ISSN No. 0976-5697

Volume 6, No. 4, June 2015 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Scenario of Cyber Crime in india - Threat to Persons, Property and Government

Dr. Neeraj Bhargava
Associate Professor,
Dept. of Computer
Science, School of
Engineering & System
Sciences,
MDS University, Ajmer, India
drneerajbhargava@yahoo.co.in

Anchal Kumawat
Research Scholar
Dept. of Computer
Science, School of
Engineering & System
Sciences,
MDS University,Ajmer, India.
Anchal.kumawat@gmail.com

Abstract: Now a days, India has witnessed of Cyber crimes like Trojan attacks, e-mail bombing, DOS attacks, hacking or the most common offence of information theft. Internet users are increasing day by day so it is easy to access information within seconds. This paper deals with various categories of cyber crime with their variants i.e. a threat which is based on person, property, government and society and also mentions preventions tips to protect any person from cyber crime.

Keywords: Cyber crime, stalking, spoofing, vandalism, terrorism, Computer crime, hacking

I. INTRODUCTION

In Today's world, large amounts of information can be easily found through the internet so the lots of crimes happen through the computer. Live serials we can see in Television like crime in India, savdhan India and cid and so on. Now a days, India has witnessed of Cyber crimes like Trojan attacks, e-mail bombing, DOS attacks, hacking or the most common offence of information theft. The frequency of cyber crime is increasing day by day over the last decade. Cyber crime is simply known as the act of performing a criminal activity using computer or the Internet network. Crime can be committed on the internet by either two ways as a tool or a targeted. All types of cyber crimes involve computer and network behind its victims.

Now a day's everything users can find on internet, we can read our books, listen music, download movies, create account on social sites, news about sports, national, international, collaborate with our friends family everyone, submit our payments through net banking, fill an online application forms for an exam, playing games, book a train, plain, bus tickets or any transport vector and so on. Each and every work a user depends on internet till data entry to data submit. Due to this we can say that each coin has a two sides mean to say has both pros and cons also. Pros are less but cons are more because the crimes done by a computer or a network like cyber stalking, spoofing, squatting, vandalism, cyber terrorism, transmitting viruses etc.

Criminals use the internet to filch the personal information from the other user's .this kind of identity theft plays an important role in cyber crime and to find the identity of interesting peoples can be easily provided by the social networking sites. Phishing and harming are the two important methods that attracts the people and ask their personal information like log in information such as user name password , your identity name ,debit card and credit card numbers or having any smart card , phone numbers ,address, bank account number or any other information that can steal easily.

It's an unlawful act where the computer can be treated as either a tool or a target or may be both [1][2][3].

II. HISTORY

Cyber crime is firstly recorded in 1820. During 1820, Joseph-Marie who is a textile manufacturer in France developed the loom. Loom is a device which provides the facility to repeat a series of steps in weaving.

III. WAYS OF CYBER CRIME

Cyber crimes can happen on 3 major ways:

A. Crime against the Persons
B. Crime against the individual Property
C. Crime against the Government

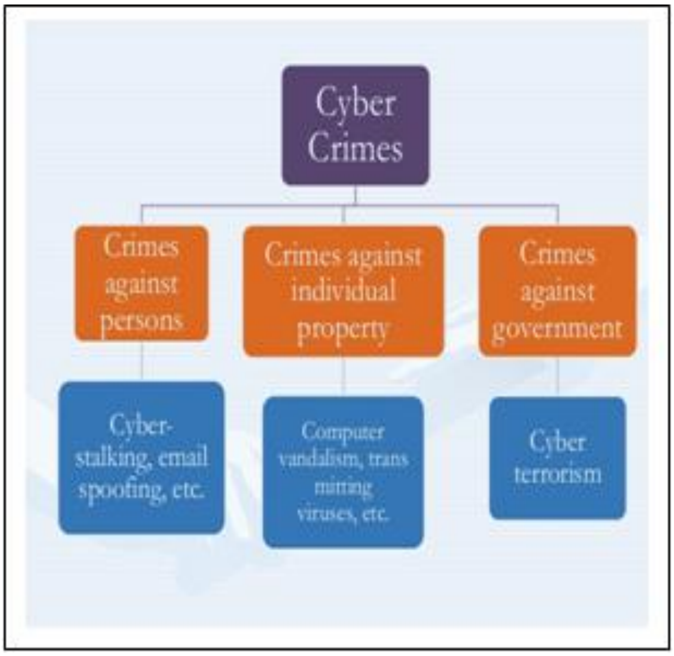
Cyber Crimes
Crimes against persons
Crimes against individual property
Crimes against government
Cyber-stalking, email spoofing, etc.
Computer vandalism, trans mitting viruses, etc.
Cyber terrorism

Figure 1. Ways of Cyber crime

Cyber Crime against person

It is the first category of Cyber crime. Transmission of child-pornography (includes trafficking and dissemination of obscene material, posting and distribution), harassment of a person can easily be done using a computer like e-mail, and fake escrow scams that refers a written agreement (or property or money) delivered to a third party are all referred as a cyber crime that committed against the persons. The most important today’s cyber crime is indecent exposure, constitutes and harassment. The expected harm of a crime to the humanity can be very difficult to explain. Cyber stalking, email spoofing are the crimes done against by person described in variants of cyber crime stanza.

Cyber Crime against individual Property

It is the second category of Cyber-crimes where the crimes recorded against individual form of property. Computer vandalism means destruction (destroy) of others' property and deliver the noxious viruses or programs to the others computer by the computer through internet. These all are considered as variants of cyber crime.

Cyber crime against government

It is the third category of Cyber-crimes that relates to against Government. Cyber terrorism is one the main example that included in this category. The Cyberspace medium is being used by the groups to threaten or individuals to the international governments as also to endanger the citizens of a country is shown by the today’s growth.

IV. VARIANTS OF CYBER CRIME

Cyber stalking

Cyber stalking is a crime where the attacker harasses a victim through an electronic communication, such as an instant messaging (IM) or e-mail or messages that can be easily posted to a Web site or any other un authentic group.

Figure 2. Example of cyber stalking

To prevent from cyber stalking the following diagram issues like do not use our name as secure name, discover ISP in case of legal action, do not put personal information online or in any social sites and while on conversation meeting beware of that etc are shown in below figure 3.

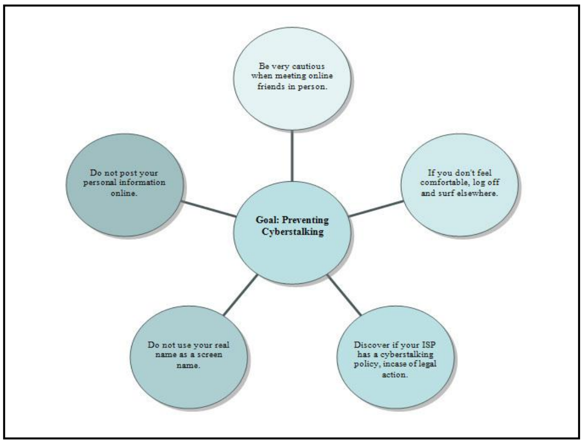
Be very cautious when meeting online friends in person.
Do not post your personal information online.
If you don't feel comfortable, log off and surf elsewhere.
Goal: Preventing Cyberstalking
Do not use your real name as a screen name.
Discover if your ISP has a cyberstalking policy, incase of legal action.

Figure 3. Prevention from cyber stalking

Email Spoofing

E-mail spoofing means a composition that imitates somebody’s style in a humorous way and also referred as the forgery of header of an e-mail so that the message seems to like that it arrives from the actual source but it doesn’t happened. Real life example user can see that in our today’s life everyone use a mail accounts such as Gmail, yahoo, rediff and so on then mail cab be transferred using SMTP protocol. Simple Mail Transfer Protocol (SMTP) is a protocol used for transferring a mail without using any authentication scheme. That’s why an email can be spoofed easily.

E-mail spoofing made possible through Simple Mail Transfer Protocol (SMTP). IETF RFC standard 2554 is a service extension of SMTP allows client to refuse a security level with the help of a mail server and this precaution is not certain taken. Then there will be the two conditions one is precaution is not taken then any person that can connect to the server with the knowledge and used to send spoofed messages. The method of sending a spoofed e-mail is that the senders insert some commands in headers that will change message information. It is also possible that message can be send by the anyone from anywhere whatever the sender wants it to say but it should be connected through the internet. Due to this, any person can send a spoofed e-mail that seems like sending by the main user but that message is another one that is not written by an authentic user[4][5][6].

Figure 4. example of cyber email spoofing

To prevent from cyber email spoofing the following diagram should be considered shown in below figure5.

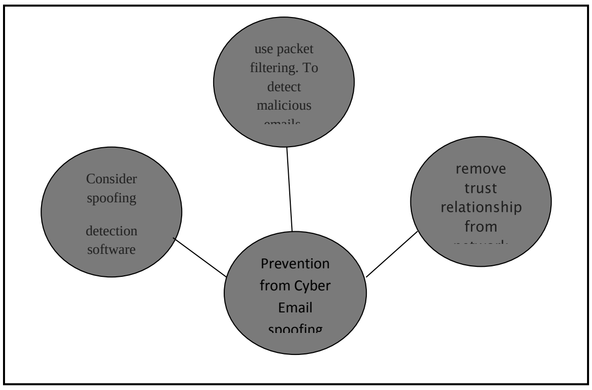
use packet filtering. To detect malicious emails
Consider spoofing detection software
remove trust relationship from network
Prevention from Cyber Email spoofing

Figure 5. Prevention from cyber Email spoofing

Computer Vandalism

Vandalism means malicious destruction of property of others. Cyber vandalism is simply referred as to destroy the data or information which is stored in the computer when the services of the network are stopped. It may also include any kind of physical harm that done through computer by any person.

Figure 6. Example of Cyber vandalism

Cyber terrorism

Cyber terrorism Indian parliament attack happens in New Delhi on 13 Dec 2001 and the recent attack fall in Mumbai comes under this category.

Figure 7. Examples of Cyber terrorism

V. PREVENTION OF CYBER CRIME

It is to be said that Prevention is better than cure. While working on the net it is better to take certain precautions. Some of the preventions of cyber crime is shown below.

- Do not enable and a specific user account should be log off to prevent access.
- Do not enable a group of user accounts. It should be log off to prevent access from attack a particular service.
- Entire system should be shut down and divert backup service on a secondary network.
- firms to meet identification of exposures.
- Avoid to disclose any personal information to an unauthentic person, the person whom they don't know avoid to share personal information.
- Avoid disclosing photographs to a stranger, the person whom they don't know avoid to send the photograph.
- Update antivirus software to prevent from viruses.
- Back up your data store in a safe place and avoiding to store in social sites.
- Avoid to send the credit card or debit card number on that site which is not secure.
- The owner of web site should check any irregularity on the site.
- IT department pass guidelines, license, authentication rules and notifications to prevent computer system.
- Some steps should be taken at the national or international level for preventing the cybercrime.
- Use a security programs to control information on sites.
- Do not enable and Dismount network devices.
- Do not enable specific applications like an e-mail system that consist a SPAM attack[7][8].

VI. CONCLUSION

This paper conclude with the conclusion i.e. within the scenario of Cyber crime, certain prevention rules must be developed to prevent from various categories of computer crime such as every person will know information about those what and why to search for the electronic proof to recover, to maintain computer crimes does have a major effect on the world where we live. This paper describe the term of cyber crime with its categories and several variants which happened through the cyber crime as well as prevention tips.

It affects each and every person who uses the internet no matter where they are from. At the end of this paper, conclude that all users that works on computer system where an internet are increasing day by day in a huge number of worldwide, where it is so easy to access any information within a few seconds. Some Precautions should be taken by all the users while surfing on the internet which will assist the user to challenging this major threat Cyber Crime that affects the person, property and government.

VII. REFERENCES

[1] Communications Fraud Control Association. 2011 global fraud loss survey. Available: http://www.cfca.org/fraudlosssurvey/, 2011.

[2] F. Lorrie, editor. “Proceedings of the Anti-Phishing Working Groups”, 2nd Annual eCrime Researchers Summit 2007, Pittsburgh, Pennsylvania, USA, October 4–5, 2007, vol. 269 of ACM International Conference Proceeding Series. ACM, 2007.

[3] I. Henry, “Machine learning to classify fraudulent websites”. 3rd Year Project Report, Computer Laboratory, University of Cambridge, 2012.

[4] Microsoft Inc. Microsoft security intelligence report, volume 9, 2010. Available: http://www.microsoft.com/security/sir/.

[5] Neilson Ratings. (2011). Top ten global web parent companies, home and work. Retrieved February 24, 2012.

[6] N. Leontiadis, T. Moore, and N. Christin. “Measuring and analyzing search-redirection attacks in the illicit online prescription drug trade”. In Proceedings of USENIX Security 2011, San Francisco, CA, August 2011.

[7] Phil Williams, Organized Crime and Cybercrime: Synergies, Trends, and Responses, Retrieved December 5, 2006 from Available: http:// www.pitt.edu/~rcss/toc.html.

[8] Steel.C. (2006), Windows Forensics: The Field Guide for Corporate Computer Investigations, Wiley.