October
December 25

Aryavart Journal of Multidisciplinary Research
(NATIONAL PEER REVIEWED E-RESEARCH JOURNAL)
E-ISSN 3107-6009

Vol - 1
Issue - 4

Digital Arrest (Cyber Arrest) Scams in India and Their Prevention

Shantanu Guha
Assistant Professor
School of Legal Studies
Aryavart University, Sehore (M.P)

ABSTRACT

Another cybercrime of digital hostage websites in India is where people are framed, and they get lured into thinking that they are under investigation for some crime by a parent. The crooks operate under the guise of being a police officer, CBI or financial regulator or cyber-crime investigator to scare victims to give them money-not in lieu of non-existent legal proceedings. These sexual predators use video calls, forged ID cards, fake legal notices or bogus back ground offices. They subsequently emotionally ladle the victim, storm the castle forcing a snap decision through scaring and intimidating. The primary purpose of the study it to determine how these scam works, why people fall into the scam and what type of strategies can be employed for preventing it. Real case scenarios, warning notices and published reliable cyber security material with trends and methodologies were reflected in all these studies. The study results demonstrate that there is a demand from the public to be told about toughened cybersecurity systems, legal changes and teaching in digisafety. To be sure, this barrier will erode as police and citizens alike use technology to work against such arrests in cyberspace. The article describes the crime psychology and offers useful ways to avoid it.

KEYWORDS

Cyber intimidation, impersonation crime, social engineering, virtual extortion, authority pressure scam.

1. INTRODUCTION

India's embrace of digital payments and online communication has provided a level of convenience to daily life, but it also is widely seen to have increased the attack surface for cybercriminals. One of the cybercrimes with the fastest growth in recent years has been digital arrest scams, where con artists impersonate law enforcement officers or regulators and accuse people of crimes. They set up video calls, flash fake badges and design backdrop rooms to look like police stations or government offices. Victims are then ordered to resolve the matter privately or be arrested, have property confiscated or pay a fine. And this fear is what compels individuals to send money through the internet or divulge sensitive banking information. India's embrace of digital payments and online communication has provided a level of convenience to daily life, but it also is widely seen to have increased the attack surface for cybercriminals. One of the cybercrimes with the fastest growth in recent years has been digital arrest scams, where con artists impersonate law enforcement officers or regulators and accuse people of crimes. They

Aryavart Journal of Multidisciplinary Research
(NATIONAL PEER REVIEWED E-RESEARCH JOURNAL)
E-ISSN 3107-6009
Vol - 1
Issue - 4

set up video calls, flash fake badges and design backdrop rooms to look like police stations or government offices. Victims are then ordered to resolve the matter privately or be arrested, have property confiscated or pay a fine. And this fear is what compels individuals to send money through the internet or divulge sensitive banking information.

It's not just tech-illiterate folks who fall victim to digital arrest scams. That's what they prey on educated professionals, business owners and students: Scammers employ sophisticated psychological skills that create panic. The unexpected charge of wrong creates confusion which hinders clear thinking. Often, bad actors leverage stolen personal data from breaches to establish trust and legitimacy. They tell victims to stay isolated, never discuss the matter and follow scripted prompts. This is a strategy that keeps other people from involving themselves and challenging the reality of what you are dealing with. The scams are a frustrating and painful trend in a national problem that marries digital manipulation with emotional control. To build intervention to decrease victim susceptibility, enhance public confidence and law enforcement response in the digital era requires a clear understanding of how these scams work.

2. PROBLEM STATEMENT

In India, digital arrest scammers despite being targeted by government cyber cells and media reporting are on the rise. The issue is people do not realize armed police officers don't use anonymous online calls to threaten arrest or demand payment in a digital form. Psychological fear, digital naivety and trust in authority are windows of opportunities for criminals to exert their grip on victims. Having traced your identity to criminal activities you didn't have a clue about most people would run mad. They perceive being quiet and cooperative will save face and shield them from legal consequences. Fraudsters play on a sense of emotional weakness and urgency to elicit an immediate non-thinking, non-fact-checking response from victims. But one of the big problems is that these scams are well organized and computerised things - you would find very little footprints, as most of them run it from international call centres.

The underreporting of incidents much contributes to the problem. Victims usually do not complain because they are embarrassed, or fear public opinion. Sometimes, they do not have confidence in the justice system or feel that they will get their money back. Not reporting crime just helps the criminals to get stronger and more cleaver. And many survivors experience long-term mental anguish, fear and financial hardship. Lack of a robust national framework for awareness, combined with sluggish legal implementation constrains the response such that not much can be achieved. Poor digital safety training in schools, at work and in the public sector also fosters an environment where people cannot assess with confidence cyber threats. It is true that cybercrime laws are in place but issues of enforcement accompanied with the continuous development of different scam techniques leaves prevention wanting. The issue is not one just of the technical but also of mind, law and society requiring a multi-faceted approach.

3. OBJECTIVES OF THE STUDY

This study aims to understand the dynamics of digital arrest scams and identify the psychological, technological, and social determinants why these cons are becoming increasingly successful in India. The study will also seek to establish how scammers are able to portray themselves as credible authorities within a matter of minutes, the psychological tactics used to force compliance and how misuse of digital identity can lead victims to rationalise decisions. It purports to examine real cases in order to identify common patterns like fear-driven inducement, non-disclosure instructions or financial pressure. The study seeks to understand why even the most educated and experienced fall victim to such scams, why they don't see it coming. This insight can be valuable to inform more effective prevention of perception strategies, which empower people to respond confidently when confronted with potentially suspicious encounters.

One additional goal is to recommend prevention measures through public awareness, tooling upgrades and improved cybersecurity solutions. The study also seeks to assess opened strategies by government departments, banks, telecommunication companies and other digital service providers against scam exposure. Another objective is to suggest policy-based reforms, including verification mechanisms, real-time fraud alerts and stringent tracking of digital transactions. The research will support the development of education programs for students as well as corporate workers and seniors who are some of the most common victims. But the goal is to help make a safer environment, where users could be more emboldened in doing their digital activities online without fear of emotional or financial abuse.

4. LITERATURE REVIEW

The ignorance or the lack of awareness has become their most effective tool for all the cybercriminals and according to some researches which were done on analyzing the cybercrime trends we have found that social engineering is now considered as one of the primary weapons by criminals. Rather than hacking into systems via technical vulnerabilities, these scammers prey on human psychology. Studies suggest that fear, urgency and authority pressure are the persuasive tactics most likely to work. Cybersecurity journals internationally published reports that the same type of digital arrest scams have been used in countries such as China, Singapore and the United States, where scammers pose as members of the legal department and request immediate payments. Scholarship indicates that scams proliferate in countries where digital literacy rises more quickly than digital awareness. A lot of investigators say victims will often cooperate not out of a trust in the scammer, but usually because they feel threatened by their own failure to comply. The results suggest that emotional forces override mechanisms of rational decision-making upon sudden threats to personal identity or legal protection.

According to the reports of the Indian Cyber Crime Coordination Centre (I4C), CERT-In advisories and NCRB data, there has been a significant increase in impersonation-based cyber

fraud. Lack of public knowledge about the legal process remains a big factor, experts stress. Articles from financial crime investigators describe how criminals may 'spoof' telephone numbers in order to display false caller IDs and establish apparent credibility. Case studies in newspapers like The Hindu and Indian Express revealed that all victims were tech-savvy, but could not react logically under emotional stress. There's also deserved mention of the challenges in capturing criminals because of across-border operations and digital camoflouging. Some researchers suggest campaigning for awareness along with deploying technology-based measures like authenticating caller ID, advanced fraud detection systems and centralized platforms for feedback. Most of the reviewed papers agree on providing assistance rather than intervening, and education making up the best defence.

5. RESEARCH METHODOLOGY

This study is based on a descriptive qualitative approach which is pivoted on secondary data. The data was extracted from cyber security reports, academic journals, cybercrime portals, newspaper archives and advisories issued by the I4C and CERT-In. The goal is to gain insight into actual patterns of incidents, technological means and the psychological effect rather than gathering statistical measures. Real cases descriptions were theme-analysed to extract recurring elements in scam. Square themes were intimidation, accosting techniques, false authority construction and exigent commands. The approach provides an observation-supported understanding of scam process and victim reaction. All publicly available data was used, therefore ethical approval is not applicable. While it is not based on independent interviews, for reasons of privacy and safety, a thorough understanding of the problem could be ascertained through confirmed documentation and acknowledged expert commentary.

5.1 Data Sources: The input for this study were drawn from credible sources, such as national cybercrime database, NCRB figures, CERT-In advisories and government circulars and reports from the area of cyber security awareness. References of case-stories published in newspapers 'The Hindu, NDTV and Times of India' were also checked to understand the real victim experiences. Cybersecurity research companies gave Fly on the Wall a glimpse of how the scammers behind impersonation worked. Conceptualization of social engineering psychology was facilitated by Academic Journals. In addition, resources consisted of webinars and cyber workshops. Together, these resources provide a wealth of information ranging from common scam strategies to victim responses and preventive tips.

5.2 Analytical: Approach: The authors use thematic content analysis to examine case descriptions and identify common behavioural themes involved. Case notes were analysed to reveal elements shared in general scam script structure, emotional ploys, identification information and payment details. The study compares patterns between various reports to grasp the victims' vulnerability and scam development. Themes such as fear and urgency, isolation and

compliance pressure were identified as dominant determinants. This procedure favours the interpretation structure and deep conclusion generation.

5.3 Research Design: A qualitative descriptive research approach was used because online arrest scams are based on emotions and mind control rather than quantifiable statistical numbers. The design enables exploration of personal experience, style of communication and behaviour in response. It is concerned with scam anatomy and mitigation, as opposed to numerical pattern generation. The focus of the study is also not all-encompassing. This structure affords a more coherent picture of human-cantered social engineering crime.

5.4 Limitations of Study: The primary limitation of the present study is the secondary nature of most data, as a consequence of embarrassment and fear there are victims who hesitates to report. Under-reporting fails to provide a full picture of the true nature and extent of the problem such information is partial. Scam tactics evolve rapidly, so there may be a revolving door of findings that need updating. In this context, access to only second-hand interviews serves to inhibit emotional nuance. But in a way the diverse sources of information make up for this by offering a realistic and multi-angle coverage.

6. CASE STUDY AND DISCUSSION

This is how digital arrest scams work, according to real case studies. One such recent case was of a Mumbai-based professional, who received a call stating that illegal documents were found in his courier package which was linked to his Aadhaar number. Call was transferred to a video call where the scammers were posing as cybercrime department officers in uniform and in professional background setup. They accused him of money laundering and threatened to come and arrest him. Panic-stricken and bewildered, he tried to learn that he must isolate himself, not call his family and transfer money to clear his name. Eventually, he lost a few lakhs before discovering that it was a fraud. This is another example of how the combination fear, confidence pressure and isolation encourage victims to become emotionally immobilized. One was a woman from Delhi, who was informed that her bank account was connected to criminal activities. She was told to make a video confession and move her money into a "secure government wallet." The emotional scars remained for months as the psychological impact proved just how far-reaching they were beyond the financial damage.

Debate on such cases provides striking patterns. First, scam callers reach out via numbers with spoofed IDs intended to appear as official. Second, they make sudden threats in order to stifle rational analysis. Third, they retain control by isolating victims and not allowing outside counsel. Fourth, the pressure urgency so to obstruct verification. The video call stage is one of the most important, as visual authority equals trust. The discussion also evidences that victims are from every background, so intellectual level is not the obstacle. Rather, resistance is

determined by emotional stability and awareness. The evidence in case is that it is prevention through education and not by technology. The cases highlight the requirement for accessible reporting structures, more rapid public awareness and national level campaigns.

7. PREVENTIVE MEASURES AND RECOMMENDATIONS

Measures need to be preventive and integrate technology, education and laws. The initial measure to avoid this situation is education. People should be aware that actual cops, or reps of the government don't require release payments in the form of online financial transactions; they also would never threaten arrest over phone calls. Schools, colleges and workplaces and community centres need digital safety modules to teach how impersonation scams work. Public awareness campaigns on television, radio, social media and banking apps can alert people to common signs of fraud. We need a digital safety curriculum nationwide. X Research Report Panda 3140x384 It's hard to help stop robos - bad calls by impersonating companies or services - when your bank and phone company won't say 'NO, this number is fake!' I will repeat: financial service companies need to add automatic scam alerts when a pattern of high-risk transfers is detected. Verification portals can also assist users in determining whether or not a number is legitimate. Digital literacy (seniors) also needs to be developed.

In the law and engineering suggestions are banning other digital VoIP services or internet call routing by which fraud calls originate. It also required cooperation between police agencies, telecom operators and cyber-security firms to trace scam networks. You still need to make it easier to report and faster response through the cybercrime portal. Adopting tougher regulations for personal data privacy could limit scammers to harvesting less information from breaches. Police departments should conduct, on a regular basis, public training sessions where they show real-world arrest and investigation procedures. Rapid action teams should be there with hotlines to help the victims and freeze transaction when something's fishy. Lastly, national cyber security policy should incorporate mandatory awareness certification for front-line public sector staff who can share it with others. Prevention is the responsibility of all of us, at every level in society: citizens and institutions but also government.

8. CONCLUSION

Online arrest scams: A huge security, trust & mental health risk for India the scams are based on manipulation, not sophisticated hacking techniques designed to outwit the victims. Offenders pose as authority, cultivate an urgency and isolate the vulnerable to establish control. Reality cases show devastating emotional and financial impacts. The study finds that limited public and private awareness, insufficient reporting systems, misused personal data and fast-paced digital growth all contribute to the proliferation of this crime. A sufficient analysis of the forms of scam and emotional patterns will certainly help to developing such a strong defensive system. Prevention is possible through education, stronger digital literacy and verification technologies

and coordinated law enforcement. Public knowledge is the best defence. We have to train people how to double-check a piece of information, how to remain calm in situations that feel like they could be threatening, and not make decisions from emotional pressure.

All of this points to the fact that much better cooperation among government agencies, technology companies and citizens can dramatically lower the amount of success scammers have. It's about having better advanced fraud prevention solutions, greater ongoing awareness of and training in cyber security policies. Advancing protection of the people against digital inches from arrest is about not just protecting their financial health but also their trust in digital systems; indeed, it could be about protecting mental well-being. A digital space that is safe needs informed users who know their rights and act wisely against threats.

REFERENCES

1. Indian Cyber Crime Coordination Centre (I4C). (2024). Report of the Committee on Cyber Crimes Awareness and Prevention. MINISTRY OF HOME AFFAIRS,GOVERNMENT OF INDIA.
2. National Crime Records Bureau. (2023). This is an offence against a person; similar to rape or murder in the IPC. Ministry of Home Affairs, India.
3. CERT-In. (2024). Cyber Security Advisories and Alerts. Indian Computer Emergency Response Team (CERT-In) under Government of India.
4. The Hindu. (2024). From India, a Rise in Online Scams and Calls to Shut Them Down National News Report.
5. NDTV. (2024). Victims Tell on Video Report on Fake Police Call Extortion Cases. Cyber Security Section.
6. Sharma, R. (2023). Psychological Threats and Fear Appeal in Cyber Fraud. Journal of Cyber Psychology and Behaviour, 12 (3), 44-56.
7. Singh, A. & Verma, K. (2022). Misuse of Technology and Cyber Crimes. Nourishment Kola, DO 2019 IJODSE INTERNATIONAL JOURNAL OF DIGITAL SECURITY AND ITS ENGINEERING (ISSN:2581-8367) Impact of Randomness and Stego Key in Transform Domain Using LSBRanking for Image Forgery Detection.
8. Gupta, S. (2023). CYBER CRIME CYBER FRAUD AWARENESS IN INDIA. Indian Journal of Criminology, 15 (2), 70-89.