Nouzový stav

Bezpečné chování při práci z domova

AEC

Pracujete z home office?
Dodržujete doporučení svého zaměstnavatele a vlády?

Aktuální situace nás nutí pracovat z domova. Internet je však plný nástrah a kyberzločinci jen v klidu čekají na vaši sebemenší nepozornost.

Neztrácejte obezřetnost. Můžete přijít o své osobní údaje, finance, ale také můžete zavirovat celou firemní síť.

Zvýšený počet bezpečnostních incidentů je v tomto období prokázaný.

Dále uvádíme základní pravidla pro práci z domova.

Znáte bezpečnostní směrnici?

Většina firem pamatuje na práci mimo kancelář ve své **bezpečnostní směrnici**.
I když se to může zdát jako nudné čtení, znovu si ji projděte.

Něčemu nerozumíte? Kontaktujte svého bezpečnostního správce nebo oddělení IT.
Nebojte se zeptat. Je v zájmu všech, aby práce byla bezpečná.

Ve firmě Vás chrání technologie, které doma nemáte. Proto více než kdy jindy dbejte na **aktualizace operačního sytému a antivirového programu**.

DATA SECURITY

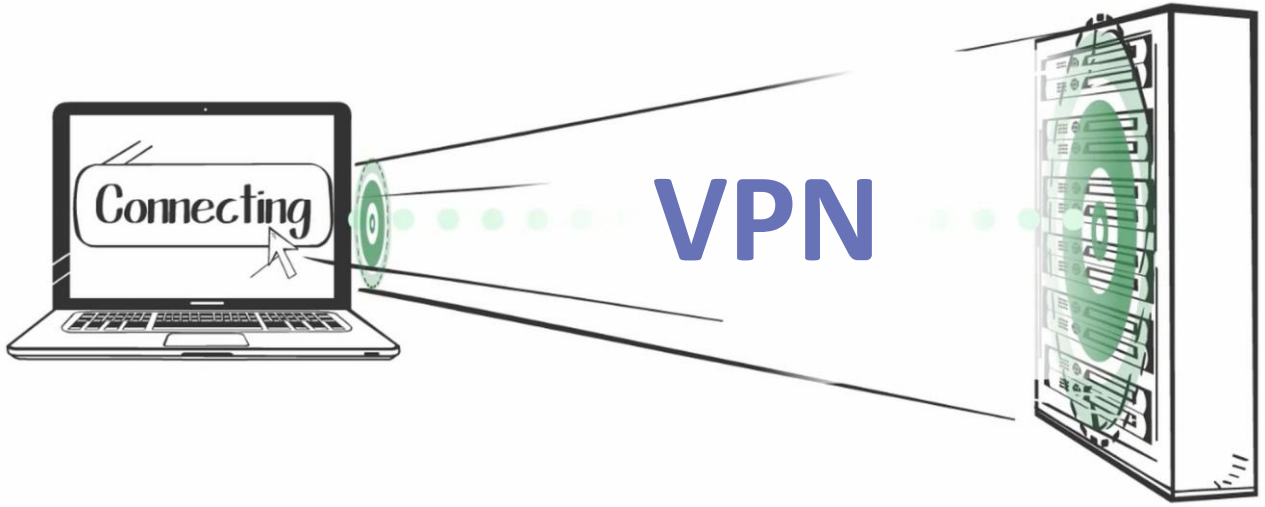
AEC

Potřebujete se připojovat k firemním serverům?

Poskytl Vám zaměstnavatel možnost připojení pomocí VPN? **Vždy ji využívejte!**

Nevíte, co je VPN? Kontaktujte své IT oddělení a zeptejte se ho. Instalace je snadná a velmi rychlá.

VPN zajistí šifrovanou komunikaci mezi vaším počítačem a sítí (internet, firemní síť). Kyberzločinci tak nemohou vaši komunikaci odchytit, protože je šifrovaná.



DATA SECURITY

AEC

Karanténa v praxi

Také zaháníte nudu nákupy přes internet, hraním, stahováním filmů a hudby?

Ano, na počítači, tabletu nebo chytrém telefonu nyní budete trávit spoustu času.

Nakupujte pouze na **ověřených e-shopech**, používejte **bezpečné metody on-line plateb**.

Seznam rizikových e-shopů je neustále aktualizován na tomto odkazu:

https://www.coi.cz/pro-spotrebitele/rizikove-e-shopy/

Nestahujte filmy, hry a hudbu **z veřejných úložišť**. I když se soubor může zdát jako skutečný film, může obsahovat škodlivý kód, který kyberzločincům otevře přístup do Vašeho počítače.

Práce z domu láká k brouzdání na Internetu

Věnujte zvýšenou pozornost Vašemu surfování po Internetu.

Lehkomyslné brouzdání zvyšuje pravděpodobnost stažení škodlivého softwaru, který může napadnout Váš počítač a následně i celou firemní síť.

Co takový škodlivý kód může ve Vašem počítači napáchat?

- Škodlivý kód Vám zašifruje disk a bude vyžadovat výkupné za odšifrování.
- Malware zpomalí běh Vašeho počítače.
- Malware smaže Vaše data.
- Malware se začne šířit na připojené okolní počítače a zařízení.

Jak neskočit podvodníkům na špek

Obdrželi jste mail s podivnou žádostí? Měli jste telefonát, kdy se Vám žádost volajícího zdála něčím podezřelá? Tak to jste pravděpodobně zažili útok některou z **metod sociálního inženýrství**. Jedná se o techniku, kdy se útočník například snaží získat citlivé údaje (Vaše, Vašich kolegů nebo vaší společnosti), nebo se Vás snaží přimět ke kliknutí na určitý (infikovaný) odkaz.

Jednoduše řečeno, útočník rybaří (odborně **phishing**). K úspěšnému rybaření ovšem potřebuje Vaši součinnost (chytnout se na háček).

DATA SECURITY

AEC

Jak se vyvarovat phishingového útoku

U e-mailů kontrolujte odesílatele. Zpravidla je využívána podobná adresa místo běžné. Např. místo info@ceskaposta.cz bude adresa info@caskaposta.cz.

Jediné změněné písmenko znamená úplně jinou adresu! Takové zprávy můžete ignorovat a přesunout je do nevyžádané pošty. Případně se telefonicky můžete dotázat na pravost.

Kontrolujte obsah emailu a nedůvěřujte přílohám.

- Pokud Vás obsah nutí kliknout na odkaz, buďte obezřetní. Zprávy i internetové stránky zpravidla vypadají podobně jako ty, za které se vydávají.
- Pokud si nejste jisti, zda na odkaz ve vaší poště kliknout, poraďte se s IT oddělením a raději na nic neklikejte ani na zprávu neodpovídejte. Původ zprávy je opět možné ověřit si telefonicky.

Jak se bezpečně chovat na internetu?

Nevyužívejte firemní emailovou adresu k soukromým účelům.

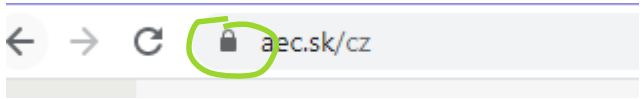
- Snížíte tím možnosti využití firemní emailové adresy k cílenému útoku útočníka.

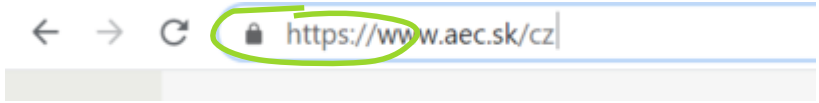
Nestahujte filmy, hudbu, hry, software, fotografie na firemní počítač.

- Snížíte riziko stažení škodlivého software.

Kontrolujte, že navštěvované stránky mají https certifikát – šifrování komunikace.

- *Vaši komunikaci nebudu moci útočníci odposlechnout.*





Pro soukromé účely nevyužívejte heslo, které používáte v práci (a naopak).

- Útočník potom nemůže toto heslo použít pro přihlášení do firemní emailové pošty nebo firemní interní sítě.

Zabezpečení domácí WiFi sítě

Zabraňte neoprávněným osobám přistupovat do Vaší domácí WiFi sítě a ochráníte tak nejenom Vás, ale i Vaše data.

Jak zabezpečit vaši WiFi síť?

- Změňte název sítě (SSID) z výroby na Vaše vlastní a síť skryjte.
- Změňte z přednastaveného hesla výrobce na své vlastní heslo.
- Pro šifrovaný přístup do Vaší WiFi sítě používejte bezpečné protokoly WPA2 nebo WPA3.
- Vyšší úroveň zabezpečení: Povolte jen MAC adresy, které mohou k Vaší síti přistupovat.

Každý router se nastavuje jinak, přečtěte si proto v návodu kapitoly týkající se zabezpečení, použijte Internet nebo zavolejte technickou podporu výrobce, aby Vám se zabezpečením poradil.

Využijte získaný čas ke sebevzdělávání

Volný čas můžete věnovat k osobnímu rozvoji. Oblast informační bezpečnosti se velmi dynamicky rozvíjí, přičemž každé pochybení mívá nepříjemné důsledky. Proto je třeba s útočníky držet krok.

Se vzděláváním v oblasti informační bezpečnosti Vám rádi pomůžeme. Nabízíme e-learningovou platformu obsahující kratičké **zábavné videokurzy základů kyberbezpečnosti**:

Pusťte si jeden zcela zdarma na adrese:

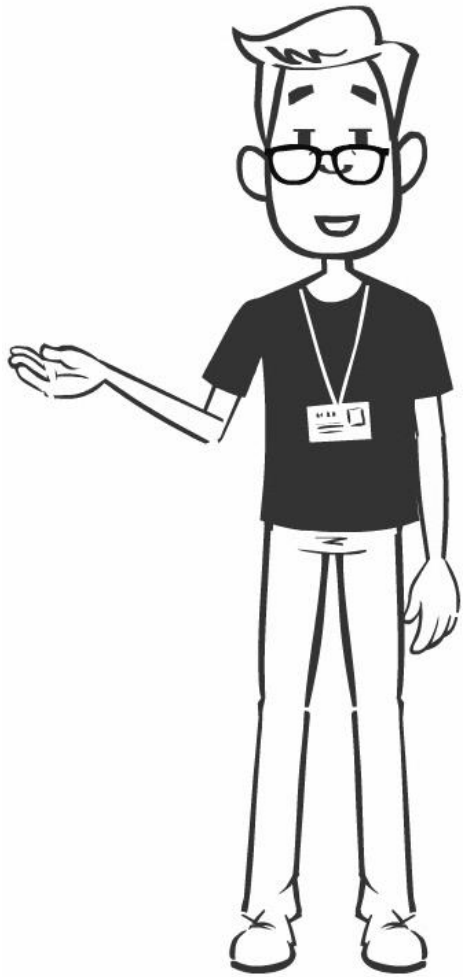
https://edu.aec.cz/demo/

DATA SECURITY

AEC

Co se naučíte

1. kapitola: **Bezpečnost mobilních zařízení**
2. kapitola: **Bezpečné chování v síti**
3. kapitola: **Bezpečné surfování na internetu**
4. kapitola: **Email bezpečně**
5. kapitola: **Hesla bezpečně**
6. kapitola: **Klasifikace informací**
7. kapitola: **Mazání a skartování informací**
8. kapitola: **Práce z domova**
9. kapitola: **Reakce zaměstnanců při bezpečnostním incidentu**
10. kapitola: **Uchovávání dat na USB**



DATA SECURITY

AEC Security Academy

https://edu.aec.cz

AEC

Děkujeme za pozornost

edu.aec.cz/demo