A Comprehensive Study on Laws against Cyber Crimes

VEENA S[1], PAVITHRA B[2,]

Post Graduate Student, Department of M.C.A, Dayananda Sagar College Of Engineering, Bangalore, India

Assistant Professor, Department of M.C.A, Dayananda Sagar College Of Engineering, Bangalore, India

Abstract: Cyber crime is an unlawful act wherein the computer is either a tool or a target or both. Cyber crimes can involve criminal activities that are traditional in nature, such as theft, fraud, forgery, defamation and mischief all of which are subjected to the Indian Penal code. Cyber law(also referred to as cyberlaw) is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace". Cyber-attacks represent a potential threat to information security. As rates of data usage and internet consumption continue to increase, cyber awareness turned to be increasingly urgent. This study focuses on the relationship between the cyber crimes and the associated laws to protect against these crimes and threats. In this research, an effort has been made to highlight the important cyber crimes and laws that protect against these crimes. In this study, the main focus is to address new age crimes that are defined under Information Technology Act 2000. This study helps to identify most happening cyber crimes and measures to protect against them.

Keywords: Cyber Crime , Cyber Laws , Cyber Security , Cyber Threats , Cyber Knowledge , Types of cybercrimes .

1.Introduction:

When Internet was developed, the founding fathers of Internet hardly had any inclination that Internet could also be misused for criminal activities. Today, there are many disturbing things happening in cyberspace. Cybercrime refers to all the activities done with criminal intent in cyberspace. These could be either the criminal activities in the conventional sense or could be activities, newly evolved with the growth of the new medium. Because of the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. The field of Cybercrime is just emerging and new forms of criminal activities in cyberspace are coming to the forefront with the passing of each new day. Cybercrimes can be basically divided into 3 major categories being Cybercrimes against persons, property and Government.

We can categorize Cyber crimes in two ways

- The Computer as a Target :-using a computer to attack other computers.

e.g. Hacking, Virus/Worm attacks, DOS attack etc.

- computer as a weapon :-using a computer to commit real world crimes.

e.g. Cyber Terrorism, IPR violations, Credit card frauds, EFT frauds, Pornography etc

2.Objective:

- To understand the concept of cyber-crime.
- To get an overview of the common types of cybercrime.
- Know the steps to prevent cybercrime

2.1.Cyber Crimes And Cyber Laws in India:

Initially, there was no idea that Internet could transform itself into an all prevading revolution which could be misused for criminal activities and which required regulation. Today, there are many disturbing things happening in cyberspace. Due to the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with impunity and people with intelligence, have been grossly misusing this aspect of the Internet to perpetuate criminal activities in cyberspace. Hence the need for Cyberlaws in India.

The first reported computer crime was in the 1820s. The enormous growth of e-commerce and the exchange of online shares led to a phenomenal outbreak in cybercrime incidents. The Information Technology Act, 2000, is the main legislation dealing with the rules and regulations relating to the cyber world, it provides a step forward in the field of law with the changing and modernized dimension of the crime world. The main objective of the law is to provide legal recognition for electronic commerce and to facilitate the submission of electronic registers to the government. The computer law also criminalizes various computer crimes and establishes severe penalties.

Cyber law (also referred to as cyberlaw) is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct field of law in the way that property or contract are as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to integrate the challenges presented by human activity on the Internet with legacy system of laws applicable to the physical world.

2.2.Evolution of Cyber Crimes:

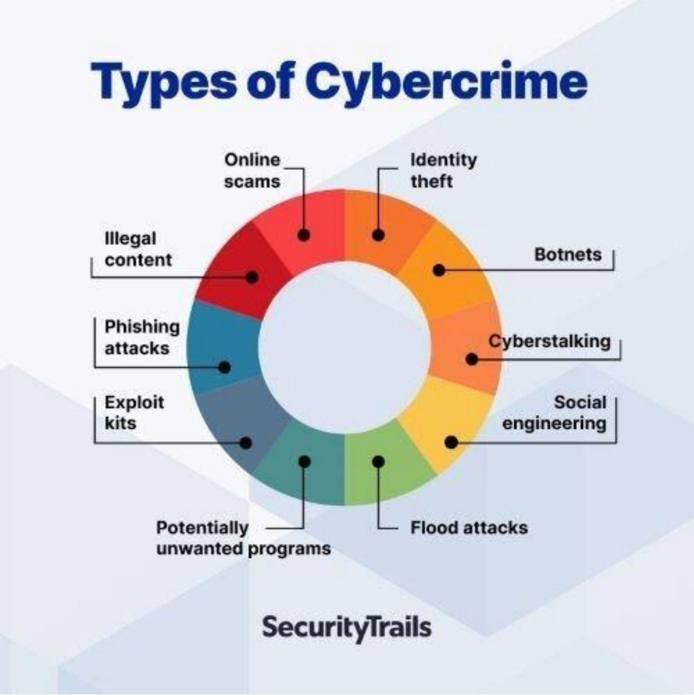
The cyber crime is evolved from Morris Worm to the ransomware. Many countries including India are working to stop such crimes or attacks, but these attacks are continuously changing and affecting our nation.

Table-1: Evolution of Cyber Crime

YEARS	TYPES OF ATTACKS
1997	Cyber crimes and viruses initiated, that includes Morris Code worm and other.
2004	Malicious code, Trojan, Advanced worm etc
2007	Identifying thief, Phishing etc
2010	DNS Attack, Rise of Botnets, SQL attacks etc
2013	Social Engineering, DOS Attack, BotNets, Malicious Emails, Ransomware attack etc.
Present	Banking Malware, Keylogger, Bitcoin wallet, Phone hijacking, Android hack, Cyber warfare etc.

2.3.Common Cyber Crimes:

The different types of computer crimes are:



Unauthorized access and piracy:

Unauthorized access means any type of access without the authorization of any legitimate or responsible computer, computer system or computer network. Hacking means an illegal intrusion into a computer system and / or a network. Every act committed to enter a computer and network is piracy. Hackers write or use computer programs to attack the target computer. They have the desire to destroy and get the kick of that destruction. Some hackers compromise personal monetary gains, such as stealing credit card information, transferring money from different bank accounts to their account, followed by withdrawing money. Government websites are the most specific sites for hackers.

Hijacking the Web:

Web hijacking means taking strong control of another person's website. In this case, the website owner loses control over his website and its content.

Pornography:

Pornography means showing sexual acts to cause sexual arousal. The definition of pornography also includes pornographic websites, pornographic magazines produced using computers and Internet pornography provided via mobile phones.

Child pornography:

Pedophiles attract children by distributing pornographic material and then try to meet them to have sex or take nude photographs, including their participation in sexual positions. Pedophiles sexually exploit children, using them as sexual objects or taking their pornographic photos to sell them on the Internet.

Cyber bullying:

Cyber bullying means repeated acts of harassment or threatening behaviour of the cyber-criminal against the victim through the use of Internet services.

Denial of Service attack:

This is an attack in which the criminal floods the victim's network bandwidth or fills his spam inbox that deprives him of the services to which he has the right to access or provide. This type of attack is designed to block the network by flooding it with unnecessary traffic.

Virus attacks:

Viruses are programs that have the ability to infect other programs and make copies of themselves and spread on another program. Viruses generally affect data on a computer by modifying or deleting them.

Software piracy:

Software piracy refers to the illegal copying of original programs or the falsification and distribution of products intended to pass through the original. These types of crimes also include copyright infringement, trademark infringement, theft of computer source code, patent infringements, etc.

Phishing:

Phishing is the act of sending an e-mail to a user who falsely claims to be a legitimate company founded in an attempt to defraud the user in providing private information that will be used for identity theft.

Email spoofing:

E-mail representation refers to e-mail that appears to come from a source but has actually been sent from another source.
Representation by e-mail can also cause monetary damage.

2.4. Importance of Cyber Law:

Cyberlaw is important because it touches almost all aspects of transactions and activities on and concerning the Internet, the World Wide Web and Cyberspace. Initially it may seem that Cyberlaws is a very technical field and that it does not have any bearing to most activities in Cyberspace. But the actual truth is that nothing could be further than the truth. Whether we realize it or not, every action and every reaction in Cyberspace has some legal and Cyber legal perspectives.

As the nature of Internet is changing and this new medium is being seen as the ultimate medium ever evolved in human history, every activity of yours in Cyberspace can and will have a Cyber legal perspective. From the time you register your Domain Name, to the time you set up your web site, to the time you promote your website, to the time when you send and receive emails , to the time you conduct electronic commerce transactions on the said site, at every point of time, there are various Cyberlaw issues involved. You may not be bothered about these issues today because you may feel that they are very distant from you and that they do not have an impact on your Cyber activities. But sooner or later, you will have to tighten your belts and take note of Cyberlaw for your own benefit.

2.5.Preventing Cyber Crimes:

Cyber laws that everyone using the internet must be aware of **:**

Internet is just like life. It is interesting and we spend a lot of time doing amusing things here, but it comes with its fair share of trouble. With the technology boom and easy Internet access across the country, cyber crime, too, has become a pretty common occurrence. From hacking into computers to making fraudulent transactions online, there are many ways in which we can become a victim of illegal cyber activities.

To regulate such activities that violate the rights of an Internet user, the Indian government has the Information Technology Act, 2000, in place. Here are some of its sections that empower Internet users and attempt to safeguard the cyberspace.

Section 65 – Tampering With Computer Source Documents

A person who intentionally conceals, destroys or alters any computer source code (such as programmes, computer commands, design and layout), when it is required to be maintained by law commits an offence and can be punished with 3 years' imprisonment or a fine of 2 Lakhs INR or both.

Section 66 – Using Passwords of Another Person

If a person fraudulently uses the password, digital signature or other unique identification of another person, he/she can face imprisonment up to 3 years or/and a fine of 1 Lakh INR.

Section 66D – Cheating Using Computer Resources

If a person cheats someone using a computer resource or a communication device, he/she could face imprisonment up to 3 years or/and fine up to 1 Lakh INR.

Section 66E – Publishing Private Images of Others

If a person captures, transmits or publishes images of a person's private parts without his/her consent or knowledge, the person is entitled to imprisonment up to 3 years of fine up to 2 Lakhs INR or both.

Section 66F – Act of Cyber Terrorism

A person can face life imprisonment if he/she denies an authorized person the access to the computer resource or attempts to penetrate/access a computer resource without authorization, with an aim to threaten the unity, integrity, security or sovereignty of the nation. This is a non-bailable offence.

Section 67 – Publishing Child Porn or Predating Children Online

If a person captures, publishes or transmits images of a child in a sexually explicit act or induces anyone under the age of 18 into a sexual act, then the person can face imprisonment up to 7 years or fine up to 10 lakhs INR or both.

Section 69 – Govt's Power to Block Websites

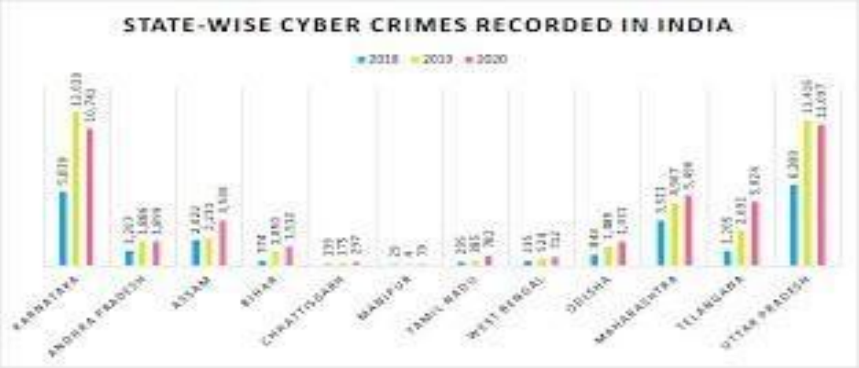
If the government feel it necessary in the interest of sovereignty and integrity of India, it can intercept, monitor or decrypt any information generated, transmitted, received or stored in any computer resource. The power is subject to compliance of procedure. Under section 69A, the central government can also block any information from public access.

Section 43A – Data Protection at Corporate Level

If a body corporate is negligent in implementing reasonable security practices which causes wrongful loss or gain to any person, such body corporate shall be liable to pay damages to the affection person.

3. Methodology

Secondary data was collected. Several magazines and newspapers have been used for this, as it is a conceptual document. Therefore, the goal is to better understand the concept, its application and the impact on the economy through other parameters. Therefore, qualitative and quantitative data were used. India ranks third in the world, after the United States and China, as a source of malicious activity in 2015, according to this 2016 report by Symantec Corp, a software security company. In 2015, India was ranked second as a source of malicious code and fourth and eighth as a source or source of web attacks and network attacks. In 2014, 9,622 computer crimes were reported, with a 69% increase compared to 2013. Of the 9,622 computer crimes reported, 7,201 were reported as crimes pursuant to the Information Technology (IT) law, 2,272 pursuant to the Criminal Code of India (IPC) and 149 under special and local laws (SLL). The state-wise cyber crimes recorded in India are given in the below picture.



4.Results and Discussions

We all must remember that Cyberspace is a common heritage of ours which we have inherited in our life times from the benefits of ever growing technologies. This cyberspace is the lifeline of the entire universe and given its irreversible position today, it is the duty of every netizen to contribute towards making the said cyberspace free of any trouble or cybercrimes , to rephrase the famous words of Rabindra Nath Tagore in today's context , "Where the cyberspace is without fear or crime and the head is held high, where knowledge is free, where tireless striving stretches its arms towards perfection, into that cyber heaven of freedom, O my father, let our humanity awake".

5.Conclusion:

It is important for every netizen to know what is happening with the internet they are on , every second. Today's life is completely dependent on the internet for every activity, so the users must always be aware of what data should be provided, shared through the internet. The internet users should not provide their personal information on any unauthorized websites. These personal information includes the identity information, debit/credit card information, phone numbers ,personal images and so on . The netizens ,if in case faces any threat then they should also be aware of the measures to be taken to protect or overcome the threats occurred.They also should be able to know cyberlaws and has to come forward to seek help from the cyber security stations legally.

6.References

1. Shabdita Pareek, "8 Cyber Laws That Everyone Using the Internet must be Aware of ", Scoopwhoop(8 Jan 2016),pp.1-5.
2. Government of India ," Cyber Laws and E-security" in Ministry of Electronics and Information Technologyupdated on Nov 1 2021.
3. Animesh Sarmah, Roshmi Sarmah , Amlan Jyoti Baruah, "A brief study on Cyber Crime and Cyber Law's of India" , IRJET,vol.4 issue.6, June 2017.

4. Prof. Saquib Ahmad Khan , “Cyber Crime in India: An Empirical Study” , IJSER, vol.11,issue.5, May 2020.
5. Animesh Sarmahand ,Anuraj Singh and Amlan Jyoti Baruah, “Cyber Crime in India: An Empirical Study” , IJSER, vol.11,issue.5, May 2020.
6. Vishi Aggarwal, Ms. Shruti, “Cybercrime Victims: A Comprehensive Study”,IJCRT,vol.6 issue.2,April 2018.