

V digitálnom svete je heslo často jedinou ochranou medzi vami a kybernetickým útokom. V tejto rubrike vám ukážeme, ako si vytvoriť silné heslá, prečo sa oplatí používať správcu hesiel a čo robiť, ak máte podozrenie na únik údajov. Jedno slabé heslo môže otvoriť dvere celému svetu - naučte sa, ako ich udržať pevne zamknuté.



Ako si vytvoriť "neprelomiteľné" digitálne kľúče?

- Dĺžka je dôležitá: čím dlhšie heslo, tým ťažšie sa láme. Ideálne by malo mať aspoň 12 znakov, no čím viac, tým lepšie.
- Kombinácia znakov: používajte kombináciu veľkých a malých písmen, číslíc a špeciálnych znakov (napr. !, @, #, \$).
- Vyhnite sa osobným informáciám: nikdy nepoužívajte svoje meno, dátum narodenia, adresu alebo iné ľahko uhádnuteľné informácie.
- Používajte náhodné slová (s úpravami): namiesto bežných slov skúste použiť nezmyselné kombinácie slov alebo frázy a nahraďte niektoré písmená číslicami alebo špeciálnymi znakmi (napr. "MojaModraMackaRadaSpiNaStreche" sa môže zmeniť na "M0j@M0dr@M@ck@R@d@Sp1N@Str3ch3!").
- Vytvárajte si unikátne heslá: pre každý online účet používajte iné heslo. Ak jeden účet bude kompromitovaný, ostatné zostanú v bezpečí.

Aké sú zásady pre bezpečnosť hesiel?

- Nikdy nezdieľajte svoje heslá.
- Pravidelne si meňte heslá.
- Používajte dvojfaktorové overenie (2FA): táto dodatočná vrstva zabezpečenia vyžaduje okrem hesla aj druhý overovací kód (napr. z SMS alebo aplikácie), čo výrazne zvyšuje bezpečnosť vašich účtov.
- Buďte opatrní na verejných Wi-Fi sieťach.
- Overujte si webové stránky: pred zadaním hesla sa uistite, že ste na legitímnej stránke (skontrolujte URL adresu a certifikát).

Zaujímajú vás praktické tipy a novinky v elektronizácii?

Sledujte nás na sociálnych sieťach a neunikne vám nič dôležité – zdieľame rady, aktuálne trendy aj užitočné informácie pre vašu digitálnu bezpečnosť.



Obsah dokumentu má len informačný charakter.

Ústredné kontaktné centrum: +421 2 35 803 083
© Odbor informačného obsahu NASES, 2025

[Odhliásť sa](#)