DIGITÁLNÍ SVĚT VAŠICH DĚTÍ

ONLINE TIPY PRO RODIČE

ONLINE RIZIKA

Nejlepší obranou proti online rizikům je otevřenost, povědomí a vzdělávání. Promluvte si se svými dětmi o jejich online životě, sdílejte jejich zkušenosti a učte se od nich. Pomozte jim používat technologie pozitivně a zodpovědně a stanovte jim hranice a poskytněte vedení a podporu. Níže je uvedeno několik rizik, o kterých si s dětmi můžete promluvit:

1 KRÁDEŽ IDENTITY

Krádež identity je krádež osobních údajů za účelem jejich využití, nejčastěji pro finanční prospěch. Nejedná se o nový problém, ale rozšířil se díky internetu, který zločincům poskytuje nové způsoby, jak získávat osobní údaje v mnohem větším rozsahu. Kriminálnici používají pro shromažďování osobních údajů různé metody – od získávání údajů zveřejněných online (například na online profilech a stránkách sociálních sítí) až po využívání kombinace technik spamování, phisingu a pharmingu. Nejlepším způsobem prevence proti krádeži identity je bezpochyby poradit dětem, aby nezveřejňovaly osobní údaje, jako jsou čísla bankovních účtů, adresy, telefonní čísla, údaje z cestovního pasu atd.

2 SPAMOVÁNÍ, PHISHING A PHARMING

Spamy jsou nevyžádané zprávy obvykle rozesílané hromadně. Spamové zprávy mohou obsahovat komerční obsah jako například pornografii, léky, pochybné finanční transakce nebo nabídky, které jsou „příliš výhodné na to, aby byly pravdivé“.

Phishingové útoky jsou případy, kdy uživatelům chodí e-maily, které se je podvodně snaží donutit, aby prostřednictvím falešné webové stránky (například imitující banky) „aktualizovali“ své osobní údaje online. Tyto webové stránky ukládají osobní údaje a používají je k nekalým účelům.

Pharming je přesměrovávání uživatelů na falešné kopie skutečných webových stránek, opět s cílem získat osobní údaje a hesla ke kriminálním účelům. Promluvte si s dětmi o tom, jak odhalit útoky phishingu a pharmingu.

3 GROOMING

Dětský grooming označuje veškeré činnosti prováděné vědomě za účelem spřátelení se a navázání citového vztahu s mladistvým. Cílem tohoto „zvláštního vztahu“ je potlačení zábran a příprava na pohlavní zneužívání nebo využívání. Dětský grooming může sloužit k nalákání mladistvých k nezákonným praktikám, jako je prostituce nebo dětská pornografie.

4 CYBERBULLYING

Kyberšikana je způsob využití technologie k vědomému poškozování, rozrušení, obtěžování a uvádění do rozpaků jiné osoby. Ke kyberšikaně může docházet prakticky v jakékoli formě obsahových médií, od sprostých textů a obrázkových zpráv odesílaných mobilním telefonem, přes kruté názory zveřejněné prostřednictvím blogů, sociálních sítí nebo e-mailů a rychlých zpráv, až po zákeřné webové stránky vytvořené výhradně za účelem zastrašování osob.

Kyberšikana může být v mnoha ohledech dokonce ještě škodlivější než běžné formy šikany. Protože existuje:

- Možnost elektronického napadení oběti v domácím a osobním prostředí
- Potenciálně početnější publikum
- Vyšší rychlost šíření nepříjemných zpráv či obrázků
- Potíž s kontrolou elektronicky zveřejněného a šířeného obsahu
- Vnímaná anonymita kyberšikany, díky které se děti mohou zapojovat, ať již jako organizátoři nebo nezúčastnění diváci, do činností, které by je v reálném světě ani nenapadly

Řekněte svým dětem, že je v pořádku blokovat „kamarády“ nebo se jednoduše odhlásit z webové stránky v případě, že se kvůli někomu nebo něčemu necítí dobře online. Konec konců samy mají nad situací kontrolu, pokud se rozhodnou někoho zablokovat nebo se odpojit. Je však vždy dobré, aby si o těchto problémech mohly promluvit s dospělým, kterému důvěřují: díky tomu se utvrdí v tom, že jednaly bezpečně a správně.

POTŘEBUJETE DALŠÍ INFORMACE?

Další informace naleznete na webu sítě Insafe:
www.saferinternet.org