



Praktický průvodce pro rodiče

Jak zajistit dětem bezpečí na internetu

bezpečnost
má  zelenou.cz



KOMUNIKACE A DŮVĚŘA



Zaveďte pravidelný „digitální pokec“

Mluvte o online světě pravidelně a v klidu, nejen když se něco stane. Ptejte se, co dítě hrálo nebo co zajímavého vidělo na sociálních sítích.



Sdílejte vlastní online zážitky

Děti se lépe otevřou, když vidí, že i dospělí řeší podobné situace. Povězte, co vám přišlo divné a jak jste to řešili.



Vysvětlete pojem digitální stopa

Co jednou zveřejníme, může být těžké nebo nemožné smazat. Stopu nezanechávají jen fotky, ale i cookies a další technická data.



Budujte důvěru místo zákazů

Přehnané zákazy vedou k tomu, že děti své online aktivity tají. Dítě musí vědět, že chyba není problém – problém je mlčení.



Mluvte o sextingu včas a bez dramatizace

Téma přirozeně napojte na rozhovor o vztazích, soukromí nebo bezpečnosti na internetu. Děti potřebují vědět, co sexting je a co dělat, pokud se dostanou do problémů.



Udělejte ze sebe „mimozemšťana“

Nechte si všechno vysvětlit, jako byste byli z jiné planety. Ptejte se: Na co se vaše děti dívají? Co to je? Jak to funguje? Proč je to baví?



Neodsuzujte

Nechte si pro sebe odsuzující komentáře. Příště vám už dítě nic neukáže a když se objeví problém, nepřijde za vámi.



PRAVIDLA A DOHODY



Nastavte si „Domácí digitální ústavu“

Dohodněte se na jasných pravidlech: jaké aplikace jsou povolené, kolik času na nich dítě tráví a jaké informace je bezpečné sdílet.



Připravte „Krizový plán“

Dítě musí dopředu vědět, co dělat, když se něco pokazí. Naučte ho 3 kroky: Ukončit komunikaci – Pořídit důkaz (screenshot) – Ohlásit (rodiči nebo v aplikaci).



Dohodněte pravidla pro sdílení osobních údajů

Děti často sdílejí jméno, fotku, název školy nebo svá oblíbená místa. Propojení těchto střípků představuje největší bezpečnostní riziko.



Odkládejte telefony při společných aktivitách

Pomáhá to budovat zdravý vztah k technologiím a udržovat rodinou pospolitost.





TECHNICKÉ ZABEZPEČENÍ



Nastavte rodičovskou kontrolu na počítači

Windows: Microsoft Family Safety (Nastavení > Účty > Rodina)
macOS: Čas u obrazovky v Systémových nastaveních



Nastavte rodičovskou kontrolu na telefonu

Android: Google Family Link (správa účtu, schvalování aplikací, časové limity).
iPhone/iPad: Čas u obrazovky v Nastavení.



Zkontrolujte nastavení soukromí na sociálních sítích

Instagram: přepněte na soukromý účet. WhatsApp: omezte viditelnost profilu.
TikTok: aktivujte Rodinné párování. YouTube: zvažte YouTube Kids.



Zabezpečte účty dítěte silnými hesly a 2FA

Pro každou síť a aplikaci nastavte unikátní silné heslo.
Aktivujte dvoufaktorové ověření (2FA) všude, kde je to možné.



Vypněte automatické zálohování citlivých fotek do cloudu

Zkontrolujte nastavení iCloudu a Google Photos.
Zabezpečte telefon PIN kódem nebo biometrikou.



Pravidelně kontrolujte přihlášená zařízení

Neznámá zařízení ihned odpojte.



OCHRANA PŘED HROZBAMI



Naučte dítě rozpoznat kyberšikanu

Vulgární zprávy, vylučování ze skupiny, šíření ponižujících fotek – to vše je kyberšikana. Více než polovina obětí (58 %) se nikomu nesvěří.



Varujte před online predátory a groomingem

Vysvětlete, jak funguje postupné budování důvěry s cílem získat intimní fotografie nebo přimět dítě k osobnímu setkání.



Promluvte o rizicích sdílení intimního obsahu

Téměř každé páté dítě poslalo intimní fotografii. Obsah nelze stáhnout zpět a může být zneužit k vydírání (sextorzi).



Upozorněte na deepfake a falešné profily (catfishing)

AI dokáže realisticky nahradit tvář nebo hlas. Naučte děti ověřovat informace z více zdrojů a nevěřit všemu, co vidí.



Omezte riziko nadměrného užívání

Sociální sítě a hry jsou navrženy tak, aby maximalizovaly čas na platformě. Nastavené časové limity a společné aktivity offline pomáhají.



VLASTNÍ DIGITÁLNÍ HYGIENA RODIČE

Omezte sharenting – sdílení dětí na sítích



Digitální stopu dětem vytváříme i my rodiče.
Vždy se ptejte dítěte na souhlas, než zveřejníte jeho fotku.

Jděte dětem příkladem



Ukazujte zdravý vztah k technologiím.
Pokud rodiče neustále klikají na telefon, děti budou dělat totéž.





KRIZOVÝ PLÁN – KDYŽ SE NĚCO STANE



Uložte důkazy (screenshoty, odkazy, časy)

Důkazy nemažte ani s nimi nemanipulujte.
Jsou zásadní pro řešení ve škole, na platformě i u policie.



Zastavte kontakt a zabezpečte účet

Na útočníka nereagujte, zablokujte ho a nahlasejte profil. Změňte hesla a zapněte 2FA.
Zároveň zrevidujte stávající metody 2FA, aby tam nebyla nějaká útočnickova.



Naučte děti, aby si řekly o pomoc dospělým

Dítě by nemělo zůstat samo. Může se obrátit nejen na rodiče,
ale i učitele, školního psychologa případně online poradnu.





KAM SE OBRÁTIT O POMOC

Linka bezpečí – 116 111

Bezplatná anonymní linka pro děti a mladistvé, nonstop.
Krizová intervence a poradenství.

E-Bezpečí (e-bezpeci.cz)

Online poradna zaměřená na rizika internetu.
Odborné poradenství obětem i rodičům.

STOPonline.cz

Anonymní hlášení nelegálního obsahu na internetu.
Spolupracuje s Policií ČR a sítí INHOPE.

Policie ČR – 158

Při závažném vyhrožování,
vydírání nebo trestné činnosti.

Rodičovská linka

Poradenství pro rodiče,
kteří si nejsou jistí, jak postupovat.

Zdroje: Safer Internet Centrum ČR – Čeští žáci v online světě 2025,
Security Avengers (Ing. David Pecl), E-Bezpečí, Policie ČR

**bezpečnost
má  zelenou.cz**