Sdílení fotek třeba z dovolené, udržování kontaktů s kamarády, kteří bydlí daleko nebo hledání informací a zajímavostí do školy. To jsou jen některé ze skvělých možností, které nám chytré technologie a internet umožňují. Ne všechny aktivity jsou ale bez problémů: i na internetu se tě může někdo snažit podvést, vydírat, urazit nebo zesměšnit. Jak se nenechat napálit a na co si dát pozor?

Monika Hanych

Facebook, Instagram, Snapchat… Vychytávky pro tvou bezpečnost

Neříkej, kde bydlíš, kam chodíš do školy a jak se skutečně jmenuješ

„Často potkávám holky nebo kluky přesvědčené o tom, že jsem si s nimi psal a domlouval schůzku, ale ve skutečnosti to byl bohužel falešný profil, kterému na sebe prozradili spoustu soukromých informací, nebo si dokonce domluvili osobní schůzku," varuje v jednom videu známý youtuber Jirka Král. Rozhodně doporučuje, abys svoje osobní údaje jako třeba příjmení, datum narození, adresu domova nebo školy nikomu cizímu na internetu nesděloval. Nikdy taky nepiš, kdy odjíždíš s rodinou na dovolenou. Zlodějům by tak velmi ulehčil práci a po návratu by vás mohlo čekat nemilé překvapení v podobě vykradeného domu!

S tím souvisí i jména a přezdívky na sociálních sítích nebo diskuzních fórech: ačkoliv po tobě vyžadují celé jméno a příjmení a ty nechceš podvádět, z důvodu bezpečnosti své celé jméno a příjmení raději nezadávej. Aby tě na sítích poznali třeba kamarádi, stačí, když zadáš třeba část svého jména, přezdívku nebo jméno uvedeš v přesmyčce. Věříme, že s vymýšlením zábavného „nicku" pro použití na sociálních sítích určitě mít problém nebudeš.

Tak si tě případný útočník nebude moci vyhledat a spojit s tím, kam chodíš do školy nebo kde bydlíš, kdyby měl v úmyslu tě vydírat nebo pronásledovat.

Pozor na falešné prosby od kamarádů

Nenaleť ani prosbám, které vypadají jako od tvých kamarádů, ale ve skutečnosti jejich účet někdo napadl. Jeden z takových případů se stal na Facebooku Petrovi. Tvářil se jako nevinná prosba od jeho kamaráda Tadeáše: „Prosím tě, pošli mi svoje telefonní číslo, omylem jsem si ho smazal." Po zaslání ale Tadeáš pokračoval: „Přepošli mi ještě kód, co ti teď přijde na mobil, potřebuju ho. Díky moc!" Nic netušící, důvěřivý Petr odeslal i tento kód.

Když další měsíc přišlo vyúčtování za mobil, nestačil se Petr spolu s rodiči divit. Proto začali zjišťovat, kde se faktura za několik tisíc korun vzala. Nakonec zjistili, že Petr není zdaleka jediný, kdo se nechal napálit. Útočník získal přístupové údaje k Facebooku mnoha lidí tak, že vytvořil falešné stránky s hlasováním do soutěže o nejhezčí auto, kam bylo pro hlasování potřeba vložit odkaz na svůj facebookový profil a heslo. Podvodník tak získal přístup k účtům mnoha lidí, z jejichž profilů pak obesílal jejich kamarády.

Rada v tomto případě zní: Dobře si rozmysli, kam vyplňuješ svoje údaje a zejména hesla! Obecně platí, že hesla bys neměl zadávat jinam než přímo na stránku, pro kterou platí. Tedy, heslo k tvému Facebooku nevyplňuj jinde než právě na této stránce. Také se vyplatí mít jiné heslo pro sociální sítě a jiné heslo k e-mailu, na školní web, k bankovnímu účtu a tak dál. Když útočník zjistí jedno z hesel, nedostane se tak ke všem tvým účtům, datům, fotkám či úsporám.

A jak ověřit, zda ti píše opravdu tvůj kamarád? Při podobné žádosti, jakou obdržel Petr, můžeš kamarádovi preventivně zavolat nebo ho prozvonit – pokud ti píše skutečně on, získá tvoje číslo a ty si ověříš, že jeho profil nikdo nehacknul (nenapadl). Případně se s ním zkus spojit ještě jinou cestou (třeba přes sourozence nebo počkej do dalšího dne ve škole) a ověř si, že ti takovou prosbu opravdu poslal on sám.

Co platí v offline světě, dodržuj i online

Kdyby ti cizí náhodný člověk zastavil na ulici s nabídkou svezení domů v jeho naleštěném autě, nasedl bys? Jasně, že ne. U takových lidí ti instinkt hned napoví, že tohle nemáš dělat. A pokud ne instinkt, stále máš ještě rozum a také si takové rady pamatuješ od rodičů, ze skautu, školy nebo z Tarsicia. Ale co ve světě internetu? Jak poznat, komu věřit, když ti přijde zpráva od někoho neznámého?

Je to překvapivě úplně stejné – cizím lidem na internetu nedůvěřuj, protože nevíš, kdo se za profilem skrývá. Jinak bohužel můžeš skončit velmi špatně – v lepším případě třeba „jen" okradením, v horším případě vydíráním, šikanou či násilím.

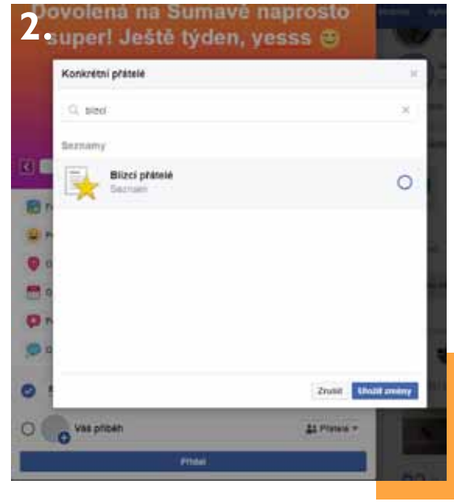
To se stalo čtrnáctiletému Dominikovi, který se na Instagramu seznámil se stejně starou pěknou slečnou. Měl pocit, že mu ve všem rozumí a rád si s ní dopisoval. Po delší době, kdy už si myslel, že se vlastně znají, byť jen přes internet, se nechal ukecat a poslal jí fotku, na které byl úplně nahý. Děvče se dožadovalo dalších a dalších fotek, které ale poslat odmítl. V tu chvíli mu začala vyhrožovat, že jeho fotky zveřejní, rozešle kamarádům, které si postupně přidala do svých přátel, a také jeho mamce.

Kdyby Dominik zpanikařil, mohlo to skončit velmi špatně: například v Kanadě kvůli studu ze své situace dvanáctiletá Amanda spáchala sebevraždu. Útočník, který se na internetu vydával za pohledného mladíka, totiž její obnažené fotky opravdu zveřejnil. Místo podpory a pochopení se ale Amanda dočkala posměchu a šikany ze strany spolužáků. Proto, pokud se někdo z tvých kamarádů do podobné situace dostane, pamatuj na to, že potřebuje pomocnou ruku a nikoliv pohrdání.

Tento typický případ vydírání ale rozhodně nemusí skončit takto. Pokud už k něčemu takovému dojde, ani v takovou chvíli není pozdě. Raději hned popros o pomoc staršího sourozence či kamaráda, rodiče nebo někoho, komu opravdu důvěřuješ. Vysvětli situaci, přiznej, žes udělal chybu a že tě na internetu někdo vydírá. Pokud máš strach se někomu blízkému svěřit, zavolej raději na Linku bezpečí nebo napiš do online poradny pro děti a mladé v nesnázích. Kontakty najdeš v rámečku vedle článku.

Jak si tedy chránit na sociálních sítích své soukromí?

Vždycky rozlišuj, s kým chceš sdílet svoje informace. Chceš se pochlubit, kde jsi na dovolené, že máš nový cool mobil nebo nadupaný počítač na hraní her? Pak to rozhodně nesdílej veřejně, jinak nahráváš možným zlodějům. Na Facebooku se vždycky ujisti, pro koho svůj status, fotky, video nebo story sdílíš. Ideální je přidávat si do přátel jen lidi, které znáš osobně a důvěřuješ jim.



2.

Osobní informace sdílej jen s vybranými kamarády či rodinou, kterým naprosto věříš.

Pokud si chceš na Facebooku do přátel přidávat i cizí lidi, pak je dobré si vytvořit různé seznamy svých přátel – například „Známí" nebo „Neznám osobně". Při sdílení osobních informací pak můžeš tyto skupiny ze sdílení vyloučit: vybereš možnost sdílet například jen s „Přátelé kromě Známí" (mrkni na obrázek č. 1, jak na to). Tak tvůj příspěvek uvidí jen ti, které sis přidal do přátel, ale nejsou ve skupině „Známí".

Stejně tak si můžeš naopak vytvořit i seznam těch, kteří jsou ti blízcí jako třeba „Rodina", „Spolužáci", „Best friends" a podobně. Pokud chceš sdílet cokoliv jen s touto jednou skupinou, zvol možnost sdílení „Konkrétní přátelé" (viz obrázek č. 2) a zadej název této skupiny. Tak vyloučíš ostatní v přátelích na svém facebooku, aby tento konkrétní sdílený obsah neviděli.

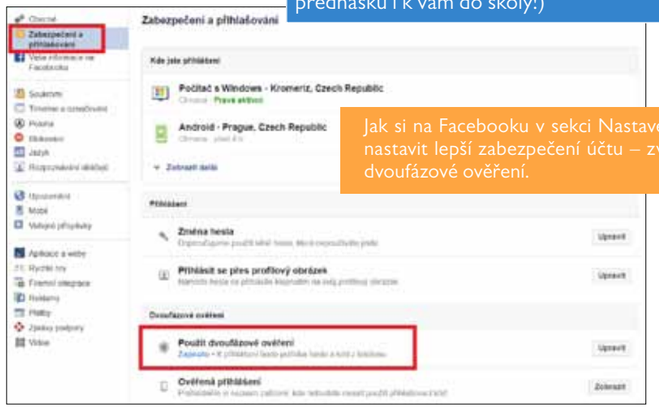
Co se týká dalších sociálních sítí nebo diskuzních fór, obecně platí, že pokud už chceš něco sdílet, vyplatí se dělat to jen pro vymezený a uzavřený okruh přátel či sledujících. Například na Instagramu si můžeš zvolit profil veřejný nebo soukromý – pokud si zvolíš veřejný, počítej s tím, že vše, co zveřejníš, bude běžně dohledatelné a spárovatelné s tvým jménem při vyhledávání například na Googlu. Opravdu chceš, aby měl do tvého pokoje doma nebo k fotkám z letní dovolené přístup úplně kdokoliv na světě?

A poslední rada: Pokud se bojíš, že se do tvého účtu na sociálních sítích nebo třeba do e-mailu někdo naboural (a bohužel se to může stát), zapni si tzv. dvoufázové ověření. Třeba na Facebooku stačí jít do Nastavení > Zabezpečení a přihlašování > a tam zvolit dvoufázové ověření přes mobil (mrkni na obrázek č. 3). Tak ti přijde smska pokaždé, pokud se k tvému účtu přihlásí pozměněné nebo nerozpoznané zařízení. Někdy to možná budeš jenom ty třeba z počítače u kamaráda, ale kdyby šlo o nabourání se do tvého účtu, ihned to zjistíš a vyřešíš.

Kam se obrátit, když si nevím rady? Když mě někdo na internetu vydírá, šikanuje či pronásleduje?
– www.linkabezpeci.cz
– www.soscentrum.cz
– Modrá linka důvěry pro děti a mládež, tel. 549 241 010, 608 902 410 (9–21 každý den)
– www.budsafeonline.cz (kampaň Youtubera Jirky Krále za lepší bezpečnost na internetu – mrkni na jeho rady a tipy. Můžeš ho pozvat na přednášku i k vám do školy!)

1.

Na sociálních sítích informace jako na tomto obrázku ideálně vůbec nesdílej. Pokud už se chceš pochlubit, pak se ujisti, že informace sdílíš jen přátelům. A ideálně jen těm, kterým můžeš důvěřovat.



3.

Jak si na Facebooku v sekci Nastavení nastavit lepší zabezpečení účtu – zvol dvoufázové ověření.

Foto: Archiv autora, Agencia de Noticias ANDES - wikipedia.org