



Bezpečně online – ochraňuj své soukromí ve světě mobilů a sociálních sítí

Vzdělávací aktivita se zaměřuje na bezpečné používání mobilních zařízení a sociálních sítí. Žáci se seznámí s ochranou soukromí online, tvorbou bezpečných hesel a vhodným chováním na sociálních sítích. Aktivita ukáže praktické tipy pro bezpečné digitální chování s důrazem na problematiku bezpečných hesel a rizik spojených s prolomením hesel. Cílem této vzdělávací aktivity je zvýšit povědomí dětí o důležitosti ochrany soukromí a rozvinout u nich dovednosti pro bezpečné používání digitálních technologií.

CHARAŇTE SVÉ SOUKROMÍ: MOBIL, SOCIÁLNÍ SÍTĚ

Chraňte svůj mobilní telefon

V dnešním světě je mobilní telefon více než jen prostředek k telefonování – je to malý počítač s mnoha funkcemi. Správné zabezpečení mobilního telefonu je nezbytné.

Jak mobil zabezpečit:

- Nastavte si silné heslo nebo PIN kód pro odemknutí telefonu.
- Aktualizujte software na nejnovější verzi, abyste měli přístup k opravám a záplatám zabezpečení – kvůli chybám v aplikacích nebo systému může dojít například k možnosti číst příchozí SMS zprávy, sledovat polohu uživatele nebo aktivovat mikrofon a stáhnout fotografie bez vědomí uživatele.
- Používejte jen bezpečné Wi-Fi sítě a vyhněte se veřejným sítím, pokud je to možné.
- Zapněte automatické uzamčení obrazovky pro ochranu před neoprávněným vniknutím.
- Pro zvýšení zabezpečení se doporučuje používat nejlépe biometrický zámek obrazovky, jako například otisk prstu nebo rozpoznání obličeje.
- Nainstalujte si důvěryhodný antivirový program.
- Neinstalujte programy z neznámých zdrojů.
- Pravidelně zálohujte svá data.
- V případě ztráty nebo krádeže mobil vzdáleně smažte.

Chraňte své účty na sociálních sítích

Jaké informace mohou útočníci získat prostřednictvím nezabezpečeného profilu na sociálních sítích:

- Jestli má smysl váš účet „hacknout“.
- Odhalit vaše hesla.



Co se stane, když útočníci prolomí vaše heslo:

- Mohou zneužít vaši identitu.
- V případě, že používáte stejné heslo pro více účtů, mohou útočníci napáchat škodu také tam.

Jak vytvořit silné heslo:

- Heslo musí být dostatečně dlouhé (minimálně 8 znaků), za dostatečný počet znaků považujeme 16 nebo více.
- Heslo musí být jedinečné a unikátní.
- Pro zvýšení bezpečnosti používejte vícefázové ověřování.
- Pro lepší ochranu vašich přihlašovacích údajů používejte správce hesel.
- Buďte opatrní při volbě bezpečnostních otázek pro obnovení hesla, abyste minimalizovali riziko útoků založených na znalosti vašich osobních informací.
- Nepoužívejte slovníková slova a osobní informace.
- Používejte různé typy znaků a jejich kombinaci.
- Nebuďte „líní“ při vytváření hesel, vyhýbejte se stejným heslům k různým účtům.
- Heslo nikdy s nikým nesdílejte.
- Pamatujte si své heslo.

Silné a neprolomitelné heslo na sociálních sítích je důležité pro zajištění bezpečnosti vašeho účtu!

Na těchto odkazech najdete podrobné informace o zásadách internetové bezpečnosti, včetně jejich výkladu a dalších relevantních informací:

[ODKAZ 1](#)

[ODKAZ 2](#)

[ODKAZ 3](#)