



Kyberprevence – prevence rizikového chování online

Checklist

6 zásad bezpečného chování v online prostoru pro zaměstnance škol

1. zásada

Nakládání s hesly

- **Používejte silná hesla** – frázová hesla, min. 12 znaků, kombinace písmen, čísel a speciálních znaků.
- **Nikdy svá hesla nesdílejte** – ani s kolegy nebo rodinnými příslušníky a jinými osobami.
- **Dvoufaktorové ověřování (2FA)** – zapněte si ho všude, kde je to možné.

2. zásada

Bezpečná komunikace a ochrana soukromí

- **Zvažujte, co na sociálních sítích sdílíte** – jednou zveřejněné informace mohou být dostupné navždy.
- **Nikdy neposílejte osobní údaje neznámým lidem** – a to ani adresu, telefonní číslo nebo rodné číslo.
- **Pozor na podvodné e-maily** – neklikejte na podezřelé odkazy, neotvírejte neznámé přílohy.
- **Používejte soukromé chaty a šifrované komunikátory.**

3. zásada

Odpovědné chování na internetu

- **Respektujte pravidla netikety** – buďte slušní a ohleduplní k ostatním.
- **Nebuďte kyberhater** – nikomu nenadávejte, nikoho neponižujte ani nevydírejte.
- **Pokud jste obětí nebo svědkem kybernetického incidentu, nahlasejte to** – odpovědným pracovníkům a aktivujte bezpečnostní postupy.
- **Nešířte hoaxy a dezinformace** – čerpejte informace z důvěryhodných zdrojů.
- **Dodržujte GDPR a občanský zákoník** – nesdílejte na internetu fotografie a jiné informace o dětech bez předchozího souhlasu jejich zákonných zástupců.

4. zásada

Ochrana zařízení a dat

- Používejte antivirový program a firewall – chrání zařízení před malwarem.
- Zálohujte důležitá data – dle směrnice školy.
- Nepřipojujte se na veřejné wi-fi bez VPN – data mohou být snadno zneužita.
- Vypínejte Bluetooth a NFC, když je nepotřebujete – zamezíte možným útokům.
- Aktualizujte software a aplikace – bezpečnostní záplaty chrání před hrozbami.

5. zásada

Umělá inteligence a bezpečnost

- Nezasílejte AI chatbotům a velkým jazykovým modelům citlivé údaje – některé nástroje mohou informace ukládat. Konkrétní odpovědi spojené s otázkou bezpečnosti a práva při využívání nástrojů generativní AI najdete zde: <https://digitalizace.rvp.cz/napric-predmety/ai#faq>.
- Pozor na deepfakes a syntetický obsah – ověřujte autenticitu videí a zpráv.
- AI může generovat nepravdivé informace – kriticky zvažujte obsah všeho, co čtete.
- Pozor na podvody – ujistěte se, že umíte rozpoznat phishing, podvodný obsah aj. Vzdělávejte se v této oblasti.

6. zásada

Pravidla jsou základ

- Dodržujte školní bezpečnostní politiku – postupujte podle interních směrnic školy.
- Oddělujte pracovní a soukromé používání digitálních technologií – např.: nepoužívejte pracovní e-mail k nákupu na e-shopu.
- Při odchodu od počítače zamykejte obrazovku – používejte klávesovou zkratku nebo nastavte automatické uzamčení obrazovky na minimální časový limit. Snižujete tak riziko neoprávněného přístupu k informacím.
- Při používání cloudových služeb buďte opatrní – dokumenty ukládejte a sdílejte jen na zabezpečených úložištích.



**Digitální svět je skvělý, ale vyžaduje odpovědné chování.
Vždy přemýšlejte o tom, co sdílíte a s kým komunikujete.
Pokud se něco stane, nebojte se říct si o pomoc.**

Dál se vzdělávejte: [Bezpečnost a tvorba hesel](#)
[Rizika kybernetické bezpečnosti a jejich prevence](#)
[Dávej kyber! pro učitele](#)



Financováno
Evropskou unií
NextGenerationEU



NÁRODNÍ
PLÁN OBNOVY



MINISTERSTVO ŠKOLSTVÍ
MLÁDEŽE A TĚLOVÝCHOVY



digitalizace.rvp.cz