A STUDY ON CYBER LAWS AND SECURITY

[1]Ms. Khushi Arora, [2]Dr. Ratandeep Kaur

[1]Student, [2]Assistant Professor
Bachelor in Computer Applications (BCA)
SGTBIMIT,DELHI ,INDIA

Abstract: As we all live in an era of cyber technologies like Computers, Laptops, Mobiles, etc., we use them to our fullest but we are not always aware of its fullest. Internet has two worlds- the world we all know and the one which is hidden. Many people are unaware of the hidden part and those who are aware may use this hidden world to do crimes and illegal activities. So, to protect the unaware potion from these crimes, the govt. of many countries made cyber laws and methods to protect the people from these crimes. In this paper, we will talk about these laws and how to protect from them.

Keywords: Cyber Security, Cyber Laws, Internet, Unauthorized Access, Punishments.

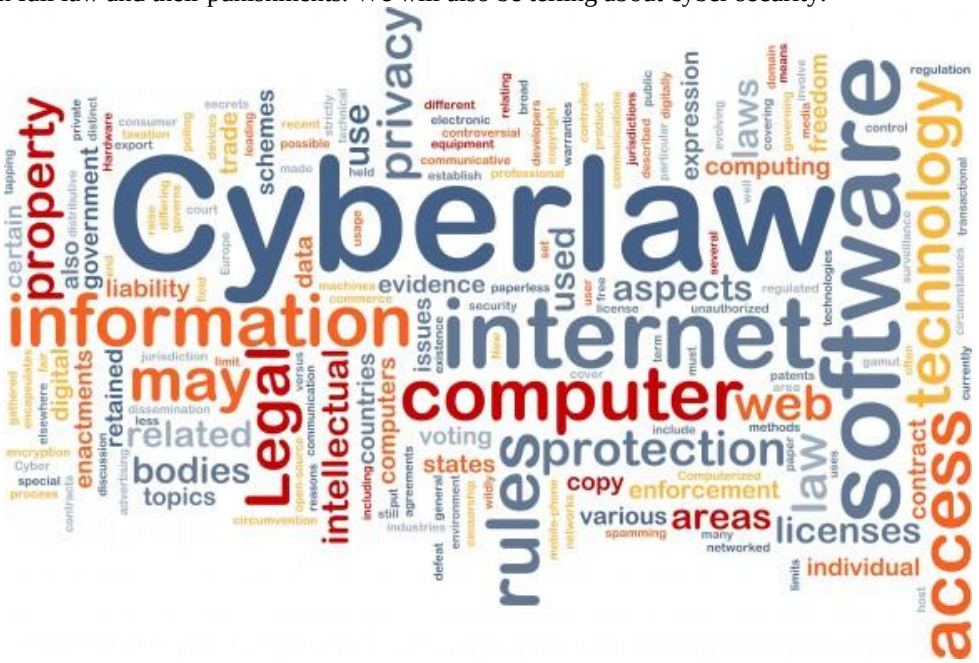
1. INTRODUCTION

In simple term we can define computer as the machine that can stores and manipulate/process information or instruction that are instructed by the user. Most computer users are utilizing the computer for the erroneous purposes either for their personal benefits or for other's benefit since decades [1]. The invention of computer was made to make ones' life easy but some people are using this very computer to do crimes and hideous activities which can lead to destruction of many lives. To save one from these crimes we need cyber security, the way to protect our information that is being transferred from one person to other or the information/data in the clouds of our phone or laptops.

Now comes the term "Cyber Law". It doesn't have a fixed definition, but in a simple term we can defined it as the law that governs the cyberspace. Cyber laws are the laws that govern cyber area. Cyber Crimes, digital and electronic signatures, data protections and privacies etc. are comprehended by the Cyber Law [2].

2. OBJECTIVE

The main purpose of this paper is to spread awareness and the knowledge of the laws imposed by the govt. against these crimes and criminals along with full law and their punishments. We will also be telling about cyber security.



3. CYBER LAWS AND SECURITY

3.1 CYBER LAW

Cyber laws were made or formed in order to take control and keep check on the crimes committed on the internet or though the usage o cyber technologies.

Cyber law, also known as cyber-crime law, is legislation focused on the acceptable behavioral use of technology including computer hardware and software, the internet, and networks. Cyber law helps protect users from harm by enabling the investigation and prosecution of online criminal activity [3].

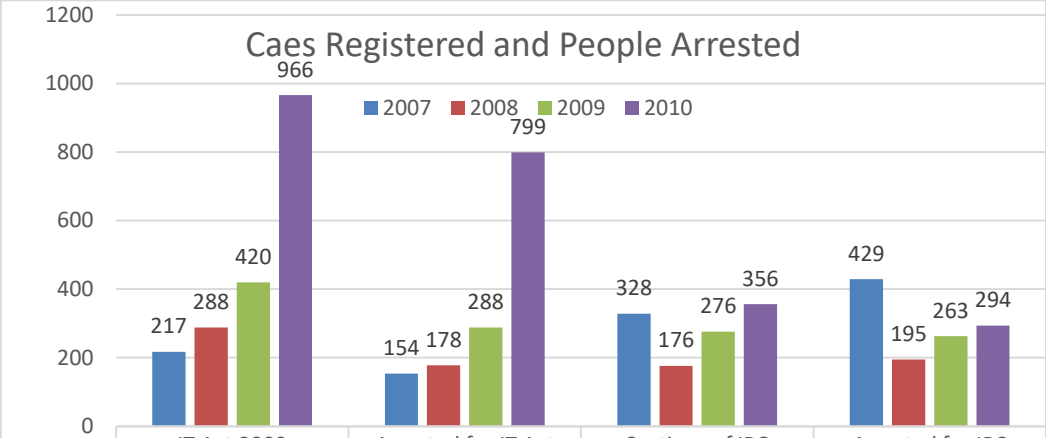
3.1.1 What is the importance of Cyber Laws?

In today's time, the world has become more digitally advanced and sophisticated and so are the crimes. Internet was initially developed as a research and information sharing tool and was in an unregulated manner. As the time passed by it became more transactional with e-business, e-commerce, e-governance and e-procurement etc. All legal issues related to internet crime are dealt

with through cyber laws. As the number of internet users is on the rise, the need for cyber laws and their application has also gathered great momentum [4].

In today's highly digitalized world, almost everyone is affected by cyber law. For example:

- Almost all transactions in shares are in demit form.
- Almost all companies extensively depend upon their computer networks and keep their valuable data in electronic form.
- Government forms including income tax returns, company law forms etc. are now filled in electronic form.
- Consumers are increasingly using credit/debit cards for shopping.
- Most people are using email, phones and SMS messages for communication.
- Cybercrime cases such as online banking frauds, online share trading fraud, source code theft, credit card fraud, tax evasion, virus attacks, cyber sabotage, phishing attacks, email hijacking, denial of service, hacking, pornography etc. are becoming common.
- Digital signatures and e-contracts are fast replacing conventional method of transacting business.



	IT Act,2000	Arrested for IT Act	Sections of IPC	Arrested for IPC
2007	217	154	328	429
2008	288	178	176	195
2009	420	288	276	263
2010	966	799	356	294

Figure 1: Cases Registered and People Arrested [4]

3.1.2 Cyber Laws in India:

There are mainly two laws in cyber section of India:

- Information and Technology Act,2000
- Indian Penal Code, 1860

3.1.2.1 Information and Technology Act,2000 (IT Act,2000)

MINISTRY OF LAW, JUSTICE AND COMPANY AFFAIRS (Legislative Department)

New Delhi, the 9th June, 2000/Jyaistha 19, 1922 (Saka)

The following Act of Parliament received the assent of the President on the 9th June, 2000, and is hereby published for general information:

THE INFORMATION TECHNOLOGY ACT, 2000 (No. 21 OF 2000)

[9th June, 2000]

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

WHEREAS the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;

AND WHEREAS the said resolution recommends inter alia that all States give favorable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-cased methods of communication and storage of information;

AND WHEREAS it is considered necessary to give effect to the said resolution and to promote efficient delivery of Government services by means of reliable electronic records.[5]

Above was the full preliminary of the IT Act,2000. Now, I will tell you about some of the sections under this preliminary and the punishment to that offence:

1. Section 65- Temping with the computers source documents

Whoever intentionally or knowingly destroy, conceal or change any computer's source code that is used for a computer, computer program, and computer system or computer network.

Punishment: Any person who involves in such crimes could be sentenced up to 3 years imprisonment or with a fine of Rs.2 lakhs or with both.

2. Section 66- Hacking with computer system, data alteration etc.

Whoever with the purpose or intention to cause any loss, damage or to destroy, delete or to alter any information that resides in a public or any person's computer. Diminish its utility, values or affects it injuriously by any means, commits hacking.

Punishment:

Any person who involves in such crimes could be sentenced up to 3 years imprisonment, or with a fine that may extend up to 2 lakhs rupees, or both.

3. Section 67: Publishing information which is obscene via electronic form

If any individual publishes or transmits any message or image which in itself is objectionable in nature, which may lower the image of the alleged person in the eyes of others, is a crime punishable.

Punishment:

Any person involved in this offence will be sentenced to imprisonment which may extend up to five years or fine up to Rs. 1 Lack.

3.1.2.2 Indian Penal Code,1860 (IPC,1860)

Apart from it some of the statutory provisions of ***Indian Penal Code, 1860*** especially in the crime of Fraud, Criminal Intimidation, Cheating, Breach of Trust, Abetment of Suicide via Blackmailing, etc. may be charged on accused having regard to the circumstances, and discretionary powers of the Court, however it must be noted that a person cannot be punished twice for the same offence, as it will violates his Fundamental Right ensured under Article 20 (2) of the Indian Constitution i.e. Double Jeopardy.

Some sections under IPC which shows offences under cyber activities:

1. Section 354-D- Voyeurism

If a man watches a woman engaging in a private act, where a reasonable assumption of privacy is expected by the women, captures her image and publishes it via an online medium.

Punishment:

One involved shall be punished with imprisonment for minimum one year, which may however be extended to three years for the first conviction, in the second conviction it shall be minimum three years, which may extend to seven years and fine.

2. Section 471- Using as genuine a forged document or electronic record

Whosoever fraudulently or dishonestly uses as genuine any document or electronic record which he knows to be forged.

Punishment:

Any person involved shall be punished with an imprisonment which may extend to two years or fine, or with both.

3. Section 506- Punishment of Criminal Intimidation

Where a person threatens other person to harm his reputation, life or property via an electronic means which induces that person to commit an illegal act or prevent him doing an act which is legally obligatory on him.

Punishment:

Anyone involved shall be punished with imprisonment which may extend to two years, or fine or both.

3.2 CYBER SECURITY

Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing.[7]

3.2.1 What is the importance of Cyber Security?

Cybersecurity is important because it protects all categories of data from theft and damage. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems.

Without a cybersecurity program, your organization cannot defend itself against data breach campaigns, making it an irresistible target for cybercriminals.[8]

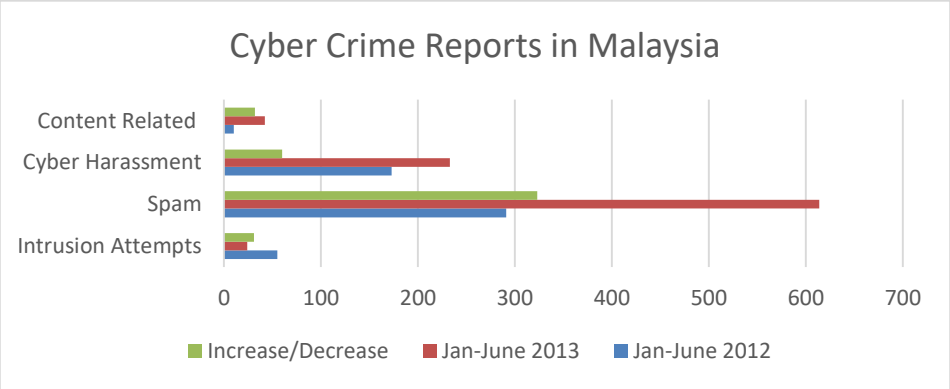


Figure 2: Cyber Crimes Reports in Malaysia in Jan-June 2012-2013 [9]

3.2.2 Cyber Security Techniques:

1. Access control and password security

The concept of user name and password has been fundamental way of protecting our information. This may be one of the first measures regarding cyber security.

2. Malware scanners

This is software that usually scans all the files and documents present in the system for malicious code or harmful viruses. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware.

3. Firewalls

A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet. All messages entering or leaving the internet pass through the firewall present, which examines each message and blocks those that do not meet the specified security criteria. Hence firewalls play an important role in detecting the malware.

4. Anti-virus software

Antivirus software is a computer program that detects, prevents, and takes action to disarm or remove malicious software programs, such as viruses and worms. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. An anti-virus software is a must and basic necessity for every system.

5. Authentication of data

The documents that we receive must always be authenticated be before downloading that is it should be checked if it has originated from a trusted and a reliable source and that they are not altered. Authenticating of these documents is usually done by the anti-virus software present in the devices. Thus, a good anti-virus software is also essential to protect the devices from viruses.[9]

4. CONCLUSION

Since the rise in the newly made technologies begins to give birth to many more cyber-crimes in recent years.

So, it is important to have protection against cyber crimes as its important for the social, cultural and security aspect of the country. Anyone can do cyber crime either being in the country or outside its physical boundaries. International harmony and coordination are important; thus, many have made their own cyber laws and with severe punishments than in India.

My main purpose to write this paper was to inform about the cyber laws in India and about the cyber security. I hope that this paper spreads awareness among all the people and they stay save from any kind of cyber crime or offence.

5. ACKNOWLEDGMENT

I express my sincere gratitude and thanks to Mrs. Ratandeep Kaur (Professor, Information Technology) of Sri Guru Tegh Bahadur Institute of Management and Information Technology (SGTBIMIT) for her valuable guidance, and support and kind coordination and co-operation during preparation of this paper and helping me in writing this paper in such a successful way.

6. REFERENCES

1. www.tigweb.org/actiontools/projects/download/4926.doc
2. An Introduction to Cyber Law - I.T. Act 2000 (India) (slideshare.net)
3. https://online.norwich.edu/academic-programs/resources/cyber-law-definition
4. https://blog.ipleaders.in/need-know-cyber-laws-india/.
5. https://www.meity.gov.in/content/preliminary
6. International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056 Volume: 04 Issue: 06 | June -2017 www.irjet.net p-ISSN: 2395-0072
7. https://www.kaspersky.co.in/resource-center/definitions/what-is-cyber-security
8. https://www.upguard.com/blog/cybersecurity-important/
9. A_Study_Of_Cyber_Security_Challenges_And_Its_Emerg.pdf