**Cybercrimes**

**Cybercrime** is commonly called a computer-oriented criminal activity that either uses or targets a network, computer system, or network device. Most cybercriminals commit cybercrimes to make money by targeting individuals. However, some professional cybercriminals can threaten an organization by damaging or disabling the entire network.

Apart from this, the cybercriminal can also use computers or networks to transfer viruses, malware, pornographic content, illegal information, etc. These activities are usually done to damage computers and their data, for reasons other than just a profit.

Usually, a primary **motive of cybercriminals** is to generate profit for them. To do this, cybercriminals may commit a variety of profit-driven criminal activities, such as stealing and reselling identities, getting access to financial accounts, misusing credit card to get money or goods, performing email frauds, trafficking in pornography or intellectual property, accessing government data for theft and resale, etc. To be specific, cybercrime can range from security breaches to identity theft.

**Cybercrime** is a type of crime that involves a computer and a network to carry out illegal activities through digital means. This can be done by individuals or small groups of people with little technical knowledge, or by highly organized global criminal groups with relatively skilled developers and professionals.

Skilled cybercriminals use advanced tools and techniques to hide their identity and location. Additionally, some cybercriminal conducts cybercrime from countries where there are weak or no cybercrime laws. This helps in reducing the chances of detection and prosecution of cybercriminals.

**The impact of cybercrime** can be mostly seen on individuals. There can be issues like data breaches, identity theft, or trafficking to malicious sites, etc. with the devices.

Businesses may suffer from sensitive data loss, financial loss, or brand damage, etc. It can directly affect the value of a company, the share price, and can also cause loss of reputation, customers, etc.

Cybercriminals use advanced tools and technologies to gain access to the government's highly sensitive data. The main purpose of targeting government data is to damage data or sell national security and defense data.

Cybercrimes can be divided into the following three categories:

Crime against Individual

This category of cybercrime usually involves one person that might be distributing malicious software or suspicious information online. Apart from this, crimes against individuals might include identity theft, cyber harassment, stalking, spoofing, distribution of child pornography, credit card fraud, etc.

Crime against Property

This category of cybercrime includes crimes that occur against property, such as a computer or a network. Cybercriminals might steal a person's bank or credit card details, gain access to funds, make online purchases, or perform phishing attacks to retrieve a person's information, etc. These crimes usually include hacking, DDoS attacks, virus distribution, copyright infringement, etc.

Crime against Government

This category of cybercrime includes crimes that occur against the government. These crimes are the most serious offense. It is also referred to as Cyber Terrorism. Typically, these crimes are committed by the terrorists or by the governments of enemy nations. These crimes include accessing confidential information, hacking, cyber warfare, pirated software, etc.

## Types of Cybercrime

There are various types of cybercrime, but all such types of cybercrime fall into the following three situations:

**•** Crime in which the computer acts as a weapon
**•** Crime in which computer is an accessory to a crime
**•** Crime in which the computing device is the target

**Phishing**

A phishing attack involves attackers sending several spam mails having malicious attachments or links. Once a receiver clicks on a link, he/she may be redirected to a malicious site asking the receiver to respond with confidential details, such as login credentials, billing information, etc. This type of attack may also take place through text messages, websites, or even social media platforms.

**Hacking**

Hacking is a type of cybercrime act where an intruder gets access to a few or complete functions within a system without your permission. **Hackers (people who perform hacking)** are tending to be computer programmers and they have an advanced understanding of computers. However, they misuse this knowledge for performing illegal activities, such as accessing corporate and government accounts, and stealing their financial data or other important information.

**Computer Viruses**

A computer virus is one of the most destructive types of attacks where cybercriminals gain unauthorized access to the system and steal personal information and other important data. Mostly, computer viruses are attached to infected software that spreads across other installed software. Viruses can come to your system through removable devices and the internet. Without proper scanning and removing them from your system, the next time you start your system, the viruses will run all over again.

**Ransomware**

Ransomware is one of the most popular types of malware-based attacks. It enters through a computer network on a local machine and encrypts files using public-key encryption. That means you cannot access encrypted files and the information stored in them. The cybercriminal will then ask for ransom (money) to unlock the files and give your data back.

**DDoS Attacks**

The **DDoS (Distributed Denial of Service)** attack is a blatant attempt by cybercriminals to take down a system or network temporarily or completely. This overwhelms a system with multiple connections requests that it cannot handle. Additionally, there may be spam traffic coming from various sources. This eventually leads to server overload. DDoS attacks are used as a distraction technique to allow cybercriminals to hack into the system meanwhile.

**Botnets**

Botnets are networks from comprised computers that are controlled externally by remote attackers, known as ‘**Bot Herders**'. The attackers target other computers and send spams or malware by using these botnets. This type of cybercrime is usually performed against businesses and governments because botnets mainly target the entire IT infrastructure.

**Cyberstalking**

This type of cybercrime involves a person being followed by the cybercriminal online. The stalker will follow the target person virtually, including all the activities. Then, the stalker might harass the victim by using social media platforms, mails, or websites, etc. Cyberstalkers first try to know their victims as much as possible and then make them feel afraid or concerned regarding their safety. In most cases, this type of cybercrime is committed against women and children by individual men and pedophiles.

**Identity Theft**

Identity theft is a specific type of cybercrime in which attackers gain access to the victim's personal information, including passwords, financial accounts, credit cards, and other confidential information. In most cases, cybercriminals use these details to steal money from your accounts, without your knowledge. Additionally, cybercriminals may use your details to commit a crime or claim government benefits, making others think it was you.

**PUPs**

PUPs is an acronym for '**Potentially Unwanted Programs**'. These are not considered much threatening as compared to other types of cybercrime. These are nothing but a type of malware program that uninstalls important software from your computer system automatically. In addition, PUPs can also remove or change your default search engines within the browsers. They can involve adware and spyware; therefore, it’s a good practice to make use of an antivirus program to prevent any malicious download.

**Social Engineering**

This type of cybercrime involves criminals making direct contact with the victim through phone, emails, or even in person. Cybercriminals first try to earn trust and then they steal confidential information like passwords, financial accounts data, etc. In most cases, cybercriminals act like a customer service agent of any legitimate company and ask for the important information. Once they get the desired information, they might sell your information or try to steal money from your accounts.

**Online Scams/Frauds**

These are crimes that involve spam advertisements or emails offering large rewards or high amounts of money. These offers are presented in such a way that they look very real. Once users click on these malicious advertisements or links, the malware reaches their system and compromises the information.

**Exploit Kits**

Exploit kits are readymade tools designed by advanced programmers. These tools include vulnerability (bug in codes of the program) that helps gain access to a victim's computer once deployed. Cybercriminals can purchase exploit kits online and use them against different users. The exploit kits receive frequent upgrades just like the other software. These kits are usually purchased via dark web hacking forums.

**Prohibited/Illegal Content**

This is a specific type of cybercrime that includes the sharing of offensive and inappropriate content over virtual platforms. Cybercriminals distribute offensive materials to make people feel hatred against other people, religions, or countries, etc. Offensive content can include but is not limited to, videos of criminal activities, sexual activities between adults, videos with intense violence, etc. Additionally, it can also contain illegal contents like terrorism supported materials or child exploitation materials.

**Spamming**

This cybercrime involves criminals using electronic messaging systems to send messages to users. These messages usually consist of malware, fake links of websites, and other malicious software. Email spamming is one of the common spamming methods in which bulk messages are sent to large numbers of users. These messages include deals, and promos from trusted companies to attract users to click on the attachments or the fake links.

**Malvertising**

Malvertising involves criminals filling websites with several advertisements containing malicious codes or links. Once users click on these advertisements, they will be redirected to fake websites that look like trusted ones. Users will submit the personal details, thinking they are legitimate. This information will further reach to the attackers. Furthermore, the websites can automatically start downloading files containing viruses and other malware.

**Software Piracy**

There are many websites that reproduce original content such as songs, movies, books, games, and other software. It falls under the Cybercrime Act as it translates to copyright infringement. Software piracy greatly affects companies and developers as duplicate products lead to huge reductions in their total income.

**Cyberbullying**

Cyberbullying is one of the biggest crimes occurring in the virtual world. It is a form of bullying on the Internet. However, global leaders are aware of this crime and pass laws and enactments that prevent the spread of cyber-attack.

## How to Fight Cybercrime

At present, almost all the devices (such as smartphones, tablets, and computers) are connected to the internet. Cybercriminals may use a device to gain access to personal information, business information, confidential government information, etc. Therefore, it is necessary to have knowledge about preventive measures that can be taken to fight against cybercrime.

The following are some tips that will help you protect your computer and your personal data:

**•** Make use of Anti-virus software and keep it updated.
**•** Keep the operating system and other installed software updated.
**•** Do not install software from untrusted sources.
**•**Be cautious while browsing the website.
**•** Make sure that websites are safe and genuine before you enter any credentials.
**•** Always use strong passwords with 14+ characters, including upper case, lower case, and numbers.
**•** Flag and report suspicious emails and do not open any attachments.
**•** Do not click on any unfamiliar links or ads.
**•** Do not share suspicious information via digital means unless you are completely sure that it is safe.
**•** Use a VPN service whenever possible.
**•** Keep on tracking your bank statements and other financial accounts.

## Conclusion

There can be various ways and types of cybercrime that attackers can use. The only way to protect yourself is to educate yourself about various types of cybercrime and how you can prevent them. Once you are a victim of cybercrime, there is no easy way to get rid of it.

*Taken from https://www.tutorialsmate.com/*