Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Study on Emerging Trends of Cyber Frauds and Digitalization in India Including Financial Cybercrime Legal Implications

[1]Dr. Sakshi Vashisth ,[2] Pankisha ,[3] Peeyush K. Mehta

[1] Assistant professor, School of law, JECRC University, Jaipur.
[2] Assistant professor, School of law, JECRC University, Jaipur.
[3] Assistant professor, School of law, JECRC University, Jaipur.
[1]sakshi.vashisth@jecrcu.edu.in
[2]Pankisha@jecrcu.edu.in
[3]peeyush.mehta@jecrcu.edu.in

ARTICLE INFO

Received: 18 Oct 2024

Revised: 25 Nov 2024

Accepted: 20 Dec 2024

ABSTRACT

Since the most recent demonetization in India, digital banking has grown in importance in the current era of digitalization. The digitization of banking has made fast financial transactions and opulent banking from anywhere at any time possible. In addition to promoting cashless transactions, the Indian government is offering financial. The current study aims to identify the many causes of fraud in the Indian banking sector and illustrate the types of fraud that have occurred since the banking industry went digital.

Since India's recent demonetization, digital banking has grown in importance in the current digitalization era. Fast financial transactions and opulent banking from any location at any time have been made possible by the digitization of banking. The Indian government offers financial incentives for digital transactions in addition to promoting the use of cashless transactions. A thorough understanding of how to use digitalization services is necessary to stop fraudulent activities because the rise in the use of digital banking transactions brought with it a variety of cybercrimes and an increase in the frequency of fraudulent activities. The current study aims to identify the many causes of fraud in the Indian banking sector and illustrates the types of frauds that have occurred since the banking industry went digital.

Keywords: Phishing, malware, information security, data security, cyber frauds, and cybersecurity.

INTRODUCTION

The growing reliance on digital technology and the internet has made cyber fraud a serious worry in India, as in many other nations. These are a few examples of typical cyber crimes that are common in India. Since 1997, the new idea of cyberspace has developed. E-commerce is one of the many business prospects that have resulted from this. Cyberspace has led to the discovery of several new crimes. These are entirely new crimes.

An offender who has committed an offense relating to cyberspace cannot be directly punished under the Indian Penal Code.

The Indian government passed "The Information Technology Act 2000" in response to this incapacity The Indian Parliament passed the Information Technology Act, intending to promote e-commerce, e-government, and the prevention of cybercrimes. The offenses include hacking, publishing pornographic material online. This special Act covers violations of confidentiality and privacy, such as publishing a fake digital signature certificate, confiscation, etc., and the perpetrator may face direct punishment under specific provisions of the IT Act 2000. E-Governance is supportive to E-Commerce, which includes legal recognition of electronic records as well as legal recognition of digital signatures. These two recognitions are very important for doing business through E-Commerce. Authentication of

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

documents is the most important aspect in E-Commerce.There are no finer words to sum up the current state of technology than those spoken by Cosmos, the antagonist in the film Sneaker.Cybercrime is defined as any unlawful behavior carried out using a computer or the Internet. Cybercrime involves copyright violations, software piracy, bank account and credit card fraud, stalking, and intimidation. Email attachments that appear harmless can frequently conceal malicious software, or malware. The purpose of phishing scams is to deceive Internet users into divulging passwords and other sensitive data. Cybercrime can be perpetrated against individuals, assets, and institutions. To safeguard sensitive data, computer networks must be closely monitored. Defamation, harassment, stalking, and spam and spoof emails are examples of cybercrimes against people. An email that seems to be from someone other than the original sender is called a spoof. Spam emails are solicitations or chain emails that contain many copies of the same email. When someone posts statements online or by email, it is considered cyber defamation. Cyberstalking is when someone monitors another person's online activities and initiates unwanted contact using chat rooms, email, and social networking sites.

Types of Cyber Fraud

1) **Phishing Scams:** Phishing schemes are attempts by con artists to fool you into divulging personal information, including [1]credit card details, bank account numbers, and passwords. These con artists will unexpectedly get in touch with you via phone, text, email, or even social media, posing as reputable companies like your bank or phone provider.
or even an internet service provider. To update their systems, the scammer can urge you to update your information. They might even invite you to survey to enter to win a prize. However, this is where the fraudster can obtain your phone number, email address, and other information**.** These fraudsters can also obtain your information by claiming that there has been suspicious or unauthorized activity on your account, after which they will request your details to resolve the matter. They will steal from you. Phishing assaults function similarly to phone scams, which
Education is being given to people. You may have noticed recent Barclays advertising campaigns similar to this one.
2) **Online Scams:** Online scams are scams that happen online. Whether that is tricking you into giving out personal details online by an ad popping up telling you have won something and asking for your card details to pay for shipping. Sadly, you will never receive anything but you will start noticing weird transactions coming from your bank account.
3) **Malware:** It is when harmful malware infiltrates your system. It is software designed with the intention of damaging equipment and data. The general term for various virus types, including Troja, is malware. Malware is frequently created using a variety of viruses that infiltrate your computer and wreak havoc by harming your phone, tablet, or computer. Criminals can steal personal information, including credit card numbers.
4) **E-Maol Bombing:** An email bomb is more of an online harassment tactic. An excessive number of emails sent to a single email address is known as "email bombing," which makes the recipient's computer lag or even crash. Even though they might not be taking anything, dealing with a slow server can be quite annoying and labour-intensive.
5) **Logic Bomb:** Although they are little programs or parts of programs that are activated by an event, they function similarly to viruses. [2]This event could be a specific time or date, a percentage of disk space being used up, the deletion of a file, and so forth. Then, a program might remove important code segments, making your software inoperable. The individuals who use logic bombs are typically put in place by insiders who have access to the system already**.**
6) **Internet Theft:** Any kind of theft that takes place online is referred to as "theft," and it can be accomplished in a variety of ways, including through malware, snooping, and phony emails and advertisements. The goal of online theft is to obtain your data and utilize it to either make purchases or withdraw funds from your bank account.

[1] PricewaterhouseCoopers, Combating Fraud in the Era of Digital Payments (2022
[2] Prateeskha Barman & Richika Kedia, Cyber Crime in India with Reference to Banking Sector (2023)

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

7) **Social Media Hack and Spamming:** As seen by the attack on the Burger King Twitter account, social media hacking is frequently carried out as a joke. Additionally, a lot of celebrities who are hacked might wind up posting weird status updates or following people they wouldn't normally. While it may seem funny to the normal person to watch a company or celebrity post strange content, it is an infringement of privacy. A hacker may, however, also disseminate inappropriate material that may be upsetting to viewers; doing so may result in your account being reported and closed. . Malicious accounts have the opportunity to continuously reply with unpleasant messages, which is another detrimental aspect of social networking. a type of trolling. While it's simple to report such behaviour to the social media site and have the person removed or blocked from viewing your post, it only takes a few minutes for someone to create a new bot account and launch another attack. Some have too much free time.
8) **Electronic Money Laundering:** Large amounts of illicitly created money must first be laundered before they can be invested or spent.
Wire transfers, which are electronic messages sent between banks, are one method of money laundering. Previously,[3] it had been impossible to keep an eye on or screen wire transfers as they happened because of the enormous volume on
Daily transactions are still occurring, but banks are cracking down on the problem and deleting any questionable activity.
9) **Sales and Investment Fraud:** Fraudsters can pose as investment brokers to obtain the contact information and account data of holders of savings or investment accounts. They will then get in touch with clients to offer them simple and lucrative chances, but they come across as much more reliable because they discuss accounts you currently have and actual outcomes.
10) **Amendment to the Information Technology Act (IT Act):** To protect the interests of the citizens, who should feel secure using these resources, the relevant agencies and the governing body should begin enforcing legal measures and penalties to reduce economic activity. A dedicated team of individuals skilled in identifying such actions should be trained by the regulating authorities, and an ethical plan should be put in place to find the offenses and respond appropriately to the legal system.
11) **Public Awareness Campaign:** To raise the level of financial literacy in the community, the relevant authorities, banks, and educational institutions should plan an awareness campaign to inform the public about these activities using a suitable real-world example.

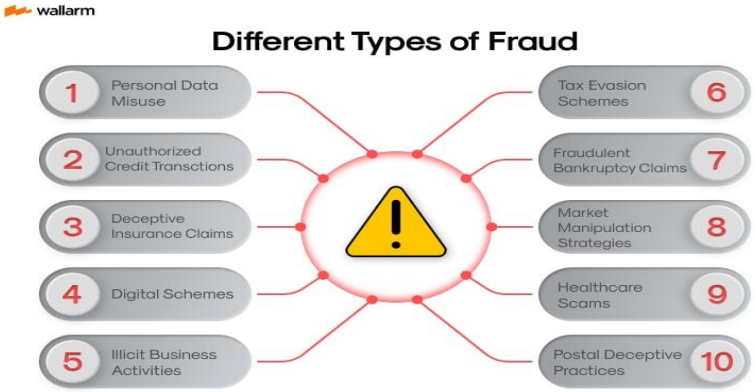

Figure 1. This Figure Shows Types of Crime

Cyber Crime and Its Effects on Society:

Since the 1960s, cyber fraud and other cybercrimes have presented the government and law enforcement with the most difficult problems in cyberspace. This could be as a result of the financial

[3] Priyanka Datta, Surya Narayana Panda & Sarvesh Tanwar, A Technical Review Report on Cyber Crimes in India (2023)

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

and business sectors being the most well-liked. those who have been using computers and the internet since the early days of modern multimedia technology.

Cyber fraud Definition: There is no definition of "cyber fraud" under India's Information Technology Act 2000. Nonetheles D. Bainbridge claims that the term "computer fraud" refers to "theft of money or property through the use of a computer that is employing a computer to fraudulently get assets such as cash and checks, credit card services, or to fraudulently avoid obligations or debossing a counterfeit bank card to get money from an automated teller machine or dishonestly instructing a computer to transfer money into a bank account are two examples.. According to Section 25 of the Indian Penal Code 1860, an individual is considered to have acted "fraudulently" if they did so with the purpose of defrauding, but not otherwise. Therefore, mens rea, or the desire to defraud, is crucial. Actus reus, or human conduct, refers to the state of mind and action. Multimedia technology is advancing civilization in this way. The use of new multimedia technology by criminals to facilitate their work in the information superhighway has a different influence on society.

CYBER FRAUD IN INDIA:- Online money transactions, e-banking, e-shopping, online auctions, online lotteries, data transmission, data chat, online ticket booking, and practically every other area of our lives in the current era of communication convergence We must traverse the expressway of life. Thus, we must traverse cyberspace.[4] As a result of globalization and liberalization, India is now prepared to handle e-governance and e-commerce. Similar to the real world, thieves pose a threat to us online, which is why India has implemented several security measures, passed the Information Technology Act 2000 and its regulations, and established several organizations, including the Cyber Crimes Cell and NASSCOM, in several states, including Delhi, Kolkata, Mumbai, Bangalore, Pune, and Hyderabad. Similar to other crimes, cyber fraud is growing daily.

No country—the United Kingdom, the United States, Russia, Canada, Israel, Australia, Pakistan, Bangladesh, or India—is safe. Even though we have our laws, the jurisdiction in cyberspace is ill-defined and unspecified, which has led to is the main source of issues in the cyber world.

LEGISLATIVE APPROACH:

1. **THE INFORMATION TECHNOLOGY ACT 2000**
2. **THE COMMUNICATION CONVERGENCE BILL 2011**
3. **THE INFORMATION TECHNOLOGY BILL**
4. **THE INFORMATION TECHNOLOGY AMENDMENT BILL 2006**

Socio-Legal Impact of Cyber Fraud In India -

Hyderabad DATA CONVERSION FRAUD OF Rs. 20 CRORE. The owner of the website InfoTech Pvt. Ltd. and the managing director of Vinsri InfoTech, Mr. C. Suresh, began his data conversion business in 1997 to provide entry tasks; to offer services for e-books, administration, medical transcription, data entry, etc.[5] He deceitfully obtained non-refundable deposits of around Rs. 2.5 lakh from each client in January 2002 under the guise of providing data input services. Additionally, in February 2003, checks issued to his clients by him were not honored since there were no funds available; instead, his clients began to demand that their bills be paid or that they be given labour in exchange for a refund of the money they had deposited. However, the accused, Mr. C. Suresh, remained mute.

As a result, his 1,500 or so clients filed individual complaints with the police. Then, on suspicion of cyber fraud involving data worth roughly Rs. 20 crore, he was taken into custody from Secundrabad. Fraudulent conversion.

Bangalore Cyber Fraud Case—More than 400 students were enrolled in the Sutra Solutions case in Bangalore City. The company had 42 branch offices operating as call centers and promised them jobs within a short period of time. months. They were seized as trainees. The Sutra collected Rs. 1.2 crore from trainees, comprising Rs. 6,000 for

[4] David Bainbridge, Introduction to Computer Law (4th ed. 2000)
[5] Sophos, Press Office, News Articles

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

customer service and Rs. 25,000 for technical assistance. Some of the learners noticed that the Sutra website, WWW.sutrasolutions.com, was offline after depositing the aforementioned funds.

Telephone and building rents were due, but they were not paying them. The victims then filed complaints against the business. Police detained Mr. Raju Krishnamurthy on suspicion of cyber fraud because Ajay Shah, the CEO, had been evading them; nevertheless, he was later freed on bail.

CYBER HACKING: INTRODUCTION

In the modern world, crime on computer-generated superhighways is a new occurrence. In this fast-paced age, a business cannot exist without e-business and e-commerce. We are unable to think of any intellectual and essential work without the use of information technology. However, crooks and deviants are abusing this new multimedia technology. As a result, we are unable to consider crime or criminals in isolation from cybercrimes or cybercriminals. Compared to regular crimes, cybercrimes inflict greater harm on society. Examples of cyberattacks that cause greater harm to human life than regular crimes include the attacks on the World Trade Center, AIMS, and Bhaba Atomic Energy Center. Whether spamming, hacking, or Cyberterrorism, cyberfraud, cybertheft, unauthorized access to computers and computer systems, etc., should all be considered more serious than regular crimes. This is a pressing global issue.

"Cyber crimes" are not defined in the Information Technology Act of 2000. Cybercrimes can be defined as forbidden human behaviour on computer-generated superhighways or in connection with computer-generated activities,[6] as well as other information technology-friendly electronics, such as cell phones, wireless, TVs with internet access, etc., in the age of communication convergence.

Cyberspace hacking poses a legal dilemma on both a national and international level, necessitating the implementation of global security standards and regulating policies through extensive worldwide study and research.

Hacking Usually represents themselves as

1. The guardian of sensitive and unsafe data and
2. Their operations fall within the bounds of the law; and
3. that they don't always breach the law.

HACKR'S CULTURE

Numerous criminologists have made an effort to comprehend and investigate the causes of hacking or the reasons behind delinquent behavior by hackers. The unpredictable nature of hackers has made it extremely challenging to deal with global circumstances. Initially, hackers were computer specialists who coined the term "hack" to refer to computer work done with a certain degree of skill. After that, they progressively grew anxious to disseminate usefulness. and the general public's ability to access computers and computer systems. However, the terms hacker and hacking have drastically evolved in the modern day.
A "hacker" is someone who engages in hacking, which is defined as breaking into or sabotaging a computer system. Hacking's[7] legal definition is linked to the act of gaining unauthorized access to data or programs stored on a computer system, or altering, changing, deleting, or attempting to do so in any way.

Essential Elements of Hacking

1. Intentionally wronging or harming people
2. knowingly harming or causing wrong to others.
3. It must relate to computer, computer system or computer network
4. The outcome must either (a) destroy, (b) delete, (c) alter, (d) reduce the information's value or utility, or (e) have an adverse effect.

[6] The Times of India, June 25, 2005 http://www.ciol.com
[7] Webster's Dictionary (2nd ed. 1996)

Journal of Information Systems Engineering and Management
2024, 9(4s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

CYBER TERRORISM

In the age of multimedia technology and new communication convergence, terrorism is a weapon in the hands of weak people or groups who like to attack people with the aim that people will learn about them. Examples of terrorist attacks include the attacks on the World Trade Center and Pentagon in the United States on September 11, 2001[8]; the London attack on July 7, 2005; the Mumbai, Kashmir, attack in 2006; the defacement of Indian military sites in India by hackers in July 2005; and even the year 2000, when the "T love you" virus was circulating to bring down computers and the internet.

Tsfati, Yariv, and Gabriel Weimann contend that contemporary terrorism can be understood as an effort to spread ideas using planned violence.

Concept of Cyber Terrorism

The word "Cyber Terrorism" is coined by a senior research fellow in California Institute for Security and Intelligence, Mr. Barry Collin in 1980s composed two concepts "Cyberspace" and "Terrorism", According to him "Cyberspace" is the place where computer data flow and computer functions.73 Back in 1997, Mathew Devort, Brian Houghton, and Neal Pollard defined "information terrorism" as "the deliberate misuse of a digital information system, network, or component for a purpose that aids or supports a terrorist campaign or action."

Modes of Cyber Terrorism

1. The precursor to war is cyberterrorism. In the Information and Communication Technology (1CT) age, one country uses modern technology against another or nations to commit acts of terrorism.
2. International cyber terrorist attack. When International Organisations of terrorists link or communicate between them through internet and their own network to attack any nation, it is called international cyber terrorist attack. For example, in the year 2001 on 11th September World Trade Centre and Pentagon attack; immediately after that in the same year on 13th December 2001 attack at Indian Parliament.
3. use of the internet and computer systems. Effective cyber tactics include terrorist organizations using computer systems and internet resources to create their own websites and networks to communicate with one another globally terrorism.
4. The "worm," "virus," and "trojan horse" are flowing. spreading "worms," "viruses," and "trojan horses" to bring down government agencies like the military, intelligence, business, academia, and health. Access to knowledge and a global electronic network is one method that makes cyberterrorism easier.

MOTIVATION. Terrorists may have psychological, cultural, or national reasons.

(i) Cultural motivations are based on sentiments about one's own country and other countries, as well as feelings about one's community, language, and other things. (ii)

(ii) Psychological motivations are based on life satisfaction and dissatisfaction with family, community, and society. (iii) National motivations are the financial motives of commercial or military personalities with specific benefits goals.

A company. In the age of information and communication technology, the importance of organization in terrorism is growing daily. Within the gang, they gather information from others and covertly plot future attacks.

Weapons and targets Everyone has access to information and communication technology, even terrorists. These are abused as weapons and targets at different periods.

Conclusion

1. Analyzing the issue of cyber frauds in India after digitalization reveals a strong positive correlation between the two. [9]This is because digitalization has created a suitable platform that allow those in need of money to use it to generate income.
2. The study of cybercrimes in India after digitization highlights the growing difficulties brought on by dishonest practices in the banking industry. To counteract the growing threat of cyber fraud, the study emphasizes the urgent need for improved cybersecurity measures, public awareness initiatives, and

[9] Bharat Reddy, Digital Financial Frauds in India: A Call for Improved Investigation Strategies (2024

Research Article

legislative frameworks. Digitalization's effect on cybercrimes has been significant, as India's demonetization campaign sparked an increase in online transactions and, in turn, fraudulent activity.[10] The study explores the underlying factors that lead to these illegal acts and emphasizes the different kinds of cyber frauds that are common in the Indian banking sector.

3. The study highlights how crucial it is to comprehend the social ramifications of fraudulent activities on community trust and the drivers of cyber fraud, which can range from greed to necessity. The exploitation of IoT device vulnerabilities, inadequate cybersecurity protocols, and a lack of consumer awareness are recognized as major contributors to India's

problems of cyber fraud. These risks have been made worse by the COVID-19 epidemic, which makes a careful analysis of the Indian economy's crisis-resilience imperative.

4. In summary, the study emphasizes how urgent it is to combat cyber fraud using a multifaceted strategy that incorporates stakeholder collaboration, legal changes, and technology developments. The study offers insightful information to lawmakers, financial institutions, and law enforcement by examining how digitization has affected cybercrimes in India. enforcement organizations to fortify cybersecurity infrastructure, reduce threats, and protect the digital economy from deception.
5. The conclusion reached by performing an analytical analysis on the topic of cyber fraud in India after digitalization highlights the significance of taking responsibility and acting responsibly to protect oneself from such actions for the country's development and progress.

[10] Supreeth Sandhu, Customers' Usage Behaviour of E-Banking Services: Interplay of Electronic Banking and Traditional Banking (2020)