Digital Arrest Scams

Source: TOI

Why in News?

The Ministry of Home Affairs (MHA) has issued a warning about an increase in **'digital arrest' scams,** where **cybercriminals** impersonate government officials to extort money from unsuspecting victims.

- The **Indian Cybercrime Coordination Centre (I4C)**, in collaboration with Microsoft, is actively combating this organised online economic crime.

What are Digital Arrest Scams?

- **Cybercriminal Impersonation**: Scammers pose as personnel from various government agencies, including the police, Central Bureau of Investigation (CBI), Narcotics Department, Reserve Bank of India (RBI), **or** Enforcement Directorate.
- **Intimidation Tactics:** Victims receive calls alleging their **involvement in illegal activities,** such as sending or receiving contraband items like drugs or fake passports.
    - Claims may also involve a loved one supposedly caught in criminal activities or accidents, with the fraudsters demanding money to resolve the 'case'.
- **Digital Confinement:** Some victims are subjected to 'digital arrest,' where they are forced to stay on video calls with the scammers until their demands are met.
- **Demands for Money**: Criminals are **extorting money in exchange** for agreeing not to expose the false legal cases that have been constructed.

What are the Steps Being Taken to Combat These Scams?

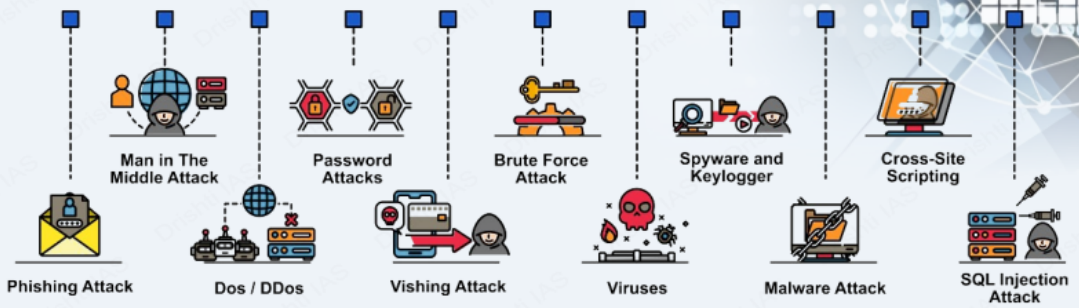
- **Blocking Fraudulent Accounts**: The I4C, has blocked over 1,000 Skype accounts linked to intimidation, blackmail, extortion, and "digital arrests" of citizens by cybercriminals posing as government personnel.
    - I4C is also facilitating the blocking of SIM cards, mobile devices, and mule accounts used by these fraudsters.
- **Cross-Border Crime Syndicates**: The MHA has identified that these scams are operated by cross-border crime syndicates, making them part of a larger, organised online economic crime network.
- **Alerts and Awareness:** I4C has issued various alerts regarding such frauds on its social media **platform "cyberdost,"** and other platforms.
    - If someone receives such a call, they should immediately report the incident on the **cybercrime helpline number** or the website **“National Cyber Crime Reporting Portal”** for assistance.

//

CYBER SECURITY

Cybersecurity refers to any technology, measure, or practice for preventing cyberattacks or mitigating their impact.

CYBER SECURITY ATTACKS



'Crime in India' Report 2022 (NCRB) highlighted 24.4% surge in cybercrimes in India since 2021.

Common Cybersecurity Myths

- Strong passwords alone are adequate protection
- Major cybersecurity risks are well-known
- All cyberattack vectors are contained
- Cybercriminals don't attack small businesses

Cyber Warfare

- Digital attacks to disrupt vital computer systems, to inflict damage, death, and destruction.

CYBER THREAT ACTORS

CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

Types of Cybersecurity

- Critical infrastructure security (Robust access controls)
- Network security (Deploying firewalls)
- Application security (Code reviews)
- Cloud Security (Tokenization)
- Information security (Data masking)

Recent Major Cyber Attacks

- WannaCry Ransomware Attack (2017)
- Cambridge Analytica Data Breach (2018)
- Financial data of 9M+ cardholders, including SBI, leaked (2022)

Regulations & Initiatives

- **International:**
  - UN Group of Governmental Experts (GGE) on Advancing Responsible State Behaviour in Cyberspace
  - NATO's Cooperative Cyber Defense Centre of Excellence (CCDCOE)
  - Budapest Convention on Cybercrime, 2001 **(India not a signatory)**
- **India:**
  - IT Act, 2000 (Sections 43, 66, 66B, 66C, 66D)
  - National Cyber Security Policy, 2013
  - National Cyber Security Strategy 2020
  - Cyber Surakshit Bharat Initiative
  - Indian Cyber Crime Coordination Centre (I4C)
  - Computer Emergency Response Team-India (CERT-In)

Steps Needed for Cyber Security

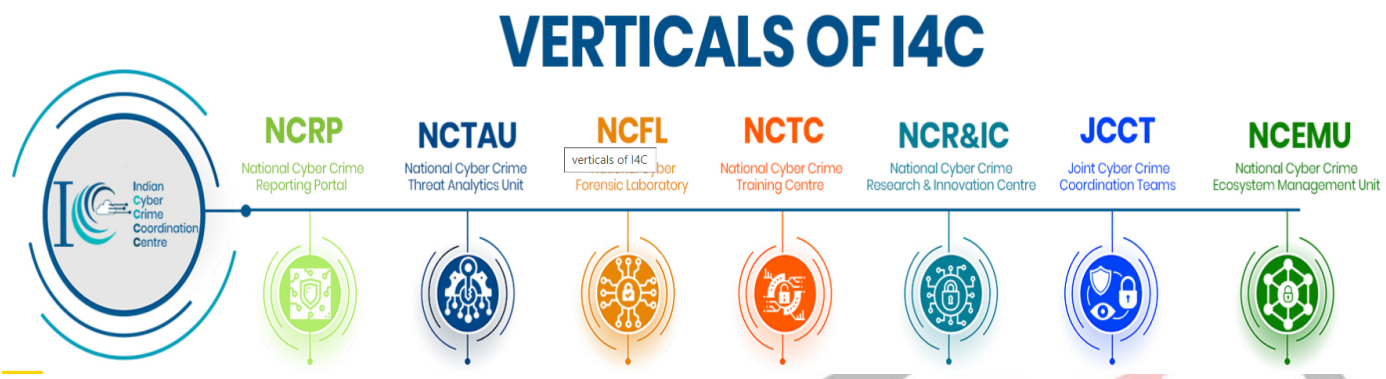
- Network Security
- Malware Protection
- Incident Management
- User Education and Awareness
- Secure Configuration
- Managing User Privileges
- Information Risk Management Regime

Drishti IAS

Indian Cybercrime Coordination Centre (I4C)

- It was established by MHA, in New Delhi to provide a framework and eco-system for **Law Enforcement Agencies (LEAs) for dealing with Cybercrime** in a coordinated and

comprehensive manner.
    - I4C is envisaged to act as the **nodal point to curb Cybercrime in the country.**
- It proposes **amendments to cyber laws to keep up with rapidly evolving technologies** and international cooperation.
- Coordinate implementation of **Mutual Legal Assistance Treaties (MLAT)** with other countries for cybercrimes in consultation with the relevant authority in MHA.
    - MLAT is a bilateral agreement between two or more countries that allows for the exchange of information and evidence to enforce criminal or public laws.



Read more: India's Cybersecurity Challenge: Threats and Strategies

UPSC Civil Services Examination, Previous Year Question (PYQ)

Q. In India, under cyber insurance for individuals, which of the following benefits are generally covered, in addition to payment for the loss of funds and other benefits? (2020)

1. Cost of restoration of the computer system in case of malware disrupting access to one's computer
2. Cost of a new computer if some miscreant wilfully damages it, if proved so
3. Cost of hiring a specialised consultant to minimise the loss in case of cyber extortion
4. Cost of defence in the Court of Law if any third party files a suit

Select the correct answer using the code given below:

(a) 1, 2 and 4 only
(b) 1, 3 and 4 only
(c) 2 and 3 only
(d) 1, 2, 3 and 4

Ans: (b)

Q. In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centres
3. Body corporate

Select the correct answer using the code given below:

(a) 1 only
(b) 1 and 2 only

(c) 3 only
(d) 1, 2 and 3

Ans: (d)

PDF Refernece URL: https://www.drishtiias.com/printpdf/digital-arrest-scams