

Unmasking Digital Arrest Scams

Posted at: 06/11/2024

Unmasking Digital Arrest Scams: ED and I4C's Crackdown on Cyber Fraud

Context

- The Enforcement Directorate (ED) recently filed a prosecution complaint under the Prevention of Money Laundering Act (PMLA) against eight individuals involved in cyber scams
- These individuals allegedly **defrauded people** through fake IPOs and stock investments, primarily using social media platforms like **WhatsApp**, **Instagram**, **and Telegram**.
- Additionally, the Indian Cyber Crime Coordination Centre (I4C) has issued a new advisory warning citizens against digital arrest scams.

Indian Cyber Crime Coordination Centre (I4C

Overview

- I4C is an initiative by the Ministry of Home Affairs to address cybercrime in a coordinated manner across the country.
- It aims to:
 - Enhance coordination between law enforcement agencies and other stakeholders.
 - Improve India's capability to tackle cybercrime.
- Launched in January 2020 to serve as a central body for combating cybercrime.

Objectives of I4C

- Central Nodal Point to tackle cybercrime across the nation.
- Strengthen measures against cybercrimes targeting women and children.
- Facilitate easy filing of cybercrime complaints and analyze cybercrime trends and patterns.
- Serve as an early warning system for proactive prevention and detection of cybercrimes.
- Raise public awareness on cybercrime prevention.

Key Initiatives

- National Cybercrime Reporting Portal (www.cybercrime.gov.in): 24/7 platform for reporting cybercrimes.
- Citizen Financial Cyber Fraud Reporting and Management System: For immediate reporting of financial cyber frauds.

- National Toll-Free Helpline '1930': Assists citizens in lodging online cyber complaints.
- National Cyber Forensic Laboratory (NCFL): A state-of-the-art facility for training and aiding state/UT investigators.
- CyTrain Portal (https://cytrain.ncrb.gov.in): MOOC platform to train police and judicial officers in cybercrime investigation, forensics, and prosecution.
- CyberDost Social Media Handle: Created to promote cybercrime awareness among citizens.

Digital Arrest Scams

About Digital Arrest Scams

- A digital arrest scam is an online fraud where scammers impersonate law enforcement officials to deceive victims.
- They falsely accuse victims of criminal activities, intimidate them, and demand payments
 to avoid supposed arrests.

How the Scam Works

- Scammers impersonate officials from agencies like the CBI, Income Tax Department, or Customs.
- They contact victims via **phone calls**, later switching to **video calls** on platforms like WhatsApp or Skype to add credibility.
- Scammers use tactics like showing a **police station setup**, threatening **arrest warrants**, or accusing victims of **legal violations**.
- Victims are pressured to make **payments to "clear their name"** or as a "security deposit" for investigations.
- Once payments are made, scammers disappear, leaving victims with financial losses.

ED Files Charge Sheet in Digital Arrest Scams

Recent Developments

- Following PM Modi's warning against digital arrest scams, investigative agencies have taken active measures to counter this cyber threat.
- The ED recently filed a charge sheet for a digital arrest scam, and I4C issued a public advisory.

PM Modi's Warning on Digital Arrest Scams

- In his recent Mann Ki Baat address, PM Modi warned citizens of scammers posing as law enforcement conducting 'digital arrests' to extort money.
- He advised the public to "stop, think, and act" to protect themselves.

ED's Investigation

• The ED's prosecution complaint under the PMLA targets eight individuals accused of cyber fraud.

- These scams, often called 'pig-butchering' scams, lure victims with promises of high returns on fake stock investments.
- Fraudsters used **fake websites** and WhatsApp groups that appeared associated with **reputable financial firms**.
- Scammers impersonated officials from agencies like Customs or the CBI, accusing victims of legal violations to coerce them into transferring money.
- Funds were routed through **mule accounts**, converted to **cryptocurrency**, and transferred abroad.
- Key accused recruited directors for shell companies and facilitated bank account openings to aid money laundering.
- Many victims were manipulated through "digital arrests" under a fake "fund regularisation process".

I4C Advisory to Citizens

- I4C's public advisory warns against digital arrest scams, emphasizing that legitimate officials do not make demands over video calls.
- Citizens are encouraged to report suspicious activities via the national cybercrime helpline (1930) or the cybercrime portal.

