ILE MULTIDISCIPLINARY JOURNAL
WHILE THERE'S RESEARCH THERE'S HOPE

ILE MULTIDISCIPLINARY JOURNAL [IF SCORE – 7.58]

VOLUME 3 AND ISSUE 1 OF 2024

APIS – 3920 – 0007 | ISSN - 2583-7230

Published by

Institute of Legal Education

https://iledu.in

AN ANALYSIS OF CYBER ECONOMIC CRIMES IDENTITY THEFT AND ONLINE FRAUD -TRENDS, AND PREVENTION ESPECIALLY IN INDIA

AUTHOR - M.SRIHARIPRASATH* & T. VAISHALI**, LLM SCHOLAR* & ASSISTANT PROFESSOR OF LAW** THE TAMIL NADU AMBEDKAR LAW UNIVERSITY, CHENNAI, TAMIL NADU, INDIA.

BEST CITATION - M.SRIHARIPRASATH & T. VAISHALI, AN ANALYSIS OF CYBER ECONOMIC CRIMES IDENTITY THEFT AND ONLINE FRAUD -TRENDS, AND PREVENTION ESPECIALLY IN INDIA, ILE MULTIDISCIPLINARY JOURNAL, 3 (1) OF 2024, PG. 325-329, APIS – 3920-0007 | ISSN - 2583-7230

Abstract

The article analyses the serious issues that are predominant in present society: identity theft and online fraud, which are part of cyber-economic crimes. With the development of new technologies, crimes also develop along with it. Identity is one of the most valuable assets of a person in the present era, in earlier days to identify a person we checked with moles, scars, and marks of a person later we used photos to identify but nowadays in the boom of technology we have to put a password, OTP's, Finger Print and even a face and eye scan to prove that you are you. When we come to online fraud most of the rural as well as old age people are affected by this compared with present generation people. The objective of this research is to find in what ways we can protect our identity and prevent ourselves from online scams to find effective methods and technologies to avoid online frauds and to analyze the recent laws and their effectiveness over these technology-based frauds and scams. In this article, the researcher uses a doctrinal method for an analysis.

KEYWORDS: Cyber, Identity, scam, technology, crime, frauds, etc.

1. INTRODUCTION

In the contemporary digital era, technology plays an important role in every aspect of life influencing major sectors like education, Business, communication, etc., We use technology to pursue education from various parts of the world to order food from home by using various apps and websites. If we want to learn coding, cooking, and even how to create a cryogenic engine everything is in our hands using an internet development, majorly after the introduction of Jio in India. Justice B.N. Srikrishna one of the distinguished Indian jurists and a retired judge of the Hon'ble Supreme Court of India observed in the context of discussing the implications of technological advancements on cybercrimes, particularly during the drafting of the Personal Data Protection Bill in India that "The rapid advancement in technology has brought about significant benefits, but it has also led to an increase in cybercrimes, including identity theft and online fraud. There is an urgent need for robust legal frameworks and stringent enforcement to protect individuals' digital identities and personal information"[1]. Identity theft and online fraud are among the parts of cyber-economic crimes. Cyber-economic crimes are crimes conducted digitally with the intent of financial benefits. Compared with traditional crimes like theft, robbery, etc., it's hard to gather evidence in the case of cyber-crimes. A person can sit and do any form of cybercrime from any part of the world, whereas traditional crimes are not like that.

Research Question:

1. What are the impacts of cybercrime on the Economy of a country?

[1] Privacy and Cyberspace in India: A critical analysis of Justice Srikrishna Committee Report and The Personal Data Protection Bill, 2018 - International Journal of Law Management & Humanities (ijlmh.com)

2. What are the preventive measures concerning cyber-economic crimes?

2. IDENTIFY THE VALUABLE ASSET

Personal identity is the most important asset in today's interconnected world, which encompasses various elements such as the name of a person, date of birth, address, financial information, and biometric data The misuse of these data leads to financial loss, damage to the reputation, emotional and social distress of a person. The act of taking once personal data of an individual is called identity theft. One of the formal definitions of Identity theft is the acquisition and use of private persons identifying information in a fraudulent matter for financial gain, which can include using someone's name, Social Security number, credit card number, or other personal data to make unauthorized purchases or transactions. Section 66C of the Information Technology Act,2000 deals with the punishment for identity theft which is 'Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.' In the case of Jaiprakash Kulkarni & Anr. Vs. Banking Ombudsman & Ors. (2022) Without any OTP verification unauthorized beneficiaries were added to the petitioner's account which led to a huge financial loss to the petitioner. Hence, the petitioner reported this to consent authorities and filed a complaint before the bank ombudsman. Still, he was rejected because the transactions were completed with valid credentials known only to the account holder, even though he said that the transaction had happened without any OTP notifications. So the petitioner approached the appropriate court and argued that there was no OTP notification received to him regarding adding beneficiaries and the bank failed to adhere to the RBI guidelines on limiting customer liability in unauthorized electronic transactions, the hon'ble court ruled that by quashing the ombudsman order directs the bank to refund the sum of the amount which was fraudulently transferred with an interest six percent per annum, this scenario is closely related to identity theft, where unauthorized access to personal information leads to financial fraud. The judgment in this case underscores the importance of robust security measures, adherence to regulatory guidelines, and the bank's responsibility to protect customer information and compensate victims of unauthorized transactions.

In the case of Dubin v. United States (2023) which happened in the United States of America where David Dubin was convicted of healthcare fraud and aggravated identity theft for overbilling Medicaid by misusing a patient's identification. The American Supreme Court ruled that the use of a means of identification must have a genuine nexus to the predicate offense. Even though there is a law related to these offenses' effectiveness plays a major role.

3. DEEP ROOTING OF ONLINE FRAUD

Online or cyber fraud is also a form of cyber-economic crime. Cyber fraud refers to the crimes committed using the internet or digital technologies to deceive an organization or an individual for financial gain, which can include activities such as phishing, Hacking, identity theft, credit and debit card frauds, investment scams, and online investment frauds, etc., Technology advancement pays a path for more developments to human society and also increase online related crimes. In the present era, we are practicing using online payments like Google Pay and Paytm etc., we store our amounts in a digital wallet which allows us to make huge amounts of transactions easily but it is also subject to getting trapped via online-related fraudulent methods. As per recent reports, India witnessed an alarming cyber fraud of amount 11,000+ crores in the year 2024 especially in stock trading scams. According to the Indian Cyber Crime Coordination Centre Stock trading scams led to a loss of 4,000 crores whereas as digital arrests accounted for a loss of more than 1,600 crores. As per the report of the Financial Ministry fraudulent scams related to UPI have increased 85% in the last financial year. Over 1.3 million fraud cases totalling over Rs 1,000 crore were reported in FY24. UPI transactions recorded a 57% increase during the same period. The Indian Cyber Crime Coordination Centre (I4C) stated that in May 2024, an average of 7,000 cybercrime complaints were recorded daily, marking a significant surge of 113.7 per cent compared to the period between 2021 and 2023, and a 60.9 per cent increase from 2022 to 2023, according to a report in the *Economic Times*. Additionally, 85 per cent of these complaints pertained to financial online fraud. The significant escalation in reported cases is evident from 2019 to 2024, with 26,049 complaints recorded in 2019, 257,777 in 2020, 452,414 in 2021, 966,790 in 2022, 1,556,218 in 2023, and 740,957 in the first four months of 2024 alone. Most victims fell prey to online investment fraud, gaming apps, algorithm manipulations, illegal lending apps, sextortion, and OTP scams. In 2023, the I4C reported over 100,000 investment fraud incidents. Digital arrests resulted in a loss of Rs 120 crore across 4,599 cases in the initial four months of 2024. Trading scams accounted for 20,043 cases, leading to a loss of Rs 1,420 crore to cybercriminals during the same period.[2] The online fraud is classified as

Phishing attacks

Phishing is a scam in which con artists use phony websites, emails, or messages to impersonate trustworthy organizations to obtain private information. To prevent phishing attempts, verify email addresses, avoid dubious links, and employ anti-phishing tools, such as browser extensions and detection software.

Fraud Involving Online Shopping

Online shopping fraud happens when phony websites or dishonest vendors defraud customers into purchasing goods that aren't there. Fraudsters fabricate believable websites or listings and then vanish once they have been paid. To prevent online debit card fraud, use secure payment methods with buyer protection, be cautious of offers that seem too good, and confirm the legitimacy of websites (check HTTPS and read reviews).

Voice Phishing (Vishing)

Vishing is when scammers call people pretending to be bank representatives, government agents, or tech support to obtain personal information, frequently in the form of threats or urgency. Verify the caller's identity, hang up, give the company a call, and use call-blocking apps to identify and stop spam or phishing calls to prevent online transaction fraud caused by vishing.

Attacks by Man-in-the-Middle (MitM)

Man-in-the-middle (MitM) attacks, which frequently use malware or unprotected Wi-Fi, intercept communications between two parties to steal information. Avoid sensitive transactions on public Wi-Fi, encrypt your connection with a VPN, and keep your device's software updated to guard against vulnerabilities to prevent MitM attacks.

Attacks Using Ransomware

Operations are disrupted when ransomware encrypts data and demands a ransom to unlock it. It spreads by taking advantage of software flaws or sending phishing emails. Regular data backups, the use and updating of anti-malware software, and exercising caution when opening email attachments—checking the sender before opening them—can all help prevent ransomware.

Fraud Using UPI

Phishing scams and fraudulent online transactions are examples of UPI fraud. Fraudsters use phony apps or messages to trick users into sharing OTPs or UPI PINs. By using official apps, enabling two-factor

[2] Cyber Frauds in India: Here is how much Indians lost to cyber frauds between Jan and Apr of 2024 | India News - Business Standard

authentication, keeping an eye on your account, avoiding unsolicited calls or messages, and never sharing your PIN or OTP, you can prevent UPI fraud.

4. DIGITAL ARREST

In recent times there has been an uprising in online scams which is happening all over India that is Digital arrest. The scammers Make a call to innocent people and force to stay on video call until their demands are met by threatening them by projecting like government officials, by making various accusations like "we came to know that you had seen child pornography" and "we got a parcel in your name which contains a Drug" 'so we will goanna arrest you if you want to be safe from arrest; you have to pay the sum of amount' likewise they scammed people by projecting them like government officials and also they sent a notice to the victims which is more like a government notice.

As per the report published by the Ministry of Home Affairs, Cybercriminals impersonating police authorities, the Central Bureau of Investigation (CBI), the Narcotics Department, the Reserve Bank of India (RBI), the Enforcement Directorate, and other law enforcement agencies are committing intimidation, blackmail, extortion, and "digital arrests," according to a significant number of complaints filed on the National Cyber Crime Reporting Portal(NCRP). These scammers usually give prospective victims a call and tell them that they have sent or are the intended recipient of a package containing drugs, illegal products, counterfeit passports, or any other type of contraband. Occasionally, they also disclose that a loved one of the victims has been apprehended after being implicated in an accident or crime. To undermine the "case," money is demanded. In certain cases, gullible victims are forced to undergo "Digital Arrest" and make themselves visually exposed to scammers via Skype or another video conferencing platform until their demands are satisfied.To look authentic, the scammers are known to dress in costumes and operate out of studios that are fashioned after government and police stations. Numerous victims have suffered significant financial losses at the hands of these fraudsters.It has been discovered that crossborder crime syndicates are responsible for this coordinated internet economic crime. Under the Ministry of Home Affairs, the Indian Cyber Crime Coordination Centre (I4C) organizes national efforts to combat cybercrime. To combat these scams, MHA is collaborating closely with the RBI, other ministries and their agencies, and other organizations. To identify and look into the cases, I4C also gives State and UT Police Authorities technical assistance and feedback. In partnership with Microsoft, I4C has also blacklisted over 1,000 Skype IDs engaged in these kinds of operations. Additionally, it makes it easier to disable the SIM cards, mobile devices, and mule accounts that these scammers employ. Additionally, I4C has released several notifications via videos and infographics on its "Cyberdost" social media platform for platforms including Facebook, Instagram, X, and others.[3]

PREVENTION AND VICTIMISATION

People must know about these scams and online-related frauds to get rid of the online-based scam wave. As per studies compared to youngsters' old people have become victims of these online-based frauds and scams. People can understand what we will do after becoming a victim of scams or frauds immediately because online crimes are universal. A person from another state even some other countries can able to make fraudulent activity with another person who is in a different place so people must have more awareness about scams and frauds especially how to act quickly after they come to know that they are scammed. The first step of prevention is that we have to use verified apps and shouldn't click the unverified links, should

[3] Press Release:Press Information Bureau

enable the two-step verifications, use masked Aadhar, use of secured connection, etc.,

Review of literature

Tripti Jaiswal(2023) examined how cybercrime affects Indian society and the economy. looked at the different kinds of cybercrimes that are common in India, their effects, and the steps that the government and other stakeholders have taken to counter this threat. The report also identifies the difficulties in combating cybercrime and offers possible solutions to lessen its negative impacts. D. Vijaya Geetha (2011) examined and reviewed the state of phishing attacks in India and offered some defenses that internet businesses can use to fend off such attacks. Dr. P. Arunachalam (2011) dealt with doctrinal research on the economic impact of identity theft in India and explained certain Western instruments. Prof. (Dr.) Sonia Grewal Mahal (2021) the researcher has modestly attempted to draw attention to the growing threat of identity theft in India and the socio-legal ramifications of this widespread crime. Additionally, an effort has been made to propose some pertinent ideas to combat this common crime in India.

Case laws Related to cyber-economic crimes:

Gurugram cyber fraud case (2024): In this case, 21 bank officials were involved in the crime, which involved both public and private bank officials who defrauded Rs.300 crores by opening fake accounts in the bank.

Poona Auto Ancillaries Pvt. Ltd. v. Punjab National Bank (2013): Here, a businessman, whose account was hacked due to scammers jumping on his response to a phishing email, was asked to receive damages from Punjab National Bank courtesy of the Maharashtra IT Secretary. The court concluded that the man himself was the main culprit in falling for the phishing trap, but the bank was mostly responsible because it did not have proper security measures to stop this type of scam. This judgment underlines the need for banks to implement watertight measures related to cybersecurity.

Conclusion

The rapid development of technology in this digital era makes life easier but also brings new threats to human life, such as identity theft, cyber fraud, etc. In this era, everyone should have at least some basic knowledge about privacy and how to keep our personal information safe in cyberspace. Recent steps taken by TRAI make a betterment for laymen, especially old age people but even though there needs to be upgradient and development in cyberspace security and also fasten the process of cyber complaints to get rid of scammers and hackers. Compared to past decades there is rapid development in the field but cyber security in India needs to develop with that. It is concluded that the government has taken steps to make their citizens vigilant and also tries to create the infrastructure in the field of cyber security and technologies that thing is that it doesn't go completely to its citizens.

REFERENCE

1. Privacy and Cyberspace in India: A critical analysis of Justice Srikrishna Committee Report and The Personal Data Protection Bill, 2018 - International Journal of Law Management & Humanities (ijlmh.com)
2. Cyber Frauds in India: Here is how much Indians lost to cyber frauds between Jan and Apr of 2024 | India News - Business Standard
3. Press Release:Press Information Bureau