International Journal of Engineering Research & Management Technology
ISSN: 2348-4039
September-2019 Volume 6, Issue-5
Email: editor@ijermt.org www.ijermt.org

CYBER CRIME AND ITS IMPACTS IN NCR: A SCRUTINY

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

ABSTRACT
There is no doubt that today's present day is of computer and internet or else it is said that today's era has given birth to the Internet revolution. 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. According to the fact that cyber crime is increasing, cyber crime is very bad for the people living in society and society, for the nation and for the economy. If it is not stopped then it will have very serious consequences which can be very difficult to imagine. Cyber crime has a very bad and big impact on people living in society and society. To understand the effects of cyber crime on society and society, analysis of its environment and behavior is very important as it is its basis. To understand the effects of cyber crime on society and society, analysis of its environment and behavior is very important as it is its basis. Therefore, in view of the time coming in this paper, the area of impact of cyber crimes, people living in the entire NCR and the impact of the society has been provided.

Keywords: Cyber Crime, Types of Cyber Crime, Cyber Law in India, Impact of Cyber Crime in NCR Region, 2019 Cyber Crimes Trends

INTRODUCTION
Due to the use of internet, today's present era is moving very fast forward. All users who are using the computer today have been able to do this by many scientists. The computer is an electronic device designed to get information. In today's present time, Internet is the largest system of information technology. Millions of computers are connected with each other through the Internet. In other words, connecting all computers with each other is called the Internet and when this network is established, it becomes a very large network called the Global Network.

Nowadays everyone experiences pleasure by using the internet. Every coin has two facets that mean the use of the Internet on the one hand and the misuse of Internet on the other hand gives rise to cyber crime. In other words, "cyber crime or computer crime is a crime under which computer and network are involved" Which relates to criminal activities like stealing personal information from someone's computer system or any other databases, manipulating on-line data etc. Finally, it is revealed that in the NCR, the Internet is growing steadily in the form of cyber crimes. Here are some cyber criminals who have been described below:

- **Script Kid's Hacker:** There is no lack of technical expertise in this type of hackers. These are usually only very weakly able to attack safe systems.
- **Scammer:** This type of hacker sends you spam or some other form like email, related to discounts, shares related, etc related to advertising.
- **Hacker Group:** These types of hackers usually make different types of tools to hack devices and silently complete their work. However, sometimes such types of hackers are used by large companies for their safety.

- **Phishers:** Thus, hackers can get all the personal information of your bank account by email or by phone. Do not come in the way of their mischief if you are trapped in their trap.
- **Commercial Group:** These types of hackers tend to take financial advantage and spread malware for political gain. According to a report it was believed that the Stoxnet worm which attacked the atomic facilities of Iran's nuclear program was made by a foreign government.
- **Insider:** This type of hacker only shows that it is very dangerous. They lose approximately 70% to 80%. These often reside within an organization.
- **Advanced Continued Threat (APT):** They are responsible for the attacks on the excessive targets and they have a very large resource, as well as new techniques have high knowledge of this, through which they reach other computing resources easily.
- **Salami Slicing Attackers:** 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. We can say that salami attack is a financial offense.
- **Cyber Bullying:** Cyber bullying means that someone is showing cyber bullying, showing dirty language and pictures on the Internet or threatening anyone on the Internet and scaring or torturing it. This crime is like cyber stocking. Crime has taken its children, youth and adults into today's society and society. In particular, this crime has targeted the children, which has a very bad effect in the lives of children.

OTHER TYPES OF GENERAL CYBER CRIMES

- **Hacking:** Hacking means if we understand in simple language, it means that logging any computer system without any permission and stole all its data. Hacking is done only by computer hackers. There are also several types of hacking such as: network hacking, e-mail hacking, website hacking, computer hacking and password hacking etc. Hackers can steal any person's personal information and financial data completely. We also call hackers an intruder in other languages.
- **Virus Dissemination:** The meaning of the virus is a kind of worm and dissonance means the spread. Simply put, the virus is spreading. These crimes are mostly from social sites. When the virus comes from somewhere in the computer system, there are some programs themselves that start to run, which you do not want to run. The basic spread of the virus is through internet and website. There is a virus in a form of malware software that spreads in computer pieces in many pieces as software.
- **Theft:** If we say theft in simple language, then it means "steal". In a way, it happens through the internet, which relates to "theft" and which we know as "Internet Thief". This crime happens through a number of mediums, Includes fake emails, and viruses. The main goal of this is to steal a person's personal information and use it illegally and steal all the money from that person's account.
- **Identity Theft:** Theft of someone's identity comes only within the purview of cyber crime. It is also seen that criminals make those people their victims, who do many transactions through online banking. This crime is committed by cyber criminals who are active on the internet at all times. These people usually get any personal information of any person such as email address, credit card number, bank account number etc.
- **Ransomware:** Ransomware is a very dangerous virus that penetrates your computer network and corrupts all your files so that you cannot access that file. This crime has also affected the country's big companies. This ransomware attack is believed to be the biggest attack in cybercrime. Ransomware is designed to completely block any computer.
- **Malicious Software:** If this type of software is inserted into any computer system, then hacker can steal all the computer data or change it with the help of that explosive device. This software is created by a software developer or hacker. This software can enter your computer from any date, Such as through a website etc.

- **Web Jacking:** In this way, the hacker takes control of it illegally by taking possession of a person's website illegally and then the entire control of the website goes to the hacker. The name of the duplicate website is changed slightly and there are other types of content like malware, Such as pnb.com at the place of pnbs.com can be written. By the way, this type of Fake website can be easily ignored.
- **Denial of Service Attack (DOS):** If this is the case of crime, the hacker targets the server in which the user has a problem and cannot use the service as he wishes. The result of this crime is that heavy traffic is sent to the hackers by which the server becomes slower and later becomes bad or inactive. So we can say that "Daniel's service" means that the user is deprived of any kind of service.

CYBER LAW IN INDIA:

In India, in every section of Cyber Law, there is a provision of penalties ranging from Rs 20,000 to Rs 1,000, 000, and there is also a provision of punishment from three years to five years. . Here are some sections which are the following –IT Act 2000, Section under – 65, 66, 66 B, 66 C, 66 D, 66 E, 66 F, 67, 67 A, 67 B, 67 C, 68, 69, 70 and 71 .

IMPACT OF CYBERCRIME IN NCR

According to a report, it was also informed that in the recent years, cyber crime "special concern" has been increasing in NCR (Noida, Faridabad, Ghaziabad and Meerut) cyber crime has increased rapidly in the NCR region in recent years. There are number of call centers. In the last 6 months of 2019, 23,852 cyber crime cases were registered in NCR. According to a report, there is a cyber crime every 10 minutes in the NCR region.

- **Impact of cybercrime in Noida :**For people moving towards the digital economy, as the people are becoming smart through social media and smart phones, Noida is growing steadily in the city as well as the number of cyber crimes in the city is increasing ever increasing. According to a report, about 1,125 cases related to cyber crime in Noida were registered in the year 2018, whereas in 2019 this figure has reached approximately 1,875, which means within one year there has been a rapid increase in cyber crime cases. From this one thing is clear that Noida is becoming a center of cyber crime.
- **Impact of cybercrime in Faridabad:** According to a report, about 1,500 cases related to cyber crime were registered in Faridabad in 2018, whereas in the year 2019 this figure has crossed 2000, meaning daily cyber crime cases arise. Here are more youths and women than the target of cyber criminals. One thing is clear that Faridabad is also becoming a center of cyber crime.
- **Impact of cybercrime in Ghaziabad:** According to a report, in the year 2018, about 1,213 cases related to cyber crime were registered in Ghaziabad, whereas in the year 2019 this figure has reached around 1800, in which cases are from Vijay Nagar city and other residential areas. There are also cases of cyber crime every day.
- **Impact of cybercrime in Meerut:** According to a report, about 1300 cases related to cyber crime were registered in Meerut in 2018, whereas in the year 2019 this figure has reached around 1850, there has also been a sharp increase in cyber crime cases. From this one thing is clear that Meerut is also becoming a center of cyber crime.

In today's modern times, cyber criminals take great advantage of the introduction of new technology. This is a useful tool especially for scammers, hackers and other cyber criminals on the Internet in which criminals hide their work behind the shield of digital ignorance. Cybercrime in the world affects the society both online and offline. According to Professor Howard Rush, "Russia, China and Brazil are ahead of cyber crime in the field of competition between individuals while software companies in the US and Europe, India, Brazil and Russia are promoting their work in the field of information technology. According to a report, "There has been a rapid increase in cyber crime in the NCR" in the number of hacking, spam, theft, fraud and other cases has increased by 50% faster than 2015 to 2019.

- **Identity Theft:** If you become a victim of cyber crime then its effect remains for a long time. In this, the cyber criminals attempt to steal the personal information of any bank or other financial institution by phishing. If you give your personal information to the cyber criminals then the culprit goes to your bank and credit accounts easily and opens a new account that eliminates the rating of your credit card. It can take several months or even years to repair this type of damage, so you have to learn to protect your personal information which is very important.
- **Security Cost:** In this, cyber criminals attack businesses on either large or small scale. The culprit can steal the information from the main server and use the machines to fulfill its objectives. The company keeps the personal information of the employees of the companies on the main server itself. According to a report, a survey was conducted in which large companies spent an average of $ 10.8 million per year.
- **Monetary Damages:** This type of cyber crime is directly related to money loss. According to a report, more than 1.8 million people are victims of some type of cyber crime in 2018. Cyber criminals have used mobile, computer and other digital devices for their own benefit.

During the visit, the researcher has observed a growing cyber crime in the NCR. Talking about the entire NCR, there are students and students of college, youth and women affected by cyber attacks. There is a case of cyber crime every day in the NCR. There are more than 15000 cases of cyber crime registered throughout the NCR. Cyber crime is having a very bad impact in our society. Here are more youths and women than the target of cyber criminals. Cyber criminals take full advantage of confidentiality and oblivion, which attack the society. Cyber criminals attack by computer viruses, cyber stalking, cyber bullying, identity theft, malware, spam, denial of service attacks and etc. Apart from this, the impact of cyber crime also affects the business. Cyber criminals attack businessmen because businessmen have important data and many times cyber criminals have been successful in attacking. According to a report, it has been reported that cyber criminals may be hidden in any corner of the country. Where they see any weakness they attack and target the same place.

Most consumers in NCR say that they want to control the privacy of the Internet without any hassle or cost, because some companies ask for their costs to protect. According to a researcher survey, 40% of respondents believe that they are not aware of cyber crime, while 60% of respondents believe they are more concerned about the privacy of the Internet.

2019 CYBER CRIME TRENDS

Today's threat is not in front of the threat of tomorrow, and therefore our responsibility should also be large. Cyber crime has taken the form of an industry all over the world. Having the resources and information in the wrong hands has increased the fear of such crimes. At present, if this is the biggest concern, then it is "cyber crime". "Cyber crime" has emerged as a major challenge in front of everyone, whether it is a private institution or a financial institution or any other government institution. Due to the misuse of the Internet hacking can be harmed by their important data. If it is not stopped at the time, then the possibility of stealing money in the coming time will increase. In today's time people are getting bullied through internet exchange. According to Central Minister," With the availability of radical ideas on the Internet, the responsibilities of agencies engaged in law and order has increased. The fundamentalist ideology has not only made a fatal change in the society but has also changed human values. The biggest challenge in the coming time will be to deal with the crimes of online methods and the expansion of terrorism. We have to think about dealing with this and have to prepare a comprehensive strategy for it. During this time, the cyber security network will break data theft and illegal transactions, computer malware and other online crimes will increase. Cybercrime has taken the status of an industry in the world. The tools and techniques to execute these are being sold openly. The service is being offered. With the availability of such technology and equipment at

affordable rates, their risk of expanding and abuse has increased. Digitization of financial services has raised huge responsibilities of alertness towards security measures. Need to strengthen the control and monitoring process to prevent online economic crimes".

Dell, a multinational computer technology company, also warned that in spite of strict security arrangements across the world in 2019, cases of cyber crime have increased, which is a matter of concern in itself. Crime in cyberspace is increasing every year by 22 percent. Cyber crime is also increasing at the same pace that the computer and the internet are using. Social media and Internet misuse in the country is becoming a matter of concern. In order to deal with cyber crime, India has extended cooperation with countries like America, Israel, Australia and Britain.

According to Einaras von Gravrock : In today's present time, cyber criminals are continuously trying to break and steal user privacy through advanced and scalable devices of high quality. According to the 2017 records, records of nearly 2 billion data were compromised, which broke the 5.6 billion records within the last 6 months of 2018. Here are the most cyber-security issues in 2019, as well as growing trends in 2020.

- **Advanced Phishing Kit:** If seen, about 4 to 5 malware samples are made by cyber criminals every second. The speed of phishing is very fast and due to its speed, it is the most accurate weapon of cyber criminals. The reason for this is that most phishing websites last for 5 to 6 hours. 25% of users report complaints of phishing attacks. This is the reason that because of the fish being online, it puts more pressure on consumers. Nowadays almost 70% of the URL is trusted. So it has been estimated that in the year 2020, the phishing attack will be the top. The root cause of this is that the number of phishing numbers is countless and it remains online on the website. Phishing will also become a dangerous attack method by high-powered equipment.
- **Attack by Remote Access:** The number of attacks of this kind continues to increase, which is in a much more complex form. According to the major report of 2018, one of the remote access attacks was a crypto jacking, which made the targets for the owners of crypto currency. According to an intelligence database, attacks by remote access attacks are a common vector in the vector, in which computer, Internet Protocol (IP); Smartphone, Network Attached Storage (NAS) and etc. devices are targeted. The reason for this is that for this type of equipment on the Internet or outside network, the port needs to be open and forwarded to it.
- **Attacks by Smartphone:** This type of attack, such as Speed Fishing, Malware and Phishing etc., is done by an insecure browsing which is the top of the Smartphone. According to a report of RSA, online fraud is done via Smartphone, which is 60%. Also 80% more fraud is done through mobile app. Most people use their phones for financial operations, while it is becoming a major threat. There is also a fact that the user usually puts all his personal information in the phone. Two factors come out first, the first is to use the phone widely and the other is that the phone is lost or stolen.
- **Vulnerabilities in Home Automation and Internet of Things:** According to Gartner's report, by the end of 2020, more than seven billion devices are expected to grow. Consumer Internet of Things devices is not considered as consumer vulnerabilities, the reason is that this is not a user interface. There may be a problem understanding this type of device that collects or manages the data. However, Internet of Things devices are not protected by the design, because its maintenance costs significantly increase due to its security. Not only does the user collect data through Internet of Things devices, but it is a point of launching a distributed denial-service for the attacker. According to an intelligence data of CUJO AI, 46% of these devices have remote access while 39% are used to detect behavior patterns.
- **Use of artificial intelligence:** As many of the major industries as of nowadays, the use of artificial intelligence and machine learning is being done in the past to properly execute their processes and improve their good performance. If seen, AI is considered as a two-pronged technique in which the first is to protect the companies from the dangers of safety and the AI-operated algorithms. This makes

hackers even more likely to be effective. AI mostly works for malicious purposes. The AI systems are anonymous, scalable, cheap and automated and they maintain a distance from the attackers by reducing the effects of cybercrime. Artificial intelligence for cyber-security theft: Cyber criminals are using various methods to avoid detection and steal. AI helps in customizing elements of various types of this process. Artificial intelligence in phishing: AI is helpful in creating a material that can pass through specific types of cyber security filters.

- **Artificial Intelligence in Social Engineering:** The popular hacking is seen by social engineering as it is one of the new techniques. It takes a lot of time to implement it well. AI can also help in collecting information. In the coming time, using AI in cyber attacks will become the most popular and dangerous. Finally, to keep "cyber safe" in the next 5 years, awareness of the same level will now be given to ensure that we are digitally safe.

CONCLUSION

This manuscript has not only highlighted the cyber crime but has also explained the impact of cyber crime on every part of the NCR. This will help to keep all kinds of online information safe. It will be helpful to control the effect of crime being lodged in the NCR. Applying AI properly to overcome these crimes will open a new way to control cyber attacks.

REFERENCES:

1. "An introduction to Cyber Crime and Cyber Law", 2008, Kamal Law House
2. Anirudh Rastogi, Cyber Law, "Law of Information Technology and Internet", (Lexiz Nexis) Reid Elsevier, India Pvt. Ltd, Gurgaon, 1st Ed. 2014.
3. Beyond Cyber Security: Protecting Your Digital Business; James M. Vaplan, Tucker Bailey, Derek O' Hall Oran, Alan Marcus., 1st Ed. 2015.
4. Blue Hand Book: Incident Response Ed; a Condensed Field Guide for the Cyber Security Incident Responder; Don Murdoch GSE., 2014.
5. "Committee on Homeland Security House Of Representatives": "Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure", Create Space Independent Publishing Platform, Jan. 2014.
6. Countdown To Zero Day: Stuxnet and the Launch of the World's First Digital Weapon; Kim Zetter., 2014.
7. "Cyber Law" Jain Book, New Delhi, 2012.
8. Cyber Crime and Cyber Warfare; Igor Bernie. 1st Ed. 2014.
9. Cyber Security in Organizations; E- Fritz vold, Omega Tech Series, Independently Published, Sept.2018.
10. http://hindi.webdunia.com/article/it-learning/
11. https://www.1hindi.com/essay-on-cyber-crime-in-hindi/
12. http://hindikiguide.com/-essay-on-cyber-crime-in-hindi.html
13. https://www.faronics.com/news/blog/7-types-of-cyber-criminals
14. https://navbharattimes.indiatimes.com/state/uttar-pradesh/noida/noida-ready-to-deal-with-increasing-cyber-crimes/articleshow/63974356.cms
15. https://yourstory.com/hindi/f6bc22269c-cyber-crime-is-a-major-problem-in-the-age-of-digital-india-to-the-credit
16. https://thefinancialexpress.com.bd/views/cyber-crime-affects-society-in-different-ways
17. https://digital.wings.uk.barclays/for-everyone/milestone/impacts-of-cyber-crime/
18. https://itstillworks.com/effects-cyber-crime-1704.html
19. https://naidunia.jagran.com/national-cyber-crime-industry-has-become-a-big-challenge-for-the-future-1605317
20. https://aajtak.intoday.in/crime/story/cyber-crime-increased-in-2015-1-856730.html
21. https://www.gov.uk/government/speeches/a-free-open-secure-cyberspace-for-all.hi
22. https://us.norton.com/cyber-security-insights-2018
23. https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf
24. https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019/
25. https://me.devoteam.com/newsroom/article-cyber-security/