Cyber Crime: Definition, Types and Prevention

blog.ccasociety.com/cyber-crime-definition-types-and-prevention

April 30, 2020

Cybercrime is any criminal activity that involves a computer, networked device or a network. While most cybercrimes are carried out in order to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them, while others use computers or networks to spread malware, illegal information, images or other materials. Some cybercrimes do both — i.e., target computers to infect them with a computer virus, which is then spread to other machines and, sometimes, entire networks.

A primary effect of cybercrime is financial; cybercrime can include many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud, and identity fraud, as well as attempts to steal financial account, credit card or other payment card information. Cybercriminals may also target an individual's private information, as well as corporate data for theft and resale.

Defining cybercrime

Cyber crimes can be defined as the unlawful acts where the computer is used either as a tool or a target or both. The term is a general term that covers crimes like phishing, credit card frauds, bank robbery, illegal downloading, industrial espionage, child pornography, kidnapping children via chat rooms, scams, cyber terrorism, creation and/or distribution of viruses, Spam and so on.

Cyber crime is a broad term that is used to define criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It also covers the traditional crimes in which computers or networks are used to enable the illicit activity.

Different types of cyber crimes

The different kinds of cyber crimes are:

1. Unauthorized Access and Hacking:

Unauthorized access means any kind of access without the permission of either of the rightful or person in charge of the computer, computer system or computer network. Hacking means an illegal intrusion into a computer system and/or network. 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. Government websites are the most targeted sites for the hackers.

2. Web Hijacking:
Web hijacking means taking forceful control of another person's website. In this case the owner of the website loses control over his website and its content.

3. Pornography:
Pornography means showing sexual acts in order to cause sexual excitement. The definition of pornography also includes pornographic websites, pornographic magazines produced using computer and the internet pornography delivered over mobile phones.

4. Child Pornography:
The Internet is being highly used as a medium to sexually abuse children. The children are viable victim to the cyber crime. Computers and internet having become a necessity of every household, the children have got an easy access to the internet. There is an easy access to the pornographic contents on the internet. Pedophiles lure the children by distributing pornographic material and 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 and 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.

5. Cyber Stalking:
In general terms, stalking can be termed 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. Cyber Stalking means repeated acts of harassment or threatening behavior of the cyber criminal towards the victim by using internet services. Both kind of Stalkers i.e., Online & Offline – have desire to control the victims life.

6. Denial of service Attack:
This is an attack in which the criminal floods the bandwidth of the victim's network or fills his e-mail box with spam mail depriving him of the services he is entitled to access or provide. This kind of attack is designed to bring the network to crash by flooding it with useless traffic. 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. 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.

7. Virus attacks:
Viruses are the programs that have the capability to infect other programs and make copies of itself and spread into other program. Programs that multiply like viruses but spread from computer to computer are called as worms. These are malicious software that attach themselves to other software. Virus, worms, Trojan Horse, Time bomb, Logic Bomb, Rabbit and Bacterium are the malicious. Viruses usually affect the data on a computer, either by altering or deleting it. On the other hand worms merely make functional copies of themselves and do this repeatedly till they eat up all the available. Trojan Horse is a program that acts like something useful but do the things that are quiet damping. Trojans come in two parts, a Client part and a Server part. When the victim (unknowingly) runs the server on its machine, the attacker will then use the Client to connect to the Server and start using the Trojan. TCP/IP protocol is the usual protocol type used for communications, but some functions of the Trojans use the UDP protocol as well.

8. Software Piracy:
Software piracy refers to the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. These kind of crimes also include copyright infringement, trademarks violations, theft of computer source code, patent violations etc.
Domain names are also trademarks and protected by ICANN's domain dispute resolution policy and also under trademark laws. Cyber squatters register domain name identical to popular service provider's name so as to attract their users and get benefit from them .

9. 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. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month.

10. Phishing:
Phishing is 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's 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.

11. Sale of illegal articles:
This category of cyber crimes includes sale of narcotics, weapons and wildlife etc., by posting information on websites, auction websites, and bulletin boards or simply by using email communication.

12. 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. Cases of hawala transactions and money laundering over the Internet have been reported.

13. Email spoofing :
Email spoofing refers to email that appears to originate from one source but actually has been sent from another source. Email spoofing can also cause monetary damage.

14. Cyber Defamation:
When a person publishes defamatory matter about someone on a website or sends e-mails containing defamatory information to all of that person's friends, it is termed as cyber defamation.

15. Forgery:
Computers, printers and scanners are used to forge counterfeit currency notes, postage and revenue stamps, mark sheets etc. These are made using computers, and high quality scanners and printers.

16. Theft of information contained in electronic form :
This includes theft of information stored in computer hard disks, removable storage media etc.

17. Email 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.

18. Data diddling :
This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed.

19. Internet time theft :
Internet time refers to usage by an unauthorized person of the Internet hours paid for by another person.

20. 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.

21. Physically damaging a computer system :
This crime is committed by physically damaging a computer or its peripherals.

22. Breach of Privacy and Confidentiality :
Privacy refers to the right of an individual/s to determine when, how and to what extent his or her personal data will be shared with others. Breach of privacy means unauthorized use or distribution or disclosure of personal information.

Confidentiality means non disclosure of information to unauthorized or unwanted persons. In addition to Personal information some other type of information which useful for business and leakage of such information to other persons may cause damage to business or person, such information should be protected.
Generally for protecting secrecy of such information, parties while sharing information forms an agreement about he procedure of handling of information and to not to disclose such information to third parties or use it in such a way that it will be disclosed to third parties. Many times party or their employees leak such valuable information for monitory gains and causes breach of contract of confidentiality. Special techniques such as Social Engineering are commonly used to obtain confidential information.

23. Data diddling:
Data diddling involves changing data prior or during input into a computer. The information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. It also include automatic changing the financial information for some time before processing and then restoring original information.

24. E-commerce/ Investment Frauds:
An offering that uses false or fraudulent claims to solicit investments or loans, or that provides for the purchase, use, or trade of forged or counterfeit securities. Merchandise or services that were purchased or contracted by individuals online are never delivered. The fraud attributable to the misrepresentation of a product advertised for sale through an Internet auction site or the non-delivery of products purchased through an Internet auction site. Investors are enticed to invest in this fraudulent scheme by the promises of abnormally high profits.

25. Cyber Terrorism:
Targeted attacks on military installations, power plants, air traffic control, banks, trail traffic control, telecommunication networks are the most likely targets. Others like police, medical, fire and rescue systems etc.

How to prevent cybercrime

While it may not be possible to completely eradicate cybercrime and ensure complete internet security, businesses can reduce their exposure to it by maintaining an effective cybersecurity strategy using a defense-in-depth approach to securing systems, networks and data.

Some steps for resisting cybercrime include the following:

- develop clear policies and procedures for the business and employees;
- create cybersecurity incident response management plans to support these policies and procedures;
- outline the security measures that are in place about how to protect systems and corporate data;

- use two-factor authentication (2FA) apps or physical security keys;
- activate 2FA on every online account when possible;
- verbally verify the authenticity of requests to send money by talking to a financial manager;
- create intrusion detection system (IDS) rules that flag emails with extensions similar to company emails;
- carefully scrutinize all email requests for transfer of funds to determine if the requests are out of the ordinary;
- continually train employees on cybersecurity policies and procedures and what to do in the event of security breaches;
- keep websites, endpoint devices and systems current with all software release updates or patches; and
- back up data and information regularly to reduce the damage in case of a ransomware attack or data breach.