

Network security

Basic vocabulary

Malware = malicious software, a term which refers to intrusive programs designed to exploit devices at the expense of the user and to the benefit of the attacker

Examples:

- spyware = various programs designed to secretly record and report a person's activities on the Internet
- ransomware = malicious software that encrypts your computer's data and provides the password to the user for money (ransom fee)
- Trojan horse = malware that disguises itself as legitimate software to trick you into executing malicious software on your computer. Because it looks trustworthy, users download it, and thus allow malware onto their device
- worms = programs that replicate themselves many times and thus slow down or stop operations of computers in the network. They may also carry viruses.
- viruses = programs that migrate through networks and OSs and may alter or delete files in them
- keyloggers = programs recording every stroke made on a keyboard of a computer

Ransomware = is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.

Cyberbullying is bullying that takes place over digital devices. It can occur through SMS, or online in social media and forums where people can participate or share content. It can include sharing personal/private information about someone else causing embarrassment or humiliation. It can be persistent (24/7), so it can be difficult for the victims to find relief, and permanent (unless reported and removed); its public character may earn both the attacker and the victim a negative online reputation and it can impact college admissions, employment or other areas of life.

Cyberstalking is the use of electronic means to stalk (follow and watch someone over a long period of time in an annoying or threatening way) or harass an individual, group, or organization. It may include false accusations, monitoring, identity theft, threats, vandalism, or gathering information that may be used to threaten, embarrass or harass.

Wiretapping = *eavesdropping* (spying) on phone conversations or email exchanges

Data mining = the process of finding anomalies, patterns and correlations within large data sets to predict outcomes

Keylogger (keystroke logger) = a computer program that records every keystroke made by a computer user. These are used to quietly monitor your computer activity while you use your device as normal. Keyloggers are used for legitimate purposes like feedback for software development but can be misused by criminals to steal your data.

Phishing = a cybercrime in which a target is contacted by email, telephone or text message by someone posing a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords

Compiled by: Valéria Medárová, PhD.

Pharming = a cyberattack intended to redirect a website's traffic to a fake site in order to obtain personal information such as passwords, account numbers, etc.

DoS attack (denial of service) = attempt to slow down or stop a computer system or network by flooding it with requests for information and data – coming from a single computer issuing repeated requests

DDoS attack (distributed denial of service) – like DoS but with coordination of several computers making repeated requests

Identity theft = illegal assumption of someone's identity for the purpose of economic gain (profit)

Internet scam = fraud using the Internet, e. g. auction fraud (deceptive presentation of products, inflated prices, not delivering products after payment), fake apps, fake money-collection for a charity, a "Nigerian scam" (an e-mail from a fake millionaire who asks you to provide your bank account information to help him safely store his money), a romance scam (a scammer pretends to be in relationship with you and asks for financial help or personal data)

Zombies = computers infected by a virus or worm that are remotely controlled, often arranged in a network called *botnet*

Rogue Wi-Fi spots = Wi-Fi networks that imitate official free public Wi-Fi networks and try to capture information that users send to websites

.....
Cookies are packets of data on a computer that store information about a user's activity on a website.

- Session cookies – short-term storage of data on the user of the website (only while you are using it), e. g. a shopping cart in an online shop
- First-party persistent cookies - collect remember analytic browsing options such as language used. They provide a better user experience, e. g. remembering you login data for a website
- Third-party persistent cookies (tracking cookies) – potentially harmful. They are accessed by third party organizations – that did not create them. They track the user on the internet without his/her knowledge. They are used mostly for advertising – to offer products and services to targeted customers

.....
Software and technologies to protect your system from cyber attackers:

A) **Firewall** = software designed to create a barrier between your information and the outside world. It prevents unauthorized access to your network and alert you to any intrusion attempts.

B) **Antivirus** = protects your computer against unauthorized code or software that may threaten your OS. It is important to run or schedule regular virus scans to keep the computer virus-free.

C) **Anti-spyware** = concentrates on detecting software that secretly monitors and collects personal information. Some spyware records every keystroke to gain access to passwords and other financial information.

D) **Password managers** – help create strong passwords

E) **Encryption** = the process of coding information to make it unreadable to other users/attackers. We use: e-mail encryption, file encryption, website encryption

F) **Biometric authentication** = security processes that verify user's identity through unique biological traits, such as retina, irises, voices, facial characteristics, fingerprints, hand geometry recognition