SBI
The banker to every Indian

INFORMATION SECURITY DEPARTMENT

Information security awareness

with tales of

SBI

The banker to every Indian

Dear Customers,

I hope this message finds you well. I want to take a moment to highlight the issue of cyber risk that has become increasingly relevant in today's digital age and the steps we are taking to protect your information and ensure your trust in our services.

As we all know, the world is becoming more interconnected, and we rely on digital platforms for everything from working, banking to shopping and socializing. While digital transformation has changed the way banking services are delivered with tremendous convenience and efficiency, it has opened the door to new types of risks which can impact not just organisations, but also individuals.

Cyber fraud is one of the most pervasive and growing threats in the world today. Cybercriminals are becoming more sophisticated in their methods, using various tactics such as phishing, identity theft, ransomware etc, besides creation of fake websites to steal personal information and money.

I want to assure you that cyber security is our top priority and as a responsible banking organisation, we are committed to take every possible measure to protect your personal information and prevent cyber fraud. We continually invest in the state of art cyber security technologies and protocols, work with expert security teams, and comply with industry standards and best practices to ensure that your data remains safe and secure.

In the cyber ecosystem, the human is the weakest link and awareness/alertness about current cyber fraud scenarios creates first layer of protection for individual and organisation. Further, cyber security is a shared responsibility. We want to empower you with knowledge and are committed to provide awareness through various means.

This booklet is designed to create a base level awareness about best cyber practices, which is useful in safeguarding your personal information and guide you to protect against cyber frauds. The actions you take to protect yourself online are just as critical to your safety as the measures we put in place. We request that you remain vigilant and continue to adopt safe practices, to help us build a cyber safe environment for everyone.
Thank you for your trust, your partnership, and your contribution in cyber security.

Stay alert and #StaySafeWithSBI.

With regards,
Baldev Prakash
Deputy Managing Director & Group Chief Risk Officer,
State Bank of India

Cybersecurity isn't a product,
it's a practice

Dear Customers,

I am delighted to share my views on information security awareness. In today's world of technology and digitalisation, the importance of safeguarding our information cannot be overstated. Whether we are at office, working remotely, or even on the move, we are constantly interacting with systems and data that requires vigilance and caution.

Our digital footprint continues to grow every day across email, social media, websites, and internal systems. This brings about significant benefits, but it also opens new avenues for threats. From cyberattacks to data breaches, the risks to organisations and personal information are ever-present.

Information security awareness is the first line of defense and informed citizens play a crucial role in cyber safe ecosystem. This is not just a one-off exercise or a set of rules to follow. It is about creating a mindset, an attitude against cyber threat, and an understanding that cyber security is everyone's responsibility. We don't have to be an expert to make a difference. It's about being vigilant, being proactive, and knowing when to ask for help. Security is not a destination it's an ongoing journey.

I also take this opportunity to provide some insight on current cyber frauds and prevention measures through the, 'booklet on best cyber practices'.

I encourage you all to spare some time to read the best practices mentioned in the booklet with an open mind and a readiness to learn. This will not only prevent cyber frauds but also create a mindset to take a conscious action while performing online tasks.

Be alert, stay safe.

With regards,
Murlidhar Nambiar
Group Chief Information Security Officer
State Bank of India

Table of content

What is information security and why is it important

Information security (InfoSec) protects personal, financial, and sensitive data from unauthorised access or theft.

It is based on 3 key principles:

Confidentiality
Ensuring only the right people can access information.

Integrity
Ensuring data is not tampered with or altered.

Availability
Ensuring authorised users can access data when needed.

Understanding information security

In today's digital world, protecting information ensures privacy, trust, continuity and security.

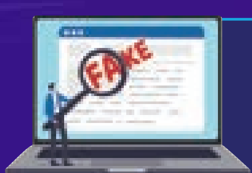
Key points

- Prevents unauthorised access and data breaches
- Protects personal and financial information
- Maintains customer trust and reputation
- Ensures system and data availability for smooth operations
- Reduces financial losses and legal risks

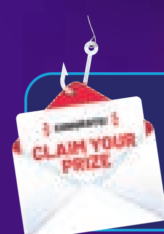
How are cyber fraudsters using technology to cheat victims

Cyber fraudsters now use advanced technology to identify, target and deceive victims. They exploit social media, messaging apps, websites and spoof caller ids to appear legit. Tools like deepfakes, phishing emails and fake payment gateways play on fear, urgency, or greed to steal personal information or money.

What are their modus operandi



Creating fake websites that mimic banking, shopping or travel portals

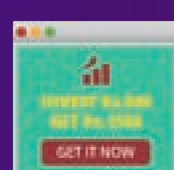


Sending phishing emails and messages posing as trusted institutions

Using spoof caller ids to impersonate banks or officials

Promoting fake investment schemes or urgent fund transfer requests

Spreading malware through malicious links or apps to steal data



Running scam ads on social media with unbelievable deals

What sensitive data are you providing and how are they using it against you

Sensitive information victims unknowingly share includes:

- **Personal details such as full name, address, date of birth.**
- **Banking information including account numbers, credit card details, and PINs.**
- **Identity documents like Aadhaar card numbers, PAN cards, or passport scans.**
- **Login credentials for emails, bank accounts, and social media profiles.**
- **OTPs (One-Time Passwords) shared over calls or messages.**

Fraudsters use this data to:

- Sell personal data on the dark web for more targeted attacks
- Impersonate the victim to scam friends, family, or colleagues
- Conduct financial fraud and drain bank accounts
- Apply for loans or credit cards in the victim's name
- Take over social media accounts for further scams

Meet our characters

Masoom

Masoom is a curious and a trusting individual. He loves exploring new things but often acts without verifying facts. This makes him vulnerable to online scams and frauds.

Samajhdaar

Samajhdaar is a knowledgeable and a cautious person. He always double-checks before taking any action and help others to stay safe from cyber frauds. He believes in, 'Think before you act!'

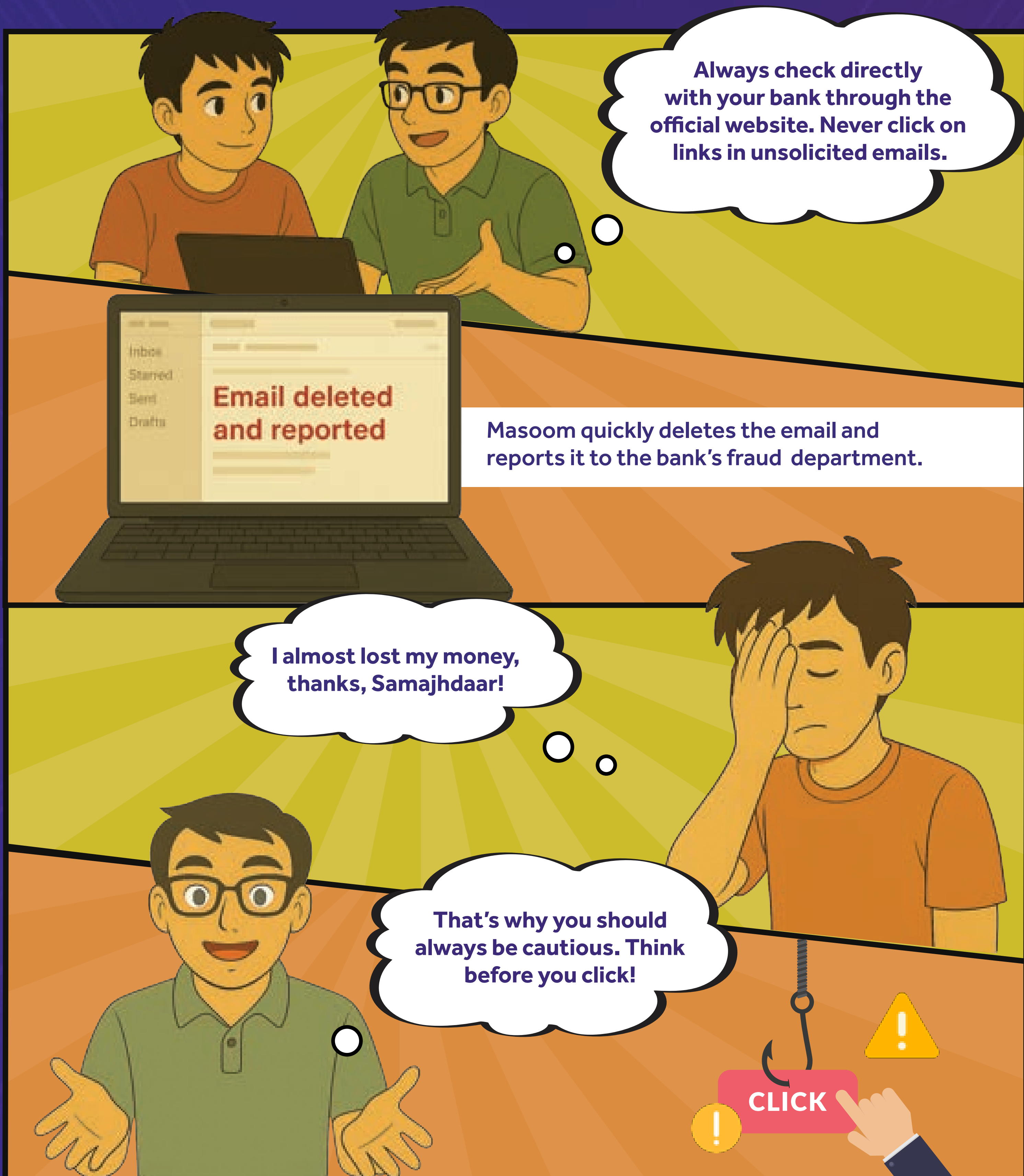
Category 1

Fraudulent offers or deceptive promises

1 Email scam

He starts filling in his personal details, including his bank account number and OTP.

Masoom, stop! Did you verify whether this email is real?
It has the bank's logo and looks official. Why would it be fake?
Scammers can create fake emails that look real! Let's check the sender's email address.
New Mail
From loan-offers@bank-secure.xyz
Exclusive Limited Loan Offer
Limited Special Loan Offer
Reply
Oh no, this isn't from the bank!


Always check directly with your bank through the official website. Never click on links in unsolicited emails.
Inbox
Starred
Sent
Drafts
Email deleted and reported
Masoom quickly deletes the email and reports it to the bank's fraud department.
I almost lost my money, thanks, Samajhdaar!
That's why you should always be cautious. Think before you click!
CLICK

2 Fake lottery scam

3 Reward point scam

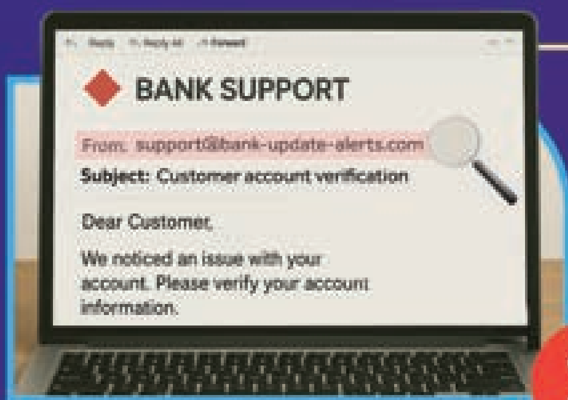
4 Fake investment scam

5 Jumped deposit scam

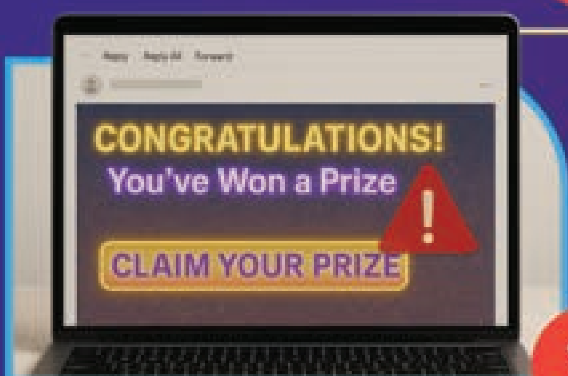

Masoom! Wait! Did you check the amount you're sending?
It's ₹ 5,000, right? That's what he said he sent.
Check again. That UPI request is for ₹ 50,000! This is a Jumped deposit scam.
What?! But he only sent ₹ 5,000!
₹5000 Deposited
Exactly. They send a small amount to build trust, then trick you into approving a huge payment request.
They check the UPI ID of the deposit it's from an unknown number.
Always verify before sending money. And never respond to suspicious payment requests.
Thank you! I almost lost ₹ 50,000!
Report this to your bank immediately.

Advisory

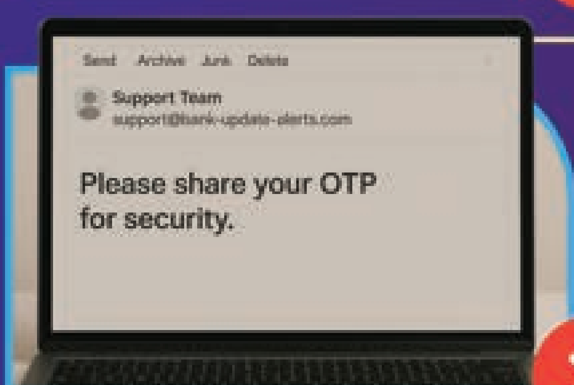
Masoom, email scams may look harmless but one wrong click can lead to big trouble. Let me show you how to spot them and stay safe, step by step.



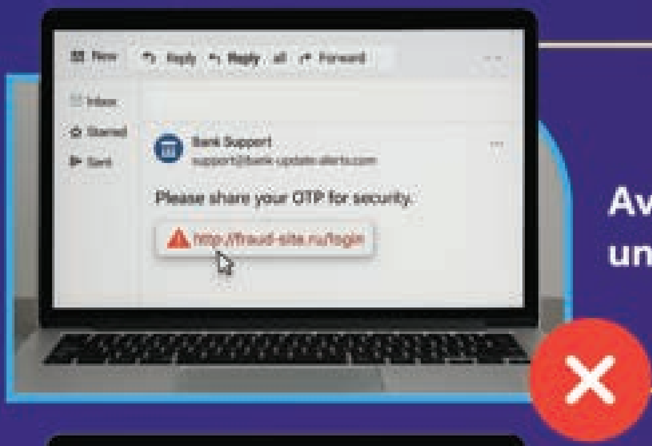
Always check the sender's full email id not just the logo



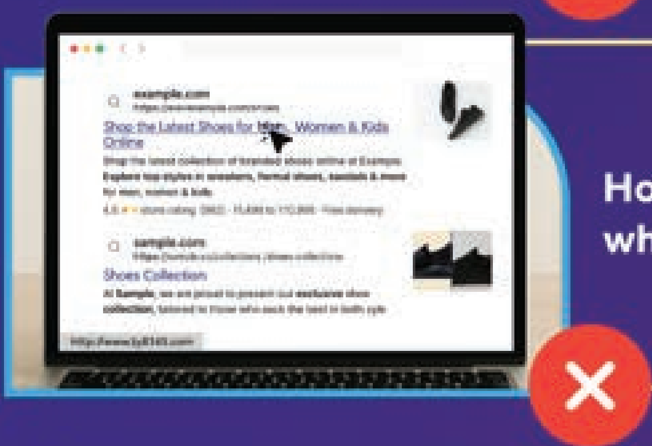
Don't trust flashy email designs they could be fake



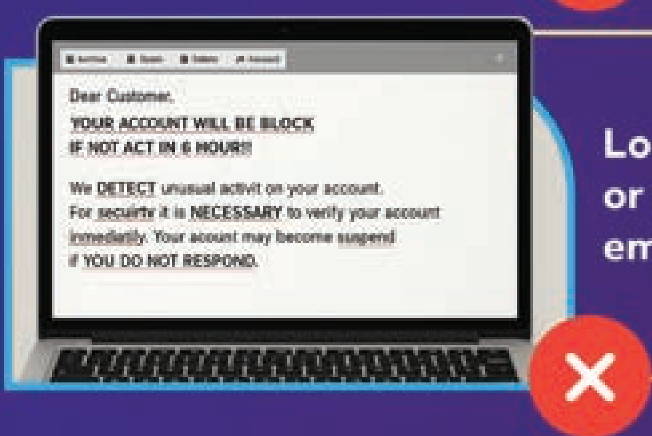
Never share OTPs, passwords, or bank details over email



Avoid clicking on links in unsolicited emails



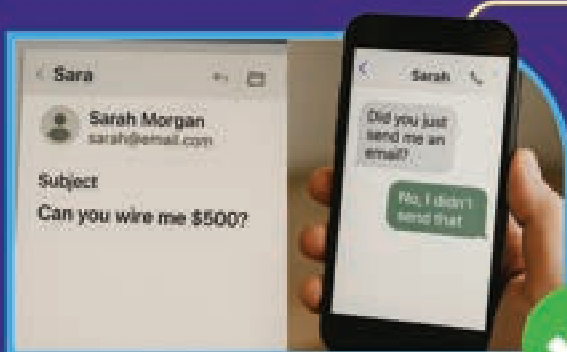
Hover over links to see where they actually lead



Look out for poor grammar or urgent language in email

Report suspicious emails to your provider or IT team

Use spam filters and keep antivirus software updated



Double-check unexpected emails from unknown contacts

Stay alert. One thoughtful second can stop a scam.Think before you click.

Category 2

Identity and personal information theft

1 The KYC update scam


And where did you receive the message from?
On WhatsApp! Look, it even has a bank logo.
Masoom, banks never send KYC update links through WhatsApp or SMS. This looks like a scam!
But what if it's real?
Let's check the proper way. Open the official bank website and see if there's any KYC update notice.
ACB BANK
Masoom searches the bank's official website but finds nothing about urgent KYC updates.
Now, call the bank's customer care number from their official website and ask them directly.
Masoom dials the number and speaks with a bank representative.


Sir, this is a scam. We never send KYC update links via WhatsApp or SMS. Please do not click on such links.
Thank you! I almost fell for it.
Wow, I didn't know scammers could make messages look so real!
That's why you should always verify first. Now, delete the message, block the number, and report it on cybercrime.gov.in.
Thanks, Samajhdaar! You just saved me from a huge scam.
That's what friends are for. Always think before you click!

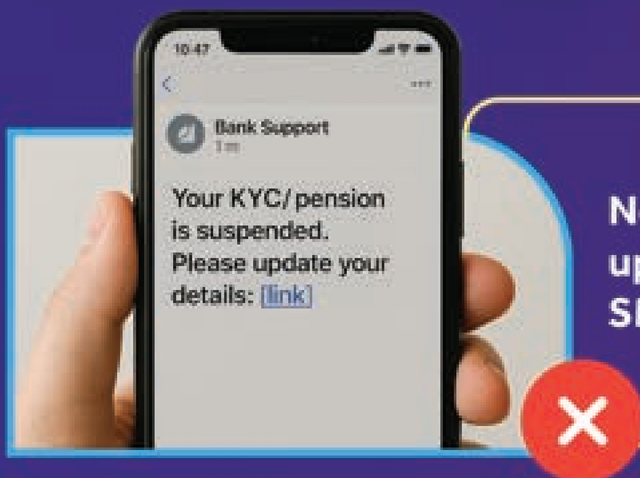
2 Online PPO generation scam

3 IT return frauds

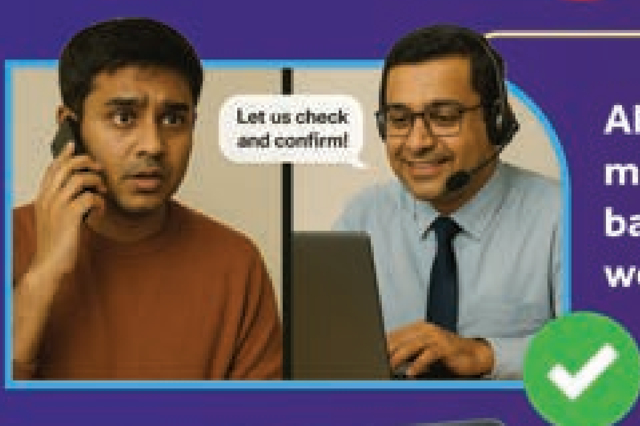

Oh no... I almost gave away all my information!
He immediately closes the tab, deletes the message, and reports the scam on cybercrime.gov.in.
1930
cybercrime.gov.in
Scammers use fake refund bait to steal your identity. Never trust random messages always verify.
Thanks again, Samajdaar. You saved me...again!
That's why I'm here. Think smart, stay safe.

Advisory

Masoom, scammers often try to steal your identity using fake messages and calls. But with a little awareness, you can keep your personal information safe. Let me show you how.

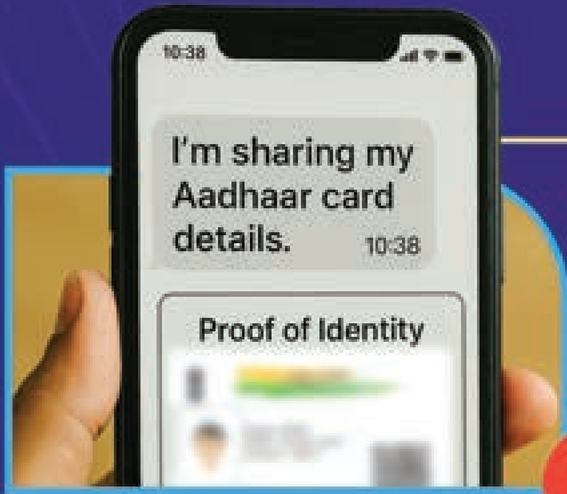


Never trust KYC or pension update messages sent via SMS or WhatsApp

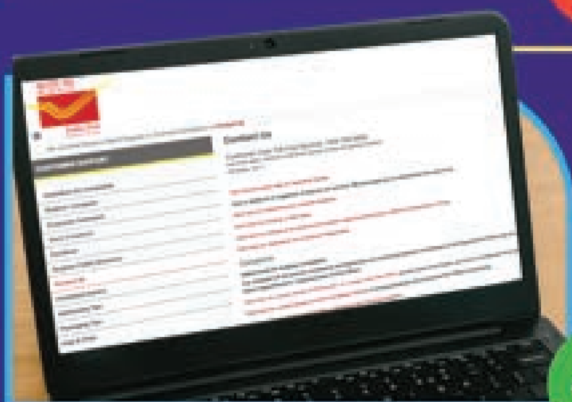


Always verify such messages using the official bank or government website

Don't click on unknown links or download suspicious apps



Never share Aadhaar, PAN, account numbers, or OTPs with unknown sources



Always use customer care numbers from official websites

Always verify on the official Income Tax Department portal before trusting any income tax refund messages

When it comes to your personal data, always pause, verify, and think before you click or share. Your caution is your best defence.

1 The voice cloning scam

Category 3

Impersonation and social engineering


Scammers now use AI to clone voices. They take samples from social media videos or calls and make fake distress calls that sound just like our loved ones.
Before you send any money, let's call Raj directly using the number saved in your contacts.
RAJ
Masoom calls Raj on his regular number.
Hey Masoom! What's up?
Wait... weren't you in an accident?
No, I'm perfectly fine. Why?
I just got a call that sounded exactly like you, asking for money.
That's a voice cloning scam. Good thing we verified first.


I can't believe how real the voice sounded!
Scammers are using AI to mimic voices and exploit emotions. Always verify, especially when there's urgency involved.
You're right. I almost got tricked because I trusted the voice.
Next time, pause, verify, and never send money without double-checking.
Thanks again, Samajhdaar. You saved me... again!
That's why I'm here. Think smart, stay safe.

2 The deepfake scam

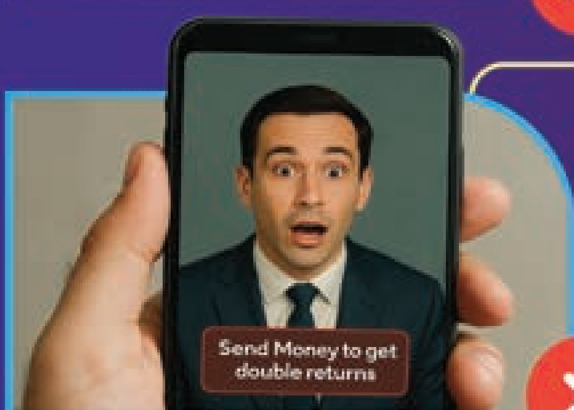
3 Digital arrest scam

Advisory

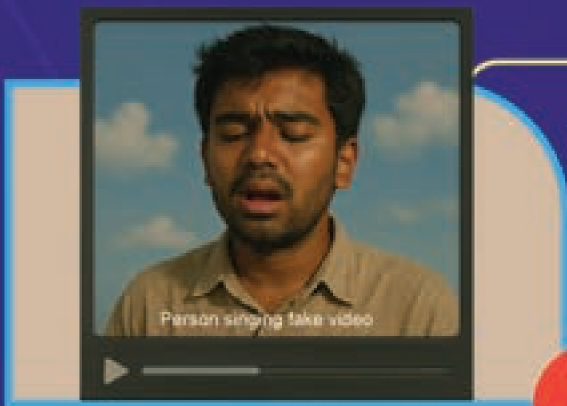
Masoom, scammers can now copy voices, faces, and even emotions to trick you. But don't worry here's how you can stay one step ahead.

Never send money just because a familiar voice asks urgently always verify with a direct call

Don't fall for emotional blackmail or emergency UPI requests without confirmation

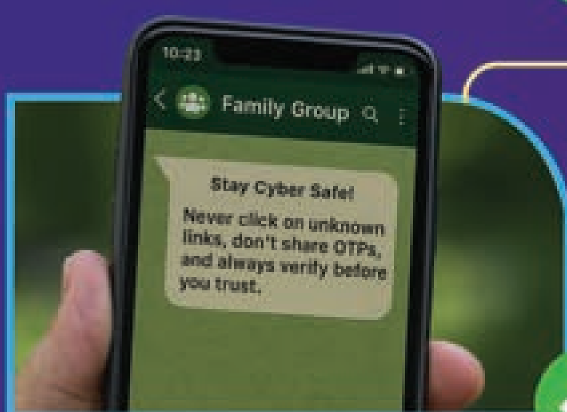


Treat all money-request videos with suspicion even if they look real



Be aware that AI deepfakes and voice clones can mimic loved ones or seniors at work

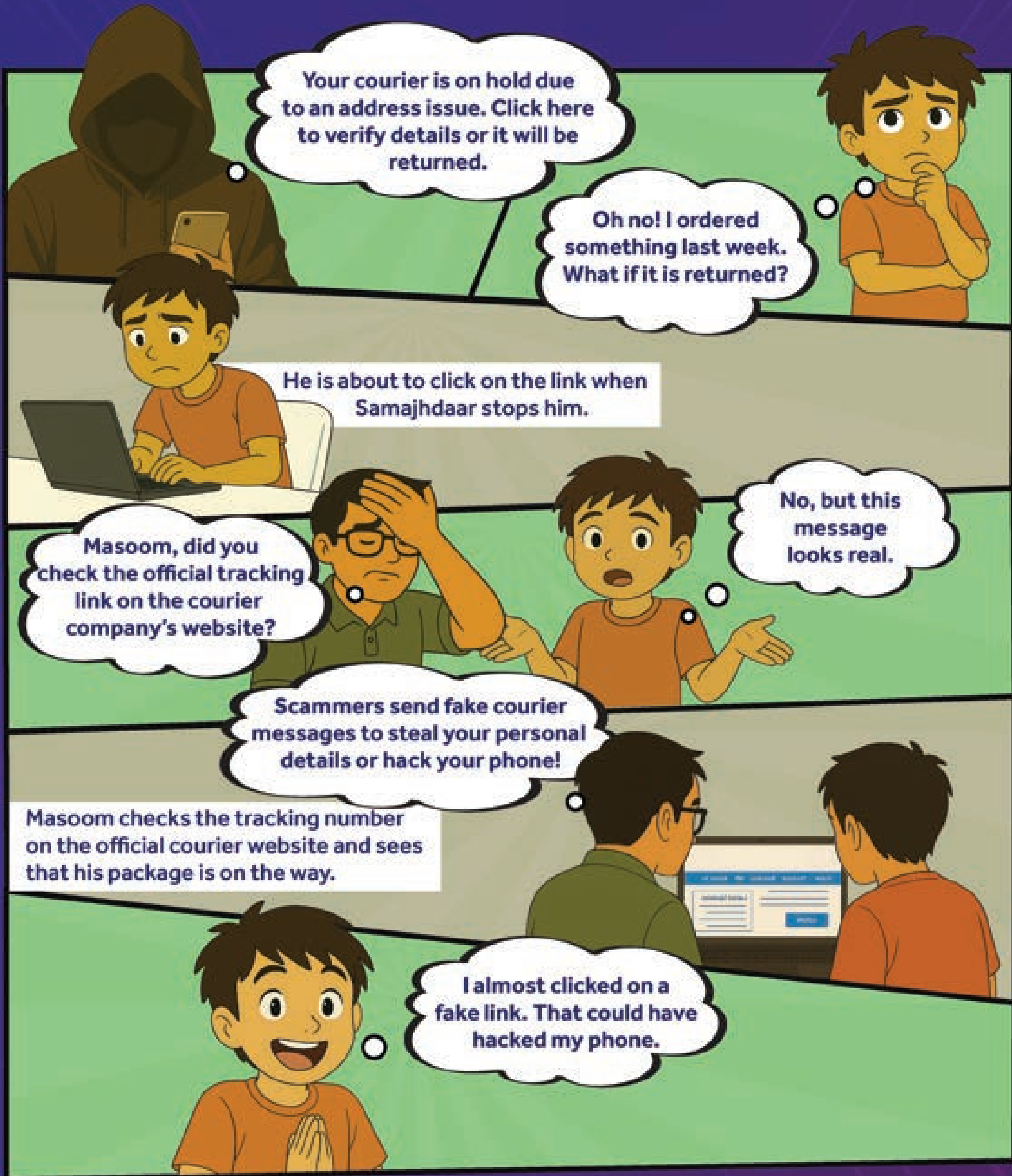
If someone threatens legal action or arrest, stay calm and call official helpline



Don't let urgency override judgment and alert your family about such scams

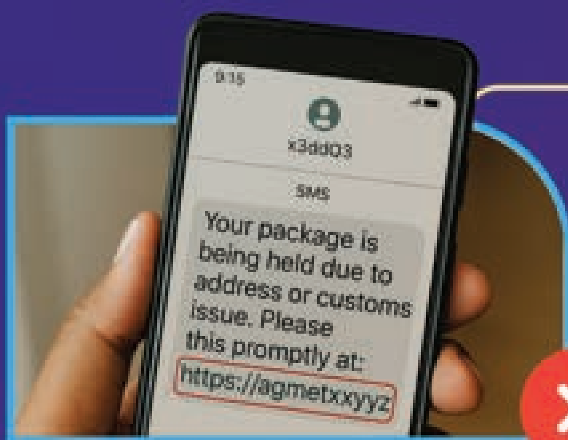
Never trust urgency, trust verification. If it feels rushed, it's probably a scam.

1 Courier/shipment scam

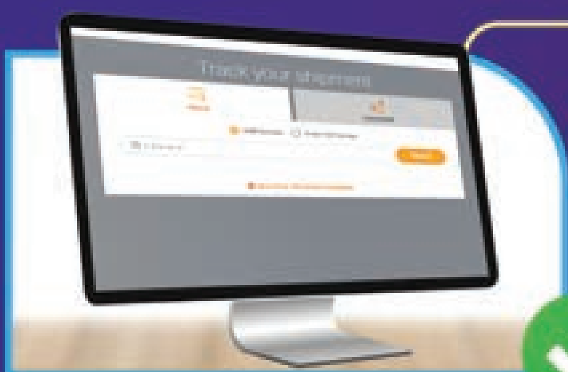


Advisory

Masoom, fake courier and customs scams are getting more common. But with the right precautions, you can protect yourself easily. Here's what to remember.



Don't click on links from SMS or emails claiming address or customs issues



Always check your parcel status only on the official courier website or app

Never provide Aadhaar, PAN, or bank information to unknown callers

If someone demands money to release your parcel it's a red flag

Report such calls and block the numbers immediately

When it comes to parcels, track smart don't react blindly. Verify first, always.

Category 5

Service or job-related scams

1 The task-based job scam

2 The TRAI scam


But it looks so official...
That's how they trick people. Once you click the link, they'll either ask for personal info or install malware on your phone.
Let's visit your telecom operator's official website and check if there's any real notice.
Exactly. And even if TRAI had any regulation changes, your telecom provider would inform you through proper channels, not sketchy SMS links.
So, this message was just to scare me into clicking?

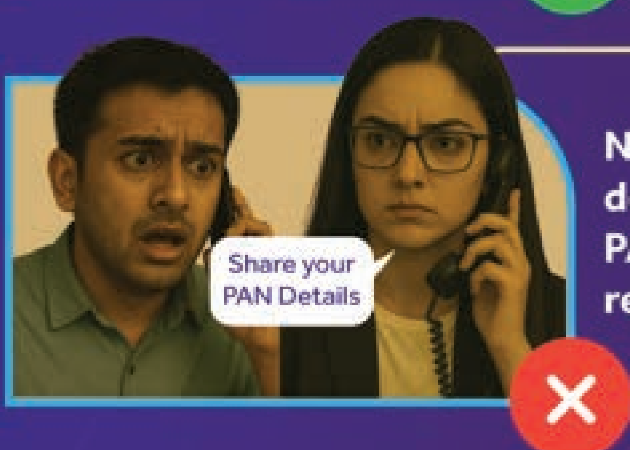

Yes. It's a phishing scam targeting mobile users.
I almost walked right into it. They even used the TRAI logo.
Scammers use fear and urgency to make you act without thinking. Always double-check with your telecom provider.
I'm deleting this and reporting it.
Thanks again, Samajhdaar. You saved my SIM and my sanity.
Masoom forwards the message to cybercrime.gov.in and deletes it from his phone.
Always here to help. When in doubt, verify first!

Advisory

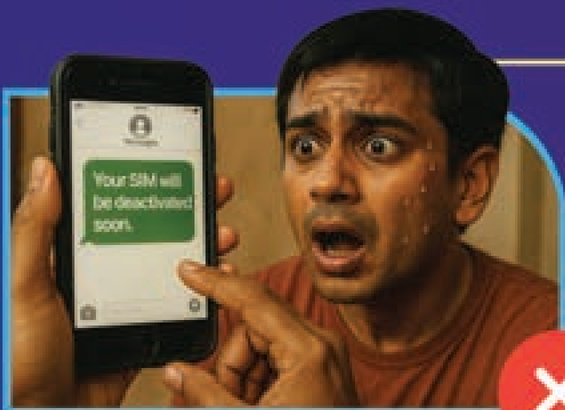
Masoom, job scams and fake SIM deactivation messages are designed to create panic and steal your information. Let me tell you how to stay safe and smart.

Never pay registration fees or deposits for jobs, genuine companies don't ask for money upfront

Verify job offers from unknown contacts by checking the company's website or calling HR



Never share personal documents like Aadhaar or PAN with unverified recruiters



If you receive a message claiming your SIM will be deactivated, don't panic contact your telecom provider directly

Delete such messages, block the sender, and report the scam

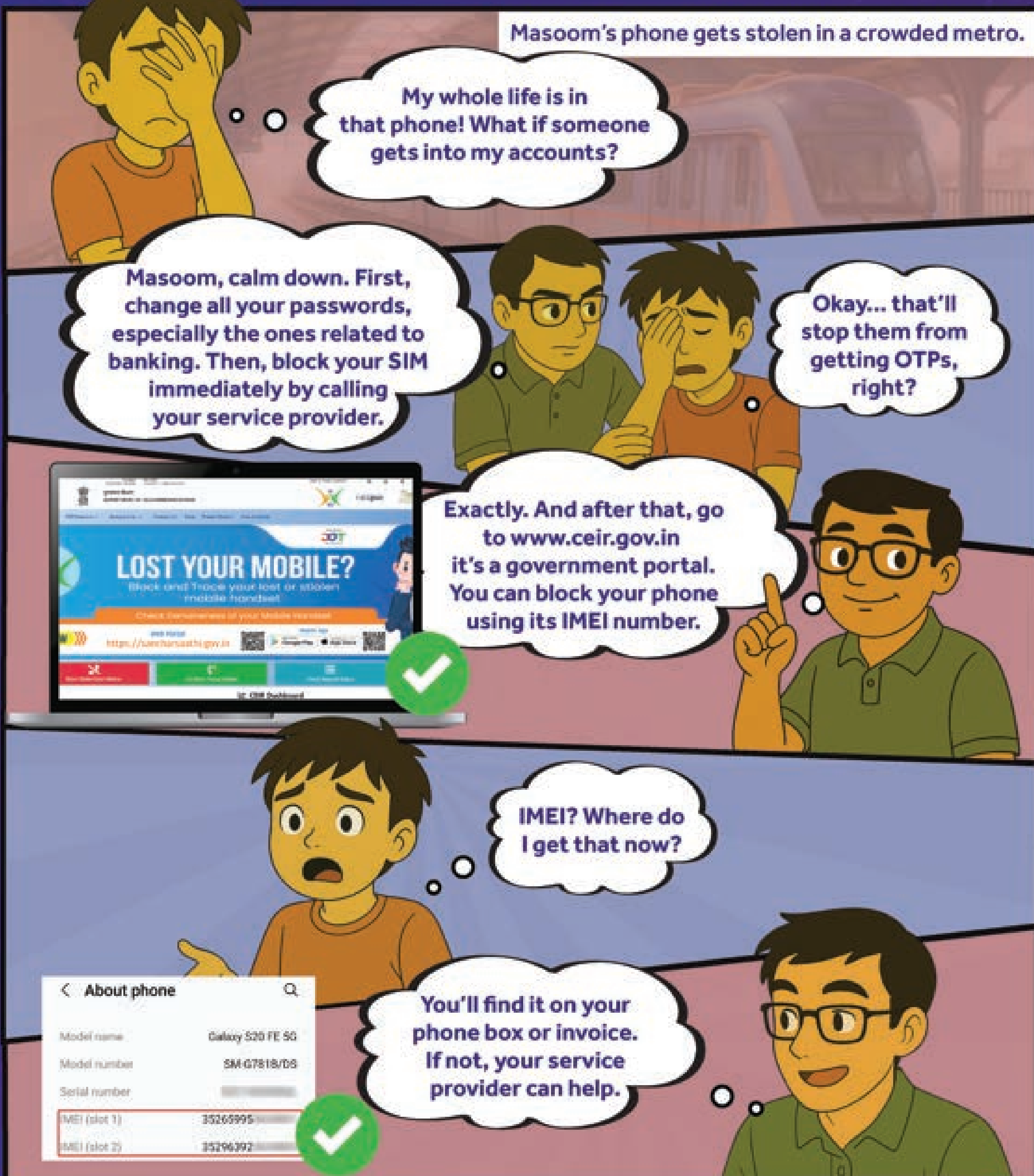
Whether it's about a job or your SIM, trust only official sources. Verify, don't comply blindly.

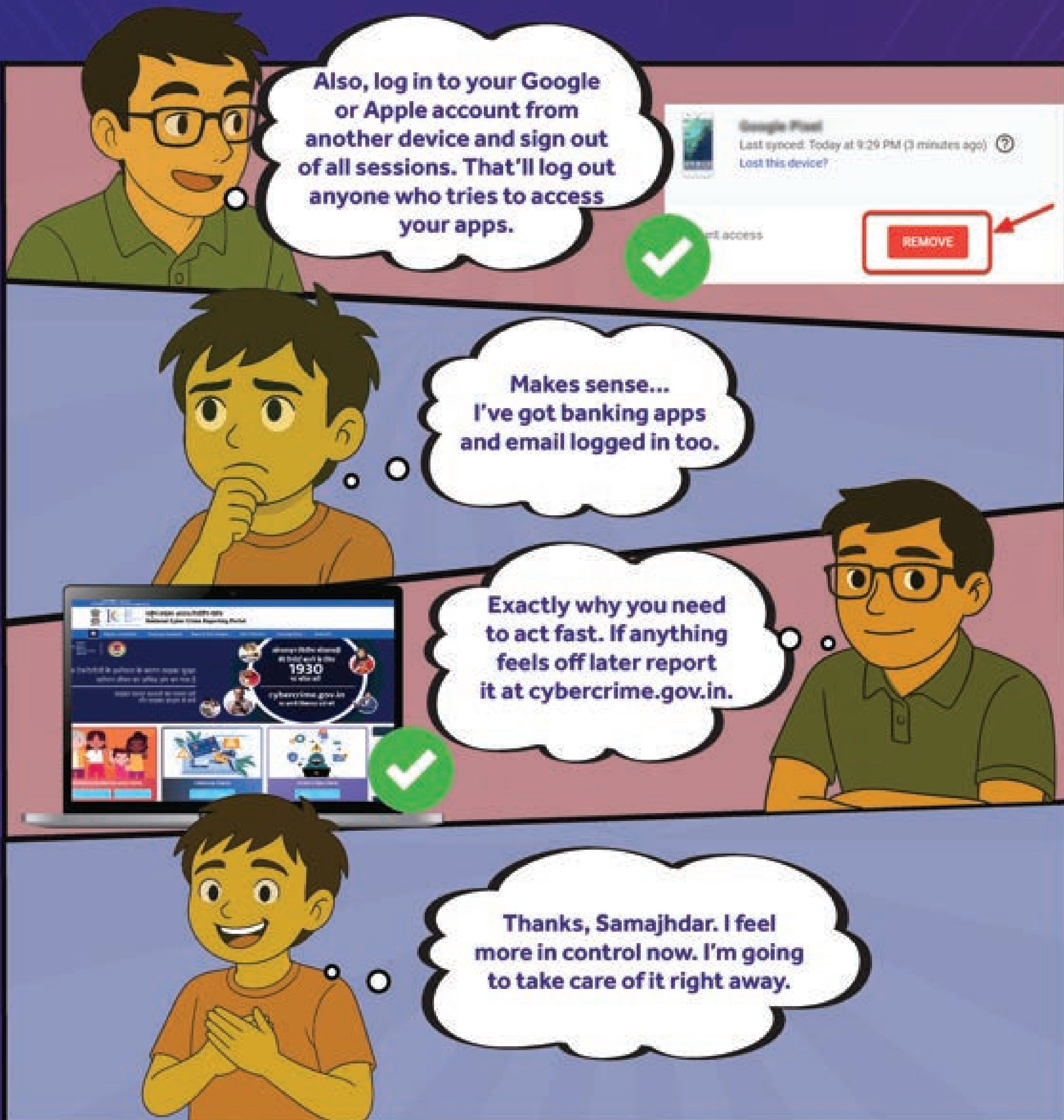
1 Google search fraud

Category 6

Fake search and stolen phone fraud

2 Stolen phone fraud

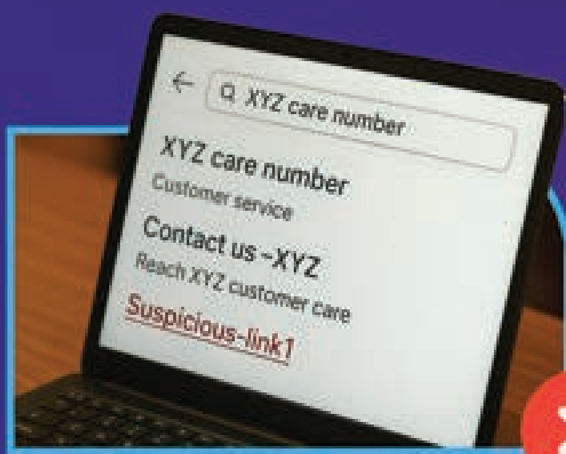




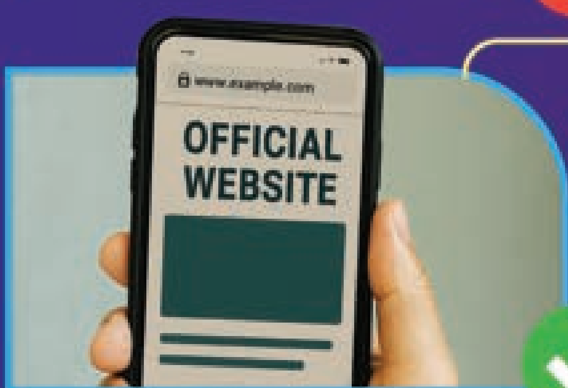
Also, log in to your Google or Apple account from another device and sign out of all sessions. That'll log out anyone who tries to access your apps.
Last synced: Today at 9:29 PM (3 minutes ago)
Lost this device?
REMOVE
Makes sense... I've got banking apps and email logged in too.
1930
cybercrime.gov.in
Exactly why you need to act fast. If anything feels off later report it at cybercrime.gov.in.
Thanks, Samajhdar. I feel more in control now. I'm going to take care of it right away.

Advisory

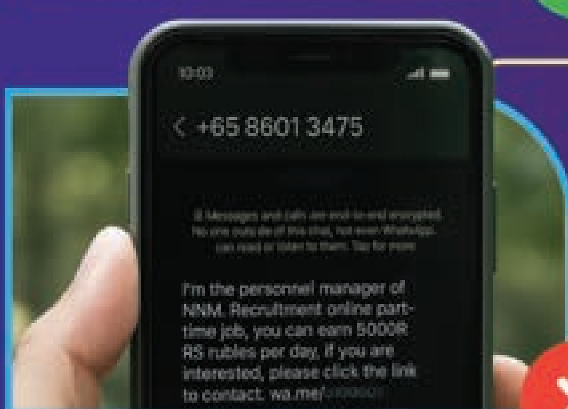
Masoom, one wrong Google search and scammers are ready to trap you. But with the right habits, you can stay safe and in control. Here's your action plan.



Never call customer care numbers directly from Google search results they could be fake



Always use official apps or company websites to get support numbers



Be cautious of paid ads or helpline numbers that don't match the company's official website

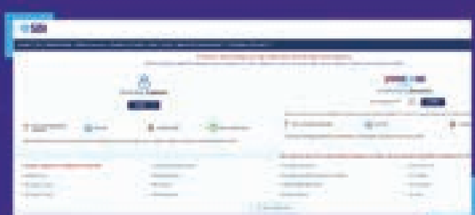
Never share sensitive details like card numbers or OTPs over phone calls from unverified numbers

The safest click is the one that's verified. Always pause, check, and then act.

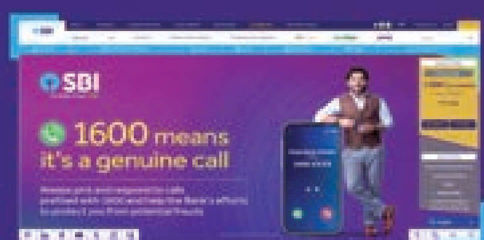
How to identify official SBI website links?

- Scammers often create fake websites that look just like SBI's official portals to trick you into entering your login credentials, card numbers, or OTPs. These fraudulent links are often shared through emails, SMS, social media, or search engine ads.
- To protect yourself, it's important to know and verify the official SBI website URLs before entering any personal or banking information.

Official SBI websites you can trust:



https://www.onlinesbi.sbi



https://bank.sbi

https://retail.onlinesbi.sbi

https://bank.sbi ✓ http://bankk.sbi ✗

Always make sure the address starts with "https://" (the 's' stands for secure) and ends with .sbi – this is the exclusive domain extension owned by SBI.

How to verify if the website is genuine?

1. Check the URL spelling carefully. Fraudsters use lookalike links like online1sbi.com or sbi67.co.in.
2. Look for HTTPS and padlock icon.

Safe banking practices

How to identify official SBI applications?

➤ With the rise in fake banking apps and phishing traps, it's critical to use only official SBI mobile applications to manage your finances. Fraudsters often circulate look alike apps that steal your login details, OTPs, or personal information.

Examples of - official SBI mobile application

App name	Purpose	Developer name
YONO SBI	All-in-one banking - investment, shopping, and lifestyle	State Bank of India
YONO Lite SBI	Mobile banking - fund transfers, account details, bill payments	State Bank of India
BHIM SBI Pay	UPI-based payments	State Bank of India
SBI Quick	Missed call services, balance check	State Bank of India

How to verify the application's authenticity?

1. Developer name should always be: State Bank of India.
2. Download only from: Google Play Store (Android) & Apple App Store (iOS).
3. Check number of downloads and user reviews. Official apps will have high number of downloads and high ratings.
4. SBI's website (https://bank.sbi) lists all official app links under the "Mobile Banking" section.
5. Avoid APKs or download links sent via SMS, email or WhatsApp.

How to identify genuine SMS messages from SBI?

- Cyber fraudsters often send fake SMSes that look like they're from your bank. These messages may ask you to click on suspicious links, share OTPs, or update your KYC. To protect yourself, it's important to know how to identify official SMS communications from SBI.

- TRAI has introduced new rules for SMS messages, effective May 6, 2025; which mandate the use of message-type suffixes in SMS headers.
These suffixes, such as (-P) for promotional, (-S) for service, (-T) for transactional, and (-G) for government messages, aim to enhance transparency and help users identify the nature of the messages they receive. Only registered entities can use these suffixes.

- SBI always sends SMS using registered SMS short codes containing (SB) or (SBI). For example: AX-SBIINB-S, VM-SBYONO-T, AX-SBIBNK-P, etc.

SBI sends SMS only from the following verified sender IDs:

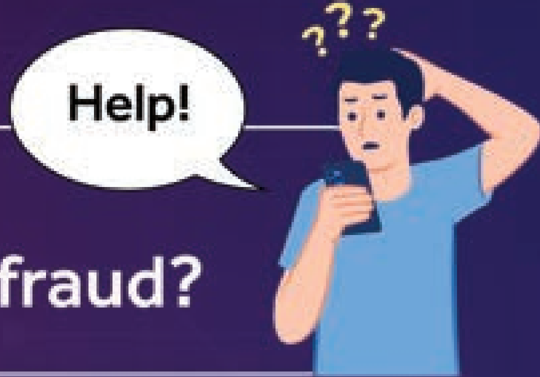
SMS Header	Used For
AD-SBIUPI-S	UPI transaction alerts & updates
AX-SBIBNK-S	General banking alerts, OTPs, account updates

AX-SBIBNK-S ✓ AX-BNKA ✗

The prefix (e.g., AD, AX) indicates the telecom circle and operator, while the body (SBIUPI-S / SBIBNK-S) is SBI's registered identifier.

1600 means it's a genuine call

Always pick and respond to calls prefixed with 1600 and help the bank's efforts to protect you from potential frauds



Where to report cyber fraud?

Call 1930
(Cyber fraud helpline)

For reporting financial frauds (UPI, net banking, card misuse, etc.). Available 24x7.

Visit
https://cybercrime.gov.in

For all types of cyber complaints including social media abuse, identity theft, scams, and more.

Visit
https://sancharsaathi.gov.in

To report suspected fraud, mobile-related scams, and unsolicited commercial communication (spam).

Reporting unauthorised SBI transactions

If you are an SBI customer and notice unauthorised electronic transactions, report it via any of the following:

- 1800 11 1109 (Toll free)
- 94491 12211 (Toll free-mobile)
- 080 - 2659 9990 (Toll number)

Every second matters. Report fast. Stay safe.

Save these contacts. Share with others.
Together, let's stay a step ahead of cyber criminals.

Stay alert and #StaySafeWithSBI.

SBI
The banker to every Indian

INFORMATION SECURITY
DEPARTMENT