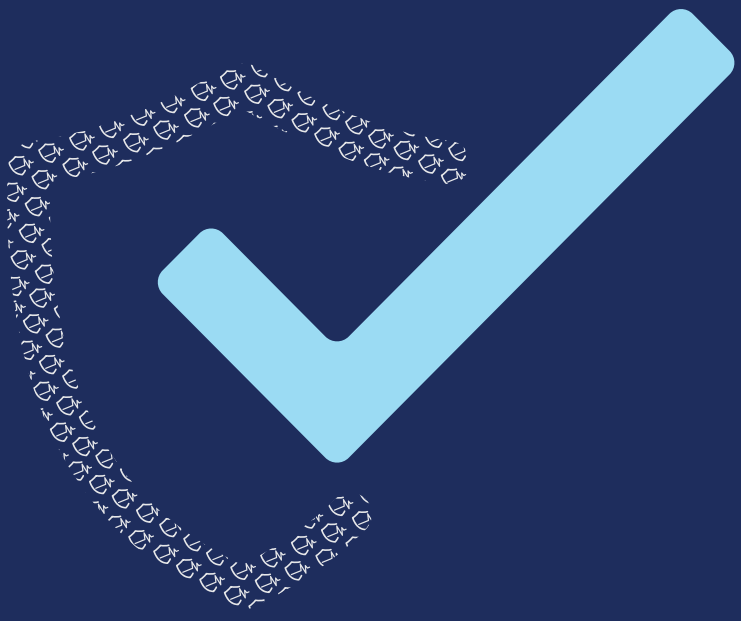
10

PRAKTICKÝCH RÁD PRE KYBERNETICKÚ BEZPEČNOSŤ

BEZPEČNOSŤ JE RUTINA



CENTRUM
KYBERNETICKEJ PODPORY
PRE ZDRAVOTNÍCTVO
<NCZI>

1 | POUŽÍVAJTE SILNÉ A JEDINEČNÉ HESLÁ

Každý účet by mal mať vlastné heslo s kombináciou malých a veľkých písmen, číslic a špeciálnych znakov. Vyhnite sa jednoduchým heslám. Minimálna dĺžka hesla by mala byť 12 znakov, odporúčaná je 15 znakov.

2 | SOFTVÉR AKTUALIZUJTE PRAVIDELNE A VČAS

Pravidelne aktualizujte operačný systém, aplikácie, antivírusové programy aj firmware vašich zariadení. Aktualizácie odstraňujú bezpečnostné chyby a chránia vaše zariadenia pred novými hrozbami.

3 | PRAVIDELNE ZÁLOHUJTE DÁTA

Zálohujte dôležité dokumenty, fotografie a ďalšie údaje na externý disk alebo do šifrovanej cloudovej služby. Zálohy vám pomôžu pri strate alebo poškodení dát. Dáta zálohujte v pravidelných intervaloch.

4 | CHRÁŇTE SVOJE SÚKROMIE A OSOBNÉ ÚDAJE

Nepublikujte ani nezadávajte svoje osobné údaje, ako sú meno, adresa, telefónne číslo, rodné číslo alebo fotografie, bez dôkladného zváženia, kto a prečo ich potrebuje. Vopred si premyslite, kto bude mať k vašim údajom prístup a ako s nimi môže nakladať. Nezverejňujte o sebe citlivé ani súkromné informácie – nikdy neviete, kto sa k nim môže dostať. Dôležité inštitúcie už vaše údaje majú a nikdy ich od vás nevyžadujú cez otvorené komunikačné kanály, ako sú e-mail, SMS správy alebo sociálne siete.

5 | POUŽÍVAJTE DVOJFAKTOROVÉ OVERENIE (2FA)

Používajte dvojfaktorové overenie všade, kde je dostupné. Do účtu sa neprihlásite len pomocou prihlasovacích údajov, ale aj druhým spôsobom overenia, napríklad kódom zo SMS správy, PIN kódom, odtlačkom prsta alebo skenom tváre. Aj v prípade prezradenia hesla zostane váš účet chránený druhým overovacím faktorom.

6 | POZOR NA PODVODNÉ E-MAILY A ODKAZY V SMS SPRÁVACH

Neklikajte na podozrivé odkazy a neotvárajte prílohy od neznámych odosielateľov. Môže ísť o phishingový útok. Kliknutím na odkaz môžete byť presmerovaní na nebezpečné webové stránky alebo si stiahnuť škodlivý softvér. Po zadaní osobných či dôverných údajov môžu byť tieto informácie zneužité. Vždy sa zamyslite, prečo vám niekto správu poslal a prečo od vás žiada kliknutie na odkaz alebo zadanie osobných údajov.

7 | POUŽÍVAJTE LEN DÔVERYHODNÝ ANTIVÍRUS, PROGRAMY A APLIKÁCIE

Antivírusové programy dokážu rozpoznať hrozby skôr, ako vám stihnú uškodiť. Používajte preto overené programy a aplikácie od známych a renomovaných spoločností. Neznámy softvér môže predstavovať bezpečnostné riziko a spôsobiť škody. Často je síce bezplatný, no zaplatiť zaň môžete svojimi osobnými údajmi.

8 | NEPOUŽÍVAJTE VEREJNÉ WI-FI BEZ OCHRANY

Vo verejných Wi-Fi sieťach sa neprihlasujte do internetového bankovníctva ani dôležitých účtov. Ak je to nevyhnutné, používajte pripojenie VPN na šifrovanie komunikácie.

9 | VŽDY SA RIADNE ODHLASUJTE Z ÚČTOV A ZARIADENÍ

Po skončení práce sa odhláste zo svojich účtov, najmä na cudzích alebo zdieľaných zariadeniach. Nikdy neukladajte prihlasovacie údaje na zariadeniach, ktoré nie sú vaše.

10 | NEUSTÁLE SA VZDELÁVAJTE

Sledujte nové hrozby a možnosti ochrany v digitálnom priestore. Informácie získavajte z dôveryhodných zdrojov. Čím viac sa dozviete, tým lepšie sa dokážete brániť. O svoje poznatky sa podeľte aj so svojimi blízkymi.