Bezpečná UK: Desatero kyberbezpečnosti

Univerzita Karlova

1. Zamykám svá IT zařízení, i když odcházím jen „na minutku“

Stačí krátký okamžik nepozornosti a někdo může nahlédnout tam, kam nemá. Zamčená obrazovka je nejjednodušší způsob, jak chránit vaše data i IT systémy univerzity.

2. Vícefaktorové ověřování (MFA) je můj digitální strážce a používám ho všude tam, kde je dostupné

MFA výrazně posiluje bezpečnost účtu. Kde je vícefaktorové ověřování k dispozici, tam ho používám. I kdyby někdo získal mé heslo, bez druhého faktoru zůstane před mým účtem stát jako před zamčenými dveřmi.

3. Tvořím silná a unikátní hesla

Osobní údaje do hesel nepatří. Silné heslo je dlouhé, jedinečné a nepoužité jinde — zkrátka takové, které útočníka spolehlivě odradí.

4. Pracovní e-mail je jen pro práci

Soukromé účely do něj nepatří.
Pracovní e-mail chrání interní data a procesy.
A pokud dorazí podezřelá zpráva, neodpovídám, neklikám, neotvírám. Phishingu se nejlépe brání jeho ignorováním.

5. Makra a neznámé přílohy neotevírám

Makra i neprověřené dokumenty v příloze e-mailu mohou být trojským koněm. Otevírám jen to, co skutečně znám, čemu důvěřuji a od ověřených odesílatelů.

6. Aktualizace beru jako pravidelný servis a zařízení udržuji zabezpečená (antivir, firewall, šifrování)

Aktualizace opravují chyby, které útočníci rádi zneužívají. Pravidelné aktualizace jsou základem bezpečné práce. Antivir, firewall i šifrování jsou potřebnou výbavou každého zodpovědného uživatele.

7. Nepřipojuji do univerzitní IT sítě nic, co tam nepatří

Neautorizovaná zařízení či nalezené USB mohou představovat bezpečnostní riziko a obsahovat škodlivý kód. Jejich připojením ohrožujete nejen sebe, ale i celou infrastrukturu UK. Nalezené zařízení patří na IT oddělení s informací, že se jedná o nalezené neautorizované zařízení.

8. Surfování na internetu s rozumem

Rizikové stránky a zakázané soubory obcházím obloukem. Nebezpečné weby a soubory mohou způsobit infekci nebo únik dat. Internet používám jen k oprávněným a pracovním účelům.

9. Důvěrná data ukládám jen tam, kde jsou v bezpečí

K ukládání dat používám pouze oficiální úložiště UK (OneDrive, SharePoint, Teams), která jsou zabezpečená. Veřejná úložiště mohou vést k úniku nebo zneužití citlivých informací.

10. Podezřelé situace hlásím bez odkladu

Ať už jde o podivný e-mail, ztracené zařízení nebo jiný incident, hlásím jej na **abuse@cuni.cz**. Rychlá reakce minimalizuje škody. Bezpečnostní tým je tu pro vás, doporučujeme hlásit jakékoli podezření raději preventivně.

Kompletní informace k desateru, včetně jeho plného znění v opatření rektora, jsou pro vás dostupné na Intranetu UK.