CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

BEZPEČNÉ HESLÁ

POUŽÍVAJTE SILNÉ HESLÁ

- Heslo má mať aspoň **12 až 16 znakov.**
- Nepoužívajte slová, ktoré možno nájsť v **slovníkoch**.
- Vyhnite sa **osobným informáciám** v hesle.
- Pri tvorbe hesiel je vhodné použiť kombináciu znakov, ako sú veľké a malé písmená, čísla a **špeciálne symboly** (napr. !, @, #, $, %).
- Vytvorte si heslá, ktoré sa nedajú ľahko uhádnuť. **Vyhnite sa** vzorom ako „12345" alebo „qwerty".
- Pre každý z vašich online účtov použite **iné** heslo. Týmto spôsobom, ak dôjde k prelomeniu jedného hesla, vaše ostatné účty zostanú v bezpečí.

- Zvážte použitie aplikácie - **správcu hesiel** na bezpečné generovanie, ukladanie a správu hesiel. Tieto nástroje dokážu vytvoriť silné heslá a zapamätať si ich za vás.
- Vždy, keď je to možné, povoľte pre svoje účty **dvojfaktorové overenie** (overenie napríklad cez SMS, či e-mail).
- Pravidelne **meňte svoje heslá**, najmä pre kritické účty.
- Zabezpečte svoje zariadenia pomocou silných **PIN kódov** alebo **hesiel**, aby ste zabránili neoprávnenému prístupu. Najvhodnejšie je nastavenie rozpoznávania tváre či odtlačku.
- **Nezadávajte** svoje heslá na verejných počítačoch alebo nezabezpečených sieťach.

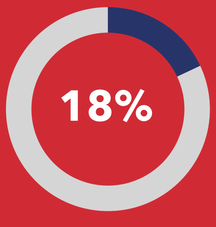
VEDELI STE, ŽE ... ?

- Napriek dôležitosti silných hesiel sa "123456" a "heslo" už roky radí medzi najbežnejšie používané heslá.
- Koncept používania hesiel siaha až do staroveku. Jeden z prvých zaznamenaných prípadov je z Rímskej ríše, kde sa na rozlíšenie priateľa od nepriateľa používalo vopred dohodnuté heslo.

- Čím dlhšie je heslo, tým ťažšie je prelomiť ho pomocou metód využívajúcich útoky hrubou silou. Pridanie len niekoľkých znakov do hesla môže exponenciálne zvýšiť jeho silu.
- Svetový deň hesiel sa oslavuje každý rok prvý štvrtok v máji. Jeho cieľom je zvýšiť povedomie o zabezpečení hesiel a podporovať dobré návyky týkajúce sa hesiel.

91% ľudí vie, že opakované použitie rovnakých hesiel predstavuje obrovské bezpečnostné riziko

59% avšak naďalej používa všade rovnaké heslo



zamestnancov zdieľa svoje heslá s kolegami

42% zamestnancov tvrdí, že to robia preto, aby ľahšie spolupracovali s členmi tímu.

38% uviedlo, že zdieľajú heslá, pretože ide o firemnú politiku.

123456	1234
12345678	password
123456789	12345
110110jp	111111
000000	martin

TOP 10 NAJČASTEJŠÍCH HESIEL NA SLOVENSKU

Zdroj: NordPass

CSIRT.SK

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

VIACFAKTOROVÁ AUTENTIFIKÁCIA

MFA je skratka pre **Multi-Factor Authentication**. Ide o bezpečnostné riešenie, ktoré vyžaduje, aby používatelia poskytli dva alebo viac overovacích faktorov na získanie prístupu k systému alebo účtu.

NIEČO, ČO POZNÁ

- Heslo
- PIN
- Odpovede na bezpečnostné otázky

NIEČO, ČO MÁ

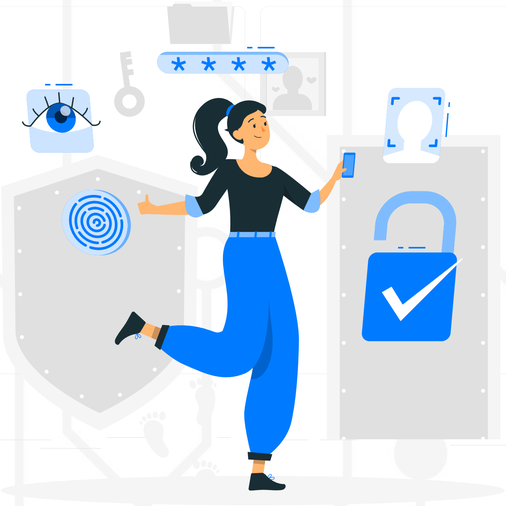
- Smartfón
- Bezpečnostný token
- Čipová karta

NIEČO, ČÍM JE

- Biometrické identifikátory
- Odtlačky prstov
- Rozpoznávanie tváre
- Skenovanie dúhovky

Požadovaním viacerých faktorov na autentifikáciu, **MFA** pridáva ďalšiu vrstvu zabezpečenia, ktorá sťažuje neoprávneným používateľom získať prístup, aj keď získali jeden faktor (napríklad heslo).

Najčastejšie používanou formou MFA je **2FA**, teda dvojfaktorová autentifikácia. Pridáva ďalšiu vrstvu overenia k tradičnej **kombinácii** používateľského mena a hesla používanej na prístup k účtu alebo systému. Najčastejšie využívané sú **tokeny** z mobilnej aplikácie, či **PIN** kódy zaslané ako **SMS** správa na telefónne číslo používateľa. Na smartfónoch sa často namiesto použitia hesla vyžaduje identifikácia pomocou **odtlačku prsta** alebo **rozpoznávanie tváre**.



VÝHODY

Rozšírené zabezpečenie:
MFA výrazne zlepšuje bezpečnosť pridaním ďalšej vrstvy overovania nad rámec len hesiel.

Ochrana pred phishingom:
MFA pomáha znižovať riziko phishingových útokov, keďže útočníci by na prístup k účtu potrebovali viac než len ukradnuté prihlasovacie údaje.

Užívateľsky prívetivé:
V závislosti od implementácie môže byť MFA užívateľsky prívetivá, najmä s metódami ako push notifikácie alebo biometrické overenie, ktoré sú často rýchlejšie a jednoduchšie ako zadávanie hesla.

NEVÝHODY

Cena:
Implementácia a správa systémov MFA môže byť zložitá a nákladná, najmä pre väčšie organizácie.

Odpor voči prijatiu:
Niektorí používatelia môžu mať nechuť k používaniu MFA z dôvodu obáv o súkromie, nepohodlia alebo neznalosti technológie.

Závislosť od externých faktorov:
Niektoré metódy MFA závisia od externých faktorov, ako je sieťové pripojenie alebo dostupnosť zariadenia. Ak tieto faktory zlyhajú alebo sú nedostupné, používatelia môžu mať problémy s prístupom k svojim účtom.