

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **79** ze dne **15.8.2024**

12 věcí, které byste nikdy neměli sdílet na sociálních sítích

V Česku používá aktivně sociální sítě přes 8 milionů lidí (odhad společnosti Statista). Sdílíme svoje fotky a videa, lajkujeme příspěvky a komentujeme, posíláme soukromé zprávy, řešíme nákupy a mnoho dalšího.

Právě s tím, jak sítě používáme, se pojí jedno nejvýraznější riziko – s nadměrným sdílením. V horším případě může nadměrné sdílení vést k odcizení identity či hesel, v případě dětí také k šikaně. Obecně jste tak snadnější terč pro všechny, kteří nemají poctivé úmysly.

Chránit soukromí si musí každý uživatel sám

Za ochranu soukromí je odpovědný především každý uživatel. Jakkoli to zní banálně, není to snadné. Sociální sítě jsou na sdílení založené, dokonce se nás svými algoritmy snaží přimět sdílet více a více. Zároveň tvoří prostředí, které nadměrné sdílení normalizuje. To je riziko hlavně pro děti nebo uživatele v seniorském věku.

Snažte se proto mít kontrolu nad tím, jakou komunitu přátel a sledujících si online vytváříte. Jak na to? Nastavte si profily jako soukromé a pečlivě zvažujte, koho si mezi sledující přidáte. V případě dětí doporučujeme, aby všechny své online přátele znaly i z fyzického světa.

I přesto, že máte profily takto uzavřené, není rozumné sdílet všechno a se všemi. Platí, že co jednou nahrajete na internet, to už online zůstane. Proto raději nesdílejte:

1. Osobní údaje

Na internet nikdy nepatří osobní údaje, které vás identifikují. Typicky jde o adresu domů, do školy či zaměstnání a telefonní čísla. Nikdy také nesdílejte fotografie dokladů a dokumentů, i když jste na své úspěchy opravdu hrdí. Například na vysvědčení dětí je rodné číslo, na prvním řidičském průkazu také.

Opatrní buďte také při sdílení informací ze soukromí. Nějaké takové informace totiž polovina z nás používá při tvorbě hesla. Typicky jde o jméno mazlíčka, datum narození, oblíbenou knihu, barvu či destinaci. Z těchto údajů tvoří útočníci obrovské databáze, které následně používají k prolomení hesel. Některé dříve populární kvízy na Facebooku sloužily přesně k takovému sběru údajů.

2. Plány na dovolené a cestování

Jasně, že se na dovolenou těšíte a chcete se o své nadšení podělit s přáteli na internetu. Bohužel tím, ale také říkáte zlodějům, že nebudete doma. Je lepší být nekonkrétní. Například: "V létě pojedeme na Bali, už se moc těšíme." Fotky a zážitky raději sdílejte až po návratu domů.

3. Údaje o poloze v reálném čase

Ze stejného důvodu byste nikdy neměli sdílet informaci o tom, kde přesně se nacházíte. Dalším důvodem je také osobní bezpečnost. Sdílení polohy totiž usnadňuje stalking nebo šikanu. Je vhodnější říci: "Jsem v Praze." než "Jsem v Praze na Václaváku." Důležité je také vypnout geolokaci, pokud ji právě nepoužíváte k navigaci.

MEATEST spol. s r.o. - sdělení pověření pro ochranu osobních údajů číslo **79** ze dne **15.8.2024**

4. Nákupy luxusního zboží

Rozmyslete si také zveřejňování fotek drahých šperků nebo nového luxusního auta. Jednak to může zbytečně vyvolat závist a také můžete opět upozornit případné zloděje.

5. Fotografie dětí

Možná patříte mezi rodiče, kteří rádi sdílejí fotografie svých dětí na internetu. Rozumíme tomu, děti jsou naší pýchou. Fenoménu, kdy rodiče sdílí informace o svých dětech, říkáme sharenting. Ten má řadu rizik.

Časem mohou informace sloužit k odcizení online identity nebo šikaně. Pokud sdílíte fotky, na kterých se děti koupou, může bohužel dojít i k tomu, že se tyto fotky dostanou k pedofilům.

Radíme proto o dětech sdílet naprosté minimum informací, například jen v soukromých konverzacích s rodinou. Pokud máte větší děti, ptejte se jich, zda to či ono sdílet smíte.

6. Pracovní nebo studijní problémy

Sociální sítě sledují i naši kolegové a spolužáci. Pokud tedy řešíte nějaký osobní problém v zaměstnání nebo při studiu a potřebujete ventilovat vztek, raději si s někým promluvte v soukromí.

7. Finanční údaje

Podvodníci z vás často zkouší vylákat údaje z platební karet. Takto zneužít se dá i fotka, na kterém je karta rozmazaná nebo daleko od objektivu. Typicky tyto údaje požadují podvodníci při podvodech na online bazarech. Číslo karty a CVV kód nikdy nikomu neříkejte. Pokud ho po vás žádá, chce vás okrást. Detaily se dočtete v tomto článku.

8. Soukromí rodiny a přátel

To, co jednou na sociální sítě nahrajete, na nich zůstává. (v Evropě je to možné jen se souhlasem uživatele). Ne každý s tím souhlasí. Proto si vždy vyžádejte souhlas, než cokoli nasdílíte. Děláte to pro své blízké, chráníte tím je samotné a jejich soukromí.

9. Soukromé rozhovory

Sociální sítě jsou ze své podstaty veřejným fórem, i když je váš účet relativně uzavřený. Proto nikdy nesdílejte to, co vám někdo řekl v soukromé zprávě nebo osobním rozhovoru. Pokud se zpráva netýká přímo vás, nesdílejte ji.

10. Intimní fotky

Nahotu obvykle sociální sítě zakazují a fotky nelze zveřejnit, nebo vám je dodatečně síť smaže za porušení pravidel. Sdílet byste je ale neměli ani ve zprávách. Vždy existuje riziko, že druhá strana materiál zneužije.

11. Nenávistné a diskriminační příspěvky

Zveřejňování urážlivých nebo diskriminačních příspěvků může mít vážné důsledky. Bývá proti pravidlům používání sociální sítě. Hrozí tedy, že na nějaký čas nebo i natrvalo přijdete o svůj účet. (Pokud uživatel opakovaně porušuje pravidla, může jej síť zablokovat.) Mohou ale také poškodit vaši pověst nebo zkomplikovat situaci při hledání zaměstnání (ano, HR čtou veřejné profily na sociálních sítích).

MEATEST spol. s r.o. - sdělení pověřence pro ochranu osobních údajů číslo **79** ze dne **15.8.2024**

12. Nepravdivé informace

Stejně striktní pravidla mají sociální sítě pro sdílení lží a dezinformací. Můžete dočasně nebo trvale přijít o svůj účet. Může se to podepsat také na vaší reputaci. V kontextu kybernetické bezpečnosti se často setkáváme se lživými reklamami, které občas lidí v dobré víře sdílí. Vždy si ověřte šokující nabídku nebo kontroverzní zprávu, než ji budete sdílet se svými přáteli.

Jak si chránit soukromí na sociálních sítích

Vždy pečlivě zvažte, co zveřejňujete. Dokonce, i když máte soukromé profily. Platí, že nad vším, co jednou zveřejníte na internetu, ztrácíte kontrolu a už to nejde odstranit.

Čas od času si zkontrolujte, koho máte v přátelích nebo sledujících. Pořád chcete být s tímto uživatelem v blízkém kontaktu? Není na škodu seznam přátel čas od času pročistit a odstranit z něj lidi, které neznáte nebo nechcete, aby si prohlíželi vaše příspěvky.

Omezte, kdo může zobrazovat váš seznam přátel a příspěvky. Snížíte tak pravděpodobnost, že někdo zneužije informace, které sdílíte.

Omezte přístup ke svým fotografiím. V ideálním případě by je měli mít možnost vidět pouze známí přátelé a členové rodiny.

Zapněte si dvoufaktorové ověřování (2FA) a používejte silná a jedinečná hesla. I když se útočníkovi podaří heslo uhodnout nebo prolomit, díky další vrstvě zabezpečení bude méně pravděpodobné, že se mu podaří ovládnout celý váš účet.

Proveďte si různé formuláře a aplikace, než do nich zadáte své osobní údaje. Často je totiž zneužívají podvodníci k phishingu, neboli sběr citlivých údajů. Spolehněte se na to, že nebudeme příliš pozorní.

Zdroj: AVcentrum ČR