International Journal of Law Research, Education and Social Sciences

Open Access Journal – Copyright © 2026 – ISSN 3048-7501
Editor-in-Chief – Prof. (Dr.) Vageshwari Deswal; Publisher – Sakshi Batham

Digital Arrest Scams: An Emerging Cyber Threat and the Adequacy of India's Legal Framework

Jaya Bharti[a]

[a]Central University of South Bihar, Gaya, India

Received 23 May 2026; Accepted 22 June 2026; Published 25 June 2026

In light of the rapid advances that are taking place in digital technology, the world today sees cybercrimes becoming increasingly sophisticated and common. A relatively new type of cybercrime is the digital arrest scam. In these types of schemes, criminals will impersonate members of the police force, CBI, customs, and any other governmental department and accuse the individuals they approach of engaging in illegal activities. Using tactics of fear, intimidation, and manipulation, the victims are usually forced to make significant payments to ensure that no legal action is taken against them. This article seeks to investigate the modus operandi of digital arrests and assess the adequacy of current Indian legislation in dealing with this form of cyber fraud. In particular, the pertinent laws found in the Bharatiya Nyaya Sanhita, 2023, as well as the provisions of the Information Technology Act, 2000, will be discussed. Finally, it evaluates the need for stronger legal measures, improved enforcement, and greater consumer awareness to effectively tackle digital arrest scams and protect citizens in the digital age.

Keywords: *digital arrest scam, cybercrime, cyber fraud, consumer protection, cyber law.*

INTRODUCTION

Digital transformation has revolutionised almost all aspects of contemporary society. Whether it is banking, transactions, e-governance, or communication, there have been tremendous improvements through the use of technology. In India, there has been immense growth through Digital India, extensive penetration of mobile phones, and adoption of financial services online. But technology is not only a boon but has also presented itself as a platform for criminals to target their victims. In addition to that, cybercrimes have become complex, and individuals have become frequent targets. According to the government data, the financial scams have caused loss of millions of rupees, and cases have increased by almost three times from 2022 to 2024, from 41,000 to 1,23,0001.[1]

Among the numerous cybercrime threats that have emerged recently, one of the most frightening is known as the 'digital arrest scam.' The perpetrators of such crimes pose themselves to be law enforcement agents like policemen, officers from the Central Bureau of Investigation (CBI), Enforcement Directorate (ED), customs officials, or representatives of other government organisations. Individuals are then informed that they stand accused of various criminal acts like money laundering, drug dealing, tax fraud, or financial crimes. To add extra fear and urgency to their demands, they arrange video conferencing, show fake documentation, and make threats of arrest and imprisonment to the victims. Consequently, under great mental duress, victims are asked to make payments into specified bank accounts for so-called verification, investigation or security purposes.

The difference between the digital arrest scam and traditional cybercrime lies in its effective exploitation of the elements of authority, threats, and psychological tactics. The scam goes beyond just technical deceit and manipulates the victim's trust in public offices and fears concerning the law. Consequently, these types of fraud have successfully deceived educated and well-off victims as well. Due to advances in digital communication technology, impersonation cases have drastically improved in nature and technique in India. Previously, impersonation crimes were relatively restricted to being conducted in the presence of the intended person or dealing with the individual directly. An impersonation, however, has emerged to become an extremely elaborate form of cybercrime in this modern era due to developments in mobile

[1] *Annual Report 2022-2023* (Reserve Bank of India 2023)

network services, internet communications, and electronic banking systems. Fake phone numbers, mass messaging capabilities, and Voice over Internet Protocol are some common techniques of impersonation in telecom services. Offenders often take advantage of caller ID spoofing of similar-looking numbers of the genuine service or government organisation. They either call or send messages claiming the deactivation of an account, an incomplete KYC process, and other dubious activities to make victims provide their OTPs or other confidential information. This type of fraud also leverages the trust consumers have in telecom infrastructure as a key means of communication, just as banking-related impersonation frauds have surged in tandem with the growth of digital payment processing.[2] The rising trend of this crime has caused grave concerns about the security and well-being of the individuals, as well as the cybersecurity, consumer protection laws, and adequacy of the existing legal means to address this emerging threat.

There is no provision to deal with the digital arrest scams as such; however, since it is a case of cybercrime, some provisions under the Bharatiya Nyaya Sanhita, 2023 (BNS) can be applied to investigate this crime. The country has an elaborate legal system to combat cybercrimes and other crimes against women through statutes like the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, etc. Nonetheless, there are legal challenges that need to be considered in this context. Problems associated with jurisdiction, the international nature of criminal gangs, untraceability of criminals, lack of evidence, and late reporting may prove to be impediments in investigating this type of crime. Another aspect is that the existence of such crimes may raise a question about the sufficiency of existing legislation to handle the emerging trend of crimes.

In this scenario, this paper aims to analyse the concept and working mechanism of digital arrest scams, along with evaluating the efficacy of laws in place in India for dealing with this scam. Furthermore, the paper will also discuss the issues related to the enforcement of laws against these digital scams, as well as the need for increased consumer protection laws in this regard.

[2] Parth Malhotra, 'DIGITAL ARREST AND ONLINE IMPERSONATION FRAUDS: A JURIDICAL EXAMINATION OF CHANGING DIMENSIONS OF CYBER-CRIME IN INDIA' (2026) 6(2) Indian Journal of Integrated Research in Law <https://ijirl.com/wp-content/uploads/2026/05/175.-DIGITAL-ARREST-AND-ONLINE-IMPERSONATION-FRAUDS-A-JURIDICAL-EXAMINATION-OF-CHANGING-DIMENSIONS-OF-CYBER-CRIME-IN-INDIA.pdf> accessed 16 May 2026

UNDERSTANDING DIGITAL ARREST SCAMS: MODUS OPERANDI AND IMPACT

Digital arrest scams represent a new kind of cybercrime that involves the use of both technology and psychology. 'Digital arrest' is not recognised in any form of Indian law because it simply refers to the creation of an impression that a particular individual is under criminal investigation or virtual detention by various law enforcement agencies. It involves intimidation through impersonation and misguiding of the victims with the sole aim of making them give away their personal information or money. According to the Indian Cybercrime Coordination Centre, Ministry of Home Affairs ("IC4"), there have been multiple case reports of people having lost around INR 120.30 crore due to digital arrest scams in the first quarter of 2024 alone.[3] According to data reported through the National Cyber Crime Reporting Portal (NCRP), incidents of digital arrest scams increased from approximately 39,925 cases in 2022 to 1,23,672 cases in 2024, while reported financial losses escalated from nearly ₹91 crore to around ₹1,935 crore during the same period. Recent Ministry of Home Affairs and Indian Cyber Crime Coordination Centre (I4C) reports further indicate that Indians lost more than ₹22,845 crore to cyber fraud in 2024 and approximately ₹22,495 crore in 2025, with digital arrest scams accounting for a substantial share of psychologically and financially motivated cybercrimes. Karnataka alone recorded losses exceeding ₹468 crore between 2023 and early 2026, demonstrating the alarming scale of victimisation despite increased awareness initiatives. As per the report of the World Cybercrime Index, India is ranked 10th among nations facing alarming cyberattacks and cybercrime-related cases.[4]

Digital arrest is a swindle created to blackmail victims through threats, lies, and intimidation. Cyber criminals assume the identity of law enforcement agencies, intimidating victims with threats such as arrest warrants, frozen bank accounts, and revoked passports to compel victims to pay a 'fine/security deposit.'

The fraud usually starts off with a telephone call, and at first glance, there might not be anything threatening about the call since the scammer may make claims ranging from a mere parcel

[3] 'Indian lost Rs 120 crore in digital arrest frauds in January-April 2024' *The Indian Express* (28 October 2024) <https://indianexpress.com/article/india/indians-lost-rs-120-crore-in-digital-arrest-frauds-in-january-april-2024-9641952/> accessed 16 May 2026

[4] 'Digital arrests, cybercrimes tripled during 2022-24; over ₹1935 crore defrauded : Govt' *The Economic Times* (13 March 2025) <https://government.economictimes.indiatimes.com/news/secure-india/digital-arrests-cybercrimes-tripled-during-2022-24-over-1935-crore-defrauded-govt/118959050> accessed 16 May 2026

delivery inquiry to a need for the victim's KYC authentication. However, what follows next are threats to ensure the victim panics by accusing him/her of involvement in criminal activities such as money laundering, cybercrime, and drug trafficking. This is done using manipulated videos, falsified documents, and spoof phone numbers.[5]

MODUS OPERANDI OF DIGITAL ARREST SCAMS

Arrest scams by digital means follow a well-thought-out method involving aspects of psychology, impersonation, technology, and financial exploitation. Though each case may have its variations, the underlying process remains more or less the same, with the objective of causing fear in the minds of the victims and forcing them to act quickly. In most cases, the scheme starts with a call, message, or other form of communication from someone pretending to be a member of the law enforcement authorities, Customs, CBI, ED, or any other governmental authority. This person tells the victim that their personal identification papers, bank accounts, cell phone numbers, or packages have been identified to be used for illegal purposes such as money laundering, drug smuggling, cybercrimes, or other financial crimes. Fear is instilled in the mind of the victim and made to believe that they can be arrested, their bank account frozen, or charged with a crime if they do not cooperate.

In order to create credibility, the scammer will often have some personal details about the individual that could be gained through a data breach or via social networking websites. They will give fabricated numbers for court cases, forge documents, fake arrest warrants, and even counterfeit identity cards. More often than not, the individual becomes part of a relayed process where each caller acts on behalf of another government agency.

A distinctive feature of these scams is the deliberate use of psychological manipulation and social engineering techniques.[6] The victims are made to stay in constant contact via videophone calls and are told that they are under "digital arrest" or online surveillance. Victims are often warned not to contact their families, friends, or lawyers since such an action might compromise the

[5] Major Sadhna Singh, 'Digital Arrest: The Modern-Day Cyber Scam' (*NITI Aayog*, 16 April 2026) <https://www.niti.gov.in/node/1642> accessed 16 May 2026

[6] Disha, 'A Critical Study of Digital Arrest Scams and the Erosion of Online Trust: A Socio-Legal Analysis of Cybercrime Regulation in the AI Era' (2026) 5(3) International Journal of Human Rights Law Review <https://humanrightlawreview.in/journal/a-critical-study-of-digital-arrest-scams-and-the-erosion-of-online-trust-a-socio-legal-analysis-of-cybercrime-regulation-in-the-ai-era/> accessed 16 May 2026

investigation. The constant isolation of the victims serves as psychological trickery to instil fear and decrease the chances of the victim exposing the scam. The scammers continue applying pressure on the victims for hours and sometimes even days. Once the victim is emotionally compromised, the fraudsters move on to the next step, i.e. blackmailing or stealing confidential data from them. The victim is asked to save themselves from any arrest or criminal charges by paying a fine amount, which is generally refundable after the process of digital settlement. Various IDs are shared, such as UPI ID or bank details, to facilitate these transactions and the victim is asked to make instant payments. In certain situations, the transactions may be repeated for a period of more than a few hours. At times, the fraudsters also ask for sensitive information such as passwords for banks or Aadhar card information and one-time passcodes. The victims are convinced of the return of their amount post the completion of the investigations. But once the transaction takes place, the fraudsters vanish.[7]

PSYCHOLOGICAL MANIPULATION AS A TOOL OF FRAUD

While conventional cybercrime exploits technology weaknesses, digital arrest scams involve manipulating psychological behaviour. Scammers always create a situation of panic and urgency. Ordinary people have little or no understanding of how criminal cases can be handled and are usually afraid to hear any criminal charges against themselves. The thought of being arrested, embarrassed, or having their reputations ruined, coupled with facing possible legal consequences, hampers their ability to make rational decisions.

To build on their manipulations, scammers utilise official language, wear uniforms, make video calls from places that look like offices, and quote various legal terms that most victims do not understand. Such tactics create a false sense of legitimacy and authority, increasing the likelihood of compliance.

IMPACT ON VICTIMS AND SOCIETY

In addition to financial losses, digital arrest scams have profound psychological effects on victims. Victims suffer from depression, anxiety, and emotional trauma following their experience. Many victims feel embarrassed, intimidated, and powerless once they realise that

[7] Uma, 'Unmasking digital arrest: An emerging threat to modern society in India' (2025) 11(5) International Journal of Law <https://www.lawjournals.org/assets/archives/2025/vol11issue5/11210.pdf> accessed 16 May 2026

they were scammed. In other instances, victims drain their finances, withdraw from investments, or incur debts to settle payments demanded by the criminals.

The effects on society are just as devastating as those on the victims. For starters, the prevalence of digital arrest scams threatens people's confidence in online banking, transactions, and communication platforms. Digital arrest scams also harm people's perception of legitimate law enforcement agencies, as criminals use the guise of being police officers in perpetrating these crimes. Additionally, digital arrest scams pose challenges to cybercrime investigation departments as scams become increasingly difficult to investigate and combat.

Overall, the prevalence of digital arrest scams presents a critical threat to cyber safety and security in the digital age.

EXISTING LEGAL FRAMEWORK IN INDIA

However, the growing trend of digital arrest scam crimes has brought to light the need for an effective legal regime that can help cope with new types of cybercrimes. While there is no specific definition or recognition of the offence known as 'digital arrest scams' in Indian law, several sections of both the criminal and cyber legislations provide sufficient basis for investigating and punishing individuals behind these frauds. In this regard, BNS, the IT Act, and other government regulations form the main legal framework to deal with such crimes.

BHARATIYA NYAYA SANHITA, 2023

There are no specific provisions for dealing with the digital arrest scams, although being a cybercrime, certain Provisions of Bhartiya Nyaya Sanhita, 2023 (BNS) can be considered while dealing with this scam.

Organised Crime:[8] In Bhartiya Nyaya Sanhita, 2023 (BNS), the concept of cybercrimes is included in the Organised Crime category. Cybercrimes may be performed either individually or as a syndicate with the help of intimidation and coercion in order to reap profits.

[8] Bhartiya Nyaya Sanhita 2023, s 111

Criminal Conspiracy:[9] Such fraud schemes generally include two or more fraudsters who masquerade as officials of some particular government authority or department. For example, the victim is called by one official who later contacts them through another official, claiming to be their superior. In this case, apart from causing terror among the victims, these fraudsters can easily convince them of their claims. Digital Arrest Scams, which constitute a recently emerging cybercrime, are unlawful acts whose common purpose includes deceiving people and scamming them for their money. Therefore, individuals involved in digital arrest scams can be considered participants of criminal conspiracies.

Wrongful Confinement:[10] In such a scam, the victims are restricted from moving out of their place and are forced to remain on the video call with their microphones and videos on for the specified time. The victims are made to feel threatened and restricted from reaching out to anyone else, thus making them pay money to the fraudster. It is, therefore, evident that the victims are illegally confined by such scammers and are restricted from moving beyond the specified limit.

Personating a Public Servant:[11] The primary modus operandi adopted by the fraudsters is personating as any official of the public and doing anything in respect of Personation. The public will come to believe that they are true public servants, and they must do as told in order to avoid serious repercussions. Personating as a public servant is one of the essential ingredients of the digital arrest scam used by the scamsters to deceive simpletons. It means that the digital arrest scammers are liable under the given section of the Bhartiya Nyaya Sanhita (BNS).

Extortion:[12] This is a kind of cybercrime where the victims are dishonestly led to believe that if they do not pay the criminals, then they will be apprehended by law enforcement agencies, as they had committed the crime. Thus, money is earned through creating fear among the victims. There are instances wherein individuals were duped to the extent of losing all their hard-earned money.

[9] *Ibid* s 61
[10] *Ibid* s 127
[11] *Ibid* s 204
[12] *Ibid* s 308

Forgery:[13] The scammers will pass on the false papers to the person who is under attack and will intend to do mental and physical damage to the individual. Through such fake papers, they build up the image of themselves as a government official and ensure that what they say cannot be refuted in any way. The purpose behind carrying out such schemes is to commit financial fraud. They will hang up once the money is transferred to their account.

All these provisions should be brought forward when trying the accused and held responsible for their actions. Digital Arrest Scams should be taken as an extremely serious crime, which is an organised crime offence. It includes crimes such as criminal conspiracy, where two or more people have been involved, cheating, wrongful confinement, personating a public servant, cheating by personation, extortion, making a false document, and forgery.

Information Technology Act, 2000: Section 66C of the IT Act is related to the criminal offence of cheating using another individual's identity. Section 66C states that any unauthorised use of an individual's digital signature, password, or unique identifying information constitutes identity theft and cheating through electronic signatures. The use of forged credentials, official identities, and stolen information to defraud victims is a common tactic among digital arrest scammers.

Section 66D of the IT Act pertains to cheating by impersonation using computer resources or electronic communication facilities. Since most digital arrest scams are committed via telephone calls, video conference apps, messaging apps, and other means of digital communication, section 66D is relevant to multiple elements of this crime.

Lastly, the Information Technology Act establishes legal guidelines for investigations of cybercrimes, the collection of electronic evidence, and the prosecution of criminals. For example, the evidence used in a criminal trial may include various electronic records such as voice recordings of phone calls, emails, text messages, transactional information, and digital communications. Nonetheless, the IT Act was passed at a time when there were no sophisticated forms of modern cybercrime such as artificial intelligence-based attacks, deepfakes, and social engineering scams.

[13] *Ibid* s 336

LEGAL AND ENFORCEMENT CHALLENGES

The presence of many legal provisions in the Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000, does not help law enforcement agencies address issues arising out of digital arrest scams effectively. While the implementation of any legal system requires, apart from the presence of legal provisions, investigation of offences, detection of offenders, collection of evidence, and securing convictions, many obstacles make this difficult in the case of digital arrest scams.

Lack of Specific Legislation: There have been a few advancements that have been made to improve the system in order to address the issue of digital arrest through a systematic approach, but unfortunately, the present legislation in India does not contain any provisions that relate to digital arrests. It has left a loophole in the system when trying to fight cybercrimes, which continue to occur with increasing frequency. In order to fight such a trend, an improvement in the legal system is required to address the issue of digital arrest and provide greater protection of people from such crimes, along with proper training for all agencies concerned with cybercrimes.[14]

Cross-Border Cooperation: Moreover, cross-border digital arrests create complications since the criminals often use the loopholes created by differences in the legal system to avoid being prosecuted, as they operate from nations that have less stringent rules. It is necessary, therefore, that there is more international collaboration, which will include setting standardised mechanisms to facilitate data exchange and extradition policies. There should be an international effort to deal with the menace of cybercrimes effectively.

Anonymity and Technological Sophistication: The digital arrest scammers tend to employ modern technology-based tools that help to remain anonymous and undetected by the investigating authorities. Technologies like the virtual private network, encrypting communication methods, and fake phone numbers and online personas can help the perpetrators to avoid any sort of identification by the relevant agencies. The criminals use temporary phone numbers, mule bank accounts, and various other techniques through the use

[14] Ankoosh Mehta et al., 'From Clicks to Cuffs: Understanding Digital Arrest in the Indian Legal Landscapes' (*Cyril Amarchand Mangaldas*, 13 February 2025) <https://disputeresolution.cyrilamarchandblogs.com/2025/02/from-clicks-to-cuffs-understanding-digital-arrest-in-the-indian-legal-landscapes/> accessed 16 May 2026

of digital technology. Technology has also helped criminals come up with highly authentic-looking fake communications. Forged government paperwork, fake identification cards, manipulation of the caller ID system, and even a well-designed interface through technology can help generate authentic-looking communication.[15]

Lack of Awareness: The reason people were easy targets of cyber scammers is that they were not aware of their modus operandi. People who are not well-informed about the concept of cybercrime and digital scams are an easier target for cybercriminals.

Technological Complexities: The use of sophisticated technologies, for instance, AI and Deepfakes, is now increasingly employed by scammers to pose as law enforcement agencies, hence making it hard to identify and trace them.

CHALLENGES IN TRACING AND RECOVERING FRAUDULENT TRANSACTIONS

A primary issue with digital arrest scams is the fast pace at which illegally acquired cash is moved. Often, once the fraud is committed, criminals transfer the money through various financial institutions, virtual wallet companies, or cryptocurrency exchanges to cover their tracks. Usually, the transfer is quick enough for the money to be withdrawn instantly or moved to other accounts belonging to third parties known as “money mules.” While innovations like the Cyber Crime Helpline (1930) have made it easier to freeze suspicious activity, it is still hard to recover lost funds if reported too late.

Comparative Perspective: The menace of digital arrest scams is not specific to India alone, as various countries around the world have faced similar scams using digital means through impersonation of government officials, financial watchdogs, or law enforcement agencies. In their attempt to counteract the menace of digital arrest scams, these countries have employed creative solutions, and analysing their efforts will provide India with a lot of lessons.

United States: The U.S. legal system is both broad and accommodating, affording prosecutors the flexibility of choosing from different anti-cyber laws that they can apply to various forms of cybercrimes. Under the Wire Fraud Statute, a crime involving impersonation through fraud and

[15] Nidhi Gupta, ‘Digital Arrest in India: Navigating Challenges and Legal framework’ (2025) 8(2) International Journal of Law Management & Humanities <https://ijlmh.com/paper/digital-arrest-in-india-navigating-challenges-and-legal-framework/> accessed 16 May 2026

deception, it is possible to apply the statute to cases where the perpetrators have used their VoIPs, emails, and other video conferencing methods to defraud other people. Perhaps most important of all, the Wire Fraud Statute does not require that the crime be accomplished; it requires only intent and use of interstate communication.

Agencies such as the FBI operate as institutions in Cybercrime investigation efforts. The FBI has established the Internet Crime Complaint Centre (IC3), where it receives complaints from victims. This is the main hub that provides analysis and gathers intelligence about criminal activities and shares the same with law enforcement agencies. The FTC complements criminal enforcement in consumer protection by working on consumer education on fraud prevention and reporting.

United Kingdom: In the United Kingdom, a more formal and specific approach is taken, mainly using the Fraud Act 2006. This act clarifies and adds to the existing legislation that covers many types of fraud by placing them in distinct categories, making the doctrine more accessible and easier to apply. The False Representation component of the Fraud Act 2006 criminalises fraud when a person makes a false representation in a manner that is dishonest with the intention of causing a "loss". This directly applies to impersonation fraud, including those that are done online.

LESSONS FOR INDIA

A comparison of these jurisdictions offers some crucial lessons for India in this regard. First, awareness on the part of consumers should be considered a crucial element towards fighting cybercrime instead of an auxiliary one. Secondly, better coordination among the different institutions, including the banking system, telecom companies, and law enforcement agencies, is needed to allow swift identification and prevention of fraudsters from perpetrating scams. Finally, the creation of special anti-scam units along with proper reporting facilities can help improve investigative effectiveness.

The case study of the United States and the United Kingdom indicates that dealing with the problem of contemporary cyber fraud involves not only legal reforms but also technological measures, as well as a significant level of consumer awareness. Such lessons can offer important points of reference in tackling digital arrest scams in India.

Real-life Incidents: Elderly woman loses ₹2.4-cr. Home, Gold Jewellery, Savings in 'evolving' Digital Assets: A 75-year-old woman in South Delhi was not only subjected to a "digital arrest", but the scamsters went a step further: they showed up at her doorstep and forced her to pawn her gold jewellery and sell her only home. Vibha (name changed), who lives alone in Vasant Kunj, received a call on her landline on April 6 claiming she was linked to a money laundering case. What followed was a month-long ordeal involving the transfer of money, gold and property, along with severe mental and physical trauma. From April 6 to 27, she remained under constant video surveillance. During this period, she was forced to transfer ₹3 lakh, take a gold loan of about ₹5 lakh by pawning jewellery weighing 83.5 grams (worth about ₹12 lakh), and sell her Vasant Kunj house, worth over ₹2 crore. The money received from the loan and the property sale was immediately siphoned off to the scamster's accounts.[16]

Maharashtra Police Arrest Seven in Rs 58 Crore Digital Arrest Scam: In connection with the digital arrest scam involving 58 crore rupees, the Maharashtra Police have arrested seven people linked to the fraud. Maharashtra Cyber, the state's nodal agency for tackling cybercrime, revealed that the masterminds behind the scam used over 6,500 fake bank accounts, spread across 13 layers, to launder the stolen money. These accounts were opened under the names of bogus companies. The case was registered by Maharashtra Cyber after a 72-year-old businessman from Mumbai reported that he had been digitally arrested and defrauded of a large sum of money. The fraudsters conducted fake court proceedings and police interrogations over video calls, tricking him into transferring 58.13 crore rupees over 40 days, wiping out his entire life savings.[17]

A 74-Year-Old Bengaluru Woman Cheated Of Rs 24 Crore In Digital Arrest Scam: A major 'Digital Arrest' cyber fraud racket was busted in Bengaluru by the Karnataka State Cyber Command Unit after scammers allegedly cheated a 74-year-old woman of nearly Rs 24 crore by impersonating senior officials from central investigation agencies. Investigators said the cyber fraudsters posed as high-ranking officials from the CBI and Enforcement Directorate (ED) and

[16] Shrimansi Kaushik, 'Elderly woman loses ₹2.4-cr. home, gold jewellery, savings in 'evolving' digital arrest' *The Hindu* (11 June 2026) <https://www.thehindu.com/news/cities/Delhi/elderly-woman-loses-24-cr-home-gold-jewellery-savings-in-evolving-digital-arrest/article71086552.ece> accessed 16 May 2026

[17] 'Maharashtra Police Arrest Seven in Rs 58 Crore Digital Arrest Scam' (*News on AIR*, 17 October 2025) <https://newsonair.gov.in/digital-arrest-scam/> accessed 16 May 2026

psychologically trapped the victim, Lakshmi Ramamurthy, a senior citizen from Bengaluru, through a fake 'digital arrest' operation.[18]

Digital arrest scam: 67-year-old woman defrauded of Rs 16 lakh: Even as police continue to warn the public against digital arrest scams, a 67-year-old woman from Sreekaryam has been defrauded of over Rs 16 lakh by cyber criminals who posed as CBI officials and falsely linked her to a money-laundering investigation. According to her complaint, the fraud began on May 18 when she received a WhatsApp video call from persons claiming to be officials with the Central Bureau of Investigation (CBI). The callers alleged that her Aadhaar card had been misused in Mumbai for illegal financial transactions and that she was under investigation in connection with a money-laundering case. To convince her that the allegations were genuine, the fraudsters sent what appeared to be official documents purportedly issued by a Notary Public in Mumbai under the title 'Notarised Supervision Acknowledgement'. The documents, coupled with repeated threats of legal action, reportedly left the woman fearful and convinced that she could face arrest.[19]

SUGGESTIONS AND WAY FORWARD

With the rise in incidents of online arrest scams, it has become clear that legal measures are not sufficient to protect individuals from being victims of online scams. Though India has formulated laws to deal with cybercrime, more proactive measures and public education are necessary.

The government needs to conduct regular campaigns to create awareness among the general public about online scam cases. People fall into traps of digital scams as they do not know that authentic police personnel, CBI officers or government officials never ask for money on the phone or via videos. Such awareness campaigns can be conducted by using media such as TV, social media sites, newspapers, educational institutes, and community centres.

[18] Deepak Bopanna, 'A 74-Year-Old Bengaluru Woman Cheated Of Rs 24 Crore In Digital Arrest Scam' (*NDTV*, 24 May 2026) <https://www.ndtv.com/india-news/74-year-old-bengaluru-woman-cheated-of-rs-24-crore-in-digital-arrest-scam-11541658> accessed 16 May 2026

[19] 'Digital arrest scam: 67-year-old woman defrauded of Rs 16 lakh' *The New Indian Express* (16 June 2026) <https://www.newindianexpress.com/amp/story/cities/thiruvananthapuram/2026/Jun/16/digital-arrest-scam-67-year-old-woman-defrauded-of-rs-16-lakh> accessed 16 May 2026

Secondly, digital literacy needs to be fostered at all levels of society. Citizens should be advised to cross-check the identity of the caller before providing any personal information or making transfers of money. Educational institutions, such as schools and colleges, together with companies that employ their staff, could also help spread awareness regarding cyber scams.

Thirdly, the banks need to enhance their system for detecting any kind of fraud in transactions. Transfers made in a surprisingly high amount or transfers made to accounts that have just been opened must sound an alarm bell right away. Better cooperation between banks and the police force would be helpful in this regard.

The telecommunication companies also play a role in fighting impersonation scams since they will be responsible for tracing suspicious numbers that are associated with these offences. With better verification techniques and stringent registration of SIM cards, fraudsters will find it hard to exploit communication channels.

Legally, law-making bodies can introduce legal statutes concerning cases of digital impersonation and digital arrests. While it is true that laws exist against offences like cheating, identity theft, and criminal intimidation, it would be better if there were laws specifically formulated for this type of crime. Cybercrime investigative units need to remain vigilant and enhance their capacity to investigate such cases through additional training and technological advancements. Considering that most fraudsters are tech-savvy and conduct their activities across jurisdictional boundaries, it is only fair that investigators have relevant knowledge and technology to trace suspects.

In addition to all this, the citizens need to be vigilant themselves. The investigative process of any governmental body does not involve asking for money by way of telephonic calls or putting a person “under digital arrest.” People need to confirm their doubts from family members and lawyers and promptly lodge complaints via the Cyber Crime Helpline (1930) or the National Cyber Crime Reporting Portal. The collaboration of the government, police department, banking institutions, telecom companies, and the citizens themselves becomes necessary to deal with these “digital arrests.” Only by raising awareness and following stringent measures can India become a more secure and safe environment for its citizens.

CONCLUSION

Digital arrest scams are currently one of the most significant types of cybercrime that India is witnessing. Through the abuse of law enforcement agencies' names and people's fear of being held accountable under the law, perpetrators manage to convince even highly educated people to commit fraud. The increase in such cases shows how cyber criminals keep changing tactics in order to exploit modern developments in technology and people's lack of knowledge.

India has a set of laws, such as Bharatiya Nyaya Sanhita, 2023 and the Information Technology Act, 2000, which can be used as a foundation in the prosecution of the perpetrators of digital arrest scams. Nevertheless, the lack of any legal definition of such scams makes it very difficult to investigate crimes. Moreover, cross-border operations, anonymity of cyber criminals, and difficulty tracking online transactions complicate investigations further.

On the other hand, the problem cannot be solely handled through legislative means. Awareness amongst the masses, proper digital literacy, reporting of such crimes, as well as coordination between different government departments, banking institutions, telecom service providers, and citizens alike are equally critical. As India moves ahead on its path to becoming a digitally-enabled nation, securing the trust of its citizens is vital.

In essence, combating digital arrest scams demands a balanced approach, with a combination of laws, stringent implementation, proper safeguards and an enlightened population being equally crucial.