Spam

U jednotlivých situací určete, jestli je zpráva spam a jestli byste s daným člověkem měli sdílet informace. Svoji odpověď na každou otázku napište na místo, které je k tomu určené.

Scénář 1

Dostanete e-mail od právníka, v němž vás informuje, že vás vzdálený příbuzný stanovil příjemcem určitého finančního obnosu. Jeho znění je následující: „Pokud chcete peníze získat, pošlete mi číslo svého bankovního účtu a identifikátor banky, abychom mohli převod peněz dokončit.“

Scénář 2

Přítel vám pošle zprávu. Píše vám, že se snaží najít fotku, kterou jste mu ukazovali, ale nemá oprávnění si ji zobrazit. Zrovna nejste u počítače, abyste mu ji mohli poslat. Odpoví vám: „Můžu se přihlásit k tvému účtu. Takhle si fotku stáhnu nejrychleji. Jaké máš heslo?“

Scénář 3

Dostanete e-mail ze školy s informací, že došlo k napadení účtů velkého počtu studentů. Budou vám tvrdit: „Nedávno jsme zaznamenali, že bylo ohroženo zabezpečení účtů mnoha studentů. Přijměte naši omluvu. Pracujeme na tom, abychom problém vyřešili. Pokud chcete svůj účet obnovit, v odpovědi na tento e-mail pošlete své uživatelské jméno a heslo.“

Scénář 4

Dostanete e-mail od vaší banky, ve které máte založený účet. E-mail obsahuje informaci o tom, že došlo k napadení jejich systému. Vyzývá vás, abyste se co nejrychleji přihlásili a změnili si heslo k tomuto účtu, ale také k dalším účtům se stejným heslem.

Spam: Verze pro školitele

U jednotlivých situací určete, jestli je zpráva spam a jestli byste s daným člověkem měli sdílet informace. Svoji odpověď na každou otázku napište na místo, které je k tomu určené.

Scénář 1

Dostanete e-mail od právníka, v němž vás informuje, že vás vzdálený příbuzný stanovil příjemcem určitého finančního obnosu. Jeho znění je následující: „Pokud chcete peníze získat, pošlete mi číslo svého bankovního účtu a identifikátor banky, abychom mohli převod peněz dokončit.“

Tento e-mail je s největší pravděpodobností spam. I když odesilatel zmiňuje skutečné jméno vašeho příbuzného, nejspíš není tím, za koho se vydává. Odesilatel mohl informace o vašem příbuzenském vztahu získat jinými prostředky. Sdílení informací o vašem bankovním účtu vždy představuje riziko, a proto byste měli být obezřetní. Své informace nikdy nikomu neposílejte, pokud dotyčného člověka nejdřív nekontaktujete. I potom ale buďte velmi opatrní. Tak například není dobrý nápad posílat své informace e-mailem, protože tato komunikace není šifrovaná. Právě z toho důvodu celá řada nemocnic, právníků a bank provozuje weby určené přímo pro komunikaci s vámi.

Scénář 2

Přítel vám pošle zprávu. Píše vám, že se snaží najít fotku, kterou jste mu ukazovali, ale nemá oprávnění si ji zobrazit. Zrovna nejste u počítače, abyste mu ji mohli poslat. Odpoví vám: „Můžu se přihlásit k tvému účtu. Takhle si fotku stáhnu nejrychleji. Jaké máš heslo?“

Není to sice spam, ale hesla byste nikdy neměli sdílet s dalším člověkem. Když bude mít někdo další vaše heslo, může vám potenciálně zablokovat přístup k účtu nebo získat přístup k dalším vašim online účtům, kde používáte stejné heslo. Pokud navíc vaši zprávu uvidí třetí strana, hacker nebo přihlížející, můžou se k vašemu účtu bez vašeho vědomí dostat další lidé.

Scénář 3

Dostanete e-mail ze školy s upozorněním, že došlo k napadení účtů velkého počtu studentů. Budou vám tvrdit: „Nedávno jsme zaznamenali, že bylo ohroženo zabezpečení účtů mnoha studentů. Přijměte naši omluvu. Pracujeme na tom, abychom problém vyřešili. Pokud chcete svůj účet obnovit, v odpovědi na tento e-mail pošlete své uživatelské jméno a heslo.“

Po uživatelích se běžně takovéto informace nepožadují. I když se odesilatel jeví věrohodně, dá se předpokládat, že e-mail vyžadující zaslání hesla je spam.

Scénář 4

Dostanete e-mail od vaší banky, ve které máte založený účet. E-mail obsahuje informaci o tom, že došlo k napadení jejich systému. Vyzývá vás, abyste se co nejrychleji přihlásili a změnili si heslo k tomuto účtu, ale také k dalším účtům se stejným heslem.

Správný postup je otevřít si nové okno prohlížeče a běžným způsobem přejít na daný web. Tento typ oznámení (o tom, že došlo k napadení účtů) by byl za normálních okolností zveřejněný na klientském portálu společnosti nebo banky. Pokyny na portálu instituce by měly vést k bezpečnému řešení problému. Žádný věrohodný subjekt po vás nebude požadovat, abyste mu e-mailem poslali přihlašovací údaje ke svému účtu, jako tomu bylo ve scénáři číslo 3.