Cyber-Crime

Kriti Bhatia

1. ABSTRACT

The crimes are increasing day to day ,everyday there is some type of crime taking place in society whether it is stealing , murder or cyber crime.In this we are going to discuss about cyber crime is the crime that hamper us directly or indirectly. Cyber-crime are creating threat to our society .These threats are leading to mental tensions like depression and various other problem .The government has made an initiative from there side by making cyber laws but there is no such benefit of these laws because people are unaware the laws so the need of an hour is there for public awareness about the cyber laws. The cyber -crimes are of different types like some are there which harm us directly and some which harm us indirectly. The cyber crime that harm us directly are malware and computer virus , Malware is a full malicious software which leads to infect the personal computer and turns it into a zombie computer while computer virus are those which replicates the data in computer system by inserting its own copy.This affects the computer hardware, data files badly make that area infected.The cybercrime that affect us indirectly are cyber-stalking, fraud and identity theft and below we will talk about cyber-crime and types of cyber-crime.

2. KEYWORDS

Cyber-stalking , pornography , identity theft, malware, cyberspace, computer virus,fraud.

3. INTRODUCTION

As new technologies are created the ways of conducting any crime is also increasing .There is a huge differnce between the traditional crime and cybercrime ,but one of the major difference is digital computer .Cybercrime is related to any sort of crime which includes computer and network. In cybercrime the computer is used as a mode of any sort of illegal activities like committing fraud, trafficking in child pornography and intellectual property now days it had become very common though the cyber laws are very strict. From mid-90's the internet is growing up high and it have become a very important part of life of the peoples specially the western industrial world because of this the cybercrime is also increasing people easily believe in what they see without having any concern what can be the side effects of that. The internet plays a huge role in globalization process but with the globalization is coming new challenge to minimize the cybercrime across the world. . Criminals do not require a computer to commit fraud, traffic in child pornography and intellectual property, steal an identity, or violate our privacy. The cybercrime occurs in cyber space. The cyberspace can be defined as the electronic medium of computer networks, in which online communication takes place. In an Australian nationwide survey conducted in 2006 it was found that two in three convicted cyber-criminals were between the age group of 15 and 26. Any kind of{1}.

Mostly the cybercrime is done so that the criminal could get excess to the data of individual, company or government. The cybercrime don't harm us directly on our physical body, but it harms us on the personal or corporate virtual body, which is the set of informational attributes that define people and institutions on the Internet. Cybercrime highlights the centrality of networked computers in our lives, as well as the fragility of such seemingly solid facts as individual identity. Cybercrime is being highlighted mainly by the mass media. Cybercrime threatens the security of the nation and also the financial health. An important aspect of cybercrime is its nonlocal character: actions can occur in jurisdictions separated by vast distances. This poses severe problems for law enforcement since previously local or even national crimes now require international cooperation. In 1996 the council of Europe, along with government representatives of the United States, Canada, as well as Japan, drafted a preliminary international treaty covering computer crime .Around world, civil libertarian groups immediately protested provisions in the treaty requiring Internet service providers (ISPs) to store information on their customers' transactions and to turn this information over . On 23 November 2001, council of Europe since this treaty with 30 states.{1}

3.1 TYPES OF CYBERCRIME:

Cybercrime includes a wide range of crimes. Cybercrime generally are of two types:

1. Crimes that target computers directly.
2. Crimes facilitated by computer networks or devices.
   - **The crimes that targets computer system directly are**:

These are those crimes which target the computer through any kind of software's or hardware they directly harm computer. They interfere in working of computer making it difficult for any individual to work on computer.

- Computer viruses
- Denial-of-service attacks
- Malware (malicious code)

➢ **The crimes that are facilitated by computer network or devices are:**

These are those crimes which are facilitated by internet , the are mainly facilitated through email or any offer that attracts people by giving them prizes and various other advantages.These crimes steal the identities of individual.

- Cyber stalking
- Fraud and identity theft
- Information warfare
- Phishing scams {2}

3.1.1 COMPUTER VIRUS

The computer virus is similar to the biological. The computer virus passes from computer to computer like human virus passes from person to person .The main purpose of computer virus is that it replicates the data in computer system by inserting its own copy.This affects the computer hardware, data files badly make that area infected. Virus performs harmful activities like stealing the space from hardware and CPU time as well. All the viruses are not same ,all the virus don't lead to destruction .The first computer virus was Creeper virus on ARPANET and forerunner on internet in early 1970's.Creeper was a self-experimental program {3}. There are different types of electronic virus but the common ones are:

- Viruses
- E-mail Viruses
- Trojan-horses
- Worms

- **Viruses**: A virus is a small piece of software that piggybacks on real programs. For example, a virus might attach itself to a program such as a spreadsheet program. Each time the spreadsheet program runs, the virus runs, too, and it has the chance to reproduce (by attaching to other programs) or wreak havoc.
- **E-mail viruses**: An e-mail virus travels as an attachment to e-mail messages, and usually replicates itself by automatically mailing itself to dozens of people in the victim's e-mail address book. Some e-mail viruses don't even require a double-click -- they launch when you view the infected message in the preview pane of your e-mail software

- **Trojan horses**: A Trojan horse is simply a computer program. The program claims to do one thing (it may claim to be a game) but instead does damage when you run it (it may erase your hard disk). Trojan horses have no way to replicate automatically.
- **Worms**: A worm is a small piece of software that uses computer networks and security holes to replicate itself. A copy of the worm scans the network for another machine that has a specific security hole. It copy itself to the new machine using the security hole, and then starts replicating from there, as well.

PREVENTIONS

- Never open the unwanted attachments in mail.
- Never open unsolicited executable files**.**
- Avoid downloading from internet it often spread virus{3}

3.1.2 MALWARE

Malware in a full malicious software which leads to infect the personal computer and turns it into a zombie computer. Malware' is a general term used to refer to a variety of forms of hostile or intrusive software.Malware is also known as computer contaminant .The malware consist of different type defective software which consist of harmful bugs which were not corrected before release.{4}

PREVENTIONS

- Download the anti-malware in your pc is best prevention from malware.
- Turn on your firewall
- Limit user privileges
- Understand how to malware works
- Get latest software updates
- Run to update data security software {5}

3.1.3 CYBERSTALKING

Cyber-stalking is harassing an individual by using internet or electronic means of communication. It includes false statement , assault statement, monitoring, making threats. Cyber-stalking is totally different from offline stalking but both type of stalking is equally offensive. Cyber-stalking is more harmful for individual as compared to offline stalking. Due to cyber-stalking threat is created of identity theft. The cyber-stalker can be a stranger or a known may be your enemy or friend.{6}

PREVENTIONS

- Do not share personal information in public spaces anywhere online, nor give it to strangers, including in e-mail or chat rooms.
  □Be extremely cautious about meeting online acquaintances in person.
- Make sure that your ISP and Internet Relay Chat (IRC) network have an acceptable use policy that prohibits cyberstalking.
  □If a situation online becomes hostile, log off or surf elsewhere.
- If you are receiving unwanted contact, make clear to that person that you would like him or her not to contact you again.

- Save all communications for evidence. .
- You may want to consider blocking or filtering messages from the harasser..

- If harassment continues after you have asked the person to stop, contact the harasser's Internet Service Provider (ISP).
- Contact your local police department and inform them of the situation in as much detail as possible.

3.1.4 IDENTITY THEFT

Identity theft is a form of stealing someone's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. The victim of identity theft (here meaning the person whose identity has been assumed by the identity thief) can suffer adverse consequences if they are held accountable for the perpetrator's actions. Identity theft occurs when someone uses another's personally identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes.

PREVENTIONS

- Don't carry your Social Security card .
- Protect your PIN..
- Watch out for "shoulder surfers"..
- Collect mail promptly.
- Pay attention to your billing cycles..
- Keep your receipts.
- Tear up or shred
- Store personal information in a safe place .
- Don't respond to unsolicited requests .
- Install firewalls .
- Check your credit report

3.1.5 INTERNET FRAUD

The use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them, for example by stealing personal information, which can even lead to identity theft. A very common form of Internet fraud is the distribution of rogue security software. Internet services can be used to present fraudulent solicitations to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme.

Internet fraud can occur in chat rooms, email, message boards, or on websites.

PREVENTIONS

1. Protect your passwords and change them regularly.
2. Install anti-virus, anti-spyware and Internet firewall tools purchased from trusted retailers or suppliers.
3. Be wary of downloading free files, programs, software or screensavers and avoid unsolicited or provocative messages (e-mail, Internet pop-ups or phone messages).
4. Never send personal and/or financial information by e-mail.
5. Ensure that you are in a secure environment when doing financial transactions online.
6. Protect your Internet connection
7. Verify your Internet connection
8. Clear your cache when you visit websites, the website addresses are stored in the cache, or memory, of your computer. Make sure you clear the cache of your browser after visiting secure sites so that nobody else can view any confidential information you may have transmitted.
9. Be cautious when using free wireless Internet connections in public places. While many are legitimate free WiFi networks made available by airports, resorts and coffee shops, some may be set up by criminals and using them could allow the fraudsters to access your personal information. Always check with the staff first to make sure you are connecting to their wireless network.
10. Check your financial and credit card statements regularly

4. "FUTURE SCOPE"

With the time technology is also advancing and along with the advancing technology comes the threat of cybercrime .The growing cloud computing and virtualization is creating a huge threat in increasing the cybercrime in world. The cloud computing and virtualization -while offering significant benefits and cost-savings - move servers outside the traditional security perimeter and expand the playing field for cybercriminals .The industry has already faced a cloud sever failure which clearly explains that computing risks that cybercriminals will likely abuse in the future.

IPv6

IPv6 is Internet Protocol version 6,as we know that internet infrastructure is changing the opportunity for cybercrime is also increasing.The next generation internet protocol is in an experimental stage of replacing current IPv4. As the users will use IPv6 the cybercriminal will aslo do so ,which make them familiar with the IPv6 and hence they will what they want to as a cybercriminal. Possible avenues for abuse include new covert channels or C&C. The company does not expect active targeting of the IPv6 address space in the near future.

Domain Name

Domain has become internationalized because of this the cybercrime is taking place.

Social Media and Networks

Social media and social networks will be used by cybercriminals to enter the users' 'circle of trust.' Given the increasing saturation of social media with content intended to be shared via online social interactions, cybercriminals will try to penetrate.

5. CONCLUSION

The conclusion of above information is that as the technology is advancing the modes of cybercrime are also increasing and ways are becoming more advanced as compared to technology. The different types of cyber-crime have different types of consequences. A suggestion from my side would be that as the technology is advancing we should advance more and more in security. As the security is very important aspect of decreasing the cyber-crime from society. The security should be increased so that the threat of life directly or indirectly can be decreased. We should take care that we are taking preventive measures from our side itself. We should never click on anonymous links they may create problem for us only.

6. REFFERENCES

{1} cybercrime and Society - Majid Yar published in 2006

{2} cybercrime Encyclopedia

{3} cybercrime Wikipedia

{4} Malware Wikipedia

{5} Microsoft malware preventions http://www.microsoft.com/security/portal/mmpc/shared/prevention.aspx

{6} Cyber-stalking Wikipedia

http://en.wikipedia.org/wiki/Cyber_stalking

Author-Kriti Bhatia currently pursuing bachelor of technology from Dronacharya College Of Engineering ,kritibhatia02@gmail.com