Průvodce on-line bezpečností

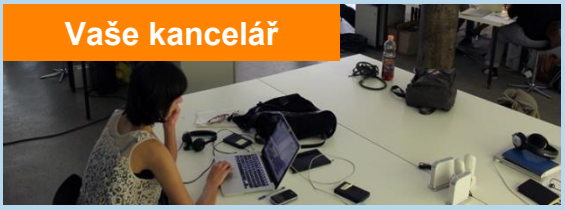
12 jednoduchých tipů jak být v bezpečí on-line

Tento průvodce je vytvořen speciálně pro neziskové organizace.

Jako nezisková organizace často spoléháte na štědrost a dobrou vůli svých dárců, podporovatelů a dalších partnerů. A oni zase spoléhají na Vás a na to, že všechna Vaše data a informační infrastruktura je v bezpečí. Tento průvodce je vytvořen právě proto, aby Vám umožnil toto bezpečí maximalizovat.

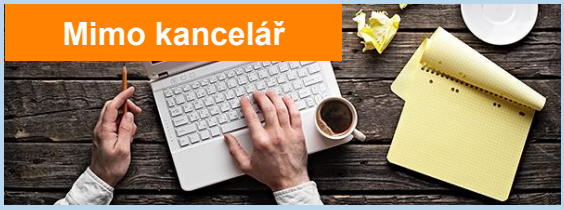
Těchto 12 tipů se věnuje čtyřem základním prostředím

Vaše kancelář



Základní pravidla, která byste měli dodržovat a na která byste vy a Vaši kolegové měli myslet během každodenní činnosti.

Mimo kancelář



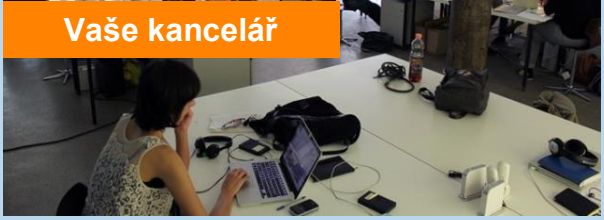
Přenosná zařízení a veřejné wi-fi sítě? Máme pro Vás tipy, jak zajistit co největší on-line bezpečnost i mimo Vaši kancelář.

Sociální sítě

Sociální sítě jsou nejčastěji navštěvovanými stránkami. Dávejte si pozor na to, co zde publikujete – v pracovní i osobní rovině.

Cloudové prostředí

Online aplikace ukládají Vaše data na internetu. Podívejte se, jak zajistit, aby všechna Vaše data zůstala v bezpečí i online.



1 Neusnadňujte to hackerům!

Používejte hesla chytře. Po fyzické bezpečnosti Vaší kanceláře jsou hesla druhou nejdůležitější věcí, kterou je třeba rozmýšlet. Používejte tzv. „silná“ hesla, která kombinují velká písmena s malými, čísla a další symboly. To Vám pomůže zabránit útoku hackerů, kteří používají náhodné i systematické odhady běžně užívaných slov. Kromě toho:

- Používejte různá hesla pro různé stránky. Pro zapamatování pak můžete použít programy pro správu hesel.
- Pro zamezení neautorizovanému přístupu k Vašim datům můžete také namísto snadno dostupných informací (Vaše datum narození, model Vašeho prvního auta, jméno Vaší kočky) jako heslo použít reálnou, nicméně ne tak snadno pochopitelnou informaci (model auta Vašeho souseda, barva Vaší kočky apod.)

Aktualizujte svůj software. Hackeři využívají zranitelnosti běžně užívaného softwaru – operačního systému, kancelářského software či prohlížečů -, která se zvyšuje používáním zastaralých verzí. Proto:

- nezapomeňte pravidelně aktualizovat Vaše programy, ideálně nastavte automatické aktualizace.
- instalujte na veškeré počítače ve Vaší organizaci anti-malware software. Pokud používáte počítače napojené do sítě, instalujte software, který Vašim počítačů zaručí bezpečnost na podnikové úrovni a bude spravovat veškeré aktualizace

Blokujte spam. Základem je dobrý „vychytávač“ spamu. Spam je stále nejběžnější cestou, skrze kterou může být Váš počítač napaden virem či poskytnout útočníkovi citlivé informace.

2 Odraďte útočníky

Vyhněte se sociálnímu inženýrství. I přesto, že máte „silná“ hesla, můžete být pomocí sociálního inženýrství různými triky zmanipulování k poskytnutí citlivých údajů. Abyste se vyhnuli takovým podvodům:

- Neposkytujte osobní údaje skrze e-mail či telefon. Pokud tak činíte, odpovídejte pouze na ověřené a důvěryhodné adresy a čísla.
- Pozor na neosobní e-maily, chybně napsaná slova, odkazy na nesouvisející či podezřelé webové stránky či příliš „výhodné“ nabídky.

Pozor na ransomware. Ransomware je typ malwaru, který je vytvořen za účelem podvést nic netušící uživatele a přesvědčit je, že jejich zařízení je infikováno virem a měli by proto zaplatit poplatek za stažení softwaru, který jejich počítač vyčistí. Spoléhejte pouze na ověřené anti -virové programy.

Pohybujte se ve světě internetu bezpečně. Před tím než poskytnete jakékoliv finanční či osobní údaje, přesvědčte se, že webová stránka, na kterou vstupujete, je řádně zabezpečená. URL bezpečné stránky začíná na https://. Ověřená stránka má rovněž často v adresním řádku zelené pozadí (zde záleží na prohlížeči, který používáte). Zvažte také vytvoření zvláštního uživatelského účtu, který by byl využíván pouze pro finanční transakce Vaší organizace (mzdy, dárcovské platby atp.). Počítač či uživatelské účet provozovaný pouze za tímto účelem by ideálně měl mít minimální přístup k internetu a zamezený přístup k e-mailu.

3 Vytvořte metodiku pro zaměstnance a dobrovolníky

Všichni zaměstnanci a dobrovolníci by si měli přečíst tohoto průvodce. Kromě toho by měli být také informováni o všech aktuálních bezpečnostních rizicích. Ideálně také:

- Vytvořte pravidla pro hesla ve Vaší organizaci a ujistěte se, že Vaši spolupracovníci svá hesla pečlivě střeží.
- Nezapomeňte o bezpečnostních rizicích a jejich možném zmírnění vyškolit nové zaměstnance či dobrovolníky.
- Ustanovte přijatelná pravidla pro používání počítačů a mobilních zařízení a ujistěte se, že každý pracovník tyto pravidla četl a porozuměl jim. Pravidla by měla obsahovat možnosti zacházení se zařízeními (co zde může být pracovníky nainstalováno a ukládáno, co je případně dovoleno na zařízení dělat po pracovní době apod.). Pravidla by zároveň měla ošetřit případy ztráty či odcizení zařízení.

4 Zajistěte mobilní zařízení a vzdálené pracovní stanice

Laptopy, tablety a mobilní telefony mohou být snadno ztraceny nebo ukradeny. Z toho důvodu:

- by mobilní zařízení nikdy neměla být jediným úložištěm důležitých dat.
- stejně jako u kancelářských počítačů zamezte náhodnému přístupu k Vašemu mobilnímu zařízení použitím PIN, hesla či biometriky.
- Všechna zařízení, která mohou být ztracena či odcizena, (včetně laptopů) by měla být zašifrována.
- Pozor na malware a aplikace vytvořené za účelem odcizení informací z Vašeho zařízení. Řádně rozmyslete instalaci jakékoliv aplikace a stahujte aplikace pouze z ověřených zdrojů.
- GPS a lokační nástroje na svých tabletech a telefonech využívejte pouze, pokud to opravdu potřebujete. Mohou Vám sice usnadnit práci, nicméně uvedení lokace u Vašeho statusu či obrázku může dát hackerům také zásadní informace pro sociální inženýrství.

Pokud je vaše zařízení ztraceno či odcizeno:

- Můžete ho zkusit najít prostřednictvím funkce Phone Finder
- Pokud ho takto najít nelze, lze v některých případech vzdáleně vymazat data ze zařízení, za předpokladu, že je on-line.

5 Buďte ostražití při používání veřejných počítačů

Každý veřejný počítač představuje potenciální bezpečnostní riziko – počítače na letištích nebo v obchodních centrech či internetové kavárny. Tyto počítače by měly být nastaveny na tzv. „kiosk mode“, v kterém nejsou ukládána žádná data, nicméně nikdy automaticky nepředpokládejte, že je počítač takto nastaven.

Pokud používáte veřejný počítač:

- Nikdy ho nepoužívejte k zadávání finančních transakcí
- Přistupujte ke své e-mailové schránce a k účtu sociálních médií v modulu „anonymní okno“, v rámci kterého si Váš prohlížeč nepamatuje jakoukoliv historii a neukládá tak žádná data. Anonymní okno otevřete jednoduše v nabídce Nastavení každého prohlížeče.

Ve veřejných prostorách je třeba dbát také o fyzickou bezpečnost:

- Nenechávejte nikde počítač bez dohledu s citlivými údaji na obrazovce
- Nezapomeňte, že to, co se děje na Vaší obrazovce může přes Vaše rameno někdo pozorovat.
- Nikdy nevkládejte externí a jiné disky do veřejných počítačů.

6 Buďte opatrní při používání veřejné Wi-Fi

Stejně jako veřejné počítače i veřejné Wi-Fi sítě jsou potenciální hrozbou.

- Používejte veřejné Wi-Fi sítě pouze pro běžné prohlížení Internetu, při kterém nepracujete s citlivými daty.
- Nikdy nezadávejte finanční a osobní transakce skrze veřejnou Wi-Fi
- Zvažte vždy bezpečnější variantu – např. zda s potřebnou osobou nemůžete mluvit osobně či po telefonu.

Pokud se musíte připojit k veřejné Wi-Fi síti:

- Připojujte se k sítím, které mají alespoň určitý stupeň ochrany. Takové sítě u svého názvu mají vždy ikonu zámku a před připojením se požadují zadání hesla či alespoň souhlas s určitými pravidly a podmínkami.
- Buďte opatrní, pokud je Vám na zařízení nabídnuto více dostupných sítí s podobnými názvy. Některé mohou být vytvořeny za účelem získat Vaše provozní data. Pokud si nejste jisti, vždy se zeptejte oprávněné osoby na to, která je ta „správná“ síť.

Pokud se chcete vyhnout těmto problémům s připojováním k veřejným sítím, nicméně řada Vašich zaměstnanců a spolupracovníků často pracuje na dálku, zvažte zřízení virtuální privátní sítě (VPN).

7 Sociální sítě jsou sociální (ne „soukromé“)

Je důležité pochopit, že cokoliv, co je online, je trvalé a přenositelné. Informace, které sdílíte a poskytujete na sociálních sítích, jsou dostupné také např. inzerentům a často jsou tyto informace více veřejně dostupné, než se může zdát.

Pokud používáte sociální média, nezapomínejte:

- Promyslet, jak moc veřejný by měl být Váš profil a informace na něm.
- Prozkoumat a vyhodnotit každou stránku a zvláště její nastavení soukromí před tím, než ji začnete používat.
- Nastavit potřebná omezení při sdílení příspěvků
- Důkladně vybírat osoby, které označíte jako „přátele“
- Být opatrní, pokud se máte osobně setkat s někým, s kým jste se poprvé setkali online, ať již z osobních či pracovních důvodů. Takové setkání si dohodněte na veřejném místě a informujte další osoby o tom, kde jste.

Nezapomínejte: Sociální média jsou velmi oblíbená v rámci phishingu a sociálního inženýrství. (Za phishing se označují pokusy získat citlivé údaje jako uživatelská jména, hesla, údaje kreditních karet [někdy take nepřímo peníze]. Útočník, tzv. “phisher”, se v elektronické komunikaci maskuje jako důvěryhodná osoba.) Lidé totiž považují často příspěvky svých přátel na sociálních sítích za velmi důvěryhodné a vykazují mnohem menší míru obezřetnosti než je tomu u e-mailových zpráv či webových stránek.

8 Pozor na to, co sdílíte!

Osobní údaje mohou být zneužity k podvodům či Vašemu vysledování. Sdílené údaje mohou rovněž ovlivnit Vaše nynější i budoucí pracovní postavení a mohou vrhat špatné světlo na Vaši organizaci.

Pro ochranu Vašeho soukromí, bezpečnosti a reputace:

- Sdílejte pouze příspěvky, které by Vám nevadilo sdílet a slyšet na veřejnosti.
- Nepřispívejte nevhodnými fotografiemi, videy či komentáři.
- Pokud používáte lokační nástroje, zvažte, kdo všechno k těmto údajům bude mít přístup. Detaily o tom, kde se právě nacházíte, mohou být snadno zneužity pro kriminální činnost. Snadno tak můžete být pronásledováni nebo okradeni.

9 Zacházejte opatrně s profilem Vaší organizace na sociálních sítích

Věnujte speciální pozornost a péči tomu, kdo dává jaké příspěvky na stránku Vaší organizace. Každý nový zaměstnanec či dobrovolník, který bude sdílet příspěvky, by měl dobře porozumět, co se od něj očekává.

- Pracovníci by měli být upozorněni, že jejich příspěvky či odpovědi na sociálních sítích by měly odpovídat organizační kultuře a hodnotám. Z toho důvodu je vhodné vytvořit dokument s pravidly pro sociální média.
- Pokud stránku používá více uživatelů, je dobré stanovit, kdo kdy.
- Některá sociální média umožňují přiřadit uživatelům různé role s různými úrovněmi privilegií. Využijte toho a přiřaďte pracovníkům vhodné role.
- Pokud někoho označíte v příspěvku na své stránce, můžete o něm nevědomky poskytnout více informací, než si myslíte a než on sám chce. Používejte tedy tuto funkci opatrně.
- Rozmažte obličeje osob na fotografiích a videích, pokud jste od těchto osob neobdrželi výslovné povolení k publikaci příspěvků.

10 Věnujte zvláštní pozornost přihlašovacím údajům a zvažte omezení přístupu ke sdíleným dokumentům

Pokud Vaše organizace využívá cloudové služby, každá osoba s potřebnými údaji bude moci přistupovat k těmto službám. Každý zaměstnanec či dobrovolník by proto měl mít své vlastní jedinečné přístupové údaje.

Většina služeb požaduje tzv. dvoufaktorovou autentizaci, kde přístupové údaje musí být potvrzeny pomocí dalšího zařízení jako je např. mobilní telefon. Pokud je to možné, využívejte tuto funkci pro zvýšení bezpečnosti.

Uživatelé by měli věnovat pozornost také tomu, kdo může přistupovat k on-line dokumentům a složkám. Tyto dokumenty jsou navrženy tak, aby mohly být snadno sdíleny. Ujistěte se, že pozvánka ke sdílení dokumentu je vždy poslána správným osobám a zvažte, zda tyto osoby mají mít práva ke čtení i úpravám dokumentu.

11 Seznamte se s pravidly a podmínky poskytovatele cloudové služby

Při využívání cloudových služeb byste měli být seznámeni zvláště s pravidly a podmínkami vztahujícími se k vlastnictví dat a jejich umístění.

Pokud by oficiální úřady požádaly poskytovatele cloudových služeb o Vaše data, budou jim s největší pravděpodobností předána. Pokud s takovým postupem Vaše organizace nesouhlasí, není pravděpodobně cloud pro Vás to pravé.

V takovém případě si organizace může pořídit tzv. soukromý či hybridní cloud, kde si organizace může vybrat úroveň exkluzivity a vyhnout se tak nechtěnému předávání dat ze strany provozovatele cloudových služeb.

12 Zálohujte offline

Zálohové služby online mohou být na čas vyřazeny z provozu a vy se pak nedostanete ke svým dokumentům. Zvažte proto, jaká data dáváte „do cloudu“ a jak Vaši organizaci může ovlivnit jejich nedostupnost.

Kopie nejdůležitějších dokumentů si stahujte do počítače, tak aby pro Vás byly dostupné i při výpadku cloudových služeb. Vaše data by u většiny cloudových služeb měla být exportována v běžně dostupných formátech. Pokut Vaše služby tuto možnost nenabízejí, zvažte přechod k jinému poskytovateli.

V úložišti dokumentů naleznete často historii verzí, kde můžete spravovat jednotlivé verze. Pravidelně kontrolujte tento odkaz a zbystřete při podezřelém chování.