Základní pravidla bezpečného chování online

Kyberbezpečnost není jen o technologiích – nejdůležitější roli hraje naše každodenní chování.
Většina bezpečnostních incidentů nevzniká kvůli složitým útokům, ale kvůli drobné nepozornosti – například kliknutí na podvodný odkaz nebo použití slabého hesla.
Dobrou zprávou je, že ochrana účtu i dat nemusí být složitá. Stačí si osvojit několik základních návyků, které výrazně sníží riziko zneužití a pomohou vám bezpečně používat univerzitní systémy i internet obecně.

Používejte silná a unikátní hesla
Vaše heslo je jako klíč od bytu – nenechávejte ho nikomu cizímu a nepoužívejte stejný pro více dveří.
Vytvářejte delší hesla (alespoň 12 znaků) a kombinujte písmena, čísla i speciální znaky.
Nikdy heslo nikomu nesdělujte – ani IT pracovníkům, ani kolegům.

Aktualizujte svá zařízení
Aktualizace nejsou jen o nových funkcích – opravují také chyby, které mohou útočníci zneužít. Zapněte si automatické aktualizace, aby byl váš počítač i mobil vždy chráněný.

Dávejte pozor na podezřelé e-maily
Phishingové e-maily se často tváří jako zprávy od kolegů, banky nebo univerzity. Pokud vám něco připadá podezřelé – například nečekaná žádost o přihlášení nebo příloha od neznámého odesílatele – raději zprávu neotvírejte a nahlaste ji lokální IT podpoře.

Instalujte software jen z ověřených zdrojů
Vyhněte se neznámým aplikacím nebo odkazům ke stažení z neoficiálních webů.
Na univerzitních počítačích používejte software schválený nebo poskytnutý vaší fakultou.

Pracujte jen na zabezpečených sítích Wi-Fi
Při práci s univerzitními systémy se připojujte pouze na zabezpečené sítě – například Eduroam . Veřejné Wi-Fi sítě (např. v kavárně nebo nádraží) používejte jen výjimečně a nikdy pro přístup k citlivým datům.

Zamkněte své zařízení, když odcházíte
Ať už jde o počítač v kanceláři, notebook nebo mobil – vždy ho zamkněte, když odcházíte od stolu. Chráníte tak nejen sebe, ale i univerzitní data.

Těchto pár jednoduchých kroků dokáže výrazně snížit riziko napadení účtu, úniku dat nebo zneužití zařízení. Bezpečnost univerzity začíná u každého z nás.

Potřebujete poradit nebo nahlásit bezpečností incident?

Podrobný postup najdete v sekci Hlášení bezpečnostního incidentu , kde se dozvíte, jak incident popsat, komu ho zaslat a jak probíhá řešení.

Často kladené dotazy (FAQ)

Jak poznám, že je e-mail falešný?

- Podezřelá adresa odesílatele, naléhavý tón "nutí vás jednat okamžitě", text emailu obsahuje chyby, neznámé odkazy nebo přílohy - to vše jsou varovné signály.

Co mám dělat, když mi přišel podezřelý e-mail?

- Neotevírejte odkazy ani přílohy. Přepošlete jej na IT podporu fakulty nebo bezpečnostní incident nahlaste.
- Podrobný postup najdete v sekci Hlášení bezpečnostního incidentu , kde se dozvíte, jak incident popsat, komu ho zaslat a jak probíhá řešení.

Co dělat, když mám podezření, že někdo získal moje heslo?

- Okamžitě si heslo změňte (v CAS nebo příslušném systému) a informujte fakultního IT správce.

Mohu používat stejné heslo pro univerzitní a osobní účet?

- Rozhodně ne. Každé prostředí by mělo mít své vlastní heslo.

Je bezpečné pracovat přes veřejnou Wi-Fi, když používám VPN?

- VPN riziko snižuje, ale neodstraňuje. Pokud to jde, použijte raději univerzitní síť Eduroam nebo vlastní mobilní připojení.

Mohu používat univerzitní účet na osobních zařízeních?

- Ano - ale zařízení musí být aktualizované a zabezpečené.

Důležité odkazy

Další informace, aktuální hrozby, doporučení a dokumenty související s kyberbezpečností:

- Nebezpečí v e-mailech
- Nebezpečné www stránky
- Zrádná hesla
- Co Nejvíc chránit
- Dokumenty a návody ke kyberbezpečnosti
- Užitečné odkazy pro řešení bezpečnostních problémů