Introduction to cyber crime

Law, Crime

The first recorded cyber crime took place in the year 1820! That is not surprising considering the fact that the abacus, which is thought to be the earliest form of a computer, has been around since 3500 B. C. in India, Japan and China. The era of modern computers, however, began with the analytical engine of Charles Babbage. Cyber crime is an evil having its origin in the growing dependence on computers in modern life. In a day and age when everything from microwave ovens and refrigerators to nuclear power plants is being run on computers, cyber crime has assumed rather sinister implications.

Major cyber crimes in the recent past include the Citibank rip off. US $ 10 million were fraudulently transferred out of the bank and into a bank account in Switzerland. A Russian hacker group led by Vladimir Kevin, a renowned hacker, perpetrated the attack. The group compromised the bank's security systems. Vladimir was allegedly using his office computer at AO Saturn, a computer firm in St. Petersburg, Russia, to break into Citibank computers. He was finally arrested on Heathrow airport on his way to Switzerland.

Defining Cyber Crime

Defining cyber crimes, as " acts that are punishable by the Information Technology Act" would be unsuitable as the Indian Penal Code also covers many cyber crimes, such as email spoofing and cyber defamation, sending threatening emails etc. A simple yet sturdy definition of cyber crime would be " unlawful acts wherein the computer is either a tool or a target or both".

Financial crimes - This would include cheating, credit card frauds, money laundering etc. To cite a recent case, a website offered to sell Alphonso mangoes at a throwaway price. Distrusting such a transaction, very few people responded to or supplied the website with their credit card numbers. These people were actually sent the Alphonso mangoes. The word about this website now spread like wildfire. Thousands of people from all over the country responded and ordered mangoes by providing their credit card numbers. The owners of what was later proven to be a bogus website then fled taking the numerous credit card numbers and proceeded to spend huge amounts of money much to the chagrin of the card owners.

Cyber pornography - (to publish and print the material) and the Internet (to download and transmit pornographic pictures, photos, writings etc). Recent Indian incidents revolving this would include pornographic websites; pornographic magazines produced using computers around cyber pornography include the Air Force Balbharati School case. A student of the Air Force Balbharati School, Delhi, was teased by all his classmates for having a pockmarked face. Tired of the cruel jokes, he decided to get back at his tormentors. He scanned photographs of his classmates and teachers, morphed them with nude photographs and put them up on a website that he uploaded on to a free web hosting service. It was only after the father of one of the class girls featured on the website objected and lodged a complaint with the police that any action was taken.

In another incident, in Mumbai a Swiss couple would gather slum children and then would force them to appear for obscene photographs. They would then upload these photographs to websites specially designed for paedophiles. The Mumbai police arrested the couple for pornography.

Sale of illegal articles - This would include sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or 167 simply by using email communication. E. g. many of the auction sites even in India are believed to be selling cocaine in the name of 'honey'.

Online gambling - There are millions of websites; all hosted on servers abroad, that offer online gambling. In fact, it is believed that many of these websites are actually fronts for money laundering.

Intellectual Property crimes - These include software piracy, copyright infringement, trademarks violations, theft of computer source code etc. A spoofed email is one that appears to originate from one source but actually has been sent from another source. E. g. Pooja has an e-mail address[email protected]Her enemy, Sameer spoofs her e-mail and sends obscene messages to all her acquaintances. Since the e-mails appear to have originated from Pooja, her friends could take offence and relationships could be spoiled for life. Email spoofing can also cause monetary damage.

In an American case, a teenager made millions of dollars by spreading false information about certain companies whose shares he had short sold. This misinformation was spread by sending spoofed emails, purportedly from news agencies like Reuters, to share brokers and investors who were informed that the companies were doing very badly. Even after the truth came out the values of the shares did not go back to the earlier levels and thousands of investors lost a lot of money.

Forgery - Counterfeit currency notes, postage and revenue stamps, mark sheets etc can be forged using sophisticated computers, printers and scanners. Outside many colleges across India, one finds touts soliciting the sale of fake mark sheets or even certificates. These are made using computers, and high quality scanners and printers. In fact, this has becoming a booming business involving thousands of Rupees being given to student gangs in exchange for these bogus but authentic looking certificates.

Cyber Defamation - This occurs when defamation takes place with the help of computers and / or the Internet. E. g. someone publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends. In a recent occurrence, Surekha (names of people have been changed), a young girl was about to be married to Suraj. She was really pleased because despite it being an arranged marriage, she had liked the boy. He had seemed to be open-minded and pleasant.

Then, one day when she met Suraj, he looked worried and even a little upset. He was not really interested in talking to her. When asked he told her that, members of his family had been receiving e-mails that contained malicious things about Surekha's character. Some of them spoke of affairs, which she had had in the past. He told her 168 that, his parents were justifiably very upset and were also considering breaking off the engagement. Fortunately, Suraj was able to prevail upon his parents and the other elders of his house to approach the police instead of blindly believing what was contained in the mails.

During investigation, it was revealed that the person sending those e-mails was none other than Surekha's stepfather. He had sent these e-mails so as to break up the marriage. The girl's marriage would have caused him to lose control of her property of which he was the guardian till she got married. Another famous case of cyber defamation occurred in America. All friends and relatives of a lady were beset with obscene e-mail messages appearing to originate from her account. These mails were giving the lady in question a bad name among her friends. The lady was an activist against pornography. In reality, a group of people displeased with her views and angry with her for opposing they had decided to get back at her by using such underhanded methods. In addition to sending spoofed obscene e-mails they also put up websites about her, that basically maligned her character and sent e-mails to her family and friends containing matter defaming her.

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.

Frequently Used Cyber Crimes

Unauthorized access to computer systems or networks - 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". Theft of information contained in electronic form, this includes information stored in computer hard disks, removable storage media etc

E-mail bombing - Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing. Some of the major email related crimes are:

1. Email spoofing 2. Sending malicious codes through email 3. Email bombing 4. Sending threatening emails 5. Defamatory emails 6. Email frauds.

Data diddling and then changing it back after the processing is completed. Electricity Boards in India have been in this kind of an attack, it involves altering raw data just before it is processed by a computer victims to data diddling programs inserted when private parties were computerizing their systems. Salami attacks - These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed.

Denial of Service attack - This involves flooding a computer resource with more requests than it can handle. This causes the resource (e. g. a web server) to crash thereby denying authorized users the service offered by the resource. Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. It is very difficult to control such attacks. The attack is initiated by sending excessive demands to the victim's computer(s), exceeding the limit that the victim's servers can support and making the servers crash.

Virus / worm attacks - Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory.

Logic bombs - These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E. g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date. Trojan attacks - A Trojan as this program is aptly called, is an unauthorized program which functions from inside what seems to be an authorized program, thereby concealing what it is actually doing.

Internet time thefts - This connotes the usage by an unauthorized person of the Internet hours paid for by another person. In a case reported before the enactment of the Information Technology Act, 2000 Colonel Bajwa, a resident of New Delhi, asked a nearby net cafe owner to come and set up his Internet connection. For this purpose, the net cafe owner needed to know his username and password.

After having set up the connection he went away with knowing the present username and password. He then sold this information to another net cafe. One week later Colonel Bajwa found that his Internet hours were almost over. Out of the 100 hours that he had bought, 94 hours had been used up within the span of that week. Surprised, he reported the incident to the Delhi police. The police could not believe that time could be stolen. They were not aware of the concept of time-theft at all. Colonel Bajwa's report was rejected. He decided to approach The Times of India, New Delhi. They, in turn carried a report about the inadequacy of the New Delhi Police in handling cyber crimes. The Commissioner of Police, Delhi then took the case into his own hands and the police under his directions raided and arrested the net cafe owner under the charge of theft as defined by the Indian Penal Code. The net cafe owner spent several weeks locked up in Tihar jail before being granted bail.

Web jacking - This occurs when someone forcefully takes control of a website (by cracking the password and later changing it). The actual owner of the website does not have any more control over what appears on that website In a recent incident reported in the USA the owner of a hobby website for children received an e-mail informing her that a group of hackers had gained control over her website.

Theft of computer system - This type of offence involves the theft of a computer, some part's of a computer or a peripheral attached to the computer, physically damaging a computer system. This crime is committed by physically damaging a computer or its peripherals.

Cyber Criminals - It seems really difficult to believe but it is true that most amateur hackers and cyber criminals are teenagers. To them, who have just begun to understand what appears to be a lot about computers, it is a matter of pride to have hacked into a computer system or a website. There is also that little issue of appearing really smart among friends. These young rebels may also commit cyber crimes without really knowing that they are doing anything wrong.

Organized hacktivists - Hacktivists are hackers with a particular (mostly political) motive. In other cases this reason can be social activism, religious activism, etc. The attacks on approximately 200 prominent Indian websites by a group of hackers known as Pakistani Cyber Warriors are a good example of political hacktivists at work.

Disgruntled employees - One can hardly believe how spiteful displeased employees can become. Till now they had the option of going on strike against their bosses. Now, with the increase independence on computers and the automation of processes, it is easier for disgruntled employees to do more harm to their employers by committing computer related crimes, which can bring entire systems down.

Professional hackers (corporate espionage) - Extensive computerization has resulted in business organizations storing all their information in electronic form. Rival organizations employ hackers to steal industrial secrets and other information that could be beneficial to them. The temptation to use professional hackers for industrial espionage also stems from the fact that physical presence required to gain access to important documents is rendered needless if hacking can retrieve those.

The World's Most Famous Hackers Vladimir Levin His claim to fame is that this mathematician who graduated from St. Petersburg Tekhnologichesky University was the brain behind the Russian hacker gang that cheated Citibank's computers into giving out $10 million. Although his first use of a computer is unknown Vladimir was allegedly using his office computer at AO Saturn, a computer firm in St. Petersburg, Russia, to break into Citibank computers. Vladimir Levin was arrested at the Heathrow airport in 1995. Tools used by him included computer, computer games and disks, a camcorder, music speakers and a TV set all of which were found by the Russian police at his apartment. During his trial, Levin alleged that one of his defence lawyers was actually an FBI agent.

Johan Helsingius He was known to run the world's most popular re-mailer programme called penet. fi. Surprisingly, this re-mailer, the busiest in the world, was run on an ordinary 486 with a 200-megabyte hard drive. His other idiosyncrasy was that he never tried to remain anonymous. The Finnish police raided Johan in 1995 due to a complaint by the Church of Scientology that a penet. fi customer was posting the " church's" secrets on the Net. At that time Johan had to abandon the re-mailer.

Kevin Mitnick Kevin Mitnick alias on the Net was Condor. As a teenager Kevin Mitnick could not afford his own computer. He would therefore go to a Radio Shack store and use the models kept there for demonstration to dial into other computers. One of the unusual things about Mitnick was that he used the Internet Relay Chat (IRC) to send messages to his friends. A judge sentenced him to one year in a residential treatment center. There, Kevin enrolled in a 12-step program to rid him of what the judge also termed his " computer addiction". Mitnick was immortalized when he became the first hacker to have his face put on an FBI " most wanted" poster. His repeated offences - and an image of a teenage hacker who refused to grow up - made him The Lost Boy of Cyberspace.