Online Theft and Digital Arrest: A Case Study of Vulnerable Sections of the Society

Dr. Jai Babber Bohra
Assistant Professor (VSY)
Dept. of Economics, Govt. Girls College, Jhalamand, Jodhpur

Abstract:-

Online theft also known as cybercrime, has become a significant threat to individuals, business and organisation. Digital Arrest is a technique used to apprehend online thieves and prevent further crimes. The rapid growth of internet and digital technologies has led to corresponding increase in such type of activities. Vulnerable sections specially senior citizen & technically inefficient have been affected more by such type of financial crime. Paper examines various type of cyber-crimes prevalent in India. This paper is a theoretical attempt to explore digital arrest and its economic impact on vulnerable sections of society along with suggesting potential strategies to mitigate its adverse effect.

Keywords:- Digital arrest, Vulnerable Section, Cyber Crimes, Internet, Economic Impact Cyberstalking.

Introduction :-

Now a days increasing use of vertical platform or internet has given rise to a new class of cyber criminals who use technology to defraud one of the most dangerous & worrying scams to emerge in recent times is the "digital arrest". In this new scam, fraudsters pose as law enforcement officials and demand money from their targets by creating an atmosphere of panic. Such type of crimes starts with an unsolicited phone call or video call from someone posing as a representative of a government body, including the police, CBI and Other Organizations. They use a variety of strategies like False allegations such as Drug trafficking, money laundry & Financial fraud threat of arrest, Financial demands and psychological manipulation.

Actually, fraudsters aggravate the victim's emotional state and make them more vulnerable by using techniques specially old age people. Some common types of cyber crimes are hacking, identify theft, phishing, malware attacks, financial fraud (digital arrest), Cyber bullying and Harassment.

In fast growing digital world certain groups such as elderly technically inefficient individuals and low income families are particularly at risk. They may lack the resources or knowledge to defend themselves against online threats, making them prime targets of exploitation many cases regarding this problem register in Cyber cell not only in India but also at-global level. (Tripti Jaiswal - 2023)

Objectives:-

1.   To evaluate the impact of digital arrest on society specially vulnerable groups.

2. To assess the economic consequence of cyber crime in India including financial losses.
3. To propose mitigation strategies and recommendation for policy maker and to minimize the adverse effects of online crimes on the Indian economy & society.

Many cases of people being called by scammers impersonating police officers and CBI officials have been reported in 2024 (Narayan Priyanjali, 2024 TOI)

According to her that cyber criminals hijack people's brains & make them follow their orders for hours and at times, even months. They use personal information from social media sites to show they are investigating officials and then use people's fear to trap and empty out their bank accounts. Further more people have been receiving emails informing them about their child pornography charges against them. There fake notices have stamps of cyber cell and intelligence Bureau. According to the Indian Cyber Crime Coordination (14C), Ministry of Home Affairs (2024) that number of cyber crime complaints were 26049 (2019) Which increased by 740957. (May 2024) and in certain instances, unsuspecting victims undergo "digital arrest" and remain visually available over Skype or Whatsapp Video calls to the fraudsters till their demands are met. Some researchers have studies the new criminal market directly.

They are from Internet Security firm team cyber have long documented online crime (for example Thomas and Martin, 2006) Franklin Perrig, Paxon & Savage (2007) mentioned the public chat channels used by online criminals to contact each others, gathering extensive data on credit / debit card and fraud spamming, phishing and the cake of compromised hosts.

Digital Arrest Case Studies

Case 1:

Dr. Pooja Goel: In a recent incident Dr. Pooja (45) Goel from Noida by professon Doctor was targeted. The fraudsters accused her by using her phone number to distribute illegal content under duress. Dr. transferred Rs. 60 Lakh before realising the scam.

Case 2:

Elderly woman in South Delhi - A 72 years old woman from CR park south Delhi who was deceived by scammers impersonating police personal. The fraudsters extorted Rs. 83 Lakh from her by fabricating a legal issues required immediate payments.

Case 3:

77 years old Bengaluru women held in "Digital Arrest" (Source: Express New Services 2024) She was lost Rs. 1.2 Crore in cyber fraud. The fraudsters posed as telecom officials and Mumbai Crime Branch personnel and told her that a SIM Card purchased in her name was being used for illegal activities. She was taken Aback and shard all the details. They asked for. They requested her bank account information and

investment proof for verification while threatening to correct her for not cooperating with investigation. To further persuade her, they showed her a copy of an FIR and an arrest warrant, making it appear that the orders were from the Supreme Court. In multiple transactions, she transferred Rs. 1, 28, 70, 000 from her account after being told it was part of an investigation. The accused promised to return the money after the process was complete.

Case 4:

Retired Major General of Age 79 years put under Digital Arrest. (Source - Hindustan Times, Aug. 29, 2024) According to Indian Army retired officer that he was allegedly put under digital arrest for five days from August 10 to August 15, 2024 by online fraudsters posing as law enforcement personnel and duped Rs. 2 Crore. He was informed that a parcel was booked in his name from Mumbai to Taiwan when customs officers opened the parcel, they fraud five passports, four Bank credit cards, 200 gm MDMA and Laptop. The caller told me that there were all illegal items and the retired officer was assured by the fraudsters that the money would return to him within half an hour but when that did not happen, he realised that he had been duped.

Case 5:

A retired female doctor from Jodhpur (Raj.) was digitally arrested. She was digitally arrested for 17 days and scammed of Rs. 87 Lakhs by Cyber fraudsters. She received call from customs officer and Mumbai Police Officials, cleaning that her parcel contained Narcotics substances. Take passports and credit card. They then scared her with the threat of an arrest-warrant and forced her to transfer the money in parts for various purposes.

Case 6:

A 72 years old senior citizen lost Rs. 12 lakhs in digital arrest fraud in Jaipur. Fraudster posing as U.P. Police Officer and called him that his Aadhar card and SIM number were being misused and he could land in serious trouble. The scammers than said they would connect him with the SHO of a Police Station in Luckhnow, U.P. the scammers than made a video call and connected him with someone pretending to be a police officer. As the victim grew more scared and panic, scammer claimed for money for verification process and asked that he had to deposit 12 lakh in an account given by them.

From above cases it is explored that why Indians specially senior citizens easy prey to digital arrest.

The scale of such operations is elaborate with make believe setting created to make it look all true. According to ethical hacker Gautam Kumawat that criminals involved in digital arrest after use AI - generated voice / video call to make victims believe they have committed a serious crime. (Ashish Mukherjee India Today 17 Sep. 2024)

Cyber Crime experts say people fall prey to digital arrest due to ignorance, fear or blind trust and lack of technological knowledge.

Actually, Cyber Criminals works in two modules. One modules arranges SIM cards using fake documents and second one Targets people specially the old, poor & technically illiterate to use their Aadhar number and change the mobile number linked to it to one held by the crooks. These accounts thousands of them are zero balance accounts are where the siphoned. A module extorts people by posing as officers of investigating agencies. The gang chief is invariable settled overseas. (TOI, Aug. 2024)

Economic Impact And Government Efforts

A. **Direct Financial Losses**: Such as fraudulent transactions unauthorised access and stolen the amount of Bank account.

B. **Indirect Financial Losses**: Such as Reputational damage, loss of investor or customer confidence / trust these factors can put adverse impact on Economic activities.

C. **Increased Cost of Cyber Security**: Such as expenditure on developing cyber security infrastructure, hiring software expertise.

D. **Cybers talking and Harassment**: Information collected by cyber criminals can be used for cyber stalking harassment or black mail. This leads to mental and emotional distress for victims and a deterioration of online safety.

E. It causes operational disruptions for both large and small enterprises.

F. In 2021, the RBI reported significant rise in banking frauds with cases involving and skimming OTP - based frauds and online banking scams which takes away, economy in negative directions.

Government Efforts

Although the cyber police and government have also made alot of effort to check such types of crimes by issuing warnings & guidelines to help citizens to recognize & avoid falling victim to the digital arrest scam.

Key Steps include

1. Indian cyber crime coordination centre (14C) under the Ministry of home affairs plays a crucial role in combating cyber crime.
2. All related cases can be registered under 16 (D) (Cheating by presonation by using computer resources) of the IT Act.

3. Delhi police has also started a campaign to raise people awareness on the MENANCE called Digital Arrest.

Conclusion and Suggestion

The scam typically begins with a video calls where the scammers falsely accused the victim of Involvement in illegal activities. There accusations are designed to create panic and compel the victim to comply with financial demand known as "Digital Arrest". A trendy word prevailing in Cyber Crimes and trapped vulnerable segments of society specially

senior citizens along with technically illiterate population Govt. and concerned authorities used to play important role to control these activities but it is necessary to awake our power of Interpretation and analysis and to learn to balance our thinking power with fear, anxiety, panic and emotional fluctuation to cope up this problem. There should not be shared personnel details on social media because scammers do back ground research on social media before calling a person.

If you get cyber scam call please hang up the call first and speak to your local police station or listen and don't respond too quickly. The more time we take to think the loss are the chances of scammed. In short, the brain is our biggest weapon, we should used it best and not let it get hijacked.

References:-

1. https://times of india. indiatimes.com / technoloygy/tech-tips/ What is digital-arrest-scam-a-comprehensive-guide.
2. https://www.indiatoday.in/sunday-special/stroy/digita-arrest-cyber-scam-fraud-crime-delhi-police-people.
3. https:// navbharat-times. indiatime.com / state / rajasthan / jaipur / what-is-digital-arrest-cases-in-jaipur.
4. https:// www.academia.edu / 237045 89 / effect of cyber crime in Indian Economy.
5. Jaiswal Tripti (2023) "The Impact of Cyber-Crime on the Indian Economy and Society published in International Journal of Creative Resources Thoughts July - 2023.
6. Franklin, James, Adrian perriag, Vern Paxan and Stefan Savage 2007 "An Inquiry into the nature and causes of the wealth of internet Miscreant" proceeding of ACM Conference on computer and communications security 1375-388.
7. Report - Indian Cyber Crime coordination centre (14C), Ministry of Home Affairs 2024.
8. Thomas, Rob and Jerry Martin 2006 "The underground Economy Priceless usenix login 31(6):7-16.