CYBER CRIME

Definition of Cyber Crime

"Cyber crime encompasses any criminal act dealing with computers and networks (called hacking). Additionally, cyber crime also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cyber crimes when the illegal activities are committed through the use of a computer and the Internet."

A generalized definition of cyber crime may be "unlawful acts wherein the computer is either a tool or target or both". The computer may be used as a tool in the following kinds of activity- financial crimes, sale of illegal articles, pornography, online gambling, intellectual property crime, e-mail spoofing, forgery, cyber defamation, cyber stalking. The computer may however be target for unlawful acts in the following cases- unauthorized access to computer/ computer system/ computer networks, theft of information contained in the electronic form, e-mail bombing, data didling, salami attacks, logic bombs, Trojan attacks, internet time thefts, web jacking, theft of computer system, physically damaging the computer system.

Types of Cyber Crime

HACKING

Hackers write or use ready-made computer programs to attack the target computer. They possess the quality to enter in to target computer and obtain the data. Some hackers hack for personal monetary gains, such as to stealing the credit card information, transferring money from various bank accounts to their own account followed by withdrawal of money. They extort money from some corporate giant threatening them to publish the stolen information which is critical in nature.

CHILD PORNOGRAPHY

The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. The easy access to the pornographic contents readily and freely available over the internet lowers the inhibitions of the children. Pedophiles lure the children by distributing pornographic material, then they try to meet them for sex or to take their nude photographs including their engagement in sexual positions. Sometimes Pedophiles contact children in the chat rooms posing as teenagers or a child of similar age, then they start becoming friendlier with them and win their confidence. Then slowly pedophiles start sexual chat to help children shed their inhibitions about sex and then call them out for personal interaction. Then starts actual exploitation of the children by offering them some money or falsely promising them good opportunities in life. The pedophiles then sexually exploit the children either by using them as sexual objects or by taking their pornographic pictures in order to sell those over the internet. The children are advised to not to chat with strangers.

CYBER STALKING

Cyber Stalking can be defined as the repeated acts harassment or threatening behavior of the cyber criminal towards the victim by using internet services. The Stalkers have desire to control the victims life. Majority of the stalkers are the dejected lovers or ex-lovers, who then want to harass the victim because they failed to satisfy their secret desires. Most of the stalkers are men and victim female.

How do Stalkers Operate

Collect all personal information about the victim such as name, family background, Telephone Numbers of residence and work place, daily routine of the victim, address of residence and place of work, date of birth etc. If the stalker is one of the acquaintances of the victim he can easily get this information. If stalker is a stranger to victim, he collects the information from the internet resources such as various profiles, the victim may have filled in while opening the chat or e-mail account or while signing an account with some website.

The stalker may post this information on any website related to sex-services or dating services, posing as if the victim is posting this information and invite the people to call the victim on her telephone numbers to have sexual services. Stalker even uses very filthy and obscene language to invite the interested persons. Presently "ORKUT" website has become prone with such filthy messages being put Stalkers on the notice board of the said site.

People of all kind from nook and corner of the World, who come across this information, start calling the victim at her residence and/or work place, asking for sexual services or relationships.

Some stalkers subscribe the e-mail account of the victim to innumerable pornographic and sex sites, because of which victim starts receiving such kind of unsolicited e-mails.

CREDIT CARD FRAUD

The unauthorized and illegal use of a credit card to purchase property. Information about the credit card is obtained by using skimmers, the most prone places to such crimes are restaurants, bars etc. Information about the Credit Card is also obtained through Phishing. In case of anyone asking for the credit card details of the user on the internet, it is advised to first confirm telephonically from that particular organization.

PHISHING

The act of sending an e-mail to a user falsely claiming to be an legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security,

and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the users information. Phishing is the idea that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting. it is advised that the user should first confirm telephonically from that particular organization to whom he thinks he is supplying the information as genuine.

NET EXTORTION

Copying the company's confidential data in order to extort said company for huge amount.

VIRUS DISSEMINATION

Malicious software that attaches itself to other software. (virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious

SOFTWARE PIRACY

Theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original.

IRC CRIME

Internet Relay Chat (IRC) servers have chat rooms in which people from anywhere the world can come together and chat with each other. It is requested that, a summary of the above mentioned Cyber related crimes may be published in leading newspapers in Public Interest, to make the innocent net users aware of the same to prevent them from falling in traps of cyber criminals.

DENIAL OF SERVICE ATTACK

This is an act by the criminal, who floods the bandwidth of the victims network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide. Denial of Service attack, is a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic.. For all known DoS attacks, there are software that fixes the system administrators and can be installed to limit the damage caused by the attacks. But, like Virus, new DoS attacks are constantly being dreamed up by Hacker. In case the user feels that he has become the victim to denial of service he should complain about the same to the police.

Marked Currency / Defaced Black Currency / Wash-wash / Money Multiplier /Black Dollar Nigerian Advance Fee Fraud Cash Cleaning Money Scams.

The Internet users in such cases usually receives a surprising e-mail in which the sender allures the receiver of getting a very huge amount of foreign currency

One aspect of the Nigerian Advance Fee Fraud involves victims being informed of the existence of case loads of banknotes which are said to have been coated or stamped in order to disguise their identity from the authorities or for "security purposes".

This may even come as a surprise to the victim who, after paying untold fees to have the money finally released, discovers it that now it needs to be cleaned by chemical dye removers before it is useable. Such a process is accompanied with, of course, yet more fees or expenses.

Each foreign currency may be said to have a smudge on its face that will prevent detection by a scanning device as it passed through Customs machines, amid claims that the money is only for overseas use. It could even be deemed un-cashable for security purposes while in transit or while being held by the security company.

The alleged money is shown to the victim, who is told that the black coating or stamps can be removed by washing it with a special compound. The exotic and expensive mix of secret chemicals for cleaning money, which could be referred to as SSD Solution, Vectrol Paste, Lactima Base 98%, microtectine and Tebi-Matonic, is needed to "clean" a trunk or security case supposedly full of these illicit foreign currency notes and other millions stored overseas in a vault.

In fact, only a few real, blackened foreign curency bank notes are shown to the victim, and the special chemical is ordinary cleaning fluid which reacts with the black mixture of Vaseline and iodine. The remainder of the material in the case is blank, blackened paper often made simply by photocopying with the lid up and cutting the sheets down to banknote size.

In some cases the actual currency has been pre-coated with a protective layer of common white glue, then dyed with tincture of iodine. This is later removed with a "secret and expensive" solution consisting of only water and crushed vitamin C tablets.

In front of the victim the criminal will appear to randomly select between two and four notes from the case. He will then wash them in a tiny portion of the solution, which he has with him, returning them to their original form as real bank notes. They are given to the victim who is invited to spend them or get them checked at the bank to confirm that they are genuine.

In reality, the criminal knows perfectly well which notes he is selecting and selects the only real ones that are there. A really dexterous criminal will invite the victim to choose notes to clean and, by using a well practiced sleight of hand similar to a card trick, trick the victim into selecting the genuine ones.

The victim is asked to provide between US$50,000 and US$100,000 for bulk supplies of the cleaning compound, which the offender offers to procure.

On some occasions, as a sign of good faith, you may be able to keep the suitcase for a short time, until you obtain the money to buy the solution. To prevent you from opening the suitcase you could even be told that exposure to air will cause the black substance to ruin the money.

After the advance payment has been received, the chemicals are not delivered to the victim, who is left with suitcases full of worthless black paper instead of the foreign currency notes.