Redamp.io

WEBINÁŘ PRO ŽIVNOSTNÍKY A MALÉ FIRMY

Používejte silná hesla.
Přidejte druhý zámek.



Jaké heslo je silné? Kam hesla uložit?
A proč heslo nestačí?

ING. DOMINIK MALČÍK, PH.D. · REDAMP.IO · ŘÍJEN 2026

pro podnikavé

ZAČNĚME OTÁZKOU

Máte stejné heslo na více místech?

Hackeři se často nenabourávají.
Přihlásí se vaším heslem.

Pokud nemáte druhý zámek, může jim stačit vaše přihlašovací jméno a heslo.

Nejde jen o velké firmy.
Jde o váš e-mail.

200 000

Až tolik lidí ročně přijde o svůj e-mail.

Jen u Seznamu. Odhad Seznamu z roku 2023.

Vaše heslo už možná někde leží.
Útočníkům stačí ho vyzkoušet.

124 mil.

hesel ukradených z napadených počítačů.

Sbírka z různých zdrojů, přidaná do HIBP v červnu 2026.

Útočníkovi nejde o vás.
Jde mu o to, co váš účet umí.



Peníze

BANKA A KARTY

Nákupy a platby na vaši kartu, reklamy placené z vašeho účtu.



Vaše jméno

SOCIÁLNÍ SÍTĚ

Píše vašim známým a zákazníkům: „Půjč mi“, „Klikni sem“, „Pošli mi kód“.



Falešné faktury

FIREMNÍ E-MAIL

Pošle vašim zákazníkům fakturu s číslem svého účtu.



Data

KONTAKTY A DOKUMENTY

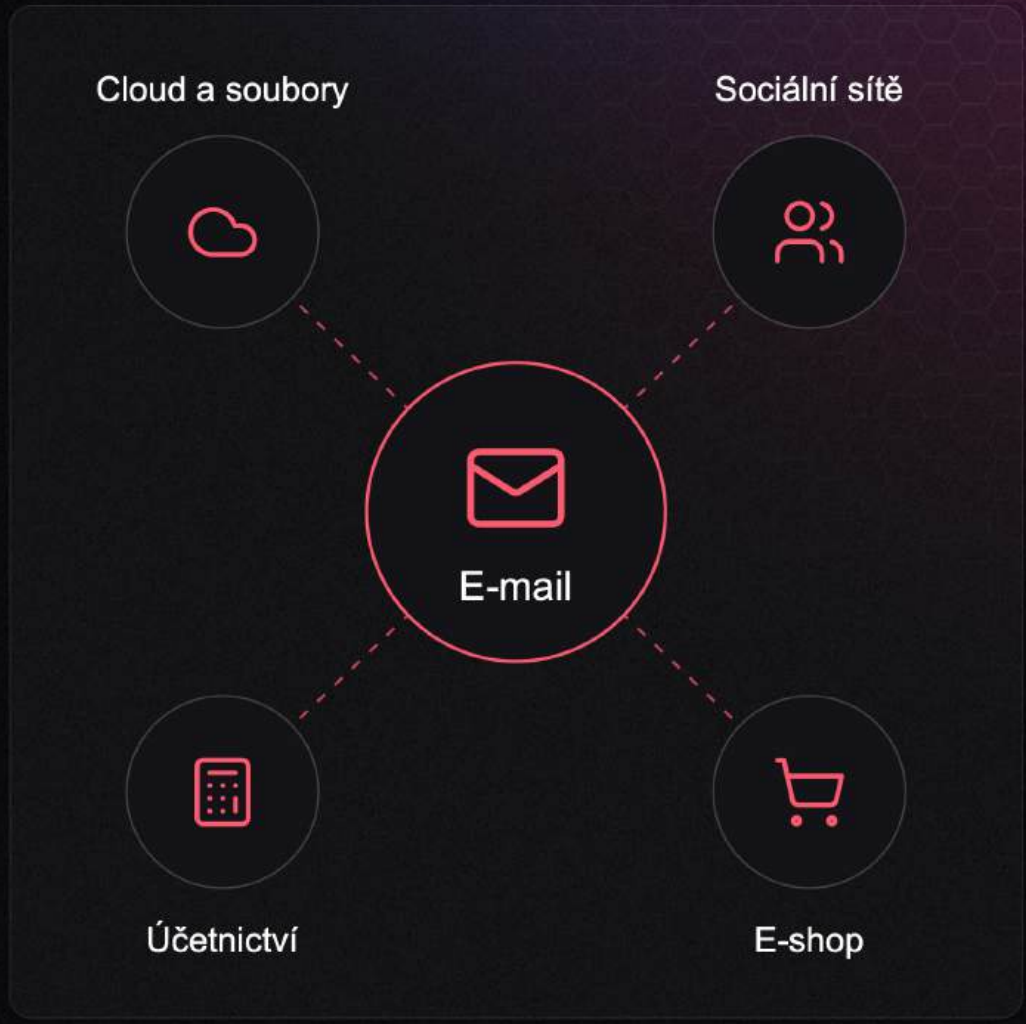
Prodá je dál, nebo vás s nimi vydírá.

PROČ ZAČÍT E-MAILEM

Váš e-mail je hlavní klíč. Otevře další účty.

Přes „Zapomněli jste heslo?“ si útočník může obnovit přístup na sociální sítě, do e-shopů, účetnictví i cloudu.

Proto e-mail zabezpečíme jako první.



PLÁN NA 40 MINUT

Dnes čtyři otázky.

01
Jaké heslo je silné?

02
Kam hesla uložit?

03
Proč heslo nestačí?

04
Jak nepřijít o účet?

Ke každé otázce konkrétní kroky pro vaše zařízení.

Silné heslo je dlouhé heslo.
Nemusí být nutně složité.

Doporučení: aspoň 15 znaků, nepředvídatelné a pro každý účet jiné. Nejsnáz to splní fráze ze čtyř a více slov od generátoru. Měňte ho, když unikne, je slabé nebo opakované.

SILNÉ HESLO

Délka poráží složitost.
A pamatuje se snáz.

Pro hesla, která si pamatujete: fráze složená z náhodných slov získaných z generátoru*, klidně s velkým písmenem nebo číslem. Ostatní hesla ať správce hesel vygeneruje jako dlouhá a náhodná.

Ukázková hesla nikdy nepoužívejte.

HESLO A · VYMYŠLENÉ · 11 ZNAKŮ

`Tr0ub4dor&3`

Slabé a těžko se pamatuje.

HESLO B · FRÁZE · 24 ZNAKŮ

`Kolo-jahoda-mrak-sesit-7`

Silné. Pro hesla, která si pamatujete.

HESLO C · SPRÁVCE HESEL · 26 ZNAKŮ

`q8#Lr2!vZp9@xT4mWc6&Kd3$Hy`

Dlouhé náhodné heslo. Nemusíte si pamatovat.

* Například bitwarden.com/passphrase-generator (zdarma)

JEDNO HESLO VŠUDE

Únik dat jednoho e-shopu. Nesmí otevřít váš e-mail.

Roboti zkoušejí uniklá hesla i na dalších službách. Automaticky a ve velkém.

Každý účet potřebuje jiné heslo.



Pamatujte si nejvýš tři hesla.
Zbytek si pamatuje správce hesel.

Počítač

HESLO 1

Přihlášení do Windows nebo Macu.

Hlavní účet

HESLO 2

Účet Apple, Google nebo Microsoft. Chrání vaše zálohy, telefon a často i e-mail.

Správce hesel

HESLO 3

Hlavní heslo, pokud ho váš správce hesel používá.

Všechno ostatní

BEZ PAMATOVÁNÍ

Vymyslí a uloží správce hesel.

Na každé z nich jiná heslová fráze. Nikde jinde ji nepoužívejte. A telefon zamkněte netriviálním kódem alespoň o šesti číslicích*.

* Platí, pokud telefon omezuje počet chybných pokusů po sobě (NIST SP 800-63B-4).

Nejčastější mýtus

„Heslo musíte měnit každé tři měsíce.“

Neplatí. Měňte ho, když unikne, je slabé nebo opakované.



Sto hesel si nezapamatujete. Nemusíte.

Správce hesel za vás.
Vymyslí, vyplní, pohlídá.

Vymyslí

GENERÁTOR

Dlouhé unikátní heslo pro každý účet.

Vyplní

VYPLŇOVÁNÍ

Sám, po otisku prstu nebo obličeji.

Pohlídá

KONTROLA

Upozorní na uniklá a opakovaná hesla.

Pozná adresu

PHISHING

Heslo nabídne podle uložené adresy webu. Když ho nenabídne, zkontrolujte adresu.

Správce hesel už máte.
Jen ho zapněte.

Apple Hesla

IPHONE, IPAD, MAC

Synchronizace přes iCloud.

Správce hesel Google

ANDROID A CHROME

Synchronizace přes Google účet.

Hesla v Edge

WINDOWS

Synchronizace přes Microsoft účet.

Zdarma. Už ve vašem zařízení.

JE TO BEZPEČNÉ?

Vestavěný správce je bezpečný. Když zamknete telefon i účet.

Hesla jsou šifrovaná. Zamkněte telefon netriviálním kódem a svůj účet Apple, Google nebo Microsoft chraňte druhým zámkem.

Trezor může někdo ukrást.
Chrání ho hlavní heslo.

Pokud váš správce používá hlavní heslo, zvolte dlouhou frázi, kterou nikde jinde nemáte.

Každý máme jiná zařízení.
Najděte svou kartu.

iPhone + Mac

APPLE HESLA

Zdarma, už ve vašem zařízení.

iPhone + Windows

APPLE HESLA NEBO BITWARDEN

Zdarma. Dvě cesty, vyberte si jednu.

Android + Windows

SPRÁVCE HESEL GOOGLE

Zdarma, v telefonu i v Chrome.

Firma spravuje hesla

FIREMNÍ SPRÁVCE HESEL

Všechna běžná zařízení, správa hesel s právy. Pár eur na člověka měsíčně podle tarifu.

Máte iPhone a Mac.
Začněte v iPhonu.

01 Zámek

Face ID nebo Touch ID a alespoň šestimístný kód.
Ne 123456, ne datum narození.

`Nastavení › Face ID a kód`

02 Ochrana odcizených zařízení

Zloděj s odkoukaným kódem se mimo známá místa k heslům nedostane.

`Face ID a kód › Ochrana odcizených zařízení`

03 Apple účet

Dvoufaktorové ověření a kontakt pro obnovení účtu.

`Nastavení › [jméno] › Přihlášení a zabezpečení`

04 Kontrola hesel

Změňte uniklá a opakovaná hesla.

`Hesla › Zabezpečení`

IPHONE A MAC

Aplikace Hesla vám ukáže, která hesla změnit.

Uniklá, opakovaná a slabá hesla najdete na jednom místě. Měňte je jedno po druhém.

V nastavení aplikace Hesla zapněte hlídání uniklých hesel.

ILUSTRAČNÍ NÁHLED



Máte iPhone a Windows.
Dvě cesty, obě zdarma.

CESTA A · APPLE HESLA VE WINDOWS

- ✓ iCloud pro Windows z Microsoft Store
- ✓ Zapněte v něm Hesla
- ✓ Rozšíření iCloud Passwords do prohlížeče

CESTA B · JEDNA APLIKACE VŠUDE

- ✓ Např. Bitwarden v iPhonu i ve Windows
- ✓ Zdarma pro jednotlivce
- ✓ Podporuje i Android

IPHONE A WINDOWS

Apple Hesla i ve Windows. Přes iCloud pro Windows.

Hesla z iPhonu vyplníte v Chrome i v Edge. Prohlížeč s iCloudem spárujete šestimístným kódem.

Potřebujete dvoufaktorové ověření Apple účtu.

ILUSTRAČNÍ NÁHLED



Apple má Hesla.
Android má Správce hesel Google.

01 Zámek telefonu

Netriviální PIN alespoň o 6 číslicích*. Podle telefonu přidejte otisk prstu nebo obličej.

02 Google účet

Dvoufázové ověření, nejlépe přístupový klíč (passkey).

`myaccount.google.com › Zabezpečení`

03 Chrome ve Windows

Stejný Google účet. Zapněte Windows Hello před vyplněním hesla.

`Správce hesel Google › Nastavení › Windows Hello`

04 Kontrola hesel

Najde uniklá, slabá a opakovaná hesla.

`passwords.google.com`

* Platí, pokud telefon omezuje počet chybných pokusů po sobě (NIST SP 800-63B-4).

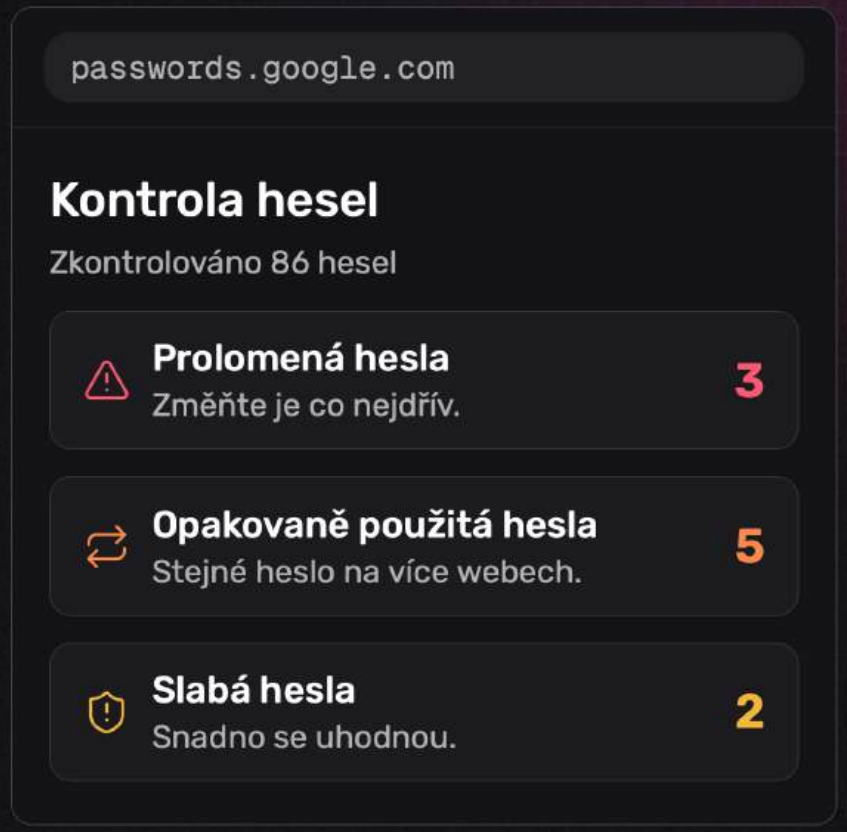
ANDROID A WINDOWS

Kontrola hesel od Googlu. Najde uniklá i opakovaná.

Stačí otevřít passwords.google.com a spustit kontrolu. V telefonu i v počítači.

Uniklá hesla změňte jako první.

ILUSTRAČNÍ NÁHLED



Hesla v prohlížeči? Ano.
Ale jen na počítači bez virů.

Aktualizace

AUTOMATICKY

Systém i prohlížeč.

Legální programy

Z OFICIÁLNÍCH ZDROJŮ

Žádné cracky ani neoficiálně upravené programy.

Antivirus

ZAPNUTÝ A AKTUÁLNÍ

Ve Windows stačí vestavěný Microsoft Defender.

Ověření

PŘED VYPLNĚNÍM

Windows Hello, otisk nebo obličej.

SDÍLENÍ HESEL

Vlastní hesla v Googlu: ano. Jeden účet pro celou firmu: nikdy.

Firma spravuje hesla přes firemního správce hesel, kde je možné přístup každému zvlášť odebrat.

Vestavěný správce stačí jednotlivcům.
Firma potřebuje firemní správu.

HLEDISKO	Vestavěný APPLE, GOOGLE, MICROSOFT	Firemní BITWARDEN, 1PASSWORD, HEYLOGIN (EU), PASSBOLT (EU)
CENA	Zdarma.	Pár eur na člověka měsíčně podle tarifu.
ZAŘÍZENÍ	Omezeně.	Všechna běžná.
SDÍLENÍ V TÝMU	Omezené.	Ano, s právy.
KDO ŘÍDÍ PŘÍSTUP	Každý sám.	Firma.
ODCHOD ZAMĚSTNANCE	Hesla mu zůstanou.	Odeberete přístup a změníte hesla.

Firemní správce hesel v kostce.
Začněte s jedním kolegou.

01 Firemní účet

Hlavní heslo jako fráze, pokud ho správce používá, a druhý zámek. Data v EU, pokud to služba nabízí.

02 Druhý správce

Vlastní účet, vlastní heslo, vlastní druhý zámek. Nikdy sdílený.

03 Sdílené složky

Třeba Účetnictví, Sociální sítě, Web a doména. Zkuste cvičnou položku.

04 Přesun hesel

Nejdřív e-mail, účetnictví a sociální sítě. Pak vypněte ukládání v prohlížečích a zapněte vyplňování ze správce hesel.

Heslo je to, co víte. Druhý zámek je to, co máte.

Odborně dvoufaktorové nebo vícefaktorové ověření (2FA, MFA).

Jeden zámek navíc.
Obrovský rozdíl.

99,2 %

nižší riziko převzetí účtu se zapnutým vícefaktorovým ověřováním.

Studie Microsoftu na firemních účtech.

Druhý zámek není jen jeden.
Vyberte ten nejsilnější.

Jen heslo

SLABÉ

Stačí ho ukrást nebo vylákat.

Kód z SMS

DOBRÉ

Lepší než nic. Dá se ale vylákat nebo přesměrovat.

Ověřovací aplikace

LEPŠÍ

Kód nebo potvrzení v aplikaci. Kód lze vylákat a cizí přihlášení omylem schválit.

Přístupový klíč

NEJLEPŠÍ

Odemyká se otiskem, obličejem nebo PINem. Na falešné stránce nefunguje.

Orientační srovnání.

POZOR NA TELEFONÁTY

Kód nikdy nikomu. Ani „bance“. Ani „Microsoftu“.

A neschvalujte přihlášení, které jste sami nezačali.

Pravidlo 3Z: Zastav. Zavěs. Zkontroluj - třeba na čísle z oficiálního webu.



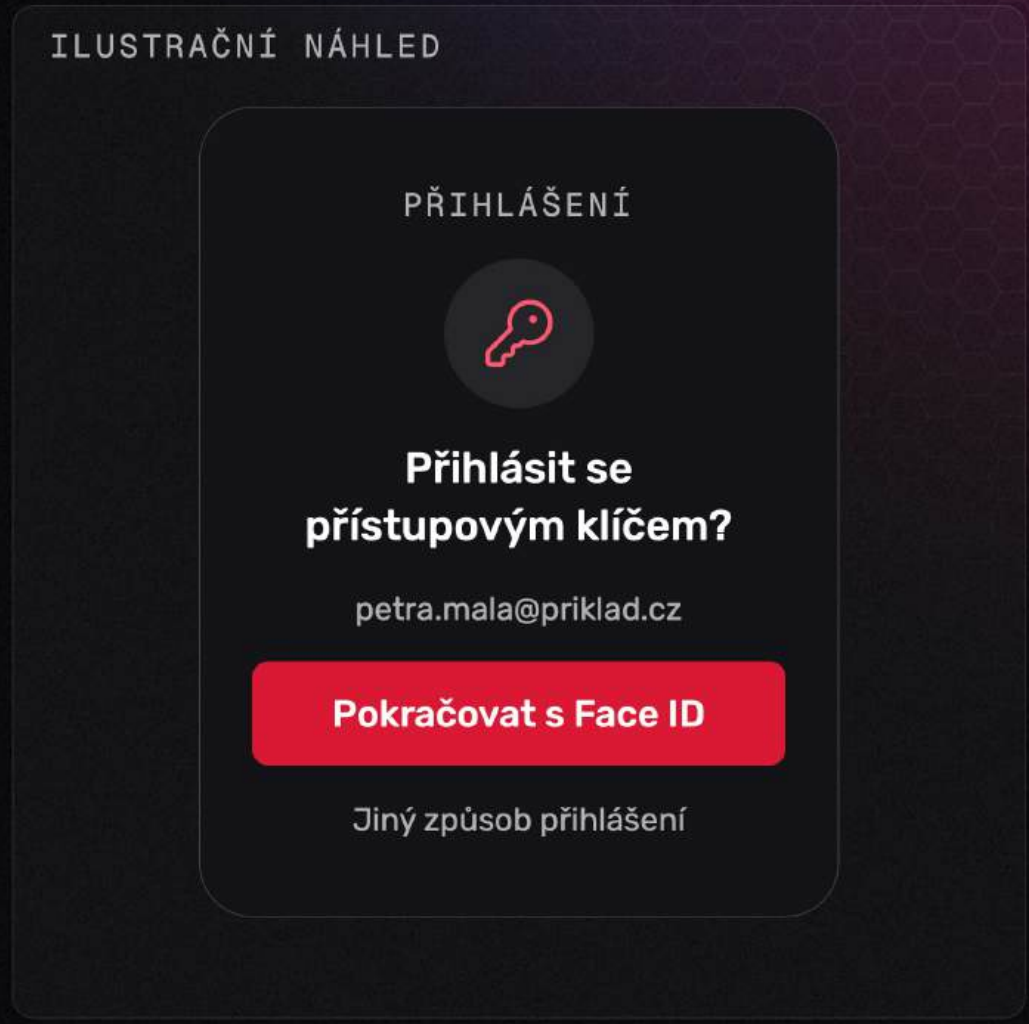
PŘIHLÁŠENÍ BEZ HESLA

Nejlepší heslo je žádné heslo. Přístupový klíč (passkey).

Odemknete ho otiskem, obličejem nebo PINem. Nahradí heslo i opisování kódu a na falešné stránce nefunguje.

Začněte u účtů Google a Microsoft.

ILUSTRAČNÍ NÁHLED



Zamčeno na dva zámky.
Teď ještě náhradní klíč.

ZÁLOHOVÁNÍ

Synchronizace není záloha. Co smažete v telefonu, zmizí všude.

Ztráta přístupu k účtu může zablokovat i uložená hesla. Proto si předem připravte záchranné kódy a obnovovací údaje.

Telefon se ztratí.
Účty vám zůstanou.

01 Záložní druhý zámek

Druhé zařízení nebo bezpečnostní klíč. Ne všechno jen v jednom telefonu.

02 Záchranné kódy*

Kde je služba nabízí, vytiskněte je a uložte mimo telefon.

03 Obnovovací údaje

Aktuální telefon a e-mail. U Apple navíc kontakt pro obnovení.

04 Zkouška obnovy

Ověřte, že se do e-mailu a správce hesel dostanete i bez původního telefonu.

* Často nahradí jen ztracený druhý zámek, ne hlavní heslo. Postup ověřte v nápovědě svého správce hesel.

Zaměstnanec odchází.
Hesla zůstávají ve firmě.

Odeberte přístup

SPRÁVCE HESEL

Ve firemním správci hesel.

Změňte hesla

HESLA

Všechna, která znal.

Odhlaste ho

ZAŘÍZENÍ

Ze všech firemních služeb. Odeberte i jeho přístupové klíče a ověřovací zařízení.

Zablokujte účty

SLUŽBY

Data převeďte, pak účty zrušte.

Pět kroků.
Ještě tento týden.

PRO VŠECHNY

- [ ] Zabezpečte e-mail: fráze a druhý zámek
- [ ] Zapněte správce hesel
- [ ] Druhý zámek na sociální sítě
- [ ] Zkontrolujte svůj e-mail na haveibeenpwned.com
- [ ] Bezpečně uložte záchranné kódy

NAVÍC PRO FIRMY

- [ ] Každý zaměstnanec má vlastní účet
- [ ] Firemní správce se dvěma správci
- [ ] Postup pro odchod zaměstnance
- [ ] Hesla nikdy přes WhatsApp ani e-mail
- [ ] Automatické aktualizace všude

JEDNA VĚC NA ZÁVĚR

Zamkněte e-mail na dva zámky. Ještě dnes.

Redamp.io

pro podnikavé

Děkuji.
Ptejte se.

Ing. Dominik Malčík, Ph.D.

Zakladatel a CEO, Redamp.io

dominik.malcik@redamp.io • +420 724 844 313

Více o Redamp.io

redamp.io →