Cyber Crime against Person

Desai Purva N.
Department of Computer Science, Veer Narmad South Gujarat University
Vivekanand College for Advance Computer & Information Science, Surat, Gujarat, India

Patel Asma M.
Department of Computer Science, Veer Narmad South Gujarat University
Vivekanand College for Advance Computer & Information Science, Surat, Gujarat, India

Abstract- Cyber crimes committed against persons include various crimes like transmission of child-pornography, harassment of any one with the use of a computer such as e-mail. The trafficking, distribution, posting, and dissemination of obscene material including pornography and indecent exposure, constitutes one of the most important Cyber crimes known today.

Keywords – Pornography, cyber smearing, cyber stalking, E-mail bombing, phishing, IRC attacks

I. INTRODUCTION

Cyber crime is "*unlawful acts wherein the computer is either a tool or target or both"*. The computer may be used as a tool in the following kinds of activity- financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases- unauthorized access to computer/ computer system/ computer networks, theft of information contained in the electronic form, e-mail bombing, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system. Cyber harassment is a distinct Cyber crime. Various kinds of harassment can and do occur in cyberspace, or through the use of cyberspace. Harassment can be sexual, racial, religious, or other. Cyber harassment as a crime also brings us to another related area of violation of privacy of citizens.

II. DIFFERENT WAPONS USED AGAINST PERSON ON CYBER SPACE

Following are the techniques used by person for harassment:

- **E-mail Spamming**

Email spam, also known as **junk email** or **unsolicited bulk email** (**UBE**). Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. In addition to wasting people's time with unwanted e-mail, spam also eats up a lot of network bandwidth.

- **E-mail Bombing**

E-mail bombing occurs through sending threatening E-mails:

- For example: Mr. X received an e-mail message from someone who called him "your friend". The attachment with the e-mail contained morphed pornographic photographs of Mr. X. The mail message said that if Mr. X were not to pay Rs. 20,000 at a specified place every month, the photographs would be uploaded to the Internet and then a copy sent to his family.

➢ **IRC related crimes:**

Three main ways to attack IRC are: verbal attacks, clone attacks and flood attacks.

a) **Verbal attack:**

Verbal attacks are people going on IRC and verbally abusing people on server.

b) **Clone attack:**

Clone attacks are where hundreds of people connect via socks proxy or Trojan Virus to the same IRC server often overloading there server or causing client with slower computers to lock up.

c) **Flood attack:**

With flood attacks, the attacker sends many random characters to the server also causing users with slower computer to lock up. Worst attacks occur when the attacker combines two or more of these attacks together.

➢ **Phishing:**

Some spoof messages purport to be from an existing company, perhaps one with which the intended victim already has a business relationship. The 'bait' (attract) in this instance may appear to be a message from 'the fraud department' of, for example, the victim's bank, which asks the customer to: "confirm their information"; "log in to their account"; "create a new password", or similar requests. If the 'fish' takes the 'bait', they are 'hooked' -- their account information is now in the hands of the con man, to do with as they wish.

"Phishing" scams are currently the most popular and thus dangerous form of email fraud. They use email messages that appear to come from a legitimate company or institution, such as your bank or university, and ask you to "update" or "verify" your personal information; the scammers then use this information to commit identity theft. And it’s also caused for account take over.

Case 1: Bogus offers

Email solicitations to purchase goods or services may be instances of attempted fraud. The fraudulent offer typically features a popular item or service, at a drastically reduced price.

Items may be offered in advance of their actual availability, for instance, the latest video game may be offered prior to its release, but at a similar price to a normal sale. In this case, the "greed factor" is the desire to get something that nobody else has, and before everyone else can get it, rather than a reduction in price. Of course, the item is never delivered, as it was not a legitimate offer in the first place.

Case 2: Request for Help

The "request for help" type of email fraud takes this form. An email is sent requesting help in some way, but including a reward for this help as a "hook," such as a large amount of money, a treasure, or some artifact of supposedly great value.

Case 3: Investments Frauds

Sales and Investment frauds, False or fraudulent advertisements, claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online remains undelivered. In this the Investors are enticed to invest in this fraudulent scheme by the promises of seemingly high profits. Buying and selling online is normally safe and reliable but occasionally people fall victim to fraudsters.

➢ **Cyber Pornography:**

Cyber pornography refers to stimulating sexual or other erotic activity over the internet. It has been traded over the internet since 1980's, it was the invention of the world wide web in 1991 as well as the opening of the Internet to the general public around the same time that led to an explosion in online pornography. There are both commercial and free pornographic sites. These sites offering photos, video clips and streaming media including live web cam access allowed greater access of pornography.

➢ **CYBER SMEARING (DEFAMATION):**

The Criminal sends emails containing defamatory (insulting) matters to all concerned of the victim or post the defamatory matters on a social networking website. (Disgruntled employee may do this against boss, ex-boys friend against girl, divorced husband against wife etc). Libelous messages placed on the Internet, regardless of whether the message or statement appears on a website, on a computer bulletin board or chat room, in an on-line newspaper, diary or weblog ("blog") or in an e-mail. Also referred to as cyber libel.

➢ **Cyber stalking:**

Cyber stalking is the use of the Internet or other electronic means to stalk someone which may be a computer crime or harassment. This term is used interchangeably with online harassment and online abuse. A cyber stalker does not present a direct physical threat to a victim, but follows the victim's online activity to gather information and make threats or other forms of verbal intimidation. The anonymity of online interaction reduces the chance of identification and makes cyber stalking more common than physical stalking. Although cyber stalking might seem relatively harmless, it can cause victims psychological and emotional harm, and it may occasionally lead to actual stalking. Cyber stalkers target and harass their victims via websites, chat rooms, discussion forums, open publishing websites (e.g. blogs and Indy media) and email.

HOW TO FILE A COMPLAINT

The complaint regarding commission of cyber crime can be made to the in-charge of the cyber crime cells which are present almost in every city. To file a complaint alleging commission of a cyber crime the following documents must be provided:

1.In case of hacking the following information should be provided:

a. Server Logs
b. Copy of defaced web page in soft copy as well as hard copy format, if your website is defaced
c. If data is compromised on your server or computer or any other network equipment, soft copy of original data and soft copy of compromised data.
d. Access control mechanism details i.e.- who had what kind of the access to the compromised system
e. List of suspects – if the victim is having any suspicion on anyone.
f. All relevant information leading to the answers to following questions –
    - What? (what is compromised)
    - Who? (who might have compromised system)
    - When?(when the system was compromised)
    - Why?(why the system might have been compromised)
    - Where?(where is the impact of attack-identifying the target system from the network)
    - How many?(How many systems have been compromised by the attack)

2. In case of e-mail abuse, vulgar e-mail etc. the following information should be provided:

a. Extract the extended headers of offending e-mail and bring soft copy as well hard copy of offending e-mail.
b. Please do not delete the offending e-mail from your e-mail box.
c. Please save the copy of offending e-mail on your computer's hard drive.

IV.CONCLUSION

This paper gives a brief description what type of crimes a person can face in E-World. This helps a new use to be aware of the current scenario, which can make alert when he/she uses the E-sites. Any unauthorized website or mails can misuse the user's personal details. In such situation how can he/she claim for justice?

REFERENCES

[1] http://library.thinkquest.org/06aug/02257/more.html

[2] http://satheeshgnair.blogspot.in/

[3] http://poleposition.uk.com/tips/instantmessagingchatrooms.html

[4] http://my.safaribooksonline.com/book/-/9781597495455/chapter-3dot-phishing-attacks/phishing_attack_scenarios_agai#X2ludGVybmFsX0J2ZGVwRmxhc2hSZWFkZXI/eG1saWQ9OTc4MTU5NzQ5NTQ1NS80Ng==

[5] E-Commerce and cyber crime By: Chetan Rathod & Purva Desai (under process)