Glossary of basic terms

Short explanation of the most common terms that may appear in connection with IT security at Charles University.

A

Antivirus - a program that protects devices from malicious software (viruses, spyware). Checks the system regularly and blocks suspicious files.

Authentication – verification of your identity when logging into the system (e.g. entering a password, confirmation in the application).

B

Backup – storing a copy of data (e.g. on a university disk or cloud) so that it can be recovered when the device is lost or attacked.

Brute force attack – an attempt to crack a password by trying all possible combinations.

D

Digital identity - a set of data that uniquely identifies you in the online world - such as your university account.

Data **(personal / university)** – all electronic information (files, documents, emails) that may contain sensitive data and must be protected.

Data leaks – situations where sensitive information reaches an unauthorized person. It can occur by mistake or by attack.

Domain reputations – trustworthiness of a web address; sites with suspicious content may be blocked by security software.

E

Encryption - a process that converts data into an unreadable form until it is unlocked with the correct key.

F

Firewall – a “protective gateway” between your device and the internet. Monitors and filters network traffic, blocks unsafe connections.

Fake login a website that pretends to be an official website (e.g. CAS CU) but tries to lure out your password.

H

Hoax – an alarm or false message that spreads over the Internet (e.g. a false warning, an invitation to forward an email).

I

Incident - any event that may compromise the security of the system or data - e.g. a breached password, a lost laptop or a phishing attack.

M

Malware – malicious software that can damage a system or steal data. This includes viruses, spyware and ransomware.

P

Phishing – a fraudulent message (e-mail, SMS, chat) that tries to get your data or make you click on a dangerous link.

PIN / biometrics – means of device security (number, fingerprint, facial recognition).

Patch (update) – software add-on that fixes bugs or vulnerabilities in the system.

Password – your key account protection. It should be strong (min. 12 characters, combination of letters, numbers and symbols) and unique.

R

Ransomware – a malicious program that encrypts your files and demands a ransom for their recovery.

S

Social engineering – manipulating people to gain their trust and thus access to sensitive data.

Spam – unsolicited emails, often with advertisement, links to malicious sites or scams.

Spear phishing – an attacker targets a specific person (e.g. a university employee) and adapts the message to appear trustworthy.

Spyware – a program that secretly tracks what you do on your computer and sends this data to attackers.

T

Two-factor authentication (2FA) - a method of logging in when, in addition to your password, you confirm your identity with a second factor - e.g. a mobile application.

Trojan horse - a program that appears to be useful, but after installation allows an attacker to access the system.

V

VPN **(Virtual Private Network)** – an encrypted connection that protects data transmission when working remotely or from public networks.

Virus – a program that spreads itself and damages files or systems.

Vishing/smishing – phishing by phone (vishing) or by SMS (smishing).

Vulnerability – a bug in the software that can be exploited by attackers.