Educational Administration: Theory and Practice
2024, 30(6), 1700-1704
ISSN: 2148-2403
https://kuey.net/

Research Article

Case Study: Unmasking A Cyber Financial Fraud

Dr. Devi Premnath[1*], Dr. M. Balathandayuthapani[2]

[1*]Professor,Jansons School of Business, devipremnath@jsb.ac.in
[2]Professor, Jansons School of Business, bala@jsb.ac.in

Citation: Dr. Devi Premnath, Dr. M. Balathandayuthapani (2024), Case Study: Unmasking A Cyber Financial Fraud , Educational Administration: Theory and Practice, 30(6), 1700-1704
Doi: 10.53555/kuey.v30i6.5573

ARTICLE INFO

ABSTRACT

Prof. D, a management school professor in Coimbatore, Tamil Nadu, has always maintained a cautious approach toward social media, keeping her private life separate from her professional endeavors. Despite not having an Instagram account, she unexpectedly found herself entangled in a cyber financial fraud scheme. The situation escalated when Naveen, one of her former students, urgently contacted her. Naveen revealed that an impostor had created a fraudulent Instagram account using Prof. D's name and profile picture. The impostor was soliciting money from Prof. D's current and former students, claiming urgent financial need. This scam not only jeopardized the students' funds but also posed a threat to Prof. D's reputation and trustworthiness

The Case

Prof D, a professor working in a management school in Coimbatore, Tamil Nadu, had always been wary of social media. She preferred to keep her private life separate from her professional endeavors and, as a result, did not have an Instagram account. However, one evening, she found herself unexpectedly embroiled in a cyber financial fraud scheme that targeted her and her former students. Prof. D received an urgent call from Naveen, one of her old students. Naveen informed her that a fraudulent Instagram account had been created using her name and profile picture. The impostor was reaching out to her current and former students, asking them to transfer money via Google Pay (GPay) to a bank account, under the pretense of needing urgent financial help. Prof. D was shocked and immediately understood the potential repercussions. This scam not only put her students at risk of losing their money but also threatened her reputation and trustworthiness.

Without wasting any time, Prof. D. promptly reported the fake profile to Instagram, detailing the impersonation and fraudulent activities being conducted under her name. Her husband immediately registered a formal complaint in the Cyber cell by providing all the necessary details, including screenshots of the fake profile and messages sent to her students. Understanding the urgency of the situation, she posted an alert message on her Facebook profile, warning her friends about the scam. She also updated her WhatsApp status with a similar warning to ensure maximum reach. The professor then reached out to her students via WhatsApp, explaining the situation and requesting their help in reporting the fraudulent account. Her students, appreciating her transparency and quick action, immediately rallied to her support. She changed all her bank account passwords and updated her security verification to a two-level authentication process to prevent any unauthorized access.

Prof D's students quickly spread the word through their common groups and personal networks. They reported the fake account en masse to Instagram, flagging it as fraudulent. Within a short period, the fake profile was inundated with reports, significantly increasing the chances of its swift removal. Thanks to the collective effort of Prof. D, her family, and students the fake Instagram account was taken down within 24 hours. The cyber cell initiated an investigation into the bank account details provided by the fraudster, aiming to trace and apprehend the perpetrator.

A Closer look into the cybercrime

Britannica defines cybercrime as "the use of a computer as an instrument to further illegal ends, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy." The term was first coined by Sussman and Heuston in 1995 and is best understood as a collection of actions rather than a single term. These actions involve offenses that impact computer systems or data. Anderson & Gardener (2015) support this definition, stating, "Cybercrimes are criminal acts implemented through the use of a computer or other forms of electronic communications." David S. Wall (2007) further elaborates that cybercrimes are networked crimes, distinct from those simply using computers. According to

Wall, "Cybercrimes are criminal or harmful activities that are informational, global, and networked. They result from networked technologies that have transformed the division of criminal labor, creating new opportunities and forms of crime, often involving the acquisition or manipulation of information across global networks for gain. These can be divided into crimes affecting the integrity of the system, crimes facilitated by networked computers, and crimes related to the content of computers."
Cybercrimes come in various forms, with the most common being hacking, phishing, malware attacks, and identity theft. Hacking involves compromising digital devices and networks through unauthorized access. Phishing, as defined by IBM's Matthew Kosinski, is a social engineering scam that manipulates victims using fake stories and pressure tactics, exploiting human error rather than directly targeting networks and resources. Malware, short for malicious software, includes intrusive software designed by cybercriminals to steal data and damage or destroy computer systems, with examples such as viruses, worms, Trojan viruses, spyware, adware, and ransomware, as explained by CISCO. Identity theft involves stealing personal data like names, addresses, and social security numbers to fraudulently assume someone's identity.
As per the report from The Economic Times, Indians have lost Rs 1700 crores from January 2024 to April 2024 to cyber fraud. The number of cybercrimes getting reported in India is expanding exponentially.
Table 1 reveals the trend in growth of number of cybercrimes being reported in India in the last 5 years.

Cybercrime cases in the last 5 years.

S.No	Year	Cases
1	2019	26049
2	2020	257777
3	2021	452414
4	2022	966790
5	2023	1556218

Cost of cybercrimes to India and the world economy.

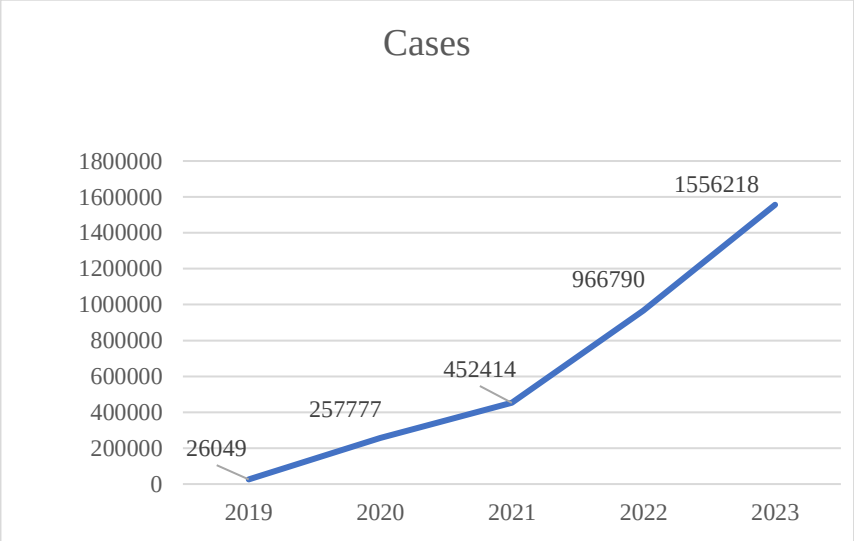

FIGURE -1
Source: Business Standard

According to The Times of India, a staggering Rs 10,319 crore was lost to online fraud across the country between April 2021 and December 31, 2023. The global cost of cybercrime is equally alarming. Steve Morgan of Cybercrime Magazine states, "Cybersecurity Ventures expects global cybercrime costs to grow by 15 percent per year over the next five years, reaching USD 10.5 trillion annually by 2025. If it were measured as a country, the cost of cybercrime would represent the third largest economy after the USA and China."
In India, financial cybercrimes have surged with the widespread adoption of UPI (Unified Payments Interface) across the nation. A report by Business Standard on financial cyber frauds in 2023 reveals that five states account for more than 50% of the reported cyber fraud cases in the country.

Cyber Financial Frauds in India: A Snapshot

• **Financial Fraud Dominance**: From January 2020 to June 2023, over 75% of cyber crimes in India were related to financial fraud. These encompassed various deceptive activities, including online payment scams, identity theft, and investment fraud.

• **UPI and Internet Banking Scams**: Nearly 50% of these cases were linked to UPI (Unified Payments Interface) and Internet banking. Cybercriminals exploit these digital payment systems' vulnerabilities to siphon off funds from unsuspecting victims.

• **Staggering Losses**: According to the National Crime Records Bureau (NCRB), cybercrimes in India during 2023 resulted in a staggering loss of ₹66.66 crore across 4,850 reported cases**.** However, a recent report by the Indian Cyber Crime Coordination Centre (I4C) revealed that digital financial frauds accounted for an astonishing ₹1.25 lakh crore over the last three years.

Challenges and Solutions:

• **Awareness**: Lack of awareness about cyber hygiene remains a significant challenge. Educating individuals and businesses about safe online practices is crucial.

• **Infrastructure**: Improving the infrastructure and processes for tackling cybercrime cases is essential. The Indian government has allocated resources to enhance cybersecurity efforts, including strengthening the Indian Computer Emergency Response Team

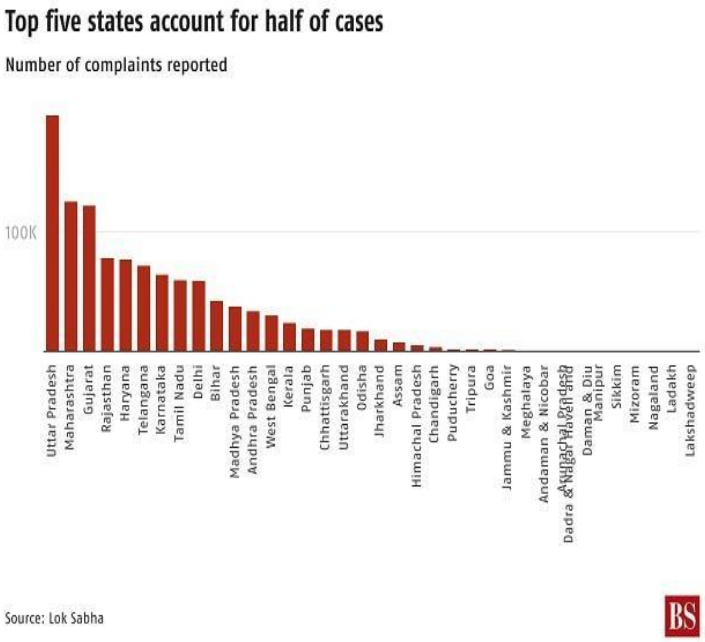

Figure 2: Financial fraud cases – state-wise registration for the year 2023

These 1.13 million cases had an amount involved of Rs 7,488.6 crore. The maximum amount was Rs 990.7 crore in Maharashtra. Telangana followed with Rs 759.1 crore. Next were Uttar Pradesh (Rs 721.1 crore), Karnataka (Rs 662.1 crore) and Tamil Nadu (Rs 661.2 crore). Lakshadweep had the least amount involved at Rs 0.2 crore (chart 2). Figure 3.

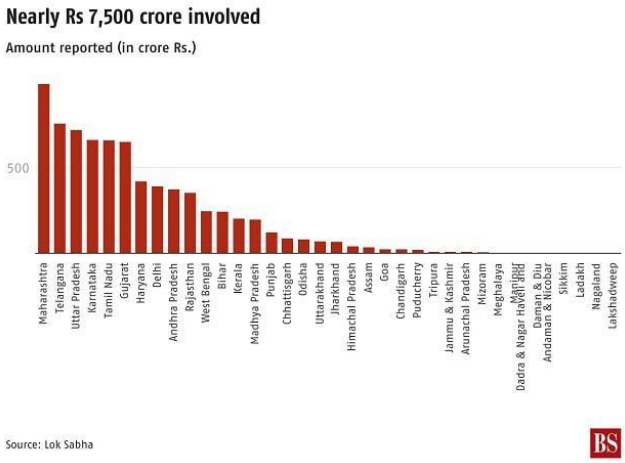

Figure 3: Amount reported in cyber frauds – state-wise in 2023

A study published by The Economic Times states that India ranked number 10 in cybercrime, with frauds involving people making advance fee payments being the most common type.
New data from the Federal Trade Commission (FTC) reveals that scams originating on social media have accounted for $2.7 billion in reported losses since 2021, surpassing other contact methods. Here are some key insights:

1. Online Shopping Scams: The most commonly reported social media scams involve online shopping. Approximately 44% of reports point to fraud related to buying or selling products online. Victims often respond to ads on platforms like Facebook or Instagram but never receive the items they ordered.

2. Investment Scams: While online shopping scams dominate in terms of frequency, investment scams account for larger overall losses. These schemes promote bogus investment opportunities via social media and constitute 53% of the money reported lost to scams in the first half of 2023. Notably, cryptocurrency plays a significant role in these scams, with more than half of the reports indicating payments made using digital currencies.

3. Romance Scams: After investment scams, romance scams rank second in reported losses on social media. Scammers exploit emotional connections, posing as friends or relatives and requesting money. Vigilance is crucial to avoid falling victim to such schemes.

Cyber law and Protection related to financial fraud in India

In recent years, the surge in online payments through platforms like UPI and Internet Banking has increased cyber financial fraud. The Reserve Bank of India (RBI) recognizes this issue and has introduced guidelines to address it. These frauds fall into various categories, including misappropriation, criminal breach of trust, fraudulent encashment through forged instruments, manipulation of accounts, and more.

I4C Scheme: Tackling Cyber Financial Fraud to combat rising cyber financial fraud, the Indian government launched the Indian Cyber Crime Coordination Centre (I4C Scheme) in 2019. Under this scheme, various units were established for investigating and identifying cybercrimes. These include the National Cybercrime Threat Analytics Unit, Cybercrime Reporting Platform, Joint Cybercrime Investigation Team, and National Cybercrime Forensic Laboratory.

Reporting a Cyber Financial Fraud: If we are a victim of cyber financial fraud, we can report the incident by calling 1930 or lodging a formal complaint on the National Cyber Crime Reporting Portal (www.cybercrime.gov.in).

Teaching notes

Understanding the nature of cyber financial fraud is crucial, especially in the context of identity theft and impersonation on social media platforms. Cyber financial fraud involves the illegal acquisition of personal financial information, leading to unauthorized transactions and financial loss. Identity theft is a common method, where fraudsters steal personal details to commit fraud, while impersonation on social media can lead to trust exploitation and further financial scams. In India, various legal provisions address these issues, including the Information Technology Act, of 2000, which covers identity theft, fraud, and unauthorized access to data. The Indian Penal Code (IPC) also includes sections related to fraud and forgery that can be applied to cyber-financial crimes. To safeguard against such threats, individuals should adopt preventive measures like regularly updating passwords, using multi-factor authentication, and being cautious about sharing personal information online. It is also important to manage online privacy settings diligently to protect both personal and professional reputation. Educating students about these aspects is essential; they should be aware of the importance of verifying online requests and recognizing phishing. Summarising below are the key points to approach the case

- **Cyber Financial Fraud**: Understand the nature of cyber financial fraud, including identity theft and impersonation on social media platforms.

- **Legal Implications**: Explore relevant legal provisions in India to address financial fraud.

- **Preventive Measures**: Discuss strategies to protect personal and professional reputation online.

- **Student Awareness**: Educate students about verifying online requests and reporting suspicious activity.

Discussion Questions

1.What steps can Prof. D take to mitigate the impact of the fraudulent Instagram account on her reputation?
2. How can educational institutions raise awareness among students about cyber financial frauds?

3. What legal actions can Prof. D pursue against the impostor under Indian laws?
4. How can social media platforms enhance security measures to prevent such scams?

References:

1) https://www.britannica.com/topic/cybercrime
2) Sussman, V. (1995) 'Policing Cyberspace', US News 38; World Rep., 23 Jan. 1995, at 54, Lexis, News Library, Us news file, 1995 WL 3113171.
3) Anderson, T. M. & Gardener, T.J. (2015). Criminal Law: Twelfth Edition. Stanford, CT: Cengage Learning
4) David S Wall (2007). Cybercrime, Polity Press Cambridge, p221
5) Cyber Frauds in India: Here is how much Indians lost to cyber frauds between Jan and Apr of 2024 | India News - Business Standard (business-standard.com)
6) What Is a Phishing Attack? | IBM
7) What Is Malware? - Definition and Examples - Cisco
8) What Are the Different Types of Cyber Crime and Introduction (eccouncil.org)
9) India News - Times of India (indiatimes.com)
10) Cybercrime To Cost the World $10.5 Trillion Annually By 2025 (cybersecurityventures.com)
11) Top Financial Scams in India – Forbes Advisor INDIA
12) India News - Business Standard (business-standard.com)
13) The Economic Times (indiatimes.com)