# A New Frontier in Cybercrime and Its Repercussions: Digital Arrest

**Dr. Archana Singh Parmar[1], Dr Monika Sharma[2]**

[1]Assistant Professor, Technological Institute of Textile and Sciences, Bhiwani, Haryana
[2]Associate Professor, Technological Institute of Textile and Sciences, Bhiwani, Hayana

**Abstract:**
Cyber risks are also changing in today's increasingly connected digital world, and they are now superpowered by AI and ML's potential. Additionally, this allows scammers to increase their chances of success in different schemes. Even though the term "digital arrest" is frequently used in relation to numerous fraudulent operations, the number of people falling victim to these scams is continually increasing. In a "Digital Arrest" scam, scammers use video calls to pose as law authorities and threaten fictitious arrests in order to demand money. In this paper all the aspect of this digital arrest scam would be discussed, the way this scam operate and what challenges are being faced and how we can protect ourself from this scam

**Keywords:** Digital Arrest, Cyber Crime, Cyber Attack

## 1. Introduction

Due to the rise in cybercrimes and the requirement for modern law enforcement tools to cope with online criminals, the idea of "digital arrests" has drawn attention in an increasingly digital environment.

Because to the COVID-19 pandemic, which forced a large percentage of the world's population online, there has been an increase in cyber fraud. A scammer acting as an executive of a courier service, like FedEx, would inform the victim that a shipment under their name was stuck at the airport because it contained something illegal. This is how digital arrest scams, a variation of courier scams, gained popularity in India in early 2023.

They would set them in contact with a fake cyber cell or customs official. In order to escape arrest, the target would then be instructed to transfer funds to a surveillance bank account that is reportedly authorized by the RBI. The smart twist is that the money would be returned to the target after their identification has been confirmed.

In India, security risks are evolving fast and digital arrest frauds are becoming a major worry. These complex techniques are catching even well-educated people unaware surprise. Newspapers are filled with "digital arrests" every day. Cybercriminals posing as law enforcement officials threaten victims with "digital arrests," forcing them to pay large sums of money to avoid being arrested. The urgency of the issue is demonstrated by the necessity for Prime Minister Narendra Modi to warn the public about "digital arrest" schemes.

### 1.1 Digital arrest: what is it?

There is nothing called digital arrest in the law. Cybercriminals pretend as law enforcement officers or government organizations, including the State police, CBI, Enforcement Directorate, and Narcotics

Bureau, in digital arrest schemes. They even mimic judge to make people in their claims. The cops make calls to unsuspecting people, alerting them that a case has been launched against them after a consignment with drugs was intercepted at an airport. They even support their claims with a fake police station.

### 1.2 What is the way they operate?

Typically, cybercriminals make contact by phone or occasionally via email. A video call from a variety of locations, such as a "airport," the police station, or even a court, will follow one or two voice calls. When their calls are answered, they use their "DP" (display picture), which is a collection of photos of judges, attorneys, and police officers taken from their social media accounts. Unbelieving victims would answer the phones when they saw the DPs of police officers. People think they are in a vast soup and that something dangerous is happening because of the large number of people involved in the racket.

They might use email or messaging apps to offer false arrest warrants, court notifications, or official-looking documents.

### 1.3 What statements are made by these scammers?

Usually, victims are accused of major crimes like drug trafficking, money laundering, or cybercrime by cybercriminals. They might claim that "your son is found to be in unlawful activity," "a consignment with drugs addressed to you has been intercepted," or "a phone number associated with your Aadhar number is involved in sending abusive messages or making threatening calls." To give their charges more weight, they can even create up evidence.

### 1.4 Why do they typically succeed?

Many people are more likely to believe the charges and threats of scammers because they are not familiar with the usual operational procedures of law enforcement authorities. Victims are more likely to comply with the demands of fraudsters when they are threatened with probable arrest because it causes extreme anxiety and terror.

Another factor at play in this case is the social shame associated with police cases and criminal accusations. Cybercriminals take advantage of this anxiety over reputational harm, particularly the possible effects on family members' reputations and the chances for children's futures. Because of this concern, victims might choose to disregard possible media attention and rejection by society for the sake of a quick, but illegal, resolution. Scammers instill a sense of urgency in their victims, forcing them to decide right away without seeking advice from others or verifying the facts. Because of this, victims lack the capacity to make decisions or seek relief.

## 2. How should you respond to threats of “digital arrest”?

The most crucial thing is to remain calm and not lose your cool. Don't provide any personal information, including PAN card or Aadhaar details. Don't send any cash. Inform the local police and cybercrime authorities about the event. Reputable law enforcement organizations will never call and demand money or threaten to arrest someone without following the correct legal procedures.

### 2.1 What are the best self-preservation techniques?

The key is prevention. Find out about typical scam techniques and tell your loved ones about them. Because they can be faked or altered, never utilize the names and DPs that are shown on caller ID services. Always use official means to independently confirm the caller's identity. Even if the caller seems genuine, you should not be afraid to request identification and supporting evidence .

You ought to stay away from making quick choices and maintain calmness. End the call if you feel under pressure. Never send money without initially authenticating the request and the receiver. Use two-step verification and create strong passwords to protect your bank accounts.

**3.1 Common types of crimes leading to digital arrests include:**

**Cyberstalking and Online Harassment**: When people are harassed, stalked, or threatened online.

**Hacking:** Unauthorized entry into network or computer system.

**Phishing:** Phishing is the fraudulent practice of posing as a reliable organization in order to get private information, such as passwords or bank account information.

**Cyberterrorism**: The use of online attacks to propagate misinformation or inflict harm on vital systems.

Financial fraud includes online crimes such as identity theft, credit card theft, and Ponzi scheme.

Pornography and child exploitation: the production or dissemination of unlawful material involving children.

Fake news: The spread of misleading information or inflammatory material that provokes violence or social disturbance is known as hate speech and fake news.

**4.1 Technology Behind Digital Arrests**

Digital arrests often involve sophisticated technology and forensic techniques:

Digital Forensics: To gather, examine, and store electronic evidence, law enforcement organizations depend on digital forensics. This can involve decrypting communications on encrypted platforms, tracing IP addresses, and recovering erased files.

Online Surveillance: Tools like IP tracking, GPS tracking, and real-time online activity monitoring help authorities with keeping watch on suspected criminals.

Social Media Monitoring: Websites such as Facebook, Instagram, and Twitter have developed into hubs for illicit activity ranging from financial fraud to hate speech. To keep an eye on questionable conduct on social media in real time, law enforcement organizations employ machine learning and artificial intelligence systems.

Data Interception: The IT Act and national security regulations allow authorities to intercept emails, social media posts, and communications on mobile networks. This technology is especially helpful in situations involving organized crime or cyberterrorism.

Social Media Monitoring: Facebook and Blockchain Tracking: As digital currencies grow more and more popular, blockchain technology is becoming essential to digital arrests. Blockchain analytics technologies are used by law enforcement to monitor and trace illegal bitcoin transactions in order to catch criminals.

**4.2 How do victims get sucked into the scam and end up losing money?**

By researching potential victims, scammers are able to execute digital arrest schemes. In certain instances, they may also be able to obtain the victim's personal data, including their online purchase orders, which may have come from compromised datasets offered for sale on the dark web.

The scammers appear more trustworthy, for example, if they tell the victim about their previous internet transactions. The victim is made to believe that only law enforcement or the government itself could possibly be aware of all these things.

Fraudsters have purportedly prompted victims to download some video calling application in order to initiate a video conference. The scammers on the call are dressed in police uniforms that seem official. Another tool scammers use to look authentic are official-looking letters and identification documents.

In India, digital crimes have increased in parallel with the country's explosive growth in internet usage and digital financial services. In response to this new environment, the Indian government and law enforcement organizations are creating policies and procedures that enable efficient digital arrests and prosecutions.

### 5. Steps You Must Take If You Become a Victim of Digital Arrest

Digital arrest can have serious and perhaps debilitating consequences. Unauthorized transactions may cause victims to suffer immediate financial losses.

Several actions are necessary to recover from these accidents, including**:**

- **Reporting the Fraud to Your Bank:** This is the first action you need to take in order to start the process of reversing unauthorized transactions and freeze accounts to stop more losses.
- **Making a Report to the Police:** For a formal investigation, report the offense to the police. In India, victims can also report instances online at www.cybercrime.gov.in or call the national cybercrime helpline (1930). The SacharSathi Portal, which provides case tracking, is another way to lodge a complaint with the Cyber Crime Cell.
- **Controlling the Impact on Credit Score:** Identity theft and unauthorized purchases can have a detrimental effect on your credit score. Working with creditors, disputing inaccuracies, and contacting credit bureaus are all necessary to resolve issue.
- **Protecting Your Devices and Accounts:** Make your passwords stronger, turn on two-factor authentication, and analyze your devices for security flaws.

The emotional toll of digital arrest can also be challenging, as victims often feel anxious about using online platforms. Acting quickly and following these steps can limit the damage and begin the recovery process.

### 6. How to Protect Yourself from Digital Arrest

To safeguard yourself from cybercrimes, consider following these practical steps:

- **Use Strong, Unique Passwords:** Avoid simple passwords and don't reuse them across sites. Include letters, numbers, and special characters for additional security.
- **Enable Two-Factor Authentication (2FA):** 2FA provides an extra layer of security by requiring two forms of verification, making it harder for scammers to access your accounts.
- **Be Cautious with Links and Emails:** Verify the sender before clicking on links or downloading attachments in emails. Scammers often use these to distribute malware or direct you to phishing sites.
- **Keep Devices Updated:** Regularly update your software, apps, and antivirus programs to defend against the latest cyber threats.
- **Monitor Bank Statements:** Regularly check account activity for any unauthorised transactions and report them immediately.
- **Use Trusted Wi-Fi Networks:** Avoid online banking on public Wi-Fi and consider using a VPN for secure browsing.

### 7. The challenges

- Absence of knowledge: A lot of victims are gullible and do not know that digital arrest frauds exist.
- International components are frequently present in these frauds, which makes it challenging for law authorities to find and apprehend the perpetrators.
- Use of deepfake technology: To make it more difficult for victims to spot fraud, scammers pose as officials using advanced technologies.
- India's cyber laws are continuously developing, and they are not always effective in combating emerging types of cybercrime.

## 8. Way forward:

- Strengthen cybercrime laws: To keep up with the quickly changing technological landscape, cyber laws must be amended.
- Public awareness efforts: To inform the public against digital arrest scams, the government needs to step up its awareness initiatives.
- Boost technology and law enforcement: To counteract cross-border cybercrimes, invest in anti-deepfake technologies and expand collaboration with international organizations.
- Working together with financial institutions: Collaborate with banks to keep an eye on questionable transactions connected to these frauds.

## 9. Conclusion:

Indian people's financial and emotional health are seriously threatened by digital arrest scams. Although public awareness efforts and government programs like I4C are positive steps, a multifaceted strategy including improved legislation, improved technology, and public education is necessary to stop this threat.

## 10. References:

1. https://www.drishtiias.com/daily-updates/daily-news-analysis/rising-digital-arrests
2. https://www.geeksforgeeks.org/what-is-digital-arrests/
3. https://xpertslegal.com/blog/understanding-digital-arrest-fraud-a-growing-menace-in-the-digital-age/
4. https://www.cyberpeace.org/resources/blogs/digital-arrest-fraud
5. https://blog.lukmaanias.com/2024/11/12/digital-arrest-scams-a-growing-cybercrime-threat/
6. https://www.rblbank.com/blog/banking/safe-banking/the-rise-of-digital-arrest#:~:text=%22Digital%20Arrest%22%20refers%20to%20an,presence%20is%20restricted%20or%20detained.