Tipy a rady

Za pomoci těchto tipů a rad používejte na internetu vhodné bezpečnostní návyky. Tento oddíl byl vypracován v součinnosti s iniciativou Get Safe Online (Spojené království) a s Ministerstvem vnitřní bezpečnosti (USA).

- Chraňte svůj osobní počítač (PC) a přenosná zařízení
- Chraňte své osobní informace a totožnost
- Chraňte podnikové informace mimo vaši organizaci
- Připojujte se opatrně
- Buďte internetově vzdělaní

Chraňte svůj osobní počítač (PC) a přenosná zařízení

PC

- Používejte firewall: Firewally chrání vaši síť před některými viry a hackery.
- Nainstalujte si antivirový software: Antivirový software brání šíření virové infekce do vašeho počítače.
- Získejte nejnovější aktualizace zabezpečení: Udržujte své aplikace a operační systém v dobrém, zdravém a aktuálním stavu.
- Zastavte spyware: Vyhýbejte se podezřelým e-mailům a přílohám a nedovolte cizím osobám dostat se do vašeho počítače.
- Pravidelně zálohujte: Chraňte svá data před nechtěnou ztrátou a selháním.

Notebooky

- Pokud nepoužíváte nebo nepotřebujete bezdrátová připojení, vypněte je.
- Svůj notebook pravidelně připojujte k důvěryhodné síti za účelem aktualizace vašich bezpečnostních mechanismů.
- Zálohujte informace uložené na vašem notebooku.
- Neponechávejte svůj notebook bez dozoru.

USB disky

- Používejte šifrovaný USB disk.
- Pomocí fyzického přepínače uveďte USB disk do stavu umožňujícího pouze čtení s cílem zabránit přenosu virů: některé USB flash disky obsahují fyzický přepínač, kterým lze disk uvést do režimu, jenž hostitelskému počítači umožňuje pouze čtení dat a brání mu v zápisu či úpravě dat na disku.

- Po zkopírování souborů z nedůvěryhodného a/nebo neoprávněného zařízení spusťte na USB disku antivirový test s cílem zabránit přenosu virů.
- Před připojením USB disku do cizího počítače vymažte všechny soubory, které nesouvisí s cílem tohoto připojení.
- Informace na svém USB disku zálohujte tak, aby bylo možné data v případě nechtěné ztráty nebo selhání obnovit.
- Ztrátě médií zabraňte připojením USB disků na řetízek s klíči nebo na šňůrku: zmenšená velikost USB flash disků vede ke zvýšené možnosti jejich ztráty či odcizení. Vyšší paměťová kapacita dále zvyšuje potenciální objem dat ohrožených neoprávněným přístupem. USB flash disky se obvykle vkládají do tašek, batohů, obalů na notebooky, sak, kapes na kalhotách nebo se nechávají připojeny k pracovním stanicím bez dozoru. Počet případů ztráty, založení, nedovoleného vypůjčení či odcizení USB disků se v poslední době zvyšuje.

Mobilní telefony a kapesní počítače

Kapesní počítače, jako jsou zařízení Windows Mobile, Palm, iPhone, Android a Blackberry, se dodávají s možností připojení k internetu a dokáží ukládat obrovské množství informací. Již jejich snadná přenosnost znamená, že je třeba s nimi zacházet se zvýšenou opatrností.

- Pokud nepoužíváte bezdrátová připojení (tj. Bluetooth a WLAN), vypněte je. Technologie Bluetooth umožňuje elektronickým zařízením vzájemnou komunikaci pomocí rádiového spojení na krátké vzdálenosti.
- Neponechávejte svůj mobilní telefon a kapesní počítač bez dozoru. Jinak může dojít ke ztrátě dat.
- Neoprávněným vzdáleným vniknutím do vašeho smartphonu zabraňte použitím hesla.

Chraňte své osobní informace a totožnost

- **Používejte silné heslo**: Vaše heslo je na internetu ekvivalentem zámku a klíče k vašemu domu. Hesla jsou významným obranným prostředkem a vytvoření správných návyků při používání hesel vám napomůže zvýšit zabezpečení vašich citlivých osobních informací a totožnosti. Heslo k vašemu počítači je klíčem k přístupu ke všem osobním i firemním informacím, které máte uloženy ve svém počítači a v účtech na internetu. Pro ochranu svých dat používejte silné heslo: používejte složitou sadu znaků; kombinujte písmena (velká a malá), čísla a symboly. Čím pestřejší kombinaci znaků budete ve svém hesle mít, tím složitější bude ji uhádnout. Nepoužívejte osobní informace (jméno, jméno dítěte, data narození apod.), které by někdo mohl již znát nebo snadno zjistit, a snažte se nepoužívat běžná slova: někteří hackeři používají programy, které zkouší každé slovo ve slovníku.
- **Své heslo pravidelně měňte**: Domníváte-li se, že došlo k narušení bezpečnosti vašeho systému, okamžitě hesla změňte.
- **Svá hesla držte v tajnosti**: Vaše heslo je jedinečné a nesmíte je nikomu vyzrazovat. Kdykoli je to možné, snažte se svá hesla zapamatovat. Mějte strategii, jak si hesla zapamatovat.

Pokud si svá hesla zapisujete, buďte opatrní, kde je ukládáte. Neponechávejte tyto záznamy svých hesel nikde, kde byste neponechali informace, které tato hesla chrání.

- **Jeden účet, jedno heslo:** Ke každému účtu na internetu, k němuž přistupujete, používejte jiné heslo (nebo mějte alespoň několik různých hesel). Používáte-li stejná hesla u více účtů, bude útočník, který získá přístup k jednomu účtu, schopen vstoupit do všech vašich účtů.
- **Své účty zabezpečte:** Řada poskytovatelů účtů nabízí doplňující způsoby, jimiž se před tím, než se na stránce začnete pohybovat, ověřuje, kdo jste.
- **Buďte pány své přítomnosti na internetu**: Kdykoli je to možné, upravte nastavení soukromí a zabezpečení na stránkách na takovou úroveň sdílení informací, která vám vyhovuje. Je vhodné omezit okruh osob, s nimiž informace sdílíte.
- **Sociální sítě používejte opatrně**: Buďte si vědomi toho, že stránky sociálních sítí mohou často spojovat mnoho rizik spojených s přítomností na internetu: šikanu na internetu, vyzrazení soukromých informací, kyberstalking, přístup k obsahu neodpovídajícímu věku uživatele a v nejkrajnějších případech tzv. grooming a zneužívání dětí prostřednictvím internetu.

Chraňte podnikové informace mimo vaši organizaci

- **Zajistěte trvalé zabezpečení citlivých informací**: Pohybujete-li se mimo svou organizaci, zajistěte, aby byly vaše citlivé informace a zařízení neustále v bezpečí, aby nedošlo k jejich odcizení či ztrátě. Zejména pokud se nacházíte na veřejných místech, zacházejte s informacemi opatrně.
- **Zachovávejte důvěrný charakter podnikových informací**: Uvědomujte si, že někdo může vaši konverzaci zaslechnout. Důvěrné informace vaší organizace nikomu nezpřístupňujte.
- **Uvědomujte si možnost nahlížení přes rameno**: Při cestách nebo práci ze vzdáleného místa se chraňte před nahlížením přes rameno (tzv. „shoulder surfing“).
- **Webmail používejte s rozmyslem**: Použití internetového prohlížeče ke čtení pošty vyžaduje stejnou opatrnost jako použití e-mailových počítačových klientů a navíc skýtá několik vlastních bezpečnostních rizik.

Připojujte se opatrně

- **Pokud nepoužíváte nebo nepotřebujete bezdrátová připojení, vypněte je.**
- **Wi-Fi hotspoty používejte s rozumem**: Při použití Wi-Fi hotspotů omezte typ prováděných činností a úpravou nastavení zabezpečení vašeho zařízení omezte okruh osob, které mohou mít k vašemu přístroji přístup.
- **Chraňte své peníze:** Při internetovém bankovnictví nebo při nákupech na internetu zkontrolujte, zda mají stránky aktivováno zabezpečení. Hledejte internetové adresy obsahující „https://“ nebo „shttp://“, což znamená, že stránka používá dodatečná opatření, která pomáhají zabezpečit vaše informace. Protokol „http://“ není zabezpečený.
- **Zastavte nevyžádané e-maily**: Spamové e-maily jsou bezpečnostní hrozbou. Neotvírejte neznámé e-maily a přílohy.

- **V případě pochybností zprávu vymažte**: Jestliže odkazy v e-mailech, tweetech, příspěvcích a reklamách na internetu vypadají podezřele, a to i pokud znáte zdroj, je nejlepší zprávu vymazat nebo v příslušných případech označit jako nevyžádaný e-mail.
- **E-mail přepošlete, pokud je to vhodné**. Před přeposláním zprávy zvažte možnost vymazat historii této zprávy.
- **Na internetu surfujte opatrně.**
- **Nestahujte dokumenty a materiály od nedůvěryhodných stran.**
- **Veřejně přístupné počítače používejte opatrně:** K veřejně přístupnému počítači se připojujte, pouze pokud máte šifrované připojení (označené v okně prohlížeče vpravo dole symbolem visacího zámku a písmeny „https://“ na začátku internetové adresy).
- **Používejte webmailové služby známých a důvěryhodných společností.**

Buďte internetově vzdělaní

- **Mějte aktuální informace:** Držte krok s novými způsoby zajištění bezpečnosti na internetu: na důvěryhodných internetových stránkách sledujte nejnovější informace, podělte se o tyto informace s rodinou, přáteli a kolegy a podporujte jejich internetovou vzdělanost. Zabezpečte svůj internetový prohlížeč.
- **Nejdříve myslete, až pak jednejte**: Buďte opatrní u sdělení, která vás vyzývají k okamžitému jednání, nabízejí něco, co zní až příliš lákavě, nebo požadují osobní informace.
- **Zálohujte**: Chraňte svou práci, hudbu, fotografie a další digitální informace vytvořením a bezpečným uložením elektronické kopie.