SHIV SHAKTI
International Journal in Multidisciplinary and Academic Research (SSIJMAR)
Vol. 2, No. 2, March-April (ISSN 2278 – 5973)

CYBER – CRIME AWARENESS

RITU DHANOA*

ABSTRACT: ***Cyber crime*** *is emerging as a very serious threat in today's world. The internet brings joy to our lives but at the same time it has some negative sides too. The cyber criminals are always in a search to find out the new ways to attack the possible internet victims. Today, everybody is using the computers i.e. from white collar employees to terrorists and from teenagers to adults. All the conventional crimes like forgery, extortion, kidnapping etc. are being done with the help of computers. New generation is growing up with computers and most important is that all the monetary transactions are moving on to the internet. So, it has become very important for us to be aware of the various cybercrimes being committed with the help of computers. The paper is an attempt to provide a glimpse of various types of cybercrimes prevalent in modern technological society and what steps can be taken to protect ourselves from these cybercrimes.*

Crime is a social and economic phenomenon and is as old as the human society. It is a legal concept and has the sanction of the law. A crime may be said to be a any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by the penal consequences. So crime or offence is "a legal wrong that can be followed by criminal proceedings which may result into punishment".

*ASTT. PROFESSOR,GURU GOBIND SINGH COLLEGE FOR WOMEN, SECTOR – 26, CHANDIGARH,MOBILE NO. – 9872431166
e- mail - dhanoaritu@gmail.com

ABSTRACT: ***Cyber crime*** *is emerging as a very serious threat in today's world. The internet brings joy to our lives but at the same time it has some negative sides too. The cyber criminals are always in a search to find out the new ways to attack the possible internet victims. Today, everybody is using the computers i.e. from white collar employees to terrorists and from teenagers to adults. All the conventional crimes like forgery, extortion, kidnapping etc. are being done with the help of computers. New generation is growing up with computers and most important is that all the monetary transactions are moving on to the internet. So, it has become very important for us to be aware of the various cybercrimes being committed with the help of computers. The paper is an attempt to provide a glimpse of various types of cybercrimes prevalent in modern technological society and what steps can be taken to protect ourselves from these cybercrimes.*

Crime is a social and economic phenomenon and is as old as the human society. It is a legal concept and has the sanction of the law. A crime may be said to be a any conduct accompanied by act or omission prohibited by law and consequential breach of which is visited by the penal consequences. So crime or offence is "a legal wrong that can be followed by criminal proceedings which may result into punishment".

CYBER-CRIME:

The internet, as we know, has grown rapidly over the last decade. It has given rise to many avenues in every field we can think of – be it education, entertainment, business, or sports. However with every boon there is a curse too. This curse is *Cybercrime* – illegal activities committed over the internet. The internet, along with its advantages, has also exposed us to security risks. Computers today are being misused for unlawful activities like e-mail espionage, credit card fraud, spam, software piracy, spreading of viruses and so on, which invade our privacy and offend our senses. Criminal activities over internet are on the rise.

The cybercrime today is the latest and perhaps the most complicated problem in the cyber world. A generalized definition of cyber crime may be "unlawful acts wherein the computer is either a tool or target or both". The other definition could be, "cyber crime is a form of crime where the internet or computers are used as a medium to commit crime". According to Pavan Duggal, Supreme Court Advocate and Cyber Law expert, "Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crimes."

The National Research Council, "Computers A Risk" , 1991 has stated:

"The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb".

The cyber crime has been a problem as early as the late 1970s. The first spam e-mail took place in 1978 and the first virus was installed on an Apple Computer in 1982. In 2006, about 2000 complaints relating to cyber crime were received and the major reasons for such

complaints were financial fraud, viruses and hackers. It has also been found that there has been a constant increase in the number of children being exposed to unwanted pornography, internet harassment and bullying.

Now the question arises that who are these cyber criminals and who are their victims? Mostly, it has been observed that these cyber criminals are:

- Children and adolescents between the age group of 6-18 years. Reason for such kind of behavior in them is due to the inquisitiveness to know and explore the things and other reason may be to prove themselves to be outstanding among other children in their group.
- The group of organized hackers, who adopt such behavior to fulfil their objectives of personal bias, fundamentalism etc. Eg. Pakistanis are said to be one of the best quality hackers in the world and their main target is the Indian Government sites to fulfill their political objectives. Also the *Microsoft* sites are always under attack by the hackers.
- The professional hackers who work for the money. These hackers are generally employed to hack the sites of the rivals and get credible, reliable and valuable information and to detect their loopholes.
- The group of discontented employees who are sacked by their employers or are dissatisfied with their employer. To avenge they normally hack the system of their employer.

Now, the various victims of the sufferers of the cybercrime are:

- Mostly, they are the companies who do not have any security awareness.
- The individuals who are *unaware* individuals, or *don't care* individuals or the *innocent* individuals.
- The another major victim is society as a whole.

Now, we will discuss the various modes/manner in which the cyber crime is committed.

DIFFERENT TYPES OF CYBER-CRIME:

As internet usage continues to rise throughout the world, the threat of cyber crime also grows. While some of the crimes are relatively harmless, others are very serious. The various crimes where computer is a tool for unlawful acts are:

HACKING:

'Hacking' is the most common type of cybercrime committed across the world. Hacking has been defined in section 66 of IT ACT 2000 as "whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person, destroys or deletes or alters any information residing in the computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking. In simple words, hacking is a crime which entails cracking systems and gaining unauthorized access to the data stored in them. Hacker is a person who breaks in or trespasses a computer system.

CYBER - STALKING:

Cyber stalking is use of internet or other electronic means to stalk someone. It is online harassment and online abuse. Mostly cyber stalking involves following a person's movement across the internet by posting threatening messages to the victim or by entering the chat-rooms frequented by the victim or by constantly bombarding the victim with the e-mails etc.

VIRUS DISSEMINATION:

Virus is the programs which attach themselves to the computer or file and then circulate themselves to other files and to other components on a network. They usually affect the data on the computer, either by altering or deleting it.

DISSEMINATION OF OBSCENE MATERIAL/ PORNOGRAPHY:

Internet has provided a medium for the facilitation of crimes like pornography. Almost 50% of the websites exhibit pornographic material today. This crime includes hosting the website containing this prohibited material, use of computers for producing these obscene materials and downloading through the internet the obscene material. These obscene matters may cause harm to the minds of adolescent and tend to corrupt their minds.

CYBER TERRORISM:

This type of cyber crime can involve using the internet to communicate with other terrorists, to transfer the money needed to fund a terrorist act or any other related activity.

CYBER DEFAMATION:

Defamation as an act to impute any person with an intention to lower the person in the estimation of right-thinking members of the society. Cyber defamation involves use of computer or the internet as a medium to commit such crime. E.g. the e-mail account of *Rahul* and some mails from his account was sent to some of his friends regarding his relationship with underworld with an intent to defame him.

ONLINE FRAUD AND CHEATING

This is also a form of cybercrime. It can be in the form of credit card crime, offering jobs etc. Certain computer viruses can log keystrokes on your keyboard and send them to the hackers, who can then take your social security numbers, credit card numbers and home addresses. This information can be used by the hacker for his own means.

PHISHING:

Phishing is one of the many frauds on the internet, trying to fool people into parting with their money. Phishing refers to the receipt of unsolicited e-mails by customers of financial institutions, requesting them to enter their username, password or other personal information to access their accounts for some reason.

E – MAIL SPOOFING:

A spoofed e-mail is one that appears to originate from one source but actually has been sent from another source. This can also be termed as e- mail forging.

FORGERY:

Sometimes counterfeit currency notes. Postage and revenue stamps, mark-sheets etc. can be forged using sophisticated computer, printers and scanners.

E-MAIL BOMBING:

It involves sending large number of mails to a victim, which can be an individual or a company, which ultimately results in crashing.

DATA DIDDLING:

It is altering of raw data before the computer processes it and then changing it back after the processing is completed. It may lead to huge losses to the organizations.

SALAMI ATTACKS:

It is a kind of cybercrime which is generally done to commit financial crimes. The key here is to make the alterations so insignificant that in a single case it would go completely unnoticed. Eg. A bank employees inserts a program into the bank's server that deducts a small amount from the account of every customer.

INTERNET TIME THEFTS:

I is a kind of theft in which the internet surfing hours of the victims are used by some another person by gaining access to their ID and password.

LOGIC BOMBS:

These are dependent programs i.e. theses programs are created to do something only when certain event occurs.e.g. some viruses may be termed as logic bombs because they lie dormant all through the year and become active only on a particular date.

TROJAN HORSE:

A Trojan is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

So, these were some of the commonly faced cybercrimes which affect millions of people every day. Time now is not only to be aware of various types of cybercrimes but also to take preventive steps so that we can protect ourselves from its damaging consequences.

PREVENTION OF CYBER CRIME:

It has been rightly said that "Prevention is better than cure" so. It is always better to take certain precautions while operating the internet. So one should keep in mind the following:

1) Children should not give their identifying information such as their name, home address, school name, phone number in chat room. They should also be advised not to give their photographs to anyone, not to respond to the messages which are obscene, threatening or suggestive. They should remember that people online might not be who they seem.
2) Parents should use content filtering software on their computers so that their child is protected from the pornography, gambling drugs and alcohol. Software can also be installed to establish time records i.e. blocking usage after particular time. Parents should also visit the sites visited by their children.
3) Keep back-up volumes so that one may not suffer data loss in case of virus contamination.
4) Always use latest and update anti-virus software to guard against virus attacks.
5) Never send your credit card number to any site which is not secured.
6) Do not panic if you find something harmful. If you feel any immediate physical danger, contact your local police. Moreover avoid getting into huge arguments online

during chat and discussions with other users. Be careful about personal information about yourself online.

7) Be cautious on meeting online introduced person. If you choose to meet, do so in a public place along with a friend. Try to keep record of all your communication for evidence. Do not edit it any way.
8) Big organizations should implement acess control system using firewalls, which allow only authorized communications between the internal and external network.
9) The use of password is most common for security of netwok system. Mostly all the systems are programmed to ask for username and password to access the computer system. Password should be changed after regular interval of time and should be alpha numeric and should be difficult to judge.
10) System managers should track down the holes, bugs and weaknesses in the network before the intruders do.

CYBER LAW IN INDIA:

To further deal with the problem of cybercrime the victims can even take the help of Information Technology Act,2000. India enacted this act to regulate and control the affairs of cyber world in an effective manner. Chapter 1X of this act deals with offences/crimes along with certain other provisions scattered in this act. The various offences which are provided under this chapter are:

Tampering with Computer source documents	Sec.65
Hacking with Computer systems, Data alteration	Sec.66
Publishing obscene information	Sec.67
Un-authorised access to protected system	Sec.70
Breach of Confidentiality and Privacy	Sec.72
Publishing false digital signature certificates	Sec.73

CONCLUSION:

No doubt, it is not possible to eliminate cybercrime in total. However, it is quite possible to check them. Legislation cannot totally succeed in eliminating crime from the globe. So, let us try to be aware of our rights and duties i.e. to report the crime as a collective duty towards the society and making the application of laws more stringent to check crime.

REFERENCES:

1) Parthasarathi Pati - Cyber Crime
2) V. Shiva Kumar - Cyber Crime - Prevention and Detection
3) Singh G. (2006), E-Commerce, Kalyani Publishers, pg 237-239
4) Dr. B.Muthukumaran – Cyber Crime Scenario In India
5) Nagpar R. - What is Cyber Crime?
6) Duggal Pawan - Cybercrime

Websites:

www.ehow.com

www.cybercellmumbai.com