What is Cybercrime?

Cybercrime is any criminal activity that involves a computer, networked device or network. While most cybercrimes are carried out to generate profit for the cybercriminals, some cybercrimes are carried out against computers or devices directly to damage or disable them. 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 accounts, credit cards or other payment card information.

Who are Cybercriminals?

A cybercriminal is a person who uses his skills in technology to do malicious acts and illegal activities. They can be individuals or teams. Cybercriminals are widely available in what is called the “Dark Web” where they mostly provide their illegal services or products.

Different types of Cybercrimes

The various cybercrimes are discussed below:

a) ***Hacking:*** Computer hacking is the practice of modifying computer hardware and software. Hacking generally refers to unauthorized entry into a computer or a network. A hacker is a person who breaks passwords to gain unauthorized entry to computer systems.

b) **E-mail bombing:** A mail bombing is sending a massive amount of emails to a specific person or system. In this case, a cybercriminal sends a huge amount of mail to someone which may simply fill up the recipient's disk space on the server and may cause the server to stop functioning.

c) **Salami attack:** A “salami attack” is used to commit financial crimes. Criminals steal money or resources a bit at a time from financial accounts on a system.

d) **Cyberbullying:** It is a form of harassment through electronic devices such as computers, mobile phones, laptops, etc. The act of making untrue statements about another which damages his/her reputation

e) **Web jacking:** The process of gaining access and control over the website of another. The information may be manipulated or changed on the website.

f) **Denial-of-service attack:** It is an attempt to make a computer or network resource unavailable to its intended users. The computer is flooded with more requests than it can handle which causes it to crash.

g) **Phishing:** Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details.

How to protect against Cybercrime

Some of the precautionary measures to protect against cybercrimes are discussed below:

a) Keep software and operating system updated: Keeping your software and operating system up to date ensures that you benefit from the latest security patches to protect your computer.

b) Use anti-virus software and keep it updated: Using anti-virus or a comprehensive internet security solution like Kaspersky, AVG and McCafe, total security is a smart way to protect your system from attacks. Anti-virus software allows you to scan, detect and remove threats before they become a problem. Having this protection in place helps to protect your computer and your data from cybercrime, giving you peace of mind. Keep your antivirus updated to receive the best level of protection.

c) **Use strong passwords:** Be sure to use strong passwords that people will not guess and do not record anywhere.

d) **Never open attachments in spam emails:** A classic way that computers get infected by malware attacks and other forms of cybercrime is via email attachments in spam emails. Never open an attachment from a sender you do not know.

e) **Do not click on links in spam emails or untrusted websites:** Another way people become victims of cybercrime is by clicking on links in spam emails or other messages, or unfamiliar websites. Avoid doing this to stay safe online.

f) **Do not give out personal information unless secure:** Never give out personal data over the phone or via email unless you are completely sure the line or email is secure.

g) **Keep an eye on your bank statements:** Spotting that you have become a victim of cybercrime quickly is important. Keep an eye on your bank statements and query any unfamiliar transactions with the bank. The bank can investigate whether they are fraudulent.

References:

1. https://www.techtarget.com/searchsecurity/definition/cybercrime
2. https://www.kaspersky.com/resource-center/threats/what-is-cybercrime
3. https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention

---

Dr. B T Sampath Kumar

Professor, Dept. of Library and Information Science

Tumkur University, Tumakuru, Karnataka, INDIA

www.sampathkumar.info