

PŘIHLAŠOVACÍ JMÉNO?

Přihlašovací jméno (anglicky *username*, *login*) je jméno, které si člověk zvolí nebo dostane, aby se mohl přihlásit do nějakého systému – třeba do školního počítače, e-mailu, Bakalářů nebo online hry.

Jak se tvoří přihlašovací jméno?

- Může to být **kombinace jména a příjmení** (např. jana.novakova).
- Někdy se používají **čísla** (např. petr123), hlavně když je jméno už obsazené.
- Může obsahovat **malá i velká písmena, čísla a některé speciální znaky** (např. tečka . nebo podtržítka _).
- **Nepoužívat diakritiku** (čárky a háčky – ěšřžáíé...)
- **Mezery se nepovolují.**

Záleží na velkých a malých písmenech?

Ve většině případech **nezáleží!**

- V emailové adrese je jedno, zda napíšeš jana.novakova@zs-habrmanova.cz nebo Jana.Novakova@zs-habrmanova.cz
- Při přihlášení do školního počítače také nerozlišujeme, zda napíšeš [karel.novak](#) nebo [Karel.Novak](#)
- Ve většině systémech se velká a malá písmena **nerozlišují** – takže Petr123 a petr123 je to samé – pozor, mluvíme o přihlašovacím jméně, nikoli o hesle.
- V některých systémech se však může rozlišovat Petr123 a petr123 – jako dvě různá jména (je to však výjimečné).

HESLO

Co je nejdůležitější při tvorbě hesla?

1. Délka hesla ★★★★★

☒ Nejdůležitější faktor

Čím je heslo delší, tím obtížněji se prolomí.

Příklad:

- Pes123 ❌
- MůjPesChodíKaždýDenNaProcházku! ☒

Doporučení: alespoň 12–16 znaků.



2. Jedinečnost hesla ★★★★★

☒ Druhý nejdůležitější faktor - každý účet by měl mít jiné heslo.

Pokud útočník získá jedno heslo a používáš ho všude, dostane se ke všem tvým účtům.

Špatně: stejné heslo pro e-mail, Instagram i školní účet

3. Nepoužívat osobní údaje ★★☆☆

Do hesla nepatří:

- | | | |
|------------|------------------------|---------------|
| ✗ jméno | ✗ datum narození | ✗ název školy |
| ✗ příjmení | ✗ jméno psa nebo kočky | |

Příklad:

- Simona2012 ✗
- Rex2020 ✗

Tyto údaje lze často dohledat na internetu nebo sociálních sítích.

4. Heslová fráze ★★☆☆

Dlouhá věta (heslová fráze) bývá bezpečnější než krátké složitě heslo.

Příklad:

- ✗ P@s5W0rd
- ✓ VSobotuJezdimNaBruslichSKamarady!

Je delší, lépe zapamatovatelná a zároveň bezpečná.

5. Kombinace různých znaků ★★☆☆

Používej:

- | | |
|-----------------|-------------------|
| ✓ malá písmena | ✓ čísla |
| ✓ velká písmena | ✓ speciální znaky |

Příklad:

- kolojezdimekazdyden
- KoloJezdimKazdyDen7!

Délka je ale stále důležitější než samotné speciální znaky.

6. Nepoužívat běžná slova ★★☆☆ Útočníci zkoušejí nejčastější výrazy:

- | | | |
|------------|----------|----------|
| ✗ heslo | ✗ fotbal | ✗ 123456 |
| ✗ password | ✗ qwerty | |

Tyto varianty bývají prolomeny během několika sekund.

7. Pravidelně kontrolovat bezpečnost účtů ★★☆☆

Heslo nemusíš měnit každý měsíc.

Změň ho hlavně tehdy, když:

- dojde k úniku dat,
- máš podezření na napadení účtu.
- někdo heslo zná,

Zapamatovací pomůcka pro žáky

1 Délka

2 Jiné heslo pro každý účet

3 Žádné osobní údaje

4 Heslová fráze

5 Velká písmena, čísla a znaky

6 Žádná běžná slova

7 Dvoufázové ověření

Ukládat hesla do prohlížeče? NIKDY!

Představ si to jako klíče od domu 🗝

Když si uložíš heslo do prohlížeče, je to podobné, jako kdybys nechal klíče zasunuté ve dveřích.

Pokud používáš:

- školní počítač,
- počítač v knihovně,
- sdílený notebook,
- počítač kamaráda,

může se k tvým účtům dostat někdo další.

Co je na ukládání hesel do prohlížeče rizikové?

- ✓ někdo může použít tvůj již přihlášený účet
- ✓ při krádeži zařízení mohou být hesla ohrožena
- ✓ některé škodlivé programy dokážou uložená hesla vyhledat
- ✓ uživatel často zapomene své skutečné heslo, protože ho nikdy nezadává

Kdy je to obzvlášť nebezpečné?

- Na školním počítači
- Na sdíleném rodinném zařízení
- Na veřejném počítači
- Na zařízení bez zamčené obrazovky

Zapamatuj si! ★

Webový prohlížeč není určen jako hlavní místo pro ukládání důležitých hesel.

Nejlepší volbou je:

- ✓ správce hesel
- ✓ silné a jedinečné heslo pro každý účet
- ✓ dvoufázové ověření
- ✓ odhlášení ze sdílených zařízení

Pravidlo do života

🔒 „Pokud počítač používá více lidí, heslo do prohlížeče nikdy neukládej.“

Otázka k diskusi:

Proč je podle tebe pohodlí někdy v rozporu s bezpečností? Uveď jeden příklad z běžného života.

PRAVIDLA PRO PRÁCI S HESLY - shrnutí

- **Tvorba bezpečného hesla**
 - Délka hesla (minimálně 16 znaků) – používat frázová hesla
 - Použití kombinace písmen, čísel a speciálních znaků
 - Velká i malá písmena
 - Čísla
 - Speciální znaky (např. !, @, #, \$)
 - Vyhnout se slovům ze slovníku
- **Pravidla pro tvorbu bezpečného hesla**
 - Nepoužívat osobní údaje (jména, data narození)
 - Jména
 - Data narození
 - Adresy
 - Nepoužívat stejná hesla pro různé účty
 - Každý účet má mít jiné heslo
 - Nepoužívat stejné heslo pro více účtů
- **Ochrana hesla**
 - Použití správce hesel
 - Použití aplikací pro správu hesel (např. LastPass, 1Password)
 - Ukládání hesel bezpečně
 - Nikdy neukládat hesla do prohlížečů
 - Dvoufaktorová autentizace (dvoufázové ověření)
 - Použití SMS kódů
 - Autentizační aplikace (Authenticator)
- **Bezpečné chování**
 - Neposílat hesla přes email nebo zprávy
 - Pravidelná změna hesel
 - Nepoužívat veřejné Wi-Fi pro přihlašování
 - Uzamykat zařízení, když nejsou používána
 - Nezůstatávat přihlášení
 - Nenechat zařízení pamatovat si naše přihlašovací údaje



Mám ráda kopretina.

M@mr@d@K0pr3t1n@.*F

M@mr@d@K0pr3t1n@.*I

M@mr@d@K0pr3t1n@.*S

Kontrolní otázky:

1. Které heslo je nejlepší?

A) Pepa2011

C) VUteryChodimSePsemDoLesa!

B) Fotbal123!

✅ Správná odpověď: C

Protože je dlouhé, neobsahuje snadno odhadnutelný osobní údaj a tvoří ho celá **heslová fráze**. 🗝️

2. Uložit heslo do prohlížeče?

Přečti si situaci:

Tomáš se přihlásil na školním notebooku do svého e-mailu. Webový prohlížeč se ho zeptal: „Chcete uložit heslo?“ Tomáš klikl na „Ano“, aby ho příště nemusel psát.

Otázky:

1. Proč může být uložení hesla do prohlížeče rizikové?
2. Co by se mohlo stát, kdyby notebook používal ještě někdo jiný?
3. Jaké bezpečnější řešení bys Tomášovi doporučil(a)?

Řešení

1. Pokud se k zařízení dostane jiná osoba, může se do účtu přihlásit bez znalosti hesla.
2. Druhý uživatel by mohl získat přístup k e-mailu, školnímu účtu nebo sociálním sítím.
3. Používat správce hesel chráněný hlavním heslem a dvoufázové ověření.

Zde jsou stránky, kde si můžeš ověřit sílu svého hesla:

<https://cs.vpnmentor.com/tools/passwordmeter/>

<https://passwordmeter.com/>



Zjisti, zda neuniklo Tvé heslo na internet?

[Have I Been Pwned: Check if your email address has been exposed in a data breach](#)

[Has Your Email Been Hacked? Free Data Leak Check | Avast](#)