ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 4, Special Issue 4, March 2017

Cybercrime and Security

G.Vasanthi.M.sc. M.Phil., B.Ed.
DEPT.OF ISM
Annai Veilankanni College of arts and science for women
Chennai
Vasanthig1279@gmail.com

T.Pavadharini. II BCA
Department of Computer Science
St. Joseph's College of Arts & Science for Women
Hosur
Dharini.riya2gmail.com

***Abstract*—: In the current period of online processing, maximum of the information is online and likely to cyber threats. Cybercrime is a criminal activity done using computers and the Internet. Cybercrime is that activities made by the people for destroying organization network, stealing others valuable data, documents, hacking bank account and transferring money to their own and so on. As the use of computer has grown, computer crime has become more important. It can be broadly defined as criminal activity involving an information technology infrastructure, including illegal access, illegal interception, data interference, system interference, misuse of devices, forgery and electronic fraud .It gives detailed information regarding cybercrime, its types, and modes of cybercrime and security measures including prevention to deal effectively with cybercrime.** (*Abstract*)

Keywords*—: Cyber crime, Security Measures, types of cyber crime, Hacking.

I. Introduction (*Heading 1*)

Crime, in whatever forms it is, directly or indirectly, always affects the society. In today's world, there is immense increase in the use of Internet in every field of the society and due to this increase in usage of Internet, a number of new crimes have evolved. Such crimes where use of computers coupled with the use of Internet is involved are broadly termed as Cyber Crimes.

Cybercrime is defined as a crime in which a computer is the object of the crime (hacking, phishing, spamming) or is used as a tool to commit an offense (child pornography, hate crimes). Cybercriminals may use computer technology to access personal information, business trade secrets.

Cybercrime includes anything from downloading illegal music files to stealing millions of dollars from online bank accounts. Cybercrime also includes non-monetary offences, such as creating and distributing viruses on other computers or posting confidential business information on the Internet.

Cybercrime may also be referred to as computer crime.

2. History :

The first recorded cybercrime took place in 1820. The first virus was installed on an Apple Computer in 1982. When computers and networks came into being in the 1990s, hacking was done basically to get more information about the systems. Hackers even competed against one another to win the tag of the best hacker. As a result, many networks were affected; right from the military to commercial organizations.

3. Categories of Cybercrime:

II. There are two categories of Cybercrime. They are:

III. a) The Computer as a target: Using a Computer to attack other Computer. E.g. Spreading VIRUS, Hacking etc.,

IV. b) The Computer as a weapon: using a computer to commit "traditional crime" that we see in the physical world (such as Credit card fraud, Cyber terrorism, Pornography etc.,).

4. Types of Cybercrime :

A. Hacking

B. Child Pornography

C. Virus dissemination

D. Computer vandalism

E. Denial Service Attacks.

F. Cyber Terrorism

G. Software Piracy.

A. Hacking :

Hackers are people who try to gain unauthorized access to your computer. This is normally done through the use of a 'backdoor' program installed on your machine. You can protect yourself from these by using a firewall and a good up-to-date anti-virus program. You would normally get such a backdoor program by opening an E-mail attachment containing the backdoor program. These programs automatically attach themselves to any e-mail you send, causing you to unintentionally send out malicious programs to your friends and associates.

Hackers can see everything you are doing, and can access any file on your disk. Hackers can write new files, delete files, edit files, and do practically anything to a file that could be done to a file. A hacker could install several programs on to your system without your knowledge. Such programs could also be used to steal personal information such as passwords and credit card information.

b) Child Pornography :

The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. As more homes have access to internet, more children would be using the internet and more are the chances of falling victim to the aggression of pedophiles. The easy access to the pornographic contents readily and freely available over the internet. Pedophiles lure the children by distributing pornographic material, then they try to meet them and take pornographic pictures in order to sell those over the internet.

Sometimes Pedophiles connect children in the chat rooms which are used by children to interact with other children.

c) Virus dissemination :

Virus is capable of self replication on a machine. It may spread between files or disks . Virus can spread themselves, without the knowledge or permission from the users to large number of programs on many machines .

Typical action of virus are : Erase files, Scramble data on a hard disk, Causes erratic screen behaviour, Halt the Computer, Just replicate itself etc., There are estimated 30,000 virus in existence.

D) Computer Vandalism :

Damaging or destroying data rather than stealing or misusing them is called Computer Vandalism. It is a program that perform malicious function such as extracting a user password or other data or erasing the hard disk. The Vandal can be downloaded from the Internet in the form of Java applet, E-mail attachment etc.,

e) Denial Service Attacks :

A Denial of Service, or DoS as it is often abbreviated, is any type of attack where the attackers (hackers) attempt to stop genuine users from accessing the service on a network. This type of attack is essentially designed to bring a network to its knees by flooding it with useless traffic, keeping the network or server busy.

Hackers use DoS attacks to stop genuine users of computer network resources. DoS attacks are characterized as :

The basic types of DoS attack include:

1. Flooding the network to stop genuine network traffic.
2. Disrupting the connections between two machines, thus stoping access to a service
3. Preventing a particular individual from accessing a service.
4. Disrupting a service to a specific system or individual
5. Disrupting the state of information, such resetting of TCP sessions

Some DoS attacks may eat up all your bandwidth or even use up all of a system resource, such as server memory.

f) Cyber Terrorism:

Cyber terrorism is one distinct kind of crime. The growth of Internet has shown that the medium of cyberspace is being used by individuals and groups to threaten the International governments as also to terrorize the citizens in the country. An example of cyber-terrorism could be hacking into a hospital computer system and changing someone's medicine prescription to a lethal dosage as an act of revenge. It sounds farfetched, but these things can and do happen.

$\alpha + \beta = \chi. \quad (1) \quad (1)$

g) Software Piracy:

Illegal copying of genuine programs, counter foiling and distribution of products. The unauthorized copying of software. Most retail programs are licensed for use at just one computer site or for use by only one user at any time. By buying the software, you become a licensed user rather than an owner. You are allowed to make copies of the program for backup purposes, but it is against the law to give copies to friends and colleagues.

Software piracy is all but impossible to stop, although software companies are launching more and more lawsuits against major infractors. Originally, software companies tried to stop software piracy by copy-protecting their software. This strategy failed, however, because it was inconvenient for users and was not 100 percent foolproof. Most software now requires some sort of registration, which may discourage would-be pirates, but doesn't really stop software piracy.

5. Cyber Security :

Cyber security involves protection of sensitive personal and business information through prevention, detection and respond to different online attacks. Cyber security actually preventing the attacks.

Privacy policy:

Before submitting your e-mail address on a website look for the sites privacy policy.

Keep Software up to date :

If the seller gives patches for the Software Operating System, install them as soon as possible. Installing them will prevent attackers form being able to take advantage. Use good password which will be difficult for thieve to guess. Do not choose option to allow your computer to remember your passwords.

Disable remote connectivity :

Some phones are equipped with wireless technologies or Bluetooth that can be used to connect other devices or computers. You should disable these features when they are not in use.

6. Safety tips to cybercrime:

a) Use Anti-virus.

b) Insert firewalls

c) Uninstall unnecessary software.

d) Maintain backup.

e) Check security checking's.

f) Never give your full name and address to strangers.

g) Learn more about internet privacy.

Advantages of cyber security:

1. *Protects system against viruses, worms, spyware and other unwanted programs.*

2. *Protection against data from theft.*

3. *Protects the computer from being hacked.*

4. *The cyber security will secure us from critical attacks.*

5. *Internet Security process all the incoming and outgoing data on your computer.*

6. *Application of cyber security needs to be updated every week.*

Conclusion:

Cybercrime is indeed getting the recognition it deserves. It is not going to restricted that easily. So, to make us safer, we must need cyber security.

References

[I]. www.slideshare.net/aki55/cyber-crime-and-security

[II]. study.com/.../what-is-cyber-crime-definition-types-examples...

[III]. www.authorstream.com/.../anukaa-486518-cyber-crime

[IV]. www.securityweek.com/cybercrime

[V]. Www.antivirusnews.com