurukul.com

+91 97116 99511

Safe UPI and Digital Payments

Learn how UPI, QR codes, cards and net banking work, and how to pay and receive money safely. You will learn the one rule that stops most frauds, recognise the common tricks fraudsters use, and know exactly what to do in the first hour if money is ever stolen.

WHO IT IS FOR	Families, students, shopkeepers and senior citizens
LEVEL	Beginner
SUBJECT AREA	Computer and office skills
WHAT IS INSIDE	11 chapters, practice questions with answers, and a glossary

HOW TO USE IT

Read one chapter at a time and try the examples as you go: on a computer, at your workbench or in your notebook. The boxes give tips, safety points and short activities. When you finish, test yourself with the practice questions and check your answers at the end. Words you may not know are explained in the glossary.



Gurukul Technicals Institute

A-10, Chief Commissioner Colony, opposite Rana Pratap Bagh, Delhi 110007

Phone 011 2721 1512 · Mobile and WhatsApp +91 97116 99511

engineergurukul@yahoo.co.in · engineergurukul.com

Free ebook. You may read, print and share this ebook for learning. It may not be sold or changed.

© 2026 Gurukul Technicals Institute. First edition, October 2026. The information was checked when it was written; software, prices and rules change, so for anything official always check the latest source.

What you will find inside

1	What UPI is and how it works	4
2	Setting up a UPI app safely	5
3	UPI IDs and QR codes	7
4	Paying and receiving: the golden rule	9
5	Cards and net banking basics	11
6	PIN, password and OTP: secrets you never share	13
7	Tricks by phone and message	14
8	Tricks with offers and payments	16
9	If you are cheated: act fast	18
10	Safe online shopping and keeping records	20
11	A family safety checklist	21
	Practice questions	23
	Answers	24
	Glossary	26

What UPI is and how it works

A few years ago, paying a shopkeeper meant counting notes and waiting for change. Today a vegetable seller in Lucknow and a tea stall in Madurai both show a small square code, and customers pay with their phones in seconds. Most of these payments use UPI.

UPI stands for Unified Payments Interface. It is a system that moves money from one bank account to another, straight away, using a phone. It was built by the National Payments Corporation of India (NPCI), the organisation that runs many of the country's payment systems. UPI works at any hour, on every day of the year, including holidays.

How a UPI payment works

When you pay with UPI, money does not sit inside the app. It moves from your bank account to the other person's bank account. The app is only the tool you use to give the order, a bit like a remote control for your bank account.

1. You open a UPI app and choose whom to pay.
2. You type the amount.
3. The app shows the name of the person or shop. You check it.
4. You enter your secret UPI PIN.
5. Your bank takes the money from your account and sends it to the other bank.
6. Both of you get a message within seconds.

The words you will meet

Word	What it means
UPI app	An app on your phone that can send and receive money through UPI
UPI ID	Your payment address, such as <code>ramesh.kumar@abcbank</code>
UPI PIN	A secret 4- or 6-digit number that approves the payments you make

Word	What it means
QR code	A square pattern of dots that holds a payment address
Transaction ID	The reference number of a payment, used to trace it

DID YOU KNOW

You can link more than one bank account to the same UPI app and choose which one to pay from each time. Each account has its own UPI PIN.

Why people like UPI

It is fast. It works for ! 10 for a cup of tea and for a month's rent. You need no exact change, and every payment leaves a record in your bank statement.

The same speed also helps fraudsters. A payment that leaves in two seconds can be very hard to bring back. Most frauds do not break the system. They trick a person into pressing the button themselves.

REMEMBER

The money in UPI is your own bank money. Treat your UPI PIN exactly as you treat your ATM PIN.

CHAPTER 2

Setting up a UPI app safely

Setting up a UPI app takes a few minutes. Doing it carefully protects you for years.

What you need

- A smartphone with internet.
- A bank account.
- The SIM card of the mobile number registered with that bank, inside the same phone. The app checks this by sending an SMS from your phone.
- Your debit card, or, where your bank allows it, Aadhaar-based verification with an OTP.

Step by step

1. Install the app only from the official app store on your phone, such as the Play Store or the App Store. Check the publisher's name. Never install a payment app from a link sent in a message.
2. Open the app and choose your language.
3. Allow it to send the SMS that verifies your mobile number.
4. Choose your bank from the list. The app finds the account linked to your number.
5. Set your UPI PIN. The app asks for some debit card details, or offers Aadhaar verification, and then sends an OTP to your phone.
6. Type the OTP into the app, then choose your UPI PIN and type it again to confirm.
7. Set a screen lock or app lock, if the app offers one.

SAFETY

You set your UPI PIN yourself, inside your own app. A bank officer, a shopkeeper or a "helpful" caller never needs to do it for you, and never needs to know it.

Choosing a good UPI PIN

Poor PIN	Why
1234, 0000, 1111	The first numbers anyone tries
Your birth year	Easy to find from your documents or social media
Your mobile number's last digits	Anyone who has your number knows them
The same as your ATM PIN	One leak opens both

Choose digits that mean nothing to anyone else. Do not write the PIN on the phone cover or in your contacts. If you must note it down while you learn it, keep that paper locked away at home, never with the phone.

Lock your phone

A phone without a screen lock is like a wallet without a zip. Use a PIN, pattern, fingerprint or face lock. If the phone is stolen, the lock buys you time to call your bank and block UPI.

EXAMPLE

Gurpreet, a college student in Ludhiana, installs a UPI app from the Play Store after checking the publisher name. He sets a 6-digit PIN that is not his birth year and adds a fingerprint lock to the app. When his younger cousin borrows the phone to play a game, his payments stay locked.

If you change your number or phone

If you get a new mobile number, update it with your bank first, then set up UPI again. If you sell or give away an old phone, remove your accounts from the UPI apps and reset the phone fully. If your SIM suddenly stops working for no clear reason, call your mobile operator and your bank at once; fraudsters sometimes trick a mobile operator into giving them a duplicate of someone else's SIM, so that the OTPs reach the fraudster.

CHAPTER 3

UPI IDs and QR codes

To pay someone with UPI, your app needs their payment address. There are three common ways to give it: a UPI ID, a QR code, or a mobile number linked to UPI.

UPI IDs

A UPI ID looks a little like an email address: a name, then @, then a short word that stands for the bank or app. For example, `meena.store@abcbank`. Many apps also let people receive money on their mobile number.

Before you approve any payment, the app shows the name registered with that UPI ID. This is the most important screen in the whole payment. Read it.

EXAMPLE

Anjali in Pune wants to pay her tailor, Salim, ₹ 450. She types his UPI ID and the app shows "SALIM KHAN". She checks it matches, enters ₹ 450 and her PIN. If the app had shown some other name, she would have stopped and asked him again.

QR codes

A QR code (Quick Response code) is a square pattern of black and white dots. It holds a payment address and sometimes an amount. You point your UPI app's scanner at it, and the app reads it in a moment.

There are two kinds you will see:

Kind	What it holds	Where you see it
Fixed QR	Only the shop's payment address. You type the amount	Printed on a stand at a shop
QR with an amount	The address and the exact amount to pay	On a bill, a screen at a billing counter, or a website

After you scan, the app shows the name and, if included, the amount. Check both before you enter your PIN.

The one thing a QR code is for

REMEMBER

Scanning a QR code is always for paying. You never scan a QR code to receive money. If anyone sends you a QR code and says "scan this to receive your money", they are trying to take your money.

Tampered QR codes

Fraudsters sometimes paste their own QR sticker over a shop's genuine one. That is why the name on the screen matters. If the shop is "Sharma General Store" and your app shows a completely different name, do not pay. Tell the shopkeeper.

TIP

Shopkeepers, check your QR stand every morning. Make sure no sticker has been stuck on top, and that the name shown when you scan it yourself is your own.

Sharing your own QR code

You can show your own QR code to receive money. Many apps have a "Receive" or "My QR" option. Showing your QR code is safe: it lets others pay you. But it lets them do only that, so there is nothing for you to approve and no PIN to enter.

TRY THIS

Open your UPI app and find your own UPI ID and QR code. Then ask a family member to scan it and send you ! 1. Notice that you did nothing at all to receive it.

CHAPTER 4

Paying and receiving: the golden rule

If you learn only one thing from this book, learn this:

REMEMBER

You enter your UPI PIN only to send money out of your account. You never need a PIN, a QR scan or an "approve" button to receive money.

Almost every UPI fraud breaks this rule. The fraudster convinces you that a PIN, a scan or an approval will bring money in, when it really sends money out. Some apps now let you approve certain payments with a fingerprint or your face instead of typing the PIN. The rule does not change: any approval sends money out.

Paying versus receiving

Question	Paying	Receiving
Who acts	You	The other person
Do you scan a QR?	Yes, theirs	No. They scan yours
Do you enter your PIN?	Yes	Never
Do you approve anything?	Yes	Never
What you share	Nothing	Only your UPI ID, mobile number or QR

How to receive money

1. Give the other person your UPI ID, your UPI mobile number or your QR code.
2. They pay from their app.
3. You get a message from your bank and the app.
4. Check the amount in your own app or bank message.

That is all. If someone says you must "accept", "scan" or "enter PIN" to receive, stop.

Collect requests

A collect request, also called a payment request, is a message inside your UPI app that asks you to pay. Shops, websites and apps use them. For example, when you choose UPI at an online checkout and type your UPI ID, the site sends a request that pops up in your app, and you approve it with your PIN.

That is fine when you started the purchase yourself. It is a trap when the request arrives out of nowhere. Fraudsters have sent requests with notes like "Refund ! 2,000" or "Cashback received". The note can say anything. If you enter your PIN, money leaves your account.

SAFETY

Approve a payment request only when you started the payment yourself, a moment ago, and the name and amount are exactly what you expect. Decline everything else.

Check before you press

Before every payment, take three seconds:

1. **Name.** Is this the person or shop I mean to pay?
2. **Amount.** Is it ! 500, not ! 5,000? Count the zeros.
3. **Reason.** Did I start this payment, or did someone push me into it?

EXAMPLE

Mr Pillai, a retired teacher in Kochi, gets a call: "Sir, you won a cashback of ! 1,500. Please accept the request in your app." A request for ! 1,500 appears. He remembers the golden rule: money coming in needs nothing from him. He declines it and hangs up. His ! 1,500 stays in his account.

If you pay the wrong person

Mistakes happen, such as one wrong digit in a number. Report it at once through the help section of your UPI app and to your bank, with the transaction ID. Getting the money back is not guaranteed, so checking the name before paying is far better than fixing it later.

CHAPTER 5

Cards and net banking basics

UPI is not the only way to pay digitally. Debit cards, credit cards and net banking are also common, and each has its own safety rules.

Debit and credit cards

Point	Debit card	Credit card
Whose money	Your own, straight from your bank account	The bank's, lent to you for a short time
When you pay	At once	Later, when the bill comes
Main risk	Your savings can be taken	Debt grows if you do not pay the full bill on time

A credit card bill must be paid by its due date. If you pay less than the full amount, the bank charges interest on the rest, and the interest can be high. Use a credit card only if you can pay the whole bill every month.

The details on a card

A card has a long card number, an expiry date and the holder's name. Most cards also have a short CVV number (card verification value), usually on the back. Together these details allow online payments, so treat them like cash. For most online card payments in India, your bank also sends an OTP that you must type to finish the payment.

SAFETY

Never share your card number, expiry date, CVV, PIN or OTP with anyone, and never photograph both sides of your card and send it to anyone. No bank needs these over the phone.

Card safety settings

Most bank apps let you control your card: switch online payments on or off, switch international use on or off, set limits, or block the card in seconds if it is lost. Keep online and international use switched off if you never use them.

Under rules set by the Reserve Bank of India, shopping sites in India no longer keep your full card number. When you save a card on a site, it keeps a token, a stand-in code that works only on that site.

At the ATM

- Cover the keypad with your other hand while typing your PIN.
- Do not accept help from strangers, however polite.
- Look at the card slot. If anything looks loose or stuck on, use another machine.
- Take your card and receipt before you walk away.

Net banking

Net banking means using your bank account on its website or official app: checking your balance, paying bills, transferring money.

1. Use the bank's official app, or type the bank's website address yourself. Never sign in through a link in a message or email.
2. Look at the address bar carefully. Fake sites copy the look of real ones.
3. Type your user ID and password, and the OTP when asked.
4. Log out when you finish, especially on a shared computer.

DID YOU KNOW

A padlock symbol next to a website address only means the connection is scrambled so others cannot read it. Fake websites can have a padlock too. The padlock does not prove a site is genuine; the exact address does.

PIN, password and OTP: secrets you never share

Every digital payment is protected by a secret: a UPI PIN, an ATM PIN, a net banking password or an OTP. Fraudsters cannot easily break these, so they try something easier. They ask you.

Who knows your secrets

Secret	Who should know it
UPI PIN	Only you
ATM or card PIN	Only you
Net banking password	Only you
OTP	Only you, and only for a payment you are making right now
CVV	Only you, and only typed into a payment page you opened yourself

No one else is on this list. Not your bank, not the police, not a delivery person, not a "customer care" officer, not a relative on the phone whose voice sounds a little strange.

REMEMBER

Your bank already knows everything it needs about your account. It never has a reason to ask you for your PIN, password, OTP or CVV.

Read the OTP message

An OTP message usually tells you what the code is for. Read the whole message, not just the number. It may say something like "OTP for payment of ₹ 9,999 to XYZ Merchant". If you are not making that payment, someone else is trying to, using your details. Do not share the code. Call your bank.

EXAMPLE

Rekha in Jaipur is told by a caller that her "reward points" are expiring and that she will get a code to "redeem" them. The SMS arrives, and she reads it fully: it is an OTP to add her card to a payment app. She tells the caller nothing and calls the number on the back of her card. The bank blocks the card and sends her a new one.

Clever ways they ask

Fraudsters rarely say "Tell me your OTP." They say:

- "Just read me the code to confirm your identity."
- "Type your PIN to check your balance for the refund."
- "Forward the SMS you just received to this number."
- "Install this app so I can help you faster."

Each of these hands them your secret.

When a stranger pushes you

Fraudsters create pressure: "Your account will be blocked in ten minutes", "Your son is in trouble", "This offer ends today". Pressure is there to stop you thinking. A genuine bank or office gives you time and lets you call back on an official number.

TIP

Make a family rule: whenever a call asks for money or a code, hang up and call back on a number you already know, such as the one on your card or in your passbook. Real problems survive a five-minute pause. Frauds do not.

CHAPTER 7

Tricks by phone and message

Most frauds begin with a call, an SMS or a chat message. The stories change every year, but the tricks stay the same, so learning the patterns helps you spot new versions too.

Fake customer care

Someone searches online for a company's helpline, for example to complain about a failed payment. Sometimes the number they find belongs to a fraudster, placed there on purpose. The "agent" sounds helpful and then asks for an OTP, a PIN or an app install.

Take helpline numbers only from the back of your card, your passbook, the official app, or the company's own website typed in yourself.

Screen-sharing apps

The caller asks you to install an app "so we can fix your problem". Some apps let another person see or control your screen. Once installed, the fraudster can watch you type your PIN and read your OTPs as they arrive.

SAFETY

Never install any app because a caller asked you to. If an app asks for permission to share or record your screen during a call with a stranger, close it at once.

"Update your KYC"

KYC means Know Your Customer: the identity checks banks must do. Fraudsters send messages like "Your account will be blocked today, update KYC" with a link or a number. The link opens a fake page that collects your details. Banks do ask for KYC updates sometimes, but you can do them at your branch or through the bank's official app, never through a link from a stranger.

Fake refunds and bill threats

"Your electricity will be cut tonight, call this officer." "Your parcel is held, pay ! 25 to release it." "You are owed a refund, scan this to receive it." Each one uses fear or a small amount to get you to click, pay or share an OTP. Check with the company yourself, using a number you already know.

"Digital arrest"

In this frightening trick, a video caller dressed as a police, customs or investigation officer says you are linked to a crime. They say you are under "digital arrest", must stay on the call, and must transfer money to "clear your name". There is no such thing as digital arrest. Real officers do not arrest people on video calls or ask for money to close a case.

EXAMPLE

Mrs Banerjee, 68, in Kolkata, gets a video call from a "police officer" in uniform who says a parcel in her name holds illegal goods and that she must tell no one. Scared, she still remembers her grandson's warning. She ends the call, phones her son, and together they report the number on 1930.

DID YOU KNOW

You can report suspected fraud calls and messages to the Department of Telecommunications through its Sanchar Saathi service, which helps them track and block numbers used for fraud.

CHAPTER 8

Tricks with offers and payments

The second family of frauds uses greed or kindness instead of fear. They promise something good, or they play on your wish to be honest.

Lotteries and prizes

"Congratulations! You have won ! 25 lakh in a lucky draw. Pay ! 8,500 processing fee to receive it." If you did not buy a ticket, you did not win. Even when the prize seems real, a genuine prize never needs you to pay first.

Job and task offers

"Earn ! 3,000 a day from home. Just like videos and review hotels." At first the fraudsters pay small amounts to win your trust. Then they ask you to "invest" to unlock bigger tasks, and the money never comes back. Other fake jobs ask for a registration or training fee. A genuine employer pays you; it does not charge you to be hired.

Investment groups

Chat groups promise to double money in weeks, with screenshots of huge "profits". Some send you to a trading app that shows rising numbers but never lets you withdraw.

REMEMBER

If someone asks you to pay money in order to receive money, it is a fraud. Prize fees, job fees and "unlock" payments all follow this pattern.

Selling something online

You put an old cooler on a selling website. A "buyer" agrees at once without bargaining. They say they will pay, then send a QR code or a payment request and ask you to "scan to receive" or "enter PIN to accept". This is the golden rule again: receiving needs nothing from you.

Fake payment proof (for shopkeepers)

A customer shows a screen saying "Payment successful" and walks off. But the screen was a fake app or an old screenshot. Or someone sends a fake SMS saying "₹ 5,000 credited" and calls: "I sent extra by mistake, please return it."

TIP

Shopkeepers, trust only your own app, your bank SMS from the bank's official sender, or your payment sound box. Never trust the customer's screen. Before "returning" any money, check your actual balance.

Lending your account

Some people are offered a commission to let others receive and send money through their bank account or UPI. This makes them a money mule: someone whose account carries stolen money. It is a crime, the account can be frozen, and the account holder can face police action. Never let anyone use your account, however small the favour.

EXAMPLE

Deepak, a first-year student in Bhopal, is offered ₹ 2,000 a week to "receive company payments" in his account and forward them. He asks his teacher, who explains the money is likely stolen. Deepak refuses and blocks the number.

CHAPTER 9

If you are cheated: act fast

Even careful people get cheated; anyone can be caught on a tired or worried day. If it happens to you, do not feel ashamed and do not wait. Speed matters more than anything, because stolen money moves quickly from one account to another.

The first steps

1. **Call your bank at once.** Use the number on your card, in your passbook or in the official app. Ask them to block your card, UPI and net banking if needed, and to record the fraud.
2. **Call 1930.** This is the national cyber crime helpline. Report the transaction details.
3. **Report on cybercrime.gov.in.** This is the national cyber crime reporting portal. File a complaint with all the details.
4. **Change passwords and PINs** that may be known to the fraudster, from your own phone.
5. **Remove any app** a caller asked you to install.

SAFETY

Call 1930 and your bank first. Write things down afterwards. Every minute you wait gives the fraudster time to move the money further.

Collect your evidence

Keep everything; do not delete any messages or call records, even if you feel embarrassed.

Keep this	Why
Transaction ID or reference number	To trace the payment
Date, time and amount	To match the bank's records
The fraudster's phone number, UPI ID or account	To report and block them
Screenshots of chats, messages and the payment	Proof of what happened
Your complaint numbers from the bank and 1930	To follow up later

After the first day

Follow up with your bank in writing and keep the complaint number. Rules from the Reserve Bank of India generally protect customers better when they report an unauthorised transaction quickly, which is another reason to call at once. If your bank does not resolve your complaint, you can approach the Reserve Bank of India's ombudsman scheme, which handles customers' complaints against banks. You may also be asked to file a complaint at your local police station; take your evidence with you.

Beware the second trick

After a fraud, some victims get calls from "recovery agents" or "cyber officers" who promise to get the money back for a fee. These are frauds too. Genuine police and banks do not charge you to recover stolen money.

EXAMPLE

Sana in Hyderabad shares an OTP with a fake customer care agent and loses ₹ 12,000. Within ten minutes she calls her bank and blocks her card, then calls 1930. She reports it on cybercrime.gov.in with screenshots and the transaction ID. Acting fast gives the best chance of the money being stopped before it disappears, though recovery is never guaranteed.

Safe online shopping and keeping records

Online shopping lets you compare prices, read reviews and get things delivered to your door. A few habits keep it safe.

Choosing where to shop

- Buy from well-known shopping apps, or a brand's own official website or app.
- Be careful with advertisements on social media that lead to unknown stores. Many are fake shops that never deliver.
- Check the website address carefully. Fake sites use names that are one letter different from real ones.
- If the price is far below what everyone else charges, ask why. A new phone at a fifth of its price is bait.
- Read the return and refund policy before you buy.

TIP

For a seller you do not know well, choose cash on delivery or pay on delivery if it is offered. You pay only when the parcel arrives, which protects you from shops that never deliver.

Paying online

1. Pay only on the checkout page of the site you opened yourself.
2. Check that the amount is right before you approve.
3. Type the OTP only when the message matches this purchase.
4. Never pay an "advance" to a seller who contacts you on a chat app.
5. Keep the order confirmation and invoice.

Refunds

A genuine refund comes back by itself, usually to the account or card you paid from. You do not need to scan anything, share an OTP or enter a PIN. If a refund is late, check the order page in the official app or contact the seller through it.

EXAMPLE

Ritu in Chandigarh orders a school bag for ₹ 899 and returns it. Two days later, a caller says, "Madam, to get your refund, scan this QR code." She knows refunds come back on their own. She hangs up, checks the official app, and sees the refund is already on its way.

Keeping records

Good records help you spot fraud early and prove a payment when needed.

Record	How to keep it
SMS alerts	Keep them switched on for every account and card
Bank statements	Download or collect them every month and read them
Payment receipts	Save screenshots of important payments with the transaction ID
Invoices	Keep the bills from online shopping in one folder
Big payments	Note the date, amount, purpose and transaction ID in a notebook

TRY THIS

Open your bank statement for last month. Can you recognise every payment on it? Mark anything you do not understand and ask your bank about it.

Read your statement

Once a month, tick every line of your statement that you recognise. A small unknown payment of ₹ 1 or ₹ 10 can be a fraudster testing whether your details work. Report anything you do not recognise straight away.

CHAPTER 11

A family safety checklist

Digital payments are safest when the whole family follows the same simple rules. Elders new to phones, teenagers who shop online and family members who run a shop each face different risks. This chapter brings the book's rules together.

The ten family rules

No.	Rule
1	Never share a PIN, password, OTP or CVV with anyone.
2	A PIN, a QR scan or an approval is only ever for paying. Receiving needs nothing.
3	Check the name and amount on the screen before every payment.
4	Take helpline numbers only from your card, passbook or official app.
5	Never install an app because a caller asked you to.
6	Never click links in messages about KYC, prizes, refunds or blocked accounts.
7	If anyone asks you to pay to receive money, it is a fraud.
8	Hang up and call back on a known number when a call creates panic.
9	Never let anyone use your bank account or UPI for their payments.
10	If cheated, call your bank and 1930 at once, then report on cybercrime.gov.in .

TRY THIS

Copy these ten rules on a sheet of paper and stick it where the family keeps its phones.

For elders

- Keep the bank's number and 1930 written on a card in your wallet.
- Agree on a family code word. If a caller claims to be a grandchild in trouble, ask for the word.
- Before paying anyone new, call a trusted family member.
- Keep a simple screen lock you can remember, but not your birth year.

For students and young people

- Do not share your parents' card details with games or apps.
- Fake job and task offers target students. Never pay to get a job.
- Never lend your account or UPI to friends of friends.

For shopkeepers

- Check the QR stand every morning.
- Confirm every payment on your own app or sound box.
- Never "return" an extra payment until you see it in your actual balance.

REMEMBER

You do not have to understand every new trick. If you follow these ten rules, almost every trick fails, because nearly all of them need you to break at least one.

EXAMPLE

The Reddy family in Visakhapatnam keeps the ten rules on their fridge. When Grandfather gets a "KYC update" SMS, he does not click. He shows it to his granddaughter, and they delete it together. The rules turn a moment of worry into a five-second decision.

CHECK YOURSELF

Practice questions

1. What does UPI stand for, and who built it?
2. Where does the money in a UPI payment actually come from?
3. Why should you install a UPI app only from the official app store?
4. Give two examples of a poor UPI PIN, and say why each is poor.
5. Which screen in a UPI payment is the most important to read, and why?
6. What is a QR code used for in UPI?
7. A buyer sends you a QR code and says, "Scan this to receive your payment." What is happening?
8. State the golden rule of receiving money.
9. What is a collect request, and when is it safe to approve one?
10. What three things should you check before every payment?

11. What is the difference between a debit card and a credit card?
12. What is a CVV, and who should know it?
13. Does a padlock next to a website address prove that the site is genuine? Explain.
14. Who should know your UPI PIN and your OTP?
15. Why should you read the whole OTP message, not just the number?
16. A caller asks you to install an app so they can "help you faster". What should you do, and why?
17. What is "digital arrest", and is it real?
18. A message says you have won ! 25 lakh but must pay a fee first. Is it genuine? Explain.
19. What is a money mule, and why is it dangerous to become one?
20. A shopkeeper is shown a "Payment successful" screen. How should the shopkeeper check?
21. You have just lost money to a fraudster. List the first three things you should do.
22. Why should you keep screenshots and the transaction ID after a fraud?
23. A caller offers to recover your stolen money for a fee. What should you do?
24. How does a genuine refund from a shopping site reach you?

ANSWER KEY

Answers

- | | |
|---|---|
| 1. Unified Payments Interface. It was built by the National Payments Corporation of India (NPCI). | 3. Fake apps sent through links can steal your details. The official store, with the publisher's name checked, is far safer. |
| 2. From your own bank account. The app only carries your instruction to the bank. | 4. Any two, for example: 1234, the first number anyone tries; your birth year, which is easy to find; the same as your ATM PIN, so one leak opens both. |

5. The screen showing the receiver's name, because it tells you whether the money is going to the person or shop you mean to pay.
6. Only for paying. You scan someone else's QR code to send them money.
7. It is a fraud. Scanning a QR code and entering your PIN would send money from your account to the "buyer".
8. You enter your PIN, scan a QR or approve a request only to send money. Receiving money needs none of these.
9. A message in your UPI app asking you to pay. Approve it only if you started that payment yourself a moment ago and the name and amount are exactly right.
10. The name of the receiver, the amount, and whether you started the payment yourself.
11. A debit card spends your own money at once. A credit card spends the bank's money, which you repay later; unpaid amounts attract interest.
12. A short code, usually on the back of a card, used for online payments. Only you should know it, and you type it only into a payment page you opened yourself.
13. No. It only means the connection is scrambled. Fake sites can have a padlock; check the exact address.
14. Only you. An OTP is for a payment you are making yourself, right now.
15. The message says what the code is for, such as a payment to a named merchant. If you are not making that payment, someone else is using your details.
16. Refuse and end the call. Some apps let another person see or control your screen, so they could watch your PIN and read your OTPs.
17. A trick in which fake officers on a video call claim you are under arrest and must pay. It is not real; officers do not arrest people on video calls or ask for money.
18. No. You cannot win a draw you never entered, and a genuine prize never needs you to pay first.
19. A person whose account is used to move stolen money. It is a crime, the account can be frozen, and the person can face police action.
20. By checking the shopkeeper's own app, bank SMS or payment sound box, never the customer's screen.
21. Call your bank to block your card or UPI, call 1930, and report on cybercrime.gov.in.
22. They help the bank and police trace the money and prove what happened.
23. Refuse. It is another fraud; genuine police and banks do not charge to recover stolen money.
24. It comes back by itself, usually to the account or card you paid from. You never need to scan, approve or share an OTP to get it.

Glossary

ATM PIN

the secret number you type to use your debit card at a cash machine.

Collect request

a message in a UPI app asking you to pay; approving it sends money out.

Credit card

a card that lets you spend the bank's money now and repay it later.

CVV

card verification value, the short code on a card used for online payments.

Debit card

a card that spends money straight from your own bank account.

Digital arrest

a fraud in which fake officers on a video call demand money; there is no such arrest.

KYC

Know Your Customer, the identity checks a bank must carry out.

Money mule

a person whose bank account is used to move stolen money.

Net banking

using your bank account through the bank's website or official app.

NPCI

National Payments Corporation of India, the organisation that runs UPI.

OTP

one-time password, a short code that approves one action and expires in minutes.

Phishing

a fake message or website made to steal your secrets.

QR code

a square pattern of dots that holds a payment address, and sometimes an amount.

Screen-sharing app

an app that lets another person see or control your phone's screen.

Token

a stand-in code a shopping site keeps instead of your real card number.

Transaction ID

the reference number of a payment, used to trace it.

UPI

Unified Payments Interface, a system for instant bank-to-bank payments by phone.

UPI ID

your payment address, written as a name, the @ sign and a short bank or app word.

UPI PIN

the secret 4- or 6-digit number that approves the UPI payments you make.

1930

the national cyber crime helpline number for reporting online fraud.



Gurukul Technicals Institute

Computer education institute in Delhi, with authorised member centres, robotics classes and science projects, working models and DIY kits.

COURSES

Computer & Office Skills · Accounting & Business Software · Programming & Web Development · Design & Digital Skills · Hardware & Networking · Robotics & Coding · Other Programmes

PROJECTS AND KITS

Ready-made school projects · DIY and STEM kits · Robotics and coding · Components and spares · Engineering projects

CONTACT

Head office: A-10, Chief Commissioner Colony, opposite Rana Pratap Bagh, Delhi 110007

Phone: 011 2721 1512 · **Mobile and WhatsApp:** +91 97116 99511

Email: engineergurukul@yahoo.co.in

Website: engineergurukul.com · **Instagram:** [@science_projects_club](https://www.instagram.com/science_projects_club)

More free ebooks for computer courses, robotics and science projects: engineergurukul.com/resources/ebooks/

Free to read, print and share. Not for sale.