Digitální sebeobrana pro normální lidi

co má cenu řešit a co ne

Petr Krčmář



7. listopadu 2026

Uvedené dílo (s výjimkou obrázků) podléhá licenci Creative Commons Uveďte autora 3.0 Česko.

O mně

- linuxák od roku 1998
- správce serverů
- lektor a konzultant
- šéfredaktor Root.cz
- člen vpsFree.cz
- organizátor LinuxDays
- můj web je petrkrcmar.cz



ROOT.CZ vpsFree.cz

Prezentace už teď na webu

www.petrkrcmar.cz

ROOT.CZ vpsFree.cz

Kam a proč míříme?

Před čím se bráníme

- **phishing** a podvodné zprávy
- falešné přihlašovací stránky
- krádež nebo prolomení účtu
- opakovaně používaná či uniklá **hesla**
- škodlivé aplikace a podvodné weby
- ztráta nebo krádež zařízení
- zneužití účtu po **úniku dat** ze služby
- podvodné telefonáty a vydávání se za někoho jiného

Phishing



Fio banka

Vážený zákazníku

Váš účet Fio Banka byl dočasně pozastaven, dokud majitel účtu nepotvrdí svou totožnost.

Kliknutím sem ověřte svůj účet

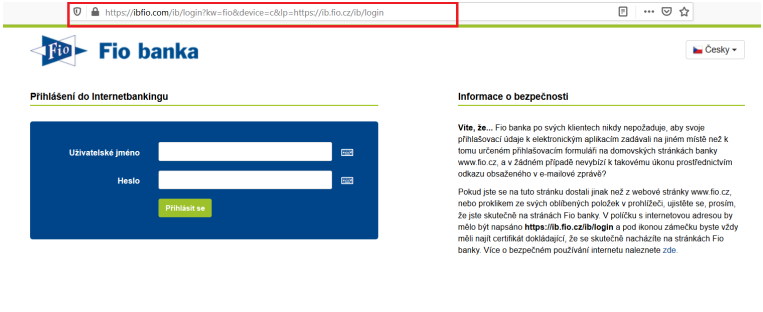
© Fio Banka. Všechna práva vyhrazena.

Unsubscribe Odhlásit odběr

Kdo a proč útočí

- podvodníci hledající **peníze**
- útočníci usilující o přístup k účtům
- automatické programy zkoušející uniklá **hesla**
- falešné profily lákající ke kliknutí nebo platbě
- zloději zařízení – získají přístup k datům
- lidé zneužívající nalezené přihlášení
- útoky často míří na mnoho lidí najednou
  - cílený útok na konkrétního člověka je jiný scénář

Phishing


https://ibfio.com/ib/login?kw=fio&device=c&lp=https://ib.fio.cz/ib/login
Fio banka
Česky
Přihlášení do Internetbankingu
Uživatelské jméno
Heslo
Přihlásit se
Informace o bezpečnosti
Víte, že... Fio banka po svých klientech nikdy nepožaduje, aby svoje přihlašovací údaje k elektronickým aplikacím zadávali na jiném místě než k tomu určeném přihlašovacím formuláři na domovských stránkách banky www.fio.cz, a v žádném případě nevybízí k takovému úkonu prostřednictvím odkazu obsaženého v e-mailové zprávě?
Pokud jste se na tuto stránku dostali jinak než z webové stránky www.fio.cz, nebo proklikem ze svých oblíbených položek v prohlížeči, ujistěte se, prosím, že jste skutečně na stránách Fio banky. V políčku s internetovou adresou by mělo být napsáno https://ib.fio.cz/ib/login a pod ikonou zámečku byste vždy měli najít certifikát dokládající, že se skutečně nacházíte na stránkách Fio banky. Více o bezpečném používání internetu naleznete zde.
Platby kartou na internetu
Obáváte se zneužití platební karty na internetu? Nastavte si nulový limit pro internetové platby. Měnit lze on-line a zdarma!
Kontakty
Infolinka 224 346 800
Kontaktní formulář napište nám
Pobočky a bankomaty seznam
Další informace
Desatero bezpečného používání Internetbankingu
Ceníky a sazebníky
Technická podpora, manuály

Digitální sebeobrana

- cílem není být neprůstřelný
- cílem je snížit pravděpodobnost průšvihu
  - a omezit škody, když se něco pokazí
- řešíme běžné účty, zařízení a návyky
- vybíráme opatření podle přínosu a námahy
- počítáme s tím, že každý někdy udělá chybu
- nechceme žít neustále pod tlakem
  - bezpečnost má pomáhat, ne překážet

Co dnes neřešíme

- obranu proti všemocnému útočníkovi
- scénáře určené pro diplomaty nebo tajné služby
- dokonalé soukromí za každou cenu
- každou teoretickou zranitelnost
- složité nástroje bez jasného přínosu
- opatření, která běžnému člověku spíš zkomplikují život
- strach z každého odkazu a každé aplikace
- bezpečnost jako soutěž o nejpřísnější režim

Ochrana zařízení

Nemáme jen mobil



ROOT.CZ vpsFree.cz

Zařízení: tři věci s největším přínosem

- zapnout automatické **aktualizace**
  - aktualizovat systém i aplikace
  - restartovat zařízení, když si aktualizace vyžádá
  - občas zkontrolovat, že aktualizace opravdu probíhají
- používat PIN nebo heslo pro **odemykání**
  - nastavit automatické zamykání obrazovky
  - zamknout zařízení, když od něj odcházím
- pravidelně **zálohovat** důležitá data
  - ochrana proti ztrátě i vydírání

ROOT.CZ vpsFree.cz

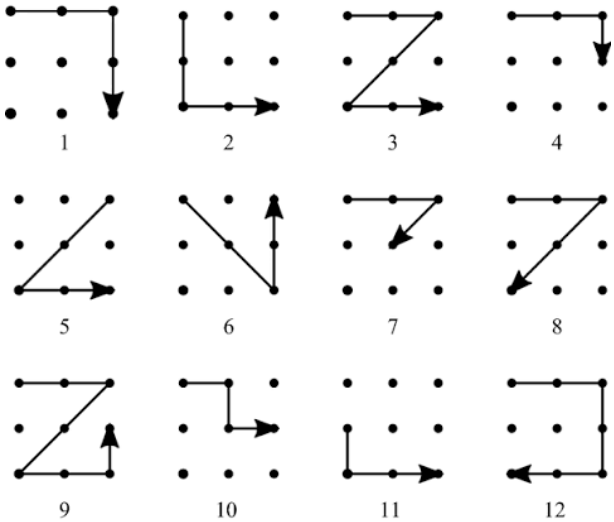
Aktualizace: jednoduchá pojistka

- opravují známé bezpečnostní **chyby**
  - týkají se systému i jednotlivých aplikací
- zapnout automatické aktualizace, kde to jde
  - aktualizovat také prohlížeč a aplikace na dokumenty
  - **neodkládat** výzvu k aktualizaci na neurčito
- po aktualizaci zařízení případně restartovat
- ověřit, že zařízení má dost místa a aktualizace se instalují
- staré zařízení bez bezpečnostní podpory časem vyměnit

Zámek, aplikace a každodenní návyky

- nastavit PIN nebo heslo, které nelze snadno uhodnout
- zapnout automatické **zamknutí** při nečinnosti
  - zamykat obrazovku i při krátkém odchodu
- aplikace instalovat z oficiálního obchodu
  - před instalací zkontrolovat, kdo aplikaci vydal
- odebrat aplikace, které už nepoužívám
- povolovat aplikacím jen **oprávnění**, která potřebují
- zařízení bez podpory výrobce vyměnit

Obrazce



Pohodlí jménem biometrie

- otisk prstu usnadňuje každodenní odemykání
- stejně potřebujeme PIN nebo heslo jako záložní způsob přístupu
  - PIN nesmí být snadno uhádnutelný
- po restartu může zařízení vyžadovat PIN nebo heslo
- biometrie **nechrání účet**, pokud unikne jeho heslo
- otisk prstu používejte k odemykání svého zařízení
  - místní přístup, ne prokázání identity službám
  - není to náhrada silného hesla k účtům
- biometrie je kompromis mezi **pohodlím a ochranou**

Záloha: pojistka proti ztrátě i vydírání

- určit, které soubory by bolelo ztratit
- nastavit **automatickou** zálohu
- zálohovat také fotografie, kontakty a dokumenty
- **ověřit**, že záloha skutečně obsahuje potřebná data
- občas vyzkoušet obnovu souboru
- externí disk po zálohování odpojit
- cloudovou zálohu chránit přístupem k účtu a šifrováním
- pozor: synchronizace není vždy totéž co záloha

Ochrana účtů

Služeb používáme stovky



Účty: začít u e-mailu

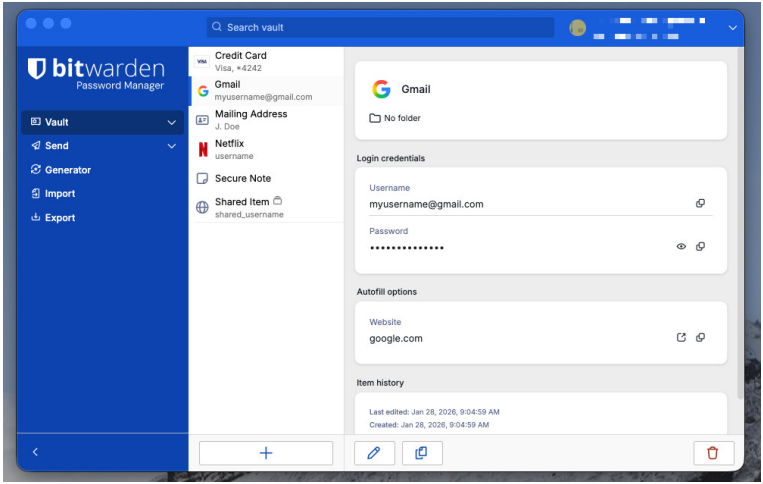
- e-mail často slouží k obnově ostatních účtů
  - proto ho musíme dobře chránit
- nastavit mu jedinečné přihlášení
- zapnout vícefaktorové ověření
- přidat dostupnou náhradní metodu přihlášení
  - uložit obnovovací kódy mimo e-mail
  - zkontrolovat, kam vedou možnosti obnovy účtu
- sledovat aktivní přihlášení a odhlásit neznámá zařízení

Hesla: jedno pro každý účet

- heslo musí být silné, neuhádnutelné a jedinečné
  - znovu použité heslo ohrožuje více účtů najednou
  - hesla ze služeb běžně **unikají**
- správce hesel vytváří a pamatuje jedinečná hesla
  - většinou stačí zapamatovat si jedno hlavní heslo
  - hlavní heslo nepoužívejte nikde jinde
- zapnout vícefaktorové ověření i u správce hesel
- začít u e-mailu, banky a dalších důležitých účtů
- nepoužívat veřejný počítač k ukládání hesel
- přejít na přístupové klíče (passkeys), pokud to služba nabízí

ROOT.CZ vpsFree.cz

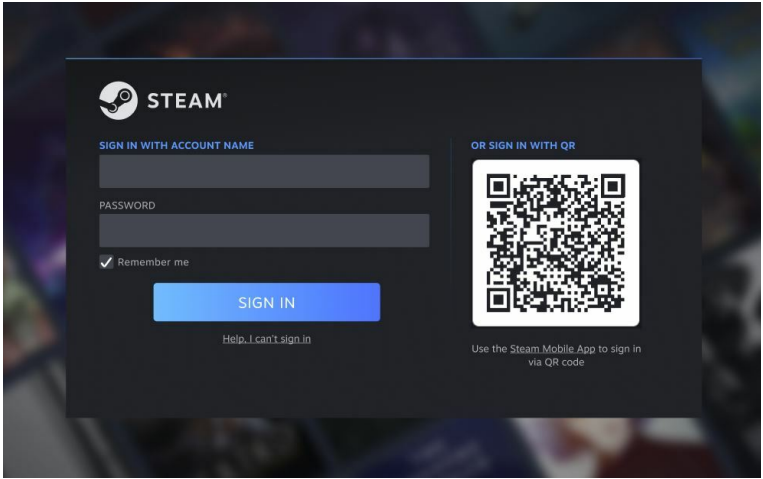
Správce hesel



Vícefaktorové ověření: druhá pojistka

- zapnout ho všude, kde je k dispozici
- začít u e-mailu, správce hesel a sociálních sítí
- vybrat přístupový klíč nebo bezpečnostní klíč, pokud lze
  - jinak použít ověřovací aplikaci
- SMS kód je lepší než žádná druhá vrstva
- nikdy nepotvrzovat přihlášení, které jsem sám nezačal
- nikomu nesdělovat ověřovací kódy
- obnovovací kódy uložit bezpečně a dostupně

Více faktorů



Podvodné přihlášení: zpomalit a ověřit

- neklikat na přihlašovací odkaz z nečekané zprávy
- otevřít službu přes uloženou záložku nebo vlastní aplikaci
- zkontrolovat adresu stránky před zadáním hesla
  - výhoda správce hesel – do cizího webu nevyplní
  - stejně tak passkeys jsou svázané s URL
- podezřelou žádost ověřit jiným komunikačním kanálem
- neposílat heslo ani kód v e-mailu nebo zprávě
- nevěřit naléhání, že účet bude okamžitě zablokován
- při podezření změnit heslo na skutečné stránce služby

Nátlak a emoce



ČS

ČSOB csob.4a61046d@klienti-csob.cz-mail1.xyz

Komu: @seznam.cz

Váš účet ČSOB byl z důvodu vaší bezpečnosti omezen.

ČSOB

Dobrý den,

Zjistili jsme neobvyklé pokusy o přihlášení k vašemu účtu ČSOB.
Z tohoto důvodu jsme dočasně zablokovali váš účet.

Znovu aktivujte svůj účet

Pro případné dotazy jsme Vám samozřejmě k dispozici na naší infolince 800 300 300.

Přejeme příjemný den.

Vaše ČSOB

Odesílatel
Československá obchodní banka, a. s., Radlická 333/150, 150 57 Praha 5, IČO: 00001350,
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B: XXXVI, vložka 46

Když už průšvih přijde

Napadený účet: nejdřív získat kontrolu

- použít vlastní nebo důvěryhodné zařízení
- přejít na oficiální stránku obnovy účtu
- začít e-mailem, pokud přes něj obnovujete další účty
  - zkontrolovat filtry a přeposílání pošty
- změnit heslo napadeného účtu
  - změnit ho i jinde, pokud bylo použito opakovaně
- odhlásit všechna zařízení a aplikace
- zkontrolovat obnovovací údaje a aktivní přihlášení

Účet je zpět: uklidit a upozornit

- zapnout vícefaktorové ověření
- odstranit neznámé aplikace s přístupem k účtu
- zkontrolovat odeslané zprávy a příspěvky
- odstranit neznámá pravidla přeposílání e-mailů
- prověřit nákupy a pohyby na účtech
- při podezřelé platbě kontaktovat banku oficiální cestou
- upozornit kontakty, ať nevěří podezřelým zprávám
- pokud se do účtu nedostanu, pokračovat přes podporu služby

Ztracený telefon nebo počítač

- ověřit, že zařízení není jen odložené jinde
- použít službu pro nalezení zařízení z jiného přístroje
- zařízení na dálku zamknout
- při krádeži telefonu kontaktovat operátora a zablokovat SIM
- odvolat přístup ztraceného zařízení k důležitým účtům
- změnit hesla k účtům přihlášeným na zařízení
- kontaktovat banku, pokud v něm byly platební údaje
- zvážit vzdálené smazání zařízení

Obnova dat ze zálohy

- nejdřív určit, co se ztratilo a co zůstalo
- ověřit datum a obsah poslední zálohy
- obnovovat jen data, která skutečně potřebuju
- po krádeži účtu nejdřív zabezpečit účet a změnit přístup
- důležité soubory zkontrolovat před opětovným použitím
- ověřit, že obnovená data fungují
- po obnově nastavit automatické zálohování znovu

Co funguje a co ne

Mýty a omyly: co samo o sobě nepomůže

- veřejná Wi-Fi znamená automaticky nebezpečí
- VPN mě udělá na internetu neviditelným
- anonymní okno skryje mou aktivitu před všemi
- antivir vyřeší každé bezpečnostní riziko
- když mám Mac nebo iPhone, problémy se mě netýkají
- častá změna hesla je základ bezpečnosti
- smazání historie smaže i všechna data o mně
- zakrytá kamera znamená, že mě nikdo nemůže sledovat

Co dělat místo toho

- veřejnou Wi-Fi používejte, ale dodržuje běžná opatření
- VPN šifruje spojení k poskytovateli VPN, ne celý provoz
- anonymní okno hlavně neukládá historii do zařízení
- antivir doplňuje aktualizace, opatrnost a zálohy, nenahrazuje je
- každé zařízení potřebuje aktualizace bez ohledu na značku
- heslo změňte hlavně při podezření na únik nebo zneužití
- omezení cookies může pomoct s částí sledování, ne se vším
- kameru zakrýt můžete, ale chraňte i účty, mikrofon a zařízení

Co si zapamatovat

Co si odnést

- zapněte automatické aktualizace zařízení i aplikací
- zamykejte obrazovku – použijte PIN nebo heslo
- používejte jedinečné heslo pro každý účet
- nechte správce hesel dělat jeho práci
- zapněte vícefaktorové ověření, hlavně u e-mailu
- zálohujte důležitá data a občas zkuste obnovu
- při podezřelé zprávě se zastavte a přemýšlejte
- když už se něco stane, nejdřív zabezpečte hlavní e-mail a účty

ROOT.CZ vpsFree.cz

Bezpečnost nemusí být složitá

- začněte jedním opatřením, které můžete udělat hned
- největší přínos často přinesou obyčejné návyky
- soustřeďte se na účty a zařízení, která používáte
- ne každé riziko vyžaduje nový nástroj
- dokonalá ochrana není realistický cíl
- lepší je jednoduché opatření, které opravdu používáte
- plán obnovy snižuje škody, když se něco pokazí
- digitální sebeobrana je průběžná údržba, ne jednorázový projekt

Odkazy

- NÚKIB: Základy kybernetické bezpečnosti
- NÚKIB: Osvětová kampaň Kyberštít
- NÚKIB: Ochraňte svůj domov proti hackerům
- NÚKIB: Doporučení
- DIA: Bezpečnost elektronické identity
- Safer Internet Centrum
- CSIRT.CZ: Projekty a služby

Otázky?



Petr Krčmář
petr.krcmar@iinfo.cz