Advances in Consumer Research
https://acr-journal.com/
Volume-2 | Issue-6 | Dec 2025

Original Researcher Article

Unveiling Digital Deceptions: A Holistic Analysis of Online Frauds in India and the Role of Cyber Law

Mariya Khan[1], Sunil Kumar Sharma[2]
[1,2]Institute of Legal Studies & Research, Mangalayatan University, Beswan, Aligarh, Uttar Pradesh-202146
Email ID : 20221414_mariya@mangalayatan.edu.in[1] , sunil.sharma9590@mangalayatan.edu.in[2]

ABSTRACT

Due to India's massive population of 900 million internet stoners and wide digitalization, multitudinous openings have arisen; still, it has also given rise to multitudinous internet- related frauds including UPI frauds, identity thefts, phishing, and multitudinous further. This paper discusses the emergence of internet fraud in India by recognizing the different types of frauds, and how these types of frauds may be viewed in terms of laws regulating technology (i.e., Information Technology Act, 2000). It also discusses statistical trends as well as individual frauds including expert and academic opinions to punctuate obstacles that enforcement agencies face, including gaps in the legislative architecture and the critical need for awareness schemes and technological advancement. This paper propose a three- rounded approach to regulate frauds in India more regulations, better policing and better stoners to help secure India's digital future from these growing complaints..

Keywords: Online Frauds, Cybercrime, India, Cyber Laws, Information Technology Act, Phishing, Identity Theft, Digital Knowledge, Data Protection and Ai- Predicated Frauds.

1. INTRODUCTION:

Dramatic advances in technology have changed many forms of communication, business and negotiations in India with the arrival of services to connect around 900 million users to the internet in the country in 2024, as indicated by the Telecom Regulatory Authority of India (TRAI). Cybercrime continues to reflect a serious part of India's growing internet services, with the increase of online fraud posing a very serious threat to the public concrete cybersecurity infrastructure of the country. In 2023, the Indian Cyber Crime Coordination Centre (I4C) reported approximately seven lakh-fifty thousand complaints of cybercrimes, mostly related to various forms of financial fraud. The alarming growth rate of fraud related crimes via connected internet services bring meaningful questions with regard to the success of our legal frameworks and policies against those destructive actions. This research covers the complex phenomena of online fraud in India through an examination of the information Technology Act of 2000, the central legislation and foundational legislation of India's cyber law framework. The discussion covers the categorization of online frauds, the incidence of fraud in Indian society, the socio-economic dimensions of the fraud as well as the responsiveness of institutions, regulations and laws today in 2023. The research highlights the habitual impact of cybercrimes on the lives of citizens.

The Digital Boom and the Rise of Frauds

India's Digital Leap:-

India's narrative about digital is exciting. We're in the process of growing from 400 million Internet users in 2016 to more than 900 million by 2024, we are all interconnected. UPI has turned our phones into ATM machines, with transactions soaring to ₹200 trillion in 2023 (NPCI). The revolution is coming to rural India where my neighbour's uncle in a small village, with a limited knowledge of the Internet, was able to use PhonePe to send payment for groceries. However, like all good things, this connectivity also can be problematic. In our case of scamming India, it would appear the common denominator is: 1.4 billion people distributed across tech novice spatially and urban tech specialist region, and trusting a so-called "bank officer" far too optimistically.

What is the common denominator level of vulnerability?

While the uptick in scams may suggest not only population ratio, there is also generational exposure to scams. Many aspiring scammers are new to the Internet, especially in rural India who needs to learn their usage of the Internet and cycle into a culture of digital transactions. Recognizing the Internet in one context is far behind awareness. Scammers have simply identified an easy and increasingly talented technique for social engineering in the form of calling experts, urgency text messages for bank peoples, and very peripheral issues like an offer that sounds too good to be true.

Types of Online Fraud in India

Online fraudsters employ several tactics to target their victims. Some categories of online fraud in India are:

Phishing Scams

- Fraudsters impersonate real companies like banks or e-commerce websites via emails, SMS, or spoof websites to con people into revealing personal or financial information.

- Even the Indian Government has warned the public of fraudulent emails pretending to be from the Indian Cyber Crime Coordination Centre (“I4C”). These fraudulent e-mails were meant to mislead recipients into believing they were from a real cybercrime tracking organisation which could result in the loss of financial or personal data.

UPI (Unified Payments Interface) Fraud

- Fraudsters are now exploiting the widespread usage of the Unified Payments Interface (“UPI”) to trick victims into sharing their UPI PIN or authorizing unauthorized transactions.

- Approximately half of India’s cybercrimes since 2020 were for the UPI. The escalation in UPI fraud has significantly heightened as more people lean toward digital transactions due to the COVID pandemic.

- Fraudsters will trick victims into sharing their UPI PIN, or OTP, or will have them remote assistance to download a remote access app giving fraudsters access to their devices and online financial accounts.

Credit Card Fraud

- Employees may fall victim to credit card fraud which occurs whenever a Credit Card number is skimmed or phished for unauthorized online purchases.

- Virtual credit card scams usually target unsuspecting individuals who rely on digital financial transactions to steal their money.

- These schemes usually attempt to create fraudulent virtual credit cards/fraud virtual credit card details to make unauthorized purchases.

- Phishing techniques may also be used to entice users into sharing their virtual card information.

Fake Delivery OTP Scam

- Crooks often impersonate delivery companies by asking for a One-Time Password (OTP) under the guise of delivery completion.

- Bank accounts are then accessed with the retrieved OTPs.

- In India, fake OTP delivery scams are designed to prey on online consumers and typically involve offenders posing as a delivery agent from a major e-commerce vendor such as Amazon or Flipkart.

- The scammer obtains the OTP as part of getting the victim to verify or complete a delivery. If the OTP is stolen from the victim, the nefarious actors will clone the victim’s phone and can extract sensitive information, culminating in theft of funds.

The Human and Economic Consequences

The Actual Cost

I4C (Indian Cybercrime Coordination Centre) reported that cyber scams robbed Indians of ₹12,000 crore in 2023, with UPI scams representing a large amount of that figure. But there is also cost beyond dollars. Think of a nurse who was conned by a UPI request and lost all of her savings. Small firms were also victims of scams. Fake QR codes or vendor scams may cost a small business months of earnings. I’ve even heard of a cafe owner in Kolkata who was victimised for ₹80,000 to a “supplier” who did not send anything.

Emotional and Social Fallout

The emotional impact is immense anguish. Victims are regretful and often do not confess it. One neighbour lost ₹30,000 to a UPI scam and waited for weeks to admit it because he was worried people would laugh at him. The fraudster expects this behaviour and this determines his illegal livelihood, the stats required to support his crime don’t reflect the true reality of the crime. Society also pays in trust. Whenever someone says they “do not trust UPI or online shopping”, that holds back India’s digital economy growth. Technophobes in rural areas return to cash and stick.

India’s Cyber Laws: The Legal Challenge

The Information Technology Act, 2000 (Amended) The Information Technology (IT) Act is a warrior on cybercrime in India, introduced in 2000 and then amended in 2008 to protect the country from digital threats. It is the law for cyber frauds which includes the following **relevant provisions:**

Section 66: This section punishes hacking or unauthorized access, creating a punishment of imprisonment for 3 years or a fine of ₹ 5 lakh. This section is very broad in nature as it deals with everything from data breaches to UPI frauds whereby credentials have been stolen.

Section 66C: It punishes for identity theft (for example, if someone uses your Aadhaar to extract a loan), and is punishable with 3 years prison and a fine of ₹ 1 lakh.

Section 66D: This section punishes cheating by impersonation, examples being phishing or UPI frauds where fraudsters impersonate bank representatives. The punishment is up to 7 years imprisonment and a fine of ₹ 7 lakh.

Section 43A: This section punishes a corporation for failure to provide reasonable security to protect user data, it is necessary for platforms like UPI apps.

Section 67C: This section obligates intermediaries (e.g., banks, apps) to hold onto the data, thereby helping investigations.

The IT (Information Technology) Act was a watershed moment for India as it gave it a framework to pursue cyber criminals at a time when the country was still transitioning from dial-up to high speed internet. It provided powers to authorities to seize devices trace IP addresses and freeze accounts. IN cases of UPI frauds, the IT Act is often invoked alongside **Section 66D** to punish the fraudster for impersonating merchants or acting on behalf of a bank official on a UPI transaction. Written before the generation of smartphones, the scams in this text cannot compete with scams against today, like phishing, bot scams or QR scam frauds. Phishing is when a scammer poses as a real organization to get money or personal/ identifying information. “Smishing” scams (SMS based UPI scams) are also in the mix here, and this once again is a grey area, - there are no clear provisions on what these scams fall under, so it puts prosecutors on the spot to stretch **Section 66D** to charge someone. Enforcement issues abound as well; the courts are inundated with a backlog of cases, and digital evidence records and transaction logs seem to disappear quickly, or are not maintained. They also have limited helpful information to provide compensation to the victims under the Act, where hey, interestingly enough, a victim can win a case under the Act; however, if they received their money back, that’s a different story! Well, while the Act has at least made a provision that they must consider and build in securing consumer data, many UPI Apps are essentially left with unpatched exposure to fraud, often due to poor verification processes in place for who they grant access to.

Other Legal Mechanisms

Indian Penal Code (IPC): Sections like 420 (cheating) and 465 (forgery) are frequently invoked in cyber fraud. The Reserve Bank of India has established its own guidelines to improve the situation. This includes ensuring that banking users must have two-factor authentication for payments, and that banks must have a fraud reporting procedure.

Consumer Protection Act, 2019: The act gives e-commerce platforms the responsibility of ensuring that the products or services sold are not false or fake; Digital Personal Data Protection Act, 2023: The newest in the bunch, it aims to protect user data; however, its rules are still being developed.

The National Cyber Crime Reporting Portal: allows a complaint can be made online and provides you with the link to the cybercrime cell. There is a "1930" helpline number connects you to the cell. These are good furniture for the current situation but they need to be more holistic.

Obstacles in Enforcement and Legislation Enforcement Issues

The primary challenge:-

Enforcement - Cybercrime cells are under-resourced, and many police stations also lack the technical skills needed to assist investigations with digitally stored evidence. A case can take years before an outcome is achieved; fraudsters often operate abroad, conceal their details behind VPNs or fake identities, and crossing borders means coordination across agencies that can be a logistical circus – try getting a government agency in another country to follow-up on cybercrime for a scam of ₹50,000.

Legislation Gaps - While the IT Act carved the path forward with regard to cyber offences and online technology, it was not designed to meet current threats. Deep fakes, AI-powered phishing, and crypto scams hardly fit into the Act as written.

Victim compensation is also a grey area – in the case of many physical crimes, recovery of funds is not a real possibility so this is common in a cybercrime environment. The DPDP Act promises improvements with regard to data privacy protections but is still untested, and compliance is intermittent.

Awareness Gap Campaigns-by the government to educate and raise awareness about online safety (like “Cyber Dost” but so far have had no meaningful impact. Rural users, first time internet users and small business have specific needs and vulnerabilities that we need to help them with – awareness and education must be tailored to their mini digital journeys. There is a need for banks to understand how to better assist their customers prevent fraud and cybersecurity issues as well. Attaching blame to the customers for “sharing OTPs” ignores potential lapses that banks may have.

The Way Forward: Solutions and Recommendations

So, what’s The Solution?

Here’s how I see it:

Enhancing Enforcement: More cyber - trained police officers and better working together of banks, technology companies, and police. Bring investigations of smaller frauds to a quicker level where scammers don’t want to scam for relatively small amounts of money.

Change the IT Act: Add provisions for AI scams, deep fakes, and crypto frauds in the updates. Also, ensure there are clear considerations for victim compensation.

Promoting Awareness: Be more clever than posters. Use short and catchy videos, in regional languages, school workshops, social media campaigns led by local influencers, and other ideas to get to millions of people. RBI’s fraud alerts need a refresh-a new approach and more appealing than a catchy jingle or an advertisement, still unclear how to do that.

Update Technology: Banks and e-commerce platforms should be looking to use AI to identify unusual transactions in real- time. Of course these will require sufficient and appropriate framework for acceptable rules and regulations that protect the privacy of users too.

Making Users More Empowered: Promoting passwords, VPNs, URL checkers and other tools for digital safety. Make reporting non-stigmatizing and simple.

Case Studies: Real Stories, Real Lessons

The UPI Scam - A Delhi shopkeeper lost ₹1 lakh (1 lakh = $1200) when he scanned a fake QR code provided by a "delivery agent". This happened to be the cause which brought into the need for issue based transaction alerts and merchant prompts.

The Crypto Trap - As a Pune engineer contributed ₹5 lakh into a Telegram-based "crypto fund" promising 200% returns, the group suddenly disappeared from the app, leaving police to trace the scam on a block chain and demonstrate what gaps in crypto regulation are becoming all too evident.

The Phishing Nightmare - a retiree from Chennai which gave out an OTP to what they thought was their bank became a victim of a loss which totalled to lakh. When it came time to apply for a refund, the bank did not reimburse due to customer/user error. As a result of the above scenarios, the fundamental principles of liability remain undecided.

These stories are not merely cautionary tales, but calls to action!

Global Context

India is not isolated in this process. According to the FBI's Internet Crime Complaint Centre statement for 2023, the total global loss due to cyber fraud was $12.5 billion in 2021; phishing scams and fake investment scams were two of the three top scams. India certainly has its unique challenges to address in combating fraud including sheer size, digital illiteracy and enforcement challenges but it also has the same attributes that make it an attractive fraud market. There could also be some fraud insights that could be useful from other jurisdictions, such as Singapore (real-time detection) or the EU (regulatory framework with strong data stipulations) and there are some possible global approaches but whatever, and however, this systemic issue is address it must acknowledge India's unique and diverse context.

2. CONCLUSION

The ubiquitous nature of online fraud, especially in the form of many UPI scams, is a human problem, and has been eroding trust and manipulating the loopholes in our law. The IT Act is doing what it can, but is a fighter from 2025, without the tools that go with it. Awareness of fraud or enforcing the law can both be enhanced, but the ingenuity of the fraudsters is nonetheless infuriatingly clever while we watch. While the solution is not easy, it is not impossible: modernize the IT Act, train potential cyber police staff, and instil the awareness of UPI safety. The rest is for us to sort out: check that QR code! Guard that PIN! Report that fraud! India is a beautiful and cherish able digital dream, but it can only remain so if we prevent the tricks from taking centre stage.

.

REFERENCES

1. Indian Cyber Crime Coordination Centre. (2023). Annual report 2023. Ministry of Home Affairs, Government of India.
2. Telecom Regulatory Authority of India. (2024). Internet subscriber data 2024. Telecom Regulatory Authority of India, Government of India.
3. National Payments Corporation of India. (2023). UPI transaction report 2023. National Payments Corporation of India.
4. Reserve Bank of India. (2024). Cyber fraud guidelines 2024. Reserve Bank of India. The Government of India. (2000). Information Technology Act, 2000. Ministry of Law and Justice, Government of India.
5. The Government of India. (2023). Digital Personal Data Protection Act, 2023. Ministry of Law and Justice, Government of India.
6. FBI Internet Crime Complaint Centre. (2023). 2023 Internet crime report. Federal Bureau of Investigation, U.S. Department of Justice.
7. Duggal, P. (2020). Cyber frauds, cybercrimes & law in India [eBook].
8. Fatima, T. (2023). Cyber crimes (3rd ed.). Eastern Book Company.
9. Mali, P. (2019). Cyber law & cyber crimes simplified. Cyber Info media Pvt. Ltd

.