# Rizika sociálních sítí

Sociální sítě jsou určeny k seznamování a k udržování kontaktů mezi kamarády a známými. Umožňují také rychlou výměnu informací. U většiny sociálních sítí jsou vámi zveřejněné údaje zobrazeny všem vašim kontaktům. Podle nastavení pak také kontaktům vašich kontaktů, všem uživatelům dané služby a v nejhorším případě všem uživatelům Internetu. Některé sociální sítě však umožňují rozdělení přátel na různé podskupiny, například rodinu a pracovní kolektiv. Na základě toho rozdělení je pak možné řídit, komu se jaká informace zobrazí.

## Všeho s mírou

Z tohoto důvodu je tedy nezbytně nutné při používání sociálních sítí přemýšlet o tom, komu chceme danou informaci poskytnout a jak velké riziko by pro nás její zveřejnění znamenalo. Vždy je třeba mít na paměti, že to, co o sobě zveřejníte na Internetu, už obvykle nejde vzít zpět. Čím bizarnější či neobvyklejší věc to bude, tím spíše si brzo začne žít v rámci Internetu vlastním životem. To samé platí také o zveřejňování informací o druhých lidech. To, co vám může připadat jako neškodná informace, může někomu jinému způsobit problémy.

Rizikem je např. i zdánlivě neškodný příspěvek o odjezdu na dovolenou, který může kromě vašich přátel zajímat také potenciální zloděje. Zveřejněné údaje také může někdo využít k vydírání, především děti pak mohou být snadno manipulovány k seznámení, případně i k osobní schůzce (pokud má útočník přehled, o co se dítě zajímá, jaké má koníčky nebo problémy, je pro něj daleko jednodušší ho někam vylákat).

S tím souvisí skutečnost, že na sociálních sítích je také možno zakládat účty pod jakýmkoliv jménem. Pokud útočník získá dostatek informací z vašeho pravého účtu, může jej snadno napodobit.

Dobře si také rozmyslete zveřejňování soukromých fotografií, především pak zveřejňování fotografií vašich dětí. Fotografie vašich dětí hrajících si na pláži u moře může být sice roztomilá, ale pro pedofily systematicky prohledávající sociální sítě to může být velice cenný artikl. Toto poslední ostatně platí obecně i o publikování takovýchto fotek kdekoliv na Internetu.

**Při používání sociálních sítí je tedy třeba přemýšlet o tom, komu a jaké informace dáváme k dispozici.**

Další záludností sociálních sítí je také snadné šíření nepravdivých informací. V tomto směru pak vyniká především šíření tzv. hoaxů (poplašná zpráva, obvykle vymyšlená tak, aby působila dojmem, že se něco takového mohlo stát). Proto je vhodné nad informacemi přijatými ze sociálních sítí i Internetu přemýšlet a snažit se je ověřit i z jiného zdroje. To že informaci sdíleli vaši přátelé ještě neznamená, že si ji sami někde ověřovali.

V neposlední řadě bývá častým jevem na sociálních sítích kyberšikana. Jedná se v podstatě o šikanu, což je dobře známý patologický jev. V tomto případě se však jedná o její formu, využívající moderní elektronické prostředky (Internet, mobilní telefon, počítače, e-mail, blogy). Časté je především vytváření falešných účtů oběti na sociálních sítích s jasným cílem oběť zesměšnit či jinak veřejně ponížit. Pachatel však může také na vlastním účtu zveřejňovat texty

a obrázky poškozující oběť. Asi nejnebezpečnější je, pokud se pachateli podaří získat přístup přímo k účtu oběti. Dopady takovéhoto útoku mohou být skutečně zdrcující. Proto je potřeba – na sociálních sítích, stejně jako jinde – dbát na kvalitu používaných hesel. Mezi časté projevy kybešikany patří také zasílání urážejících a obtěžujících e-mailů či SMS.

Za zmínku stojí také různé aplikace třetích stran, které jsou na sociálních sítích k dispozici. Ty po vás mohou chtít přístup k nejrůznějším informacím z vašeho účtu, například k datu narození. Vždy si dobře promyslete, co všechno chcete dané aplikaci povolit a zpřístupnit.

To hlavní na konec. Při registraci do jakékoliv služby, nejen do sociálních sítí si vždy důkladně prostudujte podmínky používání služby. Je dobré vědět jakým způsobem budou vaše data dále využívána.