BEZPEČNĚ V ONLINE SVĚTĚ

Chraňte firmu, instituci i sebe

V případě, že naletíte podvodníkům a ohrozíte firemní data či peníze, firma může náhradu vyžadovat po vás.

Dodržujte základy počítačové bezpečnosti pro zaměstnance a ochráníte tak nejen firemní majetek, ale i sami sebe.

bezpečí

Univerzita Palackého v Olomouci

avast

BUĎ SAFE ONLINE

KDYŽ VYTVÁŘÍTE A ZADÁVÁTE HESLA

- **Nastavte si silné a unikátní heslo** pro každý účet. Pokud se někomu podaří odhalit vaše univerzální heslo, získá přístup k veškerým vašim datům. Silné heslo obsahuje alespoň 16 znaků, malá a velká písmena, číslice a speciální znaky.
- **Aktivujte si dvoufázové ověření**, můžete si nastavit ověření přes SMS, aplikaci v mobilním telefonu nebo přes e-mail.
- **Svá hesla si chraňte**, nikomu je nesdělujte a nezadávejte je v přítomnosti ostatních. Nikdy je nezapisujte do nechráněného dokumentu nebo diáře. K ukládání hesel můžete používat **bezpečnostní aplikace** typu „správce hesel“.

KDYŽ SE PŘIPOJUJETE NA WI-FI SÍŤ

- Pokud akutně potřebujete využít nezabezpečenou Wi-Fi, **aktivujte si službu virtuální privátní síť (VPN)**, ta vám umožní prohlížet internet v soukromí.
- Bez aktivované ochrany se nikdy nepřihlašujte do citlivých služeb (internetové bankovnictví, e-mail, firemní web), útočníci mohou ukrást vaše údaje a hesla.

KDYŽ PRACUJETE S E-MAILEM

- Pro pracovní komunikaci **používejte pouze pracovní e-mail**.
- **Nenechávejte e-mail bez dozoru**. Pokud opouštíte své pracovní místo, odhlaste se nebo uzamkněte počítač.
- **Dokumenty obsahující citlivá data uzamkněte** silným heslem, předtím než je budete sdílet.

- **Adresu odesílatele si ověřujte** pomocí náhledu do hlavičky e-mailu. Zobrazí se vám najetím kurzoru na jméno odesílatele. Podvodníci se často vydávají za nadřízeného, kolegu či banku a posílají falešné faktury či příkazy. **Všímejte si také nejasností a jazykových nesrovnalostí** (lámaná čeština, absence diakritiky, špatný slovosled), může jít o strojový překlad. Pokud se vám e-mail zdá podezřelý, ověřte jeho pravost osobně či telefonicky.

- **Neotvírejte přílohy z neznámých zdrojů**, mohou obsahovat škodlivý program (malware). **Neklikejte na odkazy v podezřelých e-mailech**, ty mohou vést na podvodné stránky, které se snaží vylákat vaše osobní údaje, zejména přihlašovací jméno a heslo, které pak zneužijí ke krádeži účtu (phishing).

- **Nepřeposílejte řetězové e-maily**, rádobyvtipné či neověřené a často nepravdivé zprávy (hoax, fake news). Přeposláním šíříte dál svou e-mailovou adresu a zavádějící informace.

KDYŽ NARAZÍTE NA DOTAZNÍK ČI SOUTĚŽ

- **Nevyplňujte neznámé elektronické dotazníky** z podezřelých a neoficiálních zdrojů. Prověřte si, kdo za nimi stojí. Časté jsou také soutěže a „senzační" podvodné nabídky (scam), které od vás sbírají citlivé údaje.

KDYŽ SE PŘIHLAŠUJETE DO FIREMNÍ SÍTĚ ČI ZAŘÍZENÍ

- **Používejte antivirus** na všech zařízeních. Pravidelně bude kontrolovat a chránit váš počítač, mobil i externí disky.

- Bez svolení správce **nepřipojujte do firemní sítě své osobní zařízení** (notebook, tablet, Wi-Fi router).

KDYŽ INSTALUJETE SOFTWARE A AKTUALIZACE

- **Nestahujte a neinstalujte software bez souhlasu správce sítě**, i funkční software z neoficiálního a neschváleného zdroje může obsahovat skrytý škodlivý program (malware).
- **Nezasahujte svévolně do nastavení** firemního zařízení, zejména do nastavení operačního systému.
- **Pravidelně aktualizujte** jak operační systém, tak jednotlivé programy. Aktualizace opravuje chyby softwaru a snižuje šanci, že bude váš počítač napaden.

KDYŽ PRACUJETE S DATY A PAMĚŤOVÝMI MÉDII (USB)

- **Zálohujte si veškerá data**, se kterými pracujete, ideálně na firemním cloudovém úložišti. Své soubory vždy zálohujte na jiný disk, než je ten, na kterém jsou původně uloženy.
- **Nepřipojujte cizí paměťové médium** do svého osobního ani firemního zařízení.

KDYŽ NAVŠTĚVUJETE WEBOVÉ STRÁNKY

- **Nenavštěvujte stránky, které skýtají potenciální rizika**, tedy stránky s nelegálním, explicitním nebo pirátským obsahem. Můžete si do svého zařízení stáhnout škodlivý program (malware).

bezpečí E-Bezpeci.cz

avast Avast.cz

Univerzita Palackého v Olomouci Prvok.upol.cz

BUĎ SAFE ONLINE Budsafeonline.cz

Policie.cz

LETÁČEK K TISKU:
www.budsafeonline.cz/letacek
www.e-bezpeci.cz/prozamestnance