Cyber Crime: A Major Concern

Surbhi Bahl[1]

[1]Assistant Professor, Guru Nanak Dev University, Regional Campus, Gurdaspur (Punjab)

Abstract

In today's world there are large number of people who are dependent on computer and internet. This has lead to creation of a vast cyber space. Internet is a tool which provides many services to the people like online learning, online ticketing, online marketing, online banking etc. There are also many undesirable activities which are evolved from the internet. These days Internet is used as a tool for committing serious crimes and offences which are referred to as cyber crimes. A cyber crime is an illegal activity which is carried out through a computer or a network. Any person, government or property can be a victim of cyber crime. It can be committed by getting unauthorized access to a computer or network, stealing personal information, installation of virus, causing disruption of services, hacking, fishing, forgery, defamation etc. A cyber crime may cause any financial or non –financial loss to a person. The hackers can steal the sensitive information and use it to make gains. Cyber crime is coming up as a global issue which is a hindrance in the development of nation. A high priority should be given to the security and privacy of the users. In India the cyber laws are contained in the Information Technology Act 2000.The Government has also set up many cyber crime cells for regulating the cyber activities. Though there are many cyber laws acting in force but it is also the duty of an individual to use the computer or internet in the most responsible and safe manner.

Keywords: spoofing, hacking, virus, pornography, spamming, cyber crime.

Introduction

There has been a considerable advancement in the field of Information and Communication Technology. Internet has given a vast access to everyone. The revolution in cyber has helped to reach the masses easily. In this present tech savvy world, everyone is engaged in internet but some criminal minded people are using it for bad purpose which leads to cyber crimes. Cyber crime is a crime of very serious nature as it is illegal. It includes unsolicited emails. The people who commit these crimes are usually referred to as hackers. Joseph –Marie Jacquard, a textile manufacturer of France is recorded to be the first victim of cyber crime in 1820. He produced the loom. Loom was a device which allowed repetition of a series of steps

in the weaving of special fabrics. His employees were threatened as they thought that their employment was in danger. Jacquard's employees committed the acts of sabotage to discourage him from using this technology.

Concept

Cyber crime is a crime which uses computer or internet for carrying out criminal activity. Computer can be used both as a target or a weapon for conducting cyber crime. It is computer oriented so it is also known as a computer crime. It is evil in nature as it is a threat to an individual's privacy and it may also lead to loss of an individual's confidential data and his identity. Cyber criminals are misusing the computer technology for carrying out malicious activities. Cyber crimes can be committed by anyone including young professionals, insiders, juveniles, disgruntled employees. Cyber security has become the concern of every person.

Types of Cyber Crimes

- ➢ **Identity theft-** In this the personal identity of a person can be stolen by an intruder. They may also steal his bank account information which can further cause monetary losses to the person.
- ➢ **Hacking-** It is an illegal intrusion into a computer system or network. It is done by a hacker. The hacker is highly skilled person who gets an unauthorized access to or control over a computer network. He finds loopholes and weaknesses in the system. He can also steal the sensitive information like bank account details, card details or data. Sometimes they are also referred to as crackers.
- ➢ **Cyber stalking-** In this case the stalker monitors the activities of a person online. The main motive of the stalker is to gather all information about the person which can further be used to harass or blackmail the person.
- ➢ **Computer vandalism-** In this case the data of the computer system is neither stolen nor misused but it is actually destroyed.
- ➢ **Computer intrusion-** It is an act of getting an unauthorized access to a computer system or network and harming it. It involves activities like spreading of virus, denial of services, modification of data etc.
- ➢ **Denial of service-** In this case the attacker intends to prevent the users from accessing the network. The perpetrators make the machine or network temporary unavailable or disrupts the services of a host connected to the internet. The attackers usually target the websites which are hosted on high profile web servers like banks or credit card payment gateway.
- ➢ **Smurf attack-** It is a type of Denial of service attack (DOS) in which a large traffic is generated to the victims network which leads to crashing of the network.
- ➢ **Email bombing-** It is a malicious act in which bulk emails are sent to the victim's email account or mail server in a short period of time. It will put the victim in a frustrating situation and in some cases it may also lead to crashing of the mail server.
- ➢ **Email spoofing-** It is a very serious type of cyber crime. It is a tactic in which an email appears to originate from one source but it has actually been sent from a different source.

There is an alteration of sender's information. It is done to falsify the people as they are more likely to open an email when they think that it is from a legitimate source.

➢ **Cyber bullying-** Children are the main victim of cyber bullying. It is a type of harassment which is done by using electronic means. It includes sharing of negative information or spreading rumors about someone which can lead to harassment of a person. This lowers the self esteem of a person and ultimately leads to suicidal attempts.

➢ **Virus-** Virus is considered as very dangerous as it can bring a computer system to halt. It can be loaded into a computer system without the person's knowledge. These viruses can reproduce themselves and can also get attached to other computer programs.

➢ **Web jacking-** In this case the criminal illegally gains access and takes over the control of the website without the prior approval of the owner. The criminal can then use the webpage according to him and can also make any modifications.

➢ **Illegal pornography-** Children are the most common victim of this act. Pornography refers to showing sexual acts in order to induce sexual excitement. Pedophile makes a contact with the children and tries to fool them by offering money or opportunities. The photographs of the children are shared on internet for money. They are used as sexual objects.

➢ **Spamming-** In this case the emails or text messages are sent over to a large number of people over the internet. This is usually done for advertising the product. These messages can be unwanted, intrusive, irrelevant or unsolicited.

Preventive measures

➢ The computer systems should be protected by setting up a powerful firewall to provide security to the systems. Antivirus programs should be installed to avoid any virus affecting the operations of the computer.

➢ There should be a continuous check on the traffic of the website.

➢ There should be a proper backing up of data so that there is no loss of important information.

➢ Don't disclose your personal information with anyone as it may lead to privacy issues.

➢ The user should use a strong password comprising of alphabets, numbers and special characters so that there are less chances of hacking the password.

➢ Avoid keeping the same password for various websites.

➢ Don't keep a simple and easy to guess password.

➢ Never save your password in the computer system.

➢ Carefully read the privacy policy of a website before submitting your personal information.

➢ Any unnecessary software should be uninstalled from the computer system.

➢ The password of the computer or network should be changed after a certain period of time to avoid any kind of exploitation.

➢ The services of a security expert can be hired to detect any kind of threats.

➢ The operating system should be updated. The new updated system will avoid any time of invasion and will act as a shield to the personal information of the person.

➢ Don't share your personal photographs with anyone online as they may get misused.

Major cases of cyber crime in the world

- In 2017, UK had fallen victim to a very major cyber crime. A virus named The Wanna Cry was penetrated into NHS computer system. The hospitals and medical practitioners were victimized and they had to carry out their work offline. The NHS system went completely disabled for a week.
- In the year 2013, Yahoo had faced a very big problem of data theft. The personal information like name, phone number, passwords and email addresses of one billion users of Yahoo was stolen.
- Sony, a major entertainment company has also been a victim of cyber crime. It was in late 2014 that a virus was penetrated into their system and around 100 terabytes of sensitive information was stolen from the company.US agencies claimed that North Korea had authorized this cyber crime because they disapproved the film 'The Interview' which predicted Kim Jong-un in a humorous manner and the film even showed an attempt of assassination of The Head of the State.
- Binny Bansal, CEO of Flipkart has been a victim of Email spoofing when two emails in his name were sent to Sanjay Baweja, CFO of Flipkart. The emails directed him to transfer a huge amount of $80000 in the account of Mr. Binny Bansal. Later on it was cross checked and the fraud was detected.
- An incident of cyber spoofing was recorded on July 5, 2016 by an NGO run by Ronnie Screwvala, a renowned producer. He told his employee to transfer an amount of Rs.20.20 lakh in a bank account. Later on the criminals had sent more such emails. The fraud was detected after a whooping amount of over Rs.34 lakh was transferred. A complaint for the same was lodged with the cyber police.

Conclusion

Like any other activity, internet has also got certain advantages and disadvantages. With more people surfing on the internet, they have started using it in an inappropriate manner. Security threats have caused massive harm to the people. Computers are more vulnerable to threats because they store large amount of data and they can be easily accessed by the professionals. Computers are being misused and this has increased the scope of criminal activities. Crimes like infringing upon another person's copyrighted material and illegal downloading are also on the rise. Cyber space should be considered as a home and adequate measures should be undertaken to safeguard it. It is the duty of every user to accumulate information about the cyber crimes and to adopt preventive measures. Every user should be prepared for any kind of intrusion and should be able to identify any kind of risks. The users must be aware of their rights and duties. We cannot totally eliminate cyber crime but we can definitely have a check on them.

References

https://www.techopedia.com/definition/2387/cybercrime.

https://m.huffpost.com/us/entry/12450518.

http://cybertimes.in/?q=node/540.

http://supportz.com/the-five-most-common-types-of-cyber-crime/.

https://www.enotes.com/homework-help/define-five-categories-cybercrime-give-an-example-478828.

https://www.slideshare.net/mobile/aemankhan/cybercrimeppt-27376284.

http://www.bezaspeaks.com/cybercrime/education.htm.

http://www.helplinelaw.com/family-law/CCII/cyber-crimes-in-india-what-is-types-web-hijacking-cyber-stalking.html.

http://wsilfi.staff.gunadarma.ac.id/Downloads/files/13309/W03-Cyber+crime.pdf.

http://www.bezaspeaks.com/cybercrime/intro.htm.

http://www.byte-notes.com/what-cyber-crime.

http://www.indiaessays.com/essays/india/cyber-crime/essay-on-cyber-crime-in-india/1080 http://www.cyberlawsindia.net/index1.html.

https://www.thesun.co.uk/tech/4120942/five-of-the-worst-cases-of-cyber-crime-the-world-has-ever-seen-from-data-theft-of-one-billion-yahoo-users-to-crippling-the-nhs/.

http://blog.logix.in/email-spoofing/.