DOPORUČENÍ PRO SPRÁVU SOCIÁLNÍCH SÍTÍ

verze 1.0

1. Pojmenujte oficiální účet instituce (na jakékoliv sociální síti) stejným či jasně ztotožnitelným názvem s danou institucí. V případě více sítí, potažmo účtů vyžadovaných příslušnými agendami, rovněž podle nich.

2. Oficiální účty by měly být ve správě a vlastnictví organizace tak, aby v případě personálních změn nemuselo docházet k zakládání nových účtů, či jejich přejmenovávání, které je často problematické.

3. Jasně definujte, kdo má k účtům přístup. Omezte počet jejich správců na nezbytné minimum, nezapomeňte přitom však na zastupitelnost.

4. Zaregistrujte si na sociálních sítích i alternativní názvy Vašich oficiálních účtů. Snížíte tak pravděpodobnost, že se útočníci pokusí napodobit stránku Vaší organizace, nebo se budou vydávat za oficiální účet.

5. Pro přístup do všech účtů používejte dvoufaktorovou autentizaci. Všechny velké sociální sítě ji již podporují (například Facebook, Twitter, Instagram).

6. Účty na sociálních sítích jsou obvykle svázány s e-mailovou adresou. Pro každý účet si vytvořte dedikovaný e-mail, který budete používat výhradně a pouze pro jeho správu. Do tohoto e-mailového účtu přistupujte ze zabezpečené sítě a zařízení.

7. Vyhněte se používání soukromých zařízení k přihlašování k oficiálním účtům organizace.

8. Dodržujte politiku bezpečné tvorby a užívání hesel. Pro každý účet je nutno vytvořit vlastní silné heslo.

9. Pro přihlašování nepoužívejte odkazy v e-mailu či zkracovače URL. Vyhnete se tak riziku přesměrování na podvodnou stránku.

10. Nepřihlašujte se prostřednictvím nezabezpečených či neznámých Wi-Fi sítí. Útočníci takové sítě běžně zakládají či kompromitují k zachycení přihlašovacích i jiných údajů.

11. Pro přihlašování mimo kancelář využívejte služby VPN. Díky tomu bude veškerý odchozí provoz z Vašeho zařízení šifrovaný a můžete tak předejít některým typům útoků.

12. Pravidelně aktualizujte jak zařízení, z nichž se přihlašujete, tak také aplikace, jejichž prostřednictvím sociální sítě spravujete.

13. K přistupování ke spravovaným účtům používejte pouze důvěryhodné aplikace z oficiálních zdrojů (např. Google Play nebo App Store). Zkontrolujte například, zda se jedná o renomovaného výrobce, jaké má daná aplikace hodnocení či recenze a kolik má stažení.

14. Zajistěte u všech účtů status ověřeného účtu. Zvýšíte tím jeho důvěryhodnost pro média a veřejnost.

15. Provádějte pravidelné kontroly a audity. Například zda máte správně nastavené zabezpečení účtu, nebo jaké jsou aktuální hrozby mířící na uživatele sociálních sítí.

16. Vždy kontrolujte, zda jste se z účtu bezpečně odhlásili. Při dočasném opuštění používaného zařízení a předpokladu pokračování v aktivitě na dané sociální síti zamykejte obrazovku (Win + L). Minimalizujete riziko neautorizovaného přístupu.

17. Mějte jasně nastavenou politiku užívání sociálních sítí, která v optimálním případě obsahuje i výše zmíněné.

18. Připravte si plán, jak postupovat v případě incidentu, například při ztrátě přístupu k Vašim účtům. Součástí plánu by měl být i proces reportování uvnitř Vaší organizace. V případě trestného činu je nutno jej oznámit Policii ČR. V některých případech je nezbytné požádat o spolupráci i oficiální kontakty daných sociálních sítí.

Specifikum Facebooku: V případě vytvoření stránky Vaší organizace na Facebooku dochází k jejímu spravování nepřímo skrze uživatelské účty uživatelů. **Administrátorská práva proto svažte s účtem, který vytvoříte čistě pro tento účel. Nebude tak jinak využíván ani nebude soukromým účtem zaměstnance, nýbrž bude čistě ve správě Vaší organizace.** Běžná správa oficiální stránky bude prováděna zaměstnanci skrze jejich osobní účty, které ovšem nebudou mít nejvyšší administrátorská oprávnění. Takto zajistíte, že Vaše organizace neztratí přístup k účtu například odchodem zaměstnance či úspěšným útokem vůči jednomu pracovníkovi.