Tipy a rady

Na základe týchto tipov a rád si môžete osvojiť vhodné bezpečnostné návyky pri práci na internete. Túto sekciu sme vypracovali v koordinácii so službou Get Safe Online (Spojené kráľovstvo) a Ministerstvom vnútornej bezpečnosti USA.

- Ochrana počítačov a prenosných zariadení
- Ochrana osobných údajov a identity
- Ochrana obchodných informácií mimo vašej organizácie
- Opatrnosť pri pripájaní
- Rozvážnosť na webe

Ochrana počítačov a prenosných zariadení

Počítač

- Používajte zariadenie firewall: zariadenia firewall chránia sieť pred niektorými vírusmi a hakermi.
- Nainštalujte si antivírusový softvér: antivírusový softvér zabraňuje šíreniu vírusov v počítači.
- Nainštalujte si najnovšie aktualizácie zabezpečenia: uchovávajte aplikácie a operačný systém v bezpečnom a aktuálnom stave.
- Zastavte spyware: vyhýbajte sa podozrivým e-mailom a prílohám a zabráňte cudziemu prístupu k vášmu počítaču.
- Pravidelne zálohujte: chráňte svoje údaje pred katastrofou.

Notebooky

- Vypínajte bezdrôtovú komunikáciu, keď sa nepoužíva alebo nevyžaduje.
- Notebook pravidelne pripájajte k dôveryhodnej sieti na aktualizáciu mechanizmov zabezpečenia.
- Zálohujte údaje uložené v notebooku.
- Nenechávajte svoj notebook bez dozoru.

Kľúče USB

- Používajte šifrovaný kľúč USB.
- Prepnite kľúč USB do režimu iba na čítanie pomocou fyzického prepínača, aby sa zabránilo prenosu vírusov: niektoré kľúče USB obsahujú fyzický prepínač na prepnutie do režimu len na čítanie, aby hostiteľský počítač nemohol zapisovať údaje na disk ani upravovať údaje na disku.

- Po skopírovaní súborov z nedôveryhodného alebo neautorizovaného počítača skontrolujte kľúč USB pomocou antivírusového softvéru, aby sa zabránilo prenosu vírusu.
- Pred zapojením do cudzieho počítača odstráňte z kľúča USB všetky súbory, ktoré sa netýkajú daného úkonu.
- Zálohujte si údaje na kľúči USB, aby ste ich v prípade zlyhania mohli obnoviť.
- Pripojte si kľúče USB na remienok alebo kľúčenku, čím zabránite ich strate: kľúče USB sú malé, ľahko sa teda strácajú alebo odcudzujú. Vyššie pamäťové kapacity navyše znamenajú, že možnému neoprávnenému prístupu bude vystavené väčšie množstvo údajov. Kľúče USB sa zvyčajne vkladajú do kabeliek, ruksakov, obalov na notebook, sák, vreciek nohavíc alebo sa zabudnú vložené v počítači. V poslednom čase dochádza k čoraz väčšiemu počtu strát, krádeží, zabudnutiu alebo požičaniu kľúčov USB bez dovolenia.

Mobilné telefóny a vreckové počítače

Vreckové počítače, ako sú napríklad zariadenia Palm, iPhone, Blackberry alebo zariadenia so systémom Windows Mobile či Android, obsahujú internetové odkazy a umožňujú uložiť obrovské množstvo údajov. Ich veľmi jednoduchá prenosnosť znamená, že je potrebné narábať s nimi nanajvýš opatrne.

- Vypnite bezdrôtové pripojenia (Bluetooth a Wi-Fi), keď sa nepoužívajú. Technológia Bluetooth umožňuje vzájomnú komunikáciu medzi elektronickými zariadeniami prostredníctvom rádiového spojenia s krátkym dosahom.
- Nenechávajte svoj mobilný telefón a vreckový počítač bez dozoru. Mohlo by to mať za následok stratu údajov.
- Pred neoprávneným vniknutím do smartfónu sa chráňte pomocou hesla.

Ochrana osobných údajov a identity

- **Používajte bezpečné heslo:** Heslo je na internete ekvivalentom zámku a kľúča na dome. Heslá sú najdôležitejšou ochranou a vytvorením dobrých návykov v oblasti hesiel dokážete uchovávať citlivé osobné údaje a identitu v bezpečí. Heslo do počítača je prístupovým kľúčom ku všetkým informáciám – podnikovým aj osobným – ktoré máte uložené v počítači alebo kontách online. Na ochranu svojich údajov používajte bezpečné heslá: zložité reťazce znakov – kombinujte písmená (malé aj veľké), čísla a symboly. Čím rôznorodejšie znaky v hesle, tým zložitejšie je uhádnutie hesla. Nepoužívajte osobné údaje (svoje meno, meno dieťaťa, dátumy narodenia a pod), ktoré by už niekto mohol poznať alebo jednoducho uhádnuť. Takisto sa snažte vyhýbať normálnym slovám: niektorí hakeri používajú programy, ktoré skúšajú každé slovo v slovníku.
- **Heslo pravidelne meňte:** Ak si myslíte, že došlo k napadnutiu alebo ohrozeniu systému, okamžite si zmeňte heslo.
- **Uchovávajte heslo v tajnosti:** Vaše heslo je jedinečné a nesmiete ho nikomu prezradiť. Vždy, keď je to možné, snažte sa pamätať si heslá. Majte stratégiu na ich zapamätanie. Ak si

svoje heslá zapíšete, dávajte si pozor na to, kam si ich ukladáte. Nenechávajte si záznamy o heslách tam, kde sa nachádzajú aj informácie, ktoré sa nimi majú chrániť.

- **Iné heslo pre každé konto:** Pre každé konto online používajte iné heslo (alebo aspoň niekoľko rôznych hesiel). Ak budete mať rovnaké heslo na viacerých kontách, haker, ktorý získa prístup, k jednému kontu, bude môcť získať prístup ku všetkým vašim kontám.
- **Zabezpečte si kontá:** Mnohí poskytovatelia kont ponúkajú ďalšie spôsoby overenia totožnosti pred uskutočnením činnosti na daných stránkach.
- **Majte kontrolu nad nastaveniami ochrany súkromia:** Ak je to možné, nastavte si ochranu osobných údajov a zabezpečenie na webových stránkach podľa vlastných požiadaviek spoločného používania informácií. Je vhodné obmedziť počet osôb, s ktorými sa delíte o informácie.
- **Sociálne siete používajte opatrne:** Majte na pamäti, že sociálne siete môžu skrývať mnohé riziká súvisiace s internetom: zastrašovanie online, zverejňovanie súkromných informácií, kybernetické sledovanie, prístup k vekovo nevhodnému obsahu až po online grooming (nadväzovanie vzťahov s deťmi) a zneužívanie detí.

Ochrana obchodných informácií mimo vašej organizácie

- **Dbajte o bezpečnosť citlivých informácií:** Keď ste mimo organizácie, uchovávajte citlivé údaje a zariadenia, v ktorých sa nachádzajú, v bezpečí a predchádzajte odcudzeniu alebo strate. S informáciami narábajte obzvlášť opatrne, najmä keď sa nachádzate na verejných priestranstvách.
- **Zachovávajte dôvernosť všetkých obchodných informácií:** Majte na pamäti, že niekto môže nechtiac začuť váš rozhovor. Nedovoľte, aby sa k dôverným informáciám vašej spoločnosti dostal ktokoľvek.
- **Dávajte si pozor, aby vám nikto nepozeral cez plece:** Pri cestovaní alebo práci na diaľku si dávajte pozor, aby vám nikto nepozeral cez plece.
- **Používajte webový e-mail obozretne:** Používanie internetového prehliadača na čítanie e-mailov vyžaduje rovnakú opatrnosť ako používanie samostatných programov, dokonca zahŕňa niekoľko ďalších bezpečnostných rizík.

Opatrnosť pri pripájaní

- **Vypínajte bezdrôtovú komunikáciu, keď sa nepoužíva alebo nevyžaduje.**
- **Správajte sa uvážlivo pri pripojení cez verejný prístupový bod Wi-Fi:** Pri používaní verejných prístupových bodov Wi-Fi obmedzte typ vykonávaných činností a upravte nastavenie zabezpečenia zariadenia tak, aby sa do vášho počítača nemohol dostať ktokoľvek.
- **Chráňte svoje peniaze:** Pri internetovom bankovníctve alebo nakupovaní skontrolujte, či stránky podporujú zabezpečenie. Sledujte, či sa webové adresy začínajú na „https://“ alebo „shttp://“, čo znamená, že tieto stránky používajú dodatočné opatrenia na lepšie zabezpečenie vašich informácií. Iba „http://“ nie je bezpečné.

- **Predchádzajte neželaným e-mailom:** Nevyžiadané e-maily predstavujú ohrozenie zabezpečenia. Neotvárajte neznáme e-maily ani prílohy.
- **Ak máte pochybnosti, vymažte to:** Ak odkazy v e-mailoch, tweetoch, príspevkoch a internetových reklamách vyzerajú podozrivo, je lepšie odstrániť ich alebo označiť ako nevyžiadanú poštu napriek tomu, že poznáte jeho zdroj.
- **Kým pošlete e-mail ďalej, zvážte, či je to vhodné**. Takisto zvážte odstránenie histórie správy a pošlite iba samotný obsah, nie predchádzajúcich odosielateľov a príjemcov.
- **Surfujte na internete opatrne.**
- **Nepreberajte dokumenty a materiály od nedôveryhodných strán.**
- **Používajte verejné počítače opatrne:** Na verejných počítačoch sa pripájajte, len ak máte šifrované pripojenie (označené ikonou zámku v pravom dolnom rohu okna prehliadača a písmenami „https://“ na začiatku adresy webovej stránky).
- **Používajte služby webového e-mailu od známych a dôveryhodných spoločností.**

Rozvážnosť na webe

- **Uchovávajte počítač v aktuálnom stave:** Držte krok s novými spôsobmi bezpečnosti na internete: vyhľadávajte najnovšie informácie na dôveryhodných webových stránkach a informujte aj členov rodiny, priateľov a kolegov a nabádajte ich k rozvážnosti. Uchovávajte bezpečnosť webového prehliadača.
- **Najskôr rozmýšľajte, potom konajte:** Buďte opatrní, ak niekto od vás vyžaduje okamžitú akciu, ponúka niečo, čo znie príliš dobre na to, aby to bola pravda, alebo žiada o osobné údaje.
- **Zálohujte:** Chráňte svoju prácu, hudbu, fotografie a ďalšie digitálne informácie zhotovovaním elektronických kópií a ich bezpečným ukladaním.