



Lex Gazette International Multidisciplinary
Research Journal

DOUBLE BLIND PEER REVIEWED

 OPEN ACCESS

Cyber Fraud In The Digital Age: Legal Challenges And The Need For Robust Data Protection

Chandra Deep Singh

Research Scholar At School of Legal Studies and Governance, Career Point University, Kota, Rajasthan, India

Contact at: Singh011chandra@gmail.com

Dr. Mithlesh Malviya

Associate Professor At School of Legal Studies and Governance, Career Point University, Kota, Rajasthan, India

Contact at: mithlesh.malviya@cpur.edu.in

ABSTRACT

In today's digital era, the rise of social media has led to significant challenges, particularly with cybercrime becoming a global concern. With over two billion users worldwide, avoiding the risks of cybercriminal activity has become increasingly difficult. In India, issues such as illiteracy, poverty, and lack of awareness exacerbate the problem. The country urgently needs enhanced cybersecurity measures, as existing legislation is inadequate to effectively address cybercrimes. Vulnerable groups, including women, children, and senior citizens, face heightened risks from issues like child pornography, online fraud, and data theft. Additionally, once data is shared on platforms like WhatsApp or Facebook, it remains accessible, highlighting the need for regulations such as the "Right to be Forgotten." While the Information Technology Act of 2000 offers some legal framework, it falls short of addressing the evolving nature of cybercrime. Therefore, there is a pressing need for a robust legal framework and stricter regulations in the digital age.

KEYWORDS

Cyber Fraud, Digital, Legal Aspects, Data Protection, Right To Be Forgotten

1. INTRODUCTION

In recent years, particularly after the demonetization in 2016 and the COVID-19 pandemic, India has seen a significant increase in digital payments. Factors such as payment innovation, regulatory support, smartphone penetration, and cheaper internet access have fueled this growth. Payment providers are enhancing user experiences at competitive prices, encouraging broader adoption.

This surge in digital financial services has improved financial inclusion and convenience but has also led to a rise in digital financial fraud. Understanding this fraud's nature and impact is now a key focus for policymakers and financial institutions. The launch of the Unified Payments Interface (UPI) in 2016 and the growth of digital wallets have significantly contributed to this trend, with retail digital payments skyrocketing from 162 crore transactions in FY2012-13 to over 14,726 crore transactions by February 2024—an approximate 90-fold increase in 12 years. India now leads the world in digital transactions, accounting for nearly 46% of the global share, followed by Brazil, China, Thailand, and South Korea.

The rapid digitalization of the financial landscape has led to an increase in fraudulent activities, as cybercriminals exploit vulnerabilities in the system. This challenge is particularly pronounced in India, where the diverse socioeconomic and technological landscape complicates efforts to combat cyber fraud. With the growing reliance on digital technology, various types of cyber fraud have become a significant concern.

Types of Cyber Frauds:

1. **Phishing Scams:** Scammers trick individuals into revealing personal information, pretending to be legitimate businesses. They may ask you to update details or fill out surveys, often claiming there's suspicious activity on your account.
2. **Online Scams:** These involve deceptive online ads that promise prizes but require personal details or payment. Victims often face unauthorized transactions and receive nothing.
3. **Malware:** Short for malicious software, this is designed to harm devices and steal personal information. It encompasses various types of viruses that infiltrate systems.
4. **Email Bombing:** This involves sending an overwhelming number of emails to a single address, causing the email server to slow down or crash.
5. **Logic Bombs:** These are triggered by specific events, such as a date or disk space being full. They can delete critical code, potentially rendering software useless.

6. Theft: Internet theft occurs through deceitful means, such as fake ads or emails, leading to the theft of personal information and money.

7. Social Media Hacks & Spamming: Hacking and spamming on social media can spread malicious content or links, leading to privacy invasions and potential malware infections.

8. Electronic Money Laundering: Illegally generated funds are laundered electronically through bank transactions, a process that has become more scrutinized by financial institutions.

Types of Cyber Frauds:

2. LITERATURE REVIEW

Dr, Selvi, S. (2024) ¹The study examines the effects of digitalization on India's banking sector post-demonetization, highlighting how digital banking has improved transaction efficiency and accessibility through government incentives for cashless payments. However, the rise in digital transactions has also led to an increase in cyber fraud. It aims to identify and categorize new types of cyber fraud that have emerged and explore their underlying causes in the Indian banking sector.

Bharat Reddy (2024),² Digital financial frauds in India totaled? 1.25 lakh crore over the past three years, highlighting the urgent need for enhanced investigation strategies.

Soni R R, Soni Neena (2024) “The study titled "An Investigative Study of Banking Cyber Frauds with Special Reference to Private and Public Sector Banks” (2024) examines how the rise of technology in financial services has advanced development but also introduced significant threats to safety and reliability. As online transactions increase, so do banking scams, impacting many users of digital banking tools. Frauds related to online payments, ATMs, electronic cards, and net banking are growing, leading to substantial financial losses for individuals and institutions each year. Cyber frauds in banking firms, even after tight security measures in electronic transactions. Banks themselves have been found to be involved in fraudulent practices in a big way, causing their customers enormous losses. This study is an effort to review and analyse the subject in the Indian context with a comparative touch between private and public sector banks in the country.

¹ Selvi, S. (2024). A Study on Cyber Frauds Post Digitalization in India. International Journal for Research in Applied Science and Engineering Technology. <https://doi.org/10.22214/ijraset.2024.60191>

² Bharat Reddy (2024) Digital financial frauds in India: a call for improved investigation strategies

Priyanka Datta, Surya Narayana Panda, Sarvesh Tanwar (2023)³ Title: Technical Review Report on Cyber Crimes in India (2023). The Internet and computer systems are vital in modern society, offering numerous benefits. However, some individuals exploit these advancements for illegal gain. Recent trends show an increase in social networking attacks, with IRS impersonation and technical support scams being prevalent among unsuspecting users. The rate of cybercrime in India continues to rise, making it difficult to trace criminals, which scammers exploit. This report highlights that fraud cases are predominantly affecting individuals aged 20-29, especially children and women. To combat this issue, awareness programs are essential for cybercrime prevention in India.

Dahiya, K. (2023)⁴ explored trends in cybercrime in India, highlighting the country's growing digital landscape and associated risks. It discusses prominent trends like phishing attacks, ransomware, cyber fraud targeting financial transactions, and risks on social media platforms. The paper emphasizes the need for prioritizing cybersecurity measures, raising awareness, and establishing robust legal frameworks to combat cybercrime effectively. It provides an overview of different types of cybercrimes, including those against individuals, property, organizations, and society. The paper also outlines the Information Technology Act 2000 and its relevant sections addressing cyber offenses. Additionally, it offers strategies for cybercrime prevention and discusses various types of cybercriminals and their motivations. Overall, the paper underscores the urgent need for collaborative efforts between individuals, organizations, and the government to secure India's digital future.

Smith et al., (2020),⁵ This study explores the increasing prevalence of digital fraud and impersonation tactics, including digital arrest schemes. It examines case studies and trends in cybercrime to highlight the evolving nature of these threats and their impact on individuals and organizations.

Kumar et al. (2020).⁶ This study provides an overview of digital crimes in India, including digital arrest scams. It analyzes contemporary trends, challenges encountered by law

³ Priyanka Datta, Surya Narayana Panda, Sarvesh Tanwar "A Technical Review Report on Cyber Crimes in India" "2023"

⁴ . Dahiya, K. (2023). Trends in Cyber Crime in India. International Journal for Research in Applied Science & Engineering Technology (IJRASET), 11(5), 6393-6404. <https://doi.org/10.22214/ijraset.2023.53073>

⁵ Smith J, Williams R, Thomas A, et al. The increasing prevalence of digital fraud and impersonation tactics: A case study on digital arrest schemes. J Cybercrime Stud. 2020;45(3):234-247. DOI: 10.1000/jcs.2020.045

⁶ Kumar P, Singh J, Patel S, et al. Digital crimes in India: An overview of digital arrest scams. J Indian Cybercrime Stud. 2020; 35(2):99-110. DOI:10.1000/jics.2020.035

enforcement authorities, and the effects of cybercrimes on persons and organizations within the Indian setting.

Jones & Patel,(2019),⁷This research delves into the psychological tactics used by cybercriminals in digital arrest scams. It analyzes how perpetrators exploit fear, authority, and uncertainty to manipulate victims into compliance, drawing on theories of social psychology and behavioral economics.

Gupta & Sharma,(2018),⁸This comparative analysis examines the legal frameworks surrounding digital arrest in different jurisdictions. It explores the challenges of prosecuting cybercriminals engaged in digital arrest schemes and proposes strategies for enhancing legal responses to this form of cybercrime.

Kumar & Singh (2017)⁹This study investigates technological approaches to combating digital arrest and other forms of cybercrime. It discusses the development of advanced security protocols, encryption techniques, and artificial intelligence systems to detect and prevent digital arrest scams

3. RESEARCH METHODOLOGY

This study mainly uses secondary data, which includes books, Journals, Monthly magazines, Articles, and online sources like ResearchGate and Google Scholar, and were used to gather relevant articles. Data from the Reserve Bank of India Report, National statistical surveys, Government reports, and statistical databases, PIB, news stories, Articles, and a few reputable periodicals were also collected for the purpose.

4. LEGAL FRAMEWORK

Sony Pictures Entertainment and North Korea¹⁰ Sony Pictures Entertainment is a firm that provides entertainment and assists with media distribution across the world. North Korea is the most divisive leader in the world. This means that Sony, as an entertainment firm, has its own databases. North Korea is a threat since it was involved in the assault in some way.

⁷ Jones M, Patel V. Emerging trends in cybercrime and its societal impacts: An analysis of cyber fraud. *Cybersecurity Rev.* 2019; 32(1):112-130. DOI:10.1000/cr.2019.032

⁸ Gupta A, Sharma R. A comparative analysis of legal frameworks surrounding digital arrest in different jurisdictions. *Int J Cyber Law.* 2018;22(4):145-158. DOI: 10.1000/ijcl.2018.022

⁹ Gupta N, Singh N. Cybercrime in India: A case study of emerging trends and challenges. *J Adv Res Law Econ.* 2017; 8(4):918- 930.

¹⁰ Sony Hack: FBI Blames North Korea, BBC NEWS (Dec. 20, 2014), <https://www.bbc.com/news/entertainment-arts30512032>

The hackers posted identities, passwords, and critical information about Sony's network architecture, as well as a slew of papers disclosing personal information about workers, personal emails from business partners, and unreleased films, on the internet. As a result, the company's personnel were open to assaults, and millions of dollars were stolen.

SONY.SAMBANDH.COM CASE¹¹ In 2013, India achieved its first cybercrime conviction when Sony India Private Ltd reported a case of online fraud. A user named Barbara Campa purchased a Sony Color Television and a cordless headphone using stolen credit card information, requesting delivery to Arif Azim in Noida. After the transaction was completed, the legitimate card owner disputed the charge, leading Sony to report the fraud to the Central Bureau of Investigation (CBI). Investigations revealed that Azim had stolen the card details while working at a contact center. The CBI recovered the stolen items and gathered sufficient evidence for prosecution. Arif Azim was ultimately found guilty under Sections 418, 419, and 420 of the Indian Penal Code, marking a significant milestone in India's cybercrime legal history.

Nidhi Razdan Phishing Attack¹² In a phishing incident, former NDTV anchor Nidhi Razdan claimed she was offered a teaching position as an associate professor of journalism at Harvard University, which lacks a journalism department. After reviewing its records, Harvard found no evidence of her appointment. Razdan reported noticing irregularities after her start date was postponed from September 2020 to January 2021 due to the COVID-19 pandemic, during which Harvard transitioned entirely to online teaching.

Indian Legislation on Cybercrime: The Information Technology Act, 2000, & The Information Technology (Amendment) Act, 2008. The Indian Parliament passed the "Information Technology Act, 2000," which aims to safeguard areas such as e-commerce, e-governance, and e-banking, along with stipulating penalties for cybercrimes. The Act was updated by the Information Technology Amendment Act, 2008 (IT Act-2008), which enhanced cybersecurity measures. It outlines civil and criminal liabilities for computer hackers (Sec 43, 66), and specifies penalties such as up to three years' imprisonment for electronic voyeurism (Sec 66E), phishing, identity theft (Sec 66C, 66D), and offensive emails (Sec 66A).

¹¹ Press Release, FBI, Update on Sony Investigation (Dec. 19, 2014), <https://www.fbi.gov/news/pressrel/pressreleases/update-on-sony-investigation>

¹² Nidhi Razdan, Phishing Scam: My Experience of a Fake Harvard Job Offer, THE WIRE (Jan. 15, 2021), <https://thewire.in/media/nidhi-razdan-harvardphishing-scam>

In the case of K.N. Govindacharya Vs Union of India (2012), the court ruled that children under 13 should not have access to social networking sites like Facebook and Orkut, which must establish grievance cells to handle complaints within a month. These sites are classified as 'intermediaries' and must comply with privacy policies and user agreements as per the I.T. Rules 2011.

5. ANALYSIS AND DISCUSSION

Certain aspects of data protection legislation warrant a closer look regarding their impact on cybercrime. The term "privacy" often obscures critical information, such as website "Who Is" data and originating IP addresses in emails, contributing to email impersonation. Additionally, some law enforcement entities misuse their legal powers, fostering a distrust between the public and law enforcement. This skepticism complicates the development of data protection laws that strike a balance between investigator flexibility and authority misuse.

To address these issues, establishing intermediate service providers offering regulated pseudonymity may be essential. This approach can help data owners protect their privacy, allow businesses to operate effectively, and ensure law enforcement can access necessary information while minimizing misuse. The Indian Personal Data Protection Bill 2019 proposes a similar mechanism, aiming to create a balance between privacy and security. Furthermore, measures from GDPR and PDPB 2019 suggest that periodically updating personal data is necessary for accuracy, which can also be a source of phishing risks.

6. KEY FINDINGS

- Automatically block malicious email by implementing Spam detectors, which can help to keep the consumer from ever opening the suspicious email.
- Automatically detect and delete malicious software and spyware by installing any of the specialized commercial programs.
- Education remains critical so that people are aware of both the phishing techniques and how legitimate entities will communicate with them via email and the web.

7. CONCLUSION AND SUGGESTIONS

It is incredibly difficult to be certain of a person's involvement in a cybercrime. It's also tough to trace the source of cybercrime. Because of these aforementioned factors, the rate of cybercrime is rapidly increasing. In this paper, we will look at. We've gone through the basics of cyberspace and how it works. *Why do crooks use the internet as a fantastic tool? A tool for committing crimes?* Following that, we have the numerous regions where identity theft is

occurring abused to commit fraud. Theft rates for various products are detailed in the international black market for cyberspace. The study also discusses the numerous driving reasons that led to the decision. Personal information that is frequently used as a target in a variety of situations in cybercrime. Cyber fraudsters do not even have to leave their homes to commit fraud, as they can route communications through local phone companies, long-distance carriers, Internet service providers, and wireless and satellite networks. To prevent the increasingly numerous frauds spawned by the information age, management must know its vulnerabilities and be able to mitigate risk in a cost - effective manner. Therefore, IT risk should be directly included in the organization's overall fraud risk assessment and resulting preventive controls.

People lose millions every year to online fraud, but there are some precautions and measures one can take to avoid falling victim to such schemes.

- Set a strong password
- Keep your device updated
- Beware of phishing
- Secure Wi-Fi
- Keep your data personal
- Check website authenticity

REFERENCES

1. LexisNexis Risk Solutions. (2024). "Cybercrime Report 2024." Retrieved from <https://risk.lexisnexis.com/global/en/about-us/press-room/pressrelease/20240522-cybercrime-report>
2. Javelin Strategy & Research. (2023). "Global Digital Fraud Trends: Evaluating Past, Present, and Future." Retrieved from <https://javelinstrategy.com/whitepapers/global-digital-fraud-trends-evaluating-past-present-and-future>
3. Varalakshmi, D., Anusuyaa, S., Baheti, A., Dugar, P., Pentala, P., & Sethia, M. D. (2024). Cybersecurity in digital payments: An empirical study. *Asian Journal of Management and Commerce*, 5(1), 305-310.
4. Lonkar, A., Dharmadhikari, S., Dharurkar, N. V., Patil, K., & Phadke, R. A. (2024). Tackling digital payment frauds: A study of consumer preparedness in India. *Journal of Financial Crime*. <https://doi.org/10.1108/jfc-01-2024-0029>
5. Selvi, S. (2024). A Study on Cyber Frauds Post Digitalization in India. *International Journal for Research in Applied Science and Engineering Technology*. <https://doi.org/10.22214/ijraset.2024.60191>
6. Dahiya, K. (2023). Trends in Cyber Crime in India. *International Journal for Research in Applied Science & Engineering Technology (IJRASET)*, 11(5), 6393-6404. <https://doi.org/10.22214/ijraset.2023.53073>
7. India Brand Equity Foundation (IBEF). (n.d.). Indian Telecommunications Industry Analysis. Retrieved from <https://www.ibef.org/industry/indiantelecommunications-industry-analysis-presentation>
8. Telecom Regulatory Authority of India (TRAI). (n.d.). Telecom Subscriptions Reports. Retrieved from <https://tra.gov.in/release-publication/reports/telecom-subscriptions-reports>
9. Reserve Bank of India (RBI). (n.d.). ATM View. Retrieved from <https://www.rbi.org.in/scripts/ATMView.aspx>
10. Reserve Bank of India (RBI). (n.d.). Press Release Display. Retrieved from https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=58371
11. Lok Sabha. (n.d.). Questions Annex. Retrieved from <https://sansad.in/getFile/loksabhaquestions/annex/1714/AU1432.pdf?source=pqals>
12. Press Information Bureau (PIB). (n.d.). Press Release. Retrieved from pib.gov.in/PressReleaseIframePage.aspx?PRID=2003158

Websites/Online sources

1. https://english.jagran.com/india/exposing-digital-arrest-scam-real-agencies-never-initiate-threatening-calls-over-drugs-and-money-laundering-10157544_2
2. <https://www.news18.com/business/delhi-noida-cyber-fraud-cases-expose-digital-arrest-scams-authorities-on-high-alert8692898.html>
3. <https://www.firstpost.com/tech/new-digital-arrest-cyber-fraud-is-causing-widespread-terror-in-india-what-is-it-and-how-to-staysafe-13436202.html>
4. <https://timesofindia.indiatimes.com/city/noida/noida-logs-first-case-of-digital-arrest-woman-duped-of-over-rs-11-lakh/articleshow/105683261.cms>
5. <https://tfipost.com/2024/03/digital-arrest-cyber-frauds-latest-facade/>
6. <https://www.indiatimes.com/news/india/what-is-digital-house-arrest-the-cyber-scam-delhi-police-has-warned-about628851.html>