

KYBERBEZPEČNOST

Hesla

- Min. **12 znaků**, každá služba **jiné heslo - frázová hesla** – (např. „Nový epochální výlet pana Broučka, tentokrát do XV. století, tedy heslo bude vypadat takto: NevpB,td15.s“).
- Používej **správce hesel** (KeePass).
- Využívat **dvoufaktorové ověřování** (např. **Biometrie + PIN**).

Mobil & PC

- Vždy **zamykat zařízení**.
- Seřazení metod uzamykání **od nejslabších po silnější**: gesto, poté PIN, heslo, otisk prstu, biometrie.
- Ideální je kombinace: **Biometrie + silný PIN; otisk prstu + PIN**.

E-mail & zprávy

- Neklikat na **podezřelé odkazy**.
- Neotevírat **nečekané přílohy**.
- Pozor na **časový nátlak a zastrasování**.

Podvody

- **Phishing** – falešné **e-mail**y (mají pravopisné chyby / domény například .ru namísto .cz).
 - **Vishing** – falešné **telefonáty** (nátlak na získání přihlašovacích údajů, financí apod.).
 - **Smishing** – falešné **SMS** (součástí bývá podvodný odkaz).
 - **Baiting** – nalezená **fleška** se škodlivým souborem.
 - **Sociální sítě** – riziko zneužití sdílených informací.
-  Když váháš → **neklekej, ověř jiným kanálem**.

Důvěryhodná komunikace

- **Elektronické podpisy**:
- **Prostý el. podpis** = naskenovaný podpis; na tabletu; SMS kód.
- **Zaručený el. podpis** - vzniká certifikátem (na kartě s čipem) zajišťuje autora a neměnnost dokumentu.
- **Zaručený el. podpis s kvalifikovaným certifikátem** - ověřená totožnost podepisujícího.
- **Kvalifikovaný el. podpis** - nejvyšší úroveň (karta s čipem + PIN; Občanský průkaz).

Soubory & aplikace

- **Makra** v dokumentech **nepovolovat** (Makra = program v dokumentu. Když je povolíš, můžeš pustit virus.).
- **Ransomware** = škodlivý program který zašifruje data, soubory, nebo celé systémy, aby k nim uživatelé ani administrátoři neměli přístup → vyžaduje **výkupné** za dešifrování.

Ochrana zařízení

- Aktualizovat zařízení → zlepšování funkcí i ochrany.
- **Firewall „hrad a hradby kolem“** podle pravidel kontroluje veškerou komunikaci se zařízením a rozhoduje, co pustí dovnitř a co ven, aby zůstalo v bezpečí.

- **Antivirový program** je jako **vnitřní stráž** na hradě, která neustále kontroluje, co se už dostalo dovnitř, a když najde vetřelce, podle své „knihovny hrozeb“ ho zastaví nebo odstraní – proto musí být stále aktualizovaný.
- **Zálohování** je jako mít kopii nejprecennějších věcí z hradu **uloženou na bezpečném místě** mimo hrad – když hrad padne (např. kvůli viru nebo ransomwaru), o data nepřijedeme a můžeme je obnovit.

Stahování aplikací

- Aplikace stahuj pouze z **oficiálních obchodů** (Google Play, App Store).
- Neinstaluj aplikace z **neznámých odkazů nebo souborů**.
- Před instalací zkontroluj **oprávnění aplikace** – má odpovídat její funkci.
- Podezřelé jsou aplikace s **málo recenzemi nebo špatným hodnocením**.
- Na pracovních zařízeních **dodržuj pravidla IT oddělení**.

Internet & Wi-Fi

- Veřejná Wi-Fi = **riziko**.
- Citlivé věci (např. přihlašování) jen přes protokol **HTTPS** - komunikace mezi stránkou a naším webovým prohlížečem šifrovaná / **VPN (=virtuální privátní síť)** = šifrovaný tunel pro internetové připojení a vše, co v něm protéká.
- Koncové šifrování = odeslané zprávy dokáže číst jen jejich odesílatel a příjemce.

Zlaté pravidlo

Když něco působí divně, je to divné.

Raději se 2× zeptat než 1× litovat.

„nejslabší článek“ kybernetické bezpečnosti je nepoučený uživatel