

**SAFER
INTERNET
INDIA**



User Safety Handbook

User Safety Handbook

February 2025

Acknowledgements

Ateesh Nandi, Lalantika Arvind, Meghna Bal, Samrridhi Kumar, Siva Bhargavi Nori, Srishti Joshi and members of the Safer Internet India coalition



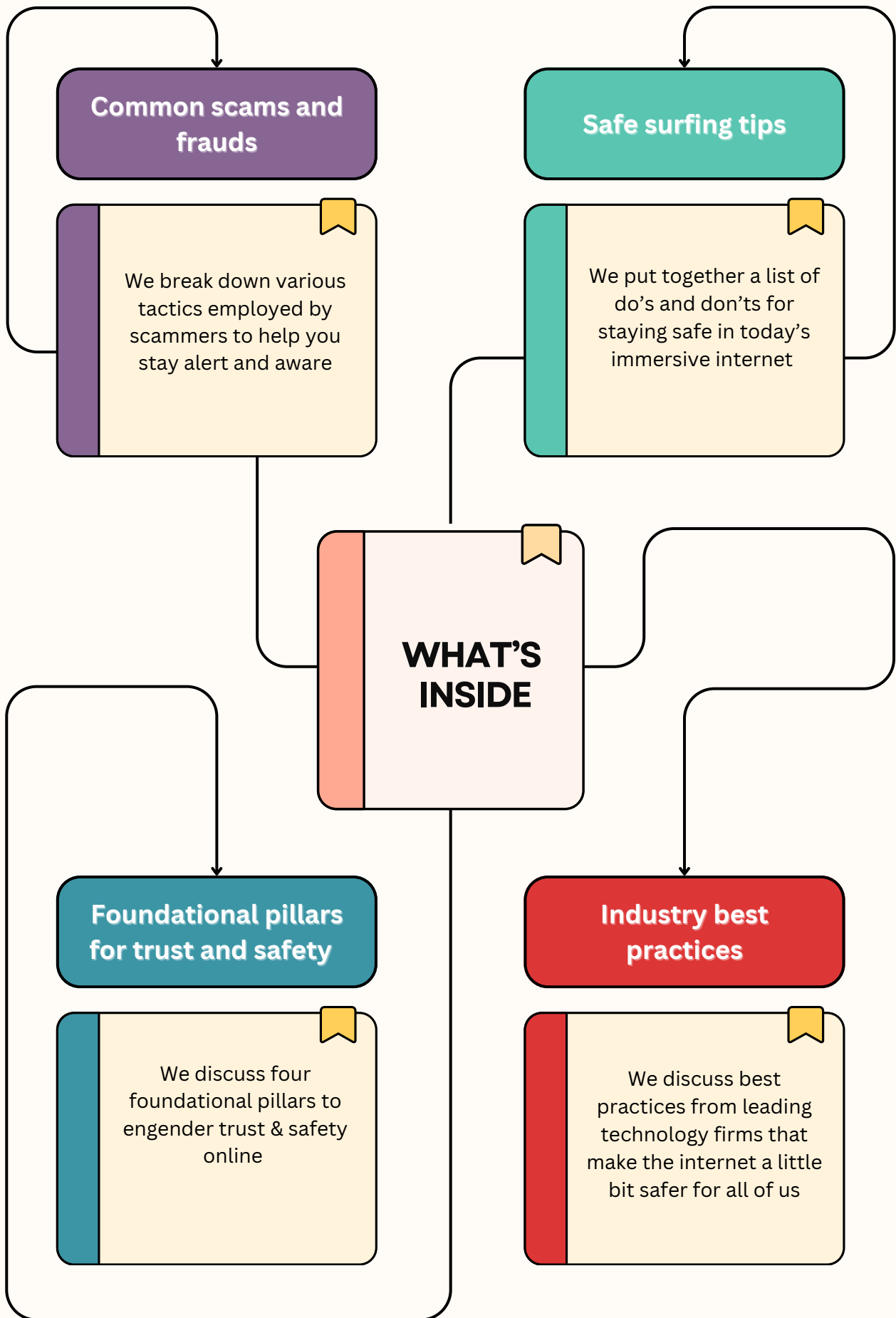


Table of contents

Introduction	06
<hr/>	
The Basics	07
<hr/>	
Common Frauds and Scams	11
<hr/>	
AI Voice Scam	11
Dating App Scam	12
Digital Arrest Scam	14
Fake Investment / Trading App Scam	16
Fake Job Offer Scam	18
Fake Link / QR Code Scam	21
Fake Loan App Scam	23
Fake Mobile Recharge Scam	25
Parcel Delivery Scam	26
Disguised Malware Scam	28
Tech Support Scam	29
OTP Scam	31
Rewards Scam	33
SIM Swapping / SIM Cloning Scam	34
Impersonation Scam	35
Skimming Machine Fraud	36
Fake Welfare Scheme Scam	37
<hr/>	
Do's and Don'ts	38
<hr/>	
Pro Tips	39
<hr/>	
Industry Best-Practices for User Safety	41
<hr/>	



Dear Reader

Safer Internet India (SII) is a coalition of like-minded companies spanning different segments of India's burgeoning digital economy.

SII responds to an urgent societal need to tackle growing instances of online scams, cyber threats, and data breaches. We bring multidisciplinary voices together to strengthen user trust and safety online.

We wrote this handbook so that internet users like you can safeguard yourselves from online frauds and scams.

This handbook details the anatomy of common frauds and scams, and recommends do's and don'ts for internet users to surf the internet and engage with digital businesses in a safe and secure way. It also recognises steps taken by businesses and policymakers to make online spaces safer.

Thanks for reading

Safer Internet India



Introduction

Digital spaces touch every aspect of our lives. India's 900 million+ internet users regularly go online to work, learn, and buy everything from household necessities to luxury goods, entertainment subscriptions, and even financial services.

However, users must be careful about who they interact with, and what they purchase online. The online world is filled with offers and deals that seem too good to be true, and most often are. Indians reportedly lost around ₹11,333 crores to online scams in the first nine months of 2024!

Fraudsters and scammers are highly adversarial, opportunistic, and adaptive. Unfortunately, they are getting ever more sophisticated, while many citizens lack basic digital skills. A 2022-23 survey by the Government of India (GoI) suggests that around half of India's internet users did not know how to send an email, and only 38 percent of people could perform an online banking transaction. Rural India is worse off than its urban counterpart when it comes to digital skills, and there are significant discrepancies across different genders. The bottom line is, scams are a whole-of society challenge. Many Indians remain at risk of being defrauded, and must be empowered with skills and awareness to protect themselves online.

The GoI recognises the need for protecting Indian internet users from the menace of online scams. The Ministry of Home Affairs (MHA) and the Ministry of Electronics and Information Technology, along with specialised bodies like the Indian Cybercrime Coordination Centre (I4C) and the Indian Computer Emergency Response Team (CERT-in) work around the clock to investigate and stop frauds and scams, and resolve related online safety issues. Regulators like the Reserve Bank of India (RBI) and the Telecom Regulatory Authority of India (TRAI) are also leveraging technology to safeguard Indians, be it AI (Artificial Intelligence) systems to detect mule accounts used in money laundering, or distributed ledger technology (DLT) based registration of telemarketers to limit spam/pesky calls, besides introducing new regulations in their domains.

But the sheer scale of the problem of online safety means we need all hands on deck - everyone must work together to keep users safe online.

The Basics

Staying safe online is more important than ever. In this section we familiarise you with some basic terms and concepts, so that you can navigate digital spaces better.

PERSONAL INFORMATION

Personal information is any detail about you that can identify who you are. This includes things like your name, address, phone number, email, date of birth, or bank details. Scammers often try to steal this information to pretend to be you or access your accounts.

SENSITIVE PERSONAL INFORMATION

Sensitive personal information is private details about you that need extra protection because they can be misused if they fall into the wrong hands. This includes things like your passwords, bank account numbers, credit card details, medical records, or government ID numbers (like Aadhaar or PAN). Protecting this information is very important to keep your identity and finances safe. Be very careful about who you share such information with.

FRAUD

Online fraud is when someone uses lies or deception to illegally take money or sensitive information through the internet. This includes things like hacking accounts, stealing payment details, or creating fake websites to trick people.

SCAM

An online scam is when someone tricks you on the internet to steal your money, personal information, or sensitive data. Scammers often pretend to be trustworthy, offering fake deals, posing as officials, or sending messages that look real to deceive you.

An online scam is a type of online fraud, but not all frauds are scams. A scam often involves convincing people to voluntarily give money or information (e.g. fake prizes or job offers). Online fraud, on the other hand, can involve actions like identity theft or hacking, where the victim might not even realise they've been targeted right away.

In short, scams rely on tricking people, while fraud includes broader methods like stealing or misusing information. This is why users must be vigilant, not only when they interact with people online but also when they go to websites or look to download apps.

HACK

A hack is when someone breaks into a computer, account, or network without permission to steal information, cause damage, or take control. Hackers often use special tools or tricks to find weaknesses and get access.

PHISHING

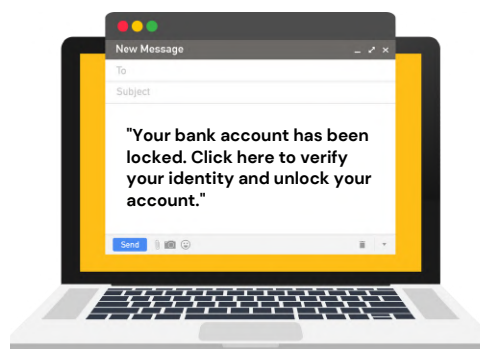
Phishing is a trick used by scammers to steal your personal information, like passwords, bank details, or credit card numbers. They usually pretend to be someone you trust, like your bank, a company, or a government agency, to make you click on fake links or share sensitive information.

Phishing attacks can take place through multiple modes. Attacks carried out through SMS / messaging apps are called smishing attacks, whereas those carried out over phone calls are called vishing (voice-phishing) attacks.

Example:

You get an email that says:

"Your bank account has been locked. Click here to verify your identity and unlock your account."



The link takes you to a fake website that looks like your bank's site, but any details you enter are accessed by the scammer.

Another example of a phishing email is when the scammer pretends to be a colleague in a person's organisation and sends them an email asking for money. In such instances, please do not transfer any money and call your colleague (even if it is your boss) to verify their identity. Another tip is to verify the email. Typically, the email will not correspond to the name of your organisation or your colleague's actual work email.

MALWARE

Malware is harmful software designed to damage, steal, or take control of your computer, phone, or other devices without your permission. It can hide in fake apps, email attachments (files that accompany emails), or websites and cause problems like stealing your information or slowing down your device.

ARTIFICIAL INTELLIGENCE

AI is technology that can analyse data, mimic human behaviour, and create realistic content, like messages or voices. Scammers can use AI to make their tricks more convincing, such as creating fake messages that sound real, mimicking someone's voice, or sending personalised emails to trick people into sharing money or personal information. AI helps scammers target victims more effectively and makes their scams harder to detect.

SPAM

Spam is unwanted or junk communication, usually made through phone calls, email, text, social media. It's often used to advertise things, but sometimes it's a part of an attempt to steal your information or money.

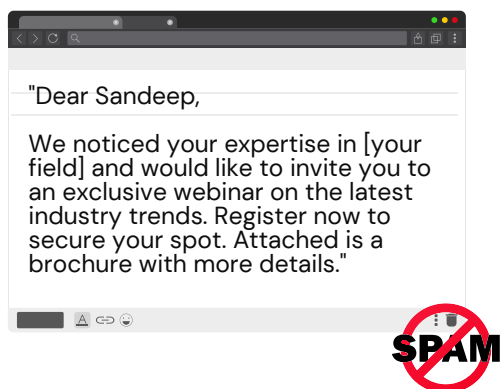
Example:

"Congratulations! You've won a \$1,000 gift card! Click here to claim your prize now."

This email is usually fake, and clicking the link could lead to a scam or infect your device with harmful software.

Spam is becoming more sophisticated and can be tailored to resemble communication that may be relevant to your business, profession, or vocation.

An example of sophisticated spam tailored to your profession could be:



The email looks professional and relevant to your work, but the link could lead to a phishing site, and the attachment might contain malware. This kind of spam is designed to trick professionals by appearing legitimate and personalised.

Common Frauds and Scams

SCAM # 1

AI VOICE SCAM

WHAT IT IS

An AI voice scam is when scammers use AI to copy someone's voice, like a family member or boss, to trick you. They might call you and ask for money, pretending it's an emergency, or give fake instructions to steal information. Since the voice sounds real, it can be very convincing and hard to spot.

HOW IT WORKS

Scammers find recordings of someone's voice from social media, videos, or voicemails. Using AI tools, they copy the person's voice to make it sound real and natural.

The scammer calls you using the fake voice and pretends to be someone you know, like a friend, family member, or boss. They create urgency, like claiming there's an emergency, and ask for money, gift cards, or sensitive information.

If you fall for it, they use what you give them to steal your money or personal information.



Be Wary of Urgency: Scammers often pressure you to act quickly. Take your time to think and verify before doing anything.



Verify the Caller: If someone asks for money or sensitive personal information, call them back on their usual number to confirm it's really them.



Ask Personal Questions: Ask something only the real person would know to catch the scammer off guard.



Use a Safe Word: Set a family or workplace "safe word" known only to trusted people, like "Dravidthewall" or "RavaDosa". If someone asks for money claiming to be a relative or boss, ask for the safe word before proceeding. A scammer wouldn't know it, helping you verify their identity.

SCAM # 2**DATING APP SCAM****WHAT IT IS**

This scam happens when someone matches with a person on a dating app and invites them to meet at a restaurant or cafe that is part of the scam. The scammer orders expensive items, sometimes things not even on the menu, then makes an excuse to leave. The victim is left with a huge bill and is forced to pay by the staff or bouncers.

HOW IT WORKS

Planning the Date: The scammer plans the date and asks the victim to meet at a particular cafe. Sometimes the scammer may propose a locality, and may ask the victim to meet at a Metro station, saying they'll choose a cafe nearby.

At the Cafe: Once inside, the scammer orders food or drinks, sometimes even things that aren't on the menu. They may fake an emergency and leave quickly.





A Surprise Bill: When the bill arrives, it's much higher than expected—often several times the usual price. If the victim protests, the cafe staff or bouncers threaten them, forcing them to pay.

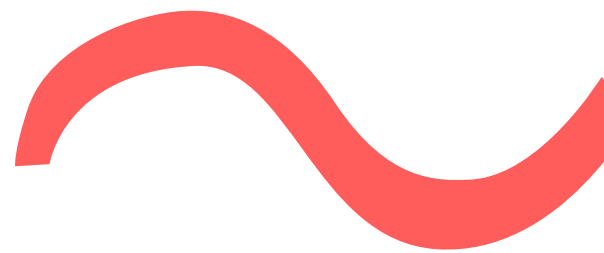
Scam Operation: The scam is run by a group that includes the cafe owner, staff including managers or bouncers, and the person who matches with the victim on the dating app. Each person gets a share of the money collected from the inflated bills.

Most victims don't report the scam because they fear embarrassment or revealing to their family that they were using a dating app.

If this happens to you, please report it to your local police station or on www.cybercrime.gov.in.



-  **Be Cautious about the Meeting Place:** Avoid meeting at locations chosen by the other person unless you're familiar with the area.
-  **Research the Cafe Suggested by the Other Person:** Look up the cafe online and check reviews to ensure it's a legitimate place. Make sure to cross-verify from multiple sources of reviews. Scammers sometimes add fake reviews to make a place seem legitimate
-  **Trust Your Instincts:** If something feels off—like the person being overly insistent on a location or they have suddenly become cold and distant once you are seated at the restaurant—be wary.
-  **Report Suspicious Behaviour:** If you suspect foul play, inform the police and the dating app to prevent others from being scammed.



SCAM # 3**DIGITAL ARREST SCAM****WHAT IT IS**

A digital arrest scam is when scammers pretend to be police or government officials like customs officials online or over the phone. They claim you are in legal trouble and demand immediate payment to "avoid arrest." They often use fear and urgency to pressure victims into paying quickly.

HOW IT WORKS

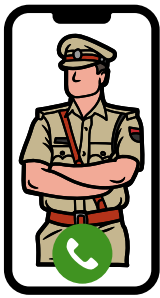
Fake Call or Message: You receive a call, email, or text claiming you've broken the law and must pay a fine or face arrest. For instance, one victim received a call from an international number claiming the scheduled delivery of a parcel had been cancelled.

Threats and Pressure: The scammer says you'll face serious consequences, like jail time, if you don't pay immediately. In the instance cited above, the caller prompted the victim to press "0" for support. As soon as they did this, someone posing as a customer support representative came on the call and claimed that a package linked to their name contained illegal substances and had been sent to China. The representative further claimed an arrest warrant had been issued against him. Fake police officers and investigators then joined the video call.

Scammers will go to great lengths to convince you that they are real cops. They will show you fake letterheads and ID cards. They even create fake police stations and dress up like cops while video calling.

Isolation and Urgency: The scammer will try to convince you to isolate yourself. They will tell you to travel to a remote location or lock yourself in a room and draw the curtains. They will also tell you to avoid taking other calls.

Relentless Payment Demands: They make relentless demands for money, usually to multiple accounts so it cannot be traced.

**Example:**

You get a call saying: "This is Officer X from the Cyber Crime Unit. We've found illegal activity linked to your account. You must pay ₹10,000 right now to avoid arrest. Failure to comply will result in an arrest."



Stay Calm: The police cannot and will not make an arrest over a phone call or a video call in India. Do not panic even if the scammer claims to know personal details about you like your address, name etc. Disconnect the call immediately and stop engaging.



Verify the Claim: Hang up and contact the official organisation directly using their official phone number or website, whether it be the police or other government officials or the organisation whose customer service representative called you.



Refuse Isolation: Never let anyone convince you to isolate yourself or avoid taking calls from friends or family. Hang up and talk to someone you trust immediately.



Do Not Make Payments: Genuine law enforcement will never ask for money over the phone. Refuse all such demands.



Watch for Red Flags: Calls from international or domestic numbers you don't recognise. Requests to "verify" personal details like your name, bank account, or ID.



Be Careful: Be cautious when answering phone calls from unknown or suspicious numbers, like calls from a foreign country.

SCAM # 4**FAKE INVESTMENT /
TRADING APP SCAM****WHAT IT IS**

The fake trading app scam involves the creation and promotion of fraudulent trading applications designed to deceive investors. These apps often promise high returns and low risks, enticing you to invest your money. However, once you deposit funds into these fake apps, you may encounter a range of deceitful practices.

HOW IT WORKS

Ads and Promotion for Fake Investment Apps: Scammers use deceptive ads to lure victims with promise of abnormally high financial returns. Often, victims are also added to WhatsApp groups by scammers, that have legitimate sounding names such as “ICICI IR Team” which make victims think that they are affiliated with licensed financial institutions. Scammers typically use these groups to share fake success stories to gain the victim’s trust.

Instructions to Download Fake Apps and Invest: Victims are instructed to download fraudulent apps that appear to offer genuine investment opportunities. These apps, like ‘IC ORGAN MAX’ and ‘Techstars.shop’, display names of well-known stocks and financial instruments to trick users into believing they are legitimate.

The app is designed to look real, with fake charts, account balances, and profit statements that make it seem like your investments are growing.

Fabricated Display of High Returns: Once victims install the fake apps and invest their money, they initially see good returns displayed on the dashboard, which encourages them to invest more. However, these returns are made-up numbers. When victims try to withdraw their money, they are asked to pay additional charges like statutory taxes or brokerage fees, so that the scammers can extract more money from them.

DECEITFUL PRACTICES

Locked Funds: You might find that you can't withdraw your money.






Demands for Fees: The app may ask for additional "fees" or "taxes" before you can access your funds.

Disappearing Act: The scammers may shut down the app altogether, taking your money with them.

Fake Support: If you reach out for help, you may encounter fake customer support that stalls or pressures you to deposit more funds.

Vanishing Scammers: Once the scam is exposed, the app is removed, and the scammers disappear, leaving victims with no way to recover their money.



-  Be wary of unwanted/unexpected messages that you have not asked for offering quick money through online investments.
-  Avoid investment opportunities that promise unrealistic returns.
-  Verify the legitimacy of investment platforms through official websites or apps. For instance, if they suggest they are affiliated with a certain bank, like ICICI, call up ICICI's customer support or check its official website to see if this is true.
-  Do not share login credentials, personal, or financial information with strangers, especially on messaging apps.
-  Avoid downloading unknown apps or files at the request of unfamiliar contacts.

SCAM # 5**FAKE JOB OFFER SCAM****WHAT IT IS**

A fake job offer scam is when scammers pretend to offer you a job to trick you into giving them money or personal information. These scams often target people searching for jobs, promising high salaries, easy work, or benefits to lure them in.

HOW IT WORKS

Attractive Job Post: Scammers create fake job ads on websites, social media, or send them through emails or messages. Sometimes, scammers may also pretend to be consultancies that guarantee you placement at a prestigious company.

Quick Selection Process: They tell you that you've been "selected" for the job, often without an interview or proper screening.

Requests for Payment or Personal Information: You're asked to pay fees for things like training, registration, work materials, or visa processing (if it's an international job).

Fake Documents or Links: They may send fake offer letters, contracts, or direct you to fraudulent websites to appear legitimate.

Vanishing Act: Once they collect the money or your personal details, the scammers disappear, and the job doesn't exist.

EXAMPLES OF FAKE JOB SCAMS

There are several types of Fake Job Scams

- **Work from Home Job Scam**
- **Job Placement Service Scams**
- **Nanny, Caregiver, and Virtual Personal Assistant Job Scams**



Work from Home Job Scam

Scammers claim to offer jobs where you can make lakhs of rupees a month working from home with little time and effort.

Common work from home job scams include reshipping scams and reselling merchandise scams.

Reshipping Scams: Scammers advertise fake jobs like quality control managers or virtual assistants. Once "hired," your task is to receive, repackage, and reship expensive items, often purchased with stolen credit cards. The paycheck never arrives, and the company disappears, leaving you involved in a crime. If you provided personal details for "payroll," you could also face identity theft.

Reselling Merchandise Scams: Scammers promise a job reselling luxury products at a profit. After you pay for the items, the package never arrives or contains worthless junk.



Nanny, Caregiver, and Virtual Personal Assistant Job Scam

Scammers post fake job ads for nannies, caregivers, and virtual assistants on job sites. Or they may send emails that look like they're from someone in your community. The message might also seem to come from someone who is part of an organisation you know, like your college or university.

If you apply, the person who hires you might send you a check. They'll tell you to deposit the check, keep part of the money for your services, and send the rest to someone else.









This is a scam. A legitimate employer will never ask you to do that. The check is fake and will bounce, and the bank will want you to repay the full amount of the fake check, while the scammer keeps the real money you sent them.



Job Placement Service Scams

The scammer will reach out to you posing as a consultancy that can help place you at a top company. They will call you for an interview. When you reach, there may be large men standing at the entrance. The scammer will pose as a consultant and ask you some general questions about your qualifications. They may even show you fake pictures of people they have allegedly placed at major multi-national companies before. After this, they will ask you for money, and the large men may force you to pay.



-  No organisation/company ever asks for money to work for them.
-  Ignore job offers sent from spam / junk emails or messages.
-  If you get an offer that includes depositing a check and then using some of the money for any reason, that's a scam. Walk away.
-  Placement firms do not ask candidates for fees. Companies pay them fees to find candidates for jobs. If a placement firm asks you for a fee – especially one you have to pay in advance – walk away. You're probably dealing with a scam.
-  If someone offers you a job and claims that you can make a lot of money in a short period of time with little work, that's almost certainly a scam.
-  Check the company's website, reviews, and official contact details.
-  Avoid offers from companies with no online presence or sketchy details.
-  Don't share sensitive details like your bank account, Aadhaar, or PAN without verifying the company.

SCAM # 6**FAKE LINK / QR CODE SCAM****WHAT IT IS**

A fake link/QR code scam tricks you into clicking a malicious link or scanning a fraudulent QR code. These scams are designed to steal personal information, payment details, or install harmful software on your device.

**HOW IT WORKS**

Fake Links: Scammers send links via emails, texts, or social media, claiming to offer something appealing (e.g. discounts, rewards, urgent updates). Clicking the link directs you to a fake website that looks legitimate but is designed to steal your information.






Fraudulent QR Codes: Scammers create QR codes that lead to phishing websites or trigger harmful actions (e.g. installing malware). These codes might be sent digitally or placed on physical posters or ads.

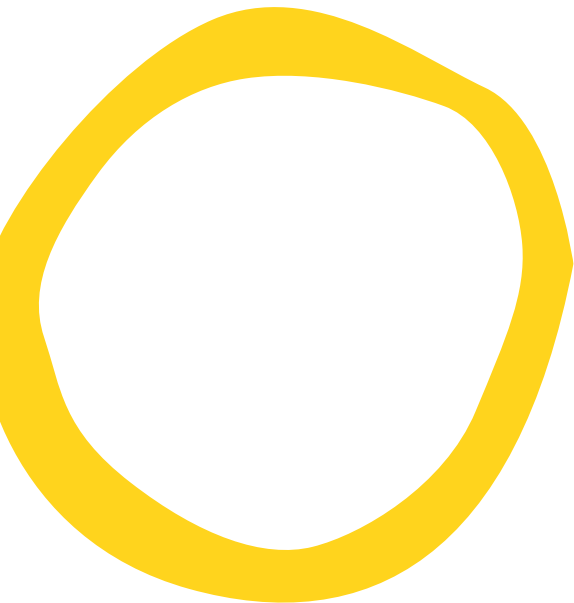
Sometimes scammers take a legitimate ad and replace the QR code with a fake one, to fool people into thinking they are legitimate.

EXAMPLES OF FAKE LINK / QR CODE SCAM

- | | |
|--|---|
| <ul style="list-style-type: none"> • A text message says your package delivery is delayed; the link asks for payment details. | <ul style="list-style-type: none"> • Scammers can also circulate fake payment links or QR codes to trick you into filling in your credit card details or UPI PINs. |
| <ul style="list-style-type: none"> • Scammers send links to fake websites which mimic the sites of legitimate entities such as banks, and ask you to update your KYC details. | <ul style="list-style-type: none"> • A QR code on a poster offers a discount but leads to a phishing site. |



-  If you see a QR code in an unexpected place, inspect the URL before you open it. If it looks like a URL you recognise, make sure it's not fake – look for misspellings or a switched letter.
-  Don't scan a QR code in an email or text message you weren't expecting – especially if it urges you to act immediately. If you think the message is legitimate, use a phone number or website you know is real to contact the company.
-  Don't click on payment links from unknown sources.
-  Always verify the name of the intended recipient when making QR code payments.
-  When asked for your KYC, verify the purpose of KYC and the identity of the person requesting such information.



SCAM # 7**FAKE LOAN APP SCAM****WHAT IT IS**

A fake loan app scam involves scammers creating fraudulent apps that promise quick and easy loans with minimal paperwork. These apps often target individuals in urgent need of money, tricking them into paying fees or sharing personal information. They often have hidden charges and very high interest rates.

HOW IT WORKS

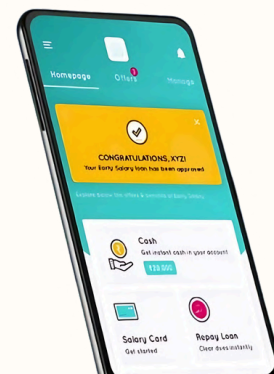
Enticing Offers: The app advertises loans with no credit checks, instant approval, or very low interest rates to get you to use their services. Scammers often choose names that are similar to reputable financial institutions such as banks to trick you into thinking they are legitimate.

Upfront Fees: Once you apply, the app demands processing fees, service charges, or other payments before disbursing the loan.

Data Theft and Malware Attacks: The app collects sensitive personal details like your bank account number, ID proof, and phone contacts. Sometimes these apps have malware installed which gets loaded onto your phone after you download the app.

Harassment: If you fail to pay, scammers will use the stolen data to harass you, your family, or contacts with threats or public shaming. For instance, they may access your photos under the excuse of conducting video-KYC and blackmail you based on what they find.

No Loan Disbursed: Often, no loan is provided even after the fees are paid, and the app disappears or stops responding.





Verify the Source: Loan apps never issue loans themselves; instead they partner with RBI-regulated banks or non-bank financial companies (NBFCs).

Check the websites of banks and NBFCs to see if they have actually partnered with the loan app that is claiming such a partnership. If you are unable to find anything on the website, call the customer service number of the bank/NBFC to verify further.



Be Cautious with Permissions: Avoid apps that ask for unnecessary access to contacts, photos, or messages.



Use Trusted Sources: Verify the app's legitimacy and reviews before using it. Make sure you check reviews from multiple sources. As mentioned earlier, scammers often put out fake reviews to seem legitimate.



Upfront Fees: Legitimate lenders typically do not ask for upfront fees. Avoid lenders who demand payment before disbursing a loan.



Red Flags: Be cautious of instant loan offers, especially if they promise guaranteed approval with no credit checks.



Interest Rates: Scrutinise the interest rates and terms carefully. If they seem too good to be true, they probably are.



Contact Information: Confirm the lender's contact details and physical address. Scammers often use fake information.



Report Suspected Fraud: If you encounter a potential cyber loan shark or believe you've been scammed, report it to the appropriate authorities immediately.

SCAM # 8**FAKE MOBILE RECHARGE SCAM****WHAT IT IS**

A fake mobile recharge scam tricks you into paying for phone recharges or offers that are fake. Scammers use fake websites, apps, or messages claiming to provide discounts, cashback, or free recharges.

HOW IT WORKS







Fake Offers: Scammers advertise unrealistic deals, such as huge discounts or "free recharges," through messages, social media, or fake apps. Sometimes scammers pretend to be officials from TRAI, to get you to trust them.

Payment for Recharge: The victim pays for the recharge via the fake platform, but no recharge is actually done.

Stealing Information: Fake recharge platforms often collect personal details, payment information, or bank details/credit card information during the process.

Phishing Links: Scammers send links via SMS or email, redirecting you to fake websites that mimic legitimate telecom recharge services.



-  **Use Trusted Platforms:** Only recharge through your mobile provider's app or the application that is linked to your UPI.
-  **Beware of Unrealistic Offers:** Ignore deals that seem too good to be true, like massive discounts or free recharges.
-  **Verify Websites and Apps:** Check the URL for fake or misspelled names and download apps only from official app stores.
-  **Don't Click on Unverified Links:** Avoid clicking on recharge links sent via SMS, WhatsApp, or email from unknown sources.
-  **Secure Payment Details:** Never share your payment information with third-party platforms that are not verified.
-  **Report Suspicious Activity:** Inform your telecom provider or local cybercrime helpline if you encounter a scam.

SCAM # 9**PARCEL DELIVERY SCAM****WHAT IT IS**

A parcel delivery scam tricks you into thinking you have a package waiting to be delivered. Scammers send fake messages or emails asking for payment or personal information to release the package.

HOW IT WORKS

Fake Notifications: You receive a text, email, or call claiming you have a package that has arrived but cannot be delivered due to incomplete address information or payment of dues. It might appear to be from a trusted courier company like FedEx, DHL, or India Post.

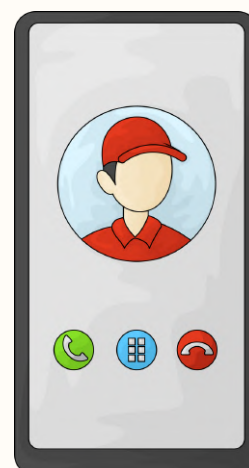
Phishing Links: The message includes a link to update your address, typically in a time bound manner, say within 12 hours. The message can also include a link to "confirm delivery" or pay a fee. Clicking the link takes you to a fake website where scammers steal your payment or personal details.

Follow up Call: Typically, an SMS or email will be accompanied by a phone call from someone posing as a representative from the courier company. They will repeat that your parcel cannot be delivered because your address is incomplete or some payment is due, and urges you to complete the formalities on the link provided.






Urgency and Pressure: The caller puts pressure on the victim, threatening that the order will be cancelled or parcel destroyed if the address is not updated or payment is not made.

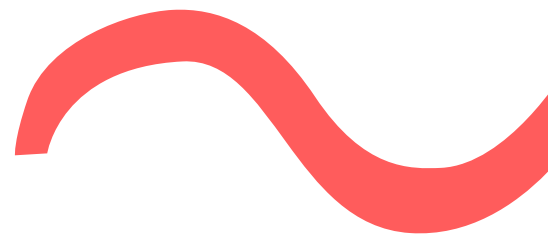
Payment Trap: You're asked to pay a small fee for re-delivery. The page only accepts debit or credit card payments, with no options for UPI or cash on delivery.

No Delivery: Once you pay or provide details, scammers disappear, leaving you with no package and potentially stolen information.





-  **Recall if You Placed an Order:** Try to recall if you actually have a package on the way or if you made an order that is yet to be delivered.
-  **Verify the Message:** Contact the courier company directly through their official website or phone number to confirm the delivery.
-  **Avoid Clicking Unknown Links:** Do not click on links in messages claiming to be about a parcel, especially from unknown senders.
-  **Look for Red Flags:** Be cautious of poor grammar, generic greetings, or suspicious email addresses.
-  **Secure Your Information:** Never share personal or payment information unless you're sure the source is legitimate.



SCAM # 10**DISGUISED MALWARE SCAM****WHAT IT IS**

A disguised malware scam induces you to click on a harmful link designed to spread malware or steal personal information. These links often look legitimate, but clicking on them can infect your device or direct you to harmful sites.

HOW IT WORKS

Placement on Websites: Scammers place these links through various means like ads on websites.

Click and Infect: When you click the link, it may:

- install malware on your device,
- redirect you to phishing websites, or
- trick you into downloading fake software or updates.



No Interaction Needed: Some harmful links don't even require a click—they can infect your device just by being displayed on certain websites (via malicious code).



Avoid Suspicious Links: Don't click on links offering unbelievable deals, free software, or urgent warnings.



Keep Software Updated: Ensure your browser and security software are up to date to block malicious ads.



Enable Security Features: Use antivirus software and browser security settings to detect and block threats. Some antivirus software come with malware protection which blocks threats if you inadvertently go to a rogue website. Ensure you get an antivirus software with such features in place. Also, make sure the risk monitoring settings on your browser are turned on.



Stick to Trusted Websites: Avoid visiting or interacting with shady or unverified websites. Use trusted and well known web browsers which warn you before opening websites which may contain harmful content, malware or lack security certifications.

SCAM # 11**TECH SUPPORT SCAM****WHAT IT IS**

A tech support scam tricks you into believing there's a problem with your computer or device. Scammers pretend to be from legitimate companies like Microsoft or Apple, offering fake "support" to fix non-existent issues, often stealing money or personal information.

HOW IT WORKS

Fake Warning Messages: You see a pop-up on your computer or phone claiming it's infected with a virus or has a critical error. It often includes a fake customer support number.







Spam Calls: Scammers call pretending to be tech support, claiming they've detected problems with your device.

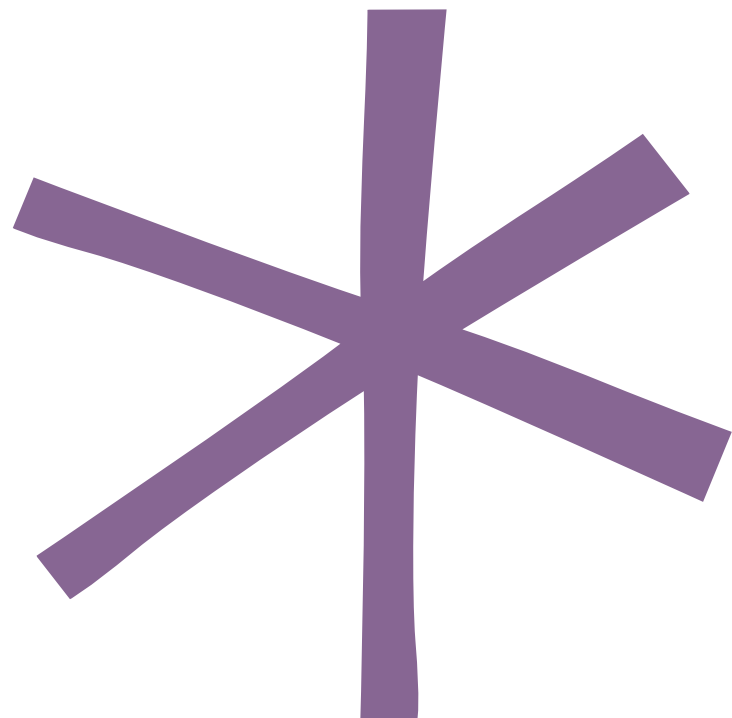
Screen Mirroring Software: Scammers ask you to download remote desktop software or screen-sharing apps on the pretext of fixing an error on your computer. They will ask you share a PIN, which will enable them to access your device from any location. Scammers can then view and make changes to your files, transfer data, install viruses and take control of your device.

Payment Demands: They claim to fix the issue and demand payment for fake services, often through credit cards or gift cards.

Data Theft: While accessing your device, they may steal sensitive information like passwords or banking details.



-  **Don't Trust Unsolicited Calls:** Legitimate companies don't call you about problems you didn't report.
-  **Ignore Pop-Ups:** Close any suspicious pop-ups, and don't call the numbers displayed. Use antivirus software to scan your device instead.
-  **Never Give Remote Access:** Don't let anyone remotely control your device unless you've contacted a trusted, verified support service.
-  **Verify Support Claims:** Contact the company directly using official contact details from their website, not those provided by the scammer.
-  **Use Antivirus Software:** Keep your devices updated and protected with reliable antivirus software.
-  **Report the Scam:** If you encounter a tech support scam, report it to local authorities or the company being impersonated.



SCAM # 12**OTP SCAM****WHAT IT IS**

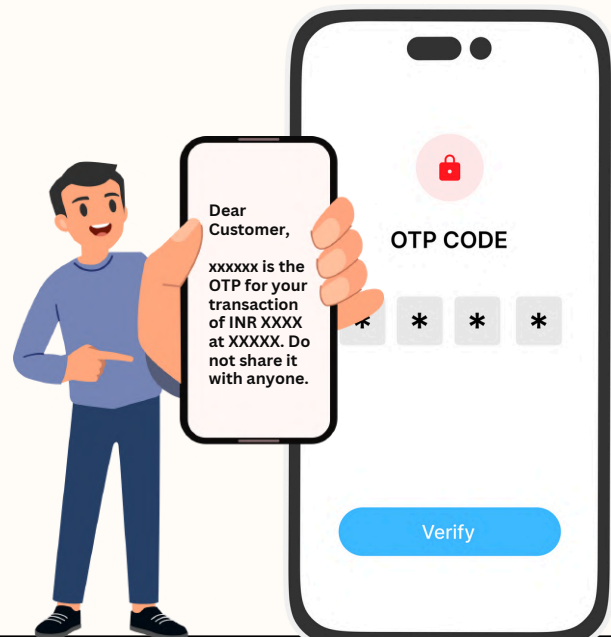
One Time Password (OTP) scam tricks you into revealing your OTPs to fraudsters. OTPs are typically used to verify your identity or authorisation for online transactions or logging into websites. These codes are usually sent via SMS or email, intended to be used only once.

HOW IT WORKS

Impersonation: Scammers impersonate legitimate services such as banks, e-commerce websites, parcel delivery services or other services providers through calls or emails.

False Sense of Urgency: Scammers create a false sense of urgency, clouding your judgement and pressuring you to share the OTP without verifying who the recipient is.

Theft of Money or Personal Information: Scammers use OTPs to access sensitive information like banking details or personal information for identity theft.





Remain Calm: Don't get sucked into the sense of urgency that is created, remain calm and trace your transaction history, verify the identity of the sender and exercise due diligence.



Be Cautious of Unknown Calls and Emails: Never share personal information or OTPs with someone who unexpectedly contacts you. Generally, only when you contact banks or other services that may require sensitive information do they ask for CVVs and other sensitive personal or financial information.



Verify Identity of the Sender: Before clicking on emails or links, verify the identity of the sender.



Exercise Due Diligence: Demand information from the caller about the exact purpose for the OTP and cross-check with your personal records if you've undertaken any such transactions, and whether they require you to share OTP over the phone or over a link.

SCAM # 13**REWARDS SCAM****WHAT IT IS**

Rewards scams trick you into sharing sensitive information under the guise of a reward.

HOW IT WORKS

Sharing Reward Communication: Scammers will send emails or SMS congratulating you for winning huge cash amounts or credit card points. It will direct you to click on a link to a website or for a fraudulent app.

It can look like: “**Dear Valued Customers, Your SBI NetBanking reward points (Rs 9980) will expire today! Now Redeem through SBI Reward App Install & claim your reward by cash deposit in your account**”.

Fake Websites: The website may seem legitimate and ask you to enter your personal or banking information. However, the data is accessed by scammers.

Fake Apps: Scammers can direct you to download seemingly legitimate apps such as ‘SBI Rewards’ to access the prizes. However, it is a malicious app and can access sensitive apps such as camera, microphone, contacts list, photos, messages and more.

Malicious Rewards: Alternatively, scammers can also state you’ve won a new phone, tablet or laptop. However, these devices are preinstalled with malicious apps or viruses that can steal your sensitive personal information, including banking data.



Be Cautious: Carefully read the contents of the message before clicking on links to claim any rewards and prizes.



Verify: Check with banks or other services if such a rewards programme is live. For instance, large companies that run rewards programmes would publicise it on their official websites.



Factory Reset: Factory reset any devices you receive as a gift or reward before inputting personal information. This is a good practice for any re-sale devices that you purchase as well.

SCAM # 14**SIM SWAPPING / SIM CLONING SCAM****WHAT IT IS**

SIM swapping, also known as SIM cloning, is when scammers duplicate your SIM card to take control of your phone number. Once they have access, they can bypass OTP-based security checks and steal money from your bank account.

HOW IT WORKS

Convincing Telecom Provider to Port Number: Scammers collect personal details using phishing emails, malware attacks, or data leaks. They then contact your mobile network provider, pretending to be you, provide fake ID proof and request a new SIM card, claiming the old one is lost or damaged.

Convincing you for SIM swap: Sometimes scammers try to make you activate a SIM swap. In this approach, the scammer makes a fake call to you posing to be an executive from your telecom provider. The scammer offers a better mobile subscription package and convinces you to share your 20 digit SIM number and press "1" to activate the offer. However, when you press "1", you end up authenticating the SIM swap on your number, and give control to the scammer.

Gaining Control: Once the provider issues a new SIM or completes the SIM swap, your original SIM is deactivated. The scammer gets access to your calls, messages and OTPs.

Financial Fraud & Identity Theft: Scammers use OTPs to transfer funds, reset passwords, and take over your financial and social media accounts.



Enable SIM Lock: Go to settings on your device and set up a SIM PIN to lock your SIM. Scammers will not be able to swap or deactivate your SIM without the SIM PIN.



Stay Alert to Network Issues: If your phone suddenly loses network while others have a signal, check with your provider immediately.



Be Careful about your Digital Footprint: Spend time reviewing your privacy settings on popular services like Google, Meta. You will know how much of your personal data is shared with third-parties.

SCAM # 15**IMPERSONATION SCAM****WHAT IT IS**

Scammers use hacking, stolen passwords and phishing techniques to impersonate your friend, relative or colleague, and then trick you into sending money. Since the messages appear to come from a known person, victims often fall for the scam.

HOW IT WORKS

Scammers hack into someone's social media account and message their contacts claiming an emergency.

Messages can look like: **“Hi, I’m stuck in Delhi where I was on vacation then was robbed. I need Rs 5000 urgently but anything you can spare me will be much appreciated, and I will refund you as soon as I am back. Please help”.**

Sometimes scammers create an email which looks similar to your colleague or boss's email ID. They write to you in an official tone, asking you to urgently send money to complete an important task.

Once you reply to the scammer on the hacked account / fake email, they ask you to transfer funds to a specific account or UPI handle. Scammers disappear and block the victim after money is sent to them.



Beware of Urgent Messages: Scammers create panic to make you act fast. Be careful about messages containing sudden urgent requests for money received on messaging apps, social media or email.



Verify Requests: Ensure you call the person directly or talk to a common friend / relative before acting on urgent requests for money.



Check for Red Flags: Does the message read like the way the sender usually communicates? Look out for unusual requests, odd grammar and formatting and requests to transfer money in new/unknown bank accounts.

SCAM # 16**SKIMMING MACHINE FRAUD****WHAT IT IS**

Skimming occurs when scammers install a hidden device in ATMs or handheld card payment machines to steal important card details like your card number, expiry date and three digit card verification value (CVV) on the back side.

These devices are often disguised to look like a normal part of the machine. Once the card details are captured, scammers create duplicate cards and make transactions from your account.

HOW IT WORKS

Placing a Skimmer: Fraudsters attach a device over the card reader of an ATM or swipe machine.

Capturing Card Data: When you insert your card, the skimmer reads your card details.

Recording PINs: A small camera or fake keypad records your PIN at an ATM.

Cloning & Fraudulent Transactions: Scammers use the stolen details to create duplicate cards and withdraw money.



Inspect ATM: Check for loose card slots, wobbly keypads or extra cameras at ATMs.



Be Careful: Always ask for the card swipe machine to be used in front of you and be careful about swiping your card at suspicious locations or machines.



Monitor Bank Statements: Regularly check your bank statements and SMS for unauthorised debit transactions.



Report Unauthorised Transactions to the Bank Immediately. You may be able to limit the loss if you inform your bank as early as possible.

SCAM # 17**FAKE WELFARE SCHEME SCAM****WHAT IT IS**

Scammers create fake portals that look exactly like websites for common schemes like PM Kisan Yojana, PM Awas Yojana, etc. Victims are lured to reveal their bank account, mobile number, and Aadhaar details to scammers.

HOW IT WORKS

Scammers call you saying that you are eligible to get funds under a social welfare scheme, but you need to first 'verify' or 'update' your bank details before the amount can be sent to you.

Scammers then ask you to share your bank account and debit card details to complete the 'verification' process. They finally ask you for an OTP to complete the verification.

But the scammer actually uses your bank and debit card details to set up a payment on your account, and the OTP is used to authorise the debit transaction. Once victims share the OTP, they realise that scammers have taken money out of their accounts.



Be Careful about Freebies: Scammers often promise freebies, tax rebates, or other incentives to lure you into sharing your personal and financial information.



Verify Government Websites: Use official portals for welfare schemes. Government websites usually have the extension ".gov.in" or ".nic.in" at the end.



Verify Scheme Details: Verify the details of any government schemes from your Gram Panchayat or Tehsildar office in your district.



Exercise Due Diligence: Read the message containing the OTP. Check if it looks legitimate, or if it's for something else. Refer to our Pro-tips on Page 38.

Do's and Don'ts

SAFE SURFING TIPS

- Periodically review the privacy settings on your browser and apps for messaging, social media, and maps to limit the information you share about yourself online.
- Ensure third-party and social media apps have limited access to the data on your device like photos and files, and device location.
- Memorise passwords or keep a physical record of them somewhere safe and secure. Make sure to routinely change your passwords and refrain from repeating passwords across different websites and apps.
- If you fall prey to a phishing scam where your bank or card details have been compromised, contact your bank and report it immediately.
- Keep location services turned off on your device unless necessary.
- If the investment scheme / job offer sounds too good to be true - it likely is.

ABSOLUTE NO-NOS

- Do not click on links from unknown origins on SMS / email or messaging apps without a careful reading.
- Do not share OTP, ATM or UPI Pin, and passwords on calls, SMS, online forms and emails.
- Do not download files (such as wedding invites) from unknown numbers on messaging apps.
- Do not accept friend requests and message requests from strangers on social media.
- Do not download and install pirated copies of software and media; they may contain malware.
- Be careful about transacting on unsecure websites (confirm that the web address starts with "https://" and not "http://").
- Be careful about entering CVVs for online transactions.

Pro Tips

1 Password hygiene

- Use a minimum of 16 characters with a mix of uppercase, lowercase, numbers and symbols.
- Avoid predictable patterns, personal information or sequential characters.
- Enable passkeys where possible. Passkeys use biometrics like fingerprints, face ID or voice recognition instead of traditional passwords.
- Set up multi factor authentication whenever available for additional security.

Weak passwords

Simple: Aditi1995 (name + birth year)

Sequential: abcdxyz123

Predictable: SalmanBhaiFan

Strong passwords

Personal: Maachbhaat&Dal92

Random words & multiple characters: C@rrOtcake&MnMs!

2 Understanding SMS codes

Fraudulent SMS messages are crafted to mimic genuine ones, often creating urgency to prompt quick action. Here's how to identify and safeguard yourself from such scams:

- Fake messages are often sent from personal mobile numbers or generic numerical IDs like 567678 or 909090.
- Genuine SMSs have the format [XY-ABCDEF]
 - X is the name of telecom service provider of the sender (Eg. J for Jio, A for Airtel and V for Vodafone).
 - Y is the name of the service area (Eg. D for Delhi, M for Mumbai and X for Karnataka).
 - ABCDEF refers to the code assigned to the sender (Eg. SPICEJ refers to Spice Jet).

.. continued

- **Illustrations:**
 - The SMS code 'AD-SHPRKT' means the sender is Ship Rocket, the sender's carrier is Airtel and the message is sent from Delhi.
 - The SMS code 'VM-SBIUPI' means the sender is State Bank of India, the sender's carrier is Vodafone and the message is sent from Mumbai.
- TRAI maintains a detailed list of service provider codes, telecom service area codes and assigned headers to businesses. Be sure to verify the authenticity of the SMS, especially before clicking on any link for payment.

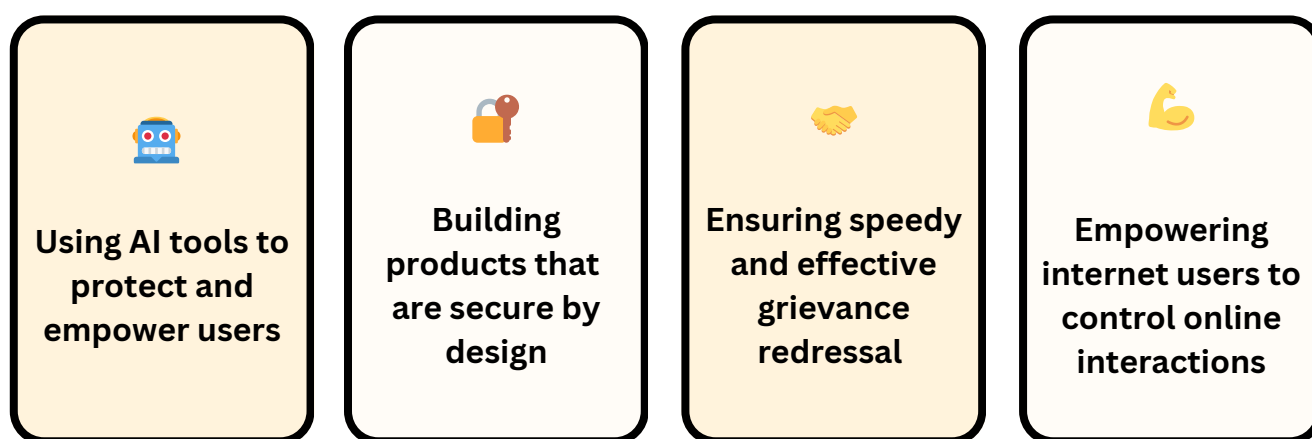
#3 Responding to scammers and fraudsters

- **Cut the call and block the number:** Do not respond to urgency or scare tactics adopted by unknown callers, even if they tell you they are bank or government representatives.
- **Report:** Get the scammer's number disabled by reporting it to 'Chakshu' on the 'Sanchar Saathi' portal (www.sancharsaathi.gov.in).
- **If you've already lost money:** Call your bank immediately and report the transaction. Also report the incident on the national cybercrime reporting portal (**dial 1930 or visit www.cybercrime.gov.in**).
- **Filter spam:** Dial 1909 and register for the spam blocking facility offered by your telecom provider as per TRAI directions.
- **Constant vigilance:** Follow the I4C on social media to keep up with the latest: (look up @CyberDost on X (twitter); CyberDostI4C on Facebook or @cyberdosti4c on Instagram).
- **Check your footprint:** Be mindful about the size of your digital footprint. Review how many companies you have given your data to. Ask them to delete your data if needed. Also, use free tools like 'www.haveibeenpwned.com' to find out if your data has been a part of any data breach.

Industry Best-Practices for User Safety

Ensuring user safety is an ongoing exercise. As digital spaces become ever more immersive, businesses must evolve their practices to inform, empower and protect users.

Four foundational principles for user safety are:



Use of AI to protect and empower users

AI (Artificial Intelligence) refers to an algorithm-based decision making system which can perform tasks that typically require human intelligence. For instance, natural language-based processing algorithms analyse text, image and video content to detect manipulated content and flag unusual activities or transactions.

What Indian authorities say

- **Spam filtering:** TRAI requires all telecom providers (like Airtel and Vodafone) to use AI for filtering out spam/pesky calls
- **Mule account monitoring:** RBI asks banks to collaborate with an AI model built by its subsidiary - RBI innovation hub (RBIH) - that help banks and financial institutions detect mule accounts being used by fraudsters and money launderers.

.. continued

- **International incoming spoofed calls prevention system:** DoT implemented a system to detect and block international spam calls that appear to be originating from India. As a result, international scammers who manipulate caller details to display Indian numbers “(+91 XXXXX XXXXX)” are automatically identified and blocked.



AI solutions in action

AIRTEL

Spam filtering

Airtel’s AI powered spam detection tool processes information such as usage patterns, SMS frequency, call duration etc. to identify spam calls and messages, in real time.

Flagging harmful messages

Airtel’s AI tools check various aspects of a text message, such as whether a link shared is blacklisted or not, for calling out if the message is suspicious.

TRUECALLER

AI Assistant

Truecaller AI Assistant screens calls using voice-to-text technology, inquires about the caller’s purpose, helping you identify spam calls and decide which calls to answer.

Search Context

Search Context flags suspicious activity in real-time, such as frequent name changes for phone numbers, enabling you to identify fraudulent callers.

Security by design

‘Security by design’ entails building technology products in a way that ensures you do not have to take additional steps to secure your device, data and network infrastructure.

Making products secure by design entails focusing on confidentiality, integrity and availability from the get-go.



Privacy-enhancing technologies (PETs) are key security tools that protect your data from unauthorised access. Techniques like encryption, anonymisation and secure computations are commonly used PETs.

These help balance the need for data utility with the need for privacy.

What Indian authorities say

- **Cloud services:** MeitY recommends businesses to implement security safeguards like ‘full disk encryption’ and ‘format preserving encryption’ to protect information while retaining the structure of data (like credit card number).

..continued

- **Financial services:** RBI requires banks and financial companies to:
 - **Mask Data:** Hide sensitive parts of information, like showing only the last four digits of a card.
 - **Use Multi-Factor Authentication** to add an extra layer of security, like CVV + OTP for online card payments.
 - **Adopt Strong Encryption:** Use tools that make it challenging for hackers to read data.

Security by design solutions in action

MICROSOFT

Zero-trust Model

Microsoft's Zero Trust model verifies, authenticates and encrypts every data access request as though it originates from an unsecure open network.

Secure Future Initiative

Security protections in Microsoft products are enabled and enforced by default, require no extra effort, and are not optional.

AIRTEL

Face Match

Airtel Payments Bank uses security algorithms which activate selfie-based facial recognition verification if the threat of identity theft or fraud is detected.

Identifying International Numbers

Airtel implements a technical solution that displays "International Call" for all calls received from outside the country.

This enables you to easily identify international calls and helps you distinguish between expected calls and potential fraud or spam.

META

End-to-End Encryption

WhatsApp ensures only the sender and the recipient can access messages, calls, photos and videos.

Limited Data Collection

WhatsApp stores only essential data, like phone numbers and avoids storing message content or location data by default.

Grievance redressal channels for users

Clear and simple grievance redressal mechanisms allow users of digital services like you to get timely recourse for issues you may face while engaging with digital businesses. Businesses address issues like delay in delivery of your e-commerce purchase, or problems with paying for a cab ride through grievance redressal channels.

Mechanisms for grievance redressal

- **Sanchar Saathi:** The Department of Telecommunications (DoT) offers various initiatives to help you combat telecom frauds. The Sanchar Saathi initiative allows you to:
 - report suspected fraud communications on Chakshu (visit www.sancharsaathi.gov.in/sfc/);
 - identify and manage all mobile connections issued in your name; and,
 - report lost/stolen mobile handset so that they can be blocked, traced and recovered.
- **Financial sector watchdog:** RBI's integrated ombudsman scheme creates a centralised grievance redressal mechanism, allowing you to complain against banks, payment service providers, credit bureaus and other financial institutions to the RBI.

..continued

- **Consumer helpline:** The Department of Consumer Affairs (DoCA) offers you multiple channels to resolve grievances against businesses and service providers: such as a WhatsApp-integrated helpline number (8800001915), the National Consumer Helpline web portal (www.consumerhelpline.gov.in), and the UMANG App.
- **Intermediary guidelines:** MeitY requires digital platforms like social media and gaming companies to set up grievance redressal mechanisms and address consumer complaints in a time bound manner. If you are not satisfied with the company's grievance redressal process, you can file an e-complaint to the Grievance Appellate Committee (GAC) appointed by the government.

👉 Grievance redressal channels in action**VODAFONE IDEA (VI)****Specialised Helplines**

Vi offers specialised helplines based on your different requirements such as mobile number portability, data activation, etc.

My VI App

The MyVi app allows you to access various product and security options. You can opt for the do-not-disturb (DND) facility, complain against telemarketers and make service requests and complaints to customer care executives.

AIRTEL**Airtel Thanks App**

The Airtel Thanks app allows you to manage/block unwanted numbers, report malicious activity and opt for the do-not-disturb (DND) service to avoid marketing messages.

Two-tier Appellate Authority for Grievances

Incase a you are dissatisfied with the resolution, you appeal before a service area based appellate authority within 30 days.

Alerts and tools to empower internet users

Businesses integrate design features into their apps and digital services that help you keep an eye on your data, adjust privacy and security settings and stay informed.

This helps you to check and control how your information is being shared to third parties, decide what information to share and what to keep private, and be notified of suspicious activity, like someone trying to access your account.

What Indian authorities say

- **Transaction notifications for recurring payments:** RBI mandates banks to issue notifications at least 24 hours before processing recurring payments, such as subscriptions or systematic investment plans.
- **Itemised privacy notices:** The Ministry of Electronics and Information Technology (MeitY) requires businesses to be clear and specific about what kind of personal data they are collecting from you, and the purpose of collection.
- **TRAI rules to combat spam/pesky calls:** TRAI mandates companies sending bulk texts containing links to apps and websites to register their content with telecom providers. This ensures only verified and whitelisted links and attachments are disseminated to the public in promotional messages.
- **Protection against dark patterns:** The Department of Consumer Affairs (DoCA) says that deceptive design patterns used by businesses can be seen as an unfair trade practice.
 - Examples of deceptive designs include apps with complex user interfaces (UI) that makes it difficult to cancel a recurring transaction, or apps which add hidden charges and extra fees just before checkout.
 - If you see such deceptive designs in action, you can complain to the DoCA by dialing 1915 or visiting the INGRAM portal (www.consumerhelpline.gov.in/user/).

Tools to empower internet users in action

MICROSOFT

Copilot Controls

You can set preferences, view, edit or delete data and manage conversation histories on Copilot.

Privacy and Reporting on Skype

You can report harmful messages, block or report suspicious messages on Skype.

META

Privacy Center

You can adjust settings to manage and control your privacy on Facebook, Instagram, Messenger and other Meta products.

WhatsApp Privacy Controls

You can customise who sees your profile photo, last seen details and also lock chats on WhatsApp.

TRUECALLER

Caller ID

Truecaller's Caller ID goes beyond showing names—it provides caller location, community ratings, and fraud alerts. Suspicious calls are flagged with labels like "Spam" or "Fraud Alert," helping you make informed decisions.

Verified Business IDs

Truecaller adds a tamper-proof name, green badge, and logo to business calls, preventing impersonation scams and helping you distinguish genuine callers from fraudsters.



Visit: www.saferinternetindia.com
Write to us at secretariat@saferinternetindia.com



Safer Internet India



@saferinternetindia



SaferInternetIN



@SaferInternetIndia