



गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS



Understanding the Digital Arrest and Online Investment Scam



Overview of I4C

The Ministry of Home Affairs has set up the 'Indian Cyber Crime Coordination Centre' (I4C) as an attached office to deal with all types of cybercrimes in the country, in a coordinated and comprehensive manner.

VISION

To create a safe cyberspace for the citizens of India

MISSION

To create an effective framework and ecosystem for the prevention, detection, investigation, and prosecution of Cybercrime in the country.



What is a Digital Arrest?

- A Digital Arrest is a new kind of online scam where cybercriminals impersonate law enforcement agencies (like police, CBI, RBI, ED, or cyber cell officers) to intimidate victims into transferring money or sharing sensitive information.
- It's called “digital arrest” because the entire deception happens online — through video calls, fake documents, and threats of legal action, without any real arrest.



**DIGITAL
ARREST**

CYBER SCAM

Understanding Digital Arrest Scams

- Victims receive fake calls from individuals posing as police or government officers.
- Scammers claim the victim is involved in illegal activity or identity misuse.
- Victims are pressured to transfer money or share sensitive data to 'avoid arrest'.
- Fraudsters may use video calls, fake IDs, and official logos for legitimacy.



155260

CyberDoot

www.cybercrime.gov.in

-  Common Signs of Digital Arrest Scam:
- Fake callers claim to be from ‘Cyber Crime Police’ or ‘RBI’.
- Use fake IDs, video calls with false police backgrounds, or forged official emails.
- Mention terms like ‘digital case’, ‘online FIR’, or ‘video investigation’.
- Demand urgent payments to avoid arrest.

How It Works (Modus Operandi):

- 1 Initial Contact** – Victim receives a call, message, or email claiming to be from police, customs, or cybercrime department.
- 2 Fake Accusation** – Scammers say the victim's phone number, Aadhaar, or bank account was linked to a crime (like drug trafficking or money laundering).
- 3 Threat & Isolation** – Victim told not to speak with anyone and kept on long video calls for 'digital custody'.
- 4 Extortion** – Asked to pay a refundable fine, verification fee, or bail amount (all fake).
- 5 Disappearance** – Once payment is made, scammers vanish.

Modus Operandi (Digital Arrest)

- ****Contact & Threat**** – Victim receives intimidating call or message.
- ****Fake Verification**** – Scammers show forged warrants or IDs.
- ****Isolation**** – Victims told not to talk to family or friends.
- ****Payment Demand**** – Asked to transfer funds to ‘verify’ or ‘settle’ cases.
- ****Disappear**** – Once money is received, scammers vanish.

Common Storylines Used in Digital Arrest Scams

- **Parcel Interception**

Victims receive a call claiming that a suspicious parcel containing illegal items (such as drugs or weapons) has been intercepted and is linked to their name or address. The scammers then escalate the situation by connecting the victim to a supposed police officer, who threatens arrest unless the victim cooperates.

- **Family Member Involvement:**

Scammers may claim that a family member has been arrested or is involved in criminal activity. They often demand immediate financial assistance to secure the release of the family member or to avoid further legal complications.

- **Aadhaar or Phone Number Misuse:**

Victims are accused of having their Aadhaar number or phone number misused for illegal activities. The scammers create a narrative that the victim is implicated in crimes like money laundering or human trafficking, pressuring them to pay fines to clear their name.

Aadhaar or Phone Number Misuse:

Victims are accused of having their Aadhaar number or phone number misused for illegal activities. The scammers create a narrative that the victim is implicated in crimes like money laundering or human trafficking, pressuring them to pay fines to clear their name.

- **Explicit Content Allegations:**

Victims receive calls alleging that their phone number has been used to share pornographic content. Scammers may claim that an FIR has been filed against them, demanding payment to clear their name and avoid arrest.

- **Fake Legal Proceedings:**

In some cases, scammers conduct fake video calls where they impersonate judges or legal officials, presenting fabricated court documents. They threaten the victim with legal action and demand payment to avoid arrest or further legal troubles.



- **Financial Fraud Allegations**

Victims are informed that they are under investigation for financial fraud, such as money laundering or tax evasion. The scammers use intimidation tactics, claiming that failure to cooperate will result in immediate arrest

- **Emergency Situations:**

Scammers may create a sense of urgency by claiming that the victim's identity has been used in illegal activities, such as identity theft or fraud. They often demand immediate action to resolve the situation, leading victims to panic and comply without verifying the claims

Some Stories of Digital Arrest Scams

- On 12 October 2023, a 23-year-old woman from Faridabad was contacted by a scammer who claimed to be a customs official based in Lucknow, alleging her involvement in a human trafficking ring. She was asked to “digitally log in” for an interrogation through Skype, during which the other associated group of scammers, posing as police officers, showed falsified evidence, including a package containing numerous ‘fake’ passports and other identification documents under her Aadhaar number.
- .On 28-29 August 2024, the Chairman and Managing Director of the renowned Vardhman Group— S P Oswal, 82-year-old, was defrauded of ₹7 crore by fraudsters posing as officials from various government agencies, including the Supreme Court of India. The victim, S P Oswal, was placed under “digital arrest” for two days as a result of the tactic, which included phoney paperwork and a “fake” virtual courtroom. He was tricked into believing he was under investigation for financial violations connected to a case involving former Jet Airways chairman Naresh Goyal. Further, the scammers tricked Oswal into thinking that his identity had been stolen and that he was being investigated for a (false) bank account, which was connected to the ongoing inquiry against Goyal.

- On 13 November 2023, a Noida-based, 50-year-old woman lost ₹11.11 lakh in a ‘digital arrest’ where cybercriminals claimed a parcel in her name linked to drug smuggling. Similar to previous cases, scammers were personified as customs and police officials. In her complaint, the victim informed that she was contacted over an IVR (Interactive Voice Response) call and told that her Aadhaar card was used to buy a mobile phone SIM card in Mumbai, which was then used for unlawful activities, including harassment of women. A scammer who claimed to be a Mumbai Police officer later took over her call, conducted the ‘initial interrogation’ over the phone, and later on Skype VC.
- On 04 March 2024, a Noida-based IT engineer lost ₹3.75 lakh after scammers posed as customs officials and claimed that a parcel in her name contained narcotic substances. Via Skype call, the scammers fabricated a “digital arrest”, intimidating her into providing personal details and transferring money to ‘clear her name’.
- On 01 August 2024, Dr Ruchika Tandon, an Associate Professor at the Neurology Department at Sanjay Gandhi Postgraduate Institute of Medical Sciences (SGPIMS), Uttar Pradesh, filed a complaint against unidentified scammers who posed as officials of TRAI (Telecom Regulatory Authority of India). The scammer informed her that 22 complaints had been filed against her mobile SIM card and that a CBI official over Skype would interrogate her. The ‘fake’ CBI official told her that she was accused of her involvement in a money laundering case, and her bank account was used for financing illicit activities, including women and child trafficking. To avoid further legal consequences, the victim paid ₹2.81 Crore to scammers.



In the case of the 72-year-old businessman, the fraudsters conducted fake court proceedings and police interrogations over video calls, tricking him into transferring 58.13 crore rupees over 40 days, wiping out his entire life savings.



Indian
Cyber
Crime
Coordination
Centre

सहयोगी कार्यवाही

Working Together With Vigour

Elderly couple loses ₹70L in 'digital arrest'

Fraudsters posed as IPS officers and NIA officials, keeping the senior citizens under 24/7 video surveillance to extort huge sums of money

Amruta Agashe
amruta.agashe@timesofindia.com

Three people have been booked by the SAR. Many police for allegedly subjecting an elderly couple to a 'digital arrest' and extracting them of Rs 70 lakh. The account reportedly introduced allegations as IPS officer Subhash Datta and other law enforcement officials.

The cyber case is light on September 29 when the victim, a 73-year-old former IAS officer, was approached by a person claiming to be an IPS officer and asking him to share his bank account details.

According to the FIR, the victim made a call to a woman who introduced herself as 'Vijaya Shama'. She told the victim that his phone number was allegedly involved in an investigation related to the witness attack in Pahalgam and claimed that personnel from air, intelligence, and administrative offices, including him, were involved. She threatened that all his bank accounts and mobile number would be frozen unless he transferred to the Anti-Terrorism Squad (ATS) office in New Delhi. She further stated that the investigation would be handled by the National Investigation Agency (NIA) with the investigating officer being KJ Prasad Kumar Gauram.



Callers told the couple that their number had been used in the terrorist attack in Pahalgam, adding prominent industrialists were also involved.

The victim initially ignored the calls but later received a call and the victim panicked. He called his daughter, who then called the police. The police then contacted the victim and the victim transferred the money to the police. The couple were reportedly kept under

digital surveillance, monitored through a 24/7 webcam, and restricted to use of all other electronic devices.

On September 26, a man impersonating IPS Subhash Datta told the victim that he could be booked under PMLA and demanded a payment. He promised the victim was making a bank State Cyber Terrorism (SCT) transfer, assuring him that an acknowledgment would be issued by the SAR.

On September 27, the couple was informed that their money would not be received and that they were "free". They received the acknowledgment from the SAR and made the final payment on September 28.

The SAR. Many police confirmed that the couple was defrauded of Rs 70 lakh and that the complaint had picked up a negative tag on SAR.

"We received the information, and the complaint registered as FIR. The SAR is

Stay safe

- Police do not arrest anyone online. Beware of digital threats.
- Never share your OTP or banking details with anyone.
- If you suspect an online threat, call 112 immediately.
- Avoid answering calls from unknown numbers.

delivered there on the arrested but later the name of IPS Subhash Datta was taken out. We have registered an FIR, and we are currently tracing the matter," the police said.

Three people have been booked under the provisions of the IT Act, whereas the complaint is a public interest and other charges under the IT Act.

Chinese gang

Six arrested in int'l 'digital arrest', cyber fraud ops

Nepal-based gang targets unemployed youths, forces victims to surrender accounts; washed nearly Rs 49L in current case

Ahmedabad Mirror Bureau
feedback@ahmedabadmirror.com

Posts @ahmedabadmirror

The city cybercrime unit has broken up a sophisticated 'digital arrest' and cyber fraud operation run by Chinese nationals from Cambodia and Nepal. Six people have been caught in the case. The gang pressured an Indian victim into sharing his bank details and took him to Nepal. They then funnelled Rs 48.85 lakh through his account before moving the money to handlers in Cambodia.



Locked in hotel

ACP Hanish Makadia of the cybercrime unit told Mirror that Pranay Bhavsar was tricked into sharing his bank account details for "Jay Ambe Garment". The scammers claimed he would receive legitimate funds from Dubai.

"They took him to Kathmandu, Nepal and locked him in a room at Hotel Cascade," explained Makadia. "Yash Yadav sent Bhavsar's account details to Anil, who passed them to Manan Goswami in Cambodia."

The stolen money went into Bhavsar's account and was converted into cryptocurrency (USDT) before reaching Chinese handlers. The gang members earned commissions for

these transactions.

"We believe this is now their standard method—taking account holders to Nepal, holding them in hotel rooms, and using their accounts to wash cyber fraud money," Makadia added. "While victims stayed in hotel, Daniel and his Lisek wife lived in a nearby penthouse."

The National Cyber Crime Reporting Portal has received nearly 200 complaints about similar incidents.

Senior cybercrime officials revealed the gang specifically went after unemployed youths. They offered fake jobs before forcing them into cybercrime activities.

Denis done in Dubai

Investigators found that Gautam Chauhan made several trips to Dubai. During one visit, he met with Chinese handlers and planned to move operations to Nepal due to increased pressure from Cambodian authorities. Gautam also regularly travelled to Singapore and Nepal as part of the operation's international network.

[Online Investment Scams](#)

- Fake investment or trading platforms promise high, risk-free returns.
- Victims see fake dashboards showing inflated profits.
- Pressure tactics: 'Limited offer' or 'exclusive opportunity'.
- Fake celebrity or government endorsements increase trust.



Modus Operandi (Investment Fraud)

- **Reconnaissance**— Gather personal info via social media or leaks.
- **Grooming** – Build trust via chat, social apps, or email.
- **Execution** – Encourage investing in fake apps or sites.
- **Fund Movement** – Divert funds through crypto or money mules.
- **Exit**— Platforms vanish; scammers rebrand and restart.



How It Works (Modus Operandi):

1 Attraction:

Victims see ads or messages on social media, WhatsApp, Telegram, or dating sites promoting “**high-profit**” investment opportunities.

2 Fake Platforms:

They direct victims to fake trading or investment apps that show false profits on dashboards to lure more deposits.

3 Pressure Tactics:

They use lines like “Limited-time offer,” “Guaranteed 200% returns,” or “Exclusive insider deal” to create urgency.

4 Payment & Lockdown:

Once victims invest large sums, **withdrawals are blocked**, and scammers demand extra fees or taxes to release funds.

Warning Signs & Red Flags

- Offers of high returns with no risk — this is always a trap.
- Unverified or fake websites and apps claiming to be investment or trading platforms.
- Asking you to pay “tax” or “fees” before getting your own money.
- Creating fear or urgency to make you act fast.
- No official proof or contact details — only WhatsApp or social media messages.

Prevention for Individuals

- Verify any law enforcement call through official helplines or local police.
- Never transfer money to settle online 'cases'.
- Check investment offers on SEBI, RBI, or official websites.
- Enable two-factor authentication and keep software updated.
- Avoid clicking on suspicious links or sharing OTPs.



For Organizations

- Conduct regular cyber awareness workshops.
- Implement KYC and transaction monitoring systems.
- Educate employees about social engineering tactics.
- Report suspicious activity promptly to authorities.



भारतीय
घर
अधिनियम
2019

भारतीय
घर
अधिनियम
2019

भारतीय
घर
अधिनियम
2019

PART TIME JOB

FULL TIME JOB

**DID YOU JUST RECEIVE
AN ONLINE JOB OFFER
IN THE NAME OF A REPUTED
ORGANIZATION**

BEWARE - THIS MAY BE A SCAM

Do not click on unverified links

Never give personal or financial
information to strangers

How to Avoid Digital Arrest /Online investment Scams

-
- Both Digital Arrest and Online Investment Scams exploit fear and greed.
- Stay calm and verify all claims through official channels.
- Report any suspicious messages, calls, or websites.
- Awareness is the strongest defense against cyber fraud.

Where to Report:

- - Cybercrime.gov.in
- - 1930 Helpline
- - Police/cyber cell
- - Bank customer care



Report a
Cybercrime on
1930

Report a Cybercrime on
www.cybercrime.gov.in



Report Suspect Data on NCRP Portal



<https://cybercrime.gov.in/>

REGISTER A COMPLAINT + TRACK YOUR COMPLAINT SUSPECT DATA - CYBER VOLUNTEERS + LEARNING CORNER + CONTACT US








- SUSPECT SEARCH (MOBILE, EMAIL, ETC.)
- SUSPECT SEARCH (WEBSITE/APP)
- REPORT SUSPECT

This facility has been created for quick reporting of Attempts made to access various 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.

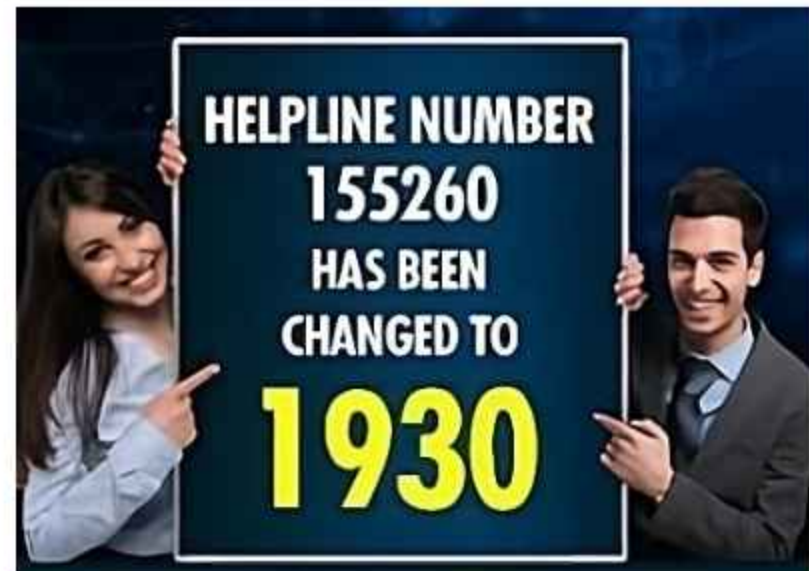
State of Incident*

What do you want to report ?

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

Report 1930

- The Ministry of Home Affairs has launched a toll-free Helpline number '1930'
- In today's digital age, the necessity of a dedicated platform to report and combat cybercrimes is more crucial than ever. The helpline plays a vital role within the National Cybercrime Reporting Portal, which aims to establish a safe cyberspace for all citizens.



Do's & Don'ts:



Do:

- Stay Calm and Think Clearly Do not panic if someone claims you are under investigation or arrest.
- Report Immediately File a report on www.cybercrime.gov.in
- Educate Family & Colleagues Inform others about this scam so they can recognize and avoid it.
- Preserve Evidence Take screenshots, record the number, and save any fake documents or videos for reporting.

Don't:

- **Don't Transfer Money** — Never send funds to any account to “settle” or “verify” a case
- **Don't Share Personal Data** — Avoid sharing Aadhaar, PAN, bank details, or OTP with anyone over a call or video.
- **Don't Stay on Long Calls** — Fraudsters keep victims on extended video calls to mentally manipulate them.
- **Don't Click Suspicious Links** — Avoid any email, SMS, or WhatsApp link claiming to be from law enforcement.
- **Don't Delay Reporting** — Immediate reporting increases the chances of tracing and freezing the transaction.

Ministry of Home Affairs
ICCC
Cyber Crime Coordination Centre

OTP Fraud
Cyber Bullying
Earning app Fraud
QR code scan
Phishing
Ransomware
Credit card Fraud
Sexortion
Investment Fraud
KYC Fraud

Don't be a Victim!

1930 and
cyberCrime.gov.in

Follow

The illustration features a large purple umbrella with a silver handle, set against a golden-yellow background. Raindrops of various sizes are falling from the umbrella, each labeled with a type of cybercrime: OTP Fraud, Cyber Bullying, Earning app Fraud, QR code scan, Phishing, Ransomware, Credit card Fraud, Sexortion, Investment Fraud, and KYC Fraud. Below the umbrella, the text 'Don't be a Victim!' is written in a bold, dark red font. Underneath this, there is a telephone icon next to the number '1930 and' and the website 'cyberCrime.gov.in'. To the right, the word 'Follow' is written in a dark red font, with a dotted line leading to a circular logo for the Cyber Crime Coordination Centre (ICCC). At the bottom of the image, there are two groups of stylized human figures. On the left, a group of four people (two men and two women) are walking and looking at their mobile phones. On the right, a group of five people (three women and two men) are walking, also looking at their mobile phones. The overall theme is awareness and prevention of cybercrime.



**CyberDost को फॉलो करो
सेफ रहो, सुरक्षित रहो**

Government Initiative:

- The Central Government has launched a comprehensive awareness programme on digital arrest scams which, inter-alia, include; newspaper advertisement, announcement in Delhi Metros, use of social media influencers to create special posts, campaign through Prasar Bharti and electronic media, special programme on Aakashvani.
- To spread awareness on cyber crime, the Central Government has taken steps which, inter-alia, include; dissemination of messages through SMS, I4C social media account i.e. X (formerly Twitter) (@CyberDost), Facebook(CyberDostI4C), Instagram (cyberDostI4C), Telegram(cyberdosti4c), Radio campaign, engaged MyGov for publicity in multiple mediums, organizing Cyber Safety and Security Awareness weeks in association with States/UTs, publishing of Handbook for Adolescents/Students, digital displays on railway stations and airports across, etc.
- Public Events & Advertisements: Ongoing awareness drives, roadshows, and digital campaigns against scams like Digital Arrest, Investment Fraud, and OTP Fraud.

- Awareness Videos Portal:

Visit: i4c.mha.gov.in/cyber-awareness-videos.aspx

- for short films on cyber safety.
- <https://i4c.mha.gov.in/awareness.aspx>



Conclusion:

Law enforcement agencies **never demand money online** or through video calls.

Always **verify the authenticity** of any threatening communication

“An Aware Citizen is a Safe Nation”





PM ON DIGITAL ARRESTS

“Beware of digital arrest frauds. There is no system like digital arrest under the law”

NARENDRA MODI, PM

HIS ADVICE

1. Stay calm and do not panic. Record or take a screen recording if possible.
2. Remember that no government agency will threaten you online.
3. Take action by calling the national cyber helpline and also inform the police about the crime

Source: Mann ki Baat



Thanks