# Cyber Crime and Cyber Security

## What is cybercrime

Cybercrime refers to any criminal activity accomplished through using a network, technological devices, and the internet. Common motives behind committing cybercrimes include monetary gains, personal gains, and creating chaos within an organization or an individual's life.

## What are the common types of cyber-attacks

### Cyber theft

Cyber theft is a type of cybercrime that involves an individual stealing money, personal information, financial data, or intellectual property through infiltrating another person or company's system. Fraudulent crimes such as identity theft and embezzlement can also fall under the cyber theft crimes umbrella.

### Cyberbullying

Cyberbullying refers to instances of bullying an individual online. Acts of cyberbullying include any threat to a person's safety, coercing a person to say or perform an action, and displays of hate or bias towards someone or a group of people.

While children tend to fall victim to cyberbullying more often, adults are not necessarily immune. According to a study, 40% of teenagers surveyed stated they had faced online harassment, and 24% of adults between ages 26–35 reported having experienced cyberbullying.

### Malware

Malware is a word used to refer to any program or software designed to infiltrate or damage a device. Viruses are an example of programs that fall under the malware umbrella. Viruses perform a variety of harmful actions once they land in a device. They may destroy files, log your keystrokes, reformat your hard drive, or manipulate your files.

### Phishing

Phishing occurs when cybercriminals pose as an organization to trick victims into sharing their sensitive information. Oftentimes, cybercriminals successfully achieve their phishing goals by using scare tactics such as informing the victim that their bank account or personal device is under attack.

### Cyber extortion

Cyber extortion is a form of online blackmailing. In these cases, cybercriminals attack or threaten to attack the victim and demand some form of compensation or response to stop their threats.

### Ransomware

Ransomware is a type of cyber extortion which uses malware to reach its end goal. This malware threatens to publish the victim's data or prevent the victim from accessing her data until the cybercriminal receives a specified amount of money.

### Cryptojacking

Crypto jacking refers to when hackers use other people's computing power to mine cryptocurrencies without consent. Cryptojacking differs from cybercrimes that use malware to infect a device since cryptojackers do not wish to pursue a victim's data. Instead, cryptojackers use the processing power of their victim's device.

Despite seeming less harmless than other cybercrimes, individuals should not take cryptojacking lightly because falling victim to it can significantly slow one's device and make it vulnerable to other cyber attacks.

**Cyber spying**

When hackers attack the network of a public or private entity to access classified data, sensitive information, or intellectual properties, they commit cyber spying. Cybercriminals may use the classified data they find for other ends, such as blackmail, extortion, public humiliation of an individual or organization, and monetary gains.

**Spyware**

Spyware refers to software that cybercriminals use to monitor their victim's activities and record their personal information. Often, a victim accidentally downloads spyware onto their device, which is how they unknowingly provide access to their data to a cybercriminal. Depending on the type of spyware used, cybercriminals can access a victim's credit card numbers, passwords, web cam, and microphone.

**Adware**

Adware is the software you may accidentally install onto your computer while downloading another application. Developers of adware programs gain monetary benefits from their activities on people's computers every time someone views or clicks on an advertisement window.

While some adware programs are legal and harmless, others are intrusive because of the type and frequency of the advertisements they show. Some adware programs are illegal in many countries because they carry spyware, viruses, and other malicious software.

**Botnets**

Botnets are networks of malware-infected computers. Cybercriminals infect and take control of these computers to perform tasks online without the user's permission to carry out fraudulent acts without being tracked. Their actions may include sending spam emails and carrying out targeted breaches into a company's assets, financial data, research data, and other valuable information.

**Romance scams**

Some cybercriminals use dating sites, chat rooms, and dating applications to masquerade as potential partners and seduce people to gain access to their data.

**Hacking**

Hacking commonly refers to any unauthorized access to a computer system. When a hacker breaks into the computers and networks of any company or individual without permission, they can gain access to sensitive business information or personal and private data without authorization.

Nonetheless, not all hackers are criminals. Some hackers often called "white hat" hackers, are hired by software companies to find flaws and holes in their security systems. These hackers hack their way through a company's network to find existing flaws in their client's system and offer them solutions to those flaws.

Sometimes, cybercriminals or "black hat" hackers might want to go clean and turn away from crime. In these cases, working as a security consultant for the companies they used to torment is one of the best options. These have more knowledge and experience about the infiltration of networks than most computer security professionals.

**Cyber security solutions**

What does cyber security mean?

Cyber security, sometimes referred to as IT security or computer security, is the body of technologies and processes designed to protect computer systems, networks, and devices from the dangers of cybercrimes. Moreover, cyber security solutions prevent damage to hardware, software, electronic data, or any disruption or misdirection of the services they provide.

The importance of cyber security solutions stems from their ability to provide comprehensive protection to users. If you wish to keep your networks and devices safe from unauthorized access or malicious attacks, then consider the different types of cyber security to determine the best one for your needs.

1. **Antivirus**

The first step in securing your device(s) is installing proper antivirus software on them.

Antivirus programs scan data and incoming files to detect unsafe software and remove any threats before they cause an issue. These programs identify and eliminate known viruses, worms, and malware based on what is available in their extensive database.

2. **Internet security**

Internet security programs establish measures against attacks over the internet to ensure the security of devices and networks. These programs prevent attacks targeted at browsers, networks, operating systems, and other applications.

Internet security software uses many methods to protect the transfer of data, including encryption and from-the-ground-up engineering. The most common and significant ones include firewalls, access controls, data loss prevention (DLP), distributed denial-of-service prevention, and email security.

3. **Firewall**

Firewalls act as filters that allow or deny access to a network, thus protecting the devices connected to it. Firewalls keep harmful files away and prevent malicious codes from being embedded into networks. Apart from that, they also screen and block dangerous traffic.

Moreover, firewalls create checkpoints between an internal private network and the public internet. They limit network exposure by hiding your private network system and information from the public internet.

4. **Endpoint security**

Endpoint security refers to a software approach for ensuring that all the endpoint devices, such as computers, tablets, scanners, and others, connected to a network remain safe. Such devices serve as access points to an enterprise network since they offer attack paths and points of entry that malicious files can exploit. Therefore, endpoint security aims to secure every endpoint to avoid potential threats.

Moreover, network administrators can use endpoint security solutions to restrict the use of sensitive data and access to certain websites to maintain compliance with the policies and standards of the organization.

These features make endpoint security solutions particularly well-suited for small and large organizations.