Ochrana zařízení

Vaše zařízení – počítač, notebook, tablet nebo telefon – jsou branou do univerzitních systémů. Stačí jedno kliknutí na podvodný odkaz nebo neaktualizovaný program a útočník může získat přístup k vašim datům i účtu.

Zabezpečení pracovních počítačů a notebooků obvykle zajišťuje centrálně IT pracoviště fakulty nebo součásti. Pokyny uvedené níže se proto týkají především vašich **soukromých počítačů, tabletů a telefonů**, a to bez ohledu na to, zda je používáte pro studijní nebo pracovní účely.
Naštěstí většinu hrozeb snadno odrazíte několika jednoduchými kroky.

Aktualizace = základ bezpečí
Aktualizace nejsou jen o „nových funkcích“ – často brání útokům a opravují bezpečnostní chyby, které útočníci zneužívají.
Zapněte **automatické aktualizace systému** (Windows, macOS, Android, iOS).
Pravidelně aktualizujte i aplikace – zejména **prohlížeč, Adobe Reader, Microsoft Office, Zoom** nebo jiné používané programy.
Nenechávejte dlouho zobrazenou hlášku „instalovat později“ – právě tehdy bývá počítač nejzranitelnější.

Antivirová ochrana a firewall
Základní ochranu zajišťují antivirové programy a firewall.
Pro běžného uživatele je zcela dostačující **Windows Defender**, který je součástí Windows a je automaticky aktualizován.
Na pracovních (univerzitních) zařízeních bývá antivirová ochrana nastavena centrálně IT pracovištěm fakulty nebo součásti. Některé fakulty zároveň nabízejí zaměstnancům možnost instalace fakultou spravovaného antivirového programu i na jejich soukromé notebooky – dostupnost této služby se ale liší, proto je vždy vhodné obrátit se na IT podporu své fakulty.
Firewall mějte vždy zapnutý – brání nechtěné komunikaci mezi vaším počítačem a cizími servery.
Tip: Spusťte si jednou za čas „Rychlou kontrolu“ antivirem, zejména po připojení neznámého USB disku.

Silné a jedinečné heslo k zařízení
I nejlepší antivir nepomůže, pokud má zařízení slabé heslo.
Používejte **heslo o délce alespoň 12 znaků** (kombinace písmen, čísel a symbolů).
Vyhněte se heslům typu „heslo123“, „student“ nebo „123456“.
Nikdy nepoužívejte stejné heslo pro pracovní a pro soukromý osobní účet.
Zvažte použití **správce hesel**, který za vás silná hesla bezpečně uloží.

Zabezpečení mobilů a notebooků
Mobilní zařízení jsou často přehlížená, přitom obsahují přístup ke všem účtům, e-mailům a souborům.
Nastavte **PIN, gesto, heslo nebo biometrické ověření** (otisk, obličej).
Aktivujte **automatické zamknutí** po 30–60 sekundách nečinnosti.
Nikdy nenechávejte zařízení bez dozoru, zvlášť na veřejných místech.
Zvažte **šifrování disku notebooku** – pokud vám ho někdo ukradne, nedostane se na data na něm uložená.

Bezpečné připojení
Na veřejných Wi-Fi sítích (kavárny, letiště, vlaky) buďte opatrní. Ideálně se k univerzitním službám připojujte přes VPN .
Nepoužívejte pro nabíjení veřejné USB zásuvky a raději použijte veřejnou zásuvku na 220V a svou vlastní USB nabíječku.
Pokud to nejde, věnujte pozornost každému varování o tom, že připojení není důvěryhodné.
Nepřihlašujte se do CAS nebo e-mailu, dokud jste na nezabezpečené síti.
Wi-Fi Eduroam je pro uživatele bezpečnější – nedovolí nikomu odposlouchávat vaši komunikaci.

Když zařízení ztratíte nebo je odcizeno
Okamžitě změňte heslo do CAS a všech služeb, které byly v zařízení přihlášené.
Pokud máte zapnutou funkci **Najít moje zařízení** nebo **Find My iPhone**, zkuste zařízení lokalizovat nebo vzdáleně smazat.

Informujte IT podporu fakulty – pomohou vám zabezpečit účty a nahlásit incident.

Často kladené dotazy (FAQ)

Je nutné mít antivir, když mám Mac nebo iPhone?

- Ano – i když je riziko menší než u Windows, malware pro macOS i iOS existuje. Doporučuje se alespoň pravidelně aktualizovat systém a neinstalovat aplikace mimo App Store.

Stačí mi antivir, nebo potřebuju i firewall?

- Obojí. Antivir chrání před škodlivými soubory, zatímco firewall blokuje nechtěné připojení z internetu.

Můžu používat veřejné Wi-Fi v kavárnách?

- Ano, ale s opatrností. Nepřihlašujte se k univerzitním systémům ani do bankovnictví. Pokud potřebujete pracovat, použijte VPN .

Ztratil/a jsem mobil, kde mám univerzitní e-mail – co mám dělat?

- Okamžitě změňte heslo do CAS , nahlaste událost IT podpoře fakulty a pokud je to možné, aktivujte vzdálené smazání zařízení.

Jak ochránit vaše zařízení v 5 bodech

Při ztrátě zařízení okamžitě změňte hesla a nahlaste incident.

Aktualizujte systém i aplikace.
Používejte antivir a zapnutý firewall.

Zamkněte zařízení, když odcházíte.
Připojujte se jen k důvěryhodným sítím.