**What is Cybercrime ?**

* Cybercrime, also called cybercrime, is the use of computers as a tool to achieve illegal goals, such as committing fraud, trafficking in child pornography and intellectual property, identity theft or invasion of privacy.
* Crimes against computers or crimes committed using computers.
* These are illegal, immoral and unauthorised acts that involve the misuse or alteration of data obtained through computer technology.

**Cybercriminal techniques :**

A cracker often uses various specific techniques and procedures to successfully achieve his goals, which are referred to as cyber attack. Some of the most well-known methods of hacking method include:

* Brute force
* Sniffing
* Backdoor
* Keylogger
* Hoax
* Phishing
* Pharming

**Brute Force :**

* Brute force, or brute attack, is a specific type of primitive (but sometimes still effective cybercriminal technique, as some users choose very trivial passwords) attack implemented by a password cracker that should be part of the repertoire of at least every somewhat skilled hacker or cracker.
* In practice, brute force is often an attempt to guess the user and their password without any knowledge of the underlying encryption key (the letters, numbers and symbols used).
* An attacker who breaks a password in this way often attempts to illegally steal money or personal data from a system, email or bank account.

**Sniffing :**

* Sniffing (sniff is the English translation of sniff, sniff or ventilate) is a specific technique that allows eavesdropping on computers on a local network (storing and then reading TCP packets), which is used, for example, in network diagnostics.
* But in the hands of a cracker, sniffing can make sense to obtain passwords in use or to covertly monitor the flow of relevant data communication and traffic of the entire network, generating useful information that can be taken into account when deploying a botnet, network worm or DDoS.
* A Trojan horse is also often used as an aid in sniffing, as it may have built-in functionality that is appropriately tailored to the sniffing technique.

**BackDoor :**

* Backdoor is a term for a malicious type of code that makes it very easy for a cracker to take control of a computer so infected without the owner knowing.
* In the worst case scenario, the infected computer then becomes another of the many zombie PCs in the botnet, where it can then serve as a pernicious tool of destruction for DDoS or sending spam or hoaxes.
* Typically a backdoor is created by a Trojan, but also by some other types of malware. Specifically, certain types of worms. But backdoors can also be a bug in the program code, buffer overflows, etc.

**Keylogger :**

* A keylogger is a program that carefully detects and stores all keystrokes on a user's PC. Everything the user types on the keyboard is clearly recorded by the keylogger, most commonly in a text file.
* And in the far worse situation, the keylogger (in which case it is malware) silently saves itself as an unsuspecting user's computer and behaves like a specific form of spyware.
* Trojan Horse is one fine example of a secret carrier of this insidious software keylogger.
* Definitely a good quality antispyware program that can detect the keylogger and then eliminate it

**Hoax :**

* A hoax is the name given to a hoax and false message (most often in the form of an email) that warns of a non-existent danger or solves some supposed problem. Hoaxes in a way can fall under malicious programs that use the label malware.
* A typical characteristic of a hoax is that it contains an invitation to spread it further to other users in the Internet world, which is most often done using a mail client to create a so-called chain e-mail.
* Perhaps the worst thing about hoaxes is that ordinary users can easily believe such messages in uncritical faith, which then has its impact on the psychological side (e.g. distrust of a certain product, etc.).

**Phishing :**

* Phishing (from the English fishing = fishing, the Czech equivalent sounds like rhybaření) is a highly dangerous cybercriminal technique of sending fraudulent emails to extort sensitive personal information (e.g. login details, credit card numbers, PINs, etc.) from the recipient of such an email.
* These emails are often sent out by the spammer and the cracker at the same time in the form of spam by one person. Phishing as a form of cyber-attack was born in the background of the warez scene.
* According to expert studies, up to around 5% of all possible users contacted are caught up in this type of cybercrime every year. Phishing first reached the Czech Republic in 2006, targeting CitiBank.

**Pharming :**

* Pharming (can be translated as farming) is a cybercriminal and professional fraud technique that uses the Internet to obtain important personal information to further the illegal activities of the attacker (cracker).
* Pharming is a slightly younger sibling of another widely used illegal cracking technique, phishing, or phishing in Czech.
* Among the most famous worldwide cases of pharming are the redirection of servers such as eBay or weather.com to fake sites, where spyware then tried to infiltrate the operating system

**Specific cases of cybercrime**

* Cyberbullying
* Cyberbullying
* Cyberstalking
* Warez

**Cybergrooming :**

- Cybergrooming(also known by the terms child grooming or cyber grooming) is a specific and very serious case of cybercrime in which a person tries to pose as a trustworthy person on the Internet and coerce minors into meeting for the purpose of physically abusing or assaulting them.

- One of the typical features of Cybergroomingis that the abuser pretends to be someone else, e.g. for a 12-year-old girl, he may take the role of a girl of the same age or impersonate an 18-year-old boy, who may even be more impressive to the girl, when in reality he may be a 40-year-old man.

**Cyberbullying :**

* Cyberbullying is a specific type of bullying that is perpetrated by a perpetrator against his or her unfortunate victim using modern electronic technologies (e.g., emails, cell phones, social networking sites, webcams, or chat services), across cyberspace.
* Cyberbullying is considered as a cybercriminal act, which is established as a serious federal crime in the USA, for example, and many other countries are thus gradually adjusting their laws and security measures to consistently eliminate this cybercriminal phenomenon.
* The typical manifestation of cyberbullying is that the perpetrator consistently harasses, humiliates, blackmails and insults his victim. Cyberbullying is thus complementary to cyberbullying, which, precisely in its later stages, exploits these typical manifestations.

**CyberStalking :**

* Cyberstalking or also cyber stalking is one of the very dangerous cybercrimes within cyberspace. A person who engages in this specific type of stalking (from the English translation: hunting, hunting, stalking) is technically called a cyberstalker.
* Perpetrators who try to literally piss off their victims in their cyberspace rampage are often lonely and confused desperate individuals.
* Paranoia or schizophrenia as mental disorders present here are also no exception, but rather one of the main factors for cyberstalking to occur in the first place.

**Warez :**

* In the Czech Republic, warez downloading of copyrighted works for personal use is considered a legal act,
* Warez is a much-mentioned slang term for the illegal distribution of copyright works (games, apps, movies, music, etc.) in cyberspace, as it is most often distributed with the help of specific online communities (forums and torrents).
* People who associate in these groups are commonly known as computer pirates. Warez environments may have many advantages for some (e.g. the latest movies available for immediate download), but they are also often a very favourable climate for various dangerous computer viruses and especially Trojan horses, with which the cracker deliberately infects illegally distributed software.
* In practice, this can look like a rootkit is installed from a downloaded application, which will mask the Trojan horse from the detecting antivirus, creating a backdoor in the warez user's operating system.

Translated with www.DeepL.com/Translator (free version)