
A Handbook on
STAYING SAFE ONLINE
APPROVED
ERROR
An initiative by
SAFER INTERNET INDIA

A Handbook on

Staying Safe Online

February 2026

Design & Illustration
Akansha Sain and Sejal Girme

Note to Reader

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.

This is the second edition of the handbook. It builds on our earlier work to reflect emerging risks, new scam patterns, and recent developments in the digital landscape.

Thank you for reading.

Safer Internet India.

What's Inside

Common scams and frauds

We break down various tactics employed by scammers, to help you stay alert and aware

Safe surfing tips

We put together a list of do's and don'ts for staying safe in today's immersive internet

Pillars for trust and safety

We discuss four pillars to engender trust & safety online

Industry best practices

We discuss best practices from leading technology firms that make the internet a little bit safer for all of us

Table of Contents

Introduction

Digital spaces continue to shape nearly every aspect of our lives. With over a billion internet users, Indians go online every day to work, learn, communicate, and access goods and services ranging from household essentials to entertainment, investments, and financial products. As digital adoption deepens and diversifies, so do the risks. Users must remain mindful of who they interact with and what they share or transact online. The online world is still rife with offers and opportunities that appear too good to be true and, all too often, are.

The scale and sophistication of online scams have increased markedly since the first edition of this handbook.

In 2024 alone, Indians reportedly lost over ₹22,000 crore to online fraud, with cybercrime complaints continuing to rise through 2025. Fraudsters are increasingly organised, technologically adept, and quick to exploit new platforms, payment systems, and moments of vulnerability.

At the same time, gaps in digital literacy persist. Government surveys continue to show that a significant proportion of internet users lack basic digital skills, from sending emails to safely carrying out online financial transactions. These gaps are more pronounced in rural areas and among women, elderly, reinforcing the reality that online scams are not merely a technological issue, but a societal challenge. Without targeted awareness and capacity building, a large section of India's population remains at risk.

The Government of India has intensified efforts to address this growing threat. The Ministry of Home Affairs and the Ministry of Electronics and Information Technology, along with specialised bodies such as the Indian Cyber Crime Coordination Centre (I4C) and the Indian Computer Emergency Response Team (CERT-In), continue to strengthen mechanisms to prevent, investigate, and respond to online fraud. Regulators including the Reserve Bank of India (RBI) and the Telecom Regulatory Authority of India (TRAI) are also leveraging technology and regulation from AI-based detection of mule accounts to distributed ledger technology–enabled registration of telemarketers to curb misuse and protect users.

Yet, the sheer scale, speed, and evolving nature of online scams mean that institutional action alone cannot fully address the problem. Ensuring online safety requires sustained collaboration across government, industry, civil society, and citizens.

This second edition builds on the foundations of the first, reflecting new trends, emerging risks, and lessons learnt. It reaffirms a simple but urgent message: keeping Indians safe online will require shared responsibility, continued vigilance, and collective action.

Report suspicious calls and scams to the cybercrime helpline number 1930 or on the website www.cybercrime.gov.in.

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.

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.

SCAM

An online scam is when someone deliberately deceives you on the internet to steal your money, personal information, or other sensitive data. Scammers often pretend to be trustworthy by posing as government officials, banks, companies, or even friends, and may promote fake offers, urgent warnings, or too-good-to-be-true deals. Their messages are designed to look real and create pressure so you act quickly without thinking.

A scam is a form of online fraud, but not all frauds are scams. Scams rely on manipulation, convincing people to voluntarily share money or information, such as claiming a fake prize or refund. Fraud can also include wider criminal activities like identity theft, account takeovers, or hacking. Staying alert while chatting online, visiting websites, clicking links, or downloading apps is essential to staying safe.

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.

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 and share sensitive information. An example of a phishing email is when the scammer pretends to be a colleague and sends you an email asking for money.

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.

SPAM

Spam is unwanted junk communication via phone, email, text, or social media. While often used for advertising, it can also be an attempt to steal your information or money. For example, a fake “Congratulations! You’ve won a ₹1,000 gift card!” message is a common scam. Clicking such links can lead to fraud or device infection. Modern spam is increasingly sophisticated and tailored to your professional or personal interests.

AI Deepfakes & Voice-Cloning

What is it?

AI (Artificial Intelligence) generated deepfake and voice-cloning scams are when scammers use AI to pretend to be real people, such as family members, colleagues, friends, or public figures. They exploit trust and create a sense of urgency to deceive victims into sharing money, personal information, or sensitive data. Because the impersonation can sound or look real, these scams can be very convincing and difficult to detect.

How does it work?

Scammers use AI to create fake content

Scammers collect short audio clips, photos, or videos of a person from social media, public appearances, or online content. Using AI tools, they clone the person's voice or create realistic fake videos that look and sound real.

Fake Call or Messages

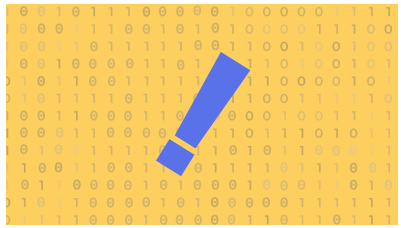
They then contact you by phone, video, or message pretending to be someone you trust, such as a family member, colleague, senior official, or well-known public figure.

Urgency and exploitation

They create urgency by claiming an emergency, legal issues, or a limited-time opportunity. If you respond, scammers use what you share to steal money or misuse your details.

Report suspicious calls and scams to the cybercrime helpline number 1930 or on the website www.cybercrime.gov.in

Helpful Tips



Be wary of urgency

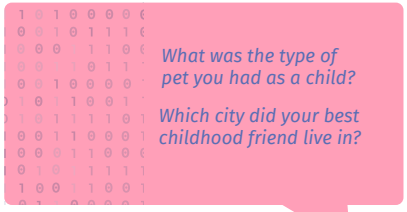
Scammers often pressure you to act quickly. Take your time to think and verify before doing anything.

Pause and verify

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

Watch for visual cues

Be alert to unnatural facial movements, mismatched lip-sync, or odd pacing in videos.

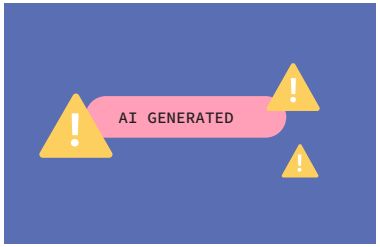


Ask personal verification questions

Use random or private details only the real person would know (e.g., a childhood pet's breed or a family detail).

Check platform labels

Look for AI-generated content tags on social media platforms. There are tools which embed imperceptible watermarks to alert users - read the industry best practices on page 62 for more information.



APK Scam

What is it?

An APK (Android Package Kit) file is a file format used to install applications on Android devices. While APK files can be legitimate, scammers often use fake or modified APK files to spread malware. Installing APK files from unknown sources can give scammers access to your device, allowing them to steal information or take control of the device.

How does it work?

01 Scammer makes contact

A link is shared with a message claiming it to be something that needs immediate action, like a traffic challan, tax notice, or limited-time offer.

02 Unverified app

When you click the link, you are asked to download and install an APK file. The app looks real but does not come from the official app store.

03 App asks for permissions

After installation, the app requests access to SMS, calls, contacts, camera, microphone, or screen sharing. Many users allow these permissions to make the app work.

04 Access to sensitive information

Once permission is granted, criminals can access OTPs, access banking apps, and remotely control the victim's phone without their knowledge.

Helpful Tips

Stick to Official App Stores

Download apps only from official app stores, such as the Google Play Store.

Check app details carefully

Review ratings, number of downloads, and the developer's name.

Control App Permissions

Limit app permissions and deny access that seems unnecessary.

Be Cautious of Links and Files

Avoid clicking on links or downloading files shared via WhatsApp, SMS, email, or social media especially messages that create urgency.

Fake Websites

What is it?

A fake website is a fraudulent website created by scammers to look identical to legitimate websites such as popular e-commerce platforms, religious institutions collecting donations, resorts, hotels, or travel booking services. These websites have no genuine business or service behind them and are designed to trick users into paying money or sharing sensitive information.

How does it work?

01 Lookalike Website or Ad

Scammer design and operate website and online advertisement that closely resembles a trusted e-commerce platform, donation portal, resort, hotel, or travel booking service. The website uses familiar logos, layouts, colours, and language to appear authentic.

02 False Offers or Requests

The website promotes attractive shopping deals, discounted travel packages, urgent donation appeals, or limited-time offers. Users are encouraged to act quickly before the offer expires, creating pressure to proceed without verifying the website.

03 Payment or Data Capture

Once you continue, the website asks for personal or financial details such as your name, address, phone number, card details, or bank information. In many cases, you are asked to make payments through direct bank transfers, QR codes, or gift cards instead of secure payment gateways.

04 Money or Information is Lost

After the payment is made or information is shared, no goods are delivered, no bookings are confirmed, and no donation receipts are issued. The scammers misuse the collected information for fraud or disappear with the money.

Helpful Tips

Use trusted platforms

Access e-commerce sites, donation portals, and booking platforms only through official apps or verified websites. Check URLs carefully for spelling or domain errors.

Avoid unsolicited links

Do not click on links received via unknown emails, SMS, WhatsApp messages, or social media ads.

Research the vendor

Check seller credentials: review ratings, feedback history, and return policies.

Use secure payments

Avoid direct bank transfers, gift cards, or QR payments to unknown websites.

Too good to be true

Be cautious of heavy discounts, urgent appeals, or limited-time offers on unfamiliar websites.

Account Pairing Scam

What is it?

An account pairing scam is when scammers exploit the companion device or “Linked Devices” feature of messaging apps to secretly access a user’s account. Once the account is paired, scammers gain silent access to chats, contacts, media, and call logs, often without triggering any alerts. The victim may not realise their account has been compromised until the damage has already been done.

How does it work?

01 Deceptive Contact

Scammers reach out through unsolicited messages, pretending to be trusted contacts, service providers, or authorities. These messages are designed to look urgent and by claiming security issues and verification requirements.

02 Malicious Link or Request

You may get a link disguised as a verification, or a device-pairing request. Victims are also tricked into sharing one-time verification codes, allowing the scammer to link their companion device.

03 Account “Rental” Trap

Younger users are often targeted with offers of easy or passive income in exchange for “renting out” their WhatsApp or messaging accounts. Once access is given, scammers take full control of the account.

04 Silent Account Misuse

Once linked, scammers can monitor conversations in real time and misuse the account to carry out fraud. Victims may face data theft, financial loss, reputational damage, or legal trouble.

Helpful Tips

Regularly review Linked Devices

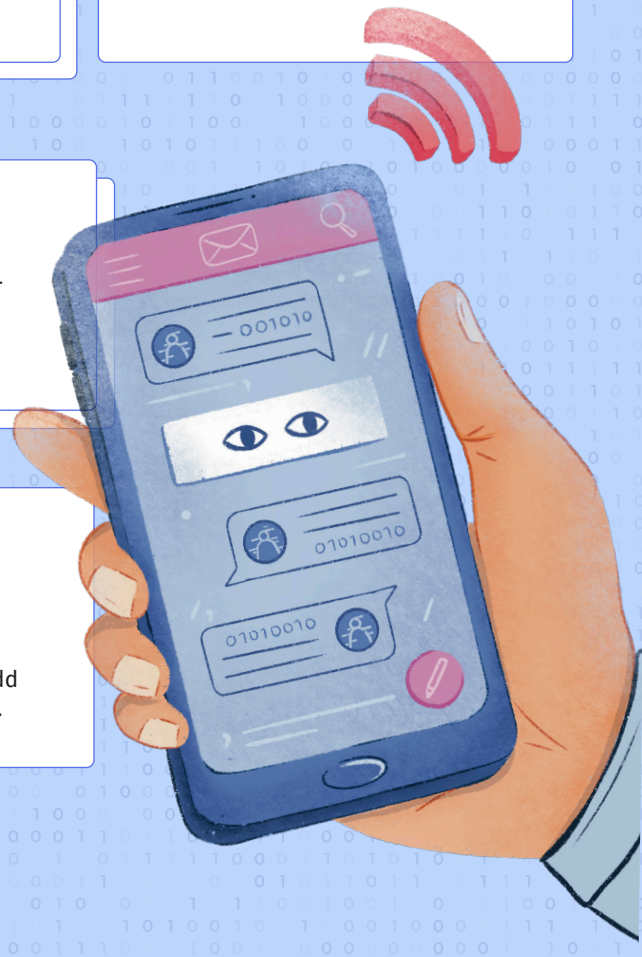
Go to WhatsApp Settings > Linked Devices and log out of any unknown devices.

Avoid “Easy Money” Offers:

Be wary of “easy money” offers involving account access or rentals.

Never Share One-Time Codes

Do not share verification codes or approve pairing requests you did not start yourself.



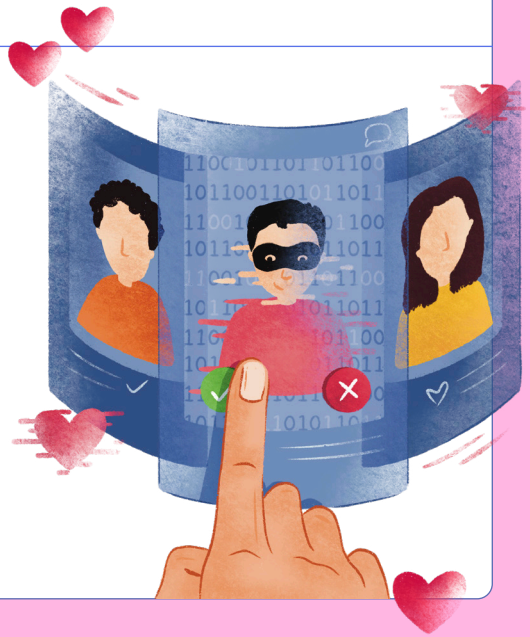
Turn on Two-Step Verification

Enable two-step verification to add an extra layer of account security.

Dating App Scam

What is it?

A dating app scam occurs when scammers use online dating platforms to deceive people into giving money, favours, or personal information. These scams often take the form of quick meet-up frauds or longer-term emotional and financial manipulation, exploiting trust built through online interactions.



How does it work?

Initial Contact and Trust Building

The scammer matches with you on a dating app and quickly builds rapport through friendly or romantic conversations. They may appear attentive, charming, and eager to connect, creating a sense of trust in a short period of time.

Short-Term Meet-Up Scam

After matching, the scammer arranges a date at a complicit venue, orders expensive items, and leaves abruptly, leaving the victim with an inflated bill and pressure from the establishment to pay.

Long-Term Relationship Scam

The scammer builds trust over time, gathers sensitive information, then exploits it to demand money, make repeated financial requests, or threaten blackmail and extortion, while victims often hesitate to report due to embarrassment and social pressure.

Helpful Tips

Be Cautious of Rushed Meetings

Be wary if someone insists on meeting quickly at a specific location they choose.

Research the Cafe or Restaurant Suggested by the Other Person

Look up the cafe/restaurant 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.

Report Suspicious Behaviour

If you suspect foul play, inform the police and the dating app to prevent others from being scammed

Slow Down on Emotional Conversations

Be cautious of fast emotional bonding or pressure to share personal information.

Trust your instincts

If you feel uncomfortable, pressured, or unsafe at any point, leave immediately.

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 the National Cybercrime Helpline by dialling *1930*. You can also visit the National Cybercrime Reporting Portal at *cybercrime.gov.in* to register your complaint online.

Digital Arrest

What is it?

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.

Threats and Pressure

The scammer says you’ll face serious consequences, like jail time, if you don’t pay immediately.

Use of Fake Police Identity

Scammers will try to look legitimate, showing fake letterheads and IDs, and wearing police uniform during video calls.

Isolation and Urgency

The scammer pressures the victim to isolate themselves. They maybe told to to travel to a remote location or lock themselves in a room and draw the curtains. They may also be instructed to avoid taking other calls.

Relentless Payment Demands

They make repeated demands for money, often asking victims to transfer funds to multiple accounts so the payments cannot be traced.

Example

A common tactic involves a fake customer-service call. For example, you may receive a call claiming to be from a parcel delivery company and be asked to press a number for support. Once connected, a fake representative alleges that a package linked to you contains illegal substances and that an arrest warrant has been issued. The call may then escalate into a video call, where multiple scammers pose as police officers or investigators

Helpful Tips

Stay Calm

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

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.

Verify the Claim

Contact the official organisation using their official phone number or website, whether it be the police or the organisation whose customer service representative called you.

Be Careful

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

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.

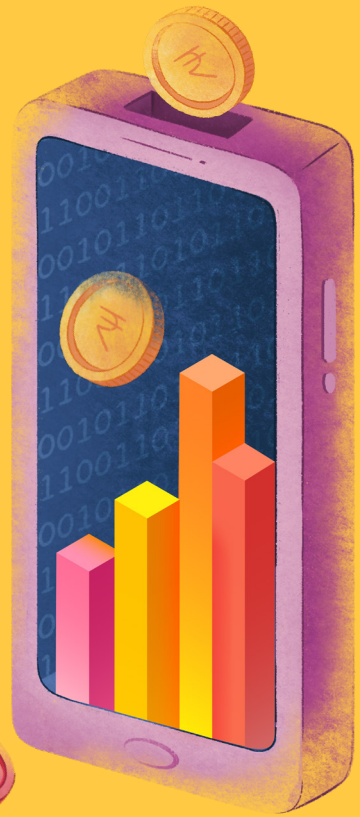
Do Not Make Payments

Genuine law enforcement will never ask for money over the phone. Refuse all such demands.

Investment Scam

What is it?

Investment Scams are where scammers create fraudulent trading or investment applications that appear legitimate. These apps promise high returns with low risk, but are designed to steal money from you. 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 you with promises of abnormally high financial returns. Often, victims are added to WhatsApp groups by scammers that have legitimate sounding names such as “ICICI IR Team” make you think they are licensed financial institutions.

Instructions to Download Fake Apps and Invest

You are instructed to download fraudulent apps that appear to offer genuine investment opportunities. These apps display names of well-known stocks and financial instruments. The app is designed to look real, with fake charts, account balances, and profit statements.

Fabricated Display of High Returns

After investing, you may see seemingly strong “returns” that encourage further deposits, but these figures are fake. When withdrawals are attempted, extra charges are demanded, before the app ultimately disappears and the investment is lost.

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.

Helpful Tips

make ₹50,000 in 3 days!

Be wary of unwanted/unexpected messages that you have not asked for offering quick money through online investments.

Turn ₹5,000 into ₹50,0000

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.

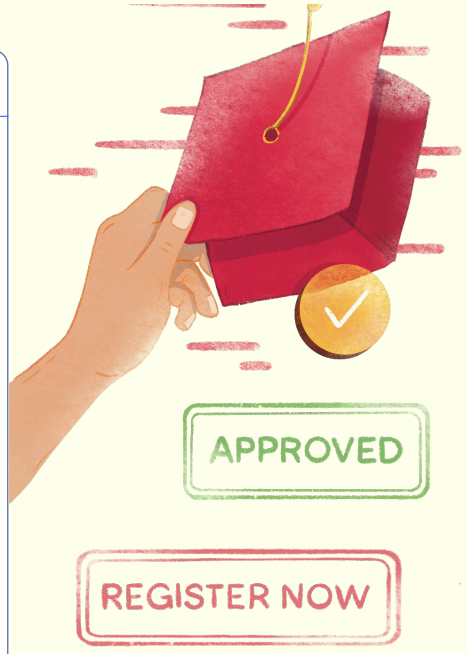
Do not share login credentials, personal, or financial information with strangers, especially on messaging apps.

Avoid downloading unknown apps or files at the request of unfamiliar contacts.

Fake Job Offer

What is it?

A Fake Job Offer Scam is a type of fraud where scammers pose as employers or placement agencies to trick job-seekers into paying money or sharing personal information.
These scams often target people actively looking for work by promising high salaries, easy tasks, quick hiring, or guaranteed placement.



How it works

Attractive Job Post

Scammers create job ads on websites, social media, or message you directly impersonating placement agencies.

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 (for international jobs).

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.

Types of fake job scams

Work-from-Home Scams

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

Victims are hired as "quality control managers" or "logistics coordinators" and asked to receive, repackage, and reship goods bought with stolen credit cards. Salaries are never paid, and victims may unknowingly participate in criminal activity and identity theft. If you provided personal details for "payroll," you could also face identity theft.

Reselling Merchandise Scams

Victims are asked to buy luxury products upfront to resell at a profit. The items never arrive or turn out to be worthless.

Personal assistant / caregiver scams

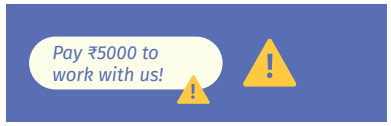
Scammers post fake job ads for nannies, caregivers, and virtual assistants on job sites. Or they may send emails that look like they're from someone in your community. The message might also seem to come from someone who is part of an organisation you know, like your college or university.

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.

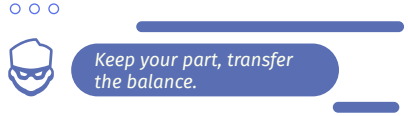
Job Placement Service Scams

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.

Helpful Tips



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.

Fake Link/ QR Code

What is it?

A Fake Link / QR Code Scam is a type of cyber fraud that tricks people into clicking malicious links or scanning fraudulent QR codes. These scams are designed to steal personal or financial information, capture 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 trigger harmful actions (e.g. installing malware). These codes are sent digitally or placed on posters and ads. Scammers also take legitimate ads and replace the real QR code with a fake one.

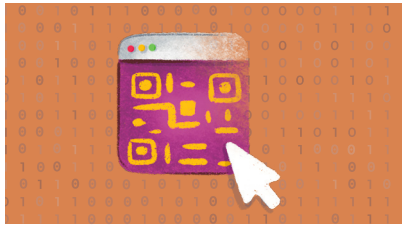
Common examples include:

- Fake bank or service-provider websites that ask you to update KYC information.
- Fraudulent payment links or QR codes that trick users into entering credit card details or UPI PINs.
- QR codes on posters or ads promising discounts or rewards but leading to phishing websites.

Helpful Tips

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.

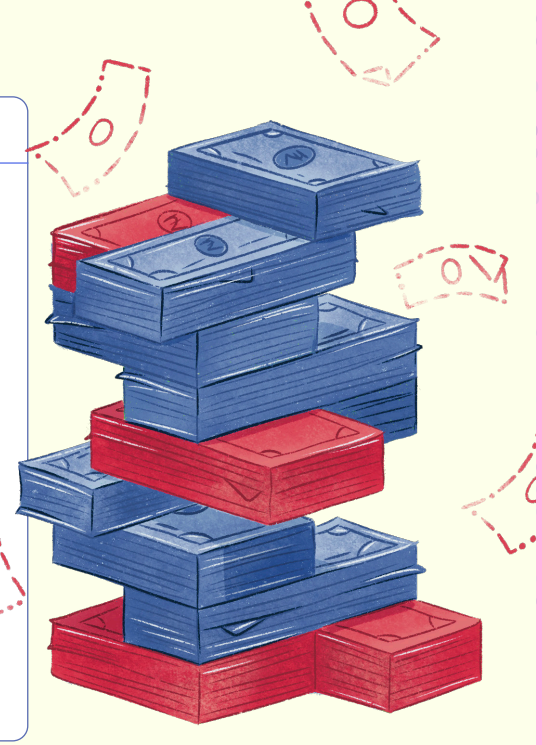
Always verify the name of the intended recipient when making QR code payments.

When asked for your KYC, verify the purpose of KYC and the identity of the person requesting such information.

Fake Loan App

What is it?

A Fake Loan App Scam involves fraudulent mobile applications that promise quick and easy loans with minimal paperwork. These apps typically target people in urgent need of money and trick them into paying fees or sharing sensitive personal data. They often hide excessive charges,and extremely high interest rates.



How does it work?

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.

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.

Upfront Fees

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

Harassment

If you fail to pay, scammers use the stolen data to harass you. For instance, they may access your photos under the excuse of conducting video-KYC and blackmail you using that.

No Loan Disbursed

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

Helpful Tips

Verify partnerships

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.

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.

Red Flags

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

Contact Information

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

Be Cautious with Permissions

Avoid apps that ask for unnecessary access to contacts, photos, or messages.

Upfront Fees

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

Interest Rates

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

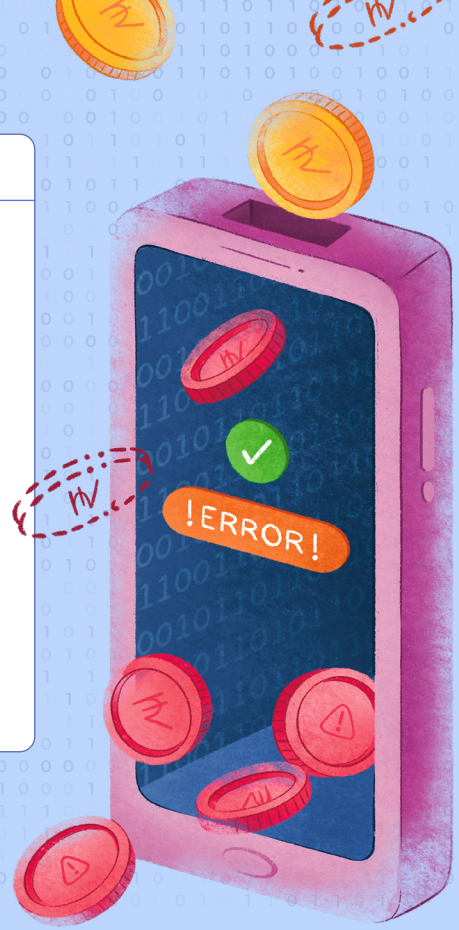
Report Suspected Fraud

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

Fake Mobile Recharge

What is it?

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 does it work?

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.

Phishing Links

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

Stealing Information

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

Payment for Recharge

You may pay the recharge via the fake platform, but no recharge is actually done.

Helpful Tips

Use Trusted Platforms

Only recharge through your mobile provider’s app or the application that is linked to your UPI.

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.

Beware of Unrealistic Offers

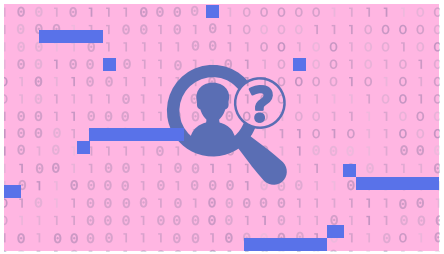
Ignore deals that seem too good to be true, like massive discounts or free recharges.

Verify Websites and Apps

Check the URL for fake or misspelled names and download apps only from official app stores.

Report Suspicious Activity

Inform your telecom provider or local cybercrime helpline if you encounter a scam.



Parcel Delivery Scam

What is it?

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 does it work?

01 Fake Notifications

You receive messages claiming a package arrived but delivery failed due to incomplete address or payment. It may appear to be from a trusted courier company like FedEx or DHL.

02 Phishing Links

The message includes a link to update your address, confirm delivery, or pay a fee. Clicking it leads to a fake website designed to steal your sensitive details

03 Follow up Call & Urgency

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

04 Payment Trap

You're asked to pay a fee for re-delivery, and they only accept debit or credit card payments.

05 No Delivery

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

Helpful Tips

Recall if You Placed an Order

Try to recall if you actually have a package on the way or if someone else may be ordering an item to you.

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.

Disguised Malware

What is it?

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 does it work?

Placement on Websites

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

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).

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

Helpful Tips

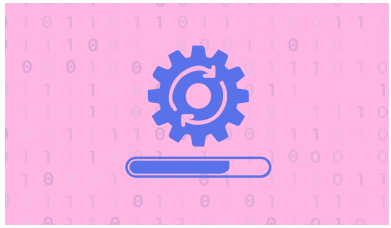
Avoid Suspicious Links

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

SECURITY FEATURES

Enable Security Features

Use antivirus software and browser security settings to detect and block threats. Some antivirus software comes 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.



Keep Software Updated

Ensure your browser and security software are up to date to block malicious ads.

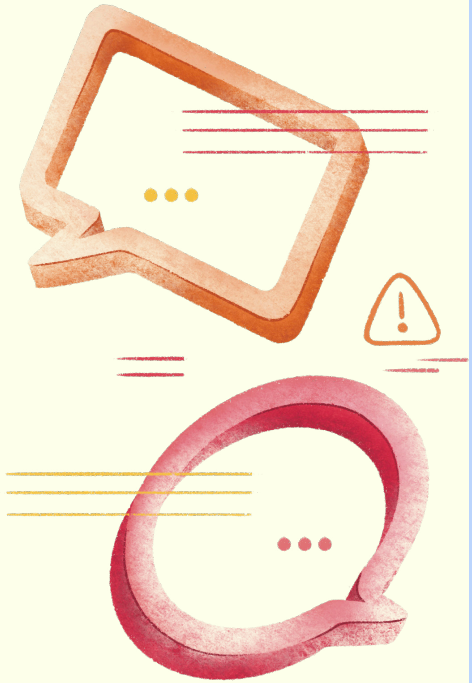
Stick to Trusted Websites

Avoid visiting or interacting with suspicious 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.

Tech Support Scam

What is it?

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 does it work?

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 to 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.

Helpful Tips

Ignore Pop-Ups

Close any suspicious pop-ups, and don't call the numbers displayed. Use antivirus software to scan your device instead.

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

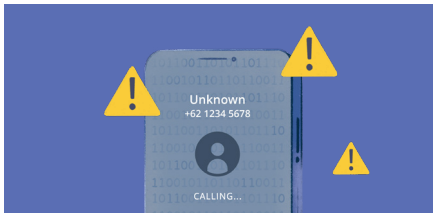
If you encounter a tech support scam, report it to local authorities or the company being impersonated.

Never Give Remote Access

Don't let anyone remotely control your device unless you've contacted a trusted, verified support service.

Do not trust unsolicited calls

Make sure the person you are talking to is from an official channel, and contact the company directly to be sure. Read the pro-tips on page 59 for more tips like this.



OTP Scam

What is it?

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 does it work?

01 Impersonation

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

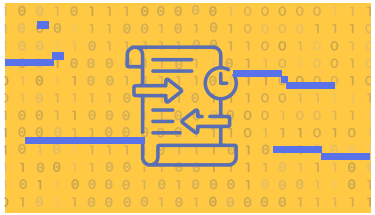
02 False Sense of Urgency

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

03 Theft of Money or Personal Information

Scammers use OTPs to access sensitive information like banking details. This can allow them to carry out fraudulent transactions, change account settings, or misuse personal information.

Helpful Tips



Remain Calm

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

Verify Identity of the Sender

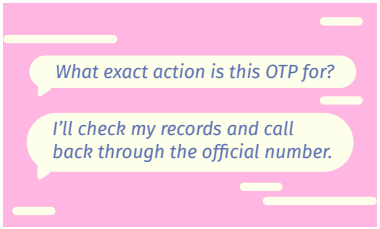
Before clicking on emails or links, verify the identity of the sender.

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.

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.



Rewards Scam

What is it?

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

How does it work?

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.

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.

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.

Helpful Tips:

Be Cautious

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

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.

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.

Sim Swapping

What is it?

SIM swapping 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 does it work?

01 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.

02 Convincing you for SIM swap

Scammers pose as a telecom executive and trick you into sharing your SIM number and authenticating a SIM swap. Your old SIM is deactivated, and the scammer gains control of your phone number, calls, messages, and OTPs

03 SIM Jacking

Scammers may also attempt to hijack your SIM card through malware or spyware installed on your phone if you click on suspicious links. Once this malicious software gets into your device, it can secretly access SIM-related information, monitor your activity, and gradually take control of your number.

04 Financial Fraud & Identity Theft

Once they gain control of your number, scammers use OTPs to transfer funds, reset passwords, and take over your financial and social media accounts.

Helpful Tips:

Stay Alert on communications from your Service Provider

For any SIM swap / eSIM upgrade, your service provider sends you intimation about the request. Immediately contact them in case you did not initiate such a request.

Avoid using public Wi-Fi when accessing SIM information

Do not access SIM information or manage your mobile account when using public Wi-Fi as attackers can easily compromise unsecured networks.

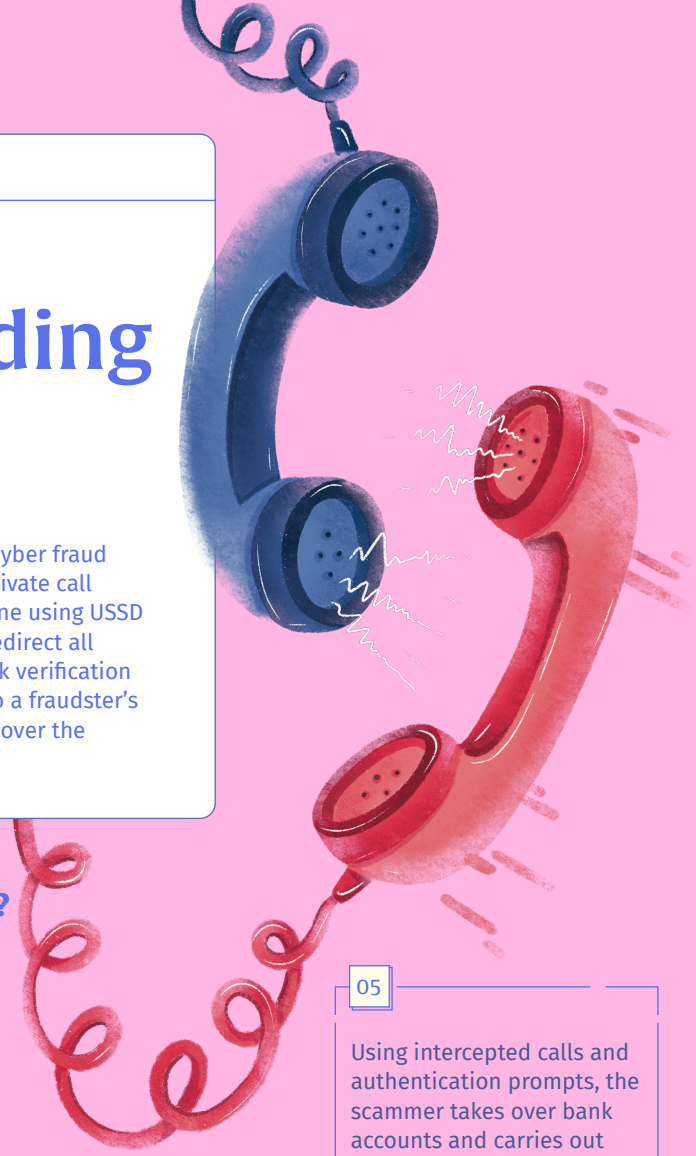
Keep your SIM card details confidential

Always keep your SIM card details such as ICCID (Integrated Circuit Card Identifier) or IMSI (International Mobile Subscriber Identity) number with anyone. Your service provider does not need this information.

Call Forwarding Scam

What is it?

A Call Forwarding Scam is a cyber fraud where scammers secretly activate call forwarding on a victim's phone using USSD codes. This allows them to redirect all incoming calls including bank verification calls and OTP-related calls to a fraudster's number, giving them control over the victim's accounts.



How does it work?

01 Scammers impersonate courier or delivery service agents, claiming there is an issue with a package.

02 Victims are asked to dial a short USSD code (often starting with symbols like * or #) to "confirm" or "reschedule" delivery.

03 Dialling the code silently activates unconditional call forwarding on the victim's phone.

04 All incoming calls, including OTP and bank verification calls, are diverted to the scammer.

05 Using intercepted calls and authentication prompts, the scammer takes over bank accounts and carries out unauthorised transactions.

Warning signs often appear late:

- Their phone suddenly stops receiving calls
- Callers say the phone is unreachable
- Bank alerts or OTP-related messages are missed or delayed

Helpful Tips:

Do not trust unsolicited calls or messages

Especially those asking you to act urgently.

Do not dial USSD codes

These are numbers starting with *21*, *61*, *67*, or similar prefixes. Only do this on the advice of a verified technician or support professional.

Verify delivery issues

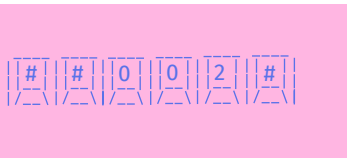
Do this directly through official courier apps or customer-care numbers.

Check your phone's call-forwarding settings

Do this regularly, especially if calls suddenly stop reaching you.

Cancel call forwarding settings

If you suspect unauthorised call forwarding, immediately dial ##002# to cancel all call-forwarding settings.



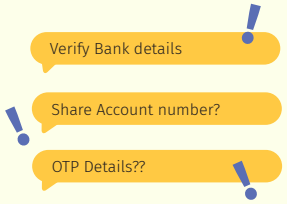
Fake Welfare Scheme

What is it?

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 does it work?

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. You are then asked to share your bank account, debit card details, and an OTP to complete the 'verification' process.



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.

Helpful Tips

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 59.

Impersonation Scam

What is it?

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 does it work?

Scammers hack into someone's social media account and message their contacts claiming there is an emergency. Messages can look like:

"Hi, I'm stuck in Delhi where I was on vacation and was robbed. I need ₹5000 urgently, but anything you can spare will be much appreciated. I will refund you as soon as I am back. Please help."

fakebutlookslegit_email.com

Sometimes, scammers create an email address that looks like your colleague's, and write to you in an official tone. Once you reply to the fake email, they may ask you to transfer funds to a specific bank account. After the money is sent, scammers disappear and block the victim.

Helpful Tips

Beware of urgent messages

Scammers create panic to make you act fast. Be cautious of sudden requests for money received on messaging apps, social media, or email.

Verify requests

Call the person directly or check with a common friend or relative before acting on urgent requests for money.

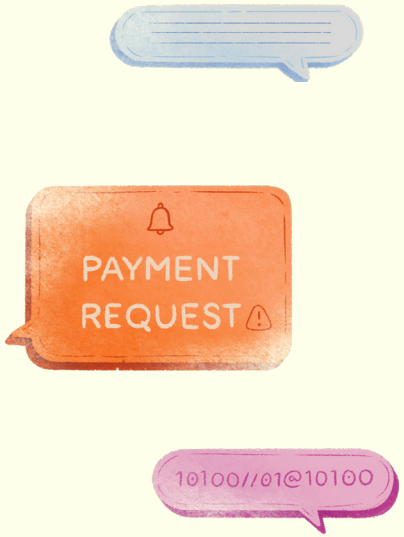
Check for red flags

Does the message sound like how the sender usually communicates? Watch out for unusual requests, odd grammar or formatting, and requests to transfer money to new or unknown bank accounts.

UPI Collect Request Scam

What is it?

A UPI Collect Request scam is where fraudsters send you a payment request through UPI apps. Instead of you receiving money, you are tricked into authorising a transfer from your account to theirs.



How does it work?

01 Misleading Payment Requests

Scammers send a UPI collect request and claim it is for receiving a refund, prize money, salary, or reimbursement. They tell you to approve the request to get the money credited.

02 False Authority and Identity

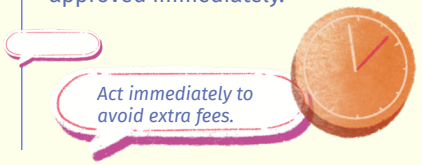
Fraudsters may pose as buyers, sellers, bank officials, customer care executives, or delivery agents to appear legitimate.

03 Request for UPI PIN

Victims are instructed to enter their UPI PIN to receive the money. However, entering a PIN always authorises a payment.

04 Urgency and Pressure

Scammers push victims to act quickly by claiming the request will expire or that the money will be reversed if not approved immediately.



05 Loss of Money

Once the collect request is approved and the PIN is entered, money is transferred from the victim's account to the scammer's account.

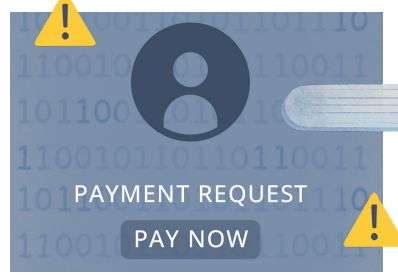
Helpful Tips:

Know the Rule

You never need to enter a UPI PIN to receive money. PINs are only required for sending money.

Report Suspicious Request

Decline and report fake collect requests through your UPI app and block the sender.



Verify the Request

Do not approve collect requests from unknown senders or for transactions you do not recognise.

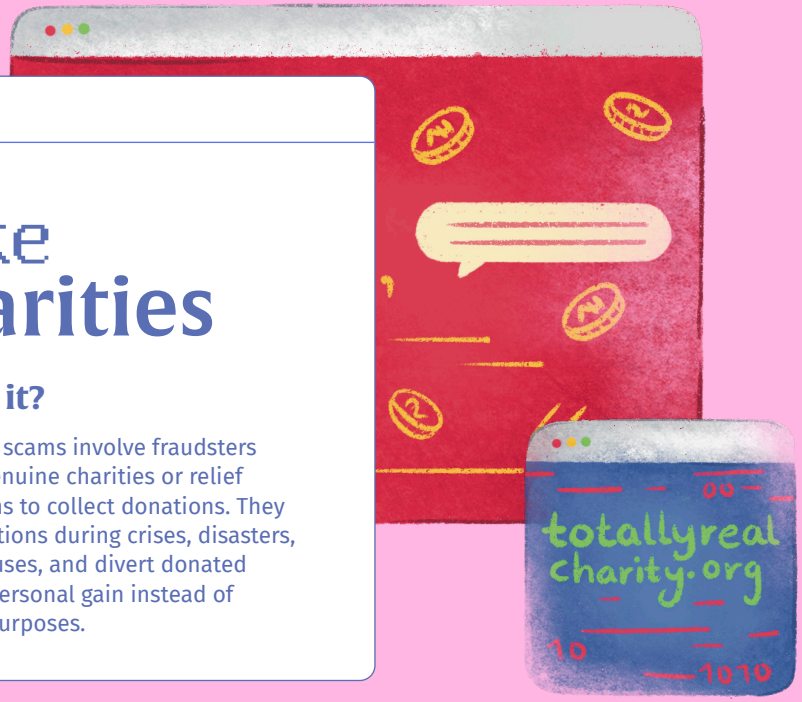
Read Before Approving

Carefully check the amount, sender name, and purpose shown on the UPI app before taking any action.

Fake Charities

What is it?

Fake charity scams involve fraudsters posing as genuine charities or relief organisations to collect donations. They exploit emotions during crises, disasters, or social causes, and divert donated money for personal gain instead of charitable purposes.



How does it work?

Emotional Appeal During Crises

Scammers create urgent messages around natural disasters, medical emergencies, wars, or social causes. They circulate donation appeals via messaging apps, social media, emails, or SMS, often using emotionally charged images and stories.

Impersonating Trusted Organisations

Fraudsters mimic well-known charities, NGOs, or government relief funds by copying names, logos, websites, or social media pages. The fake pages closely resemble legitimate ones, making them difficult to distinguish at first glance.

Direct Payment Requests

Victims are asked to donate through UPI IDs, QR codes, bank transfers, or cryptocurrency wallets that are controlled by scammers. In many cases, donors are discouraged from using official websites or platforms.

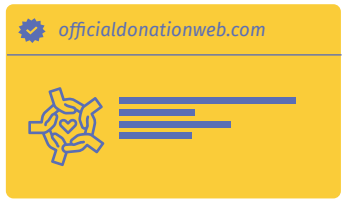
Pressuring the Victim

After initial contact, scammers may repeatedly message or call, urging immediate donations and claiming lives depend on quick action. This pressure is used to prevent verification.

Misuse of Money

Once funds are transferred, the scammers disappear. The money is never used for charity, and recovery becomes extremely difficult.

Helpful Tips



Verify Before Donating

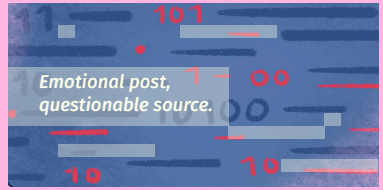
Always check the charity's official website, registration details, and government listings before contributing.

Avoid Urgent Pressure

Genuine charities do not force immediate donations or guilt-trip donors.

Donate through Official Channels

Use verified websites or recognised fundraising platforms instead of direct QR codes or personal bank accounts.



Be Cautious on Social Media

Do not rely solely on forwarded messages or viral posts for donation requests.

Fake Legal Notices

What is it?

Fake legal notice scams involve fraudsters sending fake legal notices to intimidate individuals into making immediate payments or sharing personal information. These notices falsely claim legal action, penalties, or court proceedings.

How does it work?

Impersonation of Legal Authorities

Scammers pose as lawyers, law firms, courts, government departments, or regulators. They use official sounding language, fake letterheads, seals, and reference numbers to appear credible.

Urgent Payment Demands

Immediate payment is demanded to settle the matter out of court. Victims are asked to transfer money through UPI and bank transfer to avoid further legal action.

Pressure and Fear Tactics

Scammers impose short deadlines and warn of serious consequences. This fear is used to stop victims from consulting a lawyer or verifying the notice.

Disappearance After Payment

Once payment is made or information is shared, the scammers cut off contact. No real legal case exists, and the money is lost.

False Allegations and Threats

The fraudsters send notices alleging issues such as copyright infringement, tax violations, unpaid dues, defamation, or regulatory non-compliance. The notice threatens arrest, court summons, account freezing, or criminal liability.

Helpful Tips:

Do Not Panic

Genuine legal notices do not demand instant payment or threaten arrest over messages or emails.

Verify the Source

Check the sender's details, law firm credentials, and contact information independently before responding.

Consult a Lawyer

Always seek advice from a qualified lawyer if you receive a legal notice, especially before making any payment.

Avoid Sharing Information

Do not share personal, financial, or identification details in response to unsolicited legal notices.

Do's and Dont's

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, 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.
- Practice caution entering CVVs for online transactions.
- If the investment scheme or 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 careful reading.
- Do not share OTPs, ATM or UPI Pins, and passwords on calls, messages, 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 while conducting transactions on unsecured websites and always verify that the web address begins with "https://" and not "http://".

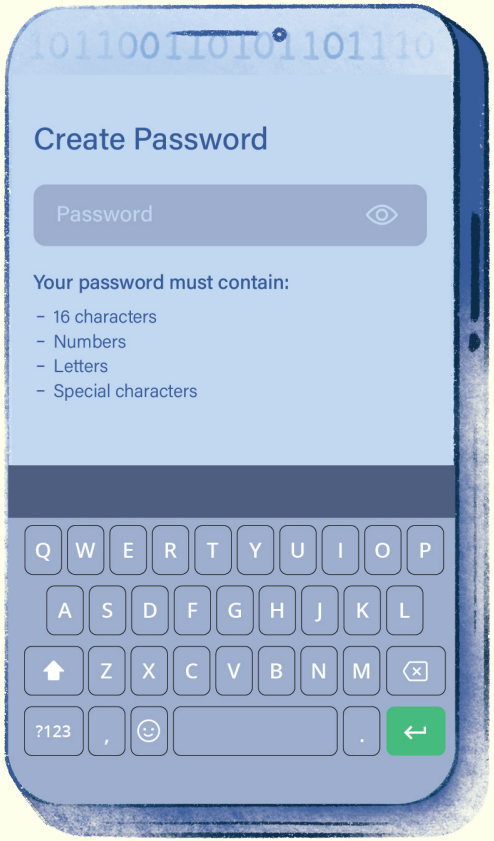
Pro Tips

01 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.

You can check for compromised passwords on your Android phones by opening Chrome and tapping More > Settings > Google Password Manager. You can then tap Checkup to see compromised passwords.
On iPhones, go to the Passwords app and then tap Security. If any account has a weak or compromised password, a message will explain the issue.



Weak passwords

Simple: Aditi1995 (name + birth year)
Sequential: abcdxyz123
Predictable: SalmanBhaiFan

Strong passwords

Personal: Maachbhaat&Dal92
Random words & multiple characters: C@rr0tcake&MnMs!

02 Understanding SMS Codes

VM-SBIUPI

567678

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

XY-ABCDEF

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 the 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).

567678: Fake msg

Illustrations

The SMS code 'AD-SHPRKT' means the sender is Shiprocket, 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.

909090

AD-SHPRKT

03 Responding to scammers and fraudsters

Cut the call & 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.

Filter spam

Dial 1909 and register for the spam blocking facility offered by your telecom provider as per TRAI directions. You can also do this via TRAI's DND app.

Constant vigilance

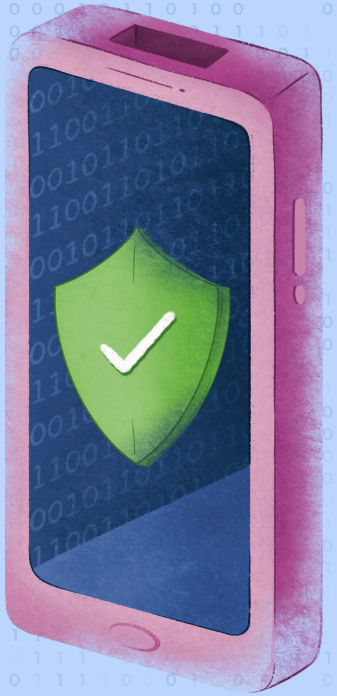
Follow the I4C on social media to keep up with the latest: (look up @CyberDost on X (twitter); CyberDostI4C on Facebook or @cyberdosti4c on Instagram.

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 pillars for user safety are:

- Using AI tools to protect and empower users
- Building products that are secure by design
- Ensuring speedy and effective grievance redressal
- Empowering internet users to control online interactions

Use of AI to protect and empower users

AI 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 calls.

Mule account monitoring

RBI asks banks to collaborate with an AI model built by its subsidiary –RBI innovation hub (RBIH)–that helps banks and financial institutions detect mule accounts being used by fraudsters and money launderers.

International incoming spoofed calls prevention system

Department of Telecommunications (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.

Financial Fraud Risk Indicator

DoT Financial Fraud Risk Indicator flags a system that flags mobile numbers linked to medium, high, or very high risk of financial fraud. Shared with banks, UPI apps, and financial institutions, FRI enables extra checks, transaction warnings, or declines when payments are attempted to risky numbers helping prevent cyber fraud before money is lost.

AI solutions in action

airtel

Spam Detection

Airtel's AI powered Spam Detection Solution combats spam by analysing user behaviour to detect and alert customers about suspicious calls and messages and alert customers about potential scammers and suspicious calls. It processes over a trillion call and message records daily, identifying threats in real time. It uses behavioural indicators such as call and SMS patterns, SIM or device changes, geo-location, and robocalling anomalies.

Fraud Detection

Airtel's Fraud Detection Solution is a real-time, network-level system that protects users from fraudulent domains and phishing links across web, SMS, email, and OTT platforms. It uses an AI-driven, continuously updated database of malicious domains and evaluates unknown links using threat intelligence signals to generate instant fraud scores and block malicious domains.

FORTINET

AI and Machine Learning for Security

FortiMail Email and Workspace Security uses AI-driven threat detection and machine learning (ML) to identify phishing, malware, and business email compromise in real time.

kaspersky

Multi-layer Mobile Security Software

Kaspersky's mobile protection delivers advanced, multi-layered anti-phishing defence at every point of contact. Malicious links are blocked in browsers before pages load, intercepted inside messaging apps, and removed directly from notifications across any app.

Google

Call Screening

Call Screening uses on-device AI to identify who's calling and why. It briefly interacts with the caller to understand intent, helping users avoid interruptions by automatically declining calls that appear to be spam or scams.

Identification of AI-Generated Content

Google's SynthID Detector is a verification portal to quickly and efficiently identify AI-generated content made with Google AI. The portal provides detection capabilities across different modalities in one place and provides essential transparency in the rapidly evolving landscape of generative media. It can also highlight which parts of the content are more likely to have been watermarked with SynthID.

Theft Protection

Android's theft protection uses AI to detect "snatch-and-run" motions, instantly locking your screen if someone grabs your phone. It also features Offline Device Lock, which secures the handset if disconnected from the internet, and Remote Lock, allowing you to secure your device using just your phone number from any location.

Scam Detection

Scam Detection uses on-device AI to detect scam patterns across calls and messages in real time. Features like Circle to Search help users identify fraudulent content, while suspicious SMS and RCS messages are flagged or diverted to spam.

Combating Invalid Traffic with AI

Google uses advanced AI and large language models to identify "invalid traffic"—like bot clicks or accidental taps. These systems analyse app content, ad placements, and user interactions in real-time. This helps block fraudulent activity.

Google Ads

Leverages AI-powered detection (LLMs and refined detection) to catch emerging scam patterns.

Google Play Store

Google Play Store labels financially approved apps. It enables users to ensure that verified stock trading apps are approved by SEBI.

mastercard

Identity Theft Protection

Mastercard's Digital Intelligence Pro is a generative AI-powered fraud detection tool that analyses vast transaction data in real time to assess risk and identify potentially fraudulent activity. It also evaluates relationships among entities and behavioural patterns across payments to ensure accuracy in identification of scams and frauds.

Decision Intelligence

Uses proprietary data, advanced ML models, and global insights to enhance fraud detection for banks. It delivers real time decision scores with rich cardholder and transaction level insights. This helps issuers approve more genuine transactions while reducing false declines across behavior, channel, and transaction type dimensions.

Meta

Facial Recognition for Prevention of Scams

Uses facial recognition technology to crack down on scams like celebrity bait ads, and helps user regain access to hacked accounts.

AI Tools for Threat Prevention

Meta uses AI and human review to act on harmful content across Facebook and Instagram, while WhatsApp combines user reporting and machine learning to curb spam, fake accounts, fraud, and bulk messaging.

Microsoft

Anti-Phishing Measures

Microsoft has developed deep-learning-based domain impersonation protection at creation stage, alongside AI systems for detecting fraudulent e-commerce sites and fake job listings. It has also introduced typo protection in Microsoft Edge, and deployed AI-powered fake job detection on LinkedIn.

Scareware Blocking

Microsoft's Scareware Blocker in its Edge browser uses local AI (Local AI means the computer itself quickly analyses threats without sending data to the internet, keeping things private and fast) to detect and stop fake pop-ups, scam alerts, and fraudulent downloads, ensuring safer browsing.

truecaller

AI-Powered Message ID and SMS Fraud Detection

The SMS Fraud Detection feature safeguards users from SMS-based fraud by detecting deceptive messages, disabling unsafe links, and restricting access until a sender is marked safe. Its AI-Powered Message ID operates offline to categorise legitimate communications (into delivery, billing, etc.) while reducing exposure to smishing and scam content.

Truecaller Caller ID

Truecaller Caller ID uses AI and community reports to identify who is calling and why. It provides real-time warnings for spam, fraud, and suspicious calls, classifies callers by type (such as delivery or customer support), and shows insights from other users' experiences so you can decide whether to answer or ignore the call.

AI-Enabled Call Recording & Transcription

Advanced call recording and transcription features help users retain evidence of suspicious or misleading calls. Automatically generated summaries and searchable transcripts support better recall, accountability, and post-incident verification in cases of harassment, fraud, or disputes.

Vi

Voice Spam Detection

Vi's Voice Spam Detection tool flags fraudulent spam calls in real time. Using advanced AI models, web crawlers, and user feedback, it identifies suspicious callers before they reach you.

SMS Spam Detection

Vi leverages AI and ML to detect spam SMS messages and tags them as "Suspected Spam" to warn you instantly.

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.

CONFIDENTIALITY	INTEGRITY	AVAILABILITY
Use of encryption tools to keep sensitive personal data like passwords private.	Use of technical measures to prevent breaches and unauthorised access of data.	Ensuring availabilty of data back ups and a comprehensive post- breach data recovery plan.

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

The Ministry of Electronics and Information Technology (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).

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.

Telecom Security

Telecom Cyber Security Rules mandate telecom entities to adopt robust cybersecurity measures, conduct risk assessments and implement infrastructural safeguards.

Enhancing User Trust in Telecom Communications

In 2026, TRAI launched Calling Name Presentation (CNAP), requiring telecom operators to verify subscribers' names and display them on call screens, helping users identify unknown callers and reducing scam and impersonation calls, including those posing as banks or government agencies.

Security by design solutions in action

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.

Google

Google Play Protect

Google Play Protect automatically scans apps daily on Android phones and works to prevent the installation of harmful apps. The enhanced fraud protection analyses and automatically blocks the installation of apps that may use sensitive permissions frequently abused for financial fraud.

End-to-End Encryption for Chats

When RCS (Rich Communication Services) is enabled, Google Messages uses next-generation SMS that supports features like secure messaging, photos, and videos. These chats are protected with end-to-end encryption and work over the internet rather than traditional cellular networks.

Safe browsing

Google Chrome’s enhanced protection mode of Safe Browsing is our highest level of protection from phishing, malware and other scams that you may encounter while browsing the web. It keeps consumers twice as safe compared with standard protection mode.

mastercard

Embedding Security-by-Design

Through tokenisation (replacing card numbers with random tokens), encryption, and authentication, Mastercard ensures user data is protected.

Meta

End-to-End Encryption

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

Forwarding limits

Instagram and Whatsapp limit message forwarding to five chats at a time. This measure helps curb the spread of shopping scams, viral misinformation, and harmful content.

Limited Data Collection

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

Seller Verification

Facebook Marketplace uses verification checkpoints for suspicious accounts to ensure compliance. Marketplace Messenger also filters risky messages into a spam folder, which includes a safety warning when opened, reminding users to take protective steps.

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 Sign-Ins

Microsoft strengthens security by mandating phishing-resistant multifactor authentication (MFA), promoting passwordless passkeys, and improving sign-in usability across products.

OpenAI

Secure Development of Models

OpenAI builds safety into its models from the start by testing them for misuse, stress-testing them with experts, and training them to avoid harmful or unsafe responses.

Infrastructure Security

It applies secure infrastructure practices like access controls, monitoring, encryption, and staged deployments to reduce abuse, data leakage, and system vulnerabilities.

SNAPCHAT

Proactive protections

Snapchat uses signal-based detection and advanced tools like PhotoDNA and CSAI Match to proactively identify and remove bad actors, detecting child sexual exploitation material before it can be shared or cause harm.

Protections for teens from unwarranted contact

Snapchat is private by default: location sharing is off, teens can only chat with accepted contacts, and messages disappear once viewed. These measures reducelong-term privacy and exposure risks.

Adoption of Safe-by-Design Practices

Snapchat applies standardised safety testing for AI features, including rigorous reviews, adversarial stress testing, safety filtering, and clear labelling of AI-generated content to identify risks and prevent misuse.

VI

International Calling Display

International Calling Display makes it easier for you to recognise genuine international calls and decide whether to accept them.

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 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 (cms.rbi.org.in/cms/indexpage.html) creates a centralised grievance redressal mechanism, allowing you to complain against banks, payment service providers, credit bureaus and other financial institutions to the RBI.

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. Consumers can also register their grievances by dialling the toll free number 1915.

Intermediary guidelines
Under India's information technology law, digital platforms like social media platforms are required to set up grievance redressal mechanisms and address user 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 (gac.gov.in).

Grievance redressal channels in action

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

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

Google

Block and report scams/ spam

Users can report suspicious text messages and phone calls as spam and block the number from reaching out again.

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.

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.

Clear and understandable consent notices

India's first data protection regime, which will come fully into force from 14 May, 2027, requires organisations to obtain consent for collecting users' data by sharing consent notices in clear and plain language.

TRAI rules to combat spam messages

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 make 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

airtel

Business Name Display Service

To ensure that legitimate businesses do not get flagged as 'Spam', Airtel offers its Business Name Display Service - a solution designed to enhance customer engagement for enterprises. The service enables businesses to display their brand name on your mobile screen during outgoing calls, thereby fostering trust and helping customers distinguish legitimate business calls from spam.

Google

Verifying Images

Google's About this image tool provides the history and origin of pictures found online. It shows when Google first indexed the image, where it first appeared, and how other sites, like news agencies, describe it.
It also identifies AI-generated content through embedded metadata.

Ads Transparency Centre

Allows users to look up any advertiser on Google's platforms to distinguish legitimate business from potential scammers.

kaspersky

Child Online Safety

Kaspersky Safe Kids is an all-in-one parental control solution designed to help families protect children both online and offline. It combines age-appropriate content filtering and Safe Search, screen-time and app-usage management, detailed activity reports, and GPS-based location tracking with safety alerts.

Meta

Safety Notices

In Messenger & Instagram, safety notices help users identify potential scams or impersonation. They provide tips on spotting suspicious behaviour and options to block, report, or ignore accounts. Notices may flag suspected impersonators, scam-like activity, or caution users when chatting with new contacts based in another country.

WhatsApp Privacy Controls

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

Microsoft

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.

OpenAI

User Autonomy

OpenAI Privacy Portal allows users to manage and opt-out of training in certain contexts, and access transparency on how personal data is handled.

SNAPCHAT

Privacy as a Feature

Snapchat ensures user privacy through default message deletion, where chats and snaps automatically disappear after viewing, reducing long-term data retention and exposure risks.

Privacy Settings

Snapchat also offers granular privacy controls such as managing location sharing via Snap Map, controlling who can contact you or view your stories.

Simple reporting tools for teens and parents

Snap offers easy ways for teens and parents to confidentially report a safety concern – directly in the app, or on the website if you don't have a snapchat account. Reports go to the safety teams, which work 24/7 to take quick action.

truecaller

Government Directory Services

The Government Phone Directory helps users avoid government-impersonation scams by enabling verification of official Central and State government numbers and helplines. The in-app integration with the 1930 national cybercrime helpline enables faster reporting of suspected fraud.

Elected Tags

Community-backed tags provide users with critical context about callers, helping identify risky, misleading, or unwanted communications. By surfacing collective user insights and enabling profile tagging, Truecaller strengthens shared protection against fraud and scams.

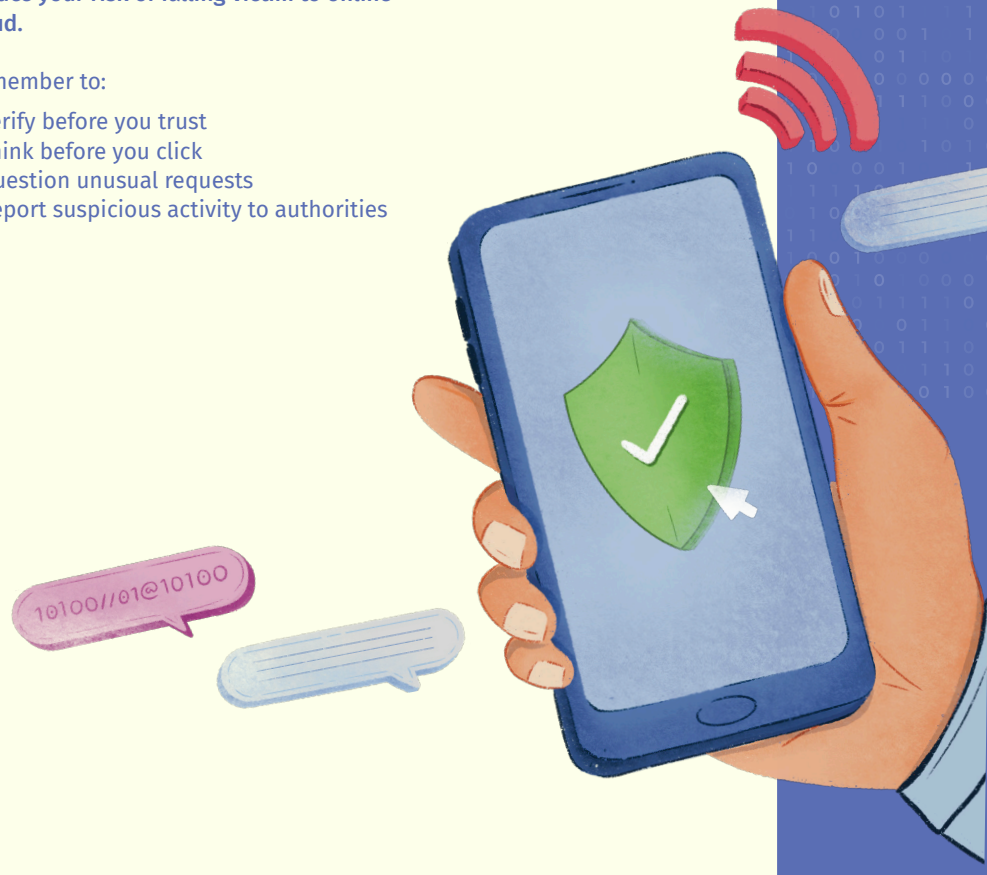
Conclusion

Keeping Indians safe online is a shared responsibility that requires ongoing collaboration between government, industry, civil society, and citizens. This handbook provides an overview of common scams and frauds, practical safety tips, and best practices implemented by leading technology companies and government authorities.

By staying informed and vigilant, you can reduce your risk of falling victim to online fraud.

Remember to:

- Verify before you trust
- Think before you click
- Question unusual requests
- Report suspicious activity to authorities



Notes

SAFER INTERNET INDIA

www.saferinternetindia.com

secretariat@saferinternetindia.com

Safer Internet India

@SaferInternetIndia

@SaferInternetIN