CYBER CRIMES AND SOLUTIONS

We are currently living in Cyber age, where Internet and computers have major impacts on our way of living, social life and the way we conduct businesses.

By: Shaikh Mohsin Ayaz

The usage of information technology has posed great security challenges and ethical questions in front of us. Just as every thing has positives and negatives, usage of information technology is beneficial as well as insecure.

With the growth of the internet, network security has become a major concern. Cyber crimes have emerged rapidly in the last few years and have major consequences. Cyber criminals are doing every thing from stealing money, hacking into others computer, stealing intellectual property, spreading viruses and worms to damage computers connected on the internet and committing frauds.

Stoppage of cyber crimes is a major concern today.

Cyber criminals make use of the vulnerabilities in computer soft wares and networks to their advantage.

Hacking:

Hacking or Cracking is a major cyber crime committed today. Hackers makes use of the weaknesses and loop holes in operating systems to destroy data and steal important information from victim's computer. Cracking is normally done through the use of a backdoor program installed on your machine. A lot of crackers also try to gain access to resources through the use of password cracking softwares. Hackers can also monitor what u do on your computer and can also import files on your computer. A hacker could install several programs on to your system without your knowledge. Such programs could also be used to steal personal information such as passwords and credit card information. Important data of a company can also be hacked to get the secret information of the future plans of the company.

Cyber-Theft:

Cyber-Theft is the use of computers and communication systems to steal information in electronic format. Hackers crack into the systems of banks and transfer money into their own bank accounts. This is a major concern, as larger amounts of money can be stolen and illegally transferred.

Many newsletters on the internet provide the investors with free advice recommending stocks where they should invest. Sometimes these recommendations are totally bogus and cause loss to the investors. Credit card fraud is also very common.

Most of the companies and banks don't reveal that they have been the victims of cyber -theft because of the fear of losing customers and share holders. Cyber-theft is the most common and the most reported of all cyber-crimes. Cyber-theft is a popular cyber-crime because it can quickly bring experienced cyber-criminals large amounts of cash resulting from very little effort. Furthermore, there is little chance of a professional cyber-criminal being apprehended by law enforcement.

Viruses and worms:

Viruses and worms is a very major threat to normal users and companies. Viruses are computer programs that are designed to damage computers. It is named virus because it spreads from one computer to another like a biological virus. A virus must be attached to some other program or documents through which it enters the computer. A worm usually exploits loop holes in software or the operating system. Trojan horse is dicey. It appears to do one thing but does something else. The system may accept it as one thing. Upon execution, it may release a virus, worm or logic bomb. A logic bomb is an attack triggered by an event, like computer clock reaching a certain date. Chernobyl and Melissa viruses are the recent examples.

Experts estimate that the Mydoom worm infected approximately a quarter-million computers in a single day in January 2004. Back in March 1999, the Melissa virus was so powerful that it forced Microsoft and a number of other very large companies to completely turn off their e-mail systems until the virus could be contained.

Solutions:

An important question arises that how can these crimes be prevented. A number of techniques and solutions have been presented but the problem still exists and are increasing day by day.

Antivirus And Anti spyware Software:

Antivirus software consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software. Anti spyware are used to restrict backdoor programs, trojans and other spyware to be installed on the computer.

Firewalls:

A firewall protects a computer network from unauthorized access. Network firewalls may be hardware devices, software programs, or a combination of the two. A network firewall typically guards an internal computer network against malicious access from outside the network.

Cryptography:

Cryptography is the science of encrypting and decrypting information. Encryption is like sending a postal mail to another party with a lock code on the envelope which is known only to the sender and the recipient. A number of cryptographic methods have been developed and some of them are still not cracked.

Cyber Ethics and Laws:

Cyber ethics and cyber laws are also being formulated to stop cyber crimes. It is a responsibility of every individual to follow cyber ethics and cyber laws so that the increasing cyber crimes shall reduce. Security software like anti viruses and anti spyware should be installed on all computers, in order to remain secure from cyber crimes. Internet Service Providers should also provide high level of security at their servers in order to keep their clients secure from all types of viruses and mallicious programs.

Article Source: http://EzineArticles.com/204167