# What is Cybercrime

* The dynamic development of information technology brings with it new socially harmful actions, which is why cybercrime is receiving increasing attention.
* The term cybercrime is derived from the term cyberspace, or cyberspace for short.
* Cyberspace is a virtual environment that has no beginning and no end, knows no national boundaries and cannot be determined how large it is.
* Cybercrime, formerly also referred to as information crime, is defined by the Police of the Czech Republic as criminal activity that is committed in the environment of information and communication technologies, including computer networks.
* The information and communication technology area itself is either the subject of the attack or the crime is committed with significant use of information and communication technology as a significant means of perpetration.

# Different types of cybercrime

## Fraudulent acts

1. The most frequent documented act is the offence of Fraud under Section 209 of the Criminal Code, where it is not uncommon to have a concurrence with Unauthorised Access to a Computer System and Information Carrier under Section 230 of the Criminal Code.
2. These offences include fraudulent e-shops, which are created under the pretext of extorting funds and after a short existence such e-shop ceases to exist. At the same time, the funds are usually exported outside the territory of our country in order to anonymise the financial flows, or virtual currencies are used.
3. A similar process is followed in the context of fraudulent advertisements (sale of cars, electronics, live animals or even renting out flats), collections and, last but not least, the practice known as 'Nigerian fraud'.
4. Fraud by means of spoofed emails or theft of money from bank accounts by phishing can also be included.

## Hacking

1. Unauthorised access to a computer system and information carrier under section 230 of the Penal Code is a criminal offence that is applicable to most of the acts referred to as hacking, data breaches, system disruption and, last but not least, misuse of equipment.
2. The most typical example that is investigated is the behaviour of an offender who overcomes the security of a computer system and gains access to the victim's data, which he can then freely dispose of.
3. These actions include, but are not limited to, the distribution of malicious codes, the implementation of so-called backdoors in freely available software, etc. An increasingly common form is the hacking of email accounts, social networking accounts, internet banking accounts, which results in the invasion of privacy, obtaining sensitive information with the possibility of damaging or destroying it or gaining financial gain.
4. Other related crimes (extortion, dangerous stalking, theft from accounts, fraud) are also linked to this.
5. Cyber-attacks (e.g. DDoS) or extortion through ransomware are also part of this type of crime.
6. Another form may be the violation of the secrecy of the messages transmitted according to Section 182 of the Criminal Code, the most common manifestation of which is referred to as sniffing, where the perpetrator intercepts ongoing communications in the network and thus obtains sensitive data not only about the traffic but also the content. This is often done on unsecured wi-fi connections, on the side of manipulated email servers and, more recently, by attacking home routers.
7. Perpetrators then gain access to sensitive data such as passwords, payment details or sensitive personal or intimate content, which they then use to pressure the victim in an attempt to enrich themselves financially or at least damage the victim's reputation.

## Blagging

1. A large number of different scams are spread via the Internet, which, among other things, use social engineering. Not only individuals but also commercial companies are at risk.
2. One of the many types of fraud on the Internet that uses social engineering is the so-called CEO - Command Executive Order - a fictitious order from an authorised person to carry out an action, in this case a payment to an account.
3. These types of scams are in most cases created based on a very good knowledge of the market, structure and customers of the company in question.
4. The information obtained is often used to make a convincing argument to make it easier for victims to be manipulated into carrying out the desired activities

## Vice offences

1. In such cases, children under the age of 18 are contacted in an attempt to obtain intimate photographs or videos of them or to lure them to a personal meeting.
2. The most common environments for contact are chat rooms, social networks and online games.
3. The material obtained in this way is then distributed or exchanged in closed discussion forums, in particular on Onion, by email messages or P2P networks.
4. This group also includes offences against minors, such as pimping, sexual coercion, trafficking, etc..

## Offences against copyright

1. Infringement of copyright, rights related to copyright and database rights under Section 270 of the Criminal Code consists in particular in the sharing of music, films and software in violation of copyright distributed on web-based mass storage or P2P networks.

## Violent speech and hate crime

1. This category includes crimes such as extortion under Section 175 of the Criminal Code, Dangerous threats under Section 353 of the Criminal Code, Dangerous stalking (also known as stalking) under Section 354 of the Criminal Code, and spreading of alarm messages under Section 357 of the Criminal Code, all of which take on a higher degree of anonymity when using information technology.
2. For this purpose, anonymizing servers or services are used, e.g. proxy servers, tor network, VPN, etc.
3. This includes extremist speeches of the nature of the offence of Defamation of a nation, race, ethnic or other group of persons under Section 355 of the Criminal Code, Incitement to hatred against a group of persons or to restriction of their rights and freedoms under Section 356 of the Criminal Code, etc.
4. On foreign servers, websites are created with extreme right-wing or left-wing themes that incite hatred, discrimination or even call for violence against minority groups or political groups.
5. Another manifestation is fictitious profiles on social networks and discussions on various articles in the media.

# How to defend against cyber attacks?

* What the user, and the company in general, can make of itself is to acquire security software.
* Next, frequent backups of data in case it needs to be restored. An integral part of protecting against attacks is, in the case of companies, thorough and ongoing training of employees on the topic of cyber security, because the most risky factor in the entire chain is usually the user.
* Unfortunately, however, it also happens that all remedial measures fail because attacks are constantly improving. And then, of course, there is also the risk of human failure.

## Keep your software and systems fully up to date

* Often cyber attacks happen because your systems or software aren’t fully up to date, leaving weaknesses.

## Ensure Endpoint Protection

* Endpoint protection protects networks that are remotely bridged to devices.
* Mobile devices, tablets and laptops that are  
  connected to corporate networks give access paths to security threats.
* These paths need protected with specific endpoint

## Install a Firewall

* There are so many different types of sophisticated data breaches and new ones surface every day and even make comebacks.

## Backup your data

* In the event of a disaster (often a cyber attack) you must have your data backed up to avoid serious downtime, loss of
* data and serious financial loss.

## Control access to your systems

* Believe it or not, one of the attacks that you can receive on your systems can be physical, having control over who can
* access your network is really really important.

## Wifi Security

* Who doesn’t have a wifi enabled device in 2020? And that’s exactly the danger, any device can get infected by connecting
* to a network, if this infected device then connects to your business network your entire system is at serious risk.

## Passwords

* Having the same password setup for everything can be dangerous. Once a hacker figures out your password, they now have
* access to everything in your system and any application you use.