



# CHRÁŇTE SA PRED KYBERNETICKÝMI BEZPEČNOSTNÝMI HROZBAMI



## 1. AKTUALIZUJTE A PLÁTAJTE

Váš počítač, smartfón, wifi router a všetky IT zariadenia musia mať vždy nainštalované posledné verzie aktualizácií a záplat operačného systému. Týka sa to aj internetového prehliadača a všetkých aplikácií. Hackeri ako prvé hľadajú známe zraniteľnosti v neaktualizovaných systémoch, čiže bezpečnostné diery. A diery treba plátať.



## 2. INŠTALUJTE SI ANTIVÍRUS

Voči útoku škodlivým kódom Vás obránia najmä antivírusové aplikácie. Nainštalujte si niektorú z nich a nastavte ju tak, aby automaticky kontrolovala prístupy na webové stránky, sťahované súbory, prílohy e-mailov a pamäťové médiá.



## 3. POUŽÍVAJTE SILNÉ HESLÁ

Silné heslá sú tie, ktoré nikto neuhádne a zároveň si ich pamätáte. Napríklad citát, alebo text skladby, kde nahradíte aspoň jedno písmeno špeciálnym znakom a pridáte číslice. Reálne slová útočníci zlomia za niekoľko sekúnd. Nepoužívajte rovnaké heslo pre viacero webových stránok alebo služieb. Ak máte hesiel veľa, použite aplikáciu manažér hesiel.



## 4. PRIHLASUJTE SA 2-STUPŇOVO

Ak to webová služba umožňuje, používajte na prihlasovanie tzv. dvojfaktorovú autentizáciu (napríklad pomocou SMS kódu). Samotné heslo nie je už dostatočnou ochranou pred zneužitím prístupových práv.



## 5. KONTROLUJTE ADRESY

Pred otvorením webovej stránky vždy najprv skontrolujte adresu. Nespúšťajte neznáme odkazy. Podhodenie adresy a presmerovanie na nebezpečnú webovú stránku je typickým spôsobom prípravy útoku. Neotvárajte neznáme prílohy a linky v správach, väčšinou je ich obsahom škodlivý kód.



## 6. NEDÔVERUJTE E-MAILOM

Správa elektronickej pošty je ako korešpondenčný lístok. Nikdy nemáte istotu, že odosielateľom je ten, za koho sa vydáva. Obsah správy môže prečítať množstvo neznámych ľudí. Pokiaľ nepoužívate šifrovaný e-mail, vážte informácie, ktoré odosielate.



## 7. ZÁLOHUJTE DÁTA

Aj pamäťové médiá sa občas pokazia a ich obsah sa stratí. Zároveň sa zvyšuje počet tzv. ransomware útokov, keď hackeri zašifrujú údaje a za ich vrátenie vyžadujú výkupné. Proti týmto hrozbám je účinná len obnova údajov z pravidelne vytváraných záloh.



## 8. PRIPÁJAJTE SA BEZPEČNE

Nechránené wifi siete bez hesla a šifrovania sú ako dokorán otvorené dvere do bytu. Zmeňte aj pôvodný továrenský názov vášho routera a zároveň sa vyvarujte použitiu takého názvu, ktorý by vás identifikoval. Oboje totiž hackerovi zjednoduší útok.



## 9. CHRÁŇTE SI SÚKROMIE

Sociálne siete navádzajú k tomu, aby ste prezradili o sebe čo najviac. Výsledkom bývajú vykradnuté domácnosti počas dovolenky, odcudzené peniaze z bankových účtov, ale aj sexuálne vydieranie či ujma na duševnom zdraví dieťaťa, napríklad prostredníctvom kyberšikany.



Kompetenčné  
a certifikačné  
centrum  
kybernetickej  
bezpečnosti

[www.cybercompetence.sk](http://www.cybercompetence.sk)



[www.akb.sk](http://www.akb.sk)



NÁRODNÝ  
BEZPEČNOSTNÝ  
ÚRAD

[www.nbu.gov.sk](http://www.nbu.gov.sk)



ÚRAD NA OCHRANU  
OSOBNÝCH ÚDAJOV  
SLOVENSKEJ REPUBLIKY

[www.dataprotection.gov.sk](http://www.dataprotection.gov.sk)