CYBER CRIMES

- **Hacking**
- **Child Pornography**
- **Cyber Stalking**
- **Denial of service Attack**
- **Virus Dissemination**
- **Phishing**

By

The Cyber Crime Investigation Cell of Mumbai Police

Ref: http://cybercellmumbai.gov.in/html/cyber-crimes/index.html

Hacking

Hacking in simple terms means an illegal intrusion into a computer system and/or network. There is an equivalent term to hacking i.e. cracking, but from Indian Laws perspective there is no difference between the term hacking and cracking. Every act committed towards breaking into a computer and/or network is hacking. Hackers write or use ready-made computer programs to attack the target computer. They possess the desire to destruct and they get the kick out of such destruction. 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 him to publish the stolen information which is critical in nature.

Government websites are the hot targets of the hackers due to the press coverage, it receives. Hackers enjoy the media coverage.

Motive behind the Crime

- Greed
- Power
- Publicity
- Revenge
- Adventure
- Desire to access forbidden information
- Destructive mindset

Child Pornography

The Internet is being highly used by its abusers to reach and abuse children sexually, worldwide. The internet is very fast becoming a household commodity in India. It explosion has made the children a viable victim to the cyber crime. As more homes have access to internet, more children would be using the internet and more are the chances of falling victim to the aggression of pedophiles.

The easy access to the pornographic contents readily and freely available over the internet lower 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.

In physical world, parents know the face of dangers and they know how to avoid & face the problems by following simple rules and accordingly they advice their children to keep away from dangerous things and ways. But in case of cyber world, most of the parents do not themselves know about the basics in internet and dangers posed by various services offered over the

internet. Hence the children are left unprotected in the cyber world. Pedophiles take advantage of this situation and lure the children, who are not advised by their parents or by their teachers about what is wrong and what is right for them while browsing the internet

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. Stalking in General terms can be referred to as the repeated acts of harassment targeting the victim such as following the victim, making harassing phone calls, killing the victims pet, vandalizing victims property, leaving written messages or objects. Stalking may be followed by serious violent acts such as physical harm to the victim and the same has to be treated and viewed seriously. It all depends on the course of conduct of the stalker.

Both kind of Stalkers Online & Offline – 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.

Definition of Cyber stalking?

Although there is no universally accepted definition of cyberstalking, the term is **used in this report to refer to the use of the Internet, e-mail, or other electronic communications devices to stalk another person.** Stalking generally involves harassing or threatening behavior that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property. Most stalking laws require that the perpetrator make a credible threat of violence against the victim; others include threats against the victim's

immediate family; and still others require only that the alleged stalker's course of conduct constitute an implied threat.(1) While some conduct involving annoying or menacing behavior might fall short of illegal stalking, such behavior may be a prelude to stalking and violence and should be treated seriously.

Nature and Extent of Cyberstalking

An existing problem aggravated by new technology
Although online harassment and threats can take many forms, cyberstalking shares important characteristics with offline stalking. Many stalkers – online or off – are motivated by a desire to exert control over their victims and engage in similar types of behavior to accomplish this end. As with offline stalking, the available evidence (which is largely anecdotal) suggests that the majority of cyberstalkers are men and the majority of their victims are women, although there have been reported cases of women cyberstalking men and of same-sex cyberstalking. In many cases, the cyberstalker and the victim had a prior relationship, and the cyberstalking begins when the victim attempts to break off the relationship. However, there also have been many instances of cyberstalking by strangers. Given the enormous amount of personal information available through the Internet, a cyberstalker can easily locate private information about a potential victim with a few mouse clicks or key strokes.

The fact that cyberstalking does not involve physical contact may create the misperception that it is more benign than physical stalking. This is not necessarily true. As the Internet becomes an ever more integral part of our

personal and professional lives, stalkers can take advantage of the ease of communications as well as increased access to personal information. In addition, the ease of use and non-confrontational, impersonal, and sometimes anonymous nature of Internet communications may remove disincentives to cyberstalking. Put another way, whereas a potential stalker may be unwilling or unable to confront a victim in person or on the telephone, he or she may have little hesitation sending harassing or threatening electronic communications to a victim. Finally, as with physical stalking, online harassment and threats may be a prelude to more serious behavior, including physical violence

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

Short for denial-of-service attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCp/IP protocols. For all known DoS attacks, there are software fixes that system administrators can install to limit the damage caused by the attacks. But, like Virus, new DoS attacks are constantly being dreamed up by Hacker

Virus Dissemination

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

Phishing

The act of sending an e-mail to a user falsely claiming to be an established 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 user information.. By spamming large groups of people, the phisher counted on the e-mail being read by a percentage of people who actually had listed credit card numbers with legitimately. Phishing, also referred to as brand spoofing or carding, is a variation on fishing, • the idea being that bait is thrown out with the hopes that while most will ignore the bait, some will be tempted into biting.