International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 09 | Sept - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

CYBER CRIMES AND PREVENTIVE MEASURES

-With special Emphasis on Cyber Laws in India and Measures for Preventions from Cyber Crimes

Dr. Abhishek Srivastava

Assistant Professor (Law)

Alliance University

Bangalore, Karnataka

India

CHAPTER 1- RESEARCH SYNOPSIS

Detailed Area of Research: *Contains the area on which the research paper revolves around and discusses the matter.*

This paper highlights the surge in Cyber Crimes in India post 2000. It also analyses the innumerable kinds of cyber crimes which have come into picture during this era. It also underlines numerous Cyber Laws which have been introduced by the government with special emphasis on Section 66 of the Information Technology Act 2000.

Title: *Should reflect the objectives of the study. It must be written after the whole synopsis, so that it is a true representative of the plan (i.e., the synopsis).*

This is the reason why the title of the research paper is "**Online Cyber Crimes and the preventive laws in India- With emphasis on the Information Technology Act and Measures for Prevention from Cyber Crimes**"

Introduction: *Should contain brief background of the selected topic. It must identify the importance of study, its relevance and applicability of results. It must clearly state the purpose of the study.*

In the era of cyber world as the usage of computers became more popular, there was expansion in the growth of technology as well, and the term 'Cyber' became more familiar to the people. The evolution of Information Technology (IT) gave birth to the cyber space wherein internet provides equal opportunities to all the people to access any information, data storage, analyse etc. with the use of high technology. Due to increase in the number of netizens, misuse of technology in the cyberspace was clutching up, which gave birth to cybercrimes at the domestic and international level as well.

Though the word Crime carries its general meaning as "a legal wrong that can be followed by criminal proceedings which may result into punishment" whereas Cyber Crime may be "unlawful acts wherein the computer is either a tool or target or both".

Objectives: *An objective is intent of what the researcher wants to state in clear measurable terms.*

The main objective behind the research here is to analyse how the Online Cyber Crimes in India have rapidly increased in the 21st Century, the tools which are being used by the cyber criminals to commit these crimes, the diversity of crimes which have occurred in past couple of decades, the laws which have been instigated to counter these acts.

Research Methodology: The Research methodology used is Doctrinal. The primary source is the Information Technology Act 2000. The Secondary sources are the Books, Articles and Journals from the library of TISS and Alliance University. The tools used are different statistics and data from various agencies on rate of Cybercrime in India, rate at which criminals are nabbed.

Hypothesis: A hypothesis is a statement showing expected results which the researcher will arrive at the end of the research.

The hypothesis is "The Absence of awareness among the people compounded with gaps in Cyber laws have led to an increase in Cyber Crimes in India"

Division of The Paper: The research paper has been divided into four chapters. The first launches the research by introducing the topic. The Second Chapter analyses Cybercrimes and its ever-increasing nexus in India. The third chapter deals about the Cyber laws in India along with famous Cyber law cases of our country .While the fourth chapter contains the measures which must be taken in order to curb the increasing rate of cybercrime in our country, spread awareness among the common citizens about how to be vigilant to prevent and protect them from cybercrime and how to expertise our Police IT department to nab cyber criminals.

Review of the Literature: Several articles, reports, guidelines and material available on websites have been reviewed while conducting this research. Different cases have also been citied and the laws relating to cybercrime in India with main focus on Information Technology Act, 2000 have been reviewed in order to assess the provisions for the prevention of Cyber crimes in our Country.

Reason of Selecting the Problem: The Rapid growth of technology has contributed a lot in the growth of the country. Technology has made life much easier for everyone and it has become integral part of everyone. However with considerably rapid use of the technology, it comes with its own shortcomings. The relentless use of the cyber techniques has enormously increased the crime, crime against women, children, banking, insurance, stock market

and many other sectors that deal with finance. Moreover several frauds have been seen as well as been done by the cyber criminals using this technology.

How it is useful to the Society: The rate at which the Cyber crime has soared in the last couple of decades, the requirement to tighten them through effective Cyber Law was required. The IT act, 2000 might have been brought for the same but the sluggish rate at which the cyber criminals are being nabbed has been point of concern. This research tries to make an effort how the cyber crimes in India can be controlled.

Chapter 2- Cyber Crimes in India

In the late 1980s, everyone across the globe was witnessing a substantial change around the world order as the Cold War seemed to have reached to its climax. The Soviet Union was facing challenges both at the Economical level and at the International level. The effort to keep the Socialism intact took a mighty blow when the Berlin wall fell down. Within 26 months USSR, a superpower which has ruled the world along with USA collapsed like a deck of cards.

The fall of the Soviet Union paved the way for a globalized world. Post 1991, the world saw an upsurge in technological growth. The biggest of all of them was opening an Internet service for the public. It changed the world forever as countries, cities and continents connected with each other. Sending and accessing information became easy like never before. The whole world became one community.

Although the Internet made life much easier, it also brought number of new challenges with itself for the law enforcement agencies across the globe as new types of crimes started to unleash themselves, and this crime involving computer was faceless. It at times has created havoc and destroyed many innocent lives, breached nation's securities and has incurred heavy financial losses on its victims.

Some of the modern era Cyber crimes include:

1. Virus Attacks
2. Online Gambling
3. E-Mail Spamming
4. Cyber Phishing
5. Cyber Stalking

6. E-Mail Bombing
7. Cross Site Scripting
8. Whale Phishing Attacks
9. Malware
10. Trojan Horses

What is Cyber Crime? Any illegal act committed through electronic devices that target the security, data, financial records etc. of an individual, organization or state could be called Cyber Crime.

Let us discuss the above-mentioned Cyber Crimes in detail:

1. **Cyber Stalking:** Cyber Stalking is one of the most frequent cybercrimes prevalent in modern times. It refers to following a person without their permission, publicly or privately and involves harassing and threatening them to use internet and other electronic modes.[1]Once considered as offence mainly confined to developed countries is widespread now in India, which is the second largest internet user. The number of cyber stalking and cyber bullying data shows that it is on high against women and children.[2] In 2018 when Government declared the first ever data, Maharashtra considered as developed state was at the top of the ladder. In number of the cases it has been seen that the victim has suffered severe trauma which has made her live with it for the rest of her life.

   It is important from the user end to not disclose vital information and keep digital hygiene from the government's end it might be important to ensure that genuine profiles are registered on the social media platforms so that it would be easily to track down the offenders. It would also ensure to make these offenders to think twice before committing offence.

2. **Cyber Phishing:** In 21st Century, Data is considered to be very vital part of people's life; the financial transactions, professional information, educational documents etc. are generally shared by the people through online transactions or electronic submissions. This made them prone to the cyber criminals, who attempt to steal these data. The stealing of data, identity theft of individual, important documents and confidential data of government and companies is called Cyber Phishing.

   At current Phishing is considered the most dangerous mode of stealing data and Cyber Criminals use

[1]Antony Brown, Marcia Gibson and Emma Short, Modes of Cyber stalking and Cyber harassment: Measuring the negative effects in the lives of victims in the UK, Annual Review of Cyber therapy and Telemedicine (2017)

[2]Pritam Banerjee* & Dr. Pradip Banerjee, Analysing the Crime Of Cyber stalking as a Threat for Privacy Right In India, ISSN 2455-4782 (2022)

numerous methods like Spear Phishing attack, voice phishing, social media attacks, text phishing and USB drop to steal the data from the victim. The threat of Phishing has consistently increased in the recent years in spite of companies spending fortunes to prevent these attacks.

One of the suggestions to counter Phishing is that the Law Enforcement agencies need to ensure that even the phishing goes unsuccessful and the person goes unscathed they catch the offenders though this would be no less challenging as the cyber space itself is a huge domain where the offenders can vanish in a second.

3. **Cross Site Scripting:** Cross Site Scripting is another method which is used by Cyber criminals to commit offence. Under this type of Cyber offence malicious script is injected in trusted websites. The end user is unable to know that this is malicious attempt of stealing the data. It occurs when :

   a. Data invade in the website from the uncertain sources

   b. The Data is included in the content of the trusted website

4. **Bot Networks:** Bot Networks are another method of committing cyber crimes used by the offenders to carry out scams and cyber attacks. The Bot net is use to commit data theft, server crashing and malware distribution[3].

   It is one of the easiest ways used by the cyber hackers as it involves small cost and some time being invested by a hacker or small group hackers to execute the scheme of cyber attack. The different stages of cyber attack through Bot Networks are:

   i) Hacker using the vulnerability of the system: The Hacker exploits the vulnerability of the system to infect it through malwares.

   ii) In the second stage the hacker becomes successful as the system he targets is infected. The victim's data and other important things stored in the system become vulnerable. One of the method by which the victim is deceived is to make them download a file which contains Trojan virus.

   iii) In the final stage the hacker starts to control the infected system at its own will. The cyber criminals don't stop there they aim to increase the number in thousands and then millions.

   Once the system is affected the hacker can read and write system data, gather the personal data of the victim etc.

5. **Hacking:** Hacking is another frequent method through which cyber criminals aim to exploit weakness and

[3] https://www.kaspersky.co.in/resource-center/threats/botnet-attacks

security of a computer system or computer network. The person who performs the act of hacking is called hacker. While the technology has advanced in recent years but it has also given more option of hacking to the criminals. Some of the hackers have done it for a long period of time successfully and were caught only because of their minor mistakes. Amit Tiwari was one such hacker who hacked 950 accounts in 11 years spanning between 2003-2014. [4]

6. **Internet Time Thefts:** Basically, Internet time theft comes under hacking. It is the use by an unauthorized person, of the Internet hours paid for by another person. The person who gets access to someone else's ISP user ID and password, either by hacking or by gaining access to it by illegal means, uses it to access the Internet without the other person's knowledge.

7. **Phishing:** Phishing refers to the act through which the cyber criminals attempt to fraudulently by retrieving passwords of the email ID's, bank accounts, and other sensitive confidential information of another person by mimicking them as communication from trustworthy public or private institution. The victim is duped in believing that the information is being asked by the genuine source. [5] The phishing have resulted in number of innocent people being duped by the scammers and it is one of the prime reason why financial institutions especially advice the public not to share their pin with anyone.

Cyber Crime in India

India has a long way to go to protect the vital information of its citizens. It has been observed that nearly 69 percent of information theft is carried out by current and ex-employees and 31 per cent by hackers.[6]In fact India is ranked second in terms of being the victim of cyber attack between 2016-18[7]. The major Indian cities are highly prone to the cyber attacks, India's home PC owners are the most targeted sector of cyber-attacks. Mumbai and Delhi are emerging as the top two cities for cybercrime.[8]

With an increasing dependence on the use of technology, there is an upsurge in cyber offences as well. In 2021, there were 52,974 reported incidents of Cyber Crimes, in India which was 6% increase from the previous year.[9] On the other hand the Cyber attacks have also increased considerably. As per the data of CERT which is the nodal agency to deal with cyber security threats and operates under the Information Technology Ministry there has been a steady increase in the rate of the cybercrime. In 2017, the number of the cyber crimes in India were 41,378 but in

[4] https://www.dnaindia.com/india/report-pune-based-global-hacker-amit-tiwari-arrested-1956626
[5]https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2014/Resources/presentations/2012/topic5-final/report.pdf
[6] Crime in India: 2011-Compendium (2012), National Crime Records Bureau, Ministry of Home Affairs, Government of India, New Delhi, India.
[7]Cyber Crime in India , Showkat Ahmad Dar, Annamalai University and Naseer Ahmad, Chandigarh University, Sambodhi, December 2020
[8] Crime in India: 2011-Compendium (2012), National Crime Records Bureau, Ministry of Home Affairs, Government of India, New Delhi, India.
[9] https://www.moneycontrol.com/news/india/cyber-crimes-in-india-rise-6-a-year-in-2021-telangana-tops-list-ncrb-data-9115161.html

2021 the number have soared up to 14,02,809. The ever increasing cyber offences raise question regarding to the Cyber security of the country as well.

Cybercrime are predicted to inflict damages totalling more than 6 trillion dollar globally, and the cost of cybercrime is estimated to grow by almost 15% every year over the next 4-5 years, reaching 10.5 trillion dollar annually by 2025. This enormous cost is jeopardising the growth of digital economy, which makes discussion and action on cyber theft very relevant for the entire world.

The Cyber Attacks doesn't target the individuals or institutions but also target country as well. A Cyber attack that targets a country is typically referred to as Cyber warfare. It can destroy civilian and governmental infrastructure and interfere with vital processes, causing harm to the state and possibly even fatalities.

There are various types of Cyber warfare which pose threat to the security of the country

1. **Espionage :** It aims to steal the secret of other countries through computer systems
2. **Sabotage:** Through Computer systems the hostile governments or terrorists group can steal information which may pose threat to the victim country.
3. **Denial-of-service (DoS) Attacks:** DoS attacks prevent legitimate users from accessing a website by flooding it with fake requests and forcing the website to handle these requests.[10]
4. **Propaganda Attacks:** Cyber Attackers also target society and country by aiming to control the minds of the people through propaganda attacks. It can be used by spreading lies to make people lose trust in their system or country.
5. **Economic Attacks:** The World economy works on computer system, the attackers take advantage of this and can target computers of economic establishments which include stock market, financial institutions, banks and other payment system thereby blocking the flow of the funds.

Some of the major Cyber Attacks in India in recent times:

1. **AIIMS Server breach:** The server of Delhi AIIMS was compromised due to ransomware cyber-attack.
2. **Air India Cyber-attack:** In February 2022, Air India faced a major Cyber Attack which compromised the data of approximately 4.5 customers.
3. **Juspay Data Breach:** In 2021, India company Juspay suffered a data breach

[10]Cyber Security in India, Clear IAS team, 16th December 2022, retrieved on 9th March 2023 at 22.29 hrs.

4. **WannaCry Ransomware attack:** In May 2017, the top five cities in India (Kolkata, Delhi, Bhubaneswar, Pune, and Mumbai) got impacted due to the WannaCry ransomware attack.

Cyber Laws in India

In India there is no specific Cyber Law. Information Technology Act 2000 was the first step taken by Government to stop cyber crime. According to an Indian law cybercrime has to be voluntary and willful, an act or omission that adversely affects a person or property. Cyber law encompasses laws relating to Cyber Crimes, Electronic and Digital Signatures, Intellectual Property, Data Protection and Privacy.

Some of the Laws which deals with Cyber Crime in India are:

1. Information Technology Act, 2000

2. Information Technology (Certifying Authorities) Rules, 2000

3. Information Technology (Security Procedure) Rules, 2004

4. Information Technology (Certifying Authority) Regulations, 2001

Information Technology Act 2000: Indian parliament passed its first "Information Technology Act, 2000" on 17th October 2000[11] to deal with cyber crime in the field of e-commerce, e-governance, e-banking as well as penalties and punishments. The Information Technology (IT) Act, 2000, specifies the acts which have been made punishable. On 17th October 2000 the Information Technology (Certifying Authorities) Rules, 2000 and Cyber Regulations Appellate Tribunal (Procedure) Rules, 20 (Security Procedure) Rules, 2004 came into force on 29th October 2004.[12]

Major Sections

1. **Section 65-** Deals with tampering with Computer Source Documents – Imprisonment up to 3 years or/and a fine up to Rs 2,00,000/
2. **Section 66-** Hacking with the Computer System
3. **Section 66 A-**Publishing offensive, false or threatening information
4. **Section 66 B –** Punishment for dishonestly receiving stolen computer resource or communication device
5. **Section 66C-** Punishment for Identity Theft

[11] Information technology Act ,2000
[12]Information technology Act ,2000

6. **Section 66 D-** Punishment for Cheating by impersonation by using computer resource
7. **Section 66 E-** Publication of Private image of others
8. **Section 66F-** Punishment for Cyber Terrorism
9. **Section 67 –** Publishing information which is obscene

The Act was later on amended in 2008 bringing multiple changes which were needed with changing times.

Prevention from Cyber Crimes Awareness to be spread among Public

Best Practices for Prevention of Cyber Crime Below mentioned security guidelines and good practices may be followed to minimize the security risk of Cybercrime

1. **Creating Awareness**: The most important preventive measure to counter Cyber Crime is to create Cyber Awareness and Education among the people. Common public must be educated regarding to the various ways in which they can be duped by the cyber offenders, preventive measures to combat them as well.
2. **Updating the Computer System:** In order to avoid Cyber –attacks, it is important that the user must frequently update the operating system. While it might not protect the system from the attack, but it will increase the percentage of safety as the hackers will find it more difficult to access the computer system.
3. **Choosing Strong Passwords:** In an era when most of us have our email, financial activities online, it is important for the user to keep a strong password. It is one of the reasons why the banks and other financial institutions suggest us to select a password having at least eight characters comprising of letters, numbers, and symbols. Having easy password means prone to being easy prey of the cyber criminals. It is also important to keep on changing the password after every 90 days.
4. **Protect Personal Information:** When we use the internet for different purposes, we are required to fill out our personal information. This information, if reached in the wrong hand can result in damages. Hence, it's the users responsibility to ensure that they are providing information to the trustworthy sources.[13]
5. **Review bank and credit card statements regularly:** The impact of identity theft and online crimes can be greatly reduced if user can catch it shortly after their data is stolen or when user gets symptoms. Regularly check bank and credit card's statements. Now, many banks and services use fraud prevention systems that call out unusual purchasing behavior.

[13]Cyber Crime (2003) by R.K. Suri and T.N. Chhabra, Pentagon Press, New Delhi, India.

6. **Secure Mobile Devices:** As the use of mobile devices has increased in the recent years, therefore mobile devices are also prone to different types of cyber offences. Therefore, it's important for the users to ensure that their mobile is protected as well.

Conclusion

In an era of unprecedented use of technology, the mankind has been exposed to a new kind of threats "Cyber Offences". These Cyber Crimes and Cyber Attacks can be threatening not only to an individual but also to the security of the country as well. Therefore it is important that strong Cyber laws must be established by the Government which acts as a shield both for the citizens and institutions as well. These Cyber Laws must be updated from time to time so that they are effective enough to counter ever changing modus operandi of the cyber criminals. These Cyber offenders always find a different method to dupe the people and financial institutions.

Apart from having strong and updated Cyber Laws, it is pertinent to create Cyber awareness among the people. They must be taught how they can protect themselves from falling in the trap of the cyber criminals and to take additional protective measures.

The government can also use the highly qualified IT workforce for strategically countering the threat of cyber crime. The private firms shall be encouraged to invest in cyber security measures. The enhanced cyber security will also increase the reputation of India as well which means more secured environment.

The fight against Cyber Crimes cannot be countered alone everyone has to be united in this cause to ensure that this new era crime is defeated.

Bibliography and References

- *Cyber Law & Information Technology (2011)* by Talwant Singh, Additional District & Sessions Judge, New Delhi, India.
- *Introduction to Indian Cyber Law (2008)* by Rohas Nagpal, Asian School of Cyber Laws, Pune, India
- *Cyber Crime (2003)* by R.K. Suri and T.N. Chhabra, Pentagon Press, New Delhi, India
- *Cyber Laws in the Information Technology Age (2009)* by Karnika Seth, Jain Book Depot, New Delhi, India.
- *Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives (2012)* by Nina Godbole

and Sunil Belapure, Wiley India Pvt. Ltd, New Delhi, India.

- *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations (2011)* by Debarati Haldaer (Centre for Cyber Victim Counseling, India) and K. Jaishankar (ManonmaniamSundaranar University, India), IGI Global, USA.
- *Crime in India: 2011-Compendium (2012),* National Crime Records Bureau, Ministry of Home Affairs, Government of India, New Delhi, India.