Journal of Advanced Zoology

ISSN: 0253-7214
*Volume **43** Issue **S-1 Year 2022** Page **76:82***

Mapping The Victims of Digital Crime

Neha Bahl[1], Shikha Bhatnagar[2]

[1]DME Law School, Noida.
[2]Teacher's Law College, Bangalore

**Corresponding author's E-mail: Neha Bahl*

Article History

Received: 06 June 2023
Revised: 05 Sept 2023
Accepted: 16 Dec 2023

Abstract

Mapping the victims of digital crimes can be a challenging task, as digital crimes can affect individuals from all walks of life, regardless of their demographic background or geographic locations. Overall, mapping the victims of digital crimes can be useful for understanding the pattern and risk factors associated with digital victimization and for developing targeted prevention and intervention strategies. Digital crime/Cybercrime is the most prevalent form of crime with the lowest enforcement rate. India has been ranked 4th on the list of global cybercrimes by the Federal Bureau of Investigation (FBI) in its recent report, while US, UK and Canada backing the 1st, 2nd and 3rd positions. Indian Government has established a central cyber security agency named 'Indian Computer Emergency Response Team (CERT-In)' which works in coordination with similar other agencies across other countries in the world. This agency monitors all kinds of cyber threats. Also, Cyber Police Stations have been set up all over to deal with this menace across India. This paper aims to provide a thorough insight regarding digital crimes and mapping its victims in the present world. Even though Indian government has enacted various laws for making such crimes punishable but are these laws self-sufficient or something more is required??, as digital crimes are the most prevalent form of crimes with the lowest enforcement rates. To address this, the Union Government needs to confront various challenges that are distinctive to digital crimes. Measures taken by Indian government along with preventive steps that can be taken at individual level by the victims are also discussed.

Keywords: *Cyberspace, Cyber Networking, International Forensic Standards, e-crimes, NCRB*

1. Introduction

Meaning of Digital Crimes

Technology today serves as the cornerstone of modernisation, making the rise in technologically related crime inevitable. Digital crimes, or cybercrimes as they are often known, are crimes committed while using digital tools like computers, smartphones, and other gadgets. Digital crimes are those that include unlawful access, theft, modification, corruption, or disturbance of computer data or the connected digital systems.

Any illegal behaviour that occurs on or through a computer, the internet, or another piece of technology recognised under the Information Technology Act is referred to as such. The most pervasive crime that has a severe impact on contemporary India is cybercrime. Any unlawful behaviour that uses a computer or the internet as a tool, a target, or both is considered a cyber-crime. Although it may be legally interpreted in some decisions rendered by Indian courts, the term "cybercrime" is not defined in any acts or laws passed by the Indian Legislature.

Cybercrime, electronic crime, and computer crime are a few of the synonyms for the term digital crime. In the beginning, the phrase "computer crime" was used to refer to any illegal behaviour that involved computers, networks, or the use of a computer as a tool. Yet in recent years, similar crimes have spread to include other digital devices, such as cell phones, hence the phrase "digital crime" has been in use. The focus of digital crime is on offences against computer data or systems, unlawful access to, alteration of, or degradation of a computer or digital system. There is currently no universal definition for this category of crimes, and it is difficult to establish one.

Types of Digital Crimes

Cyber-crime against Individuals: E-Mail Spoofing: Spoofed emails are those that look to come from one source but were actually sent by another. Another name for this is email forgery. The attacker's main objective in this instance is to send the victim a lot of emails in order to disrupt his email service. Phishing: When consumers of financial institutions receive unsolicited emails asking for their username, password, or other personal information to access their account, this is referred to as phishing. The customer's online bank account and the funds in it are now accessible to the criminal. Customers provide their information by clicking the links in the email; thus, they are ignorant that fraud has taken place. Spamming: Sending the same message to the same person repeatedly for commercial advertising, non-commercial proselytising, or any other illegal reason (especially the fraudulent purpose of phishing). It also refers to the practise of sending several unsolicited messages (also known as spam) to numerous recipients through messaging platforms. Cyber-Defamation: This is when someone uses their email account to send offensive communications to other individuals in an effort to harm the reputation or dignity of another person. Cyberstalking and Harassment: Repeatedly harassing someone, a group of people, or an organisation online. The motives behind this harassment could be anger or they could be sexual in character.

Computer Sabotage is the use of the internet to introduce worms, viruses, or logic bombs into a computer system in order to prevent it from operating normally. Malware: Malware is any software that hijacks a user's computer, spreads a bug to other users' devices or social media accounts, and corrupts a computer system without the owner's knowledge or consent. Cyberbullying: It is a type of electronic bullying or harassment. Online bullying also includes cyberbullying and cyber-harassment. Growing in popularity, particularly among teenagers, when someone, usually a teenager, bullies or harasses someone else online or in other digital places, especially on social media, this is known as cyberbullying. A.P. Mali defines Cyberpornography as "the graphic, sexually explicit subordination of women through pictures or words, which also includes pornography, which is verbal or visual material that represents or describes sexual behaviour that is degrading or abusive to one or more participants in such a way as to endorse the degradation."

Cyber-Morphing is a type of criminal activity in which an unauthorised user or someone using a false identity edits the original image. Female users' photos are copied from their profiles and edited before being uploaded for sexual reasons by bogus accounts on several websites. The users' lack of understanding is what encourages crooks to perpetrate such horrible actions. Online Trolling: It is a type of online violence that occurs on social media sites where users have the freedom to express themselves. Those who voice their thoughts and believe differently from the prevalent society norms are frequently the targets of online harassers. Females who are the targets of cyberbullies are represented in this section. "Women who are vocal online, especially on subjects that have traditionally been considered to be 'male expertise' like religion or politics, or about women's experiences, including those of sexuality, menstruation, or speaking out about patriarchy, are subjected to a vicious form of trolling, usually from self-identified right-wing accounts on Twitter," claims a report by Digital Hifazat.

Crime Against Property: Intellectual Property Crimes: Crimes include any unlawful act that wholly or partially denies the owner their rights. Software piracy, copyright infringement, trademark infringement, and computer source code theft are the most prevalent types of crimes etc. Cyber Squatting: It involves two people claiming ownership of the same domain name by stating that they registered it first, or both. For instance, www.yahoo.com and www.yahhoo.com are two websites with identical names. Cyber Vandalism: Vandalism refers to destroying someone else's property. So, when a network service is interrupted or suspended, cyber vandalism refers to the destruction or damage of data or information held in computers. Hacking Computer System: simply, hacking is the illicit intrusion of a computer system or network. Hacking attacks involve unauthorised access to or control of popular social networking sites like Facebook, Twitter, and blogging platforms. Data and computer systems will be lost as a result of hacking activity. Altering in an unauthorized way. This requires little technical expertise and is common form of theft by employees altering the data before entry or entering false data, or by entering unauthorized instructions or using unauthorized processes; Altering, destroying, suppressing, or stealing output, usually to conceal unauthorized transactions.

Mode and Manner of Committing Digital Crimes

Hacking - A technique used by cybercriminals to gain unauthorized access to any person, group, or network of computers in order to obtain personal information that can be used to perpetrate financial fraud, cheating, etc. Email Bombing - refers to sending a large volume of emails to a recipient's account, which causes the recipient's mail server to crash and gives the cybercriminal the chance to

access the victim's account and obtain the information they need, or to copy all data from the victim's device to their own device. Data Diddling - This type of attack entails changing unprocessed data right before it is handled by a computer and then changing it back after the preparation is complete. Salami Attacks - The purpose of these assaults is to commit financial offences. The trick here is to make the alteration so insignificant that in a single instance it would go completely unnoticed, for instance, a bank representative may embed a program into the bank's employees that automatically deducts a small sum of money, say Rs. 10 each month, from each client's account. This unauthorized charge will likely go unnoticed by the record holder, but the bank employee will still earn a substantial sum of money each month.

Denial of Service (DoS) Attack - This includes sending a computer asset more solicitations than it can handle. This results in the assets such as web worker, crashing, depriving authorized clients of the assistance the asset offers. A Distributed Denial of Service (DDoS) attack is a variation on the standard Denial of Service attack in which there are several, geographically dispersed perpetrators. The regulation of such assaults is difficult. The attack begins by making excessive demands to the victim's computer, exceeding the limit that the workers can handle, causing the workers to crash. Attacks based on refusal of service have a long history and have already brought down websites including Amazon, CNN, Yahoo, and eBay. Worm Attacks - Viruses are programs that append themselves to a computer or a record and afterward circle themselves to different documents and to different computers on an organization. They generally influence the information on a computer, either by modifying or erasing it. Worms, dissimilar to infections need not bother with the host to connect themselves to. They only make useful duplicates of themselves and do this over and over till they gobble up all the accessible space on computer memory. The VBS_LOVELETTER infection also called the Love Bug or the I LOVEYOU infection was purportedly composed by a Filipino undergrad. In May 2000, this lethal infection beat the Melissa infection empty and turned into the world’s most common infection. It struck one in every five computers on the planet. At the point when the infection was brought under check, the genuine extent of the misfortunes was boundless. Misfortunes brought about during this infection assault were fixed at US $ 10 billion.

Logic Bombs - These are occasion subordinate projects, made to accomplish something just when a specific occasion, known as a trigger occasion, happens. Indeed, even some infections might be named rationale bombs since they lie torpid all during that time and become dynamic just on a specific date. Trojan Attacks - A Trojan, as this program is appropriately called, is an unapproved program that capacities from inside what is by all accounts an approved program, along these lines covering what it is really doing. This term has its opening point in the word ‘deception’. In the programming field, this implies an unapproved program, which latently deals with another’s framework by addressing itself as an approved program. The most well-known type of introducing a Trojan is through email. Web Jacking - This happens when somebody strongly assumes responsibility for a site by breaking the secret key and later evolving it. The genuine proprietor of the site does not have any more command over what shows up on that site.

Phishing Attacks - Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is usually done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim’s machine. Ransomware Attacks - Ransomware is a type of malware from crypto virology that threatens to publish the victim's personal data or permanently block access to it unless a ransom is paid off. Ransomware is a type of malware attack in which the attacker locks and encrypts the victim’s data, important files and then demands a payment to unlock and decrypt the data.

Who are the Victims of Digital Crimes??

In this 21st century with the changing time lot of technological advancements has taken place in our present society. Now a days each and every one is using internet in one or the other way. Unfortunately, only few of them knows how to make an effective use of digital platforms. With increasing utilization of internet leads to several types of cyber-crimes such cyber defamation, cyber bullying, Identity theft, financial frauds etc. If we go through the official statistics majorly financial frauds are committed daily. As slowly and gradually India is moving towards digital India because of which mostly all financial transactions whether it is related to banks, or public accessing e-commerce websites for purchasing articles. In these situations, a customer’s personal information, including debit and credit card information, is compromised by skilled hackers who then utilise those credentials in a harmful way. Similar to this, there are numerous other organisations, such as educational websites and occasionally even federal or state government websites where data is compromised, for instance. The year 2022 saw one of the worst cyberattacks in India as the country's

main institution, All India Institute of Medical Science (AIIMS), was struck by a ransomware attack. Before authorities were able to recover data and bring systems back, the AIIMS server was offline for almost two weeks.

Strategies for Mapping the Victims of Digital Crimes: Cybercrime strategies focus exclusively on crime prevention and criminal justice policies, programmes, and practices. By contrast, cyber security strategies provide guidance on cyber security matters (which can include cybercrime prevention), and map out objectives, action plans, measures, and the responsibilities of institutions in meeting these objectives. These strategies include legal, procedural, technical, and institutional measures designed to safeguard systems, networks, services, and data. Focus Areas Strategic Objectives Action Items Legal Framework Develop a more effective legal framework to investigate and prosecute cyber-crime.

Requirements for a Strategy: Establish a Project Authority: Development of a national cybercrime strategy requires cooperation from many different stakeholders. A common challenge in delivering a cybercrime strategy is securing and maintaining the commitment of relevant parties. It is therefore important to identify a 'project authority' made up of a senior official, ideally a minister, and a project team with responsibility for developing, implementing and revising the cybercrime strategy. As an example, the senior official could be the Minister of Home Affairs and the project team could consist of members of the national cybercrime unit. Alternatively, the project team could be a joint task force. Obtain Intra-Governmental Cooperation: For the development of a strategy to be effective, it requires intra-agency cooperation. This can prove difficult and requires good leadership, effective collaboration, and often compromise. Effective intra-agency cooperation is crucial for all stages of the project, such as the drafting and implementation of the cybercrime strategy. Cyber-crime and Digital forensics personnel, cybersecurity personnel including CERTs. Some examples of agencies listed here include National Police Agency – departments and units such as National cybersecurity agency or department, National Computer Security Incident Response Team (CSIRT) and/or CERT, National, regional and state/province level justice or law ministry, Central Authority for managing Mutual Legal Assistance Treaties (MLATs), National Security or Intelligence Agency, Other national agencies responsible for cyber-enabled crime (e.g., fraud, exploitation, etc.), other state or province-level police services with active cybercrime investigation units.

Substantive Legislation such as Laws: covering personal data protection or data privacy; laws criminalising offences such as hacking and data theft; laws criminalising the sale of tools or services for hacking; laws against online harassment; and laws outlining requirements for protecting critical infrastructure.

Legal Framework for Reducing Digital Crimes: The Internet has two distinctive characteristics. First of all, it is not restricted to a certain area and a cybercriminal can carry out their crime from anywhere in the world. The second distinctive quality is that it gives its users anonymity, which has benefits and drawbacks of its own. It's a blessing for those who use anonymity to voice their opinions to the world, but it's a curse for those who use anonymity to commit crimes. As a result, these qualities present difficulties for both enforcing the law and preventing crime. There isn't a specific statute dealing with cybercrime against women as of right now. There are other rules that may apply in this scenario; however, most women are most women are not aware of. Women does not know about their rights or that such rights exist.

Cybercrime is punishable under numerous statutes and regulations. However, the Indian Penal Code (IPC), 1860, and the Information Technology Act (IT Act), 2000, are the sources of the majority of the laws. The IPC is India's general criminal code, which outlines offences and stipulates penalties for them. IPC, which has been legislatively updated and judiciously interpreted to be applicable to cybercriminals, covers laws and punishments pertaining to the physical world. The IT Act, on the other hand, is a particular code that addresses the use of information technology and crimes that are committed using it. The IT Amendment Act, which includes several cybercrimes, was passed in 2008. In 2008 IT Amendment Act was enacted including certain crimes related to cyber world. Both IT Act and IPC are complementary to each other on cyber-crime against women.

Cyber Laws: Cyber-crimes are a new class of crimes which are increasing day by day due to extensive use of the internet these days. To combat the crimes related to internet The Information Technology Act, 2000 was enacted with prime objective to create an enabling environment for commercial use of IT. The IT Act specifies the acts which have been made punishable. The Indian Penal Code, 1860 has also been amended to take into its purview cyber-crimes. The various offenses related to internet which have been made punishable under the IT Act and the IPC are enumerated below:

- Tampering with Computer source documents – Section 65

- Hacking with Computer systems, Data alteration – Section 66
- Publishing obscene information – Section 67
- Unauthorized access to protected system Section 70
- Breach of Confidentiality and Privacy – Section 72
- Publishing false digital signature certificates – Section 73
- Cyber Crimes under IPC and Special Laws:
- Sending threatening messages by email - Section 503 IPC
- Sending defamatory messages by email - Section 499 IPC
- Forgery of electronic records - Section 463 IPC
- Bogus websites, cyber frauds - Section 420 IPC
- Email spoofing - Section 463 IPC
- Web-Jacking - Section 383 IPC
- E-Mail Abuse – Section 500 IPC

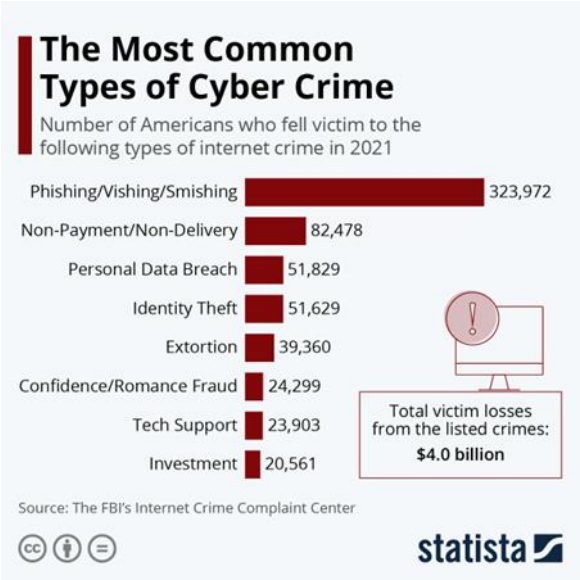
Sections under the Information Technology (Amendment) Act, 2008	**Punishment**
Section 66A: *Cyber Stalking*, i.e., sending offensive messages through any communication services like a computer or mobile phone	Imprisonment up to 3 years long with a fine.
Section 66B: *Receiving stolen computer's resources or communication device dishonestly*	Imprisonment which may extend up to 3 years, or with a fine of rupee 1 lakh or both.
Section 66C: *Identity Theft*	Imprisonment which may extend up to 3 years along with a fine that may extend up to rupee 1 lakh.
Section 66D: *Phishing*, i.e., punishment for cheating by personation using computer resources	Imprisonment which may extend up to 3 years along with a fine that may extend up to rupee 1 lakh.
Section 66E: *Voyeurism*, i.e., punishment for violating privacy of an individual	Imprisonment for 3 years along with a fine which may be extended up to 2 lakh rupees or both.
Section 66F: *Cyber Terrorism*	Life imprisonment.
Section 67A: *Publishing/ or transmitting material in electronic form containing sexually explicit content.*	Imprisonment up to 5 years along with a fine that could extend up to 10 lakh rupees in the first convict; and imprisonment can be extended up to 7 years with fine of 20 lakh rupees in the second convict.
Section 67B: *Child pornography*	Imprisonment up to 5 years along with a fine that could extend up to 10 lakh rupees in the first conviction; and imprisonment can be extended up to 7 years with an extended fine of 10 lakh rupees in the second conviction.

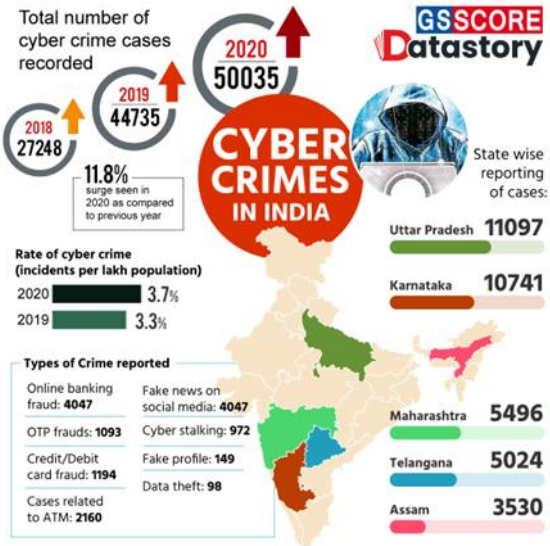
Following are some of the important Sections under Indian Penal Code for protection of individuals from Cybercrimes:

Sections under Indian Penal Code (IPC)	**Punishment**
Section 354A punishes the offence of *Sexual Harassment*	**3 years of imprisonment and/or fine.**
Section 354C criminalizes the offence of *Voyeurism*, i.e., the act of capturing the image of a woman engaging in a private act, and/or disseminating said image, without her consent	3 years of imprisonment for the first conviction and 7 years of imprisonment on the second conviction along with fine.
Section 503 punishes *Criminal Intimidation* as threats made to any person with injury to her reputation	Imprisonment which may extend up to 2 years, and/or fine.
Section 507 punishes *Criminal Intimidation* by an anonymous communication	Imprisonment which may extent up to two years.
Section 228A deals with *vengeful posting of images or videos of rape victims*	Imprisonment which may extend up to two years and fine.

The Indian Computer Emergency Response Team (CERT-IN or ICERT) is an office within the Ministry of Electronics and Information Technology of the Government of India. It was formed on 19 January 2004. It is the nodal agency to deal with cyber security threats like hacking and phishing. It strengthens security-related defence of the Indian Internet domain. National cyber-crime reporting portal has been establishes by the government of India under ministry of home affairs.

Graphical Data of Digital Crimes in India: In the first 2 months of 2022 alone, there were a reported 212,485 cyber-crimes, more than the entirety of 2018. The figures rose more sharply through the pandemic, with reported crime jumping from 394,499 cases in 2019 to 1,158,208 in 2020 and 1,402,809 in 2021. The Indian Computer Emergency Response Team (CERT-In) received and tracked as many as 12.67 lakh cyber-attack incidents this year by November 2022, said Rajeev Chandrasekhar, Minister of State for Electronics and Information Technology (MeitY) in the Parliament on December 14, 2022. Gradual increase in cyber-attacks: During the winter session, MP Manish Tiwari asked the government whether the number of cyber-attacks in India had increased over the last five years. Accordingly, CERT-In data showed that cyber-attacks had increased from 41,378 attacks in 2017 to 14,02,809 attacks in 2021. However, this number appears to have decreased somewhat in 2022 where 12,67,564 attacks were reported until November.





2. Conclusion

We are living in a digital age and cyberspace is not limited to one's boundaries, rather it covers an entire world. As a result, cybercrime is increasing day by day in all the countries including India. The

biggest challenge relates to cybercrime being its dynamic nature because of the ongoing evolution of digital technology. As a result, new cybercrime methods and techniques come into practice. Therefore, cybercrime should be given as much importance as other crime happening in our society be it theft, rape, murder etc.

Suggestions

While using online platform not divulging any personal data is almost impossible and thus, one should beware while sharing any personal information online. It is essential that an eye should be kept on false email messages and such emails should not be responded to if they ask for personal information. Also, email address should be guarded. While engaging in online activities it is imperative that attention should be paid to privacy policies on websites and steer clear of fraudulent websites used to steal personal information. It is also necessary that response to offences on the internet against women should be seen as part of the broader movement against harassment and abuse. Broader efforts should be initiated as it is ultimately a people- centred challenge.

Keeping up with the pace of change is the need of the hour. Keeping up with the technological advancements is a challenge that is essential to overcome as most of the online crimes takes place due to the lack of knowledge and awareness among the users. A collaborative effort among media, clubs, associations and women's media networks is critical to promote women's leadership and decision making in the society. Online diligence, monitoring and reporting against violence and cyber-crime should be done effectively and efficiently.

There should be an E-portal where women can report their problems online themselves without suffering from the stigma of involving police in such matters. Also, the database of criminals should be maintained which could help in law enforcement. Women should be made aware about using online media platforms and adequate procedures should be followed by them. They need to be aware of their right in the cyberspace.

Education systems must initiate contemporary issues regarding online crimes and awareness should be spread regarding safe internet uses.

The government should make more rigid rules to apply on the Internet Service Providers (ISPs) as they have the entire record of the data that is accuses by the users surfing on the web. Also, in case of any suspicious activities a report should be made by them in order to prevent crimes at an early stage.

References:

An Introduction to Digital Crimes, International Journal in Foundations of Computer Science & Technology, May 2015

https://www.bbau.ac.in/dept/Law/TM/1.pdf

https://lawcorner.in/modes-and-manners-of-committing-cybercrime/

https://timesofindia.indiatimes.com/gadgets-news/50-government-websites-hacked

https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=Cyber%20crime%20in%20India&text=In%20the%20first%202%20months,2020%20and%201%2C402%2C809%2

https://www.medianama.com/2022/12/223-12-67-lakh-cyber-attacks-reported-november-2022-meity/

Abbreviations

- CERT-In Computer Emergency Response Team
- CSIRT Computer Security Incident Response Team
- DoS Denial of Service
- FBI Federal Bureau of Investigation
- IPC Indian Penal Code
- MeitY Minister of State for Electronics and Information Technology
- MLATs Mutual Legal Assistance Treaties
- US United States of America
- UK United Kingdom