AFFECT OF CYBER CRIME

Written by By ***Dr. Mohd Aamir Khan***
(LL.M, Ph.D, NET, M.A. Eng Lit.)

"It is excellent To have a giant's strength,
but it is tyrannous To use it like a giant" (Shakespeare In Measure for Measure)

"Kya Yeh Tehzeeb Apne Khanjar Se Aap Hi Khudkashi Karegi" .?
(Is this civilization is going to commit suicide with its own knife.?)

From the discovery of wheel till the Newtonic Physics, the humanity has experienced many revolutions. And the last 200 years are marked as the era of Science and Technology. Even the specialists can't claim to have full knowledge of their subject. Science and technology are probably the most debated topics in society. Scientific and technological developments have been debated as to whether they affect people's life styles and cause hassle. Or on the contrary, science and technology has improved our way of life for the better of mankind. The vital role of science in modern life is not overstated in view of today's world. Science and technology have profoundly influenced the course of human civilization. Science has provided us remarkable insights into the world we live in. The scientific revolutions of the 21st century have led to many technologies, which promise to herald wholly new eras in many fields. This century marks especially the progress in Information and Technology. All over the web computer and internet is spread. It is just a matter of clicking the mouse and we can travel across the globe. Many people are profiting from it but there are many who are misusing or rather using it for their own advantage in spreading hatred, violence, terror etc. As we stand today at the beginning of a new century, we have to ensure fullest use of these developments for the wellbeing of our people and mankind.

Cyber Crime

To protect the society and individual from all this new laws especially "Cyber Law" has been created. "Cyber" is a prefix used to describe a person, thing, or idea as part of the computer and information age. A combining form representing computer (cyber talk; cyber art; cybercafé) and by extension meaning “very modern” (cyber fashion).

As Internet usage is growing daily the world is coming closer. The World Wide Web sounds like a vast phenomenon but surprisingly one of its qualities is bringing the world closer making it a smaller place to live in for its users. However, it has also managed to create another problem for people who spend long hours browsing the Cyber World – which is cyber-crimes. While law enforcement agencies are trying to tackle this problem, it is growing steadily and many people have become victims of hacking, theft, identity theft and malicious software. One of the best ways to avoid being a victim of cyber-crimes and protecting your sensitive information is by making use of impenetrable security that uses a unified system of software and hardware to authenticate any information that is sent or accessed over the Internet. However, before we can understand more about this system, let us find out more about cyber-crimes.

Causes of Cyber Crime

Wherever the rate of return on investment is high and the risk is low, you are bound to find people willing to take advantage of the situation. This is exactly what happens in cyber-crime. Accessing sensitive information and data and using it means a rich harvest of returns and catching such criminals is difficult. Hence, this has led to a rise in cyber crime across the world.

History of Cyber Crime

When computers and networks came into being in the 1990s, hacking was done basically to get more information about the systems. Hackers even competed against one another to win the tag of the best hacker. As a result, many networks were affected; right from the military to commercial organizations. Initially, these hacking attempts were brushed off as mere nuisance as they did not pose a long-term threat. However, with malicious software becoming ubiquitous during the same period, hacking started making networks and systems slow. As hackers became

more skillful, they started using their knowledge and expertise to gain benefit by exploiting and victimizing others.

Cyber Crime in Modern Society

Today, criminals that indulge in cyber crimes are not driven by ego or expertise. Instead, they want to use their knowledge to gain benefits quickly. They are using their expertise to steal, deceive and exploit people as they find it easy to earn money without having to do an honest day's work.

Cyber crimes have become a real threat today and are quite different from old-school crimes, such as robbing, mugging or stealing. Unlike these crimes, cyber crimes can be committed single handedly and does not require the physical presence of the criminals. The crimes can be committed from a remote location and the criminals need not worry about the law enforcement agencies in the country where they are committing crimes. The same systems that have made it easier for people to conduct e-commerce and online transactions are now being exploited by cyber criminals.

Cyber Crimes: Classified

Types of Cyber Crimes

When any crime is committed over the Internet it is referred to as a cyber crime. There are many types of cyber crimes and the most common ones are explained below:
The subject of cyber crime may be broadly classified under the following three groups. They are-

1. Against Individuals

a. their person &
b. their property of an individual

2. Against Organization

a. Government

c. Firm, Company, Group of Individuals.

3. Against Society at large

The following are the crimes, which can be committed against the followings group

Against Individuals

i. Harassment via e-mails.

ii. Cyber-stalking.

iii. Dissemination of obscene material.

iv. Defamation.

v. Unauthorized control/access over computer system.

vi. Indecent exposure

vii. Email spoofing

viii. Cheating & Fraud

Against Individual Property

i. Computer vandalism.

ii. Transmitting virus.

iii. Netrespass

iv. Unauthorized control/access over computer system.

v. Intellectual Property crimes

vi. Internet time thefts

Against Organization

i. Unauthorized control/access over computer system
ii. Possession of unauthorized information.
iii. Cyber terrorism against the government organization.
iv. Distribution of pirated software etc.

Against Society at large

i. Pornography (basically child pornography).
ii. Polluting the youth through indecent exposure.
iii. Trafficking
iv. Financial crimes
v.Sale of illegal articles
vi.Online gambling
vii. Forgery

The above mentioned offences may discussed in brief as follows:

1. Hacking- This is a type of crime wherein a person's computer is broken into so that his personal or sensitive information can be accessed. In the United States, hacking is classified as a felony and punishable as such. This is different from ethical hacking, which many organizations use to check their Internet security protection. In hacking, the criminal uses a variety of software to enter a person's computer and the person may not be aware that his computer is being accessed from a remote location.

2. Theft- This crime occurs when a person violates copyrights and downloads music, movies, games and software. There are even peer sharing websites which encourage

software piracy and many of these websites are now being targeted by the FBI. Today, the justice system is addressing this cyber crime and there are laws that prevent people from illegal downloading.

3. Cyber Stalking - The Oxford dictionary defines stalking as "pursuing stealthily". Cyber stalking involves following a person's movements across the Internet by posting messages (sometimes threatening) on the bulletin boards frequented by the victim, entering the chat-rooms frequented by the victim, constantly bombarding the victim with emails etc.

4. Identity Theft - This has become a major problem with people using the Internet for cash transactions and banking services. In this cyber crime, a criminal accesses data about a person's bank account, credit cards, Social Security, debit card and other sensitive information to siphon money or to buy things online in the victim's name. It can result in major financial losses for the victim and even spoil the victim's credit history.

5. Malicious Software - These are Internet-based software or programs that are used to disrupt a network. The software is used to gain access to a system to steal sensitive information or data or causing damage to software present in the system.

6. Dissemination of obscene material/ Indecent exposure/ Pornography (basically child pornography),Child soliciting and Abuse/ Polluting through indecent exposure - This is also a type of cyber crime wherein criminals solicit minors via chat rooms for the purpose of child pornography. The FBI has been spending a lot of time monitoring chat rooms frequented by children with the hopes of reducing and preventing child abuse and soliciting.

7. Pornography on the net may take various forms. It may include the hosting of web site containing these prohibited materials. Use of computers for producing these obscene materials. Downloading through the Internet, obscene materials. These obscene matters

may cause harm to the mind of the adolescent and tend to deprave or corrupt their mind. Two known cases of pornography are the Delhi Bal Bharati case and the Bombay case wherein two Swiss couple used to force the slum children for obscene photographs. The Mumbai police later arrested them.

8. Harassment via e-mails- Harassment through e-mails is not a new concept. It is very similar to harassing through letters. Recently I had received a mail from a lady wherein she complained about the same. Her former boy friend was sending her mails constantly sometimes emotionally blackmailing her and also threatening her. This is a very common type of harassment via e-mails.

9. Defamation - It is an act of imputing any person with intent to lower the person in the estimation of the right-thinking members of society generally or to cause him to be shunned or avoided or to expose him to hatred, contempt or ridicule. Cyber defamation is not different from conventional defamation except the involvement of a virtual medium. E.g. the mail account of Rohit was hacked and some mails were sent from his account to some of his batch mates regarding his affair with a girl with intent to defame him.

10. Unauthorized control/access over computer system-This activity is commonly referred to as hacking. The Indian law has however given a different connotation to the term hacking, so we will not use the term "unauthorized access" interchangeably with the term "hacking" to prevent confusion as the term used in the Act of 2000 is much wider than hacking.

11. E mail spoofing(Transmitting virus/worms)- A spoofed e-mail may be said to be one, which misrepresents its origin. It shows it's origin to be different from which actually it originates. An spoofed e-mail can contained virus.

12. Computer vandalism- Vandalism means deliberately destroying or damaging property of another. Thus computer vandalism may include within its purview any kind of physical harm done to the computer of any person. These acts may take the form of the

theft of a computer, some part of a computer or a peripheral attached to the computer or by physically damaging a computer or its peripherals.

13. Intellectual Property crimes / Distribution of pirated software- Intellectual property consists of a bundle of rights. Any unlawful act by which the owner is deprived completely or partially of his rights is an offence. The common form of IPR violation may be said to be software piracy, copyright infringement, trademark and service mark violation, theft of computer source code, etc.

14. Cyber terrorism against the government organization -Cyber terrorism and Cyber crime both are criminal acts. However there is a compelling need to distinguish between both these crimes. A cyber crime is generally a domestic issue, which may have international consequences, however cyber terrorism is a global concern, which has domestic as well as international consequences. The common form of these terrorist attacks on the Internet is by distributed denial of service attacks, hate websites and hate emails, attacks on sensitive computer networks, etc. Technology savvy terrorists are using 512-bit encryption, which is next to impossible to decrypt.

Cyber terrorism may be defined to be " the premeditated use of disruptive activities, or the threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives"

Another definition may be attempted to cover within its ambit every act of cyber terrorism.

A terrorist means a person who indulges in wanton killing of persons or in violence or in disruption of services or means of communications essential to the community or in damaging property with the view to –

(1) putting the public or any section of the public in fear; or

(2) affecting adversely the harmony between different religious, racial, language or regional groups or castes or communities; or

(3) coercing or overawing the government established by law; or

(4) endangering the sovereignty and integrity of the nation

and a cyber terrorist is the person who uses the computer system as a means or ends to achieve the above objectives. Every act done in pursuance thereof is an act of cyber terrorism.

15. Trafficking -Trafficking may assume different forms. It may be trafficking in drugs, human beings, arms weapons etc. These forms of trafficking are going unchecked because they are carried on under pseudonyms. A racket was busted in Chennai where drugs were being sold under the pseudonym of honey.

16. Fraud & Cheating-Online fraud and cheating is one of the most lucrative businesses that are growing today in the cyber space. It may assume different forms. Some of the cases of online fraud and cheating that have come to light are those pertaining to credit card crimes, contractual crimes, offering jobs, etc

In the end, one can conclude that by Science and technology the society has benefitted but some problems have also supplemented it. It has been seen that most cyber criminals have a loose network wherein they collaborate and cooperate with one another. Unlike the real world, these criminals do not fight one another for supremacy or control. Instead they work together to improve their skills and even help out each other with new opportunities. Hence, the usual methods of fighting crime cannot be used against cyber criminals. While law enforcement agencies are trying to keep pace with cyber criminals, it is proving to be a Herculean task. This is primarily because the methods used by cyber criminals and technology keeps changing too quickly for law enforcement agencies to be effective. That is why commercial institutions and government organizations need to look at other methods of safeguarding themselves.

Popping up over time that will need something bigger, better or a new cure for. Prevention is always better than cure. It is always better to take certain precaution while operating the net. A

should make them his part of cyber life. Precaution, Prevention, Protection, Preservation and Perseverance. A netizen should keep in mind the following things-

1. To prevent cyber stalking avoid disclosing any information pertaining to oneself. This is as good as disclosing your identity to strangers in public place.
2. Always avoid sending any photograph online particularly to strangers and chat friends as there have been incidents of misuse of the photographs.
3. Always use latest and up date anti virus software to guard against virus attacks.
4. Always keep back up volumes so that one may not suffer data loss in case of virus contamination
5. Never send your credit card number to any site that is not secured, to guard against frauds.
6. Always keep a watch on the sites that our children are accessing to prevent any kind of harassment or depravation in children.
7. It is better to use a security programme that gives control over the cookies and send information back to the site as leaving the cookies unguarded might prove fatal.
8. Web site owners should watch traffic and check any irregularity on the site. Putting host-based intrusion detection devices on servers may do this.
9. Use of firewalls may be beneficial.
10. Web servers running public sites must be physically separate protected from internal corporate network.

There are many major reasons why cyber-crime happen.

1. Loopholes in system- Operating systems have complex codes that can be decoded or manipulated to gain access to the system. There are always loopholes in security that a professional cyber criminal can find and hack into. The traditional bank robber researched the security system and took advantage of it; a cyber thief is not much different, except he can breach security virtually.

2. Lack of Evidence -One cause of increasing cyber crime is the lack of evidence to bind the criminal by law. There are so many ways to hide the trail of a cyber crime and little to actually police the criminal.Also loss of evidence is a very common & obvious

problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of Crime Investigation.

3. New Form of Crime - There are so many modes of criminal activity on the Net that the traditional policing methods and the laws that bind criminals at times lose jurisdiction in cyber crime cases. This is why there are so many crimes being committed online.

4. Negligence- Sometimes simple negligence can give rise to criminal activities, such as saving a password on an official computer, using official data in a public place and even storing data without protecting it. The cyber criminal can take advantage of such negligence and use it to obtain, manipulate and forge information. Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a Cyber Criminal to gain access and control over the computer system.

5. Confidential Information is online -Confidential data from security firms, scientific databases, financial institutes and even governmental organizations is stored online and on networks. This allows cyber criminals to initiate unauthorized access and use it for their own needs. Complex technology can be manipulated and firewalls can be bypassed, allowing criminals to gain access to security codes, bank accounts and other information.

6. Desire of Making quick money-Another cause of cyber-crime is to make quick money. Greed motivates and create criminals, who tamper with data on the net or system especially, e-commerce, e-banking data information with the sole aim of committing fraud and swindling money off unsuspecting customers.