Volume 5, Issue 8, August 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

General Awareness on Cyber Crime

Gifty Aggarwal
M.Tech Student, Department of Computer Science& Engineering, CEC, Landran, Mohali,
Punjab Technical University, Punjab, India

Abstract- Cyber crime is the crime that is done using computer and internet. Cyber crime is the fast growing area of crime. Both the computer and the person can be the victim of cyber crime. Criminals are taking advantage of the fast internet speed and convenience provided by the internet to perform large and different criminal activities. Cyber crime can be categorized as the crime against individual, property or the government. Cyber crime can be any crime related to information theft, hacking, virus, Trojan attack, stealing money while transactions etc. As the internet users have increased considerably, so does the cyber crime. So, it's the duty of one and all that uses internet to be aware of the cyber crime and the cyber law made to deal with cyber crimes. In this paper, I have discussed the types of cyber crime, which can help people to identify the crime that they have been victim of. In this paper, I have discussed the cyber law, its awareness program and Information Act 2000 that was made to deal with cyber crimes.

Keywords- Cyber Crime, Stalking, Spoofing, Cyber Law, Transaction, IT Act 2000

I. INTRODUCTION

Any crime that is done using computer and internet is known as cyber crime or computer crime. Dr. Debarati Halder and Dr. K Jaishankar defines cyber crimes as "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". Both the computer and the person can be the victim of cyber crime. It just depends on who is the main target. Cyber crime is done by the persons who are expert in computers and know the technique of hacking. Cyber crime does not only mean to steal money from someone's account using online transactions, but it can also be information theft, Trojan attacks, e-mail bombing, DOS attack, hacking someone's system, downloading illegal files. Virus is a small program that is sent to different computers using internet which may harm the other systems is also a cyber crime. The growing problem of cyber crime is an important issue. The number of internet users has grown tremendously and so does cyber crimes. The purpose of this paper is to make awareness regarding cyber crime and cyber law made to avoid the misuse of internet.

II. CATEGORIES OF CYBER CRIME

Cyber crime can be categorized as, the crime against-

A. Individual

The cyber crimes which are done to harm a particular individual come under this category. The crime against individual can be such as cyber stalking, trafficking, grooming and distributing pornography. These crimes are very serious and the government is taking steps to protect the victims and arrest the criminals.

B. Property

The cyber crime which is done to harm the property of an individual or of an organization come under this category. This type of crime involves stealing and robbing i.e. criminals can steal person's bank details and transfer money to his account; criminals can misuse the credit card details of the person to purchase online; criminals can use special software to steal organization's confidential data; malicious software can also damage the hardware and software of the organization.

C. Government

Crimes against government are known as cyber terrorism. Cyber attacks against government are not as common as other 2 categories. Criminals attack government websites, military websites which create chaos among civilians.

III. TYPES OF CYBER CRIME

Cyber crimes can be of the following types-

A. ***Hacking***- In this type of crime person's computer is accessed by criminals without the knowledge of person from remote locations. Hacking is done to access the personal, confidential or sensitive information from person's computer. Hacking can also be done to change the passwords of login accounts either of social networking sites or any other business transaction site and use the information against them.

B. Theft- When a person violates or breaks the copyrights of a particular website and download songs, games, movies and software is known as theft. There are many websites which allow downloading the data that is copied from other websites. It is known as pirated data as the quality of data is not up to the mark.

C. Identity theft- In this type of crime, criminals steal data about person's bank account number, credit card number, debit card and other confidential data to transfer money to his account or buy things online by acting as the original person i.e. the criminal stalks the identity of person and thus it is known as identity theft. This theft can result in huge economical loss to the victim.

D. Defamation- In this attack, the criminal hacks the email account of a person and send mails using abusive languages to known persons' mail accounts so as to lower the dignity or fame of the person.

E. Malicious software- These are the programs or software that are used to access the system to steal confidential data of the organization or this software can be used to damage the hardware and software of the system.

F. Cyber Stalking- This is the type of attack where online messages and e-mails are bombarded on victim's system. In cyber staking, internet is used to harass an individual, group or organization by using defamation, identity theft, solicitation for sex, false accusations etc.

G. E-mail harassment- In this type of attack, the victim is harassed by receiving letters, attachments in files and folders of e-mails.

H. Spoofing- Spoofing attack is a situation in which criminal masquerade as another person i.e. the criminal acts as another person by using his identity and therefore takes advantage of illegally accessing data of the other person.

I. Fraud- Fraud is done by transferring money from victim's bank accounts either by using their bank account numbers or credit cards.

J. Virus- Virus is a small program that is loaded on the victim's computer without his knowledge which causes a large amount of damage to the system. Viruses attach themselves to files and circulate themselves to other files on the network which leads to damage of the system.

K. Trojan horse- Trojan horse is a harmful code which is present inside data such that it convinces the victim to install his code as it is useful which after being installed causes damage to the system.

L. Phishing- Phishing is an attack in which criminal sends genuine looking emails to victim to gather personal and financial information of the victim which can then be used against him.

M. Grooming- Grooming is the process of influencing the children and youth emotionally for sexual exploitation. In this process, an adult wins the trust of victim by giving flattery offers and then attempts to sexualize the relation between them which leads to pornography or sex trafficking.

IV. CYBER LAW

The crime that is done using internet i.e. cyber crime has been taking place tremendously. Internet is the place where large number of criminal activities can take place and people that have intelligence can misuse the internet which leads to lasting of criminal activities in cyber space. So, to control the criminal activities in cyberspace, cyber law was made. Cyber law is made to help the people if any cyber crime has happened with them. At some places, there is special team of intelligent officers that work to arrest the criminals.

Cyber law deals with all the online transactions, activities going on the internet and cyberspace. Every action in cyberspace has cyber legal perspective. There are various cyber laws issues associated at every point of time. From the time of registering domain name for website to the time to promote your website to the time when you send and receive mails to the time of online transactions, at every point of time these cyber law issues are involved. Everyone must understand the cyber law for their own benefit.

V. CYBER LAW AWARENESS PROGRAM

All the persons who use internet today must be aware of the criminal activities taking place on the cyber space. Online transactions have made a large impact on the internet as it has totally changed the old and conventional methods of doing business. The identity of the customer with which you are dealing must be verified to prevent identity theft. Data and information must be protected on your website to protect it from illegal and unauthorized access. For strong relationship between the owner and the customer, the legal issues of online transactions must be addressed from the beginning. Clear information must be provided for doing online transaction.

A person should know have the following knowledge to be aware about the cyber crimes-

1. The basics of internet security.
2. The basic information of cyber law.
3. Impact of technology on crime.
4. Minimum hardware and software required to protect data from theft.
5. Internet policies required for working of organization.

VI. IT ACT 2000

Cyber laws provide ways to deal with cyber crime. IT (Information Technology) Act 2000 was made to deal with cyber crimes. This law was made to help people make transactions over the net using credit cards without any fear of misuse. With the arrival of this Act, everything seems to be digitized. The Act gives the power to government departments to create and retain the official documents in digital format. The digitized records can be authenticated by using digital signatures. If the digital signature is valid, then the message is believed to be received from a known sender.

Some key points of the IT Act 2000 are as follows-

1. E-mail is now considered as a valid and legal form of communication.
2. Digital signatures have been given legal validity in the Act.
3. Act has given birth to new business to companies to issue digital certificates by becoming the Certifying Authorities.
4. The Act allows the government to issue notices on internet through e-governance.
5. The communication between the companies or between the company and the government can be done through internet.
6. The most important feature of the Act is that it addresses the issue of security. It introduced the concept of digital signatures which verifies the identity of a person on internet.
7. In case of any damage or loss done to the company by criminals, the Act provides a remedy in the form of money to the company.

VII. CONCLUSION

With the increase in the users of internet, the increase in cyber crimes can also be seen. Hacking is the method in which the criminals get access to the victim's system without their knowledge. Cyber crime can be done mainly by using the technique of hacking. All the persons who use internet and especially those make money transactions through internet must be beware of the cyber criminals. It is the need of today's world to have knowledge about the crimes that are associated with the internet. It is the duty of each one of us to be aware of the basic internet security like changing the passwords regularly, keeping long passwords, avoids disclosing personal information to strangers on the internet or entering credit card details on unsecured websites to avoid any fraud, etc. Government is also making efforts to have a control on these cyber crimes. Government has made cyber laws to help people learn about the cyber crimes and cyber security. IT Act 2000 is made to deal with the cyber crimes. Both the government and people should work hand in hand to catch the criminals. People who have been the victim of cyber crime should come forward and file a complaint against the crime in special anti cyber crime cells. Government should also employee officers with very high intelligent quotient and the knowledge about all the cyber crimes. This will help to catch the criminals very easily and all the criminals must be given hard punishments which can a lesson for millions of other cyber criminals. Awareness of the persons using internet will definitely help to curb the cyber crimes and once, all the people are aware of the cyber crime, no criminal would ever think to commit the cyber crime.

REFERENCES

[1] Information regarding cyber laws, IT Act 2000 from http://www.cyberlawsindia.net/cyber-india.html
[2] Halder, D., & Jaishankar, K. (2011) Cyber crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9
[3] Network security threats available from http://www.slideshare.net/Colin058/network-security-threats-and-solutions-1018888
[4] Grooming attacks of children available from http://www.peacepalacelibrary.nl/2013/10/protecting-children-from-cybercrime-online-child-grooming/
[5] An introduction to cyber crime from http://www.crossdomainsolutions.com/cyber-crime/
[6] Er. Harpreet Singh, Cyber crime- a threat to persons, property, government and societies,IJARCSSE,997-1002, volume 3, issue 5 May2013, **ISSN: 2277 128X**
[7] Phil Williams, Organized Crime and Cybercrime: Synergies, Trends, and Responses, Retrieved December 5, 2006 from Available: http:// www.pitt.edu/~rcss/toc.html

