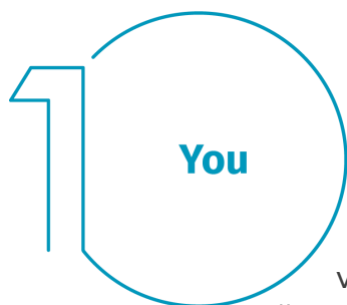


5 nejlepších kroků pro bezpečnou práci z domova

Víme, že práce z domova může být pro některé z vás novinkou, která vás možná zahltí, jak se budete přizpůsobovat novému prostředí. Jedním z našich cílů je umožnit vám pracovat z domova co možná nejbezpečněji. Níže je pět jednoduchých kroků pro bezpečnou práci. Nejlepší na tom je, že tyto kroky vám pomohou nejen zabezpečit práci, ale také ochrání vás a vaši rodinu, neboť si vytvoříte kyber zabezpečený domov.



Vy: Důležité je podotknout, že samotná technologie vás neochrání – tou nejlepší ochranou jste vy. Útočníci zjistili, že nejjednodušší způsob, jak získat, co chtějí, je zaměřit se přímo na vás namísto vašeho počítače či ostatních zařízení. Pokud chtějí vaše heslo, pracovní data či kontrolu nad vaším počítačem, pokusí se vás oklamat, abyste jim je dali – často tak, že vytvoří pocit naléhavosti. Například vám zavolají, budou se vydávat za technickou podporu Microsoftu a budou tvrdit, že váš počítač je infikovaný. Anebo vám třeba pošlou e-mailem varování, že nějaký balíček nemohl být doručen, čímž vás oklamou a přimějí kliknout na škodlivý odkaz. Mezi nejčastější známky útoku využívajícího sociální inženýrství patří:

- Někdo, kdo vytváří obrovský pocit naléhavosti, často prostřednictvím strachu, zastrašování, krize či důležitého termínu. Kyber útočníci umí dobře vytvářet přesvědčivé zprávy, které vypadají, že pocházejí z důvěryhodných organizací, jako jsou banky, vláda či mezinárodní organizace.
- Tlak na to, abyste obešli či ignorovali bezpečnostní pravidla či postupy, nebo až příliš výhodná nabídka (ne, v žádné loterii jste nevyhráli!).
- Zpráva od přítele či kolegy, jejíž podpis, znění či tón se jeho stylu nepodobá.

Vůbec tou nejlepší obranou proti těmto útokům jste vy.

2 Home Network

Domácí síť: Prakticky každá domácí síť začíná u bezdrátové sítě (často se jí říká Wi-Fi). Díky ní můžete všechna svá zařízení připojovat k internetu. Většinu domácích bezdrátových sítí ovládá internetový router nebo samostatný bezdrátový přístupový bod. Obojí funguje stejně: vysílají bezdrátové signály, na které se domácí zařízení připojují. To znamená, že zabezpečení vaší bezdrátové sítě je klíčovou součástí ochrany vašeho života. V rámci jejího zabezpečení doporučujeme tyto kroky:

- Změnit výchozí administrátorské heslo u zařízení, které ovládá vaši bezdrátovou síť. Administrátorský účet vám umožňuje spravovat nastavení bezdrátové sítě.
- Postarejte se, aby se k vaší bezdrátové síti mohli připojit pouze lidé, kterým věříte. To uděláte tak, že povolíte silné zabezpečení. Když ho povolíte, budou lidi pro připojení k vaší bezdrátové síti potřebovat heslo, a když se připojí, jejich online aktivita bude šifrovaná.
- Postarejte se, aby heslo, kterým se budou lidé připojovat k vaší bezdrátové síti, bylo silné a jiné než administrátorské heslo. Pamatujte, že na každém zařízení musíte heslo zadat pouze jednou, neboť si heslo uloží a zapamatují.

Nevíte, jak tyto kroky provést? Zeptejte se svého poskytovatele internetu, podívejte se na jeho stránky, přečtěte si dokumentaci pro svůj bezdrátový přístupový bod nebo se podívejte na stránky prodejce.

3 Passwords

Hesla: Když vás nějaká stránka požádá o vytvoření hesla: Vytvořte silné heslo – čím víc znaků má, tím je silnější. Jedním z nejjednodušších způsobů, jak mít jistotu, že máte silné heslo, je použít heslovou frázi. Heslová fráze není nic jiného než heslo složené z několika slov, jako třeba "*med krupice whiskey*." Používání jedinečné heslové fráze znamená používat jinou frázi pro každé zařízení či online účet. Pokud totiž bude jedna z heslových frází prozrazena, všechny vaše ostatní účty a zařízení budou nadále v bezpečí. Nedokážete si všechny heslové fráze zapamatovat?

Používejte správce hesel, což je specializovaný program, který bezpečně ukládá všechny vaše heslové fráze v zašifrovaném formátu (a má spoustu dalších skvělých funkcí!). A nakonec povolte dvoufázové ověření (také známé jako dvoufaktorové ověření či ověření ve více krocích), kdykoliv je to možné. To

používá vaše heslo, ale zároveň přidává druhý krok, jako třeba kód odeslaný na chytrý telefon nebo aplikaci, která vám kód vygeneruje. Dvoufázové ověření je dost možná ten nejdůležitější krok, kterým můžete chránit své online účty, a je mnohem snazší, než si možná myslíte.

4 Updates

Aktualizace: Zkontrolujte si, jestli všechny vaše počítače, mobilní zařízení, programy a aplikace používají nejnovější verzi softwaru. Kyber útočníci neustále hledají nové slabiny v softwaru, který vaše zařízení používají. Když takové slabiny odhalí, používají speciální programy, aby je využili a nabourali se do zařízení, která používáte. Firmy, které software pro zařízení vytvářejí, se mezitím tyto slabiny snaží opravit vydáváním aktualizací. Když se postaráte, aby si je vaše počítače a mobilní zařízení neprodleně nainstalovaly, bude pro ostatní mnohem těžší vás hacknout. Abyste zůstali aktuální, stačí povolit automatické aktualizace, kdykoliv je to možné. Toto pravidlo platí pro prakticky jakoukoliv technologii připojenou k síti, nejen včetně vašich pracovních zařízení, ale i televizí, chůviček, bezpečnostních kamer, domácích routerů, herních konzolí i vašeho auta, pokud se dokážou připojit k internetu.

5 Kids & Guests

Děti / Hosté: V kanceláři si nejspíš nemusíte dělat hlavu s tím, že váš pracovní notebook či jiná pracovní zařízení budou používat děti, hosté či ostatní členové rodiny. Postarejte se, aby vaše rodina a přátelé chápali, že nesmí používat vaše pracovní zařízení, protože by mohli omylem smazat či modifikovat data anebo ještě hůř, vaše zařízení nechtěně infikovat.