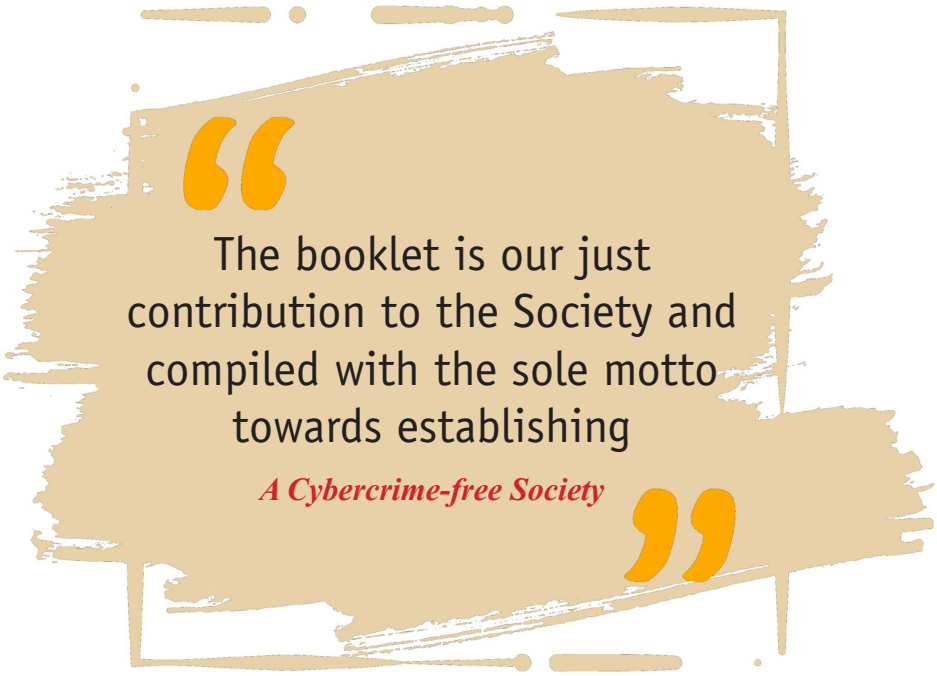
# PROTECT YOURSELF

## Cybercrime Awareness Booklet

**Prepared by**
**State Bank of India Staff Association**
**Bhubaneswar Circle**

blank


The booklet is our just contribution to the Society and compiled with the sole motto towards establishing
A Cybercrime-free Society

blank

# Preface

Dear Reader,

In an era where technology is deeply embedded in every aspect of our daily lives, the rise of cyber fraud poses unprecedented challenges to individuals, businesses, and society as a whole. The convenience and opportunities offered by the digital world are significant, but they also bring increased risks of online scams, identity theft, and financial losses. Fraudsters are persistently seeking new ways to exploit vulnerabilities, making online fraud bigger, smarter, and bolder than ever before.

This booklet aims to enhance your awareness of these threats and equip you with the knowledge and practical tools necessary to minimize your risks and navigate cyberspace responsibly. While governments and law enforcement agencies are increasing their capabilities to combat these issues, personal vigilance and a proactive security mindset are your first and most crucial lines of defense.

The information provided herein is designed to be reader-friendly, covering a range of topics from common types of cyber fraud (such as phishing, online shopping scams, and Business Email Compromise) to essential prevention strategies. We explore real-world examples and best practices, emphasizing simple, actionable steps like using strong passwords, enabling multi-factor authentication, and exercising caution with unsolicited communications.

We trust that this guide will empower you to protect your personal information, secure your digital assets, and foster a safer online environment for yourself and your community. Stay informed, stay alert, and remember that when it comes to cyber security, awareness is the best prevention.

Bhubaneswar
20.11.2025

(Dr. Chittaranjan Panda)
GENERAL SECRETARY

# Contents



# Initiatives of
# State Bank of India

## DIGITAL FRAUD – PREVENTION – AWARENESS

A virtual programme on "Digital Fraud – Prevention – Awareness" conducted on the 13 th August 2024 by the Proactive Risk Management Department, Corporate Centre, Jaipur & Hyderabad.

The questionnaire presented by the Proactive Risk Management Department, Jaipur are furnished hereunder:

**QUESTION-1** :: You receive a call from a constable of Mumbai Cyber Crime Office, who informs you that there are several illegal transactions in your newly opened Current Account with ABC Bank. He also shares some details, which actually pertains to you. You deny for having any such account and ask him for further details / help.

In response, he agrees to arrange for a call from his senior officer after some time. Till then, he advises you neither to leave your place or contact anyone, as this may have some serious consequences. You are instructed to keep your mobile camera "ON" throughout. Do you accept the help of this constable? Yes / No

**Answer** – No :: Police never inform you about your crime in such way. Immediately block that number and report this to Cyber Crime Cell 1930 or Local Police.

**QUESTION-2** :: You were added in a Whatsapp group by some unknown number. This group has 44 members, who share investment / share trading ideas. The admin of this group give calls and members use to trade and making profits. You need previous 4-5 day's chats and decided to start invest.

The admin, on your request, advises you to download an app "Money Makers" by providing a link and also creates your account. Here you invest Rs.10,000/- and trade as per advices of group admin. By the end of the day, you made a profit of Rs.2,000/Now you are thinking to invest more. Should you? Yes / No

**Answer** – No :: These types of groups are fraud groups. The amount you invest may give, initially, small but handsome profit, but in the end, you will lose all your money.

**QUESTION-3** :: You receive a call from your Bank. The caller asks you to confirm the recent transactions, which are suspicious in nature. You are not sure that this call is from your Bank. Should you respond this call? Yes / No

**Answer** – Yes :: Bank may monitor the suspicious activities in your account and may ask you for your confirmation, as a proactive risk management. However, Bank never asks for your OTP, Password or Credential.

**QUESTION-4** :: You receive an e-mail, offering a part-time employment as work from home for 3-4 hours per day. According to sender of e-mail, you have to participate in 4-5 online surveys in a day, and you will get Rs.1,000/- per survey. For this, you have to register yourself on the company's website (link given in the same e-mail) and to make payment of Rs.500/- from your Bank through Internet Banking, to get your account verified.It is an attractive offer for you, as you can easily spend 4-5 hours per day as part-timer after your retirement. Should you accept this offer? Yes/No

**Answer** – No :: These Employment offers are usually fraud attempts. You may be compromising your personal details and Bank account credentials. So, Beware of such employment offers.

**QUESTION-5**:: You receive a Call from your Bank for updation of KYC in your account. The caller offers help, by updating the KYC over phone. After asking your details, he requests you to share an OTP received on your mobile, as verification of updation of your KYC, failing which, your account will be blocked.

Will you provide the same, as it is a welcome move from your Bank for updation of KYC, without visiting the Branch? Yes / No

**Answer** – No :: Bank never asks for the KYC and / or personal details over phone. Sharing of OTP may lead to a fraud.

**QUESTION-6** :: You have received an SMS around 6 p.m. that your electricity connection will be disconnected by 9 p.m. today, as you have not paid the bill yet. You revert to the sender, and he advises you to pay the bill online, for that he will send a link to download the mobile application of DISCOM on your mobile.

Will you pay the Bill online to avoid disconnection of your electricity? Yes / No

**Answer** – No :: Never click on any link for any type of digital payment, without confirming the genuineness. Always download any application from the trusted sources viz. Google Play Store, Apple Store, etc. and not from the unknown sources.

**QUESTION-7** :: Your Bank Manger suggested you for an investment-cum-insurance plan, and you agreed for the same. On very next day, you receive a call from the bank's executive, for verification of personal details of your proposal. Should you share details with him? Yes / No

**Answer** – Yes :: This may be a genuine verification call. Please note that the executive may already have your details with him, as provided by you in your proposal. He will only verify the same and may also offer you information about your plan and clarification of your doubt. He will not ask to share any OTP / Password / Bank account credentials.

**QUESTION-8** ::You receive call from Ms. Swati, who claims to be Service Manager of your Bank. She informs you that your account is put on hold due to some suspicious transactions observed in your account in the past one month.

You remember that you have not done any unusual transactions. However, in last few weeks your neighbour has given you cash in 4 – 5 instances, with request to transfer that money to third party's account, as your neighbour was unable to remit the amount from his account.You visit your branch and Ms. Swati enquires about these entries.

Should you provide the information, as she is not an appropriate authority for any enquiry? Yes / No

**Answer** – Yes :: There are chances that your account is being used as Mule Account, without your knowing. You should respond the queries of your Bank, positively to prevent any further damage.

**QUESTION-9** :: You receive message from INDIA POST that your parcel can not be delivered due to incomplete address. However, you may update your address by clicking the link, given in the same message / e-mail. After you update your address, you receive a call from India Post, where caller asks you to tell him the OTP sent to you, as a verification of address updation.

Should you go for your address updation, as directed by the India Post's caller? Yes / No

**Answer** – No :: These are the fraud messages/calls. The fraudster will try to steal your credentials and track your mobile. He will generate UPI / Other online payment request and complete the transaction by asking you OTP.

**QUESTION-10** :: You have filed your Income Tax Return. After two days, you also received an SMS and e-mail from Income Tax Department for verification of your account details for Tax Refund, for which a link is provided in the same SMS/ e-mail.

How to deal with this situation? Should you proceed with the verification link? Yes / No

**Answer** – No :: This link may lead to a fraud. For verification of your account, you should login on Income Tax Department's website and log in to your account to complete the verification.

**QUESTION-11** :: Some person calls you and requests you to return the money, erroneously deposited into your bank account. Bank account credit message is also received by you.

You wish to refund the excess amount. The caller sends you an UPI request and ask for the refund. He is also guiding you the steps for refund of the amount.

Should you follow the instructions of the caller? Yes / No

**Answer** – No :: This is a fraud; Your account may not be actually credited. In such case you may advise caller to make the request through His Bank Branch to Your Bank for the refund. Accordingly, your Bank will ask you for your confirmation and will act thereon.

**QUESTION-12** :: You have received a message on whatsapp from your college time friend. You recognize him from his profile picture. After a few messages, he requests you through a voice message, to send Rupees Five Thousand online to a reputed hospital, as he in urgent need of money due to medical emergency and does not have his wallet with him at that time. He assures you to repay the money in the evening, same day. Should you consider his request? After all he is your old friend, in need. Yes / No

Answer – No :: This may be a case of Identity Theft. You may ask him for a call / video call to check the genuineness. Be careful with you online social life.

SUMMARY OF CUSTOMER'S LIABILITY

| Time taken to report the fraudulent transaction from the date of receiving the communication | Customer's Liability ? |
|---|---|
| Within 3 working days | Zero liability |
| Within 4 to 7 working days | The transaction value or the amount mentioned in Table-1, whichever is lower |
| Beyond 7 working days | As per Bank's Board approved Policy |

| Table-1 | |
|---|---|
| Basic Saving Bank Deposit Accounts | Rs.5,000/- |
| All other Savings Bank Accounts | Rs.10,000/- |

# Liability of a Customer

## Zero Liability of a Customer

A Customer's entitlement to zero liability shall arise where the unauthorized transaction occurs in the following events:

(i) Contributory fraud / negligence / deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the Customer).

(ii) Third party breach where the deficiency lies neither with the Bank nor with the Customer but lies elsewhere in the system, and the customer notifies the Bank within three working days of receiving the communication from the Bank regarding the unauthorized transaction.

### LIMITED LIABILITY OF A CUSTOMER

A Customer shall be liable for the loss occurring due to unauthorized transactions in the following cases:

(i) In cases where the loss is due to negligence by a Customer, such as where he has shared the payment credentials, the Customer will bear the entire loss until he reports the unauthorized transaction to the Bank. Any loss occurring after the reporting of the unauthorized transaction shall be borne by the Bank.

(ii) In cases where the responsibility for the unauthorized electronic banking transaction lies neither with the Bank nor with the Customer, but lies elsewhere in the system and when there is delay of four to seven days after receiving the communication from the Bank on the part of the customer in notifying the Bank of such a transaction, the per transaction liability of the Customer shall be limited to the transaction value or Rupees 10,000/- in All Saving Bank Accounts (Except BSBD A/c.), whichever is lower.

## SBI BHUBANESWAR CIRCLE INITIATIVES ON DIGITAL FRAUD AWARENESS

- State Bank of India, Bhubaneswar Circle observed Digital Frauds Awareness from 17.11.2025 to 30.11.2025
- Arranged for a tent in front of Branches / prominent places of the Town with volunteers to spread the awareness.
- Associated with local voluntary service organisations, local clubs (Youth Clubs, Rotary Club, etc.), Pensioners' Association for the activity.
- Arranged for Banners for display in the Tent as well as outside/inside Branches.
- Arranged for distribution of pamphlets that had awareness on the digital frauds on one side and services available at contact centre on the other side.
- Organised morning walk in more than 100 parks in the State for spreading the awareness.
- Played the awareness videos available in Bank YouTube Channel in the Tents/in the TVs available in Branches/ local Cable TV network, etc.
- Branch Managers and employees visited nearby Schools / Colleges/ Trade Associations / Government Staff Associations and other organisations and conducted awareness programmes covering large group of people.
- Conducted Awareness Training Program (Webinar) through Microsoft Teams to all Staff to disseminate the awareness on Digital Frauds, importance of KYC in arresting opening of Mule accounts and to bring awareness on services available at contact center.
- The posters displayed by SBI are in the following pages.

SBI

The banker to every Indian

# 10 COMMON TRICKS USED BY SCAMMERS!

## Be Aware and Be Scam-Safe

1. **TRAI Phone Scam:** Scammers threaten to suspend your mobile services, citing illegal activity or KYC non-compliance.
   **Reality: TRAI doesn't suspend services; only telecom companies can.**
2. **Parcel Stuck at Customs:** Scammers claim a parcel addressed to you has been intercepted for containing illegal goods and demand a fine.
   **Action: Disconnect and report the number.**
3. **Digital Arrest:** Scammers pose as fake police officers and threaten to interrogate you online for a made-up criminal activity.
   **Reality: Police don't conduct digital arrests or online interrogations.**
4. **Family Member Arrested:** Scammers claim a relative has been arrested and demand payment.
   **Action: Verify with family members before taking action.**
5. **Get Rich Quick Trading:** Social media ads promising high returns on stock investments.
   **Reality: High-return schemes are likely scams.**
6. **Easy Tasks/ Online jobs for Big Rewards:** Scammers offer high sums for simple tasks then ask for an investment/security deposit.
   **Reality: Easy money schemes are scams.**
7. **Lottery in your Name:** SMS/email stating you've won a lottery and asking for account details or a security deposit.
   **Action: Ignore/delete the message/email.**
8. **Mistaken Money Transfer:** Scammers claim incorrect credit transactions and ask for refunds.
   **Action: Verify transactions with your bank.**
9. **KYC Expired:** Scammers ask for KYC updates via links/phone calls.
   **Reality: Banks do not call or send links for updates.**
10. **Generous Tax Refund:** Fraudsters pose as tax officials asking for bank details.
    **Reality: Tax departments already have bank details and communicate directly.**

***FIGHT AGAINST CYBER CRIMES***

***STAY ALERT, STAY SAFE!***

SBI

The banker to every Indian

# CYBER CRIMES - STAY INFORMED, STAY VIGILANT!

1. Verify information before acting
2. Don't click on suspicious links
3. Don't download any unknown/screen-sharing apps
4. Contact your bank's contact centre on 18001234 for banking queries
5. Update KYC in person/video KYC
6. Don't share your personal/banking credentials such as CIF, account number, card number, CVV, OTP or MPIN
7. Don't fall victim to threats
8. Don't fall into the greed trap
9. Be cautious of high-return schemes
10. Report suspicious calls/numbers via the Chakshu Portal
11. Don't act on video calls/messages (deepfakes). First, verify separately with the concerned person
12. Keep your mobile number and email address updated in your bank records
13. Disconnect suspicious calls and redial after verifying if needed

## REPORT SCAMS

1. National Cybercrime Helpline - **1930**
2. Cyber Crime Reporting Portal - **www.cybercrime.gov.in**
3. Report to - **report.fishing@sbi.co.in**
4. Dial - **100 and report the incident**
5. **Report to Local Police Station**

SBI
The banker to every Indian

# DIGITAL ARREST SCAM

Scammers use intimidation, blackmail and **"Digital House Arrests"** to deceive victims. This scam involves fraudsters impersonating Law Enforcement Officials and falsely claim to investigate crimes.

## ⚠ How the Scam Works: ⚠

- Making video calls through platforms like Skype, Telegram, or WhatsApp
- Create fake police stations and wear uniforms to appear authentic
- Claim to have discovered illegal items, such as drugs or fake passports, in a parcel addressed to the victim
- Issue an arrest warrant on fabricated charges such as money laundering
- Make victim transfer huge money to resolve these fake charges
- Force them to stay on video calls, experiencing a **"Digital Arrest,"** until they transfer money

## How to prevent Digital Arrest Scams:

- Verify the caller by contacting the relevant law enforcement agency using official contact details published on their official website.
- Do not share personal or financial information over phone or video calls.
- Do not transfer money based on such calls or threats.
- Report any such incidents to your local cyber police authorities.
- Call **1930** to report any cyber frauds.

**Officials dealing with customers are advised to educate them about digital arrest scams.**

SBI
The banker to every Indian

# FAKE INVESTMENT SCAM

The Reserve Bank of India has flagged a rising trend of fake investment scams. In this scam, fraudsters create fake investment groups on platforms like WhatsApp and Telegram, presenting themselves as financial experts. They attract victims with free stock tips and

## How the Scam Works:

- ⚠ Adding victims to multiple fake investment groups.
- ⚠ Providing free stock tips and investment advice, which initially seems promising.
- ⚠ Directing victims to download a fake trading application, designed to look legitimate.
- ⚠ Providing some tips benefit group members to build trust, encouraging more investments.
- ⚠ When victims attempt to withdraw funds or express doubts, their accounts are disabled, the group is shut down, and the scammers disappear with the money.

## How to prevent such frauds:

- Always research and verify investment opportunities through credible financial advisors and institutions.
- Avoid downloading investment apps from unknown sources. Use only trusted platforms such as Google Store or AppStore to download apps.
- Do not share personal or financial information with unknown contacts or groups online.
- Be wary of unsolicited investment tips and offers from social media groups or unknown sources.
- For help or to report incidents, contact the cybercrime helpline at 1930 or visit www.cybercrime.gov.in.

**Officials dealing customers are advised to educate customers about such fake investment scams.**

# Some of the Typical Modus Operandi being used by Fraudsters

## HOW THE FRAUDSTERS CHEAT YOU?

Fraudsters attempt to get confidential details like user id, login / transaction password, OTP (one time password), debit / credit card details such as PIN, CVV, expiry date and other personal information. Some of the typical modus operandi being used by fraudsters are –

### VISHING

Phone calls pretending to be from bank / non-bank e-wallet providers / telecom service providers in order to lure customers into sharing confidential details in the pretext of KYC-updation, unblocking of account / SIM-card, crediting debited amount, etc.

### PHISHING

Spoofed emails and / or SMSs designed to dupe customers into thinking that the communication has originated from their bank / e-wallet provider and contain links to extract confidential details.

### FAKE INVESTMENT SCHEMES SCAM

In this scam, fraudsters lure victims with promises of high returns on "unbelievable" investment opportunities. They generally connect with users online through popular channels like WhatsApp, Telegram, or others and offer ways to earn money through investments in cryptocurrency, work-from-home jobs, or get-rich-quick programs.

### SOCIAL MEDIA SCAMS

In such scams, scammers create fake profiles or hijack existing ones to exploit trust and spread misinformation. They may offer fake products, impersonate celebrities, or run online contests that turn out to be cons.

### REMOTE ACCESS

By luring customers to download an application on their mobile phone / computer which is able to access all the customers' data on that customer device. Misuse the 'collect request' feature of UPI by sending fake payment requests with messages like 'Enter your UPI PIN' to receive money. Fake numbers of banks / e-wallet providers on webpages / social media and displayed by search engines, etc.

### VOICE CLONING SCAM

**What is voice cloning scam?**

A voice cloning scam involves using artificial intelligence (AI) technology to replicate someone's voice, typically for fraudulent purposes.

Scammers can use these clones to impersonate individuals and trick them or others into giving up personal information, transfer of money or access to accounts.

**How it works?**

- Voice Gathering Scammers might collect voice samples of the targeted person from various sources, like social media videos, public speeches or even intercepted phone calls.
- These samples are used to train AI algorithms to learn and mimic the targeted person's voice patterns, intonation, and speech characteristics;
- After training, the AI can generate realistic audio that sounds like the targeted person, even saying new phrases or sentences.
- Scammers then use the cloned voice to carry out fraudulent activities such as

1. **Phishing:** They call or leave voicemail messages impersonating trusted entities like Banks, Companies or even the victim's friends or family, attempting to steal personal information or money.
2. **Social Engineering:** They impersonate the victim themselves to manipulate someone into taking an action, like transferring of funds or revealing sensitive details.
3. **Fraudulent Orders:** They use the cloned voice to place orders or make transactions over the phone, pretending to be the real person.

In short, the voice of a person, may be your son or daughter, is cloned in the above manner and Scammers utilise that to commit frauds. You will grow wary and wondering what to do when you get a call from someone threatening to implicate your child in a criminal case if you do not meet their demands. The next minute, however, you hear your sobbing child over the phone and you fear it may be true after all. And so you pay up — only to realise later that it was, indeed, a scam.

## TELECOM AND BANK SCAMS

There has been a surge in telecom and bank scams, where fraudsters impersonate officials to deceive individuals into pressing specific numbers on their phone keypads. These scams have led to significant financial losses and reputational damage for the victims.

**Why this matters?**

The surge in telecom and bank scams highlights the need for increased awareness and vigilance among citizens to protect themselves from financial fraud. If left unchecked, these scams can lead to a breakdown of trust in institutions and have farreaching consequences for the economy and society as a whole.

Singer Chinmayi recently shared her experience on Twitter, revealing that she received a deceitful call from someone claiming to be from the telecom department. The scammer threatened to block all phone numbers under her name unless she pressed 9 on the number pad within two hours. Another victim, D. Laxman, received a similar call from a person purportedly from the State Bank of India (SBI), insisting he clear his credit card payment by pressing 9.

The modus operandi of these scammers involves impersonating trusted entities like telecom departments or banks, fabricating urgent issues such as phone blocking or bank account problems. Victims are coerced into believing that pressing a designated number will resolve the issue or prevent adverse consequences. Unwittingly, victims may authorize transactions or compromise their personal information.

By staying vigilant and informed, citizens can safeguard their finances and personal information from these deceptive schemes.

## SMISHING ATTACK

One type of phishing attack — smishing (SMS phishing) is now being used to dupe customers of banks. If you have a bank account, you must be aware of it to avoid falling prey to this latest scam. What is it? How do fraudsters use it to empty your bank account?

### What is smishing?

Smishing is a scam where you get a fraudulent text message designed to trick you into sharing sensitive information.

"Smishing, a form of cyberattack, combines SMS and phishing. It leverages text messaging to manipulate victims into giving away sensitive information or taking harmful actions. This social engineering tactic preys on human trust and emotions, as well as a sense of urgency, to influence potential victims' decision-making".

### How fraudsters are using smishing to dupe you?

In the latest version of the smishing scam, you usually get an SMS from a mobile number saying a certain amount of money has been credited to your bank account. Right after receiving this SMS, you will get a call saying that a large amount of money has been mistakenly sent to your bank account. You will be asked to return it immediately to a certain UPI number.

The trick is that the message is very similar to the messages your bank usually sends when money is been debited or credited to your account. At first glance, it may look like a genuine message from the bank.

### Here is an example:

"Rs. 15,000 credited to a/c XXXXX9082 on 10-05-24 by a/c linked to VPA XXXX9082 ( UPI Ref No 41356463189)."

However, if you examine it closely and check who has sent it, you will often find a mobile number. Now the bank never sends such messages from a mobile number.

"Scamsters craft deceptive messages that closely resemble legitimate communications from trusted entities such as banks, consultancies, or government agencies. These messages are designed to create urgency or scare tactics to prompt immediate response and compel recipients to click on malicious links, share personal data, or download malware-infected attachments."

The Reserve Bank of India (RBI) has a specific guideline on how banks must inform their customers about transactions in their accounts. **"As per Reserve Bank of India guidelines, banks should use a registered sender ID for sending SMS, which should be a six-character alphanumeric code that represents the bank's name or brand. For example, HDFCBK, ICICIB, SBINNN, etc. The sender ID should not be a random or generic number, such as 567678, 909090, etc.,"**

**How to identify whether the SMS you got is real or a scam?**

Scamsters often send SMS messages from personal mobile numbers to fool customers. Banks, however, will never use personal mobile numbers to send SMS alerts for several reasons.

As per rules banks have to follow a standard SMS format to notify the customers about transactions.

For example, a valid SMS format for a debit transaction of Rs. 500 at a POS terminal using a debit card issued by a Bank would be: [Bank's sender ID] 10/05/24 08:33 Debit Rs. 500 Bal Rs. 10,000 POS 1234567890

This set format helps customers to easily identify and verify the validity of the SMS.

## AI VOICE MANIPULATION NEW TREND FOR MONEY TRANSFERS

In a disturbing new trend in cybercrime, scammers are using artificial intelligence (AI) driven voice manipulation to deceive victims. In the latest case, a victim attempting to send money to a friend living in the US was duped into transferring a sum of Rs.1.8 lakh by a scammer using an AI-generated voice. According to a police source, these cases usually fall under the category of impersonation since the accused pretends to be someone else. However, the use of AI to talk to victims by posing as their friend or relative adds a new dimension.

In this case, the victim received a call purportedly from his friend's WhatsApp number, requesting urgent financial assistance and asking him to transfer the amount to an acquaintance. Behind the scenes, the voice was manipulated using AI technology, making it sound identical to the friend's voice. This form of impersonation is gaining traction among cybercriminals, who trick people into believing they are speaking to someone they know personally, police said.

Despite being cautious of cybercrimes, the victim thought he was helping his friend. The fraudsters exploited the trust between the victim and the impersonated person. In another twist, the victim was advised to seek assistance from bank employees. He contacted the customer care unit of a bank for help with the transaction. However, this number turned out to be another impersonation, and the so-called 'customer service representative' scammed him as well, police said.

## FAKE LINKS FOR FESTIVAL GIFTS

The festival season could bring delightful moments; but the entire season could go for a

toss if you unsuspectingly click unverified gift and greetings links from SMSES, Whatsapp messages and social media posts.

Please do not click any unknown links as cybercriminals target people with dubious Festival gift vouchers and gift links."Once victims click these links, their phones would be infected with dangerous malware, which will collect the data of victims and take control of their digital banking."

Fraudsters have been circulating these posts on social media platforms and sending messages through SMS and Whatsapp to target innocent victims.

Clicking on the links could download dangerous malware into the phones of victims, that can steal data and get access to digital banking.

**The manager of a NGO was trapped in a cyber-fraud. He received a call from a person, who introduced himself as an army person, and assured to help him in donating for orphans on the occasion of Diwali.**

**The caller asked him for his account number, GPay number and IFSC code and sent Rs.10/-. Within ten minutes, he received withdrawal messages of Rs.15,000 and Rs.1,01,000 from his account.**

## SCAMSTERS TRICK PEOPLE ABOUT CASES, ASKING FOR FUND TRANSFER

A new trend in scams has emerged, where fraudsters make phone calls to people claiming that a case has been lodged against them in the High Court, and demand money from them.

Operating with devious persuasion, these deceitful callers are manipulating victims into believing that they must promptly settle fines or face dire legal consequences in the High Court.

To make matters worse, they are sharing personal details of the potential victims to lure them into believing the case is real. Under fear and urgency, the individuals transfer money assuming they are resolving the legal issue.

A victim, requesting anonymity, said the fraudster used his full name and cited his previous location to inspire confidence in him. "The guy on call said a case has been booked against me, and I have to pay Rs.7,000 immediately or I will be arrested and charged under some sections. I panicked and paid the amount to his UPI number," the victim said.

These luring tactics act upon the trust and vulnerability of innocent people, who are intimidated by the legal problems.

Exploiting the sense of urgency, the fraudsters are leaving victims with little time to verify the authenticity of the claims.

## SCAMMERS USING IVR FOR PHISHING CALLS TO CHEAT PEOPLE

Bank and government related phone call scams are on the rise, and fraudsters are making

use of interactive voice response (IVR) telephony to imitate government offices.

Such scams are of a growing concern to authorities and consumers. With IVR technology, fraudsters can create untrue voice response systems and replicate the lines used by government institutions.

When people get these calls, they hear the formal recorded message which is very similar to the calls from a genuine government office. Such systems can also guide callers to not just data scams but also financial scams.

Many people were receiving voice phishing calls, also known as vishing calls. One common tactic involves scammers claiming to be from the tax office. They inform the victim that they owe a large sum of money in unpaid taxes, which they must pay immediately in order to avoid heavy penalties. The victims are then directed to provide personal information or transfer funds to a specified account. In many cases, these fake calls create a sense of urgency, frightening people into complying without taking time to verify the legitimacy of the call.

Another method involves scammers posing as government representatives. They may ask for personal details under the guise of updating records or resolving issues, which are then used for identity theft or other fraudulent activities. Security experts urge citizens to be more careful and sceptical when answering calls from strangers, who say they work for different departments of the government.

**People should never share personal information or make payments without confirming the caller's identity, they said.**

### SCAMSTERS FIND WAYS TO 'SEXTORT' VICTIMS
### EMAILS SENT TO INNOCENT VICTIMS THREATENING ARRESTS

A new form of cybercrime has emerged where victims receive emails from scammers posing as Intelligence Bureau officials scaring them of arrests for watching child pornography.

These scammers first send such emails and threaten victims of arrest if they don't receive a response within 24 hours. In this particular scam, criminals directly target Central government institutions and use the signatures and seals of officials to make the emails appear legitimate.

A woman based out of Hyderabad received an email along with a letter attached to it. The letter read: "By the mandate of Mr Tapan Deka,

Director of the INTELLIGENCE BUREAU; in partnership with INDIAN CYBER SQUARD and BUREAU OF POLICE RESEARCH & DEVELOPMENT; which is the National Nodal Agencies for INTERPOL in India: I, hereby notify you of a computerized seizure of cyberinfiltration captured on your internet protocol address."

Failure to respond within 24 hours from now, the prosecutor will establish a warrant of arrest against you through the closest police station.

On reddit, a user posted, "An email came to my father's email address, saying that I was visiting porn sites and watching it. I have not seen the email personally but I have been told it came from a name and it tells to answer some questions. I admit I visited a few sites before but didn't give any email or number. So is this real or a scam? Please answer me as I just turned 18 so it is a delicate topic between me and my parents. Thank you for your help."

It is important to understand that any enforcement authority would never send an email to anyone.

**In this particular scam, criminals directly target Central government institutions and use the signatures and seals of officials to make the emails appear legitimate.**

Stock market discussion groups and broadcast channels are mushrooming on WhatsApp and Telegram promising insider tips and quick returns, luring unsuspecting individuals into downloading fraudulent apps and investing in lucrative businesses. Many people have lost lakhs of rupees in these scams.

The group members gained the victim's trust by initially giving return on investment, and later lured the victim for their money.

These groups operate by first building trust among their members. They share seemingly genuine tips and advice, encouraging active participation and provide return on investments as well. Once a level of trust is established, the administrators introduce the fraudulent apps, claiming they offer exclusive insights and advanced trading options. The apps usually appear professional and legitimate, with realistic interfaces and functioning features. However, they are designed to steal money from users. Victims typically find that their investments disappear, and attempts to withdraw funds are met with silence or excuses from the app's support team.

## FRAUDS POSE AS COPS, EXTORT MONEY IN FAKE RAPE CASES
## NEW CYBERCRIME USES AI AND FAKE POLICE PICS TO EXPLOIT PEOPLE

Many people have complained of the emergence of a new form of cybercrime where the parents or relatives of the victim receive Whatsapp calls from Pakistani numbers, with an Indian police officer's display picture. The fake police officer alleges that their son has been arrested or is involved in a rape case.

If the target responds, instead of simply disconnecting the phone, they state that the matter could be resolved if they gave money.

A victim posted on a social media platform, "Today my father got a call supposed to be from a police that I had raped someone and had been arrested.My parents called me, worried with the phone call. I told them it was a scam call."

He said there was a similar incident in his brother's college. "I suspect my data was leaked by the university or when the Aadhaar data leak happened some months ago.

Now I want to report it to the police," he said.

Another netizen, who alleged his voice was morphed using AI, posted, "My nanaji got the exact same call. Exact same scenario. They even used my voice to convince my nanaji about this. I still can't figure out how they got this information. Tcallers were using Pakistani number (sic)."

A fake voice scam was also widely prevalent some time back, where the scamster would use AI-generated voice of a real person and would call their family from an unknown number, asking for money as their phone was running low on battery.

**Reporting a similar incident, another netizen posted: "My request to everyone is to never ever share anything personal (Aadhaar, PAN or any document) on the internet and be very careful of what links we click on from a Whatsapp text and educate parents as they are easy targets due to their lack of tech knowledge. Privacy of a common man is literally a joke in this country."**

## FRAUDSTERS STICK NEW QR CODES ON ORIGINAL ONES

In a new online scam that has surfaced, scammers are exploiting the convenience of online payments by sticking their own UPI QR codes over those of legitimate vendors. This tactic, if unnoticed by the vendor, will cause unsuspecting customers to send money directly to the fraudsters instead of the intended business.

The method is simple and effective. Scammers print their QR codes and paste them over a vendor's original code, often in busy marketplaces where the chances of detection are slim. Quite a few cases have surfaced recently.

A seller said, "Most of my customers pay me online through UPI. One day, around 7-8 payments were made, but I did not receive the money. I contacted the bank, they said there was no payment made at all. Then I found a different QR code stuck over mine. I was shocked, and immediately tore off the QR code," he said.

Another seller said he had contacted the UPI provider immediately, and his customer, who made the payment, got the refund. Customers can also file a complaint with the National Payments Corporation of India (NCPI) if their issue is not resolved with the UPI provider's customer care office.

The above modus-operandi was shown in the Rajanikanth Starrer movie "VettaiyanThe Hunter"

## BSNL USERS ON RADAR OF SCAMMERS

### Messages are sent about suspension of SIM for want of KYC

The subscribers of BSNL's mobile services are being targeted by fraudsters by sending fake messages about an imminent suspension of their SIM cards for the want of KYC verification.

In a purported notice from BSNL, the fraudster's message reads: "Your BSNL Sim KYC

has been suspended by Telecom Regulatory Authority of India. Your Sim card will be blocked within 24 hours. Call immediately." The message is sent through Whatsapp from 8822076791, which is not a BSNL number.

The notice also gives out the contact details of the so-called KYC verification executive and implores the customer to contact the service provider immediately before the account was suspended.

When users contact the provided number to update KYC (Know Your Customer), they are pressured into making a payment to "unblock" their SIM card. In reality, there is no such suspension, and the entire scheme is a ruse to extort money.

BSNL issued an official warning to its users several months ago, saying no such notice has been issued by them and advised users not to respond to such messages or calls.

But the messages and scams are on the rise again.

**BSNL ISSUED warnings to its users saying no such notice has been issued by them and advised users not to respond to such messages or calls.**

An executive of BSNL said, "Many people receive such messages, and the scammer tries extorting money from the user. BSNL never sends any such messages or documents saying their KYC has been suspended."

### SCAMMERS USE TAG OF US BANK FOR DUPING PEOPLE
### THEY TRICK ON VICTIMS TO INVEST IN STOCKS; THEN APP LOCKS THEM OUT

Scammers are impersonating as chief investment officers of a US based multinational bank to lure gullible people into paying huge amounts of money in investment scams. The scammers initially gain the trust of people and subsequently decamp with their money.

Victims are added to the Whatsapp groups and channels run by the scammers using the name of the bank and the tag 'Securities India Limited'. These groups contain hundreds of members, with a mix of fake profiles and some real users.

One of the scammers, introducing himself as chief investment officer and teacher Vikram Nadar, regularly posts investment tips. The scammer begins persuading the members to invest. The fake members respond positively and post fake screenshots of the deposited amount and massive profits, giving a false impression of successful transactions.

The scammers further trick their targets by asking them to download an app and urge the members to purchase the shares through that app. After downloading the app, victims who invest are given small returns to gain their trust, but after investing huge sums of money, the app locks them out.

In September, a retired Navy officer from Noida was cheated of Rs.3.43 crores by an investment group, headed by Vikram Nadar.

There are several tricks with which scammers try to catch the attention of people and lure them into the scam. IPOS which offer heavy return on investment, schemes offering

high returns with little to no risks, and experts and advisors giving free stock tips are all common baits used by scammers to lure investment-seeking people into falling for their trap.

## BEWARE! CYBER CRIMINALS ARE MAKING CALLS AS CASTE CENSUS ENUMERATORS

Cyber criminals are leaving no opportunity to dupe gullible persons by sending links and OTP frauds. And they keep changing the approach. In the newest instance, many cyber fraudsters have been posing as staff of the ongoing samagra survey (caste census) to target individuals and are trapping them. With suspected fraudsters making calls and sending text messages while posing as survey officials.

Hyderabad cybercrime police officials have cautioned the people not to respond to any calls and not reveal details of OTPs, links being sent by the miscreants. However, no complaint has been lodged with the police. Hyderabad cybercrime ACP said that they noticed the posts and videos, which have gone viral.

The fraudsters are making calls to people on the pretext of collecting details for the survey, he said. "The government has appointed enumerators who will visit every household to collect the details as part of the caste census. If any person makes calls, do not trust them. It is a fake caller," the ACP said.

In the recent times, miscreants also indulged in making calls from foreign numbers with the DP of an IPS officer. Cybercrime officials confirmed that they had received information about the misuse of an IPS officer's picture as part of the dubious plan.

## COURIER SCAM DUPES 100 PEOPLE A MONTH PEOPLE IN IT SECTORS, HIGH-PROFILE JOBS VULNERABLE

The courier services scam, which has emerged as the latest form of cybercrime, is leaving many gullible individuals in financial and emotional distress. A bigger cause for worry is that those in the IT sector and high-profile positions are the more vulnerable targets.

Police officials point out that many, including the educated lot, fall victim because they get carried away by the sweet talk besides which they are driven by the greed to earn a fast buck.Newspaper reports confirm that over 110 cases of courier scams have been registered in the less than a month.

"The smart operators pretend to be from courier services and contact people through email or phone. They trick them into believing that there is a parcel in their name, which could be drugs or some illegal material. They ask for money towards customs fees or taxes. Victims fall into this trap. Instilling a fear that they are involved in something illegal is a sneaky way to cheat people," he added.

He urged such potential victims to lodge a complaint on 1930 within two hours of getting the call as it would be easy to freeze the victim's account and minimise the losses.

"Some individuals who have lost money to this devious method contemplate suicide as a

last resort. We identify such vulnerable people and provide them with the support they need during the traumatic phase. We have a support system that offers them a lifeline," said cyber expert.

### What is the 'WEDDING INVITATION SCAM'

Amid growing trend of people choosing to send wedding invites on Whatsapp, Himachal Pradesh Police officials warned about 'WEDDING INVITATION SCAMS'. Officials said scammers are now sending malicious wedding invitations through Whatsapp in the form of APK files. Once downloaded, these files infect people's phones with malware that allows cyber criminals to gain full access and hack their devices.

### PLEASE DO NOT OPEN APK FILES

### *A NEW SCAM....*

You arrive at your hotel and check in at the front desk. Typically, when checking in, you give the front desk your credit card (for any charges to your room) and they don't retain the card. You go to your room and settle in. All good so far.

The hotel receives a call and the caller asks for (as an example) *room 620* - which happens to be your room. The phone rings in your room. You answer and the person on the other end says the following:

'This is the front desk. When checking in, we came across a problem with your charge card information.' Please re-read me your credit card numbers and verify the last 3 digits numbers at the reverse side of your charge card.

Not thinking anything wrong, since the call seems to come from the front desk you oblige. But actually, *it is a scam by someone calling from outside the hotel*. They have asked for a *random room number*, then *ask you for your credit card and address information. They sound so professional, that you think you are talking to the front desk.

If you ever encounter this scenario on your travels, tell the caller that you will be down to the front desk to clear up any problems.Then, go to the front desk or call directly and ask if there was a problem.If there was none, inform the manager of the hotel that someone tried to scam you of your credit card information, acting like a front desk employee.

### FAKE CUSTOMER CARE NUMBERS

Callers beware! Over 31,000 fake customer care numbers are out there to scam you

- **88 % of the fake customer care numbers were distributed via Facebook advertisements.**
- **Entities in the banking and finance sectors were the primary targets of impersonation.**
- **There have been instances where a customer lost as much as Rs.16 lakh due to a fake customer care number.**

When we face any difficulty regarding a product or service, we tend to automatically reach out to the customer service department for a resolution. However, fake customer service calling numbers set up by fraudsters to deceive customers are thriving, as per a report by CloudSEK, an AI company that predicts cyberthreats.

XVigil's (CloudSEK's risk monitoring platform) Fake Customer Care module has flagged 31,179 such fraudulent numbers, with many of them having been active for over 2 years. The findings show that about 56% (i.e. 17,285) of these were Indian numbers, while the rest were non-Indian. Further, 80% of the Indian numbers were found to be valid and still operational.

Analysis of the content present on the source domains associated with each number also showed that entities in the banking and finance sectors (39.4%) were the primary targets of impersonation, followed by those in the telecommunication (31.2%) and healthcare sectors (9.9%).

This is an apt modern-day phishing technique, which builds around the trust created in solving customer queries and deceives people into revealing sensitive information, allowing the fraudsters to steal user data.

In its report, CloudSEK researchers have analysed a sample of around 20,000 Indian mobile numbers used by fraudsters to run such customer care scams. It found that none of the major telecom carriers, which have vast network connectivity, have been spared by scammers.

### Social media channels: Scamsters' vehicle of choice

Such fake numbers are disseminated predominantly by social media channels. About 88% (15,271) of the fake customer care numbers were distributed via Facebook advertisements, posts, profiles, and pages. Out of the remaining 12% of the numbers, Twitter emerged as the most popular distribution medium, accounting for 6.2% of the total traffic. Twitter was followed by Google.

Despite Facebook claiming to have taken down close to 2 billion fake accounts per quarter, scammers continue to flood Facebook with fake profiles and pages. Social media continues to be the preferred medium for scammers to trick people because it allows them to reach a large user base in a short period.

To create an impression of authenticity, scammers frequently include a brief introduction and links to their social media accounts or posts alongside the counterfeit customer support numbers. However, a closer examination of these links reveals that they typically lead users to fake domains and fraudulent Whatsapp or Telegram accounts; and sometimes even the email addresses are fake. Scammers leverage social media accounts to lure customers to call on fake customer numbers, visit phishing sites and send emails from their personal accounts, thus compromising their email IDs.

The unwary users search for customer care numbers and may end up calling a fake

customer care number. When customers call these fake call centres, the scamsters use this opportunity to retrieve financial information, OTP, etc., from aggrieved customers via social engineering methods – which refers to techniques used illegitimately to manipulate people to perform certain actions or reveal specific information.

Generally, scammers try to leverage impersonation and the fear factor to collect money from the victims. Thereafter, the threat actors gain access to the victim's bank account and purchase gift cards, etc, or transfer the amount to another account. There have been instances where a customer lost as much as Rs.16 lakh due to a wrong google search leading to a fake customer care number, CloudSEK said.

Fake customer care numbers have been thriving under the cyber radar purely because people tend to be ignorant while engaging with customer care numbers.

### Delivery boys by the day, cyber criminals at night: How 5 men from Pune operated 120 bank accounts for international masterminds

The cyber cell of the Pimpri Chinchwad police was probing a case of online share trading fraud in which a 46-year-old woman from Pashan Sus Road was cheated of Rs 35 lakh by cyber frauds, who promised her high returns against the investment of her money in stocks.

Police said the suspects come from weak educational and economic backgrounds and worked as delivery executives for various courier and food delivery services.

They worked as delivery boys by day but their moonlighting jobs were way more complex. Five men in their twenties, who are now in police custody, together operated a web of 120 bank accounts used by international cyber criminals to receive funds swindled from the victims of online share trading frauds.

In a crackdown against a group of alleged cyber foot soldiers in Pune, the probe by the Pimpri Chinchwad police revealed these men not just operated surrogate bank accounts but also facilitated purchase of cryptocurrency to be sent to the pockets of their international masterminds — for a meagre cut.

### Woman sedated, blackmailed for Rs. 13 lakh by 'astrologer' she met online

The sequence of events has taken place from late 2022 to late 2023, according to the FIR. The complainant has said that due to the domestic issues she was facing, she had logged on to an online astrology solutions platform which connected users with astrologers.

An FIR was registered at Swargate police station by a woman who is in her late 20s and is a government employee.

A WOMAN who was looking for 'astrological remedies' for her domestic issues logged on to an online platform. The astrologer she connected with claimed that there was a spell of 'black magic on her family' and gave her sedatives on the pretext of performing rituals and blackmailed her into giving Rs. 13 lakh using objectionable photos he clicked while she was unconscious.

The suspect came to meet her in Pune and claimed that there was a spell of black magic on her family for which a ritual will have to be performed. He took Rs two lakh for performing the rituals. At the time, he gave her a laddu to eat after which she felt dizzy and passed out. Months later, as her domestic problems continued, she called the astrologer who claimed that the 'rituals' may have failed. He visited her again in Pune and this time gave her a yellow coloured liquid to drink during the rituals, after which she again felt dizzy and passed out. When she woke up, she found several valuables from her home including jewellery worth a total of Rs. 2.3 lakh were stolen.

She later received objectionable photos of herself on her phone which were taken when she was unconscious. It was followed by a message blackmailing her into sending money. She was forced to send Rs. 13 lakh through online transfers as she was threatened that the photos will be released to people in her contact. She recently approached the police and an FIR was registered at Swargate police station. Police have invoked provisions of IPC related to cheating along with Information Technology Act.

**Elderly doctor gets a call to update his electricity bill, conned of nearly Rs 6 lakh**

For Shiv Shankar Saha, a call to update his electricity bill seemed like a regular one from customer care. It was only after the call ended that the 67-year-old realised that a whopping sum of nearly Rs. 6 lakh had been charged to his credit card.

On June 16, Saha, a doctor and a resident of Safdarjung Enclave, registered a complaint on the National Cybercrime Reporting Portal (NCRP) alleging he received a call to update his BSES electricity bill. The caller asked him to pay a nominal amount of Rs. 10 for updating the bill and Saha paid with his HSBC credit card.

Police said the accused allegedly used a remote access app — which lets one control other devices from your own — to virtually access Saha's phone while he was entering his credit card details into it.

**"If it's too Good to be true then, it's NOT"**

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

G20

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

Digital India
Power To Empower

Quad Cyber Challenge

# New scam alert!!

## E-CHALLAN SCAM

Your Challan No is **348915784195032** for PB08DJ8182 having total challan amount as Rs. 500. For online payment of challan visit: **https://echallanparivahan.in/** you can also contact RTO office for disposal of challan.
Regards,
RTO

Today 11:57 AM

## Beware!!

**If you receive a link for traffic challan, don't click these links.**

**As clicking upon these links for payment, fraudsters can hack your bank account.**

**ORIGINAL LINK**
https://echallan.parivahan.gov.in/

**FAKE LINK**
https://echallanparivahan.in/

नये घोटाले की चेतावनी!! ई-चालान घोटाला सावधान!! अगर आपको ट्रैफिक चालान का लिंक मिलता है तो इन लिंक पर क्लिक न करें। भुगतान के लिए इन लिंक पर क्लिक करते ही जालसाज आपका बैंक खाता हैक कर सकते हैं।

#Be Safe
Stay Safe
www.staysafeonline.in

वसुधैव कुटुम्बकम्
ONE EARTH • ONE FAMILY • ONE FUTURE

In association with

certin | साइबर स्वच्छता केन्द्र | NeGD | NIC | MyGov | ISEA | www.infosecawareness.in

# Cybercrime complaints
# Newspaper Reports

## VOICE CLONING / DIGITAL ARREST

01. Mr. X, who works as a superintending engineer in the Municipal Corporation of Delhi, dropped his 18-year-old son at JEE mock test centre near Rajendra Nagar Metro station in Ghaziabad and then left to take care of his work.

An hour later, he got a call from a number with a '+92' country code from a caller, who claimed he was a police inspector said to Mr.X that his son had been caught with a gang of rapists and demanded for payment of Rs. 30,000 through Paytm immediately to get his son's name cleared. The caller said that Mr.X can even talk to his son. The next minute, Mr. X heard a voice saying 'Papa please pay him, they are real policemen, please save me'. Mr.X could not doubt even for a second as the style of speaking, crying and everything was the same like his son.

Despite the confusion, still suspicious, Mr.X asked the caller which police station he was posted at but the man didn't respond. Mr.X told him that he doesn't use online services but has Rs. 10,000 in cash and could give it to him in person. But the caller refused, insisting to seek a shopkeeper's help to transfer the money. Mr.X was afraid that the caller may be a kidnapper and asked his driver to pose as a shopkeeper and handed over the phone to him to send Rs. 10,000. The transaction failed the first time but was successful on the second attempt. Then the man kept demanding more. By that time, Mr.X reached the test centre, but the security personnel didn't allow him to check on his son. Later, he sought help from local police, who took a picture of his son sitting inside, assuring he was safe. After that, Mr. X approached the cyber cell in Noida and filed a written complaint.

02. Mr. Y, an MCD engineer who lives in Delhi's Pitampura had received a call from a number with a '+92' country code from a person threatening to implicate his son, who is pursuing his MBA in Hyderabad, in a rape case. The caller told him that his son was caught with a gang involved in heinous crimes and as he seemed to be from a good family, they intended to release him, provided Mr.Y pay them. Mr.Y heard his son crying over the phone, which sounded exactly like his voice. First, they demanded Rs. 50,000. When Mr.Y said he didn't have that much of money, they asked Mr.Y to pay Rs. 30,000 and Mr.Y paid.

Mr.Y's friend suggested him to call his son to check on him. Mr.Y could come to know after payment of Rs.30,000 to fraudsters that son was in college and was fine.

03. A couple from Narayanguda, Hyderabad were scared to even step out of their house after a four-day long of what they believed was a 'digital arrest'. Apart from losing over Rs.2 crore, the elderly couple were constantly troubled by surveillance by scammers posing as law enforcement authorities. To get rid of it, the couple had at once thought of ending their lives.

The couple, aged between 65 and 70 years, were living alone in the city as their children were settled in the US. One evening, they get a call from a scamster. After picking the phone call, the husband heard an automated caller say that his SIM had been blocked, and that he should press 1 for more details.

On pressing 1, the call got connected to a scamster, who, posing as a Mumbai crime branch officer, told them that there was suspicious activity noticed on their number.

The couple was further threatened that a case has been registered against them and that the only resort to getting out was to transfer money to the scamster's bank account for a purported verification.

"Followed by this, the couple was asked to stay on the video call and not step out. The couple was intimidated to an extent where they were told that police were waiting outside their house and if they so much as peep out of their window, they would be arrested," an official from the cybercrime wing of the Hyderabad police said, quoting from the complaint.

04. A doctor got a call from a scamster while she was in her cabin at the hospital. The scamster, posing as a CBI officer, quoted her Aadhaar number. They made her isolate herself in a cabin, and asked her to tell everybody to step out and even threatened her saying she was under surveillance 24/7,"

The victim was asked to go home and lock herself up, while the scamster would stay on call all that time. After staying on the call, she finally decided to inform her husband. During that time, the victim was shown legal documents that consisted of fake signatures of a former Chief Justice of India.

After she informed her husband, he guided her to report it to the cybercrime police. By then, the victim had transferred Rs.3 crore.

**"The very start of such a call is scary for most people. It is an automated call and starts with a threat of a legal issue. A normal person, especially someone coming from a high-level society would never want such a case against them. There are certain professions where people do not bother to know much about current affairs and legal procedures," the Cybercrime DCP said.**

**Speaking of the solutions to deal with such issues, the Police said, "Firstly, we would urge the people to know that there is nothing like a digital arrest. The very concept of it is a scam. Secondly, always try to disconnect the call if it is an automated one. Disconnect and cross check. We get that legal procedures can be scary for some, but it is always good to reach out to the nearest police stations first."** "What needs to be understood fundamentally is that no such provision in the law exists. Even if there has been a suspicious activity noticed, any genuine authority would first reach out to the police station closest to one's residence. So if at all one feels there might be a case against them, to clear the suspicion, always reach out to the police station and check if there is a case."

05. Cyber fraudsters posing as crime branch officers "digital arrested" a 45-year-old Hyderabad man for two days and duped him of Rs.7.5 lakh by falsely claiming that that his name had turned up in courier case. In what could turn out to be new trend, they contacted his relatives as well.

The victim lodged a complaint with the cybercrime unit (CCU), stating he received a call alleging that a shipment from Mumbai to China containing five passports, drugs and a laptop was linked to him. The caller threatened to escalate the matter to the crime branch.

"The fraudsters claimed the victim's Aadhaar and PAN details were used for the shipment. They contacted the victim's relatives and friends, causing further panic. Under their instructions, the victim downloaded Skype but noticed the fraudsters' camera was off," a CCU officer said.

The victim stated that the fraudsters told him an arrest warrant had been issued against him for money laundering. They warned that police would arrive at his office within five minutes unless he complied.

Later the fraudster instructed the victim to share his screen and stayed in touch with him over the phone for two days, monitoring all his activities. The fraudsters directed the victim to go to a silent place and not inform anyone about the situation, the victim then received a call from a "crime branch DCP, the only person who could help". The victim stated that he was terrified as he received a copy of the supposed arrest warrant from the fraudster. The fraudsters then instructed the victim to transfer 95 per cent of his savings into their account, supposedly to verify its genuineness. They promised to refund the amount later, with a 'police clearance certificate'. Believing the call to be genuine, the victim transferred a substantial amount of Rs.7,50,197 into the fraudster's account for verification purposes and lost the money.

### 06. Techie falls prey to 'digital arrest', loses Rs 6.29 crore to cyber frauds posing as CBI officers

**An FIR was registered at the cybercrime police station of Pune City on 20th November 2024 by the 59-year-old resident of Pashan in Pune, who currently works at a top executive position at an IT company in Mumbai.**

In the largest individual cyber fraud ever registered with Pune City police, a 59-year-old senior IT executive from Pashan lost a staggering Rs. 6.29 crore — nearly his entire life savings — to online criminals who posed as CBI officers.

The fraudsters threatened action in connection with a money laundering case, placing him under 'digital arrest' at his home and forcing him to remain on video call over several hours on the pretext of 'surveillance.' The complainant underwent the ordeal for over a week, starting from November 9.

Deputy Commissioner of Police (cyber and economic offences) said: "The complainant was approached by cyber criminals posing as CBI officers. They told him that his role was

being probed in a money laundering case. On the pretext of conducting the probe, all his personal and financial information was sought by the cyber criminals. He was asked to stay at home, not to communicate with anyone and remain under what they said was digital arrest. The cyber criminals asked him to liquidate all his fixed deposits, investments and transfer all the funds to various fraudulent accounts — saying those were accounts of the RBI — on the pretext of verification. All over four-five days, he was asked to remain on video call as part of the digital arrest."

Cybercrime police further said: "The cyber criminals had the victim so terrorised…they asked him to keep the video call on even when he went to the bank to liquidate his fixed deposits and investments. The bank officials, who became suspicious as to why the victim was suddenly liquidating his assets, kept asking him the reason. Despite their repeated insistence, the victim did not divulge anything and ended up sending Rs. 6.29 crore in five large transactions to mule accounts of cyber criminals. It was only when he mentioned this to some of his family members that he realised he fell for a cyber fraud. This is the largest-ever individual cybercrime registered with the Pune city police. Some other jurisdictions have reported amounts larger than this in cases of digital arrests."

DCP added: "When the complainant approached us, he was traumatised and under tremendous mental stress. We counselled him and guided him through the process of registering the FIR. We have launched a coordinated probe in the case."

### 07. **Elderly woman kept under digital arrest, loses Rs. 3.80 crore**

A 77-year-old woman from Mumbai was kept under "digital arrest" for a month by cyber fraudsters who posed as law enforcement officials and made her transfer Rs. 3.8 crore, claiming her Aadhaar card was used in a money laundering case.

The woman's ordeal began a month ago when an unknown man made a WhatsApp call and told the victim that a parcel sent by her to Taiwan contained MDMA drugs, five passports, a bank card, and clothes.

When the homemaker, who lives with her retired husband in south Mumbai, told the caller that she didn't send any parcel, the person said details of her Aadhaar card were used in the crime. The caller then connected the woman to a "Mumbai Police officer" who told her that her Aadhaar card was linked to a money laundering case under investigation. "The caller asked the woman to download the Skype app and told her that police officers would talk to her. She was ordered not to disconnect the call and disclose the matter," the official said.

Later, a man who identified himself as an IPS officer sought details of her bank accounts. Another man, claiming to be an IPS officer from the finance department, asked the woman to transfer money to bank accounts provided by them. "They told her that the money would be returned if no illegality is found," the official said. The accused returned the Rs. 15 lakh transferred by the woman, apparently to gain her trust.

"They subsequently asked the woman to send all her money from the joint bank accounts of her husband. She ended up transferring Rs 3.8 crore in several transactions to six bank accounts," the official said. The complainant suspected something was amiss when she didn't get her money back even as the accused kept demanding more funds in the name of taxes to release the money she had transferred to them.

"The woman called up her daughter who lives abroad. Her daughter told her she was being conned and asked her to approach police," the official said.

The woman subsequently dialled the cyber helpline number 1930, following which investigators froze the six bank accounts where the money was transferred, he said, adding that the crime branch was probing the case.

### 08. Cyber Crooks Make a Joke of the System in Rs.43-Lakh Fraud

Cyber crooks defrauded a woman from Hyderabad of Rs.43 lakh by masquerading as officials from Mumbai police, after 'digitally arresting' the victim and sending her notes using forged letterheads of the Supreme Court and the Reserve Bank of India.

As per the woman's complaint to the police, the accused called her and said they were officials of the Telecom Regulatory Authority of India. She was told her number will be blocked as the Andheri police, during a raid at someone's home in Pune, found an ATM card with the victim's name on it. This card was used in money laundering to the tune of Rs.6.8 crore, the accused said.

After threatening her with digital arrest, the scamsters told her to send all her money to a specific bank account where it would be checked to ascertain if it was legally sourced. The victim broke her fixed deposits and paid the fraudsters through payment gateways and was waiting for the refund. After a few days of not getting the money, she approached the Hyderabad cybercrime police.

### 09. 84- yr-old loses Rs.2.8 cr in fraud

Threatening the victim that he would be arrested for his involvement in a Rs.68-crore fraud case, the fraudsters squeezed Rs.2.88 crore from a city-based octogenarian. While the investigation is underway, the police teams also worked on recovering the lost money and successfully refunded the victim Rs.1.56 crore so far.

According to the Hyderabad cybercrime police, some unidentified fraudsters digital arrested a Hyderabad based 84-year-old victim. The gang claimed that they were from the CBI and kept the victim in touch with various fraudsters, who were impersonating CBI officials and prosecutors. They claimed that his name came up in an investigation of 300 fraud cases and the victim received a share of Rs.68 crore.

They demanded victim transfer the amount he possessed and said they would refund the amount once it was verified as genuine. The victim was terrified that he would be sent to jail. During the digital arrest, he was confined and told not to discuss the case with

anyone. Meanwhile, he was forced to transfer the amount in different intervals.

Hyderabad cybercrime investigated the case and found that the amounts were transferred to Axis and SBI bank accounts. Police secured court orders to the banks for a refund of the amount. They could recover Rs.53 lakh from Axis Bank, Surat, in the first stage and Rs.50 lakh from SBI, Kerala, in the second stage; and refund it to the victim.

With their regular follow-up with bank officials, police transferred another Rs.53 lakh to the complainant's bank account on Wednesday. A total of Rs.1.56 crore has been restituted so far.

### 10. Hyderabad Man Loses Rs. 5 Lakh in Courier Scam

A 44-year-old private company employee from the city was duped in a courier fraud. The scamster had the Aadhaar number of the victim, according to the police. The caller told the victim that a parcel booked to his name from Mumbai to Singapore contained 150 strips of LSD.

The caller claimed that the Mumbai police had intercepted the parcel quoted a complaint number. The caller also said that an accused in illegal activities was associated with the parcel. The fraudster informed the victim that 29 bank officials had been arrested in connection with this case.

The caller then transferred the call to a person who posed as an official from Mumbai narcotics department who directed the victim to install Skype and call the fraudster. Following his, the fraudster demanded that the victim transfer Rs. 5 lakh through RTGS to remove his name as a suspect, When the victim said RTGS did not allow transactions above Rs. 2 lakh at a time, the fraudster directed him to use IMPS.

Consequently, the victim transferred the entire amount to the fraudster's bank account, believing it to belong to the Reserve Bank of India (RBI).

Meanwhile, the victim received calls from his clients and his wife but the fraudster did not allow him to accept them. Upon suspicion, the victim searched on the internet and realised that he had been cheated. Following this, the victim approached the city cybercrime unit, a press release issued by DCP cybercrimes stated.

### 11. Hyderabad Woman Duped of Rs. 9.2 Lakh by Scammers

An employee working in a private firm, was duped of Rs. 9.2 lakh by scammers. The 50-year-old victim received a call claiming that her mobile number was linked to 247 debit card fraud cases.

The caller posing as a cybercrime officer, thereafter, transferred the call to a person who was impersonating an official from the Mumbai police. The police official told the victim that transactions of Rs. 2 crore had been done using her name, phone number and debit card and a money laundering case was registered with the Mumbai police.

The scammer forced the victim to pay the amount for carrying out the prior investigation.

The gullible paid the amount but later realised that she was cheated by the fraudsters.

### 12. Caller identifies himself as Mumbai Crime Branch officer, dupes Chandigarh woman of Rs. 80 lakh

The accused caller told the woman that she would be arrested soon as the mobile number issued against her Aaadhar card had 24 complaints of money laundering registered, police said.

The accused caller told the woman that she would be arrested soon as the mobile number issued against her Aaadhar card had 24 complaints of money laundering registered, police said.

Identifying himself as a Mumbai Crime Branch officer, an unidentified caller duped a 76-year-old Chandigarh woman of Rs 80 lakh, while threatening her with arrest in connection with 24 money laundering cases against her, police said Saturday.

According to police, complainant told police that she received a call from an unidentified caller, who stated that he was calling from the Mumbai Crime Branch.

The accused caller told the woman that she would be arrested soon as the mobile number issued against her Aaadhar card had 24 complaints of money laundering registered, police said.

The caller told the complainant that she would have to deposit Rs 80 lakh in a secret account for surveillance, which would be refunded if she was found innocent, police said.

The woman, thus, deposited Rs. 80,31,764 in the account through RTGS as directed by the accused, but when she again called the accused on his phone number, it was found switched off, police said.

Finding that she was duped, the woman approached the Cyber Crime Cell of the Chandigarh Police with a complaint.

### 13. Fraudsters dupe Dadar businesswoman of Rs. 5.88 crore with fake drug parcel story

According to police, the incident took place between March 30 and April 5 when someone purporting to be an executive from a courier company called the woman and told her that a package sent to Iran in her name contained MDMA drugs.

The fraudsters claimed that they were investigating a money laundering case related to the package.

A 47-year-old businesswoman from Dadar has filed a complaint with the cyber police after allegedly being duped of Rs. 5.88 crore by unknown individuals by convincing her about a parcel of drugs sent in her name.

### 14. Pune doctor manipulated by cyber criminals for a week, lost over Rs. 1 crore in fraud

Amid threats of his identity being stolen and being misused in drug trafficking and money

laundering, a Pune-based doctor went through a harrowing week-long ordeal. The doctor was asked to isolate himself in a hotel, was made to stay on audio calls continuously for 'surveillance' and was manipulated into liquidating investments to transfer the money to 'government safe accounts' as he ended up losing over Rs one crore to the cyber criminals.

An FIR in the case has been registered at Cyber police station by the senior medical practitioner in Pune, who is in his early 50s. Officials said that while the modus operandi for the cyber fraud mirrored that of a 'drugs in parcel' scam, the relentless pressure from the perpetrators compounded the severity of the situation for the victim. Over the span of six days in the first week of March, the doctor found himself entangled in a web of deceit and extortion masterminded by cyber criminals.

## FAKE CUSTOMER CARE NUMBER

### 15. Pune businessman contacts phone number from a website to cancel air tickets, loses Rs. 8.86 lakh to cyber scammers

The businessman, who is a 59-year-old resident of Kothrud, lodged a First Information Report (FIR) at the Kothrud police station.As per the FIR, about a month ago, the businessman was searching online how to cancel air tickets when he came across the website which claimed to provide the service. He subsequently contacted the mobile phone number on July 14, 2024.

The person who received his call asked for his bank and debit card details. Once the businessman shared his bank and debit card information, he was further asked to download an online application on his mobile phone.After he downloaded the application, Rs. 8.86 lakh was transferred from his bank account to two other bank accounts through net banking on July 15.

The businessman then realised that he had been scammed and contacted the bank authorities and the cyber police station to complain about the unauthorised transactions from his account.

An investigation revealed that when the businessman downloaded the mobile application, the cyber fraudsters got "remote access" of his mobile phone and without his knowledge and consent, added two "beneficiaries", identified as Ismail and Sohail, to his bank account. The cyber fraudsters transferred the money to Ismail and Sohail through multiple online transactions.

### 16. Principal falls for fake customer care scam

The principal of a school in Hyderabad reportedly lost Rs.1.1 lakh to a fake customer support scamster, after she paid the SSC exam fees of her students.According to the cybercrime police, who received a complaint, the Principal paid the exam fee online onbehalf of the school students.She did not receive an acknowledgement for her payment. Confused, the victim attempted to call the bank's customer support. She searched online and came up with a number.

On calling it, a fake executive managed to manipulate her into believing that the transaction had never taken place.The Principal asked for help to complete the exam fee payment.

The fraudster shared a link with her and asked her to fill in her bank details. After she submitted the form, the scamster gained access to her phone and extracted the money from her account. The victim realised it was a fraud when she started receiving messages of the money getting debited without her even making the transaction.

The victim reported it to the police.Never go to google for customer support, always check within the app. Even if one goes, due to lack of awareness, it is advisable not to click any suspicious links or fill any forms.

## INVESTMENT SCAM

### 17. Share trading cyber scam: Dreaming of becoming rich, three in Mumbai lose Rs. 2.37 crore

The complainant received an SMS with a link to join a WhatsApp group called "Fortune UC Stock Group," where "Professor Jonathan Simon" and "Raju Patel" gave lectures on buying and selling 'Block Deal & Upper Circuit Stocks.'

Similarly, a 67-year-old resident of Parel lost Rs.47.21 lakh in another share trading fraud.

Cyber fraudsters in Mumbai continue to exploit victims through fraudulent "make wealth using share trading" schemes. In the past 10 days, three persons had approached the Mumbai Cyber Police, reporting losses totalling Rs.2.37 crore after being lured by promises of incredible profits through online stock trading. The police are currently tracing the suspects by following the money trail.

In the first case, a 71-year-old resident of Sion lost Rs.1.1 crore in an online trading scam. According to police, the complainant was added to a random WhatsApp group called 'TF 011 APOLLO 1000% Profit Plan,' where supposed 'foreign experts' provided tips on smart stock trading.

### 18. Mumbai man clicks on an Instagram post, gets added to a WhatsApp group, ends up losing Rs. 46.4 lakh

According to the police, one of the admins of the WhatsApp group on May 9, on an individual WhatsApp chat, encouraged the complainant to earn a good profit via their mobile application, 'FIVE PAISA SES'.

A 40-year-old man has filed a complaint with the Mumbai Cyber Police after he lost Rs. 46.4 lakh to a share trading cyber fraud. The police have begun an investigation and are trying to locate the culprits.

The Goregaon-based complainant works as a manager for a tech company. On April 6, he clicked on an Instagram post and was automatically added to a WhatsApp group '5 Paisa J03 Value Investment Portfolio'.

The WhatsApp group had over 171 members, and information regarding various stocks was being shared on the platform, encouraging people to trade.

### 19. Ghaziabad woman duped of Rs. 40 lakh on the pretext of 'investment'

Officials said that the matter is under investigation and attempts are on to nab the accused.

An FIR under IPC section 420 (cheating) and section 66D of the Information Technology ( Amendment) Act, 2008, has been registered in Wave City police station.

A Ghaziabad woman has been allegedly duped of around Rs. 40 lakh by cyber criminals on the pretext of 'investment' and a work-from-home job offer.

Narrating her ordeal, complainant, a resident of Dream Homes in Wave City, said she received a WhatsApp message regarding a job last year. "On November 9, 2023, I received a WhatsApp message wherein a woman introduced herself as Roshni, from Laqshya Media Group. She asked me to join a group on another messaging app — Telegram, where I would be assigned certain tasks and would be paid on completing it. Initially, they transferred Rs. 150, 300, 500, 2,800 into my account through UPI," the victim said in her complaint to the police.

The woman further said, "They told me about some prepaid tasks, in which first I had to transfer money to them. I was asked to follow some steps on their website following which they would return me the money along with the profit. I followed all the instructions. Later they said there was something wrong with my data and asked me to transfer money again. I was told they would have to open a separate account as it was not possible to withdraw money and I was asked to send money again."

The victim said that in this way she sent around Rs 40 lakh to the scamsters and each time in different accounts. "Lastly, the accused told me that in order to withdraw my amount, they would have to increase my score and again asked me to transfer another Rs. 20 lakh, promising to return all my money after this. I became suspicious about it and informed about the incident at home.

### 20. Instagram ad, Rs. 10,000 seed fund used as baits to cheat Pune woman of Rs. 3 crore in online share trading fraud

Police caution people on online share trading fraud 'epidemic'

Between the first and last week of March, the woman was manipulated into making 30 transactions to 12 fraudulent bank accounts totalling Rs. 3.04 crore, before realising that she was being cheated.

A captivating Instagram advertisement, coupled with the offer of a 'trial seed fund' of Rs. 10,000 proved to be the bait that led a Pune woman to fall victim to an online share trading fraud, in which she lost a staggering Rs. 3 crore from her life savings. A fraudulent

application she was made to log on showed that she had earned profits of Rs. 20 crore against her 'investment'.

A First Information Report in the case was registered at Cyber crime police station of Pune city last week by the woman, who is a resident of Mohammadwadi area and is in her late 50s. Between the first and last week of March 2024, the woman was manipulated into making 30 transactions to 12 fraudulent bank accounts totalling Rs. 3.04 crore, before realising that she was being cheated.

In January this year, the complainant came across an advertisement on Instagram which promised multifold returns. After clicking the link, she was added to a WhatsApp group. A large number of members of the group were discussing how their 'institutional accounts' helped them earn huge profits on investments in equity. After reading the messages for close to two months, the complainant was offered a 'seed amount' of Rs. 10,000 for investment, which was directly transferred to her account. She was then made to download and log on to a phone-based application, which the probe has now revealed was fraudulent.

Over the coming one month, the cyber criminals kept telling her about new investment opportunities in the stock market and the complainant continued making large transfers. All this while, the phone-based app kept showing over six times her 'investments' as profits. In between, she was allowed to make small withdrawals totalling around Rs. 1 lakh. After 30 large transfers to 12 bank accounts totalling Rs. 3.04 crore, her account on the app reflected profits of Rs. 20.66 crore. When she expressed willingness to withdraw all the money, she was told that before withdrawing the money she would have to pay 30 per cent of the total profits as charity and 10 per cent as fees. It was at this point that she realised she was being cheated. She subsequently approached the Cyber crime police station and an FIR was registered.

In another case, a Pune-based CA was cheated of a staggering Rs. 3.4 crore in an elaborate share trading by cyber frauds, of which over Rs. 2 crore was taken by him as loans from various banks. The cyber criminals used a WhatsApp group named after a British financial major to lure him with high returns on 'block trade' and 'upper circuit trading.'

### 21. **Hyderabad Woman Duped of Rs. 4.49 Lakh in Trade Market Fraud Scheme**

Cyber fraudsters duped a 40-year-old housewife from the city to the tune of Rs. 4,49,740 in the name of a trade market investment scheme.

In a complaint lodged with the city cybercrime unit (CCCU), she said that some persons had called her on her Whatsapp some months back offering to hire her and pay huge commissions to promote videos and photos by way of liking, rating, and sharing them. Initially, the scammers assigned the victim a task to give a 5-star rating.

For the first task, she received Rs. 120 and for completing the second task, she was paid Rs. 300 to demonstrate their genuineness. On her request for work,she was sent a link (https://t.me/+0E6-RobciMo2MzZh) via WhatsApp asking her to create an account.

She was told to pay Rs. 1,000 against getting Rs. 1,300 in return, which they did, a CCU officer said. The fraudsters convinced her to invest larger amounts, promising significant returns, he said.

After collecting Rs. 4,49,740 overall, they stopped returning money but promised a refund. In fact, they asked her to invest more. Realising that was cheated, she approached CCU, the officer said.

### 22. Senior citizen falls for fake insurance policy trick

A 62-year-old businessman from Rourkela was flooded with calls, offering a loan at a zero per cent interest rate if he bought an insurance policy worth Rs. 10 lakh.

The representatives, claiming to be from a finance company, provided details via Whatsapp and asked the victim to submit an application form (Number SD8506846) for a 'guaranteed pension plan'. They further instructed the victim to transfer Rs. 80,000 to their account.

Later, the scammers demanded Rs. 56,050 for a health insurance policy to secure additional loan subsidies, which the victim paid as indicated.

Another call then informed the victim that as he was 62, he needed a second two-year health policy. The victim made additional payments, but the promised loan was never approved.

The amount lost by the victim is Rs. 1,73,713. The victim lodged a complaint with the cybercrime police.

### 23. Bhubaneswar man loses Rs. 50 lakh after joining WhatsApp group to learn stock market investment

An elderly man from Bhubaneswar fell victim to a WhatsApp-based stock market scam, losing Rs. 50 lakh after being lured by promises of high returns.

In one such recent case, a 63-year-old man fell victim to a fraudulent stock market scheme organised via a WhatsApp group. The scheme reportedly promised high returns on investments but ended up costing him Rs. 50 lakh.

The scam began when the victim joined a WhatsApp group titled Stock Discussion Group. The group administrator, Kunal Singh, introduced himself as a reputed financial advisor, claiming that his stock trading guidance had brought exceptional returns for previous clients,

He further described his "2022 stock classes" as highly successful, boasting returns as high as 500 per cent on specific stocks. Impressed by the conversation and the promise of high returns, the victim decided to enrol in the proposed online classes, hoping to learn strategies for stock trading and investment.

The sessions were reportedly conducted through links shared within the WhatsApp group, leading participants to join private online classes where the scammer allegedly offered

guidance on market trends and specific stocks.

During these sessions, the scammers directed the victim and others to invest through a platform named Skyrim Capital, which they introduced as a legitimate financial service provider.

Initially, the victim was encouraged to invest small amounts, which reportedly showed promising profits, increasing his confidence in the scheme. However, as time went on, the scammer convinced him to make larger investments for more significant profits, ultimately leading the victim to invest a total of Rs. 50 lakh. He reportedly transferred this money across multiple beneficiary names and accounts, likely to evade suspicion and tracking.But when the victim tried to withdraw his profits, he realised it was a scam, as the scammers denied the withdrawal.

According to the police, scams like these are increasingly common, especially through messaging platforms where fraudsters can quickly reach and deceive a large number of people.

24. **Accountant relieved of Rs. 10.10 cr**

Fraudsters lured him into investing in stock market to earn huge profits

In a high-value stock market investment fraud, cybercheats duped an accountant from Hyderabad of Rs. 10.10 crore.According to the city cybercrime unit (CCU), the victim, in his complaint, stated that fraudsters lured him to invest in the stock market to earn huge profits.

Initially, the fraudsters in order to gain the victim's confidence released a profit of Rs. 19,000/- and then transferred a huge amount. Subsequently, across instalments, they made the victim transfer around Rs. 10.1 crore virtually and showed him a profit of Rs. 24.36 crore. When he wanted to withdraw the promised sum, the fraudsters cut off all contact. He then approached the CCU office.

According to a cybercrime officer, the victim, a 32-year-old accountant, was added to a Whatsapp group named after a prominent a mutual fund investment company on October 2, by unknown persons. The fraudsters showed massive returns in the stock market.

A fraudster introduced himself as Chetan Sehgal, a representative of the company, and gave the victim advice on investments whereas his associate, a woman reportedly named Meerkat, used to negotiate with the accountant, assuring huge returns on investing on with the company.

The woman compelled the victim to open a VIP trading account, police said. He opened the account on October 17. From then on, he ended up paying Rs. 10.10 crore in 27 transactions, ACP said.

25. **Pensioner trusts WA group for stock tips, loses Rs. 1.06 cr**
**Scammers pose as trading experts, ask victim to join Whatsapp groups**

In yet another case of online fraud, a septuagenarian was deceived to a staggering amount

of Rs. 1.06 crore in the name of trading and IPOS. The case relates to a retired government employee of Rs. 1,05,96,031.

The 73year-oldvictim was targeted by scammers posing as representatives from a company claiming to facilitate bulk trading in the stock market. The victim received a Whatsapp message from a group. The fraudsters on the other end of the phone introduced themselves as trading experts and invited him to join several Whatsapp groups.

Following the joining, the victim began receiving frequent communications from a person named Saili Jaiswal. She advertised various investment opportunities, particularly in IPOS and lured him to invest. The victim was encouraged by the high returns and registered on a fraudulent website, yessecurities-vip.com.

He invested substantial amounts in multiple stocks and IPOS ranging from Rs. 10,000 to Rs. 10 lakh. However, when the victim attempted to withdraw his earnings, he was informed that a 30 per cent service fee on his profits was to be paid and it was at this point that he realised he was scammed. The victim promptly filed a complaint with the Rachakonda police where a case was registered under the BNS and IT Act and the teams are pursuing investigation.

### 26. Fraudsters Dupe Businessman of Rs. 78 Lakh in Stocks Fraud

A businessman, who had basic knowledge of stocks, started investing based on the advice of his friends. However, fraudsters, who claimed to be a Sebi-registered firm, swindled a staggering amount of Rs. 78 lakh from him.

The victim, a 44-year-old businessman from Nacharam, Hyderabad, said that he had little knowledge of stocks and shares and had never shown much interest in them. When he finally did, he suffered a huge loss.

The victim said, "I never showed interest in stocks and shares. But I heard success stories from my friends, and once again, I was encouraged to trade wisely. Soon, I started receiving messages on WhatsApp from some people claiming to be from RBL Securities, which they claimed was registered with the BSE (Bombay Stock Exchange). I trusted them, thinking it was genuine."To trap the victim, the fraudsters made him believe that he could earn money by investing. Initially, he was offered free trading tips, which earned approximately Rs. 80,000. After a month, they asked him to take their membership.

The victim said, "After a month of offering free tips, they told me they couldn't continue offering free tips and offered a VIP plan for Rs. 10,000 for the first month and subsequently Rs. 1 lakh a month."

After purchasing the membership, the victim was made to invest in IPO subscriptions, but the funds were transferred to other entities. When he tried to withdraw, the representatives claimed he needed to have 70 IPO subscription points. "Though I didn't have any funds, I borrowed money and invested again. But when they demanded more investment, I realised it was a fraud and reported it to the Cybercrime police," the victim said.

A case has been registered with the Rachakonda cybercrime police under the BNS and IT Acts and is being investigated.

### 27. 31- yr-old private staffer loses Rs. 12.6L in fraudulent stocks

A successful stock market investment could double your money in no time, goes the fake claim. This lure makes the Whatsapp and Telegram-based "advisers" extremely attractive to a lot of aspiring stock market investors.

These companies are mostly scams and commoners lose money quickly.

To one such too-good-to-be-true investment scheme, a 31-year-old private employee from Hyderabad lost Rs. 12.6 lakh to a fraudulent stock investment scheme. The scammers initially offered the victim a one-month free trial and gained his trust with stock recommendations that seemed successful. They lured the victim with free trial and anniversary offers.

According to the police, during the trial, the scammers' stock tips appeared to perform well, gaining the victim's trust. After the trial ended, the victim was invited to subscribe to a paid service for Rs. 10,000, which he paid after background checks, which showed the scammers as a Sebi-registered entity.

Shortly after, the fraudsters promised a gift of Rs. 2,000 as part of their anniversary celebration. They urged the victim to invest Rs. 2 lakh with the promise of doubling the money. The victim was convinced about the returns during the free trial and he transferred the amount. He was not aware that he was being shown the fake numbers.

The scam grew as the fraudsters introduced a fake Initial Public Offer allocation feature.

The victim transferred additional funds to the scamsters to apply for IPOS.

Over time, the victim sent Rs. 12.6 lakh to the scammers. When he attempted to withdraw his money, scammers demanded a 20 per cent tax payment, which raised suspicions.

Upon further investigation, the victim realised he had been scammed and filed a complaint with the Hyderabad cybercrime wing.

### 28. Inside Rs. 96.2 Lakh Investment Fraud – How They Lured Victims and Got Busted by CID Jharkhand

Ranchi CID busts a multi-crore cyber scam, arresting key criminals involved in a Rs. 96.2 lakh investment fraud. Victims were lured via WhatsApp with false promises of massive returns.

The Criminal Investigation Department (CID) in Ranchi, Jharkhand, has apprehended a key member of a sophisticated cybercrime network involved in a multi-crore investment scam. The arrest, made in collaboration with the Indian Cyber Crime Coordination Centre (I4C) and West Bengal Police, sheds light on an elaborate scheme that has victimized individuals across multiple states.

The case, registered on May 3, 2024, under various sections of the Indian Penal Code and Information Technology Act, stemmed from a complaint filed by a Ranchi resident who lost a staggering Rs. 96.2 lakh rupees to the fraudsters. The investigation revealed a complex web of international accomplices using WhatsApp to lure victims with promises of tenfold returns on investments within a month.

The modus operandi involved directing victims to a fraudulent investment website, https://poemsvip.vip, where they were prompted to register and transfer funds to multiple bank accounts. The website displayed illusory profits, tricking victims into believing their investments were growing.

Cybercrime experts traced the website's IP address to Alibaba cloud servers in China, while financial trails led to servers in Hong Kong and Japan. This international dimension highlights the growing sophistication of cybercriminal networks.

The arrested suspect, identified as Dinesh Mondal, 32, from South 24 Parganas, West Bengal, is believed to be a key player in operating mule bank accounts across various states. Authorities seized incriminating evidence, including corporate internet banking credentials of accounts registered under proprietorship firms.

Further investigation uncovered the use of Aadhar, PAN card, Udyam registration ( MSME), and GST registration to open corporate bank accounts under the name "Dinesh Paints" in multiple banks. One such account in Jana Small Finance Bank showed transactions totalling over Rs. 2.30 crore rupees.

The case has revealed links to at least 27 complaints reported on the National Cyber Crime Reporting Portal from various states, all related to investment fraud. Additionally, an RBL Bank account associated with the scam has been linked to 13 complaints involving illegal loan applications and investment frauds.

Three other individuals have been previously arrested in connection with this case, including suspects from Maharashtra and West Bengal.

## JOB SCAM

### 29. Unemployed Woman Loses Rs. 61 Lakh in Job Scam via WhatsApp

An unemployed woman looking for a job stumbled upon a promising offer: Write reviews of hotels and earn a fee. Only, she failed to realise that signing up was the first step in a slippery slope that eventually cost her Rs. 61 lakh.

According to a complaint registered with the Rachakonda cybercrime police, the 34- year-old Uppal resident came across a WhatsApp message that contained an offer for a part-time job. All she had to do was write reviews of hotels online and get paid.

She applied and was approved to started posting her reviews. Every time she posted a review, she was shown a false receipt showing that some amount had been deposited in her bank account. When she wanted to withdraw some money, a caller victim told her that

she had to pay a fee first. The victim first paid the fraudster Rs. 5,000. Over the period of a week, she ended up paying Rs. 61,65,200.

Whenever she hesitated to pay up, the group members on WhatsApp insulted her for not trusting the job and the bosses. She finally realised that there was no chance to withdraw any money and approached Rachakonda cybercrime police who booked a case and began investigations.

### 30. Fraudsters dupe retired man of over Rs. 21 lakh

A 67 year-old retired employee was cheated of Rs. 21.9 lakh that he invested in what turned out to be an online scam, Rachakonda cybercrime officials said.

The victim, a resident of Saroornagar, Hyderabad had shown interest in starting a part-time job. He was asked to review products / outlets online for a small wage. This offer came to him via WhatsApp. Through these contacts, he was given a link to a Telegram group where he received online training. The victim was made to believe that if he invested Rs. 21.9 lakh, he would make a profit of Rs. 28 lakh.

The victim complied. When the complainant tried to withdraw the amount, he was asked to pay Rs. 16 lakh more as purported "channel fees". The victim then approached the police.

## WHATSAPP, APK FILES, KYC, OTP, PIN, ETC.

### 31. New scam emerges now with WhatsApp getting compromised

What appeared to be a transfer of money to a relative with the genuine intention to help turned out into a cyber fraud for a 65-year-old victim, who lost Rs. 2 lakh. The victim had received a WhatsApp message purportedly from his daughter-in-law's father, asking for Rs. 2 lakh and promising to return the money in two days. It turned out that the message was from a scamster.

"This was the first time they had asked me for money in years. That too with their contact number, display picture, everything in place. Initially, we knew that we could get messages from unknown numbers claiming to be family. But we get messages from a known number. How is it possible for one to differentiate," the victim asked.

A day later, when the victim met his relative and asked for the reason behind the request for money. The relative replied that he had never asked for money and that his WhatsApp had been hacked.

"I had saved the amount after my retirement and my son's marriage. It was heartbreaking when I lost it in just a couple of minutes," the victim said.

Director of TG Cyber Security Bureausaid, "Be it any scam, one of the tricks that works 99 per cent of the time is to disconnect and call back. If a scamster calls you, try to stay composed and disconnect the call and then call them back. Ninety nine per cent of the time, the call won't go through, as the scamster does not call you the way people normally

make calls. There are just outgoing services in their phones, not incoming."

Speaking of the nature of the scam that the pensioner fell far, DGP said, "Earlier, we would get calls from other numbers where people would deepfake the voice and make it sound similar to a known person. Now they directly hack into your accounts. The only way not to get scammed is by just calling back that relative and checking if they need money." She said that to avoid such hacks, cyber hygiene is a must. Clicking suspicious links or files is always dangerous and is a pathway for the scamster to put one's data in a compromisable position.

Recently, a victim received a phone call from the person claiming to be a bank executive, offering an increase in credit limit. Soon after the victim was asked for his credit card credentials and was sent an APK file to install, the victim lost over Rs. 2.5 lakh.

"There are two ways of doing this scam, one when they install the display pictures of people who do not have them protected, and the other through suspicious links and APK files. In the case of APK files, the device gets compromised, so apart from just scamming the person whose phone got compromised, the scamster also texts everybody through their WhatsApp number.

### 32. IAF veteran loses Rs. 3.64 lakh in cyber fraud on pretext of gas bill payment in Pune

The veteran received a WhatsApp message, which said that his MNGL gas connection bill was pending payment and would be disconnected at 9 pm that night if not paid.

The veteran replied to the message and sent the screenshot of the last bill payment made.

AN OCTOGENARIAN veteran of the Indian Air Force (IAF) who was recently on a visit to Australia, fell victim to cyber criminals posing as officers of the Maharashtra Natural Gas Ltd (MNGL) who allegedly gained unauthorised access to his phone by manipulating him into sharing sensitive details, siphoning Rs. 3.64 lakh from his bank accounts.

An FIR in the case has been registered with Pune City police by the nephew of the IAF veteran. The FIR states that the incident took place in the third week of August when the veteran, who is in his early 80s, was visiting Australia for personal reasons.

### 33. Impersonator gypped employee of Rs. 1.7 lakh

A 30 year-old woman from Hyderabad lost Rs. 1.7 lakh to a scammer who claimed that he was her boss, and was in need of money. The victim was an employee with the private company, Police said. Her ordeal began with a WhatsApp message from what looked like her boss's number in which he claimed that he was in need of money.

The message was sent from a different series of mobile number but after the scamster claimed he was the boss, the victim as convinced. He claimed he was need of money and that his mobile payment app was not working. He provided a different number and asked her to transfer the amount for an urgent business transaction. He promised to repay the next morning. The victim sent a total of Rs. 1.7 lakh.

She discovered the scam when her boss informed her that he had not sent any message nor made any request for money. After investigating, it was revealed that the fraudster gained access to her boss's WhatsApp account, and used it to impersonate him. Cases are filed for impersonation and cheating.

### 34. Doctor, Govt Employee Lose Rs. 74.78 Lakh to Cyber Crooks

Over two days, a doctor and a government employee have lost nearly Rs. 74.78 lakh to cyber fraudsters in Jagtial district. According to a complaint filed on, a doctor of Metpally mandal lost Rs. 74.38 lakh to cyber criminals. He opened a link in Instagram and invested Rs. 24 lakh on the promise that it would grow to Rs. 1.27 crore in a few months.

A few days ago, he received a WhatsApp call from cyber criminals who told him to deposit Rs. 50 lakh to claim the promised amount. The doctor deposited the money. Later, he received another call asking him to pay 30 per cent of the promised Rs. 1.27 crore towards service tax. When he refused, the fraudsters stopped sending messages to him. The doctor then lodged a complaint with the Metpally police.

In Sarangapur mandal, a government employee lost Rs. 40,000 to cyber criminals. Shiva Prasad received a WhatsApp link with a bank logo. Believing that bank officials had sent the link, he opened it and sent his bank details as he was told. After half an hour, the cyber criminals started withdrawing money from his bank account. He rushed to Sarangapur police station and lodged a complaint.

### 35. RTC conductor duped of Rs. 11 lakh by scammers

Rameshwar, an RTC conductor of Jangaon Bus Depot, lost Rs. 11 lakh to cybercriminals. The matter came to the fore on the next day when he lodged a complaint. Rameshwar had kept the money in his account for the construction of a house.

Rameshwar received a message with a link from a bank where he has an account. Thinking that the Bank might have sent the message, he clicked on the link but did not understand the message.

The next day he visited the Bank and checked with the officials. When they said they had not sent any message, he checked his account and was shocked to see Rs. 11 lakh withdrawn from his account.

### 36. Elderly Man Lost Rs. 1.1 Lakh in KYC Fraud

In yet another fraud involving an APK (Android Package Kit) file, a hexagenarian clicked on a link provided by a fraudster which cost him Rs. 1.11 lakh. Clicking on the APK file sent by the fraudster allowed him access to the victim's phone, police said.

The 60-year-old victim from Hyderabad approached the city cybercrime officials after he was duped. In his complaint, he stated that he received a link in his WhatsApp claiming to be an update on a bank's KYC procedure.

Being a customer of the bank, the victim clicked on the link, and an APK file with a

malicious bug was downloaded on his phone without his knowledge. In no time, he started receiving the messages comprising OTPs. The victim even before realising what was happening with his cell phone, had an amount of Rs. 1.11 lakh debited from his bank account.

The victim in his complaint also said that the messages he received were related to Aadhaar card authentication. The APK files compromise mobile phones, provide access of our cell phones to conmen and leave us no choice. Police have been urging citizens to stay vigilant about the suspicious links that are received on any platform.

### 37. Fraudsters swindle senior citizen of Rs. 4.7L in OTP scam
### Scammers sent APK files to victim, she clicked on it, money debited

Cyberfraudsters duped a senior citizen of Rs. 4.7 lakh in a one-time password (OTP) scam, cheated by someone whom she believed to be an e-commerce customer helpline executive. This was a repeat of a recent incident where another pensioner had tried to access the helpline of a pharmacy app, and landed up with a fraudster who cheated him of Rs. 4 lakh.

In the latest complaint, a 67-year-old victim lodged a complaint at the city cybercrime unit (CCU) after she noticed Rs. 4.7 lakh transferred from her account after she attempted to pay for a parcel that she had ordered from the e-commerce portal. The victim received a call from a person who claimed to be a delivery agent for the e-commerce portal and had come to deliver her order. However, she found it was not the article that she had ordered.

The victim then called the e-commerce portal helpline. A person who spoke Hindi received her call and asked her to transfer Rs. 10 as the fee to raise a complaint, a CCU official said, citing from the complaint. Trusting him, she transferred Rs. 10 through a payment app. The fraudster sent an APK file to her Whatsapp number in the name of customer care and asked her to click it, the officer said. The moment the victim clicked on that file, she got a message that Rs. 4.7 lakh was debited from her account. “We have received the victim’s complaint and have informed the National Cybercrime Reporting Portal (NCRP). The investigation is in progress,” said the investigation officer.

This was similar to the scam that took place on November 10. A retired employee from Ramanthapur, Hyderabad was attempting to update his address on a medicine delivery app. He searched for the app’s customer care on a search engine, and called a number that came up. An executive asked him to pay Rs. 2 to update his address. The pensioner did so without hesitation.He then saw money getting debited from his account and eventually ended up poorer by Rs. 4 lakh

### 38. 54 year-old loses Rs. 1.13 lakhs to fraud

A 54 year-old man lost Rs. 1.13 lakhs to a cyber fraud after responding to a WhatsApp call from a purported bank employee. The caller asked the victim that his international credit card was about to be blocked and asked him to renew it.

The victim, who later lodged a complaint, said that the fraudster persuaded him by talking in banking terms and providing some details. When the victim agreed, he received OTPs and noticed multiple unauthorised transactions on his credit card account totalling Rs. 1,13,000.

The victim has filed a complaint with the Hyderabad Cybercrime police seeking recovery of his loss amount.

### 39. Victim's Prompt Action Saves him Losing Rs. 1.9Cr in OTP Fraud

In a strange cybercrime case, a city resident was about to lose Rs. 1.9 crore in an OTP fraud. The strange aspect was that the victim never was approached by any scamster. He reacted quickly and approached the bank which helped freeze an amount of Rs. 1.5 crore.

The victim started receiving OTPs purportedly from the bank he has an account with — AU Small Finance Bank. The victim checked with the bank regarding the OTPs but it was clueless.

Later, to the victim's shock, he received a message about Rs. 1.9 crore being debited from his account. The victim reported the same to the bank, which froze Rs. 1.5 crore payments. Another Rs. 40 lakh was sent to other accounts by the fraudster. The victim then reached out to the Hyderabad cybercrimes unit, who registered a case.

### 40. Man clicks on link, App, loses Rs. 1.77 lakhs

A 32 year-old man from the city lost Rs. 1,77,580/- after he clicked on a link that came as an SMS with a message that did not have a mobile number. The victim believed it to be a reward notification from a credit card, clicked the link and downloaded an app and fed in all the information that it sought. After the submit button, he received multiple OTPs within a few minutes, and money were automatically debited from his credit card. It appeared that the scammers hacked the victim's phone through the malicious link and accessed his credit card details. The victim contacted the bank customer care and reported the incident. Subsequently, the bank blocked his credit card. In total, the victim lost an amount of Rs. 1,77,580/-. The victim also complained to the police.

### 41. Woman Loses Rs. 2.97 Lakh in Cyber Scam

A 30-year-old homemaker lost Rs. 2.97 lakh to a cyberfraudster who tricked her into revealing financial details.

The victim told the police in her complaint that she had received a call from someone pretending to be from an insurance company. The caller falsely told her that insurance amount would be deducted from her account and to prevent this the victim should download a mobile app through a link provided by the scammer and enter her banking information. She did so, but immediately informed the bank which blocked her credit card. However, the scammer had used the details to withdraw Rs. 2,97,700. The victim immediately reported the fraud to the cybercrime helpline 1930.

# How to keep your Children safe in the Digital Space

Digital safety starts at home. Together, we can foster a culture of awareness and responsibility in the virtual realm.

1. In the current digital era, ensuring children's safety online is a top concern for parents. This parental control guide provides essential insights and resources to assist parents in establishing suitable limits for screen time, encouraging discussions about online safety, and identifying and tackling issues like cyberbullying.

2. It features straightforward instructions for enabling parental controls on different social media platforms. Additionally, fostering open communication and setting clear expectations with your child is crucial for cultivating a positive and responsible digital environment.

3. **UNDERSTANDING PARENTAL CONTROLS:** Parental controls are features found on different devices, software, and platforms that help parents monitor and manage their children's online activities, ensuring their safety from potential dangers. The internet provides a wealth of information and resources, but it also presents potential risks for children. Implementing parental controls is crucial for safeguarding kids from inappropriate content, managing screen time, encouraging healthy habits, fostering responsible online behaviour, strengthening communication and trust, and protecting against misinformation and online scams.

4. **SETTING DIGITAL BOUNDARIES:** Fostering open communication and working together with your child is crucial for ensuring their online safety. This approach helps create a secure and supportive environment, empowering them to navigate the digital world with confidence and responsibility.

5. **AGE - APPROPRIATE RULES** Establish guidelines that grow with your teen's age and maturity.

   **FAMILY DISCUSSION** Have open conversations about safe internet use and family rules.

   **ENCOURAGE OPENNESS** Let teens know they can share online experiences without fear of judgment.

   **DEVICE CURFEWS** Set a time each evening when all devices are put away.

   **SCREEN-FREE SPACES** Make certain rooms or times, like family meals, free of digital devices.

   **SETAN EXAMPLES** how balanced tech use by taking regular breaks and focusing on family time.

6. **DISCUSSING DIGITAL SAFETY WITH YOURCHILD:**

Talk Openly and Regularly
Discuss online experiences as part of daily conversations.

Use Open-Ended Questions
Ask questions that encourage sharing and discussion.

Listen Without Judgment
Respond calmly and keep the conversation open.

Teach Reporting
Show them how to report inappropriate or harmful content.

Importance of Strong Passwords
Teach them to create and protect strong passwords.

Teach Thoughtful Posting
Emphasize respectful and mindful online sharing.

7. **IDENTIFYING AND DEALING WITH CYBERBULLYING**

Notice Changes in Behaviour
Watch for signs like mood swings, withdrawal, or secrecy.

Keep Records
Save screenshots or messages as evidence of bullying.

Maintain Open Communication
Reassure them they can come to you for support.

Report and Block
Guide them on reporting the bullying and blocking the user.

Seek Additional Support
If needed, reach out to teachers or mental health professionals.

8. **GUIDE FOR SPECIFIC APPS**

**INSTAGRAM**

App Overview
Instagram encourages creativity and self-expression, Connects friends and family, Provides exposure to diverse perspectives

Risks

Risks of cyberbullying and harassment, Exposure to inappropriate content, Potential for privacy breaches and identity theft.

Parental Measures

Private Account, Comment Filters, Family Center, Location Sharing.
1 .Go to Profile, Tap on Settings. 2.Select Supervision under Privacy and activate Family Center. 3.Invite your teen to join supervision via the app.

## X (FORMERLY TWITTER)

App Overview

X gives you quick access to news and information, Engages in public discourse and community engagement, Encourages sharing of ideas and opinions.

Risks

Exposure to harmful or offensive content, Cyberbullying and trolling can occur, Privacy concerns with personal information sharing.

Parental Measures

Privacy Settings, Block and Mute features.

1 .Go to Settings and Privacy ? Tap on Privacy and Safety. 2.Select Audience and Tagging to manage who can see posts. 3.Enable Sensitive Content Filter and Mute Blocked Words. 4.Turn on Restricted DMs to limit messaging options.

## YOUTUBE

App Overview

Educational content available on diverse subjects, Encourages creativity through video creation, Provides a platform for self-expression

Risks

Exposure to inappropriate or harmful content, Risk of cyberbullying in comments, Potential for excessive screen time.

Go to Settings

Select 'Family Center'

Click 'Manage kids profile and features for teens' (Tools to connect parents, kids, and teens on YouTube)

Family center – Select '+ Add a YouTube kid's profile' or '+ invite a teen'

## YOUTUBE KIDS

App Overview

YouTube is a video-sharing platform that allows users to upload, view, and interact with videos across a wide range of topics. It is a popular source for entertainment, education, and information.

Risks

Exposure to inappropriate content, risk of cyberbullying in comments, and potential for excessive screen time.

Parental Measures

1 .Download YouTube Kids and set up a Kids Profile. 2.Select Content Settings based on age (Preschool, Younger, Older). 3.Manage screen time limits and monitor viewing history.

## SNAPCHAT

App Overview

Snapchat is a photo/video messaging app with creative filters. Content/message disappears after viewing.

Risks

Inappropriate content sharing, Potential for cyberbullying and peer pressure, Disappearing messages may create a false sense of security.

Parental Measures

Monitor child's chats, hide location on Snap Map, accept only known friends. 1 .Search "Family Center" in the app. 2.Invite your teen to join Family Center for monitoring. From Family Center, you can view your teen's friends and manage privacy settings.

## FACEBOOK

App Overview

Connects friends and family, Allows sharing of updates, photos, and life events, Provides a platform for community building and discussions.

Risks

Potential for privacy breaches and data misuse, Exposure to misinformation and fake news, Risk of social comparison and negative mental health impacts.

Parental Measures

Activity Monitoring, Customisable privacy settings, Blocking and unfollowing, Educating on identifying reliable sources. 1.Open Settings ? Go to Privacy Settings. 2

.Activate Profile Privacy Controls to restrict who can see posts. 3.Use Family Center to set up parental supervision with your child.

### GAMING CONSOLES:

Parents can access the following links to learn more about how to activate parental controls on gaming consoles.

### PLAY STATION

Parental Measures

1 .Sign in to Account Management with your account, then select Family Management. 2. If you're adding a member for the first time, select Set Up Now > Add a Child. 3.To add another child, select Add Family Member > Add a Child.
4 .Enter the child's date of birth, then click Next. Applicable legal terms may appear. Upon review, you can accept and then follow the on-screen instructions to set up parental controls

### NINTENDO

Parental Measures

Download Nintendo Switch Parental Controls App on your phone. 2.Link the app to the console. Set time limits, age restrictions, and content filters for games and interactions.

### XBOX

Parental Measures

1 . Go to Settings, Select Account, Family Settings. 2. Set screen time, app access, and age limits. 3. Enable content filters to block mature content.

### DEALING WITH CYBER BULLYING AND HARASSMENT

Parents play a crucial role in addressing cyberbullying and online harassment.

Here are the steps they can take to report these issues effectively :

Encourage your child to take screenshots of any harassing messages, images, or comments. This documentation is vital for reporting the incident.

Most social media and online games offer reporting features. Parents should help children use these tools to report abusive behaviour or content. If the harassment escalates or poses a threat to your child's safety, report it to local law enforcement. Provide them with the documented evidence for investigation.

### REPORTING CYBERBULLYING AND HARASSMENT

Parents can reach out to helplines such as 1930 or the Cyber Crime Reporting Portal

(cybercrime.gov.in) for guidance and support in dealing with cyberbullying cases

You can also visit the nearest Cybercrime Police station or a Bharosa Center to report the incident.

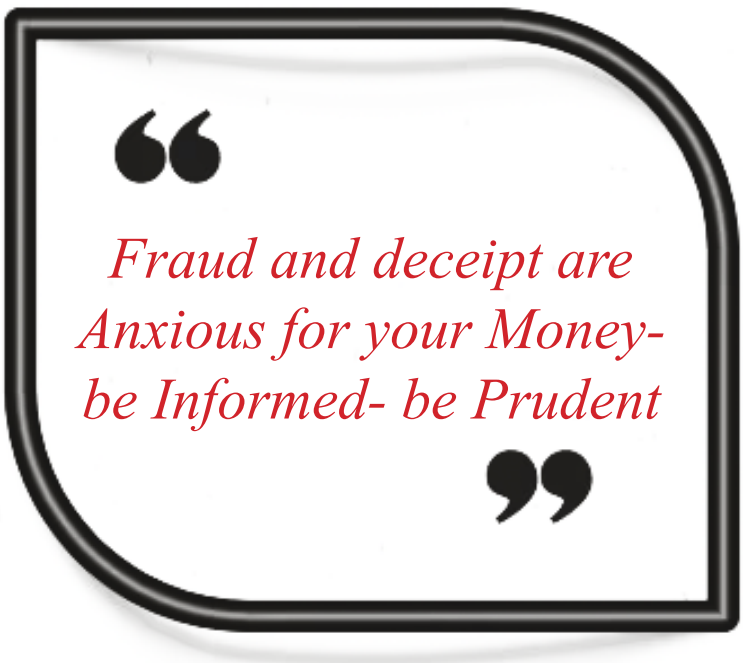
## UNDERSTANDING THE LAWS

POSCO (Protection of Children from Sexual Offences Act) To ensure children's safety in the digital space, parents should be informed about key legal protections such as the Protection of Children from Sexual Offences Act (POSCO), Section 64 of Bharatiya Nyaya Sanhitha (BNS) and Information Technology Act, 2000.

POSCO was enacted to protect children from sexual abuse and exploitation. The act criminalizes : Child Pornography : Sharing, producing, or downloading sexually explicit material involving minors. Cyberbullying and Harassment : Online grooming or any attempts to engage children in inappropriate or harmful activities. Rape and Sexual Assault : Includes all forms of non-consensual physical or digital sexual acts, emphasizing stringent penalties for offenders.

Section 64 of Bharatiya Nyaya Sanhitha It addresses rape, sexual assault, and digital exploitation, including Bodily or Non-consensual Sexual Acts, ensuring stringent penalties for offenders.

Information Technology Act, 2000 This act criminalizes non-consensual capturing or sharing of private images. Also, prohibits the publication or transmission of sexually explicit material, impersonation, cyber bullying, stalking and harassment.



# Odisha Police Cyber Security Cell, Advisories

## CYBER HYGIENE

### Do's

* Use strong and lengthy passwords and change them frequently.
* Use privacy settings on your social media accounts and keep them Private
* Lock your computers and mobile phones when not in use.
* Enable Two-Factor authentications for your online accounts.
* Think before allowing access to Calls, Contacts, messages, Media and Locations while installing mobile applications.
* Check for "https:" in URLs before you browse a website.
* Remember that UPI pin is used to send the money , not to recieve.

### Don'ts

* Do not click on the links sent by strangers or pop ups on websites.
* Do not answer and furnish your personal information, OTP, Credit/Debit Card information including CVV, to strangers
* Do not believe in messages/emails sent to you on mails making false allegations of viewing porn sites.
* Do not believe messages requesting money from your friends, relatives, or employers through WhatsApp by seeing DP.
* Do not open mail or attachments from an untrusted source.
* Do not install unsecured/unverified programs on your computers/mobiles.
* Avoid downloading remote applications like any desk or team viewer quick support.
* Do not use open/public Wi-Fi networks.
* Avoid using charging USB ports at public places for charging your devices.
* Do not respond to calls or messages offering part time jobs or work from home.
* Authorities urge the public to remain vigilant.

* Not to believe any call, which demand immediate payment.
* No court will call a person and ask for an immediate payment of fines over a phone call.
* Exercise caution when joining groups and downloading unfamiliar apps.
* Do not give your money to anyone who meets you online and pay huge amounts of money in the name of investment tips.
* Do not fall prey to part-time jobs and investment frauds.
* Be alert and understand that fake loan apps promise fast cash, but deceive.
* Always download apps from official websites and app stores and not from any unknown sources.
* Always check whether or not the lender is approved by RBI and/or is associated with a financial institution.
* Apply for loans only through applications related to Nonbanking Financial Corporation (NBFC) or authorised banks.
* Elderly individuals, who may be unfamiliar with online threats, need to avoid joining investment or financial advice groups on social media or messaging platforms unless the group is from a verified source.
* Keep in mind that legitimate financial advisors and institutions typically do not operate exclusively through platforms like WhatsApp.
* Promises of guaranteed or high returns are often a red flag. Investments in stock markets are inherently risky, and no genuine financial expert would claim a guaranteed percentage return, especially one as high as 500 per cent.
* Before making any significant investment, especially with new platforms or advisors, consult with a certified financial advisor or a trusted family member
* Always try to call back the person and verify without relying on just a text
* Do not let images/videos out there, have verification processes and utilise safety features provided by the application
* Never click on any suspicious links or install any APK files/ remote apps
* Be it any scam, disconnect the call first and then try to call back, 99 per cent the call won't go through.
* Police urged mobile phone users to avoid such scams by not responding to

unknown callers, especially those seeking personal details. Experts advised users never to share sensitive information such as User ID, password, PIN, CVV or OTP to anyone.

* On Whatsapp, to avoid letting unknown people add you into groups, you can go to Settings > Privacy > Groups and set the option to 'My Contacts' or 'My Contacts Except' and choose who can add you into groups.

* The first hour after a cyber-incident, the golden hour, is critical and greatly increase chances of recovering the money. **Hence, immediately dial 1930, visit cybercrime.gov.in or call on WhatsApp 8712665171.**

**STATE BANK OF INDIA**

* Do not respond to emails and messages with embedded links. "Immediately change your passwords/CVV/PIN if you have accidentally revealed your credentials."

# Appreciable Role of SBI Employees, Bhubaneswar Circle

1. **Suspicious Remittance – A Cyber fraud prevented**
   The timely intervention of Com. Hemangini Das, Associate of Kendrapara branch prevented a Cyber Fraud of Rs.5.00 lakhs on 05.06.2025

   At around 11.30 am, a customer walked into Kendrapara Branch looking anxious but determined. He wanted to remit Rs.5.00 lakh to a UAE Account. He explained that a UAE based bank had approved Rs.50 Lakh loan for him and this payment was required for processing charges.

   He requested a forex transaction but our staff did not feel right to process the same by hearing from the customer about the urgency, Fake loan approval messages, foreign number, the foreign bank story and the large remittance amount. Trusting any instinct, she gently asked him a few more questions.

   At first he insisted that the money was being sent to a relative but his hesitation and the details he shared did not match. She requested him to show the whatsaap message and call history related to the loan. The moment our staff saw the conversations – It was clear that it was a case of cyber fraud trap.

   She explained to the customer patiently how scammers operate:

   a. They offer huge loans from abroad
   b. Ask for processing fee.
   c. Collect personal document
   d. Vanish once money is sent

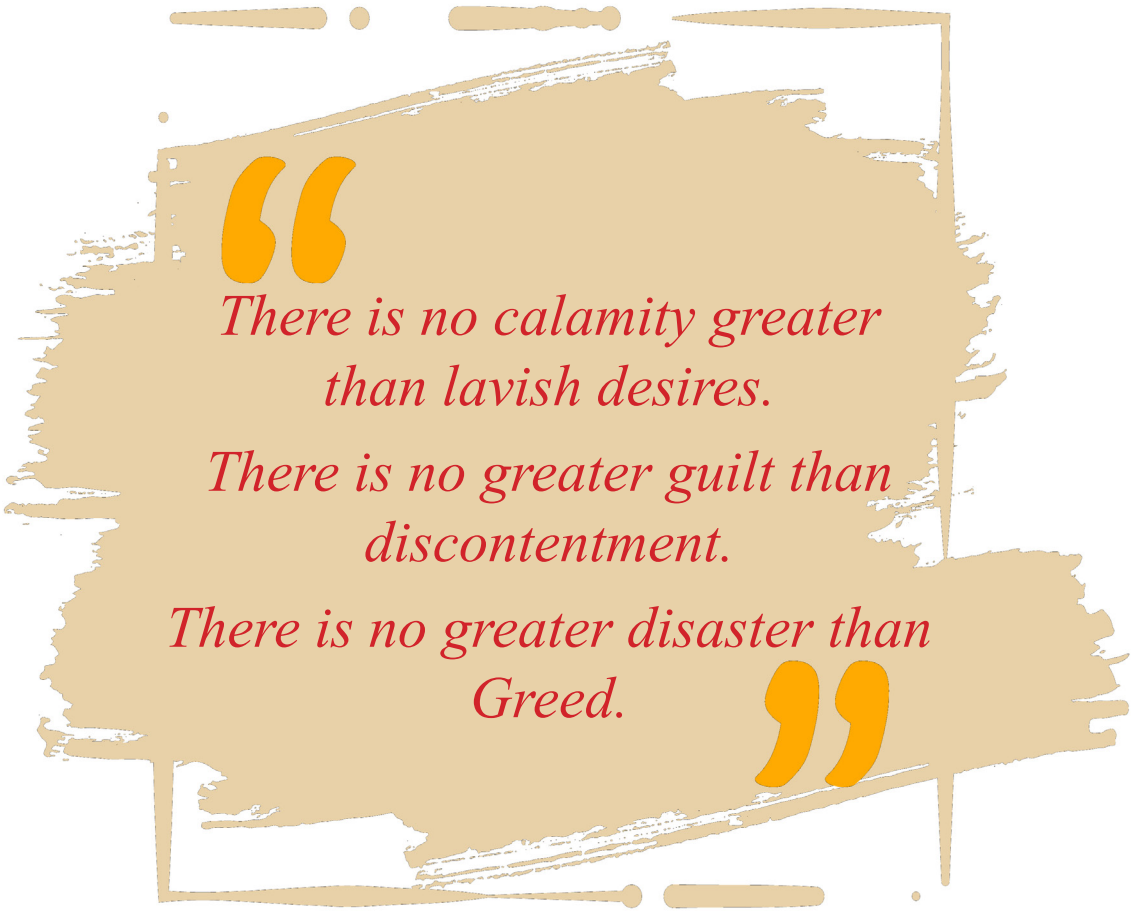
At last, the customer realised his mistakes by already sharing sensitive personal details with fraudsters. Our staff reassured him and immediately took action like stopped all his international transaction access, temporarily blocked UPI and guided him to report the issue on 1930 and cybercrime.gov.in.

The customer thanked her and all other bank staff for their timely intervention.

2. **SBI STAFF PRESENCE OF MIND AVERTS DIGITAL ARREST SCAM**
   State Bank of India staff of Kendrapara Bazar branch saved one of its customers from digital arrest and cyber fraud on 14.07.2025

   Sri Prasanta Kumar Sahoo, customer of our Kendrapara Bazar branch was digitally arrested by some imposter citing that his personal details like Aadhar No. is complicit in illegal activity. The imposter shared letter of RBI, CBI and Enforcement Directorate with the customer and demanded money. Out of fear the customer made withdrawal of Rs.49900.00 from his account to deposit cash of 1.00 lakh in the account of the

fraudster and transfer 2.00 lakhs afterwards. Smelling some mishappening, the dealing SWO Mrs. Subhashree Mohanty approached the Branch Manager Shri Mukesh Kumar Samal along with the customer. On verifying all the data and video calls, the Branch Manager became sure of the fraud. He then explained to the customer regarding the fraud and convinced him that he has been digitally arrested by the imposter and this is a new fraudulent way to extract money from innocent people. He advised him to block the mobile number from which calls are being received and inform the same immediately to Cyber Crime Cell. Due to timely intervention and counselling by the Branch Manager, a financial loss of Rs.3.00 lakhs to the customer could be averted.



# Initiatives by Reserve Bank of India

RBI urges the members of public to practice safe digital banking by taking all due precautions, while carrying out any digital (online / mobile) banking / payment transactions. These will help in preventing financial and / or other loss to them.

## SAFE DIGITAL BANKING PRACTICES

- Never share your account details such as account number, login ID, password, PIN, UPI-PIN, OTP, ATM / Debit card / credit card details with anyone, not even with bank officials, however genuine they might sound.
- Do not download any unknown app on your phone / device. The app may access your confidential data secretly.
- Transactions involving receipt of money do not require scanning barcodes / QR codes or entering MPIN. Thus, exercise caution if asked to do so.
- Any phone call / email threatening the blocking of your account on the pretext of non-updation of KYC and suggestion to click link for updating the same is a common modus operandi of fraudsters. Do not respond to offers for getting KYC updated / expedited. Always access the official website of your bank / NBFC / e-wallet provider or contact the branch.
- Always access the official website of bank / NBFC / e-wallet provider for contact details. Contact numbers on internet search engines may be fraudulent.
- Check URLs and domain names received in emails / SMSs for spelling errors. Use only verified, secured, and trusted websites / apps for online banking, that is, websites starting with ''https". In case of suspicion, notify local police / cybercrime branch immediately.
- If you receive an OTP for debiting your account for a transaction not initiated by you, inform your bank / e-wallet provider immediately. If you receive a debit SMS for a transaction not done, inform your bank / e-wallet provider immediately and block all modes of debit, including UPI. If you suspect any fraudulent activity in your account, check for any addition to the beneficiary list enabled for internet / mobile banking.
- Do not share the password of your email linked to your bank / e-wallet account. Do not have common passwords for e-commerce / social media sites and your bank account / email linked to your bank account. Avoid banking through public, open or free networks.
- Do not set your email password as the word "password" while registering in any website / application with your email as user-id. The password used for accessing your email, especially if linked with your account, should be unique and used only for email access and not for accessing any other website / application.

- Do not be misled by advices intimating deposit of money on your behalf with RBI for foreign remittances, receipt of commission, or wins of lottery.
- Regularly check your email and phone messages for alerts from your financial service provider. Report any un-authorized transaction observed to your bank / NBFC / Service provider immediately for blocking the card / account / wallet, so as to prevent any further losses.
- Secure your cards and set daily limit for transactions. You may also set limits and activate / deactivate for domestic / international use. This can limit loss due to fraud.

**RBI Advertisement in Newspapers:**

Beware of impersonation / parcel scams!

Beware of audio/video calls from CYBERCRIMINALS posing as officials from RBI/ Banks/ Government Agencies/ Courier Companies THREATENING with Legal Action or Asking for Immediate Transfer of Money or Freezing or Blocking your bank accounts or debit/ credit cards.

**DON'Ts**

- Don't panic – fraudsters may trap you
- Don't share any personal information
- Don't click on unknown links for making payments

**DO's**

- Always verify the genuineness of the caller/ fund request
- Immediately report to cybercrime.gov.in or call 1930 for help

**RBI asked banks to collaborate with Mulehunter.ai initiative to weed out mule accounts used in financial frauds.**

Mulehunter.ai has been developed by the Reserve Bank Innovation Hub to help banks deal with mule bank accounts expeditiously and reduce digital frauds. The initiative is being piloted with two public sector banks.

"Financial frauds involving mule accounts have become a significant challenge for the banking industry and the Indian economy, with some large banks reporting fraudulent transactions of `400500 crore every month. These accounts, often used to launder proceeds of cybercrimes, undermine trust in the financial system," said Chief Executive Officer, BCT Digital.

"The centre froze around Rs. 4.5 lakh mule bank accounts in the past year, showcasing the scale and urgency of the issue."

CEO further said that the RBI is running a hackathon on 'zero financial frauds'. It also aims to develop innovative solutions to contain the use of mule accounts.

Meanwhile, the central bank proposed to constitute a committee to develop a framework for responsible and ethical enablement of AI (Freeai) in the financial sector

The RBI remarked that technologies like artificial intelligence, machine learning, tokenisation, cloud computing hold huge potential as they can handle enormous volumes of data, automate processes, enhance decisionmaking, and bring in efficiencies.

"While the benefits are many, the attendant risks like algorithmic bias, explainability of decisions, data privacy, etc, are also high. To harness the benefits, it is critical to address the attendant risks early in the adoption cycle," said the RBI.

## EXCLUSIVE '.bank.in' & '.fin.in' Domain

A Verified & Exclusive Domain The **.bank.in** domain is exclusive to financial institutions verified and regulated by the Reserve Bank of India (RBI) and .fin.in for non-banking financial companies (NBFCs), insurance companies, fintech firms, and other registered financial service providers in India.RBI has mandated all licensed banks to migrate to this domain by October 31, 2025.This prevents fraudsters from easily creating fake lookalike websites.

Enhanced Security this initiative is a direct response to rising digital payment fraud, designed to strengthen the cyber security framework and minimize phishing attacks.

Easy Identification The uniform .bank.in suffix makes it simpler for customers to visually identify genuine banking websites, enhancing public confidence in digital banking.

Examples of Bank Websites: Several major banks have already migrated to the new domain. You can now access their net banking services at:

State Bank of India (SBI): https://onlinesbi.sbi.bank.in/
Indian Bank: https://indianbank.bank.in/
ICICI Bank: https://www.icici.bank.in/
HDFC Bank: https://www.hdfc.bank.in/

## The 1600xx series

The 1600 series is an initiative led by the Telecom Regulatory Authority of India (TRAI), in collaboration with the Department of Telecommunications (DoT) and financial sector regulators including the Reserve Bank of India (RBI) and the Securities and Exchange Board of India (SEBI).

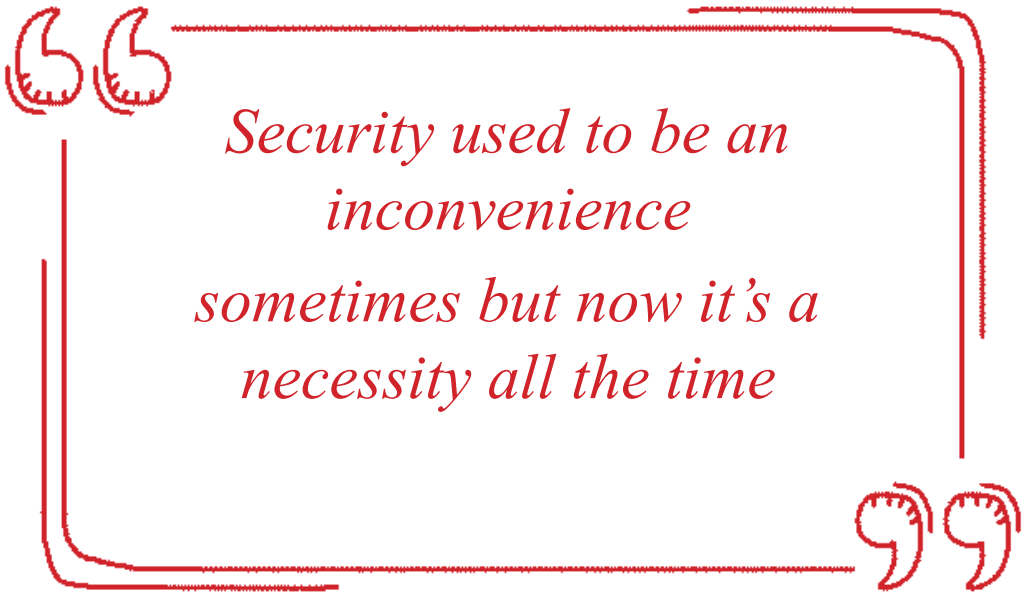
The State Bank of India (SBI) has already started using this system for its service calls. The bank assures that calls from numbers starting with +91-1600 are genuine and secure. SBI uses these exclusively for important service-related communication.

SBI's Official Advisory: "If you receive a call from a number starting with +91-1600, rest

assured-it's a genuine and legitimate call. These numbers are used for transactional and service-related calls to customers".

SBI has published a list of official 1600 numbers they use, including 1600-01-8000, 1600-11-7012, and several others.

Purpose To create a trusted, exclusive numbering series for service/transactional calls from financial entities, helping customers distinguish them from spam and fraudulent calls.



# You should Know

## Not all cybercriminals are super-qualified professionals

More than half of those suspected of committing cyber fraud are not super-qualified professionals, it turns out.

About 35 per cent had only cleared their SSC or had dropped out earlier, and another 20 per cent had only cleared their Intermediate, according to data developed by the Telangana Cybercrime Security Bureau.

The bureau said the remaining 45 per cent of those indulging in cyber fraud were techies with BTech of MCA degrees or those holding MBA, after analysing data pertaining to 165 persons it had arrested from across the country in the six months.

The bureau said these 165 suspects were wanted in 795 cybercrime cases in the state and 3,357 cases across the country. The bureau also said that almost half 49 per cent to be exact of cybercrime suspects were in the age group of 21-30 years.

Among the suspects, 34 per cent identified themselves as businessmen, hoteliers and realtors by profession. The rest included digital content creators, cab drivers, gym trainers, event managers, quacks, and those employed in a variety of establishments including delivery services.

Among the others were the unemployed (14 per cent), students (nine), farmers and labourers (five) and government employees (three per cent. The bureau said the major factors behind their involvement included earning easy money, criminal family background, debts, and the influence of a third person.

## FAKE CUSTOMER CARE SCAMS

"Attention, valued customer, your credit card is at risk of being blocked unless you provide the last 4 digits of your card number immediately!" Such alarming calls are all too common, exploiting urgency and fear to manipulate unsuspecting victims.

Each day, we receive a plethora of customer care calls with claims of lottery wins, retail discounts, and urgent banking matters. However, a significant portion of these calls are not what they seem, they are fake customer care scam calls.

A fake customer care scam occurs when individuals receive calls from seemingly legitimate helpline numbers that are, in fact, fronts for scammers. These impostors impersonate representatives from reputable brands or services, creating convincing scenarios designed to dupe unsuspecting victims into taking urgent and ill-advised actions.

The real challenge lies in distinguishing between a genuine customer care call and a fake customer care scam call.

### Fake Customer Care Scams via UPI Platforms

The **Unified Payment Interface** (UPI) has revolutionised our payment habits, allowing us to confidently go cashless as nearly every establishment now supports UPI transactions. However, this widespread adoption has also attracted scammers, leading to a surge in fake customer care scams.

UPI enables instant fund transfers, a feature that scammers take advantage of to execute their fake customer care scams. Unlike traditional bank transfers that might take time to reflect, UPI transactions happen in seconds, making it easier for fraudsters to extract money from victims. According to government data, over 95,000 UPI fraud cases have been reported in India, highlighting the growing risks of fake customer care scams.

Fake customer care scams via UPI are rapidly increasing, with the number of fraud cases doubling each year. Recognising the signs of a fake customer care scam and understanding how scammers operate can help you safeguard your financial transactions and personal information.

#### WHAT TO DO IF YOU FELL FOR ONLINE SCAM?

If you fall victim to such a scam and lose money, here are the steps you should take to mitigate the damage and prevent further loss.

Stop Communication: First of all, cease all contact with the scammer. Don't respond to their calls, emails, or messages.
Notify Your Bank or Payment Service Provider: After ceasing communication, contact your bank or the payment service provider (such as Paytm, Google Pay, or PayPal) immediately. Explain the situation in detail and request them to block your account to prevent further unauthorised transactions. Most banks have a 24-hour customer service number specifically for reporting fraud. Early reporting increases the likelihood of recovering your money.

Change Your Passwords and Secure Your Accounts: Meanwhile, change the passwords for all your online accounts, especially those related to banking and financial services. Use strong, unique passwords that combine letters, numbers, and special characters. Enable two-factor authentication (2FA) where possible to add an extra layer of security. Also, if you use online banking, block your debit or credit cards.

Report online scam to cyber cell

Provide all relevant details, including transaction IDs, emails, and any communication with the scammer. Note that the earlier you inform the authorities, the better the chances of recovering your money.

**The message circulated by Telecom Regulatory Authority of India (TRAI), in this connection, is reproduced hereunder:**

"TRAI never sends any message or makes any call for verification/ disconnection/ reporting unlawful activities of mobile numbers. Beware of such messages / calls in the name of TRAI. Any call or message claiming to be from TRAI should be considered potentially fraudulent and may be reported to the National Cyber Crime Reporting Portal (www.cybercrime.gov.in) or Cyber Crime Helpline (1930)"

### What should you do if you have got a fraud bank SMS and a call?

One of the agendas of these fraudsters is to create a sense of urgency, hence when they call you, they will say things like: "I am at the doctor's chamber and need you to pay me back" or "I am at the medicine shop buying life-saving medicines" etc. The primary motive behind this urgency is to make you ignore the sender's ID of the SMS which is a regular 10-digit mobile number and not a real bank's sender ID.

Experts say that one should be cautious and check the sender ID before taking any action based on the SMS.

"To combat these scams, individuals must scrutinise message content, verify sender details and its ID, and closely examine domains, logos, and grammar for inconsistencies. Additionally, it is important to be cautious of urgent or immediate action requests that come across as unprofessional, as legitimate institutions typically communicate in a more professional and measured manner. By staying vigilant and adopting proactive security measures, users can thwart these increasingly sophisticated smishing attempts." **New cybercrime targets housewives, students**

### Pig butchering scam is a global phenomenon and involves money laundering and cyber slavery

A new cyber fraud known as "pig butchering scam" or "investment scam" has emerged, targeting unemployed youths, housewives, students, and needy people who are made to lose large sums of money daily, the latest annual report of the Union home ministry has said.

As per report, the cybercriminals have also been using Google services platforms to initiate these crimes. "Google Advertisement platform provides a convenient facility for targeted advertisement from across the border. This scam, known as 'Pig Butchering Scam' or 'Investment Scam' is a global phenomenon and involves large-scale money laundering and even cyber slavery," it said.

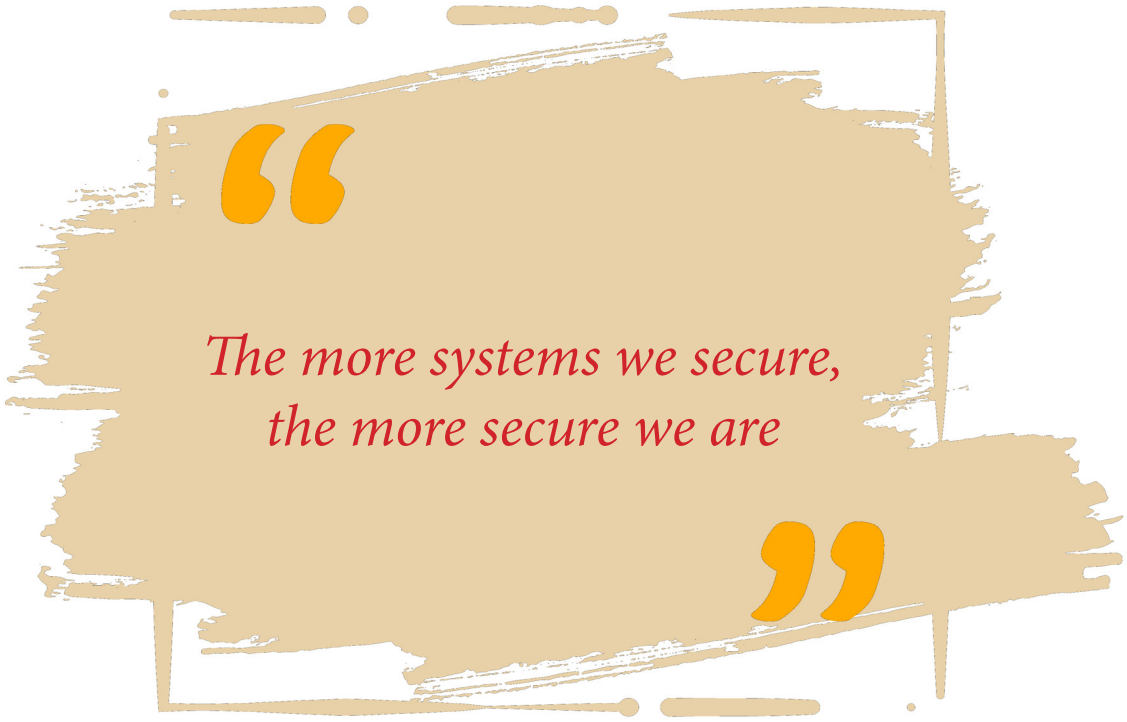
To curb the menace, the Indian Cyber Crime Coordination Centre (I4C), under the Union home ministry has partnered with Google to share the threat intelligence for urgent action periodically.The cybercriminals are using sponsored Facebook to launch illegal lending applications in India, the report said. "Such links are proactively identified and shared with Facebook, along with Facebook pages for necessary action," it said.

Whatsapp remains the biggest social media platform that is possibly misused by cyber criminals in India, the report said. The data published in the report on "cyber crimecomplaints where Big Tech platforms have been misused" shows that 14,746 complaints were related to Whatsapp, 7,651 against Telegram, 7,152 against Instagram, 7,051 against Facebook, and 1,135 against Youtube till March 2024.

"Big techs play an important role in proactive identification and action on cyber criminals. I4C has partnered with Google and Facebook for sharing intelligence and signals for proactive actions," the report said.

National Cybercrime Threat Analytical Unit (NCTAU) of I4C analyses the complaints reported on the portal and prepares analysis reports on the latest trends of cybercrime and misuse of services provided by service providers, it said."These reports are shared with all the concerned stakeholders such as banks, wallets, merchants, payments aggregators, payment gateways, ecommerce and other departments to take preventive measures and mitigate the misuse of their platforms/services," the report said.

The pig butchering scam, which is believed to have started in China in 2016, targets gullible individuals with whom cyber criminals build trust over time, ultimately convincing them to invest in crypto currency or some other lucrative scheme when their money is stolen. The analogy to pig butchering comes from the fattening of swine before their slaughter. The ministry has also rolled out a cyber volunteer framework, which enables citizens to enrol as cyber volunteers for reporting unlawful content on the Internet.



# Protect Yourself

The increased usage of internet services and smartphones has made social networking one of the most popular online activities. Social media enables users to connect, communicate and share information, photographs or videos with anyone across the globe. Some of the popular social media platforms are Facebook, Twitter, Instagram, YouTube, LinkedIn, WhatsApp, Snapchat, Tinder, Hike, WeChat, Tumblr etc.

The penetration of social media is continuously increasing worldwide. The tremendous growth in use of social media platforms / social networking platforms has provided a fertile ground to cyber criminals to engage in illegal activities.

Here are some of important steps you should take to protect yourself and your information while using social media platforms :

Do not accept friend requests from strangers on social networking sites.

Do not trust online users unless you know and can trust them in real life.

Do not share your personal information such as address, phone number, date of birth etc. on social media. Identity thieves can easily access and use this information Do not share your sensitive personal photographs and videos on social media.

Share your photos and videos only with your trusted friends by selecting right privacy settings on social media

Immediately inform the social media service provider, if you notice that a fake account has been created by using your personal information.

Always use a strong password by using alphabets in upper case and lower case, numbers and special characters for your social media accounts

Do not share your vacations, travel plans etc. on social media

Do not allow social networking sites to scan your email account to look for your friends and send spam mails to them without your consent or knowledge.

Always keep location services turned off on your devices unless necessary.

Do not announce your vacations, travel plans etc. on social media. Criminals can use it as an opportunity for theft etc.

When chatting with someone online and you feel suspicious about your chat partner, try asking some unrelated scientific or mathematical questions. If it does not answer or acknowledge the question, it may mean that you are chatting with an automated computer bot.

Do not use public computer/ cyber cafe to access social networking websites, it may be infected/ installed with a key logger application which will capture your keystrokes including the login credentials.

Many social networking sites prompt you to download third-party applications that lets you access more pages. Do not download unverified third-party applications without doing research about its safety.

Do not hesitate to report, if someone is posting offensive and abusive content on social media.

Do not share or forward unverified posts/ news on social media forums. These may contain fake news or contain sensitive information which may mislead people.

## FIVE WAYS TO PROTECT YOURSELF AGAINST FAKE CUSTOMER CARE SCAMS

### Practice Caution

Fraudsters often disguise themselves as family members, friends, or known contacts to gain your trust. Always listen carefully and verify the phone number before transferring money to any unknown link. This vigilance can help you avoid falling victim to a fake customer care scam.

### Do Not Engage with Unknown Links

If you receive a payment request on your UPI app from an unknown account, always decline it. Engaging with unknown links is a common tactic used in fake customer care scams to extract money from unsuspecting users.

### Never Reveal Your PIN to Strangers

Scammers might create a sense of urgency, pretending to help you through a difficult situation, and then ask for your PIN. Remember, never share your PIN with anyone, as it is the key to finalising any transaction. Revealing it can easily lead to a fake customer care scam.

### Avoid Downloading Unverified Apps

Many fraudulent apps mimic the appearance of legitimate banking apps to deceive users. These counterfeit apps can be downloaded and installed easily, leading to the theft of sensitive data. Always verify the authenticity of an app before downloading it to protect yourself from fake customer care scams.

### Enable and Monitor Notifications

Keep push notifications and transaction alerts enabled on your UPI apps. Regular updates to your UPI apps ensure you are protected with the latest security measures. Monitoring your notifications helps you stay informed about every transaction, which is crucial in defending against a fake customer care scam.

## HOW TO PROTECT YOURSELF FROM ONLINE SCAMS?

**Be Wary of Unsolicited Offers :** If an offer seems too good to be true, it probably is not. Do not get lured by unrealistic promises of high returns or easy money.

**Verify Information :** Always double-check the sender's email address, website legitimacy, and phone numbers before clicking on links or sharing personal information.

**Beware of Emotional Triggers :** Scammers often use fear, like threats of legal action, or excitement to manipulate emotions. Stay calm and exercise caution.

**Strong Passwords & 2FA :** Use strong, unique passwords for all your online accounts and enable two-factor authentication wherever available.

**Stay Informed :** Educate yourself about common online scams and keep up-to-date with the latest tactics used by fraudsters.

VOICE CLONING SCAMS can be particularly hard to detect, as the voice sounds genuine. However, we need to exercise the following precautions:

* Be wary of unexpected calls or messages, especially from unknown numbers or claiming urgency.
* Pay attention to any inconsistency in the voice, like robotic-sounding delivery or unnatural pauses.
* Be cautious about sharing your voice online.
* Limit the amount of personal information you share publicly including audio recordings.
* Verify caller Identity – Do not trust caller ID alone. Always try to verify the caller's identity through other channels before sharing any personal information.

## PRECAUTIONS TO PROTECT FROM FALLING PREY TO TELECOM/BANK SCAMS

Individuals must exercise caution when receiving unsolicited calls from unknown numbers.

Individuals must refrain from pressing any numbers or divulging personal details, which is essential.

Individuals must verify the authenticity of calls by contacting the relevant organizations directly that can help prevent financial loss and reputational damage.

There are a few things to keep in mind that will help you protect yourself against these attacks through **FRAUD BANK SMS AND A CALL**

**Do not respond.** Even prompts to reply like texting "STOP" to unsubscribe can be a trick to identify active phone numbers.

**Slow down if a message is urgent.**

**Call your bank or merchant directly if doubtful.**

**Avoid using any links or contact info in the message.**

**Check the phone number.** Odd-looking phone numbers, such as 4-digit ones, can be evidence of email-to-text services. This is one of many tactics a scammer can use to mask their true phone number.

*Cybersecurity is a race between attackers and Defenders.*
*Staying informed is the Only way win.*

*Cybercrime isn't just about stealing money;*
*it's about stealing identities,*
*Trust, and even lives*