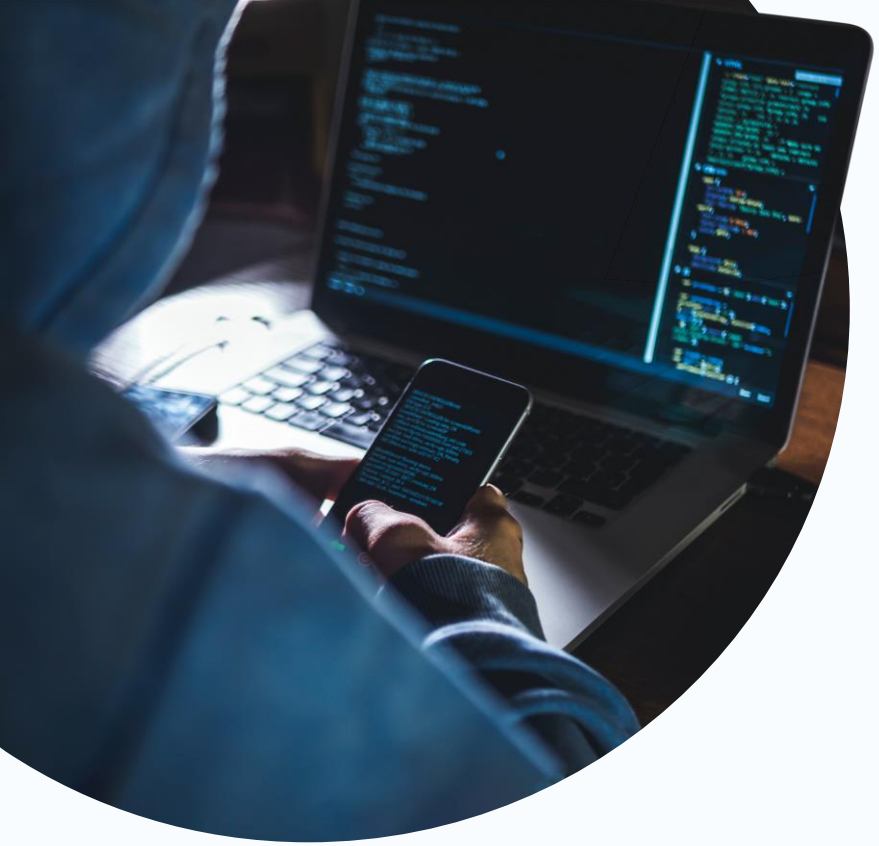


ČSOB
jdeme vám naproti

Digitální moudrost

Hrozby v digitálním světě a zabezpečení vašich financí

Fórum dárců, Hradec Králové

27.04.2026

Petr Vosála

- Manažer bezpečnosti digitálních kanálů skupiny ČSOB
- Bankovní praxe 25+ let

Kyberkriminalita se týká každého z nás

- Volač a Klikač okrádají Česko!
- Jdou po vašich penězích, heslech, PINech, kartách, ...
- Ukradli už miliardy korun

Počet registrovaných skutků na internetu

Zdroj: Policie ČR

Novodobí „šmejdi“ digitálního světa

Volač
vás může okrást
telefonátem

Klikač
vás může okrást,
když kliknete „vedle“

Fyzická vs. digitální existence (identita)

Dva světy = dvě existence (identity)

Chránit musíme obě, digitální podceňujeme

Fyzický útok je ojedinělý, digitální spíše naopak

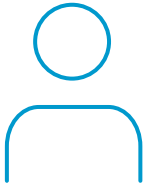
Fyzický útok poznáme hned, digitální ne

Trendy posledních let

Počet útoků na data a účty klientů meziročně roste

Útoky jsou důmyslnější, organizovanější a úspěšnější

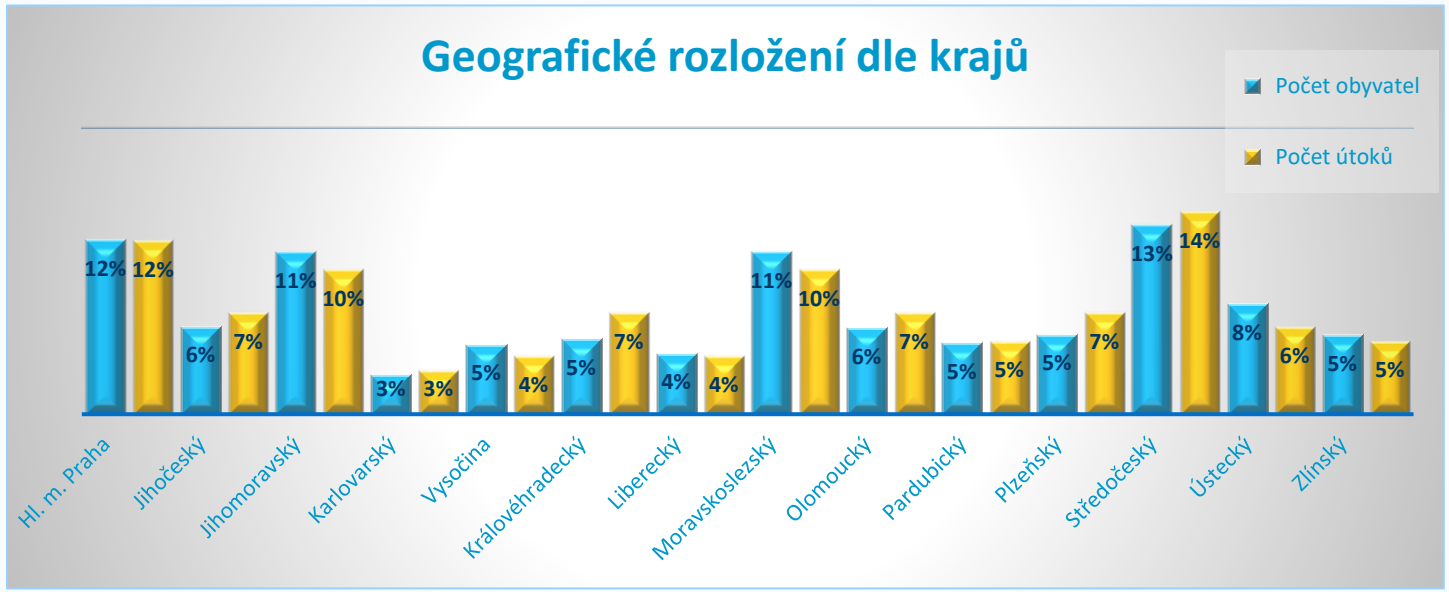
Banky jsou obvykle dobře chráněny



Nejslabší článek je neznalý či nepozorný uživatel

Obětí může být kdokoliv z nás

- Muži 36%, ženy 64% (poměr škody 57% vs 43%)
- 31% VŠ vzdělání
- Nejčastěji ve věku 40 až 49 let
- Nejstarší 88 let a nejmladší 15 let, průměrný věk 40 let
- Průřezově napříč celou republikou



S čím se nejčastěji setkáváme I

- **Podvodné maily/SMS/WhatsApp (phishing)**

zprávy, které se tváří jako zprávy od banky, pošty, přepravní společnosti či jiné důvěryhodné instituce, cílem útočníků je vylákat číslo karty, přihlašovací údaje do internetového bankovnictví, data o platebních kartách apod.

- **Podvodná volání (vishing)**

útočník kontaktuje klienta v rámci nákupu investic do kryptoměny (akcie ČEZu apod.) a přesvědčí ho o nutnosti udělení přístupu do svého počítače přes vzdálenou správu nebo mu „zachrání“ peníze z napadeného účtu vkladem na technický účet (legenda „Falešný bankéř“)

Už to na vás někdo zkusil? Uvěříte vlastní IT podpoře po telefonu?

S čím se nejčastěji setkáváme II

- **Podvodná vylákání plateb - CEO fraud**

Podvodník si na internetu vyhlédne firmu, zjistí kdo je manažer, kdo zpracovává faktury a jaká je firemní kultura. Odešle jménem manažera účetní e-mail ve smyslu: „Realizoval jsem obchod a potřebuji odeslat peníze, expresně“, následuje částka a číslo účtu (může i volat - AI)

- **Podvodné faktury**

Podvodné faktury vypadají na první pohled velmi věrohodně, liší se pouze v detailech: přijdou z jiné e-mailové adresy, platba má být uskutečněna ve prospěch jiného účtu než obvykle, je uvedena jiná kontaktní osoba s jiným telefonním číslem pro případné ověření; může jít o „man in the middle“ útok

Jak ověřujete oprávněnost fakturace před proplacením? Jak poznáte v mailu nebo po telefonu svého „šéfa“, nebo, stačí vaše rozhodnutí po telefonu, pokud jste v pozici šéfa vy sami?

S čím se nejčastěji setkáváme III

- **Bazarové podvody**

prodávající na online bazaru je podvodníkem kontaktován pro ověření účtu nebo požádán o vyplnění čísla karty, na kterou mu podvodník, jakožto kupující, zašle peníze za zakoupené zboží. Podvodný zájemce se objeví zpravidla velmi rychle po uveřejnění inzerátu

- **Převzetí SIM karty (SIM swap)**

„klientský poradce mobilního operátora“ klienta telefonicky vyzve ke stažení aplikace pro správu mobilních služeb. Prostřednictvím aplikace si pak útočník nechá vystavit tzv. e-SIM s telefonním číslem klienta a ta mu pak umožní přístup k dalším citlivým údajům, e-mailům, sociálním sítím apod.

Poslali byste někomu, třeba v rámci rodiny, přihlašovací údaje do internetového bankovnictví? Co když vás někdo požádá o autorizační kód v SMS?

S čím se nejčastěji setkáváme IV

- **Vyděračské programy - Ransomware**

Cílem útoku je zašifrovat data a znemožnit k nim přístup. Podvodníci následně požadují výkupné (obvykle v Bitcoinech s tvrzením, že pokud uživatel zaplatí, znovu získá přístup ke svým souborům. Ani zaplacení však neposkytuje garanci rozšifrování (navíc je trestné)

- **Fyzická bezpečnost (síťové prvky, ID karty)**

Pokud je společnost příliš otevřená v komunikaci týkající se používaných technologií, interních mechanismů chodu firmy, či v případě, že zaměstnanci vystavují (např. na LinkedIn) fotografie vstupních karet, mají podvodníci větší šanci úspěšně zaútočit

Jak bezpečné jsou vstupy do vaší firmy? Jak snadné je instalovat něco na vašich počítačích?

6 nejčastějších podvodů zaměřených na seniory

1. **Podvodné zprávy (Phishing)**
   Nevyžádaný e-mail, SMS, či zpráva na sociálních sítích - podvodník se vydává za důvěryhodnou společnost (např. banku, přepravní společnost, poštu) a požaduje, abyste klikli na odkaz a poskytli mu přihlašovací údaje k účtu
2. **Romantické podvody (Romance fraud)**
   Podvodníci si vytvoří falešné profily na seznamkách, spřátelí se s osamělými srdci a vybudují si s nimi vztah s cílem vylákat peníze např. „na cestu za svou láskou...“
3. **Podvody při online nakupování**
   Podvodníci vytvářejí důvěryhodně vypadající internetové obchody a lákají k jejich návštěvě. Zboží je často za neuvěřitelné ceny

6 nejčastějších podvodů zaměřených na seniory

4. **Investiční podvody**
   Podvodníci vám nabídnou možnost rychlého zbohatnutí, slibují nízké riziko a zaručené výnosy, často prostřednictvím investic do kryptoměn
5. **Loterijní podvody**
   Podvodník zavolá a tvrdí, že jste vyhráli v loterii a jediné, co musíte udělat, abyste získali svou výhru, je poslat předem malý poplatek za zpracování, odeslání nebo daň
6. **Podvody prarodičů**
   Podvodník vám neohlášeně zavolá a vydává se za příbuzného v ohrožení. Obvykle začne slovy jako “Ahoj babičko, víš, kdo to je?” a pak pokračuje příběhem, který vás má přesvědčit abyste mu poskytli peníze

volně dle: https://cyberblog.cz/nejnovejsi/10-nejcastejsich-podvodu-zamerenych-na-seniory-a-jak-ochranit-sve-penize

Příběhy jak z Hollywoodu

Panu Jelínkovi z ničeho nic volají z banky, že mají na jeho jméno sjednanou několikasettisícovou půjčku. Pan Jelínek jako dlouholetý klient úplně jiné banky si je naprosto jistý, že o žádnou půjčku nežádal, a že musí jít o nějaký omyl. Nedej bože rovnou o podvod.

„Dobrá," tvrdí operátor z cizí banky, „my to prověříme, zavoláme do vaší banky a na policii". Pan Jelínek je z telefonátu nervózní, a do toho mu za pár minut zvoní mobil znovu. Tentokrát volá někdo z banky, kde má opravdu účet. A dozvídá se, že jeho účet opravdu někdo chtěl napadnout!

„Zatím buďte v klidu. Snad vám ještě stihneme ty peníze zachránit. Musíte ale jednat rychle a dělat přesně to, co vám řeknu," klade na srdce panu Jelínkovi hlas v telefonu. Konto je potřeba restartovat, tedy vybrat z něj všechnu hotovost a převést ji na speciální dispoziční účet.

Panu Jelínkovi to přijde zvláštní, v tu ránu se mu ale dostane telefonické ubezpečení přímo od policie. Hlas zní profesionálně a přesvědčivě: „Váš případ monitorujeme, vybrané bankovky budou označené a všechno máme na kamerách. Následujte pokyny od své banky a bude to v pořádku."

Policistou uchlácholený pan Jelínek splní pokyny operátora do puntíku. Vybere všechnu hotovost, ke které si ještě další peníze půjčí online na telefonickou radu pána z banky. Po částech pak všechno navkládá do kryptoměnového bankomatu, dohromady víc než 600 000 Kč. Že je to celé habaďůra, zjišťuje pan Jelínek teprve ve chvíli, kdy přijde osobně na pobočku své banky, kde nikdo o ničem neví. To už je ale pozdě. Případ teď řeší s opravdovou policií a není vůbec jisté, že své peníze ještě někdy uvidí.

Jak nenaletět kyberzločincům

1. PINy a hesla nikomu neprozrazujte. Ani bance ani policii, prostě nikomu
2. Nespěchejte. Chladná hlava je důležitější než rychlost
3. Vždy dávejte pozor, kam se hlásíte, za co platíte a co potvrzujete
4. Nevěřte pohádkám o bohatství bez práce a bez rizika
5. Nepouštějte si do počítače cizí lidi

Jak se chovat k chytrému telefonu

1. Nastavte si zámek obrazovky
2. Stahujte aplikace pouze z důvěryhodných zdrojů
3. Instalujte si bezpečnostní aktualizace operačního systému, prohlížeče a aplikací
4. Sledujte oprávnění vyžadovaná při instalaci aplikací
5. Nainstalujte si antivirový program

Desatero bezpečného bankovnictví

1. Používejte bezpečný počítač/telefon
2. Chraňte své přihlašovací údaje
3. Hesla volte pečlivě
4. Mobil nedávejte z ruky
5. Adresu internetového bankovnictví zadávejte ručně

6. Neotvírejte podezřelé e-maily a soubory
7. Neklikejte na neznámé odkazy
8. Průběžně kontrolujte historii plateb
9. Čtěte komunikaci s bankou
10. Neváhejte se kdykoliv zeptat své banky

Braňte se rozumem - https://www.csob.cz/branteserozumem

10 nejnebezpečnějších kybernetických hrozeb

FALEŠNÝ BANKÉŘ
Nenaleťte příběhu o napadeném účtu

PODVODNÉ INVESTICE
Nevěřte na zázračné zbohatnutí

LÁSKA MEZI KONTINENTY
Nedůvěřujte pohádkovým princům a pri

PODVODNÉ SMS A E-MAILY
Nedávejte z ruky své citlivé údaje

DEZINFORMACE
Nenechte se vyděsit manipulativními z

PRODEJE A NÁKUPY
cházejte zbytečně o zboží nebo peníze

JÁ, PODVODNÍK?
Neuděleite ze sebe bílého koně

KYBERŠIKANA
Nenechte se fackovat ani na sociálních sítích

DIGITÁLNÍ IDENTITA
Chraňte si své soukromí i v on-line světě

UMĚLÁ INTELIGENCE
Prezident mi doporučuje výhodnou investici???

Děkuji vám za pozornost

a chovejme se digibezpečně!

ČSOB
jdeme vám naproti