Review on Cyber Crime: Threats And Preventions

Miss. Poonam Wavare

Lecturer, Computer Engineering Department, V.P.M's Polytechnic, Thane, Maharashtra, India

Abstract – *Crime is a common word that we always heard in this globalization era. Crimes refer to any violation of law or the commission of an act forbidden by law. Over the past two decades, cybercrime has become an increasingly widely debated topic across many walks of life. It's clear that rapid growth of the internet has created unprecedented new opportunities for offending. It is defined as crimes committed on the internet using the computer as either a tool or a targeted victim. This paper presents the types of Cybercrime Activities, important issues on the Security, Prevention, and Detection of Cyber Crime.*

***Key Words*: Cyber Crime, Malware, Fraud, Hacking, Phishing etc.**

1. INTRODUCTION

Crime and criminality have been associated with man since long time. Cyber crime is also known as computer crime that refers to any crime that involves a computer and a network. It is an ago. There are different strategies used by different countries to contend with crime. It is depending on their extent and nature attack on information about individuals, corporations, or governments. Although the attacks do not take place on a physical body, they do take place on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. Computer can be considered as a tool in cyber crime when the individual is the main target of cyber-crime.

The term cyber crime can also be defined as an act committed or omitted in violation of a law forbidding or commanding it and for which punishment is imposed upon conviction. Other words represents the cyber crime as ―Criminal activity directly related to the use of computers, specifically illegal trespass into the computer system or database of another, manipulation or theft of stored or on-line data, or sabotage of equipment and data.

1.1 Types of Cybercrime Activities

Cybercrime ranges across a spectrum of activities. At one end, are crimes that involve fundamental breaches of personal or corporate privacy, such as assaults on the integrity of information held in digital depositories and the use of illegally obtained digital information to blackmail a firm or an individual. At the other end of the spectrum are those crimes that involve attempts to disrupt the actual workings of the Internet. These ranges from spam, hacking, and denial of service attacks against specific sites to acts of cyber terrorism—that is, the use of the Internet to cause public disturbances and even death. Criminals committing cybercrime use number of methods, depending on their skill-set and their goal. Here are some of the different ways cybercrime can take shape:

- Theft of personal data
- Copyright infringement
- Fraud
- Child pornography
- Cyber stalking
- Bullying

2. DIFFERENT TYPES OF SECURITY THREATS

2.1. MALWARE:

Malware short for malicious software . It is used to interrupt computer operations, gather such kind of information or display unwanted advertise. 'Malware' include computer viruses, worms, Trojan horses, ransomware, spyware, adware and other malicious program. Malware is classified into several different types of term like:-

• Ransomware :
It is a type of mal ware. It is used to restrict to access to your computer or your files and they display demanding payment message in order for the restriction to be removed.

• Trojan horses:
Trojan horses is not familiar with everyone but it's good to know about it and how to protect it. It is also a part of malicious program. Trojan horses is executable file that will install itself and run automatically after once it is by mistake downloaded.

• Computer viruses:
A computer virus is a program or code that cause damage or steal some information and modify data, send e-mail and sometime its some combination of these actions. When you have some more important data or information then you must install antivirus in your computer. antivirus protect your computer against viruses.

• Worms:
Worms are common threat to computers. Worm goes to work on its own without attaching itself to files or programs. It lives in your computer memory but doesn't damage.

• Spy ware :
Spyware and adware are used by third party to interrupt your computer. Spyware means you don't know and spyware collect your personal information about you. Sometimes, they come in form of a "free" download and install automatically

without your permission or knowledge. These spyware difficult to remove and can infect your computer with viruses.

2.2. Fraud

Social networking sites also invite fake people to take good opportunity to become wealthy by applying fake schemes.

2.3. Criminal Activity and Money laundering

Today, Crime is very serious issues because internet media is a major resource for developing crime. Internet is growing day by day, In many ways online criminals try to present fake plans. Social networking sites has major challenge in financial and organized crime which damage the system.

2.4. Email Spoofing

Email spoofing is technique that is often used in conjunction with phishing in an attempt to steal some information to your computer. It is passing through email address so, you don't verify that the sender is real or not, because an email address may also include your name and the name of someone you know. Email spoofing is possible because SMTP (Simple mail transfer protocol) doesn't provide the mechanism for address authentication.

2.5. Phishing

Phishing is a threat, largely it use in social media like face book, twitter etc. In it attacker send several emails to more the victim. Attackers create a clone of web site and tell you to fill some personal detail which is in emailed to them. Phishing is very easy way to steal some information or data in another user or person. because phishing Attackers mostly attack people using these sites at their home, workplace etc to affect the user or company. With the use of these information attacker can change that person's username, password and some other personal detail also.

2.6. Communal Violence and Fanning Tensions

Social media playing a significant role in polarizing various communities in India and its security challenges. The false updates of communal clashes, viral videos, riots and terrorists attack have created a massive impact in the life of public. The power of media and the process of public opinion formation in a free society had undergone radical change due to Internet and faster means of communications like SMS, whats app, viber and simplified mobile internet. The chain of events beginning with the clashes in our Northeast and which caused very serious and mass exodus of Northeast population from several Indian cities has revealed the fragility of our national Cohesion.

2.7. Hacking

In a computer security, hacker is someone who abuse weaknesses in a computer system. Hackers attack the target computer using ready-made computer programs. Hackers break the security and steal the important data of save using social media. In social network, Hackers need very little technical skill to hacking something. Some time, hackers wants to use the victim's computer to store illegal materials like some software, pornography etc. and hack that computer and operate that personal data. It is like advantage and disadvantage of hacking. Hackers are also create or set-up fake ecommerce sites to access credit card details and gain all the details of credit card after that misuse that detail. Some - times people wants to revenge. Password cracking is a type of hacking. Social engineering, wire sniffing, man-in-the-middle, password guessing, key logger these all are the type of hacking.

2.8. Cyber bullying

Cyber bullying means harming or harassing via information technology networks in a repeated manner. That could be done via text messages or images, personal remarks posted online, hate speeches etc. cyber bullies may also disclose victims' personal data (Like real name, address) on website.

2.9. Cyber stalking

Cyber stalking use of the internet, e-mail, or other electronic communications devices to stalk another person. Cyber stalking is a criminal offense under various state anti-stalking and harassment law. Sometimes, cyber stalking includes identity theft, vandalism or sexual harassment.

3. CYBER PREVENTION AND DETECTION

The mantra of any good security engineer is: 'Security is a not a product, but a process.' It's more than designing strong cryptography into a system; it's designing the entire system such that all security measures, including cryptography, work together.
A state of computer "security" is the conceptual idea, attained by use of three processes: threat prevention, detection, and response. These processes are based on various policies and system components, which include the following:

- User account access controls and cryptography can protect systems files and data, respectively.

- Firewalls are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering.

- Intrusion Detection Systems (IDSs) are designed to detect network attacks in progress and assist in post-attack forensics, while audit trails and logs serve a similar function for individual systems.

- "Response" is necessarily defined by the assessed security requirements of an individual system and may cover the range from simple upgrade of protections to notification of legal authorities, counter-attacks, and the like.

4. PREVENTION TIPS

- Keep your computer current with the latest patches and updates
- Make sure your computer is configured securely
- Choose strong passwords and keep them safe
- Protect your computer with security software
- Protect your personal information
- Review bank and credit card statements regularly

5. CONCLUSION

This manuscript put its eye not only on the understanding of the cyber crimes but also explains the different types of security threats and preventions. This will help to the community to secure all the online information critical organizations which are not safe due to such cyber crimes. The understanding of the behavior of cyber criminals and impacts of cyber crimes on society will help to find out the sufficient means to overcome the situation.

REFERENCES

[1] Amit Wadhwa, Neerja Arora, "A Review on Cyber Crime: Major Threats and Solutions", International Journal of Advanced Research in Computer Science (IJARCS) ISSN: 0976-5697, Volume 8, No. 5, May – June 2017

[2]http://www.beverlypd.org/pdf/PERSONAL%20SAFETY/CYBERSTALKING.pdf

[3] Hemraj Saini, Yerra Shankar Rao, T. C. Panda, " Cyber-Crimes and their Impacts: A Review", International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622, Vol. 2, Issue 2, Mar-Apr 2012