International Journal of Advanced Research in Engineering Technology & Science
ISSN: 2349-2819
Email: editor@ijarets.org Volume-6, Issue-9 September- 2019 www.ijarets.org

A STUDY ON CYBER CRIME AND CYBER LAW IN NCR REGION

Vipin Kumar Thakur
Research Scholar
Dept of Computer Science,
Shri Venkateshwara University, Gajraula

ABSTRACT:
Today every corner of the world is connected to computers and internet. Talk about this present age of today, online banking, online transaction, online shopping, online buying and selling and information about any area, etc. This new world of computer and the Internet has given a new dimension to human life but this computer and internet misuse has created a different direction for the new world of computers and the Internet Has turned in. Everything is online but cyber is the biggest threat to them. Nowadays anyone can access the internet from anywhere. If seen, the number of cyber crimes is continuously increasing. Initially it is difficult to understand the environment of cyber-related crimes; this is the reason why it is difficult to stop it at the beginning. Speaking of cyber crime, it is done knowingly or unconsciously. If cyber crime is intentionally done then in reality this is a very serious topic. Crime through computer, internet or other digital devices is called cybercrime or computer crime. In order to prevent cyber crime, a cyber law has been created by the government, so that the culprit can be punished. In this letter, the continuous increase in cyber crime in the NCR, cyber law, Classifications of cyber crime, the provision of punishment for criminals for cyber crime, safe access to the internet and online security of the social media has been included.

Key words: Cyber Crime, Cyber Law, Types of Cyber Crime, Continuous Increase Cyber Crime in the NCR, Cyber Law in India**,** Provision of Punishment for Criminals for Cyber Crime and Safe Access to the Internet and Online Security of the Social Media.

INTRODUCTION:

The origin of the computer has given human life a new dimension. Today, people from all over the world can use the Internet from anywhere but misuse of Internet and computer has given rise to a new curse known as 'cyber crime'. However, we cannot even give it to internet crime. Computer and Internet are being used by some as a tool. The number of crimes in the NCR region is continuously increasing. Some people are using computers and the internet to get their personal benefits. In other words, cybercrime is born when a computer is manipulated by any kind of information stored and used in the wrong direction. Today's present era is of computers and the Internet, and it is becoming very difficult to imagine any work without the help of computer. There is no doubt that criminals who commit cyber crime are also becoming very high tech. These criminals are using computers, internet, android phones and sites to execute their crimes.

Cyber Crime:

'Cyber crime', ‘is a crime under which many types of crimes like spreading viruses in computers or sending emails through e-mail and blackmailing. This offense committed by criminals is known in the language of computer and internet as 'cyber crime'.

- 'Cybercrime', ‘is a kind of illegal act, under which the criminal uses the computer as a tool to commit crime’.
- 'Cybercrime' ‘is a type of illegal act, under which computer is used as a tool’.

Cyber Law: Under the 'Cyber Law' documents which are in the form of electronic law, it gives law recognition and under it a provision has been made to support any files which are electronic or in electronic commerce transactions. In this, a law has been made to investigate the crimes related to cyber crime, which is called 'cyber law'.

History of Cyber Crime:

Today's present age is based on computers and the Internet. The new era of this internet has given a new dimension to the lifestyle of man and on the other hand has given birth to a 'cyber crime'. In the year 1970, it was discovered by some facts that criminals at that time used telephone lines to commit crimes. The talk is from the time when a man of John Draper Nan took the US and used a public telephone to call. Impressed by John Draper, Steve Jobs and Steve Wozniak also worked with them after this Steve Jobs and Steve Wozniak founded Apple, a world-famous computer company. It was seen that no cybercrime act was done till the end of 1980, but after that in 1981, a person named Ian Murphy was able to steal someone's valuable information and manipulate some of his important data, only hacked the computer. Ian Murphy, known as Captain Zap, used to manipulate a clock to hack an American telephone company, which allows people to make free calls. The first thing that was the target of the criminals was telephone companies, but now banking, website and anybody's personal information is also in the target of criminals. There is also the point that according to the way that new technologies came into the world, hackers also changed the star to commit crime. Talking about today's present time, it is very popular for people to transact online money, but there is danger anywhere in it. Online banking is the first place on the target of criminals. Such as the criminal user name or log-in code, can change their password and keep their password with this, when a person creates an account, then someone else can use that account. Here's one thing that cyber crime is the biggest threat to the user who still keeps his data or information secure. On one hand, where Internet users provide all their services, on the other hand, too many threats are brought to the fore. Therefore users should use VPN to protect their personal information.

Evolution of cyber crime: Along with India, other countries are also working on a continuous new aspect to prevent cyber crime. Other countries are also changing with India due to cyber crime being developed continuously.

Effected Organization

- Sony Play station – 77 million users data leaked, April 2011
- Adobe – 2.9 million accounts hacked, October 2013
- Target – 110 million customer banking data hacked, December 2013
- South Korea – 110 million credit cards details hacked, January 2014
- IT security company – 1.2 billion login & password on 420,000 websites had stolen by Russian Hackers, August 2014
- Yahoo – effected 500 million user account, 2014
- Dating site – 20 years of personal data was stolen (more than 400 million), 2015
- Equifax (an American credit company) – 143 million American, Canada & British customers 200,000 credit card numbers stolen, July 2017
- Marriott hotels – 500 million customer's data stolen, September 2018
- Marketing analytic firm – 123 million U.S. households, Database publicly exposed online

Types of cyber crime:

When a crime is done by internet, computer or other digital devices, then that crime is called 'cyber crime'. There are several types of cyber crime, some of which are the following:

- Property: If seen to be a criminal, then the criminal targets one person and then stole all of that person and reaching the bank account of that person with easy access to all the money steals. In the type of crime, the cyber criminals can steal the information of the victim's bank and information about the log etc. Along with this, the criminal can give financial distress to the victim. Hackers send some malware or malicious software to the user.
- **Individual:** There is only one person involved in this type of crime who personally reaches the goal of his crime. These crimes are mostly done online through the Internet. The criminal has illegal information in it, which he personally sends forth or distributes or transmits it online. Such as cyber stocking, sending or distributing pornography, trafficking or grooming etc.
- **Government:** Talk about the current time of the day - as new - new technologies are evolving, in the way the ways of doing the work are also changing. If any crime is against the government then it goes to Cyber Terrorist. If the culprits doing this kind of crime are successful, then all the government departments' website, official website and even the military website can get huge losses, which can break the back of a country's economic situation.
- **Cyber Stalking**: Cyber stalking is a group of individuals or individuals in crime that follows the other person's Internet. He tries to harass and harm him in every possible way. In cyber stalking, giving threats to any person like anybody, abusing any person online, harassing any person mentally and trying to harm the entire data of any person.
- **Phishing Scams:** Phishing scam has a simple meaning: You are trapped in the trap, There is way to do a phishing scam in which the scammer tells you that you have got some wrong activity in your account, you need to refresh the computer and then they ask you for your personal information so that they can target the crime Could complete.
- **Malware:** Malware is a program of software that is very harmful and dangerous for a computer system. Hackers steal your personal database with the help of this software.
- Software Piracy: It is a very serious crime that comes under cyber crime. It is said that a duplicate copy of the program is illegally or illegally copied in it.
- **Data Diddling:** Data diddling meant to change any kind of data from its original form to other forms. This change can be done by a person who is collecting data or typing or by computer viruses.
- **Salami Slicing Attack:** This means stealing money from someone's account. This is a new technology used in a way that has been developed by cyber criminals. Criminals use this salami attack in such a way that the person in front does not seem to know this.
- **Hacking:** Hacking means if we understand in simple language, it means that logging any computer system without any permission and stole all its data.
- **K) Logic Bomb**: Logic bomb works in a manner similar to viruses. It is also called "slag code" in other words. It is made up of a very important program. When it is inserted into a program, it keeps quiet but when the time of the program comes, it gets started.

The Continuous Increase Cyber Crime in the NCR:

According to a report, Cyber Crime in the NCR is constantly spreading. According to the security expert, there is cybercrime in the entire NCR area almost every 10 minutes. Before that, more than 23,852 complaints were recorded in 2018 six months. Most of the people who commit cyber crime in the NCR region are young or students. If seen, a 7th class student also keeps track of the computer's password well hacking. According to a report, a conference was organized by the Ministry of Telecommunications and Information Technology on Cyberspace in 2017.

Internet and Online Security:

Today, the use of computers, the Internet and other digital devices continues to grow. Just like the computer, the internet and other digital devices, we all need security as the security surrounds us.

- **Internet security:** It means 'keep your network, important information and data away from the wrong person'. It includes Authentication, Access Control, and Cryptography.

- **Authentication:** Under this, the user name, user ID and password are verified through a secret code.
- **Access Control:** This includes access to some important information through a thumb impression, card or voice, called access control.
- **Cryptography:** Any information or important data contained in it would have been sent in the form of a secret form before sending it through the Internet, and the receiver has its usual form.
- **Firewall:** This is a mechanism to secure a computer that is in the form of software and it prevents heavy traffic entering the computer.

Make a Strong Password to Protect Your Personal Information and Data:

- Do not use the same password for more than one website.
- Password should be changed at regular times.
- Never use passwords like 1234, 0000, 1111 or XYZ, because any hacker first tries similar passwords and they are successful too many times.
- The password should never be too small.
- Make your password big and worth remembering.
- The password should be made according to different digits, letters and special type of symbols.
- The bigger the password and the special character, the more secure it is.

What should not be used? :

- Do not use personal information in creating passwords.
- Never create passwords that people know about for example - Do not use the first letter of your name or name.
- Do not use the name of your child's name or family members.
- Do not use your date of birth.
- Do not use the name of your locality.
- Do not use abcd or 1234.

Social Media:

Talk about today's current time, Social Media or Social Networking Website has given a new dimension to the lifestyle of people. Social Networking Sites and Social Media have become a new way of talking to each other. Social Networking Website has become a tool for Social Media Business, Relatives and Friends etc.

What to do with Security in Social Media / Social Networking Website

- Never tell your personal information to the stranger.
- Do not tell more about your business.
- Do not tell the information of your bank or ATM on social media.
- Do not tell about your company issues on social media.
- Do not tell anyone about any of your programs.

So, in the end, we want to say that by forgetting, never tell your personal information on social media. Carefully use social media, the internet and computers that will keep you safe.

A glimpse of cyber crime in India (a few cyber crime cases)

- **July 3, 2019: 25 five thousand rupees, 2 cyber criminals arrested by Annie's desk app:** Cyber criminals called as fake bank officers. During this time, the bank asked to update KYC and asked to download the desk app. As soon as the app is downloaded, 25 thousand rupees have been flown from the account.
- **27, May 2019: The CID lapsed millions of crores placed on the credit card company, all the son of the inspector:** According to the police, these people used to make credit cards of American Express Bank in Australia via fake basis and PAN card.

- **20 May, 2019: Friendships on social media and then foreigners lime millions of rupees:** The cyber crime police have issued advisories for the general public. It says that - beware of an unknown person on social media. Do not befriend an unknown person. Also, do not share any of your documents on social media.
- **Oct 6, 2017**: **online fraud of millions of people across the country exposed, fir in meerut:** In the name of advertising, there is a massive online disclosure of fake online disclosures. About 30 million rupees are coming out so far. The FIR has been registered in Meerut after the investigation. Dishonestly clicking on some emails, clicking on clicks may lead to losses. For example: Hello, Purchase, Urgent, Important, Follow-up and Request etc.

Here some of the cyber crime and punishment under IT Act 2000 is shown which the following is.

- **Hacking: Sections and Punishment:** Under the provisions of section 43 (A), Section 66-IPC, 379 and 406 of the IT (Amendment) Act 2008, a fine upto three years imprisonment or up to five lakh rupees can be fined.
- **Steal any kind of information or data:** In such cases, according to Section 43 (B), Section 66 (E), 67 (C), Section 379, 405, 420 of IPC and conviction under copyright law, According to the severity of the crime. Up to three years jail or up to two lakh rupees can be a fine.
- **Spreading any type of virus:** In such cases, Section 43 (C), Section 66 of the IT (Amendment) Act 2008, Section 268 of the IPC and Section 66 (F) related to cyber terrorism is also installed on the virus spread to threaten the country's security. There is a provision for life imprisonment in cases related to cyber-war and cyber-terrorism, while in other cases there can be up to three years of prisons or fines.
- **Stealing someone's identity:** Theft of identity and the use of private information in an unauthorized manner are also called cyber-crime. In such cases, there is a provision for section 43, 66 (c), Section 419 of the IPC, of IT (Amendment) Act 2008. Where the conviction is proved, there can be up to three years jail or up to one lakh rupees fine.
- **Frauding via e-mail:** If anybody falsifies any kind of e-mail, then in such cases, Section 77B of IT Act 2000, Section 66D of IT (Amendment) Act 2008, section 417, 419, 420 and 465 of IPC There is a provision to go. Upon three years of conviction, a jail or a fine can be up to three years.
- **Expanding pornography:** In any case, there is a provision for punishment under Section 67 (A) of the IT (Amendment) Act 2008, Section 292, 293, 294, 500, 506 and 509 of the IPC. In the case of seriousness of the crime, the first mistake can be up to five years' imprisonment for a jail or up to ten lakh rupees but for the second time, the jail sentence can increase for seven years.
- **Child pornography:** In serious cases such as child pornography, there is provision for punishment under Section 67 (B), IPC sections 292, 293, 294, 500, 506 and 509 under the IT (Amendment) Act 2009. First offense can be a penalty of up to five years of jail or up to ten lakh rupees. But on the second offense, there can be up to seven years jail or up to Rs. 10 lakh fine.

Cyber Law in India

List of Offenses and Related Penalties

Offenses	Penalty	Section
Manipulating Computer Source Documents	Up to three years of imprisonment, or up to 200,000 fines	65
Hacking	Up to three years of imprisonment, or up to 500,000 fines	66
Getting stolen computer or communication equipment	Up to three years of imprisonment, or up to 100,000 fines	66 B
Using someone else's password	Up to three years of imprisonment, or up to 100,000 fines	66 C

Cheating using computer resources	Up to three years of imprisonment, or up to 100,000 fines	66 D
Publishing personal images of others	Up to three years of imprisonment, or up to 200,000 fines	66 E
Acts of Cyber Terrorism	Up to life imprisonment	66 F
Publishing information in electronic form	Up to five years of imprisonment, or up to 1,000,000 fines	67
Publishing pictures of sexual acts	Up to seven years of imprisonment, or up to 1,000,000 fines	67 A
Publishing child porn	Up to five years of imprisonment, or up to 1,000,000 fines on first conviction and Up to seven years of imprisonment, or up to 1,000,000 fines on first conviction on second conviction	67 B
Failure to maintain record	Up to three years of imprisonment, or up to fines	67 C
Failure to follow orders / denial	Up to three years of imprisonment, or up to 200,000 fines	68
Failure / Decline to Decrypt Data	Up to seven years of imprisonment, or up to fines	69
Securing access or secure access to a protected system	Up to ten years of imprisonment, or up to fines	70
Seduce/Misrepresentation	Up to three years of imprisonment, or up to 100,000 fines	71

Conclusion:

In today's present time there is no threat to cyber crime than humans. Protecting people from any country's society and society in terms of security is a key part of keeping cyber crime safe. With the introduction of new technologies, cyber criminals are increasingly increasing crime and speed. The Indian government has created IT Act, 2000 to deal with the growing cyber crime. Cybercrime can be done by sitting in any corner of the world; it is very difficult to catch the criminals who commit cyber crime outside. Given the situation of today's cyber crime, all countries will have to fight together against cyber crime. Therefore, our main objective of writing this paper is to make people aware about the continuous cyber crime in the NCR. In the end, through this paper 'A Study on Cyber Crime and Cyber Law in NCR Region', we want to say that continuous cyber crime in NCR can never be accepted. In the future, if a person is attacked by the cyber, if the victim is attacked, then help him and register the case in the city's cyber cell or police station. All criminals who commit a cyber crime will get severe penalties so that they cannot do cyber crime again in future and if the cyber criminals do not complain, they will not be punished and will continue to do some cyber crime at all times.

Acknowledgement

I would like to thank Dr. Manoj Kumar (Associate Professor, Computer Science) of Shri Venkateshwara University for his incomparable guidance. Who have helped me write this paper and wrote this review paper successfully.

REFERENCES

1. Handbook Of Research On Modern Cryptographic Solutions For Computer And Cyber Security; Brij Gupta., Dharma P. Agarwal , Shingo Yamaguchi , 1st Ed.2016.
2. Information Technology, “Law and Practice: Cyber Law and E- Commerce”, 2004.

3. Industrial Network Security, 2nd Ed: Security Critical Infrastructure Networks for Smart Grid, Scada, and Other Industrial Control Systems; 2nd Ed. Eric D. Kanapp, Joel Thomas Langill., 2014.
4. John R. Vacca., "Cyber Security and IT Infrastructure Protection", Sept. 2013.
5. Justice Yatindra Singh, "Cyber Laws", 2010.
6. Jyoti Rattan, "Cyber Laws and Information Technology" (Bharat Law House Pvt. Ltd, New Delhi 4th Ed. 2014.
7. https://goosevpn.com/blog/origrn-cybercrime
8. https;//outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks
9. http://editorial.mithilesh2020.com/2016/05/online-security-tips-in-hindi-article.html
10. https://computerhindinotes.com/what-is-internet-security/
11. https://economictimes.indiatimes.com/tech/internet/do-you-know-how-to-report-a-cyber-crime-heres-a-guide-for-victims/articleshow/61464084.cms?from=mdr
12. https://www.youthkiawaaz.com/2018/06/common-cyber-crime-scenarios-and-applicability-of-legal-sections/
13. https://indianexpress.com/about/cyber-crime/
14. https://navbharattimes.indiatimes.com/india/one-cyber-crime-happens-every-10-minutes-in-india/articleshow/59709786.cms
15. https://hindi.news18.com/news/jharkhand/ranchi-ranchi-police-arrested-2-cyber-criminals-jhnj-2169085.html
16. https://www.businessinsider.in/The-12-Most-Common-Email-Mistakes-Professionals-Make/articleshow/38154720.cms
17. https://optinmonster.com/email-marketing-mistakes/
18. https://niiconsulting.com/checkmate/2014/06/it-act-2000-penalties-offences-with-case-studies/
19. http://www.mondaq.com/india/x/785836/White+Collar+Crime+Fraud/Cyber+Theft+A+Serious+Concern+In+India
20. https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/the-12-types-of-cyber-crime.html
21. https://itstillworks.com/types-cyber-crimes-penalties-1808.html
22. https://aajtak.intoday.in/crime/story/these-ipc-sections-impose-on-cyber-criminals-1-855373.html
23. https://hinditechacademy.com/india-me-cyber-crime-karne-par-kanoon-aur-saja/
24. http://nagapol.gov.in/PDF/IT%20Act%20(Amendments)2008.pdf
25. http://onlinekpsc.blogspot.com/2015/12/important-sections-of-it-act-2000.html
26. https://en.wikipedia.org/wiki/Information_Technology_Act,_2000