BIJU PATNAIK STATE POLICE ACADEMY ODISHA

THOUGHT KNOWLEDGE VISION

akshaya

Awareness on various Cyber Crime Offences

Cyber crimes, climate change new threats to human rights: President Murmu

In her address at an event hosted by the NHRC here to mark the Human Rights Day, the President also underlined that cyber crimes and climate change are new threats to human rights

Cyber crimes and climate change are new threats to human rights," President Murmu said.
"The digital era, while being transformative, had brought with it complex issues such as cyber bullying, deep fake, privacy concerns and spread of misinformation," she added.

DIGITAL ARRESTS: THIS IS WHAT PM MODI SAID...

6.7L SIMs, 1.3L IMEIs suspected to be linked to cybercrimes blocked: Govt

TIMES NEWS NETWORK

New Delhi: Around 6.7 lakh SIM cards and 1.32 lakh IMEIs (international mobile equipment identity) suspected to be linked to cybercrimes have been blocked by the govt till Nov 15 this year, the home ministry informed Rajya Sabha on Wednesday.

Detailing the mechanisms put in place to deal with cybercrimes, including digital arrests, junior home minister Bandi Sanjay Kumar said the central govt and telecom service providers (TSPs) have devised a system to identify and block incoming international spoofed calls made by cybercriminals in recent cases of digital arrests, "FedEx scams" and impersonation as

MHA REPORT IN RAJYA SABHA

govt or police officers, among others. "Directions have been issued to TSPs for blocking of such incoming international spoofed calls," Kumar said in a written reply to a question in the House.

The ministry said the 'Citizen Financial Cyber Fraud Reporting and Management System', under I4C, was launched in 2021 for immediate reporting of financial frauds and to stop siphoning off funds by fraudsters. So far, a financial amount of more than Rs 3,431 crore has been saved in more than 9.94 lakh complaints.

On infrastructure created to prevent and counter cybercrimes, it said a cyber fraud mitigation centre has been set up within the Indian Cyber Crime Coordination Centre (I4C), with representatives of major banks, financial intermediaries, payment aggregators, TSPs, IT intermediaries and state/UT law enforcement agencies.

Samanvaya was made operational from April 2022 to serve as a joint management information system platform, data repository and a coordination platform for LEAs for cybercrime data sharing and analytics. It provides analytics-based inter-state linkages of crimes and criminals. The module 'Pratibimb' maps locations of criminals and crime infrastructure on a map to give visibility to jurisdictional officers.

A suspect registry of identifiers of cybercriminals was launched by I4C on Sept 10 in collaboration with banks and financial institutions.

Seven joint cyber coordination teams (JCCTs) have been constituted for Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Visakhapatnam, and Guwahati, based upon cybercrime hotspots/areas having multi-jurisdictional issues.

Digital Arrest

An organized online economic crime operated by cross-border crime Syndicates

Other nomenclature:

- TRAI Phone Scam
- Parcel Stuck at Customs
- Family Member Arrested

Modus Operandi

- The fraudsters under the guise of law enforcement officials or regulatory authorities like CBI/TRAI/ED/Income Tax/Customs Department/ Mumbai & Delhi Police usually contacted a potential victim through the following means:
  - WhatsApp (+92 Numbers with DP of Senior Police Officials)
  - Calls through Skype (Having Logo of Maharashtra Police / Delhi Police)
  - E-mail (Spoof e-mails resembling Police Organization)

Methods Adopted

With an information that the victim has sent or intended recipient of a **parcel**, which contains illegal goods, drugs, fake passports or any other contraband item.

Another Method adopted

The fraudsters are posing as officials of TRAI, saying that his / her phone number was being used to circulate illegal obscene videos.

Modus Operandi

- The unsuspecting victims are made to undergo “Digital Arrest” and remain visually available over Skype or other video conferencing platform to the fraudsters, till their demands are met.
- False arrest warrant will be served through WhatsApp/ mail.
- The fraudsters are known to use studios modeled on Police Stations, Government offices, Fake Court Rooms and wear uniforms / dresses to appear genuine.
- The Victim Persons are grilled for hours & hours till transfer of money.

Transaction Processes involved:

- Then money will be demanded to compromise the case.
- Transaction Processes involved:

[Money transferred to a number of bank accounts]

  - Money transferred through NEFT/ RTGS/IMPS [Internet Banking]
  - UPI
  - Deposit through Cash / Cheque

Bengaluru journalist loses Rs 1.20 crore in FedEx courier scam

Cyber fraudsters, posing as FedEx courier staff and a Narcotics Control Bureau official, told the woman that they claimed to possess a parcel in her name that contained illegal items.

By: Express News Service

Bengaluru | Updated: January 17, 2024 09:16 IST

NewsGuard

Follow Us

Lucknow Professor Loses Rs 2.81 Crore In 'Digital Arrest' Scam: How To Stay Safe

A Lucknow professor lost Rs 2.81 crore in a 'Digital Arrest' scam. Learn crucial tips to protect yourself from similar cyber frauds.

Authored by: Shubham Arora | Updated Aug 16, 2024, 13:32 IST

TOI City Ahmedabad Mumbai Delhi Bengaluru Hyderabad Kolkata Chennai Agra Agartala •••

4 Taiwanese men among 17 held for 'digital arrest' fraud in Ahmedabad

TNN / Updated: Oct 15, 2024, 08:13 IST

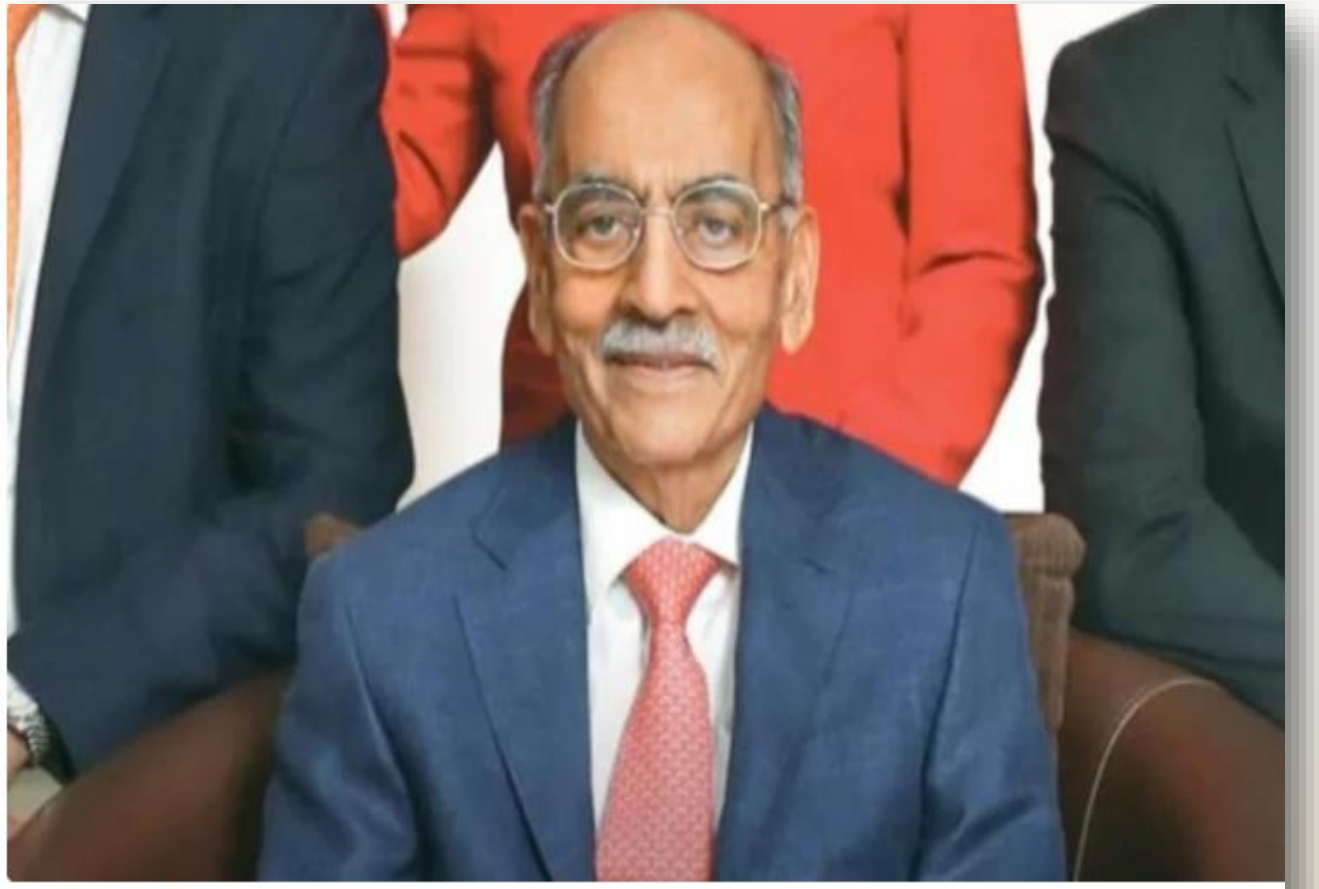
SHARE AA FOLLOW US

Ahmedabad cybercrime branch arrested 17 people, including four Taiwanese nationals, for running a 'digital arrest' racket. Victims were confined and forced to transfer large sums of money. The racket involved using apps to transfer money to accoun ... Read More

AHMEDABAD: Seventeen individuals, including four from Taiwan, were arrested by Ahmedabad cybercrime branch on Monday for allegedly operating a nationwide "digital arrest" racket.

Digital arrest and Rs 7 crore heist: How Vardhman Group head was tricked

The fraudsters used fake court orders and impersonated the Chief Justice of India to convince Oswal he was part of a money laundering investigation



Vardhman Group CEO S P Oswal. (Photo Credit: Vardhman.Com)

Case Scenario:

- Suspected in a money laundering investigation
- Fraudsters posed as CBI Officials
- Serving of False Arrest Warrant duly issued by ED
- “Digital arrest" for two days
- Direction to deposit Rs. 7 crore into different bank accounts
- Supreme Court order sent to Oswal appeared authentic, complete with the court's emblem, bar code, and digital signature
- Fake Court Room of CJI
- Arrest of 02 accused persons from Assam
- Recovery of Rs. 5 Crore

CYBER CRIME

Over 1,000 Skype IDs Blocked: Inside the Government's Battle Against 'Digital Arrest' Scams

– Fake officials use Skype to enforce 'Digital Arrests'
– Government blocks over 1,000 IDs to combat fraud

Government Issues Instructions To Block Thousands Of Mobile Phones To Curb Cyber Fraud

The central government has entered mission mode to halt cyber fraud occurring across the country. The Department of Telecom, police of different states, and the Home Ministry have collectively decided to block 28,200 mobile phones. Additionally, more than 20 lakh mobile numbers will be re-verified - Reports ETV Bharat's Saurabh Shukla.

DIP & Chakshu: Government Launches Powerful Weapons Against Cybercrime

DoT's new tools to combat cyber fraud: Digital Intelligence Platform & Chakshu on Sanchar Saathi

Operation Thiraineeku: Tamil Nadu police arrest 70 cyber fraudsters in three days

> *This large-scale operation was based on accused profiling through the NCRP (National Cyber Crime Reporting) Portal and databases with the Indian Cyber Crime Coordination Centre (I4C) and also through bank fund trail linkages established by financial data analysis of cybercriminal networks, targeting those involved in 158 NCRP complaints.*

STOP sharing your personal information

THINK why a govt agency will threaten you on the phone

TAKE ACTION by disconnecting the call & reporting the scam on 1930

Arrested on a call

POLICE OR CYBER THUG?

DIRECTORATE OF ENFORCEMENT

Foreign Exchange Management Act (FEMA) &
Prevention of Money Laundering Act (PMLA)
Ministry of Finance Dept. of Revenue

Issuing unit: Supreme Court of India **12/06/2024**
Co-organizer: Central Bureau of Investigation
Suspect : **DURGA PRASAD BEHERA** Aadhaar Card No: **(9371-9510-2224)**

Description: Arrest and Freezing control orders
Execute the warrants before: **12/06/2024**

Subject: The suspect **DURGA PRASAD BEHERA** with Aadhaar Card No: **(9371-9510-2224)** involved in the case is suspected of providing personal information for the main suspect Shri Ashok Gupta to open an illegal account at HDFC Bank, which has been involved in money laundering case.

1. According to the provisions of the Anti-Money Laundering Regulations, the law enforcement department of the Supreme Court of India may notify criminal suspect to report the flow of funds in the account, prove the flow of funds, and prove the flow of funds in the account, property, or provide other necessary materials, and refer all funds to the Supreme Court to review whether there is illegal black money related to the money laundered Rs 6.8 crore.

2. Suspect alleged in Money Laundering, against with the Law Enforcement Violations. All properties and materials (including land, houses, cars, deposits, investments, salary income, etc.) must be prepared according to their usage. According to the Marriage Law of our country, the property acquired by the husband and wife during the existence of the marriage relationship shall be jointly owned by the both. The husband and wife have equal rights to dispose of common property, and the department should jointly check, accept investigation, explain the status of the property, and freeze the collection according to law.

3. According to The Prevention of Money-Laundering Act, 2002 of Section 3, Section 4, Section 10, the "Financial Regulations", who does not appear in court without justifiable reasons, and fails to cooperate after being notified in accordance with the law, the court will order the suspect to appear in court. Case (including confiscation of property, wanted persons, restricted exit, etc. must apply to the prosecutorate for arrest and detention).

04. The suspect involved in this case shall not publish any content related to this case in any form (communication, broadcast, speech) during the investigation and trial. In case of violation, it will be punished as the crime of intentionally leaking National Secrets in accordance with the provisions of Article 209 of the IPC of our country, the punishments under the Act range from three to seven years of imprisonment and a fine of INR 5,00,000.00. A person prosecuted under this Act can be charged with the crime even if the action was unintentional and not intended to endanger the security of the state.

5. The receiver of an execution order for criminal detention shall be detained immediately, for 21 days and their property shall be frozen for 27 months, effective immediately.

Rahul Navin

Rahul Navin,Assistant Director,

Directorate of Enforcement Delhi

ACKNOWLEDGEMENT LETTER FROM FINANCIAL DEPARTMENT

MUMBAI CRIME BRANCH AND CENTRAL BUREAU OF INVESTIGATION

MONEY LAUNDERING CASE Mrs. SAROJINI BRAHMA Indian Nationality number 4367 0171 9350 suspected for money laundering and drug dealing case. That person bank accounts to be verified with financial and CBI department of India. The person bank accounts having legal amount transferred to financial department and the amount will be verified and refunded after the verification of 15 minutes of investigation time. { If having some illegal transactions in bank account, we don't transfer the money back to the same account }

1.Three types of cases are charged against this person. money laundering, drug dealing, and smuggling.

2.We have a suspect that the accused person has linked with international criminal Mohammad islam malik {nawab malik} suspected person also suspect for receiving an illegal amount in her account.

3.This person bank accounts and bank amount to be fully verified by the CBI department and financial department.

4.In-case of misunderstanding ,if the person does not want to verify her bank accounts and account funds,immediately email to the RBI department for freezing of all accounts and all the account funds and send her the order of property detention and arrest warrant. also within 1 hour take her to the custody.

5.The case will be proceeding under the section shall be deemed to be judicial proceeding within the meaning of section 193 {PMLA - PREVENTATION OF MONEY LAUNDERING} and section 228 of the Indian penal code {IPC} ,you will be processed under the {CRPC - 436A} session of judicial division within one hour. This is approved by CBI and crime branch Department.

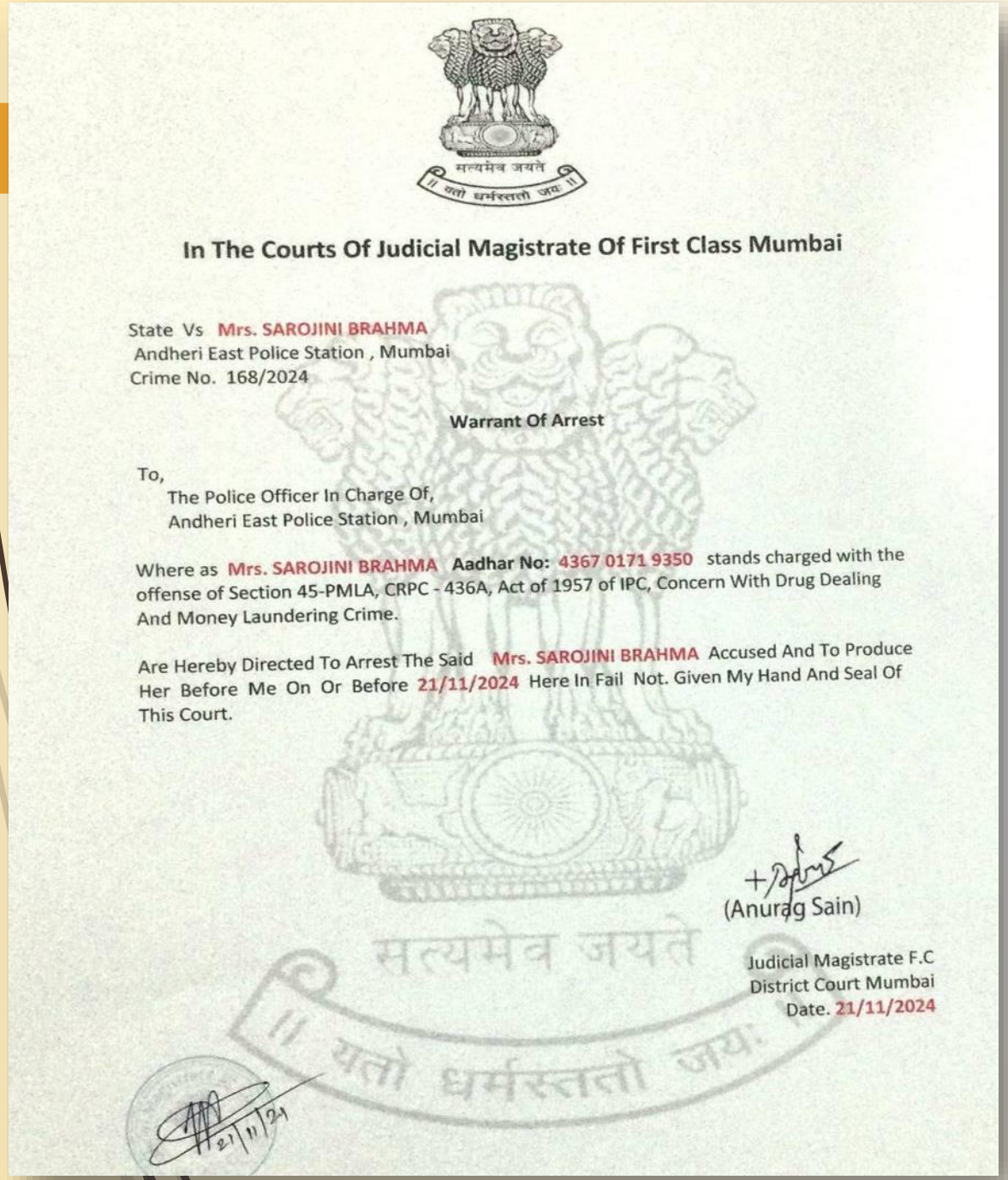
6. IPC INDIAN PENAL CODE
The case against the person falsification of accounts and receiving the illegal amount under the act of 477 CRPC - PMLA 45 (PREVENTATION OF MONEY LAUNDERING ACT) it carries the same Punishment as act of 477A which is imprisonment of 7 years with 20 lakhs of fine.

Department officials involving in this case.

1.MILIND BHARAMBE D.C.P {CYBER CRIME}

2.NITIN PATIL IPS {CRIME BRANCH COMMISSIONER}

3.GEORGE MATHEW IPS {FINANCIAL DEPARTMENT}



सत्यमेव जयते
यतो धर्मस्ततो जयः

In The Courts Of Judicial Magistrate Of First Class Mumbai

State Vs **Mrs. SAROJINI BRAHMA**
Andheri East Police Station , Mumbai
Crime No. 168/2024

Warrant Of Arrest

To,
The Police Officer In Charge Of,
Andheri East Police Station , Mumbai

Where as **Mrs. SAROJINI BRAHMA** **Aadhar No: 4367 0171 9350** stands charged with the offense of Section 45-PMLA, CRPC - 436A, Act of 1957 of IPC, Concern With Drug Dealing And Money Laundering Crime.

Are Hereby Directed To Arrest The Said **Mrs. SAROJINI BRAHMA** Accused And To Produce Her Before Me On Or Before **21/11/2024** Here In Fail Not. Given My Hand And Seal Of This Court.

(Anurag Sain)

Judicial Magistrate F.C
District Court Mumbai
Date. **21/11/2024**

सत्यमेव जयते
यतो धर्मस्ततो जयः

21/11/24

Fake Arrest Warrant

Beware of Digital Arrest

Don't Panic

There is no concept of Digital or Virtual arrest in the Indian Law

Legal Provisions:

- FIR will be registered against the fraudsters u/s 308(2)/318(2)/318(4)/319(2)/336(2)/336(3)/351 (2)/ 351(3)/351(4)/61 (2) (b)/3 (5) of BNS r/w Sec. 66C/66D of Information Technology Act

Remedies available:

- Nationalized Cyber Crime Help Desk Number: **Dial 1930 to file complaint**
- Complaint through www.cybercrime.gov.in
- Complaint to be filed at the nearest Police Station / Cyber Crime Police Station
- Complaint to be filed at the concerned Bank

Investment Fraud

Beware... No risk, high return tips cost Rs 37 crore to investors

Sep 9, 2024, 22:15 IST

SHARE | AA | FOLLOW US

Bhopal: In recent months, the state capital has witnessed a sharp rise in cyberfraud cases, with scammers luring unsuspecting victims into bogus stock market investment schemes. Promising high returns and leveraging the growing interest in online trading, fraudsters use exploiting digital platforms to siphon off money from individuals eager to invest.

The cybercriminals utilise WhatsApp or Telegram groups to carry out their scams.

Bengaluru techie couple loses ₹1.53 crore in investment scam, cops recover ₹1.4 crore: Report

THE ECONOMIC TIMES | News

Subscribe | Sign In

Festive Offer on ETPrime

English Edition ▾ | Today's ePaper

Home | ETPrime | Markets | Market Data | News | Industry | Rise | Politics | Wealth | MF | Tech | Careers | Opinion | NRI | Panache | Luxury | Videos

India | Decoded | Web Stories | Morning Brief Podcast | Newsblogs | Economy ▾ | Industry | ET Explains | Politics | More ▾

Business News › News › India › How a woman stock trader lost Rs 7.6 crore in share market investment fraud

How a woman stock trader lost Rs 7.6 crore in share market investment fraud

ED: Retired army officer duped of Rs 45 cr in investment fraud case

ED said that probe revealed that the accused falsely claimed to have been running a firm with a valuation of Rs 200 crore

Kerala man loses Rs 7.55 crores after falling for online investment scam

A businessman from Cherthala, Kerala, lost Rs 7.55 crores in an elaborate online investment scam. The police are investigating the case and have issued warnings to the public to be cautious of such fraudulent schemes.

Mumbai Cyber Fraud: 49-Year-Old IT Professional Duped Of ₹1.16 Crore In Share Market Investment Scam In Just 4 Days, Case Registered

4 Axis Bank officials among 8 held for Rs 97-cr investment fraud in Bengaluru

The Bengaluru cybercrime police cracked a case of online fraud involving investment and trading and arrested eight people, including four officials from Axis Bank.

Fraudsters floating advertisement in various Social Media Platforms for an “investment expert” / “investment gurus” on stock market trading along with a link.

After clicking the link, he was added to a WhatsApp /Telegram group.

10 held in China-linked Rs 6 crore investment fraud

TNN / Updated: Sep 30, 2024, 07:17 IST

SHARE AA FOLLOW US

In Bengaluru, ten men were arrested for allegedly defrauding people from 21 states out of Rs 6 crore by promising high investment returns. Police seized various items including mobile phones and debit cards. The gang's handlers were based in China. The masterminds are local residents with varying educational backgrounds.

Fraudsters lured the victim with “expert guidance” to obtain high returns on investments in the stock market and a “joining bonus” in crypto currency trading.

Hindrances for LEA

- ✓ The bank accounts used by fraudsters to siphon money from victims are often "mule" or hired accounts.
- ✓ Funds received from victims are quickly converted into USD, then further transformed into cryptocurrency, and ultimately withdrawn at various international locations, including Dubai, China, and Hong Kong.
- ✓ WhatsApp groups and Telegram channels used for these activities are frequently operated from regions like Cambodia and Hong Kong, making it even harder for police to trace and intercept these cross- border fraud networks.

Stock market fraud via WhatsApp, Facebook, Telegram: Two investors lost over Rs 3 crore; how to identify scam and protect yourself

By Anulekha Ray, ET Online • Last Updated: May 25, 2024, 02:36:00 PM IST

Synopsis
Stock market scams via WhatsApp, Telegram, Facebook or Instagram: Two investors lost over Rs 3 crore in separate scams, highlighting a concerning trend. Fraudsters lure victims via social media with promises of high returns. They use fake profiles, apps, and WhatsApp groups to build trust before blocking withdrawals. Beware social media stock tips promising high returns. It's a scam! Learn how to identify fraudsters and protect yourself. Read for modus operandi and red flags here.

Two incidents were reported in a week of individual investors allegedly losing over Rs 3 crore in two different **stock market frauds**. Such **scams** are on the rise and common people end up losing their savings to them. How can you identify when a fraudster is trying to

Man loses ₹4.5 cr. to stock market investment fraud in Bengaluru

The Hindu Bureau
BENGALURU

A 77-year-old man lost his life's savings of ₹4.5 crore to a stock market investment scam, in one of the most common forms of online cybercrimes that continue unabated, senior police officer say.

The victim, a resident of Bengaluru's Rajajinagar, filed a complaint with the north division cybercrime police on Friday, following which efforts are on to freeze the bank accounts to stop transactions.

In his complaint, the victim said he got a call from an unknown number offering investment in stocks for high returns in the first week of March and was even offered training on how to make right investments for better returns.

Stock market investment scam is one of the most common forms of cybercrimes continuing unabated, police say. GETTY IMAGES

The victim agreed and joined the WhatsApp group having many people. The group admin used to take a one-hour class every afternoon for a few days to teach the members on how to invest in stocks and block trading at the right time for better results.

A few days later, the accused proposed to the victim an offer of bulk stocks with up to 40% discount and shared a link to invest.

Excited by the offer, the victim followed the instructions and transferred ₹3.6 crore online and within a few days, the website was showing a total amount of ₹5.7 crore. When the victim tried to withdraw the money, the accused asked him to pay a commission of ₹72 lakh.

The fraud came to light when the victim tried to withdraw the money, but he could not. The police could not track the transaction details as it was a weekend and bank holiday.

One Case Study:

- Victim received a message on WhatsApp from an unknown number.
- Invitation to join a WhatsApp Group e.g., “Stock Vanguard 150”, “Vanguard Club V5”
- Victim was added in various WhatsApp Group like: “Stock Vanguard (XM-5)”
- Accused under the name: “Professor Ganesh Ranga” conducted video conference on WhatsApp and imparted knowledge on stock investment.
- The victim was asked to login a website to know the status of investment / stock like: "app.alicexa.com".

Fake Investment App Graphs showing high return

MO adopted by accused:

- The website looked genuine and gave updates on various stocks, the prices, details of stock purchases, sales and transactions.
- To withdraw the invested money, the victim was asked to pay 15% tax.
- The victim was asked to deposit 30% of their balance as a refundable deposit.
- The victim was then asked to pay 1% of the total portfolio value.

Beware of Investment Fraud

Modus Operandi

- **Greediness and ignorance is the main reason behind the said type of Cyber Crime.**
- Fraudsters lured gullible public of high returns in a short time with investments in stock markets, shares, Mutual Funds and IPO allotments.
- **1st:** Inducement to join WhatsApp and Telegram groups promising high returns on investments in a short duration.
- **2nd**: Fraudsters designed fake investment platforms which will display high returns and high valued wallet money.
- **3rd:** Fraudsters shared the link of those Platforms to the victim and lured them to invest more amount of money to the tune of lakhs & Crores,.

Remedies available:

- Nationalized Cyber Crime Help Desk Number: Dial **1930** to file complaint.
- Complaint through **www.cybercrime.gov.in**
- Complaint to be filed at the nearest Police Station / Cyber Crime Police Station.
- Complaint to be filed at the concerned Bank.

Legal Provisions:

FIR will be registered against the fraudsters u/s 308(2)/318(2)/318(4)/319(2)/336(2)/ 336(3)/61 (2) (b)/3 (5) of BNS r/w Sec. 66C/66D of Information Technology Act

TELEGRAM Part-Time Job Scam

BEWARE THE PART-TIME JOB SCAM

IT COULD COST YOU LAKHS

Modus Operandi

- The fraudster will send a small amount, typically around ₹5,000, to the victim's bank account through UPI.
- This unexpected deposit would trigger a notification via an SMS, prompting a person to check the balance in his/her account.
- The scammer then immediately initiates a withdrawal request by sending a suspicious malware driven link.
- When the victim out of curiosity clicks on the said link and enter the UPI PIN / MPIN to verify the deposit, the fraudulent withdrawal gets approved and a higher amount of money will be deducted.

Jumped Deposit Scam

Never click on any suspicious link

Do not open
Unknown/ suspicious Files
that end in .APK or .EXE

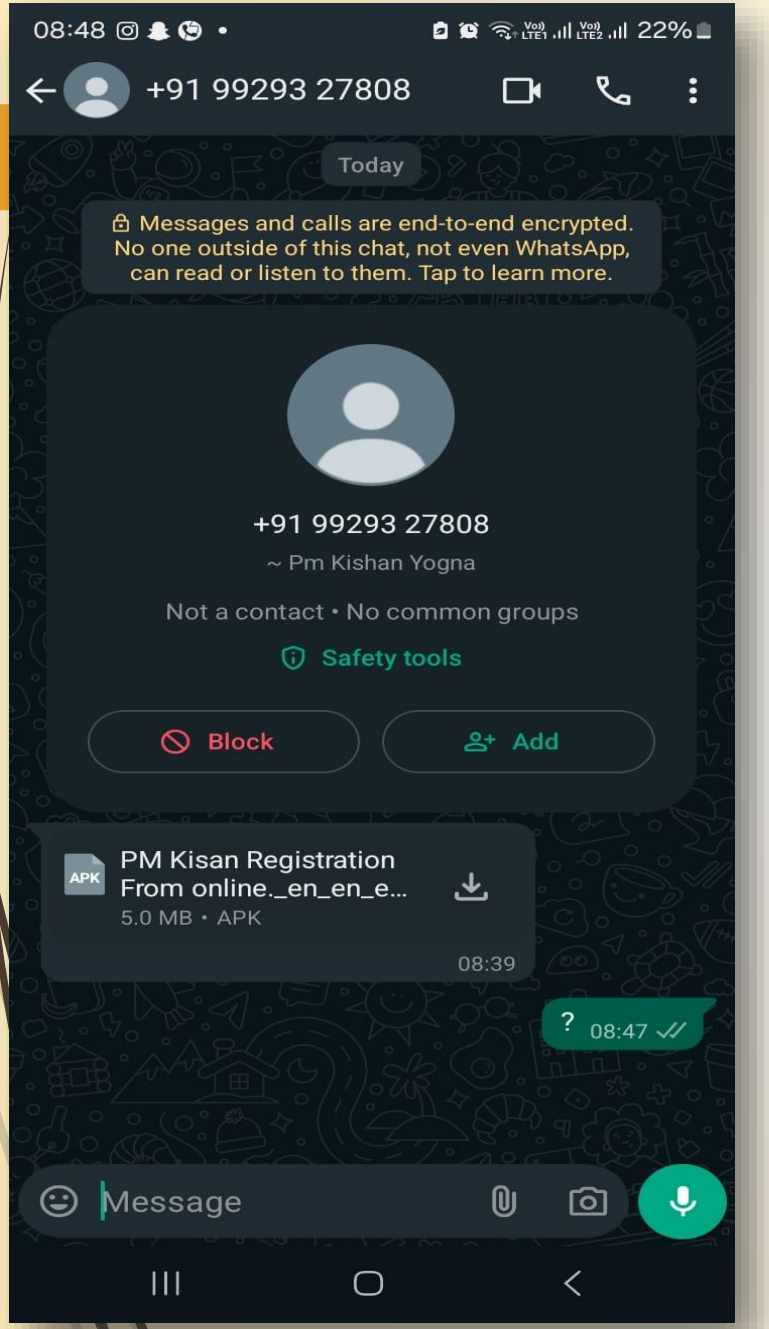
BEWARE ⚠

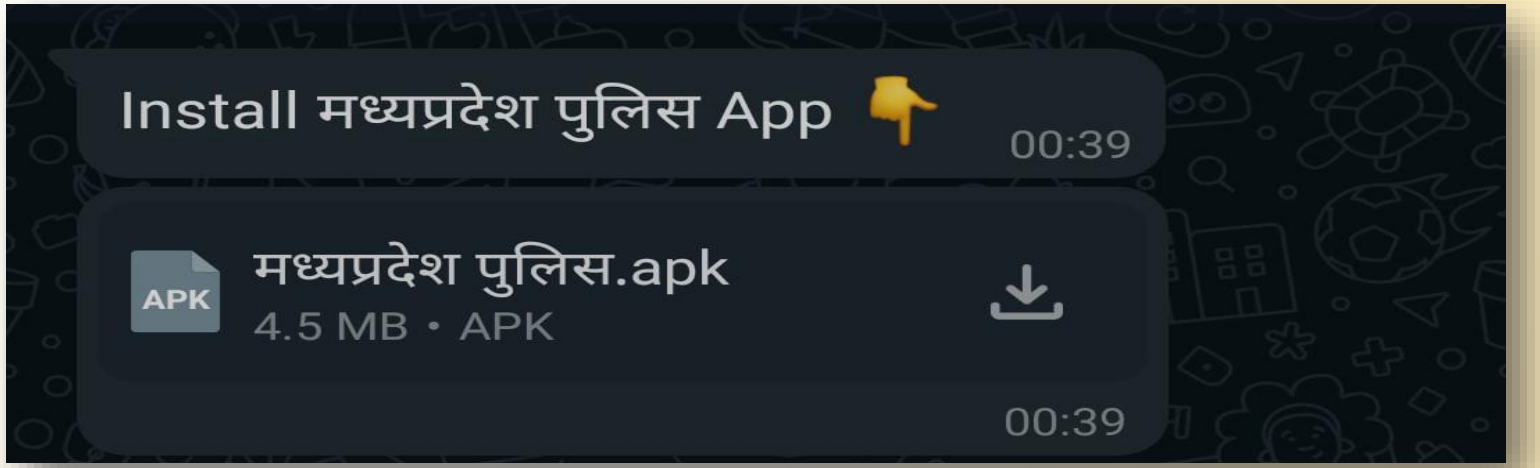
Exercise Caution with .exe Files

BEFORE OPENING AN .EXE FILE RECEIVED VIA EMAIL OR DOWNLOADED FROM THE INTERNET, ALWAYS CONFIRM THAT IT'S FROM A TRUSTWORTHY SOURCE. PROTECT YOUR DIGITAL ENVIRONMENT BY PREVENTING THE EXECUTION OF POTENTIALLY DANGEROUS PROGRAMS.

Stay Safe, Stay Vigiliant

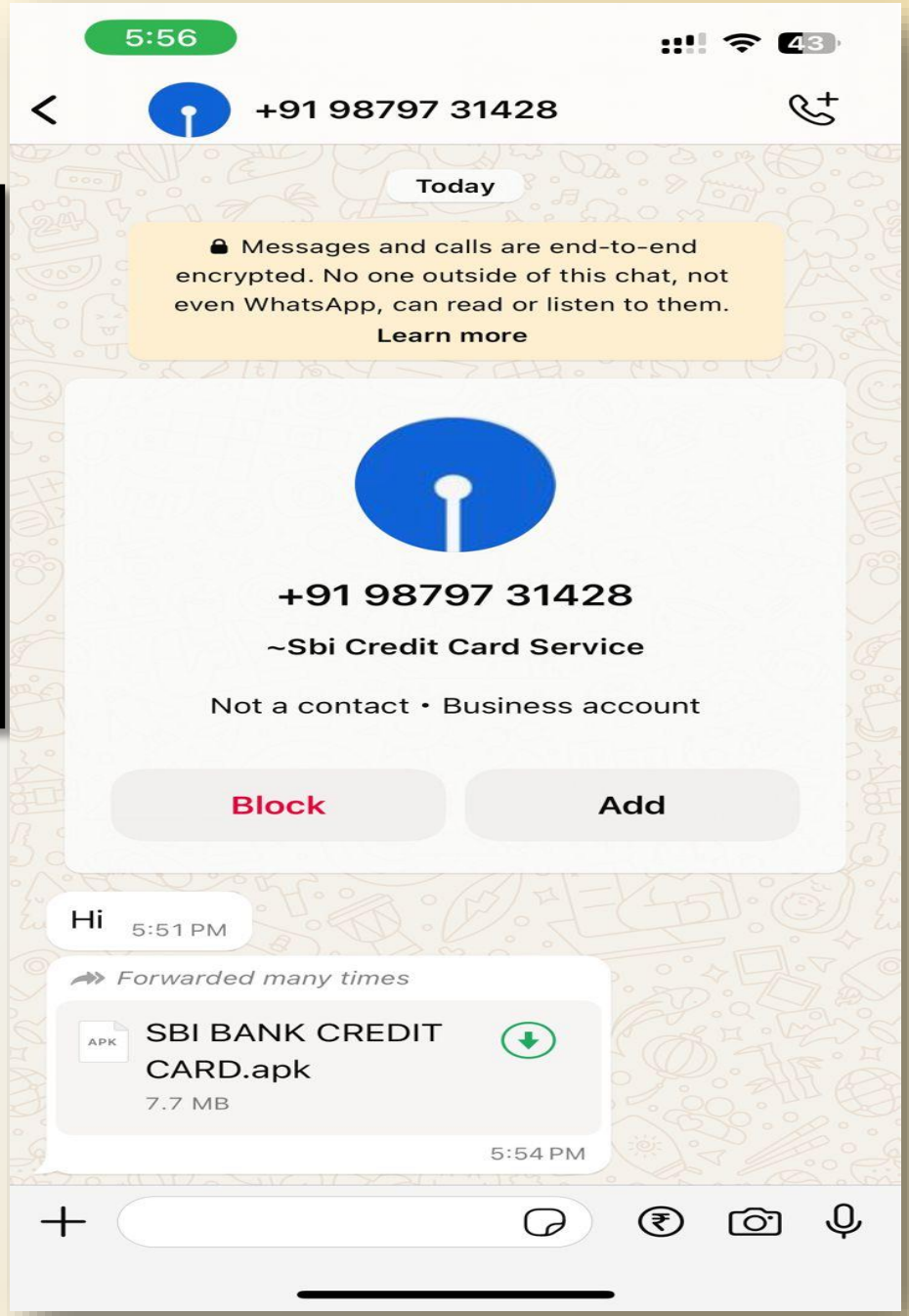
Fraudsters use APK Files for installation of Malware into the devices

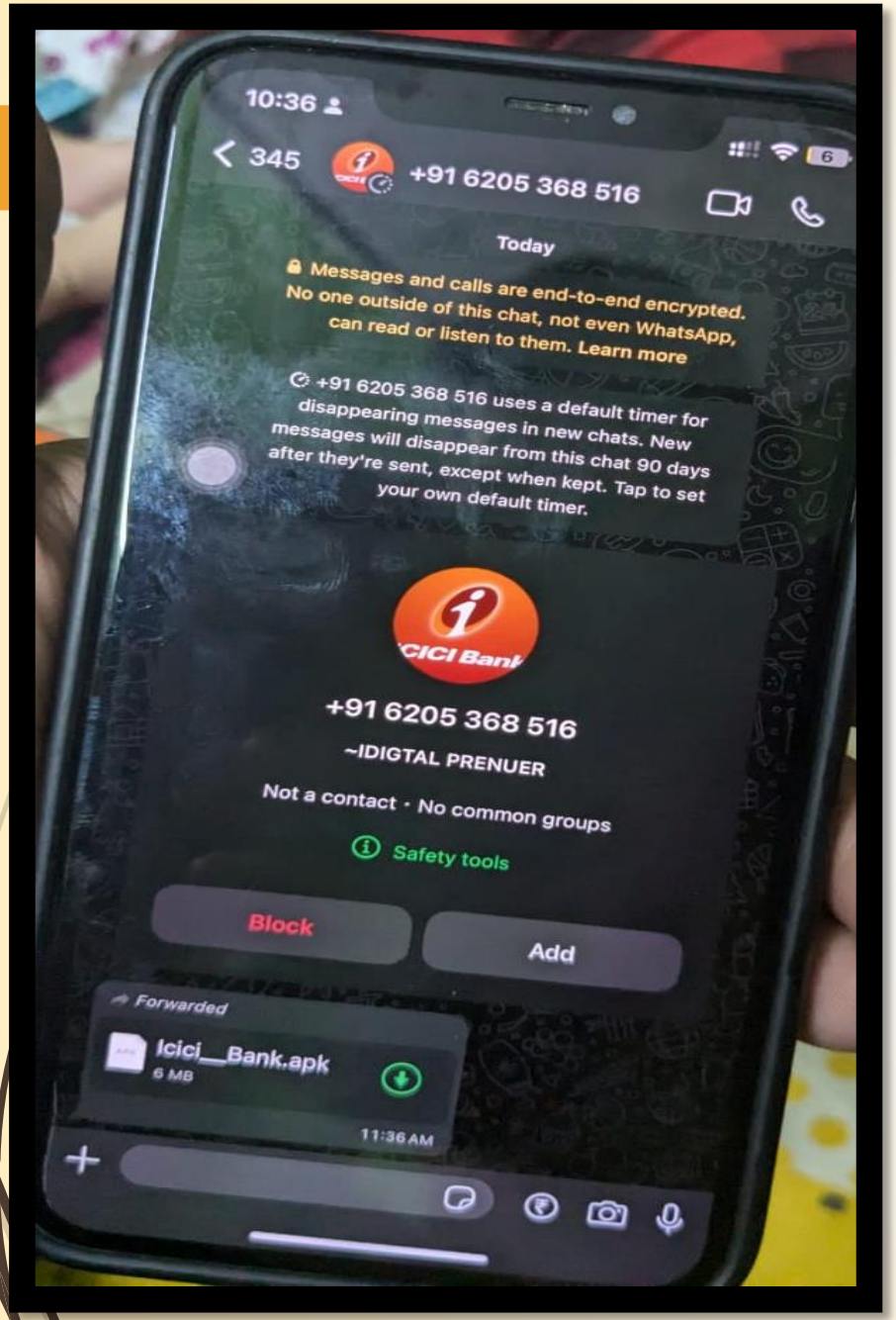




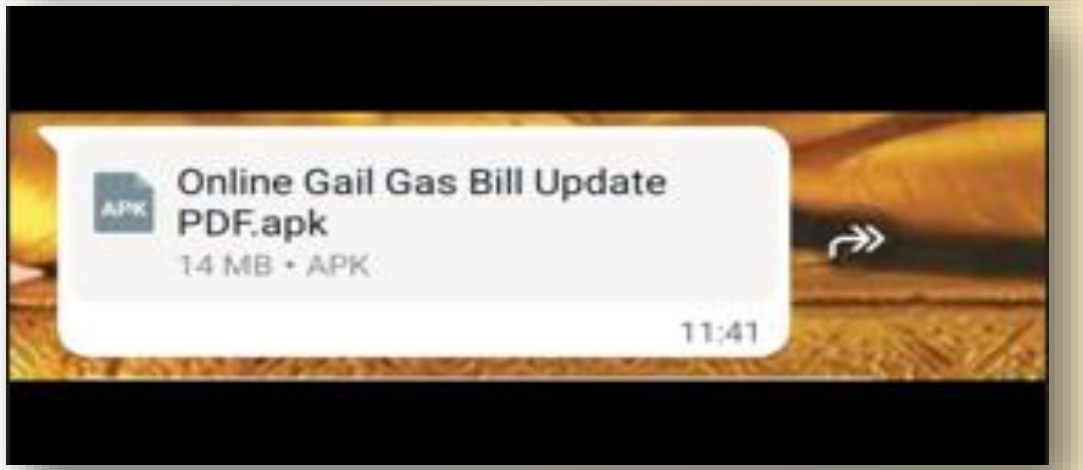
Dear Value Customer
B.o.i Rewards (Rs 6580.00)
is Successfully Activated & Will Expire Today ! Now Redeem
Through B.o.i Rewards Apk Install & Claim Your Reward By Cash Deposit in Your Account
Thank you
Team - BOI

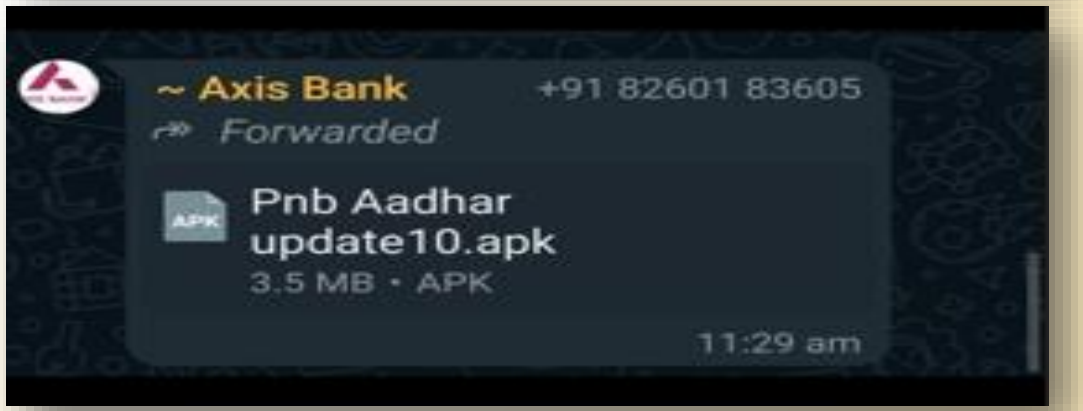
BOI Mobile Digital T12.apk
APK • 5 MB

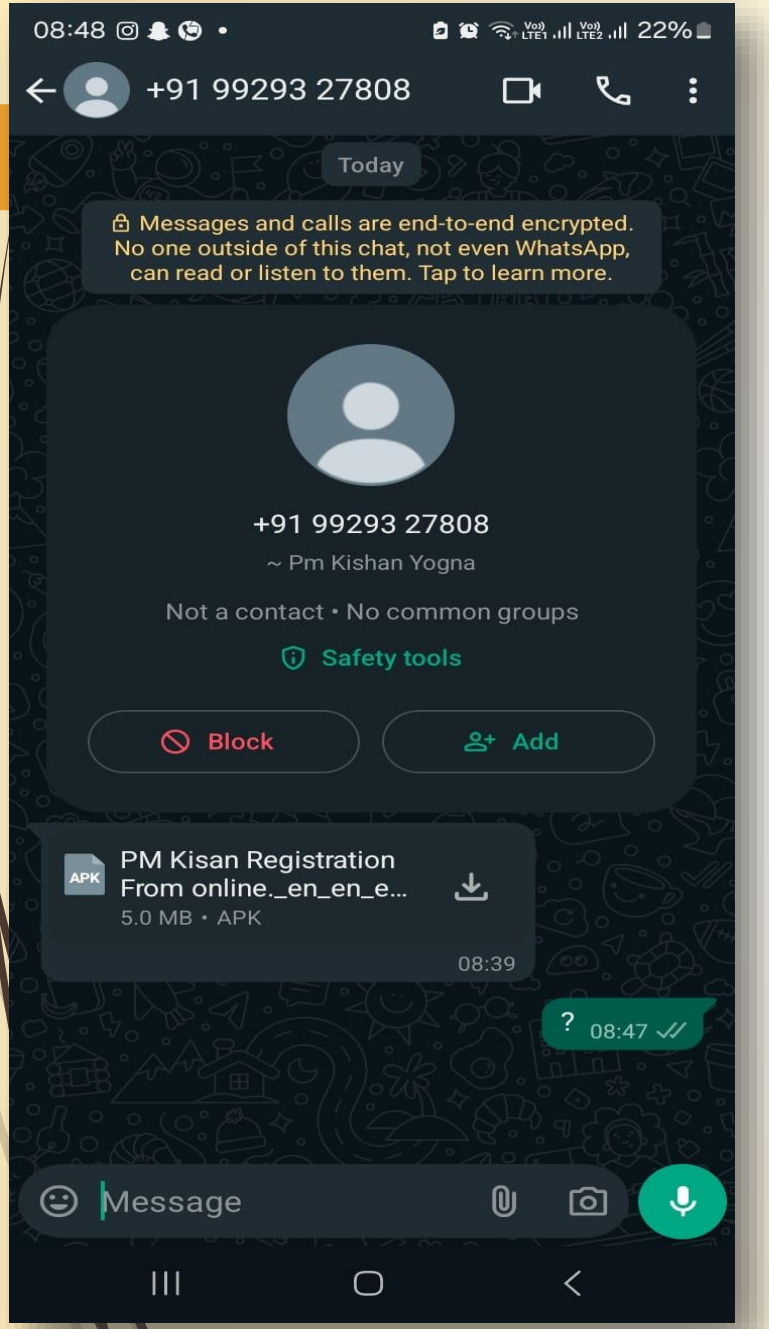




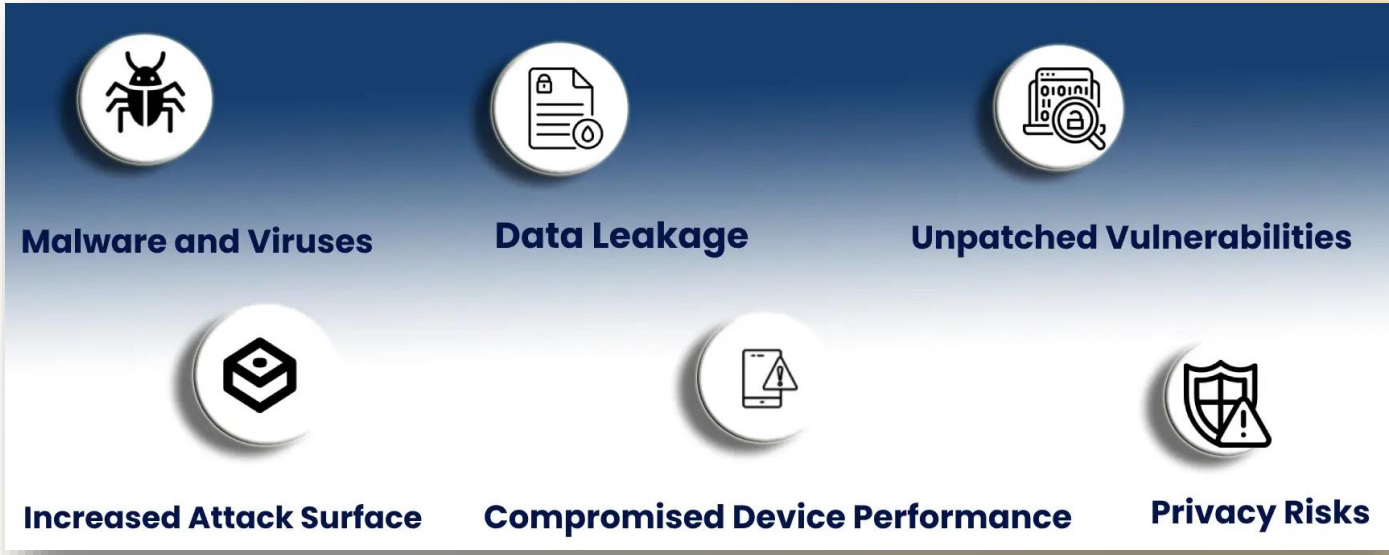
- BOI Mobile Digital T12.apk
- Express Money Payment.apk
- PM KISHAN_1.20_clone.apk
- PM_Helth Card Apply.apk
- SBI YONO REWARDZ .apk





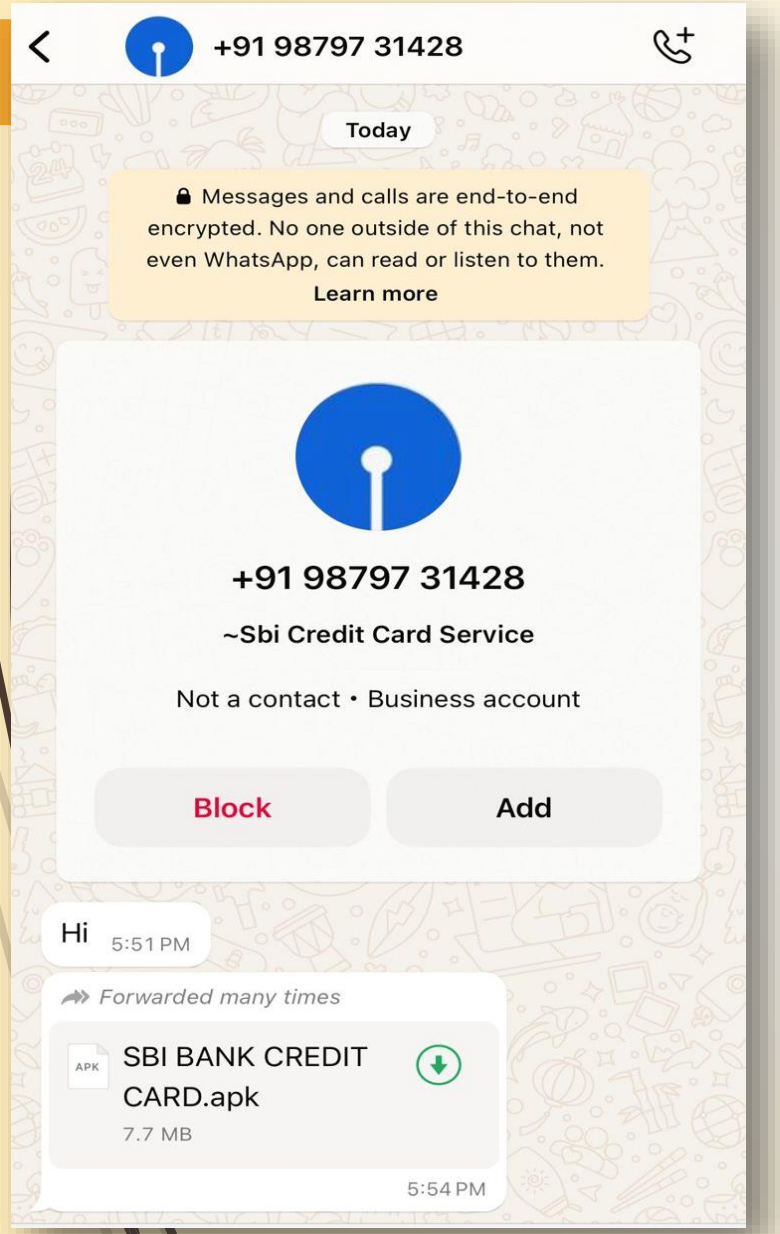


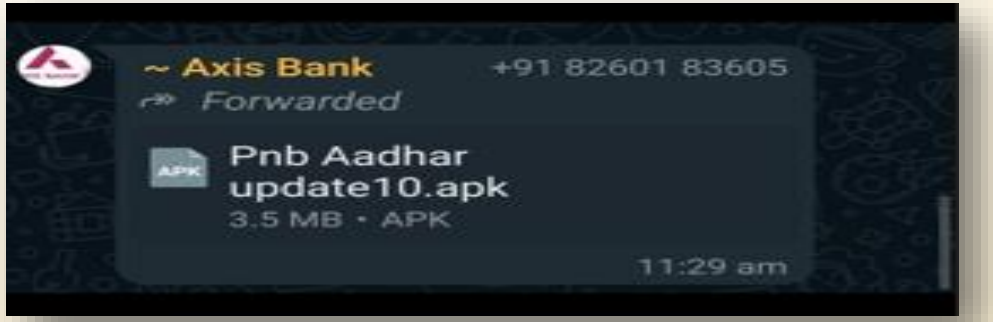
Frauds relating to Sideloading /Third Party Apps

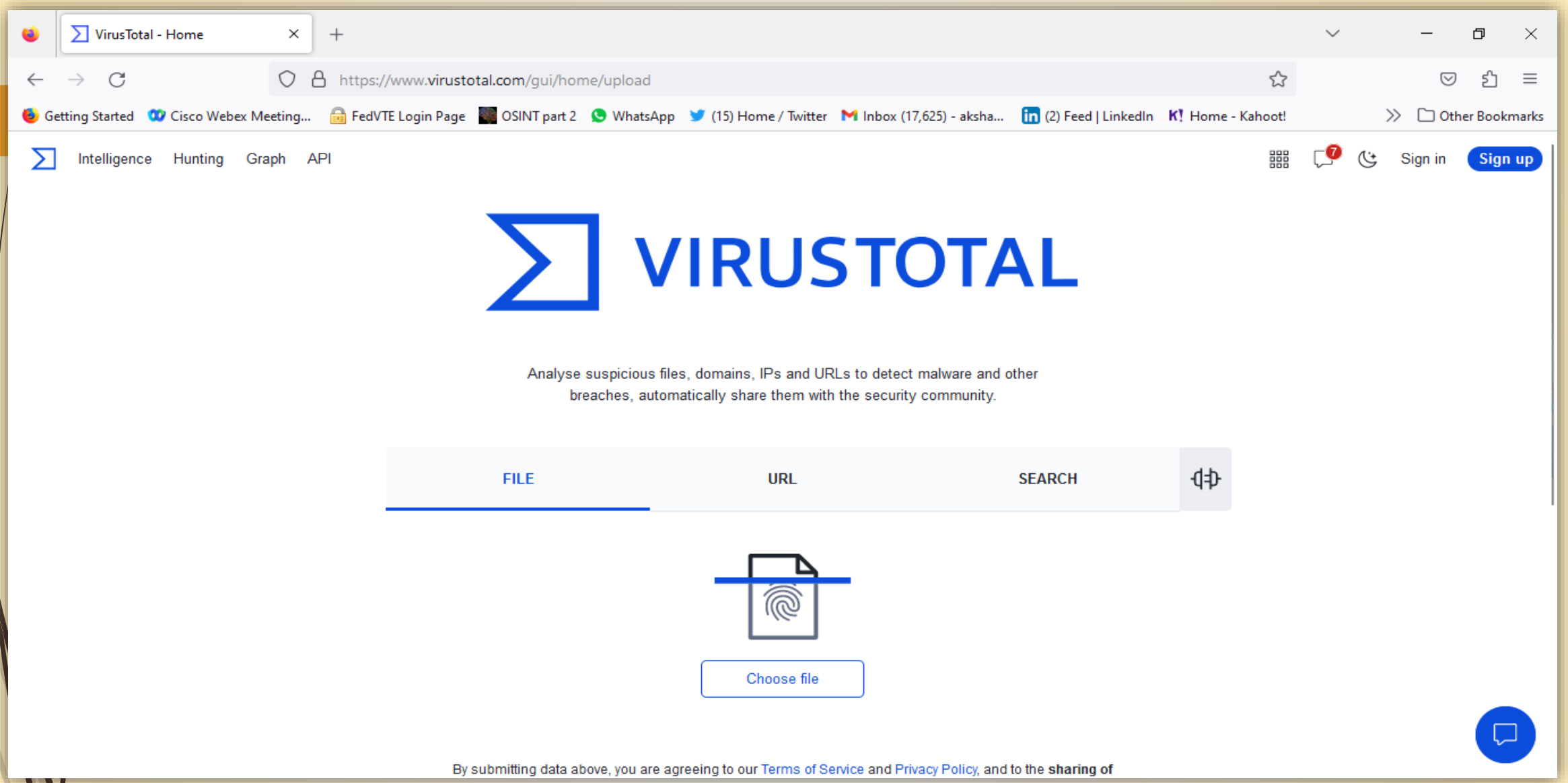


Never download APK Files /3rd Party / Side-loading applications

Your messages, contact information, banking related data & other valuable information from the mobile phone will be hacked.

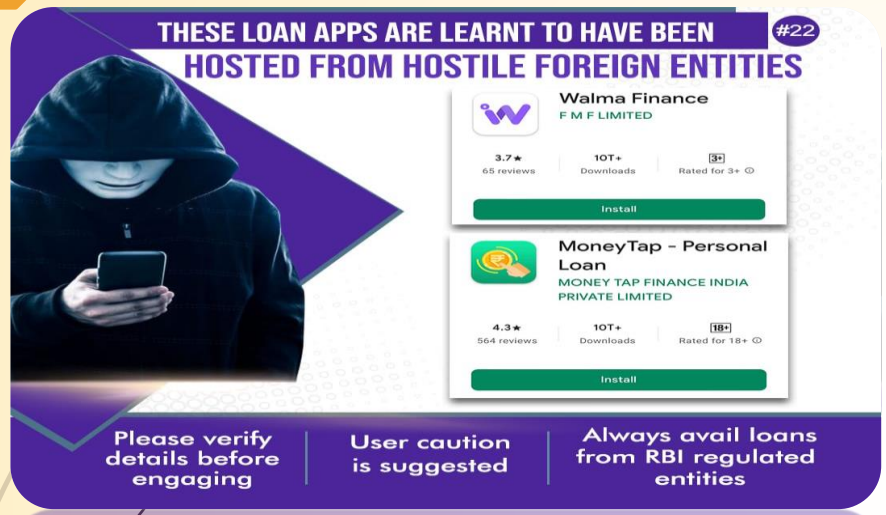


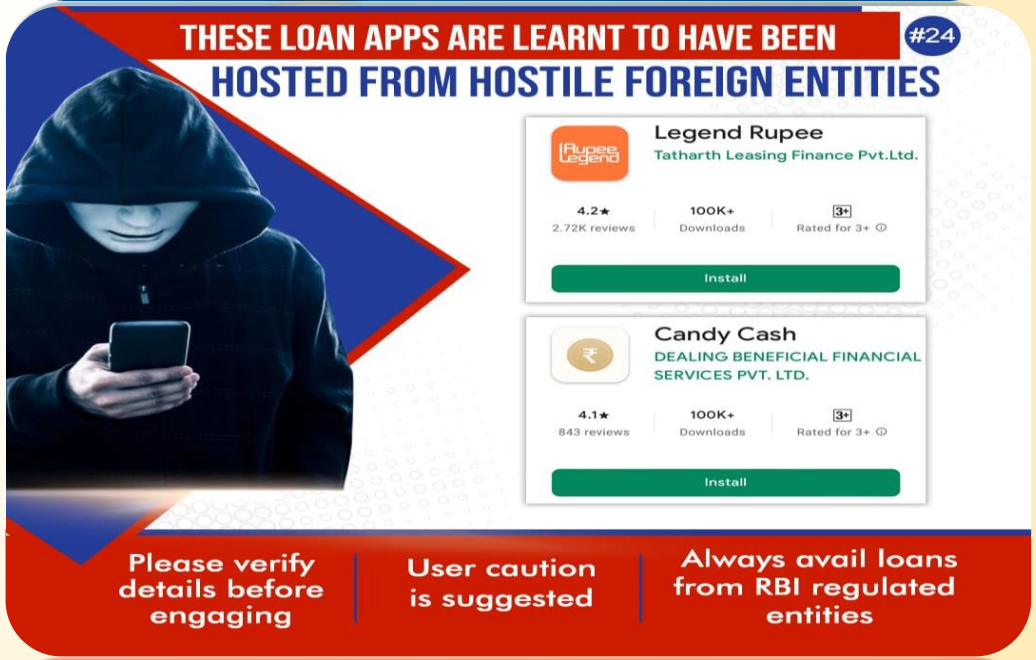




https://www.virustotal.com

Fake Loan App Fraud



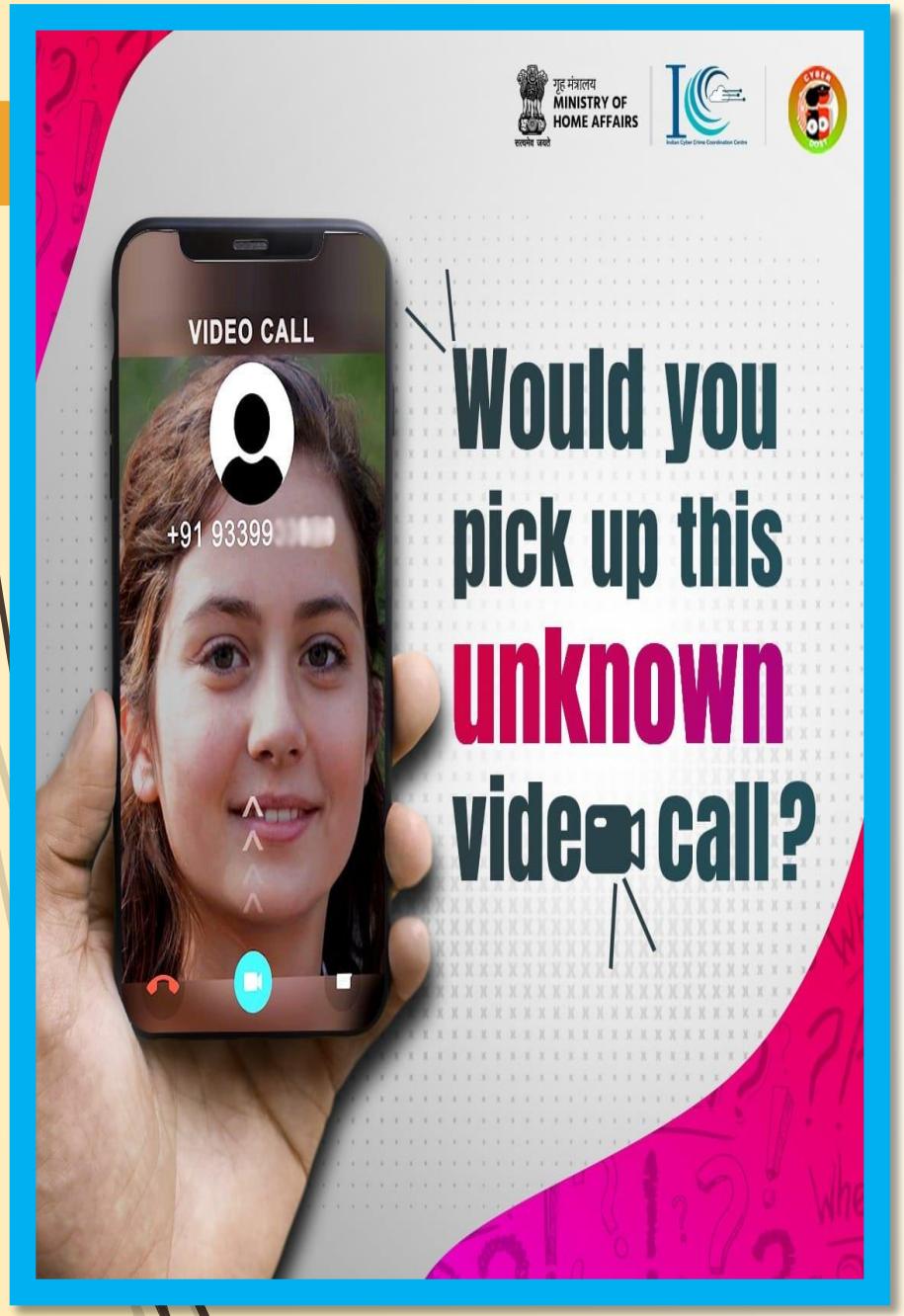


Loan Apps are unauthorized app. or unregistered NBFCs.

Check the details of Non Banking Financial Companies (NBFCs) on https://rbi.org.in/scripts/bs_nbfclist.aspx

- Use Sachet portal https://sachet.rbi.org.in to file an on-line complaint
- Use www.cybercrime.gov.in to file complaint

SEXTORTION



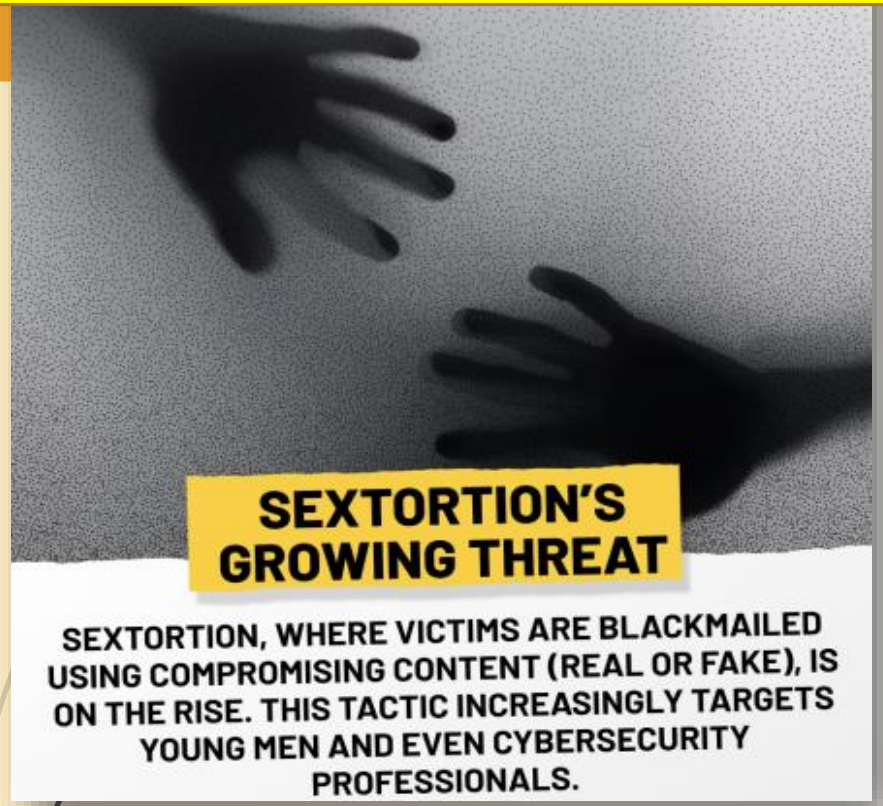
Beware of Sextortion Scam

Avoid picking unknown online video calls


DON'T POST TOO MUCH PERSONAL INFORMATION
USE YOUR SOCIAL MEDIA PRIVACY SETTINGS
USE A NICKNAME ON DATING SITES
HOW TO PREVENT SEXTORTION
NEVER ACCEPT UNKNOWN FRIEND REQUESTS
DON'T CLICK ON LINKS OR DOWNLOAD FILES
COVER YOUR WEBCAM
INSTALL GOOD ANTIVIRUS SOFTWARE


MINISTRY OF HOME AFFAIRS
BEWARE OF SEXTORTION SCAMS
SCAM ALERT
• Avoid clicking on links from unknown or suspicious sources.
• Cover your webcam when it is not in use to prevent unauthorized access.

Beware of Sextortion Scam

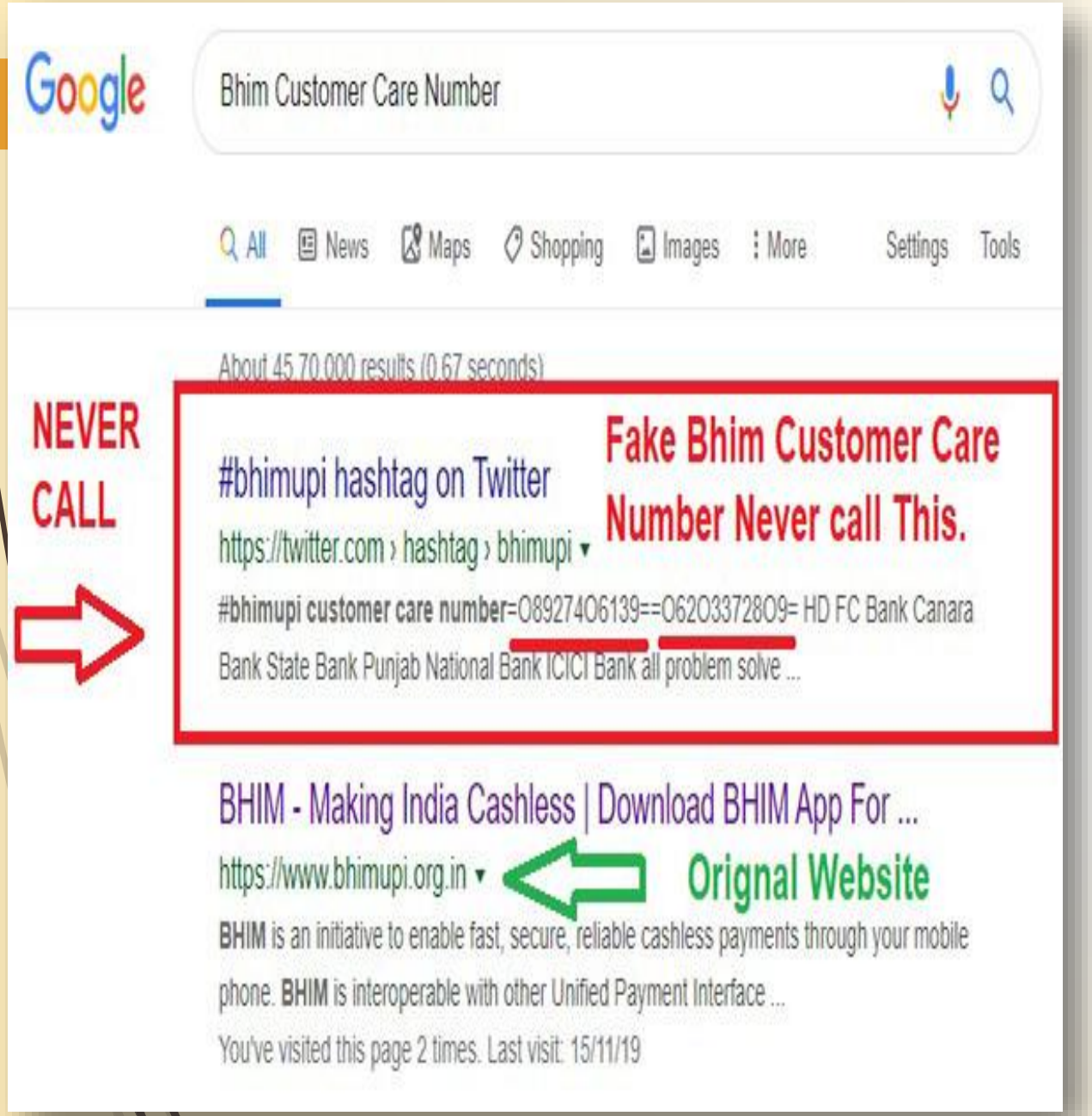


Legal Provisions:

- FIR will be registered against the fraudsters u/s 308(2)/318(2)/318(4)/319(2)/336(2)/ 336(4)/294/296/351 (2)/351(3)/351(4) of BNS r/w Sec. 66C/66D/66E/67/67A of Information Technology Act

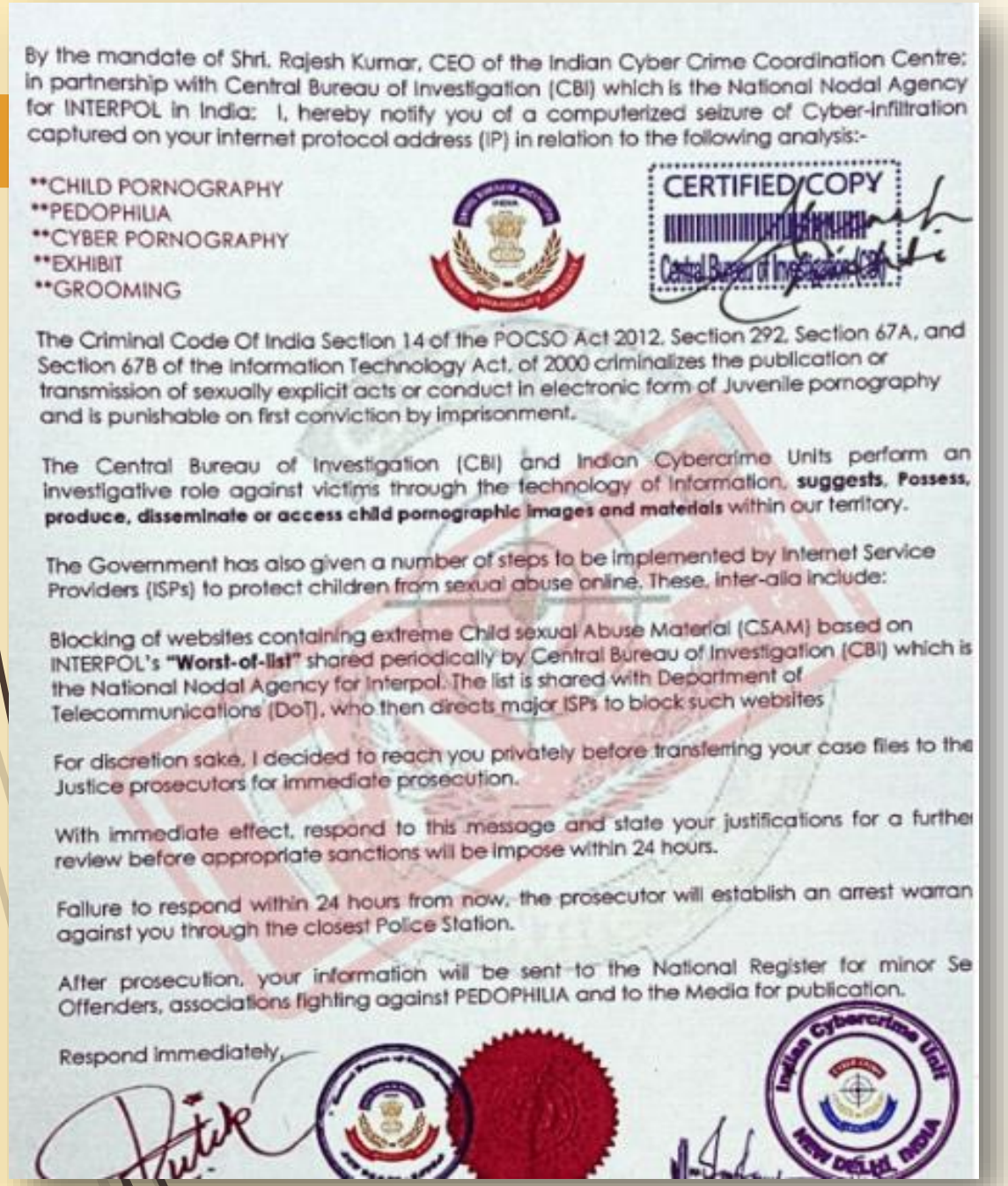
Remedies available:

- Nationalized Cyber Crime Help Desk Number: Dial 1930 to file complaint
- Complaint through www.cybercrime.gov.in and https://cybercrime.gov.in/Webform/cyber_suspect.aspx
- Complaint to be filed at the nearest Police Station / Cyber Crime Police Station
- Complaint to be filed in Sanchar Saathi Portal (Chakshu) https://sancharsaathi.gov.in/sfc/



Customer Care Fraud

Fake Cashback Fraud / Reward Scam



By the mandate of Shri. Rajesh Kumar, CEO of the Indian Cyber Crime Coordination Centre: in partnership with Central Bureau of Investigation (CBI) which is the National Nodal Agency for INTERPOL in India: I, hereby notify you of a computerized seizure of Cyber-infiltration captured on your internet protocol address (IP) in relation to the following analysis:-

**CHILD PORNOGRAPHY
**PEDOPHILIA
**CYBER PORNOGRAPHY
**EXHIBIT
**GROOMING

CERTIFIED COPY

The Criminal Code Of India Section 14 of the POCSO Act 2012. Section 292, Section 67A, and Section 67B of the information Technology Act, of 2000 criminalizes the publication or transmission of sexually explicit acts or conduct in electronic form of Juvenile pornography and is punishable on first conviction by imprisonment.

The Central Bureau of Investigation (CBI) and Indian Cybercrime Units perform an investigative role against victims through the technology of information, **suggests, Possess, produce, disseminate or access child pornographic images and materials** within our territory.

The Government has also given a number of steps to be implemented by Internet Service Providers (ISPs) to protect children from sexual abuse online. These, inter-alia include:

Blocking of websites containing extreme Child sexual Abuse Material (CSAM) based on INTERPOL's **"Worst-of-list"** shared periodically by Central Bureau of Investigation (CBI) which is the National Nodal Agency for Interpol. The list is shared with Department of Telecommunications (DoT), who then directs major ISPs to block such websites

For discretion sake, I decided to reach you privately before transferring your case files to the Justice prosecutors for immediate prosecution.

With immediate effect, respond to this message and state your justifications for a further review before appropriate sanctions will be impose within 24 hours.

Failure to respond within 24 hours from now, the prosecutor will establish an arrest warran against you through the closest Police Station.

After prosecution, your information will be sent to the National Register for minor Se Offenders, associations fighting against PEDOPHILIA and to the Media for publication.

Respond immediately,

Indian Cybercrime Unit
New Delhi, India

Cyber Fraud in the name of I4C /CBI Official

Fake Payment Scam

Fake Hotel Booking Scam

Mumbai: IT consultant director loses Rs 3.84 Lakh in online hotel booking scam

V Narayan / TNN / Oct 8, 2023, 19:32 IST

SHARE AA FOLLOW US

New For You

Finger in every pie? 'Double voters' press button where they are an...

Congress wanted to spend 15% of Budget on Muslims: PM Modi

Airport police that registered the case said the victim, PK Javed (48), realised that he was duped when he rushed to the hotel to verify and check the online booking he had made by calling on the number that showed belonged to the hotel and learned that he was duped by an online fraudster.

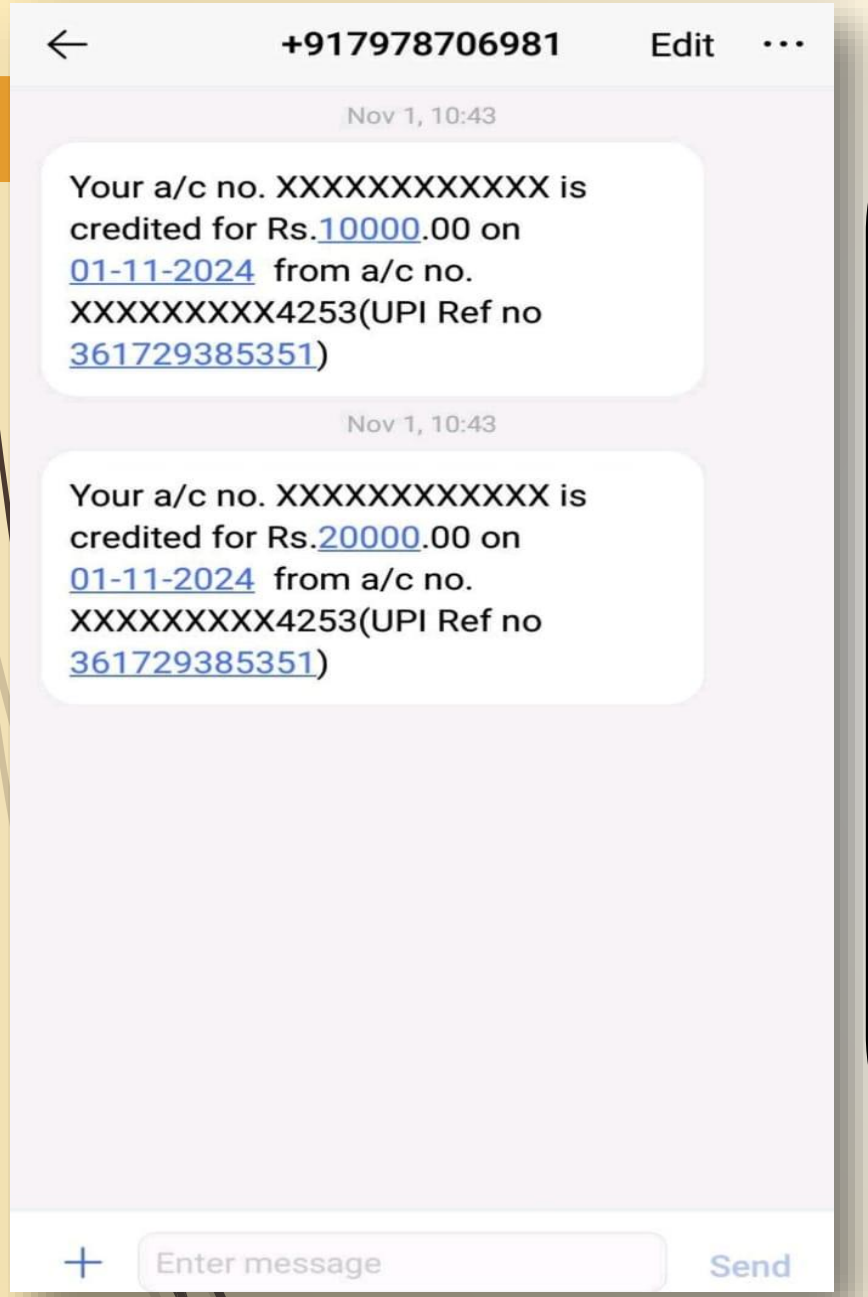
Read Less

CRYPTOCURRENCY SCAM

- Bitcoin Investment Schemes
- Rug Pull Scams
- Phishing Scams
- Investment Scams
- Fake Apps
- Giveaway Scams
- Man-in-the-middle Attack
- Fake Crypto Exchanges
- Employment Offers and Fraudulent Employees
- Blackmail Scams

Money Transfer / revert back Fraud

Fake Insurance Fraud



Beware of UPI Scam

Modus Operandi:

- Receipt of fake message towards credit of money in the bank account by the victim.
- The drafted message sent by the fraudster with the intention to deceive the receiver.
- The fraudster used the pressure tactics and insist the receiver to return the said fraud amount to an unknown UPI ID / Bank account.

Fake Call Centre Fraud

84 employees arrested by Noida police from fake call centre cheating Americans.

Ludhiana: ‘Fake’ call centre duping US citizen busted, 9 held

By HT Correspondent, Ludhiana

Aug 23, 2024 10:32 PM IST

The Sadar police of commissionerate uncovered an allegedly fraudulent call centre duping US nationals by posing as software engineers and technical support providers, officials said on Friday.

Accused for running fake call center; in the custody of Sadar police in Ludhiana on Friday, August 23, 2024. (HT Photo)

Two fake call centres duping US citizens busted in Mohali, 155 held

Chandigarh, May 17 The Cybercrime Division of the Punjab Police has busted two fake call centres running in Mohali and arrested 155 employees of these centres for making fraudulent calls to people living in the US and duping them, said...

Lucknow Police Crack Down on Fake Call Centre: 12 Cyber Fraudsters Held

Modus operandi

Payday Fraud:

- Target are US Citizen
- Lured them to provide low-interest loans even if their credit score was low.
- The customers were exploited by making them buy gift cards in the hope of a loan, later redeemed by the kingpin.

Amazon fraud:

- The caller, pretending to be an Amazon representative
- Fraudsters threatened the customer that a parcel ordered by them had illegal items and that federal police would be informed.
- Fraudsters asked a specific amount was obtained through a cash app or via an Amazon gift card to cancel the order

Microsoft Scam:

- The targeted people would get a pop-up on their computers with a message that the system was compromised and provided with a number to make a call.
- The victim would get a link to download an app that allowed screen viewing.
- Thereafter, money from the bank accounts was fraudulently transferred to mule accounts in the US and received in India through hawala.

Anti-virus Scam:

- The targeted people would get a call that the Antivirus installed in the computer system is expired.
- The victim would get a link to download an app that allowed screen viewing.
- The customers were exploited by making them buy gift cards in the hope of installation of Antivirus and remote Tech Support, later redeemed by the kingpin.

Legal Provisions:

- FIR will be registered against the fraudsters u/s 308(2)/318(2)/318(4)/319(2)/336(2)/336(3)/61 (2) (b)/3 (5) of BNS r/w Sec. 66C/66D of Information Technology Act

Remedies available:

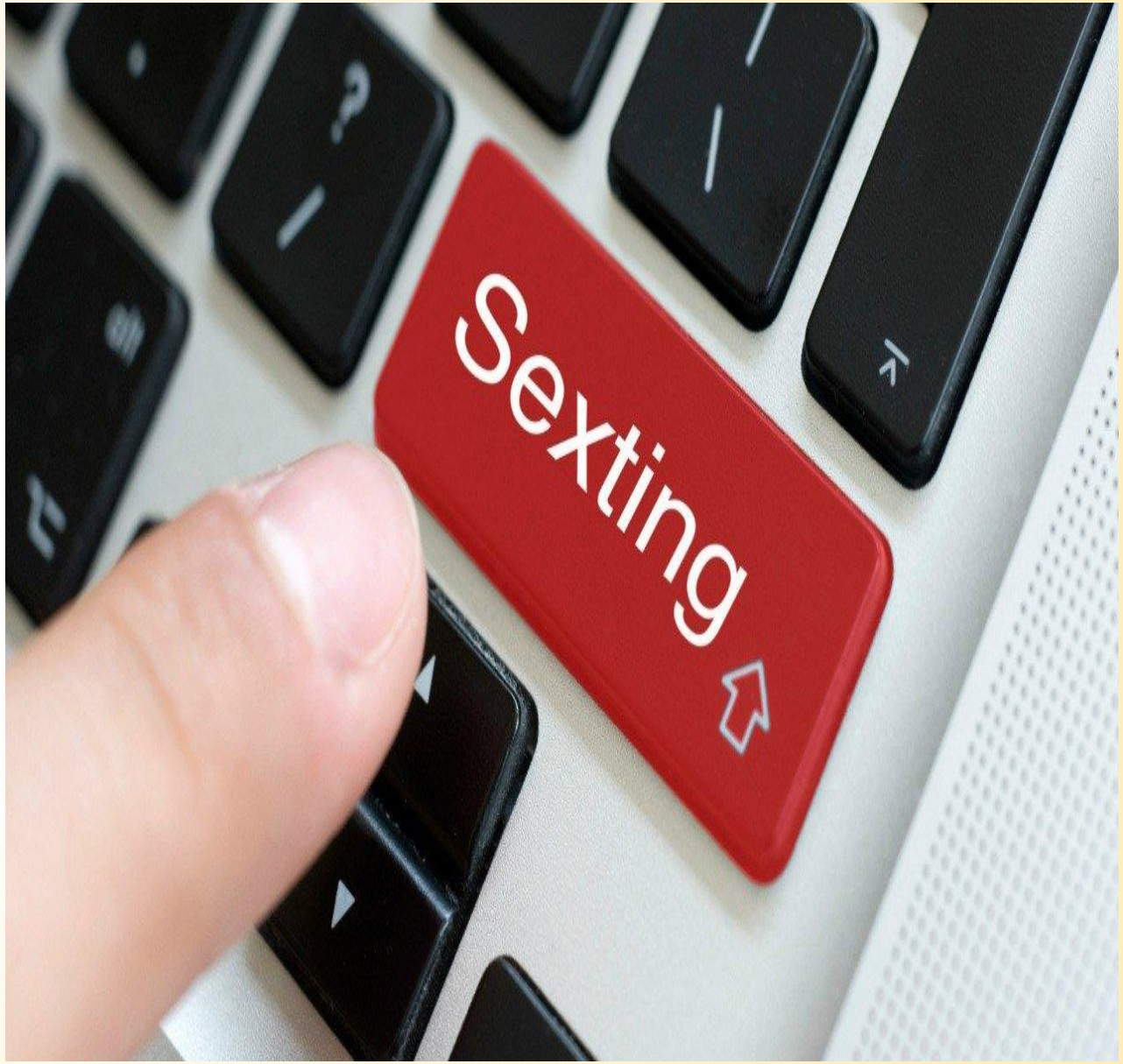
- Nationalized Cyber Crime Help Desk Number: Dial 1930 to file complaint
- Complaint through www.cybercrime.gov.in
- Complaint to be filed at the nearest Police Station / Cyber Crime Police Station
- Complaint to be filed at the concerned Bank

Never post sexually coloured remarks / obscene content in Social Media Platforms

It's a type of cybercrime and punishable under Sections 75 (2) & (3) / 79 / 294 (2) / 296 of BNS and Section 67/67A of Information Technology Act:
Imprisonment for five years

Sexting is the combination of two words, Sex, and texting. So sexting basically means sending or receiving sexual messages.

Sexting is punishable as per Indian Laws



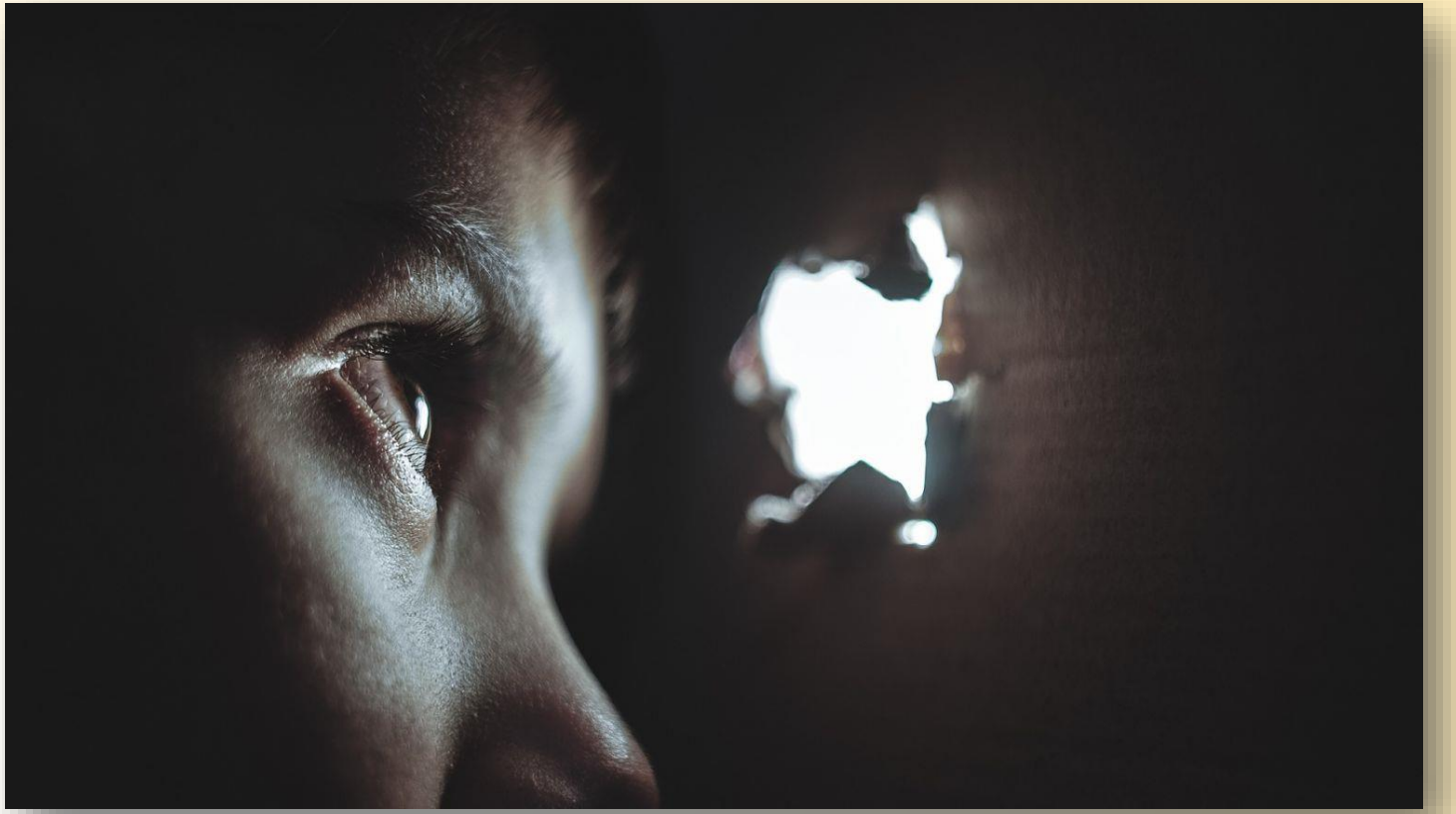
Sexting

It's a type of cybercrime and punishable under Sections 75 (2) & (3) / 78 / 79 / 294(2)/296 of BNS and Section 67/67A of Information Technology Act: Imprisonment for five years

Hacking of Facebook/ Instagram / E-mail /WhatsApp accounts

It’s a type of cybercrime and punishable under Section 66 of Information Technology Act:
Imprisonment for three years

Voyeurism



It’s a type of cybercrime and punishable under Section 77 of BNS / Section 66E of Information Technology Act : Imprisonment shall not be less than one year and extend to three years

STOP CYBER STALKING

Randomly never accept every friend request through online

Never disclose sensitive information in social media platforms

It’s a type of cybercrime and punishable under Section 78 (2) BNS: Imprisonment for three years

Block the cyber stalker and report against the user in the Platform

Never browse Child Sexual Exploitative and Abuse Material (CSEAM) through online.

It’s a type of cybercrime and punishable under Sections. 79 /Sec. 294 (2) /Sec. 296 BNS & Sec. 67/ 67B of Information Technology Act:

Imprisonment for five years

Identity theft /
Creation of fake accounts in various Social Networking Platforms /IMPERSONATION [Fake Facebook / Instagram / E-mail account]

It's a type of cybercrime and punishable under Sections: 319 (2)/ 336 (2) & (4) of BNS and Section: 66C/66D of Information Technology Act:

Imprisonment for three years

MORPHING

It's a type of cybercrime and punishable under Section: 319 (2)/ 336 (2) & (4) BNS and Section: 66C/66D of Information Technology Act: Imprisonment for three years

- Never share your personal pictures online publicly on social media accounts
- Use watermark while sharing pictures
- Use two factor authentication with strong passwords for your social media accounts
- If you observe your fake profile or any such objectionable post on social media, then file complaint at Police Station or through online (**Cyber Crime Help Desk Number: 1930**)

Be careful what you post and make public online

Don’t send intimate photographs / video files

Never send money to unknown person

Beware of Romance Scam

Beware of Like / Subscribe Scam

Don’t click on unknown / suspicious links

Don’t join any unknown WhatsApp Groups or Telegram Channel

Don’t deposit / transfer money in any unknown bank accounts or UPI IDs

Don’t share personal information

Never share your sensitive personal photographs

Always be careful while dealing with ‘NRI’ profiles on matrimonial websites

Never deposit / transfer money in any unknown bank accounts

Beware of Dating Scam / Matrimonial Fraud

Criminal Intimidation

Punishable under Sec. 351 (2)/(3)/(4) of BNS

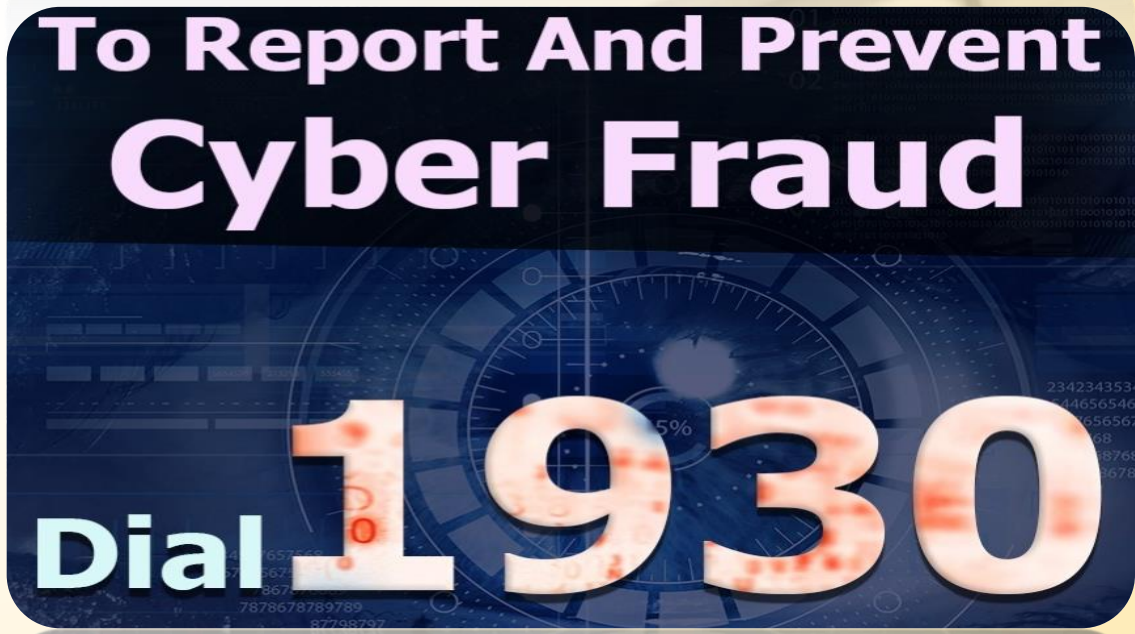

BE VIGILANT, BE CYBER SAFE
DIAL 1930
FOR ONLINE FINANCIAL FRAUD AND
REPORT ANY CYBERCRIME AT
WWW.CYBERCRIME.GOV.IN

3 ways to report Cyber Fraud:

1. Call 1930 to register any complaint about Cyber Crime
2. Contact the nearest Police Station to file your complaint
3. File your complaint online through www.cybercrime.gov.in

Documents needed for filing complaint:

- **Screenshots of the alleged contents/ profile**
- **Screenshot copy of URL of alleged contents**
- **Contents should be in the form of both hard and soft copy**
- **Soft copy should be given in CD /DVD / USB Drive**



- If you encounter any suspicious online activities or become victims of any kind of cyber frauds or crime, you should immediately report such incidents promptly by dialing Toll Free **1930 Cyber Crime Help Line or log on to www.cybercrime.gov.in** and register their complaint without delay.
- You can also report suspected fraud numbers in the **CHAKSHU** portal of Department of Telecommunication
- https://sancharsaathi.gov.in/sfc/ or
- cybercrime reporting portal of i4C, MHA
- https://cybercrime.gov.in/Webform/cyber_suspect.aspx.

sachet.rbi.org.in

07:52:54 AM Thursday, May 16 2024

A+ A A-

सचेत
An SLCC initiative

This site is also available in : Assamese (অসমীয়া) | Bengali (বাঙালি) | English | Gujarati (ગુજરાતી) | Hindi (हिंदी) | Kannada (ಕನ್ನಡ) | Malayalam (മലയാളം) | Marathi (मराठी) | Odia (ଓଡ଼ିଆ) | Punjabi (ਪੰਜਾਬੀ) | Tamil (தமிழ்) | Telugu (తెలుగు) | Urdu (اردو)

Login for SLCC Members.

About Us | Investor Awareness | FAQs

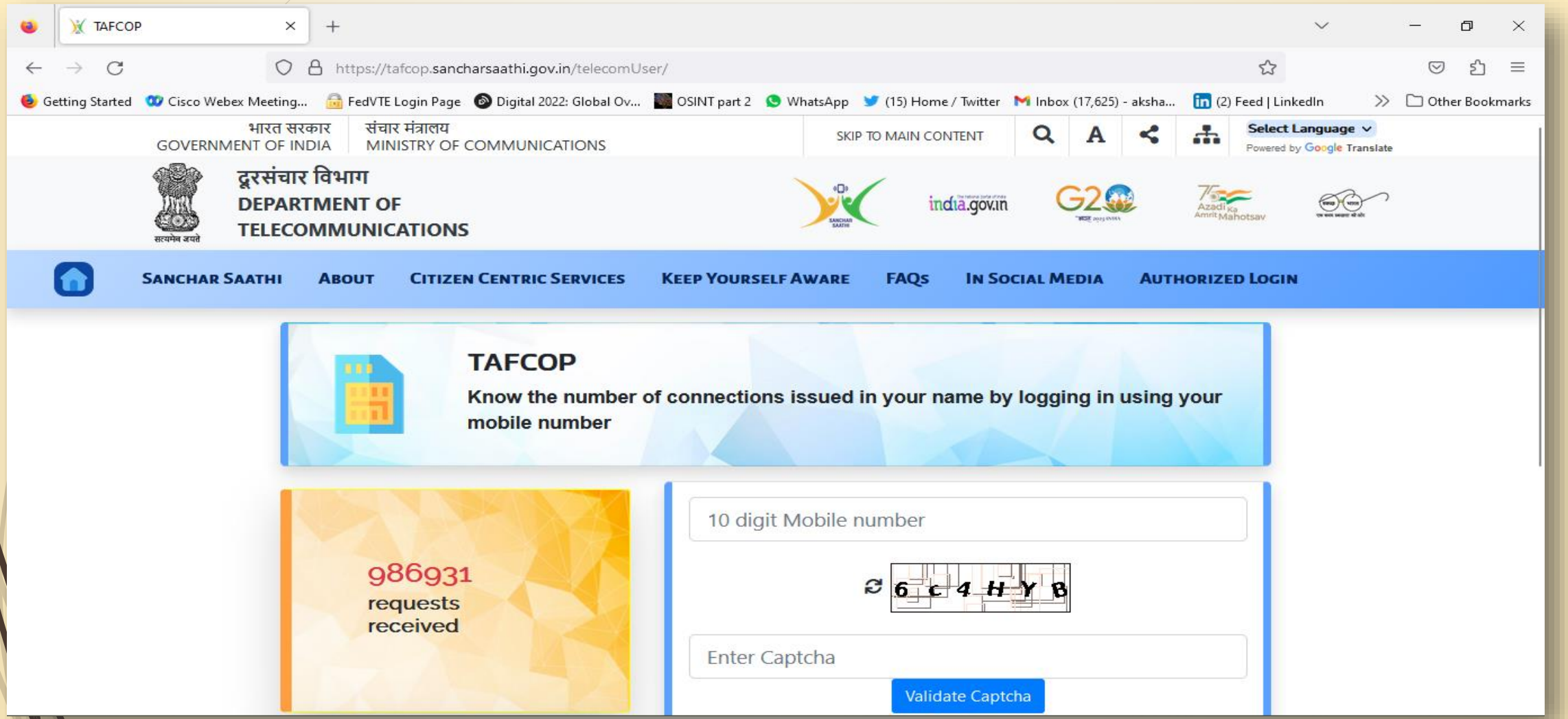
Please click here for Latest Information / Vide

File a Complaint

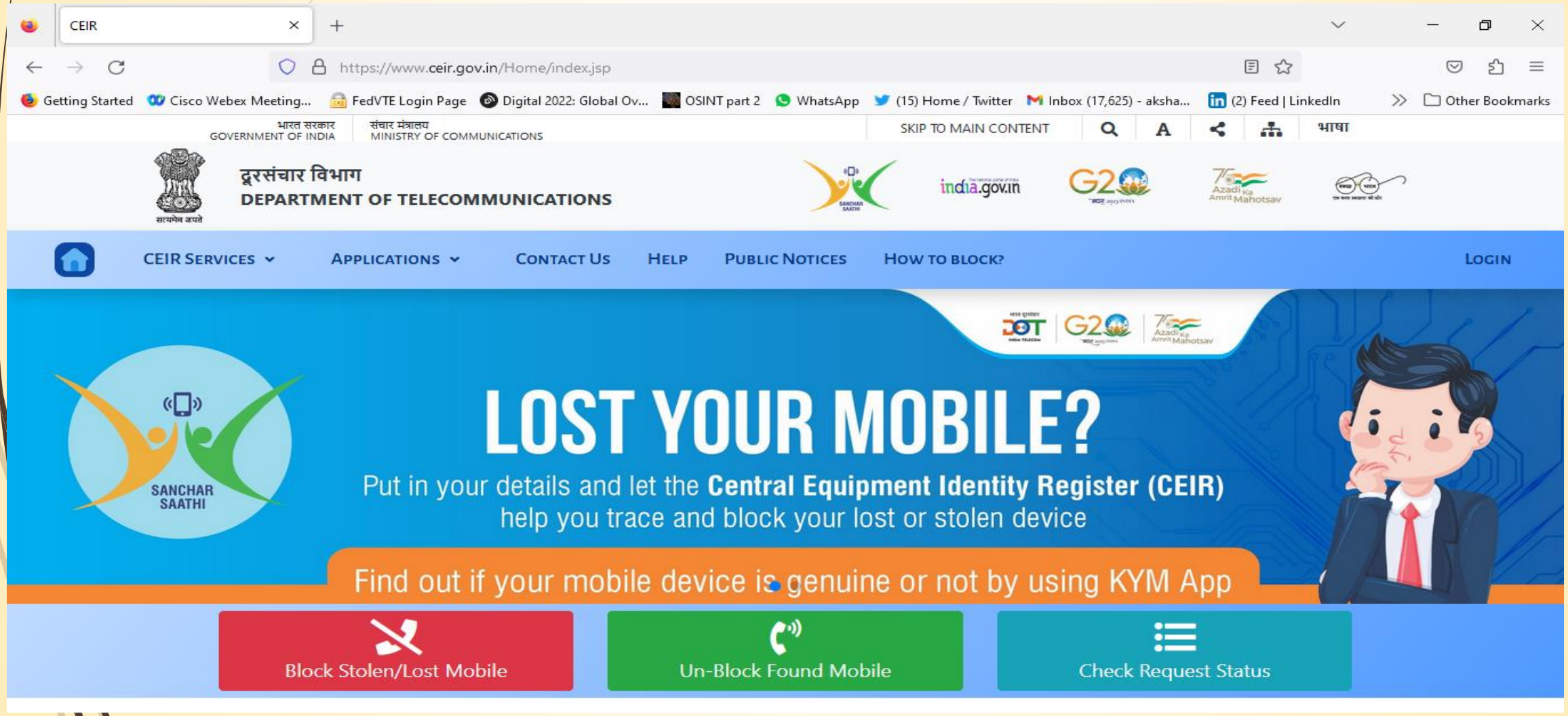
Track your complaint

Help your Regulator

https://tafcop.sancharsaathi.gov.in/telecomUser/



https://www.ceir.gov.in/Home/index.jsp



https://sancharsaathi.gov.in/sfc/

Search

Getting Started

भारत सरकार
GOVERNMENT OF INDIA

संचार मंत्रालय
MINISTRY OF COMMUNICATIONS

SKIP TO MAIN CONTENT

दूरसंचार विभाग
DEPARTMENT OF
TELECOMMUNICATIONS

सत्यमेव जयते

SANCHAR SAATHI

india.gov.in

Azadi Ka Amrit Mahotsav

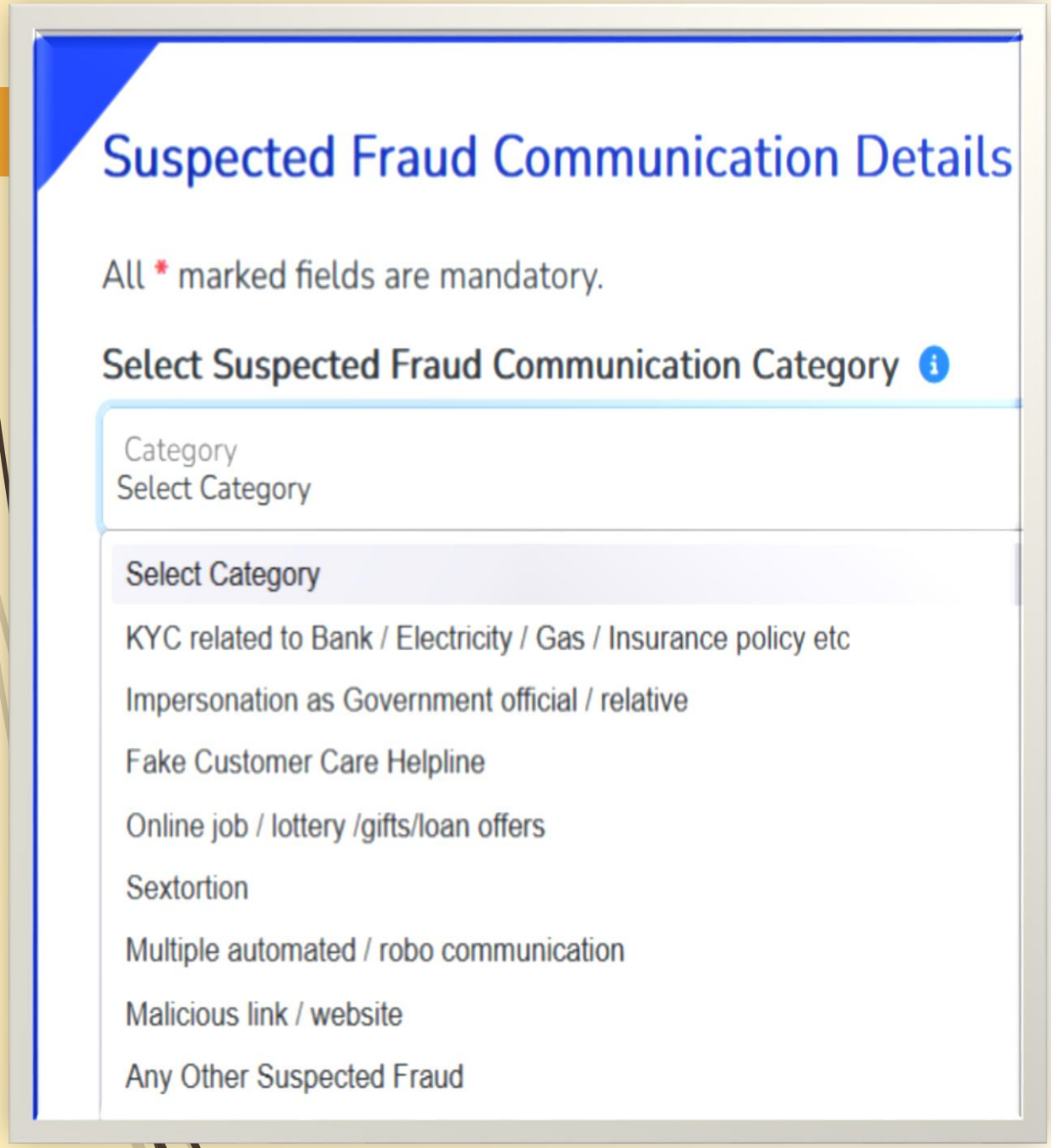
HOME | CITIZEN CENTRIC SERVICES | ABOUT | KEEP YOURSELF AWARE | FAQS | IN SOCIAL MEDIA | IMAGE GALLERY

चक्षु - Report Suspected Fraud Communication

(Report any suspected fraud communication received within last 30 days)

Chakshu

Chakshu facilitates citizens to report the suspected fraud communications with the intention of defrauding telecom service users for cyber-crime, financial frauds, non-bonafide purpose like impersonation or any other misuse through Call, SMS or WhatsApp.



- Following steps are to be taken: Visit Sanchar Saathi portal at www.sancharsaathi.gov.in
- Click Citizen Centric Services and then click on 'Chakshu - Report Suspected Fraud Communication'.
- Select the medium and category of suspected fraud communication.
- Provide the details of suspected fraud communication. Screenshot of the communication received may also be uploaded which is optional.
- Verify your mobile number with OTP and enter your name.
- Click submit button to submit the request.

- Suspected or unsolicited communications received through **call, SMS or WhatsApp** which are intended for:-

a. cyber-crime
b. financial frauds
c. Impersonation
d. fake customer services
e. lottery offer
f. loan offer
g. job offer
h. installation of mobile tower
i. disconnection of services or KYC update / loan etc. or any other misuse.

- Some of the suspected communication, received by the users, are related to frauds in the name of the following:
  - Expiry or deactivation of bank account
  - payment wallet
  - electric connection / mobile or SIM connection / gas connection
  - KYC update etc.

- Customer care helpline
- Impersonation as Government official / office or known persons / relatives
- Creating emergency in name of accident, custom duty violation etc.
- Online job / lottery / product / gift / services offer
- **Sextortion**
- Loan / lending
- Installation of mobile tower
- Multiple automated / robo calls
- Malicious links / website / URLs

https://www.cybercrime.gov.in/

cybercrime.gov.in/Webform/cyber_suspect.aspx

भारत सरकार
GOVERNMENT OF INDIA

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

Language

Indian Cyber Crime Coordination Centre
साइबर अपराध से निपटने के लिए एक साथ काम करना • Working Together With Vigour

सत्यमेव जयते

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
National Cyber Crime Reporting Portal

आज़ादी का अमृत महोत्सव

Report Suspect

This facility has been created for quick reporting of Attempts made to commit cybercrime using suspicious Website URLs, Whatsapp Numbers/ Telegram Handles, Phone Numbers, Email-IDs, SMS Headers/ Numbers and Social Media URLs etc. This will be used to build up a repository for analysis and monitoring of cybercrime.

If you have become a victim of Cybercrime, please report immediately at https://www.cybercrime.gov.in/ or 1930 National Helpline Number.

State of Incident* ---Select---

What do you want to report ?

- Website URL
- Whatsapp Number / Telegram Handle
- Phone number
- Email Id
- SMS Header/ Number
- Social Media URL
- Deepfake

stopncii.org

StopNCII.org
Stop Non-Consensual Intimate Image Abuse

Privacy Policy | Create Your Case | English

Check Case Status | Resources and Support | How It Works | About Us | Partners | FAQ

Watch out for fake StopNCII.org scams asking for your photos. The real StopNCII.org never asks to share or upload your pictures or videos. Only trust our official website and our approved Global Network of Partners.

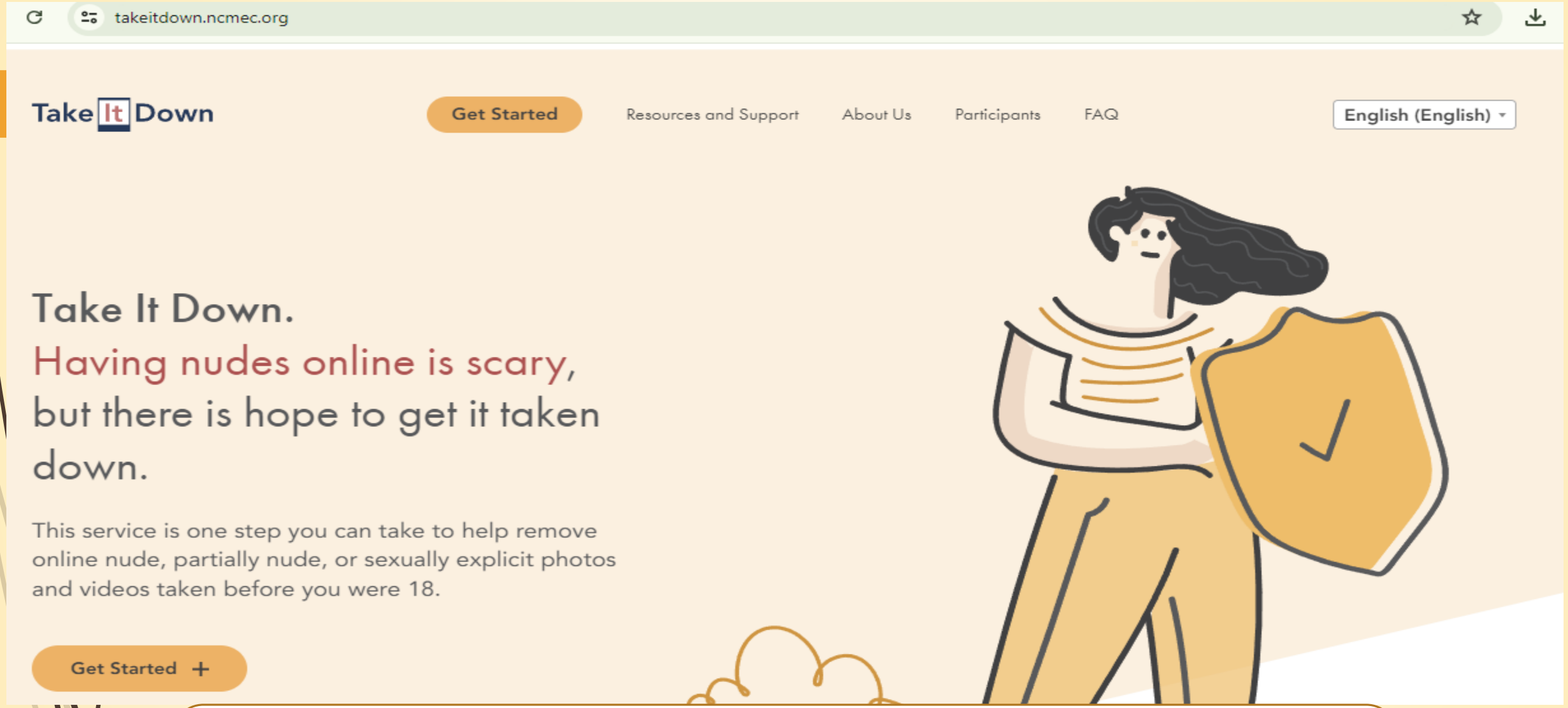
What do you do if someone is **threatening to share** your intimate images?

Create Your Case

Age 18 Yrs or Over

NON-CONSENSUAL INTIMATE IMAGE (NCII)

The tool works by generating a hash /digital fingerprint from intimate image(s)/video(s) and then StopNCII.org shares the hash with participating companies so they can help detect and remove the images from being shared online.



https://takeitdown.ncmec.org/

Age less than 18 Yrs

भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

RBI/DOS/2024-25/118
DOS.CO.FMG.SEC.No.5/23.04.001/2024-25 July 15, 2024

The Chairman / Managing Director / Chief Executive Officer
All Commercial Banks (including Regional Rural Banks)
All India Financial Institutions (AIFIs)[1]

5. Reporting of Frauds to Law Enforcement Agencies (LEAs)[23]

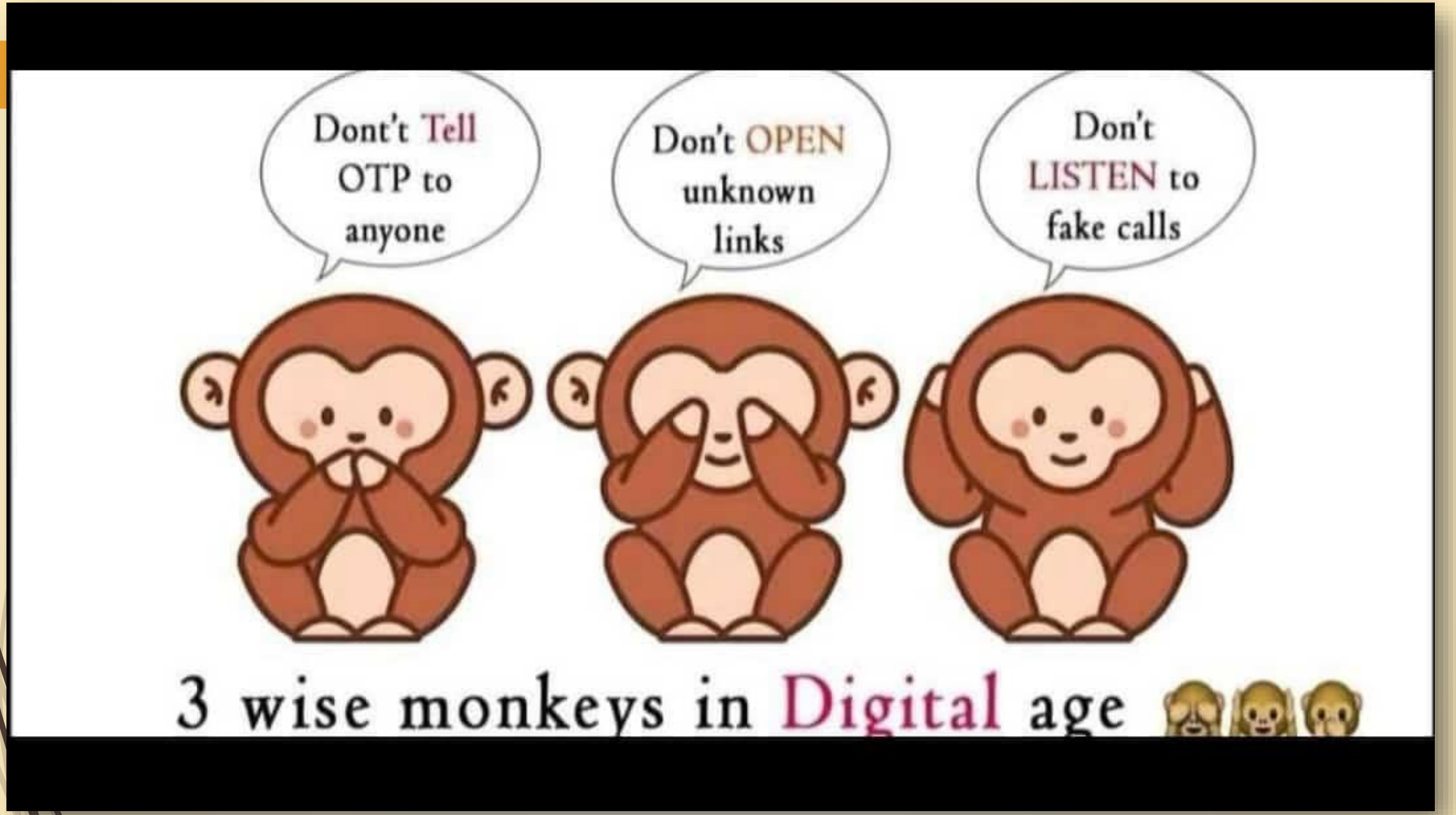
5.1 Banks shall immediately report the incidents of fraud to LEAs, subject to applicable laws, as indicated below[24]:

Category of bank	Amount involved in the fraud	LEA to whom complaint should be lodged	Remarks
Private Sector / Foreign Banks	Below ₹1 crore	State / Union Territory (UT) Police	
	₹1 crore and above	In addition to State/UT Police, Serious Fraud Investigation Office (SFIO), Ministry of Corporate Affairs, Government of India	Details of fraud are to be reported to SFIO in Fraud Monitoring Return (FMR) format.
Public Sector Banks / Regional Rural Banks	(a) Below ₹6 crore[25]	State / UT Police	
	(b) ₹6 crore and above	Central Bureau of Investigation (CBI)	

4.4 Penal Measures

4.4.1 Persons / Entities classified and reported as fraud by banks and also Entities and Persons associated[21] with such Entities, shall be debarred from raising of funds and / or seeking additional credit facilities from financial entities regulated by RBI, for a period of five years from the date of full repayment of the defrauded amount / settlement amount agreed upon in case of a compromise settlement.

4.4.2 Lending to such Persons / Entities, being commercial decisions, the lending banks shall have the sole discretion to entertain or decline such requests for credit facilities after the expiry of the mandatory cooling period as mentioned at Para 4.4.1 above.


Dont't Tell OTP to anyone
Don't OPEN unknown links
Don't LISTEN to fake calls
3 wise monkeys in Digital age

JOIN LATEST JUDGMENTS FOR LAWYERS WHATSAPP GROUP @ 7347447651

JOIN LATEST JUDGMENTS FOR LAWYERS WHATSAPP GROUP TO UPDATE YOURSELF FOR:

LATEST LEGAL UPDATES,
JOB ALERTS,
INTERNSHIP NOTIFICATIONS,
NOTES,
PDF FILES,
LAW RELATED VIDEOS,
LEGAL DRAFTS,
JUDGMENTS OF SUPREME COURT
&
HIGH COURTS OF INDIA.

PLEASE CONTRIBUTE PERMANENT MEMBERSHIP FEES (LIFETIME) OF RS 999/- ONLY TO JOIN THE GROUP.

PAY THROUGH GOOGLE PAY/PHONEPE/ PAYTM @ MOB. 7347447651.

CONTRIBUTE PERMANENT MEMBERSHIP FEES (LIFETIME) OF Rs 999/- ONLY TO JOIN THE GROUP.
PAY THROUGH GOOGLE PAY/PHONEPE/ PAYTM @ MOB 7347447651

AKSHAYA
pp channel

Akshaya Nayak, OPS
Dy.S.P., BPSPA
M.No. 8144033879