PLUTUS IAS

CURRENT AFFAIRS

Argasia Education PVT. Ltd. (GST NO.-09AAPCAI478E1ZH)
Address: Basement C59 Noida, opposite to Priyagold Building gate, Sector 02,
Pocket I, Noida, Uttar Pradesh, 201301, CONTACT NO:-8448440231

Date –30 NOVEMBER 2024

"DIGITAL ARRESTS: THE INTERSECTION OF TECHNOLOGY AND CRIMINAL JUSTICE"

SYLLABUS MAPPING:

GS-3-Internal security challenges (Cyber Security)-"Digital Arrests: The Intersection of Technology and Criminal Justice"

FOR PRELIMS:

What is a digital arrest scam, and various govt initiatives in this regard?

FOR MAINS:

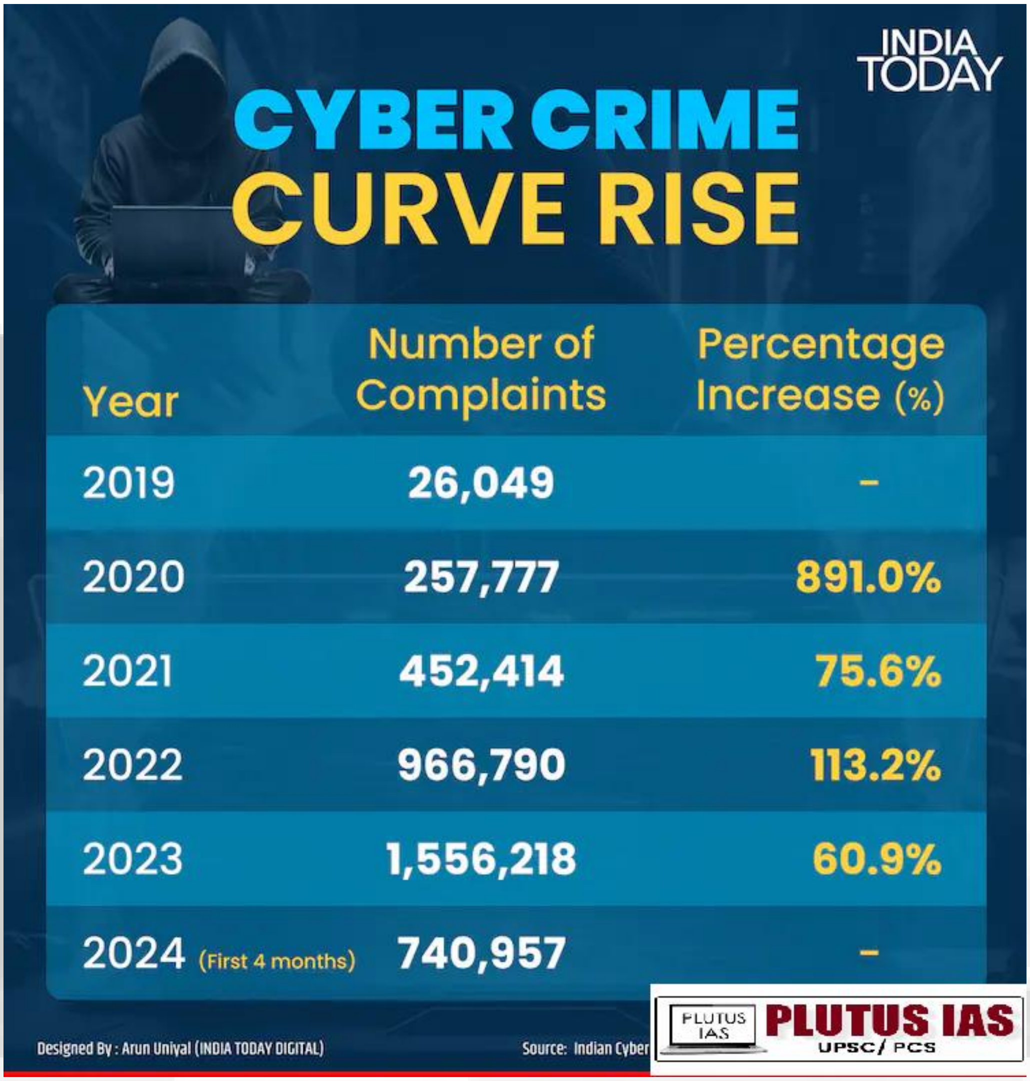
"What are the modus operandi of cybercrime and issues arising out of it and govt initiatives and way forward

WHY IN THE NEWS?

In his Mann Ki Baat address to the nation, Prime Minister Narendra Modi expressed concerns about the growing issue of "digital arrest fraud." During his speech, he shared an audio-visual clip featuring a man impersonating a police officer, pressuring the victim to provide their Aadhaar number in order to block a mobile number. This deceptive tactic plays on people's fears of digital arrest, with fraudsters exploiting these concerns to scam individuals. Digital arrest fraud represents a new and serious form of cybercrime in India, posing significant risks. These cybercrimes must be dealt with promptly to prevent further harm.

WHAT IS A DIGITAL ARREST SCAM?

A digital arrest scam is an online fraud where scammers deceive victims into handing over their hard-earned money. They use intimidation tactics to falsely accuse individuals of illegal activities, pressuring them into paying a ransom to avoid arrest or legal consequences.



INDIA TODAY

CYBER CRIME CURVE RISE

Year	Number of Complaints	Percentage Increase (%)
2019	26,049	-
2020	257,777	891.0%
2021	452,414	75.6%
2022	966,790	113.2%
2023	1,556,218	60.9%
2024 (First 4 months)	740,957	-

Designed By : Arun Uniyal (INDIA TODAY DIGITAL)

Source: Indian Cyber

EXAMPLE OF DIGITAL ARREST:

1. Mumbai (2023): In one of the major cases, a man in Mumbai was duped by fraudsters who posed as officials from the Income Tax Department. The scammers contacted him via phone, accusing him of tax evasion and threatening a digital arrest unless he immediately paid a large sum to clear the charges. The victim was directed to a Video call, where the scammers used a police station backdrop to intimidate him. Fearing arrest, he transferred the money but later realized it was a scam when he couldn’t contact the so-called officers again.

2. Delhi (2022): A woman in Delhi received a call from someone claiming to be from the Central Bureau of Investigation (CBI). The caller informed her that her name was linked to a financial crime and that a digital arrest warrant had been issued. She was told she could avoid arrest by paying a refundable security deposit to “clear her name.” The scammer pressured her to make the payment quickly and provided bank account details. After transferring the money, she discovered that the CBI had no such case and the call was a scam.

3. Bengaluru (2023): In Bengaluru, a businessman was targeted by fraudsters who impersonated customs officials. They claimed the businessman was involved in illegal import activities and threatened a digital arrest unless he paid a substantial fee. The scammers used a fake police set up during a video call to make the scam appear legitimate. They demanded money through a UPI transfer. After paying the amount, the businessman realized it was a scam when he could not contact the authorities again.

WAY OF DIGITAL ARREST /MODUS OPERANDI:

Step	Description
Initial Contact	Cybercriminals reach out via phone calls, text messages, or emails, impersonating law enforcement officials.
Call Progression	After audio calls, scammers switch to video calls, appearing to be in official locations like police stations or courthouses.
Use of Fake Identities	Scammers use images of real police officers, lawyers, or judges to display pictures during calls to increase credibility.
Document Forgery	Fake arrest warrants, legal notices, or official-looking documents are sent via email or messaging apps to intimidate the victim.
Creation of False Urgency	Scammers pressure victims by claiming they must resolve the issue quickly, such as saying, “Pay now or face arrest.”
Threat of Digital Arrest	Victims are threatened with a digital arrest warrant for alleged illegal activities, such as financial crimes or tax evasion.
Fake Payment Demands	Scammers demand immediate payments through bank transfers, UPI IDs, or cryptocurrency, claiming it will avoid arrest or resolve the issue.
Simulated Legal Procedure	Fraudsters create fake courtrooms, police stations, or legal processes using manipulated videos to appear more legitimate.
Fake Verification Codes	Victims may be asked to provide OTPs (One-Time Passwords) to access bank accounts or personal details.
Exploiting Panic and Emotional Pressure	Scammers increase emotional distress by claiming a family member is involved, pushing victims to act quickly.
Use of Technology to Mask Location	Scammers use VPNs or virtual phone numbers to disguise their location and prevent verification of the call’s authenticity.
Impersonation of Known Entities	Fraudsters may impersonate family members or friends involved in the alleged legal issue to make the scam feel more personal.

CONCERNS RELATED TO DIGITAL ARREST:

1. Financial Losses: Victims often suffer severe financial setbacks, with the funds being virtually impossible to recover. Scammers usually demand payment through hard-to-trace methods such as cryptocurrency, gift cards, or wire transfers, making it difficult for authorities to track the transactions.

2. Emotional and Psychological Distress: The emotional toll on victims can be significant. The scammers use high-pressure tactics, threatening the victim with consequences such as jail time, asset seizures, or deportation. This can cause extreme anxiety, stress, and long-term psychological impact on the individual.

3. Identity Theft and Data Exploitation: Personal information obtained during the scam can be used for identity theft. Scammers might open bank accounts, take out loans, or apply for credit cards in the victim’s name, leading to further financial harm and long-term damage to their credit reputation.

4. The Role of AI in Scams: The increasing use of artificial intelligence, such as deepfake technology and voice modulation, is making it more challenging to detect and expose digital arrest scams. These technologies allow scammers to convincingly impersonate authority figures, making the scams more difficult to identify.

5. Challenges in Tracing and Prosecution: Digital arrest scams often originate from international locations, complicating efforts by law enforcement to track down the perpetrators. The global nature of these crimes makes it harder to pursue legal action and hold scammers accountable.

GOVT. INITIATIVES TO AVOID SUCH FRAUD:

1. Citizen Financial Cyber Fraud Reporting and Management System: A system to report financial frauds immediately

2. Indian Cybercrime Coordination Centre (I4C): The Indian Cybercrime Coordination Centre (I4C), part of the cyber and information security division of the Union Ministry of Home Affairs, is dedicated to addressing rising cybercrime. Between January and April 2024, I4C recorded Rs 120.30 crore in losses by Indians due to digital arrest scams.

3. Aadhaar Authentication Safeguards: The Unique Identification Authority of India (UIDAI) has introduced several security measures to prevent Aadhaar-related fraud. These measures include biometric authentication, two-factor authentication, and guidelines that prohibit the sharing of Aadhaar details over calls or unverified websites.

4. Formation of Cybercrime Cells: State and central law enforcement agencies have established cybercrime cells that specialize in tackling online fraud. These cells focus on investigating digital crimes, including phishing, identity theft, and digital arrest scams, and work with other agencies to track down perpetrators.

5. Digital Literacy and Security Programs: The government promotes digital literacy programs like the Pradhan Mantri Gramin Digital Saksharta Abhiyan (PMGDISHA) to teach people, especially in rural areas, about safe online practices. These programs include educating citizens on how to spot scams, protect personal information, and avoid sharing sensitive details over phone calls or online.

6. Public Awareness of Fake Calls and Scams: Government bodies like the Ministry of Electronics and Information Technology (MeitY) and the National Security Council Secretariat often issue advisories to alert the public about the latest scams, including digital arrest frauds. These advisories help citizens understand how to verify the authenticity of official calls and prevent falling victim to scams.

7. Chakshu: A platform to report suspicious communication, such as requests for bank account details, KYC updates, or SIM cards

HOW TO AVOID BECOMING A VICTIM OF A DIGITAL ARREST SCAM?

1. Be skeptical of calls from unknown officials claiming you are in trouble. Real law enforcement agencies will never ask for payments or bank details over the phone.
2. Don’t succumb to pressure tactics. Scammers often create a false sense of urgency to get you to act quickly.
3. Verify their identity if you suspect a scam. Contact the agency they claim to represent directly to confirm their legitimacy.
4. Stay calm, and don’t panic. Avoid making rash decisions during the call.
5. Do not share sensitive information, including personal or financial details, over phone calls or video chats with unknown contacts.
6. Be aware that government agencies don’t use platforms like WhatsApp or Skype for official communication.

CONCLUSION:

Digital arrest scams are a growing threat, exploiting people's fears and causing financial and emotional distress. While the government has taken significant steps, such as launching the Indian Cybercrime Coordination Centre (I4C), raising awareness, and implementing security measures like Aadhaar safeguards, the increasing use of advanced technology by fraudsters presents new challenges. Public awareness and digital literacy are key to preventing such scams. Strengthening cybersecurity, enhancing law enforcement capabilities, and encouraging vigilance among citizens are essential to combating these threats and ensuring a safer digital environment.

PRELIMS QUESTION:

Q. Which Indian government initiative focuses on reporting cyber frauds and helps manage financial scams, including digital arrest frauds?

A. Digital India Campaign
b. Indian Cybercrime Coordination Centre (I4C)
C. Cyber Suraksha Yojana
D. National Cybersecurity Strategy
Answer: B

MAINS QUESTION:

Q."Digital arrest scams are a growing concern in India, leading to significant financial and emotional distress for victims. Critically analyze the role of technology in facilitating such scams and the challenges faced by law enforcement in tackling them."
(250 words, 15 marks)

Ritik singh