

FACEBOOK - ZÁKLADNÍ ZABEZPEČENÍ A OCHRANA SOUKROMÍ

Lukáš KUBALA

Výzkum České děti v kybersvětě v loňském roce ukázal, že české děti na internetu tráví nejvíce času na sociálních sítích. Nejvyšší příčky ne zcela překvapivě obsadily sociální sítě a online nástroje, které děti aktivně využívají již několik let. Ovšem od posledních výzkumů cílených na online služby se ve výsledcích začínají nově objevovat novinky jako je TikTok nebo Tellonym. Celkově se dle průzkumu jedná o pestrobarevnou paletu služeb, které mají mnohdy složité a specifické způsoby, jak si zabezpečit uživatelský profil. Není divu, že pro dospělé i děti může být občas složité vyznat se v rozhraní těchto služeb, přičemž uživatelé mnohdy ani netuší, co vše lze nastavit a zabezpečit. Než se pustíte do užívání a nastavování jakékoliv sociální sítě či online služby, nezapomeňte – na internetu soukromí neexistuje. Myslete na to, že cokoliv umístíte na internet, už z něj pravděpodobně nikdy doopravdy neodstraníte. Jakákoliv fotografie, video či text si kdykoliv může najít cestu k lidem, kteří tento materiál mohou nějakým způsobem zneužít.

Základní nastavení

Facebook vyvolává falešný dojem, že vše, co na něj nasdílíme je bezpečně uloženo a pouze naše. Firma však s daty svých uživatelů nakládá všelijak, a proto je soukromí uživatelů jen relativní pojem. A že o svých uživatelích ví Facebook více než oni sami, to už nám tato sociální síť v minulosti dokázala několikrát. Nesmíme ale zapomínat, že naše osobní údaje mohou padnout do cizích rukou nejen vinou Facebooku. Je proto vhodné si řadu věcí nastavit nebo minimálně zkontrolovat zabezpečení

našeho profilu. Vše najdeme v pravém horním rohu v **Nastavení**. Doporučujeme projít si všechny kategorie a zvláště věnovat pozornost nabídkám **Soukromí** a **Timeline a označování**.



V nabídce **Soukromí** si zkontrolujte, kdo všechno uvidí vaše budoucí příspěvky. Pravděpodobně budete mít defaultně nastaveno **Veřejný** – příspěvky může vidět kdokoliv na Facebooku i mimo něj. Na výběr však máte z několika možností, optimální volbou je **Přátelé**. Jakmile váš profil navštíví někdo cizí, na rozdíl od uživatelů z vašeho seznamu přátel neuvidí na vaší zdi žádný příspěvek. Zajímavou alternativou je kategorizace přátel do skupin, které si zvolíte. Můžete tak své příspěvky sdílet např. jen s rodinou či spolužáky/kolegy. Toto nastavení lze měnit i individuálně u jednotlivých příspěvků.

Ať už zvolíte jakoukoliv možnost, vyhněte se přehnanému sdílení osobních informací. Rozhodně **nikdy na Facebooku nesdílejte informace o tom, že jedete na dovolenou a váš dům či byt bude opuštěný!** Rázem se z vás může stát terč tzv. bytařů, kteří aktivně sledují sociální síť.



Dále lze nastavit, kdo vám může zaslat žádost o přátelství nebo kdo vás může vyhledat pomocí e-mailové adresy či telefonního čísla (pokud jste jej zadali). Rozhodně nevynechejte možnost nastavit si, **kdo vidí seznam vašich přátel**. Pokud zvolíte **Jenom já**, nikdo jiný se k seznamu nedostane. Díky tomu se můžete vyvarovat např. internetovému podvodu, během kterého útočník naklonuje profil vybraného uživatele z vašeho seznamu a přebere jeho identitu. Následně vás osloví s žádostí o pomoc při obnově fiktivní zablokované služby jakožto váš falešný přítel. Místo odblokování zablokovaného účtu však pachateli umožníte potvrdit finanční transakci u vašeho mobilního operátora.

Jak podvodné jednání odhalit? Stačí si ověřit identitu žadatele o přátelství – třeba tím, že mu zatelefonujete. Rozhodně nikdy nevyužívejte v prostředí sociálních sítí m-platby a nikomu neposílejte platební kódy a další platební informace.

Jak celý podvod funguje najdete zde: www.e-bezpeci.cz/index.php/emata/sociotechnika/774-podvodne-platby-na-facebooku a další informace zde: www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/sociotechnikax/1253-klonovani-profilu.

Mezi další užitečné nabídky patří zmíněné nastavení profilu **Timeline a označování**. Opět nastavujeme, kdo vidí náš obsah na Facebooku a kdo může přidávat obsah na naši zeď. Pro úplnou kontrolu doporučujeme u otázky „Kdo může na vaši timeline přidávat příspěvky?“ nastavit **Jenom já**. Taktéž si v sekci **Kontrola** u otázky „Chcete kontrolovat příspěvky, ve kterých vás někdo označil...“ **zapněte kontrolu Timeline**. Poté veškeré příspěvky, u kterých vás někdo označí nebo je bude vkládat na vaši zeď, musíte nejprve schválit. Tím se vyhnete nepříjemným situacím, které mohou nastat. Jeden příklad za všechny – někdo vás vyfotí v nevhodné situaci a fotografii umístí na váš veřejný profil se zavádějícím komentářem. Než si takového příspěvku všimnete, mohou jej vidět, stáhnout či přeposlat desítky až tisíce uživatelů. Ovšem **pozor, toto nastavení nezamezí dotyčné osobě publikovat či komentovat příspěvek, u kterého jste označení**.

Pokud si během nastavování změn v profilu nejste jisti, co je, nebo není viditelné, vyzkoušejte šikovnou funkci v sekci **Kontrola** – „Zkontrolujte si, co ostatní lidé vidí na vaší timeline.“ Po kliknutí na: **zobrazit jako**, přejdete do náhledu vašeho profilu a uvidíte vše, co vidí uživatelé mimo seznam vašich přátel i lidé mimo Facebook.

Na co dalšího si u Facebooku dát pozor?

Pokud si potřebujete změnit heslo nebo víte, že váš účet není dostatečně zabezpečený, projděte si v **Nastavení** nabídku **Zabezpečení a přihlašování**. Najdete zde informace o tom, odkud a z jakého zařízení se přihlašujete do Facebooku, možnost změnit dosavadní heslo, aktivovat dvoufázové ověření nebo šifrování notifikačních e-mailů atd.

Obecně platí, že do každé další služby na internetu byste měli používat samostatné přihlašovací údaje. Tzn. Jedinečné přihlašovací údaje pro každou službu. Proto **nepoužívejte**

Facebook ani jiné sociální sítě pro přihlašování k dalším službám. Hlídejte si, jakým aplikacím dáváte práva k přístupu k vašemu účtu.

Chcete-li zjistit, které aplikace tato práva mají nebo v minulosti měla, podívejte se do nabídky **Aplikace a weby**. Možná vás překvapí, s čím vším jste v minulosti sdíleli svá data. Může se jednat o vaše příspěvky, fotografie a videa, seznam přátel atd.



A co Facebook Messenger?

Chatovací platforma Messenger patří v současnosti mezi nejpoužívanější komunikační nástroje. Ještě v minulém roce bylo možné používat Messenger bez nutnosti vlastnit profil na Facebooku. Pro nové uživatele to již neplatí. Pokud jste mezi nimi a tato povinnost vám nevyhovuje, můžete svůj profil deaktivovat. **Messenger lze používat i poté, co provedete deaktivaci účtu na Facebooku.**

Jestliže jste všechna výše popsaná zabezpečení provedli v **Nastavení** vašeho Facebookového profilu, není potřeba vše nastavovat zvlášť i pro aplikaci Messenger. Ovšem jestli si chcete projít možnosti nastavení a zabezpečení účtu přímo v aplikaci, **pro přístup do hlavní nabídky stačí klepnout na vaši profilovou fotografii v levém horním rohu.**

V menu si nastavte, kdo může vidět, že jste aktivní, kdo může sledovat vaše Příběhy, případně lze využít tajné konverzace. To nejdůležitější mezi nabízenými možnostmi najdete v **Nastavení účtu**. Zde zvolte **Zabezpečení** a v následující nabídce už můžete provádět stejné změny jako ve webovém prohlížeči. Věnujte pozornost přehledu o tom, z jakého zařízení a odkud se k Messengeru přihlašujete. Pokud by se někdo neoprávněně pronikl do vašeho účtu, zde to zjistíte.



Další a podrobnější informace najdete v Centru nápovědy: www.facebook.com/help

Pro E-Bezpečí,
Lukáš Kubala

Zdroje

<https://www.e-bezpeci.cz/index.php/veda-a-vyzkum/ceske-deti-v-kybersvete-2019>

<https://www.facebook.com/help>

<https://www.e-bezpeci.cz/index.php/temata/sociotechnika/774-podvodne-platby-na-facebooku>

<https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/sociotechnikax/1253-klonovani-profilu>