Swami Vivekananda Advanced Journal for Research and Studies
Online Copy of Document Available on: www.svajrs.com

ISSN:2584-105X **Pg. 205-208**

Digital Arrest Scam in India: Trending Cyber Crime in the Digital Era

Dr. Awadhesh Kumar
Buddha Law College, Gorakhpur
Assistant Professor

Accepted: 22/08/2025
Published: 29/08/2025 ***DOI: http://doi.org/10.5281/zenodo.16992454***

Abstract

The rapid development of information and digital technologies have changed the nature of traditional crime and given rise to cyber-crimes cases. Digital arrest scams, in which cyber-criminals impersonate law enforcement agencies to demand money from victims, have grown to be a significant cyber-crime issue in India. These scams usually involve advanced technique, like whatsapp and skype video calls from fake government places, to coerce victims into delivering money on the pretence of evading legal action. Due to the rapid digitisation of computer and technology and the lack of awareness regarding cyber-security, use of technology these types of cyber-frauds are now more prevalent in India. The Indian government has taken imitative like public awareness programs at time to time and restricting online communication channels in an effort to stop these digital arrest scams. The legal, moral, and technological ramifications of law enforcement in the digital era are the main focus of this research paper's exploration of the effect of "digital arrest scam". The Parliament has enacted the Information Technology Act 2000 in the year 2000. After 25 years of this Act, it is not so effective in today's context.

Keywords: *Digital Arrest Scam, Cybercrime, Cyberfraud, IT Act 2000, Technology*

Introduction

Cyber-crimes have spread beyond geographical borders due to the increased of the internet services and digital connectivity, 'digital arrests scams' are a crucial component of contemporary law enforcement agencies. Hacking, identity theft, online financial fraud, cyber-stalking, and online terrorism are examples of digital cyber-crimes. The term "digital arrest" describes the use of computer with the connection of internet, AI-powered monitoring, and cyber-security measures to apprehend and prosecute hackers.

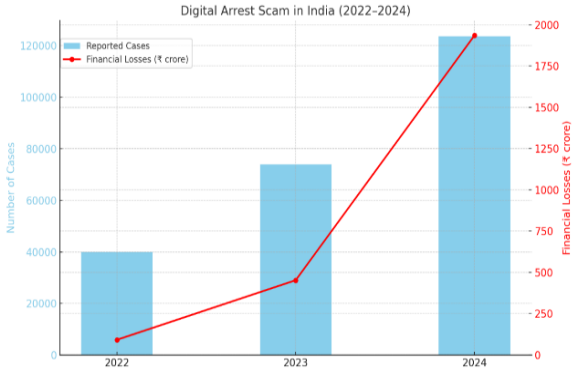
"Digital arrest" is a term used in India to describe a sophisticated cyber-crime in which scammers pose as government or law enforcement officials in order to extort money from the victim. These scammers frequently use skype video calls, presenting phoney official settings, to accuse victims of involvement in illegal activities like drug trafficking or money laundering cases and then force victims to transfer money in order to avoid false legal consequences.

In recent years, there has been a large number of such digital arrest scams. India reported losses from cyber fraud of almost ₹11,333 crore in the first 9 months of 2024 alone.[1] In the first 4 months of 2024, "the Indian Cyber Crime Coordination Centre (I4C)" received over 740,000 cybercrime complaints, with an average of almost 7,000 complaints every day.[2]

Numerous high-profile incidences have brought attention to the seriousness of digital arrest scams. For example, a businessman was defrauded of $830,000 after being summoned to a fake online Supreme Court hearing, where person impersonating top judicial officials coerced him into transferring funds.[3]

In another case, a marketing consultant lost ₹6 crore to scammers posing as law enforcement officers.[4] An 86 years old-woman from Mumbai city lost more than 20 crore Rs. In a digital arrest fraud.[5] On "the National Cybercrime Reporting Portal (NCRP)" in the last 3 years, which disclosed 39,925 such incidents being reported in the year 2022 with a total defrauded amount of Rs 91.1 crore.

"In the year 2024, the number of cases nearly tripled to 1,23,672 with the total defrauded amount described on the portal increasing by a stunning twenty-one times to Rs 19,35.51 crore, the data disclosed. According to the statistics, within 2 months of the year 2025, 17,718 cases with a total deceived amount of Rs 210.21 crore have been reported till February 28."[6]



Digital Arrest Scam cases and Financial Losses in India from 2022 to 2024:

- **The blue bars represent the number of reported scam cases.**
- **The red line shows the corresponding financial losses (in ₹ crore).**

Digital arrest scams have become increasingly prevalent in India, with several notable cases highlighting the sophistication and impact of these fraudulent activities –

1. High-Profile Businessman Defrauded

In a particularly elaborate scheme, S.P. Oswal, chairman of the "Vardhman Group" was cheated into transferring $830,000. Fraudsters, posing as federal investigators, summoned him to a fake

[1] https://indianexpress.com/article/india/cyber-scams-india-pm-modi-9692771/ (last visited on 10 May 2025).
[2] https://www.statista.com/statistics/1499739/india-cyber-crime-cases-reported-to-i4c/ (last visited on 11 May 2025).
[3] https://www.reuters.com/world/india/indian-textile-baron-duped-with-fake-supreme-court-hearing-document-shows-2024-09-30/ (last visited on 22 May 2025).
[4] https://economictimes.indiatimes.com/news/india/2024-was-the-year-digital-arrest-scams-became-mainstream-one-persons-fightback-holds-a-mirror-to-the-system/articleshow/116947220.cms from=mdr (last visited on 23 May 2025).
[5] https://www.thehindu.com/news/cities/mumbai/elderly-woman-loses-20-crore-to-digital-arrest-fraud-3-held/article69353437.ece (last visited on 09 June 2025).
[6] https://www.business-standard.com/india-news/digital-arrests-cyber-crimes-tripled-during-2022-24-govt-tells-parliament-125031200978_1.html (last visited on 09 June 2025).

online Supreme Court hearing where an individual impersonating Chief Justice D.Y. Chandrachud ordered the fund transfer to a "secret supervision account". This case underscores the advanced tactics employed by scammers, including the creation of counterfeit legal proceedings.[7]

2. Significant Financial Losses Reported

A marketing consultant named Vidya fell victim to a digital arrest scam, resulting in a loss of ₹6 crore. Through persistent efforts, she managed to recover approximately ₹60 lakh, highlighting the challenges victims face in recouping their losses. This incident emphasizes the substantial financial impact these scams can have on individuals.[8]

3. Surge in Reported Cases

Data indicates a sharp rise in digital arrest scams, with over 92,323 cases reported between Jan. and Nov. 2024, as per the "Indian Cyber Crime Coordination Centre (I4C)". This surge reflects the growing prevalence of such scams across the country.[9]

4. Law Enforcement Actions

Delhi Police reported about 40 fraud cases with sums exceeding ₹50 lakhs, mostly in 2024, in response to the growing menace. Government have started awareness programs and educational programs in residential communities and educational institutions to counter this trend.[10]

II. CHALLENGES OF DIGITAL ARREST SCAM

There are many challenges which are as follows:

1. Exploitation of Rapid Digitalization

India's swift adoption of digital technologies has outpaced public awareness of cybersecurity measures. Scammers exploit this gap, leveraging advanced techniques to deceive individuals unfamiliar with potential online threats. The disparity between technological advancement and user education creates a fertile ground for such frauds.[11]

2. Sophistication of Scam Operations

Fraudsters employ elaborate schemes, including impersonating high-ranking officials and staging fake legal proceedings. A notable case involved a businessman who was defrauded of $830,000 after being summoned to a counterfeit online Supreme Court hearing, where fraudsters impersonated himself judicial authorities. It is very difficult for victims to determine genuineness because of the complexity of these activities.

3. Psychological Manipulation

Fraudsters use haste and intimidation to force victims to comply. They in still fear by threatening arrest and legal action, which leads victim to behave rashly without checking the veracity of the charges. A powerful tool in the fraudster's toolbox is this psychological pressure.

4. Jurisdictional and Enforcement Hurdles

For the law enforcement agencies, the global aspect of 'digital arrest scams' presents serious difficulties. Digital arrest scam may be committed by outside any country. Cyber fraudster has committed such crime from India and also outside India. Cross-border coordination calls for significant resources and frequently absent legal frameworks.

5. Resource Limitations

Because of systemic problems in banking and law enforcement, many victims have trouble getting their money back. A case study emphasised the systemic difficulties in tracking and recovering cheated money by focussing on a victim who, despite diligent attempts, was only able to collect a small portion of the ₹6 crore that she had lost.

6. Public Awareness Deficit

A large percentage of the population is still ignorant of digital arrest scams, despite government warnings, which leaves them vulnerable to fraud because they are ill-equipped to identify or react to such threats. To close this knowledge gap, ongoing public education is crucial.

---

[7] https://www.reuters.com/world/india/indian-textile-baron-duped-with-fake-supreme-court-hearing-document-shows-2024-09-30/ (last visited on 12 June 2025).

[8] https://economictimes.indiatimes.com/news/india/2024-was-the-year-digital-arrest-scams-became-mainstream-one-persons-fightback-holds-a-mirror-to-the-system/articleshow/116947220.cms from=mdr (last visited on 8 June 2025).

[9] https://indianexpress.com/article/technology/tech-news-technology/digital-arrest-scams-why-many-are-falling-for-them-9706065/ (last visited on 5 June 2025).

[10] https://www.hindustantimes.com/htcity/htcity-delhi-junction/digital-arrest-scams-all-you-need-to-know-101736409777645.html (last visited on 1 June 2025).

[11] https://economictimes.indiatimes.com/news/india/indias-digital-arrest-scammers-stealing-savings/articleshow/117386870.cms from=mdr (last visited on 25 May 2025).

III. LEGAL PROVISION TO CONTROL DIGITAL ARREST SCAM

The Relevant Legal Frameworks Include:

1. **Bharatiya Nyaya Sanhita 2023**

- Section 319: Cheating by Personation

This section penalizes individuals who deceive others by pretending to be someone else. Offenders will face imprisonment for up to 3 years, a fine, or both.

- Section 318: Cheating and Dishonestly Inducing Delivery of Property

This provision addresses cheating that leads to the "delivery of property" or "valuable security". Convicted person can be sentenced to imprisonment for up to 7 years and may also be liable to a fine.

- Sections 336 and 340: Forgery and Forgery for Purpose of Cheating

These sections deal with creating false documents with the intent to commit fraud. Punishments include imprisonment and fines, with Section 336 Sub Section 2, 3 and 4 specifically focusing on forgery intended for cheating.

2. Information Technology (IT) Act, 2000

- Section 66C: Identity Theft

This section penalizes the fraudulent or dishonest use of another person's electronic-signature, password, or other exclusive identification features. Offenders may face imprisonment of up to 3 years and a fine of up to ₹1 lakh.

- Section 66D: Cheating by Personation Using Computer Resources

This provision addresses cheating by personation through any communication device or computer resource. Convicted individuals can face imprisonment of up to 3 years and a fine of up to ₹1 lakh.

3. Section 111 of BNS 2023: Organised Crimes

Organised crime encompasses any continuing unlawful activity such as Cyber crimes shall be punished minimum 5 years, up to life imprisonment, plus a minimum of fine of ₹ 5 lakh.

4. Criminal Procedure and Enforcement

Law enforcement agencies in India are empowered to investigate and prosecute offenses under these provisions. The Ministry of Home Affairs has issued advisories to States and Union Territories to enhance awareness and enforcement against such cybercrimes. Additionally, the Indian Cyber Crime Coordination Centre (I4C) provides a platform for citizens to report cybercrimes, facilitating prompt action.

While these legal provisions offer a framework to combat digital arrest scams, continuous efforts in public awareness, capacity building of law enforcement, and international cooperation are essential to effectively address the evolving nature of such cyber threats.

IV. CONCLUSION

There are number of cases of Digital Arrest Scams in India. Such Scams have been increased in India as per data published by Indian Cyber Crime Coordination Centre. This crime can be controlled by the multidimensional approach in which all the stakeholder will participate. Government, Businesses, and individuals will participate to make a strength law and legal framework to control such crimes. Legal framework like I T Act 2000 is 25 years old Act which is not very effective in today's time. Punishment provided in this Act is not so effective to create fear in the minds of cyber criminals. Therefore, I T Act 2000 will be review again by the Parliamentary committee.

Again, such crime can be committed outside Country. It is borderless crime. That is why All the Country must come together for making a Internation treaty. Internation treaty will provide power to law enforcement agencies to make investigation among the countries. Awareness program should be conducted at time to time because people are not aware of such type of cybercrime.

REFERENCES

3. The Information Technology Act 2000
4. The Bharatiya Nyaya Sanhita 2023
5. The Bharatiya Nagarik Suraksha Sanhita 2023
6. http:// economictimes.indiatimes.com/
7. http://www.the hindu.com/
8. Reports of Indian Cybercrime Coordination Centre

****