

Kyberpodvody 2026

vývoj, trendy, psychologie obětí i e-šmejdů

Helena Sováková, Pavel Šašek

KYBERNETICKÉ PODVODY 1. POLOLETÍ 2026 – SHRNU TÍ

Scénáře se mění, ale princip zůstává stejný: emoce, autorita a časový tlak

ROZSAH PODVODŮ ROSTE

+33 %

napadených karet

+49 %

napadených klientů
v oblasti
platebního styku

NEJVĚTŠÍ HROZBY

61 %

phishing
Karetní podvody

48 %

investice a krypto
Platební podvody

39 %

Vishing
Platební podvody

Nové formy podvodů mají stejný cíl: přimět oběť jednat bez ověření

Úroveň zabezpečení



NOVÉ A SÍLÍCÍ SCÉNÁŘE

- 01 osobní **předání hotovosti** falešnému kurýrovi;
- 02 **falešná bankovní aplikace** a **NFC relay** attack;
- 03 zneužití skutečných **rezervací ubytování**;
- 04 **převzetí WhatsApp profilu** a žádosti o půjčku.

POČET KYBERÚTOKŮ VZROSTL V 1. POLOLETÍ O **41 %**

KARETNÍ PODVODY – 1. POLOLETÍ ROKU 2026

- 33 %** nárůst napadených karet
- 61 %** phishing
- 80 %** nárůst objemu podvodných transakcí
- 45 %** zvýšení klientských škod v rámci podané reklamace
- 4900 Kč** průměrná částka

PLATEBNÍ PODVODY – 1. POLOLETÍ ROKU 2026

- 49 %** nárůst napadených klientů
- 48 %** investiční podvody
- 39 %** vishing
- 110 %** nárůst objemu podvodných transakcí
- 150 %** zvýšení klientských škod
- 76 %** nárůst zachráněných prostředků
- 199 000 Kč** průměrná částka

KB V BOJI PROTI E-ŠMEJDŮM

24/7

expertní dohled

300+

preventivních a detekčních pravidel

DATA

historie, lokace, IP adresy a další signály

OBLAST KARETNÍCH PODVODŮ

AKTUÁLNÍ SCÉNÁŘE



PODVODNÉ ZPRÁVY A EMAILY



INVESTICE A KRYPTOMĚNY



WHATSAPPOVÉ PODVODY



NFC RELAY ATTACK



PŘEDÁNÍ HOTOVOSTI



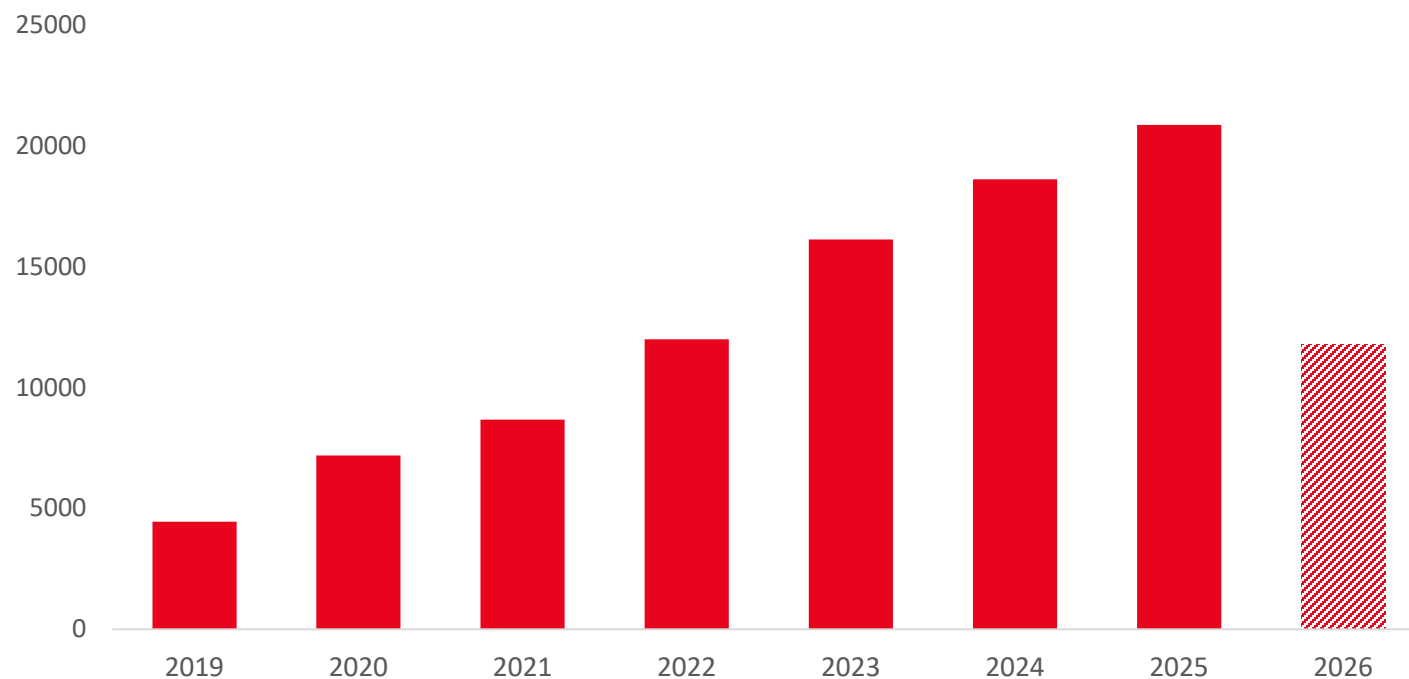
REZERVACE UBYTOVÁNÍ



PODVODNÉ ESHOPY

Úroveň zabezpečení

Počet napadených karet 2019 – 1H 2026



KARETNÍ PODVODY V DATECH



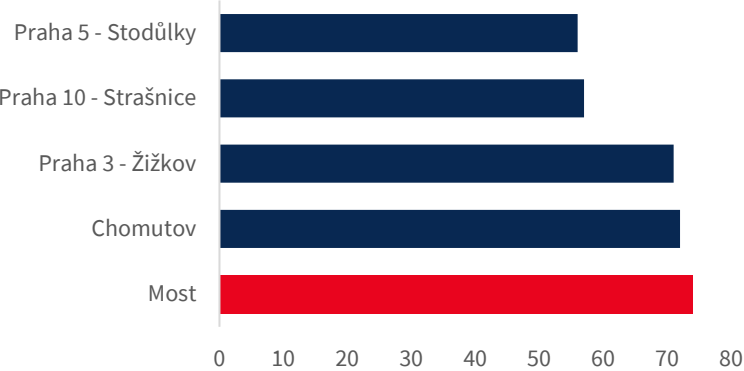
Úroveň zabezpečení

POHLAVÍ



TOP 5 LOKALIT

počet evidovaných případů



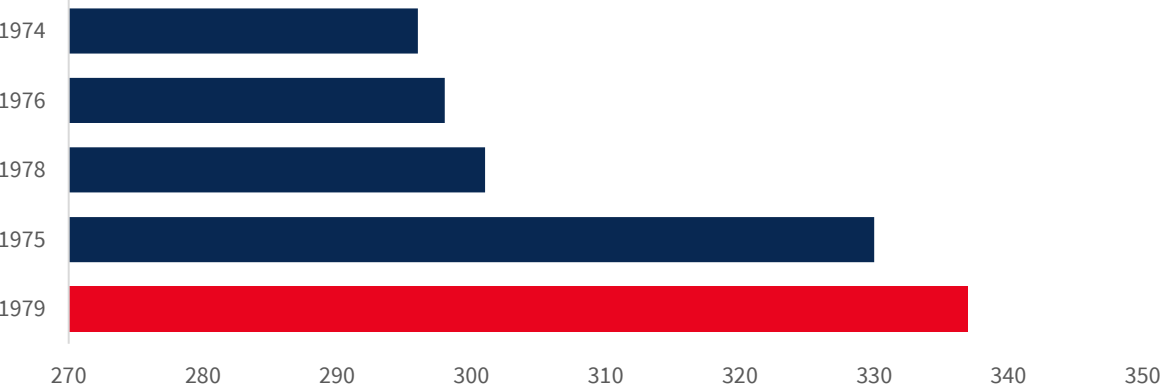
NEJČASTĚJŠÍ JMÉNA

TOP 5 podle pohlaví

PETR	362	JANA	262
JAN	348	KATEŘINA	154
JIRÍ	320	PETRA	151
MARTIN	291	LENKA	146
PAVEL	261	HANA	146

NEJČASTĚJŠÍ ROKY NAROZENÍ

počet evidovaných případů

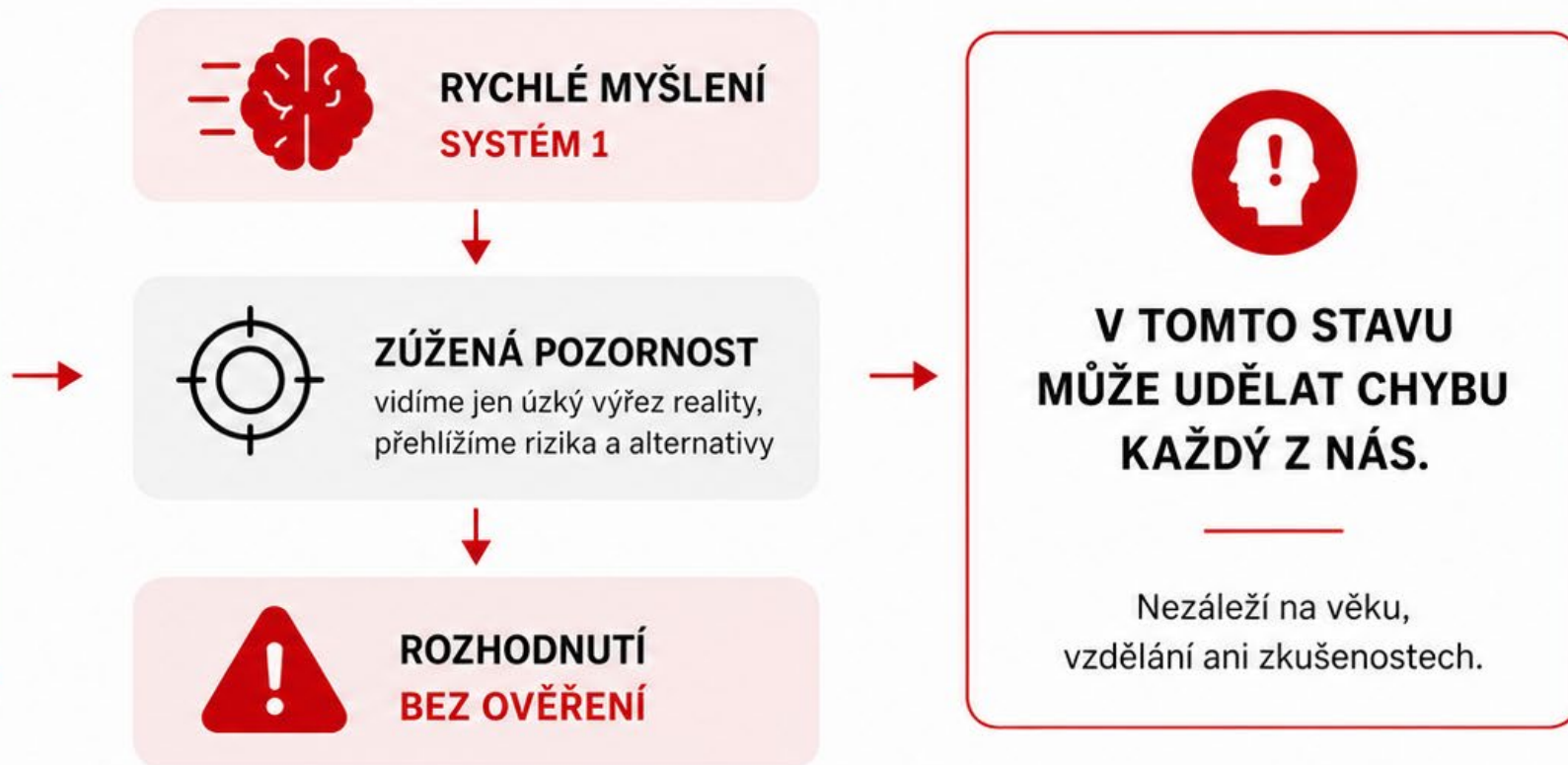


PROČ NALÉTNOU CHYTŘÍ LIDÉ?

Podvodník neútočí na naši inteligenci. **Útočí na naše emoce.**

CO PODVODNÍK V NÁS VYVOLÁVÁ

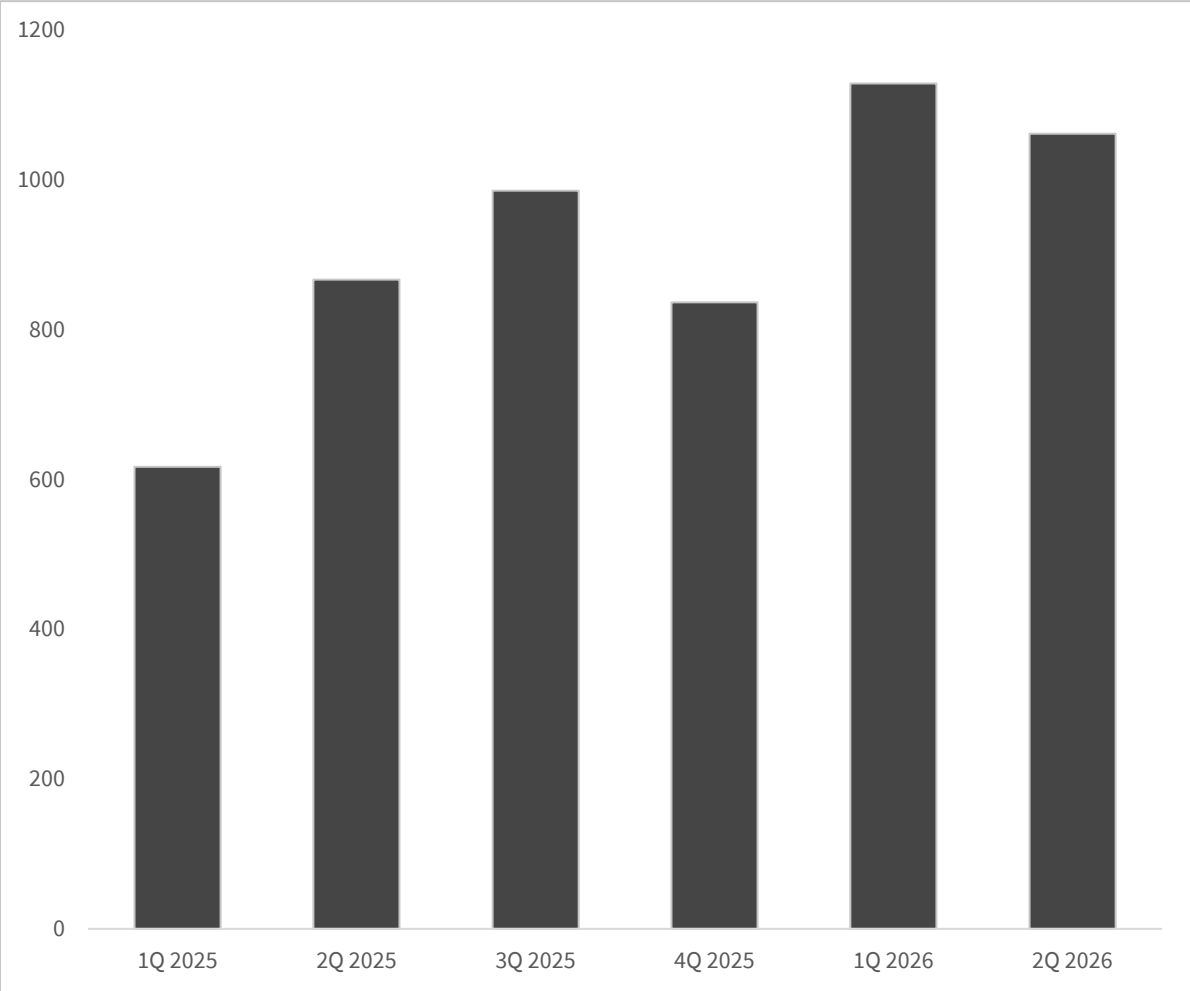
-  **STRACH**
ze ztráty, problému,
ohrožení
-  **ČASOVÝ TLAK**
musíte jednat hned,
bez odkladu
-  **IZOLACE OD OSTATNÍCH**
„Nikomu to neříkejte.“
-  **OKAMŽITÉ JEDNÁNÍ**
neodkládejte,
jednejte teď



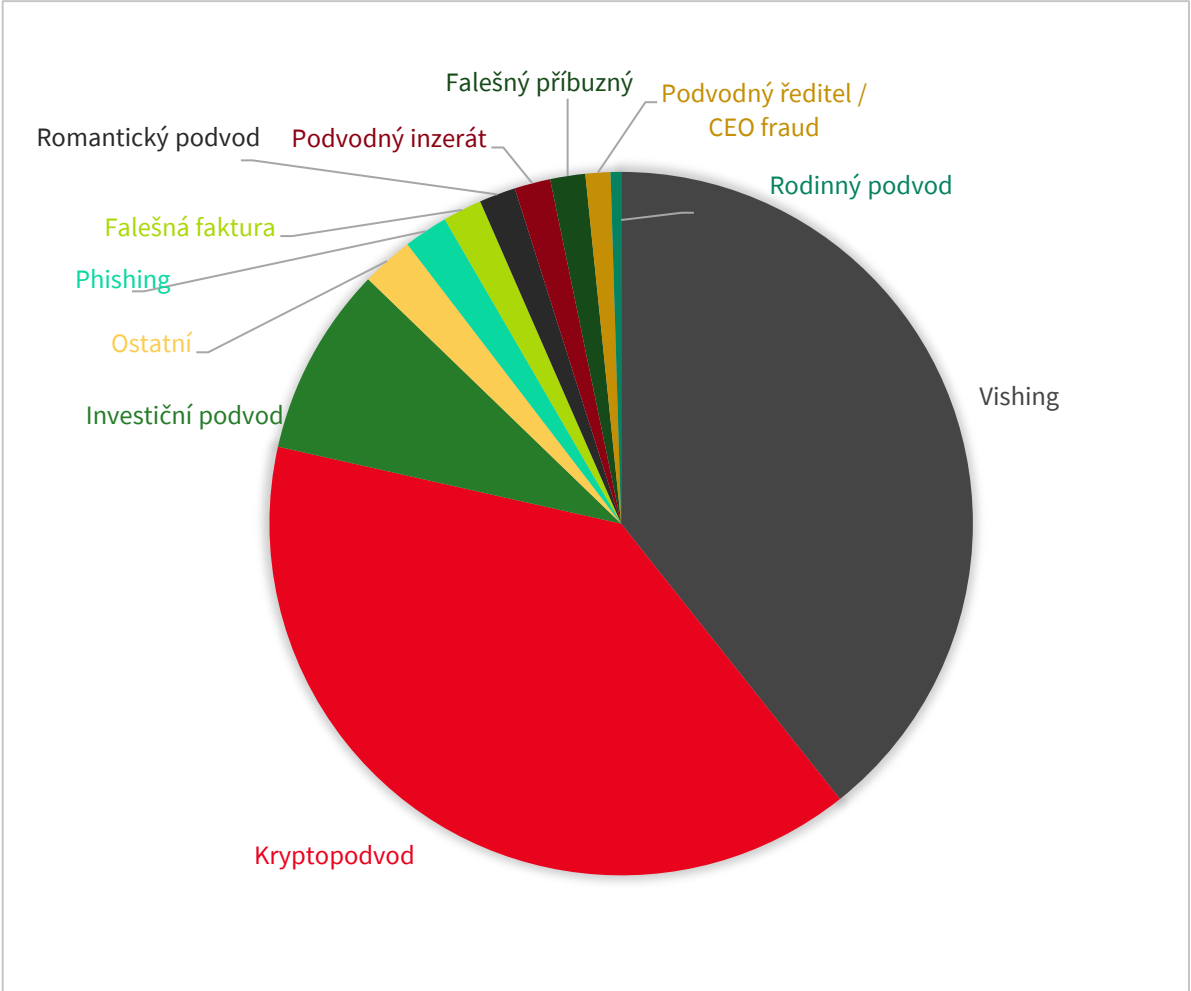
KDYŽ SE SPOJÍ SILNÉ EMOCE, ČASOVÝ TLAK A IZOLACE,
PŘEBÍRÁ ŘÍZENÍ RYCHLÉ MYŠLENÍ. **PRÁVĚ NA TO PODVODNÍCI SPOLÉHAJÍ.**

OBLAST PLATEBNÍCH PODVODŮ

POČET NAPADENÝCH KLIENTŮ



TYPY PODVODŮ



PHISHING

61 %

**případů karetních
podvodů**

v 1. pololetí 2026

JAK POZNAT PHISHING:

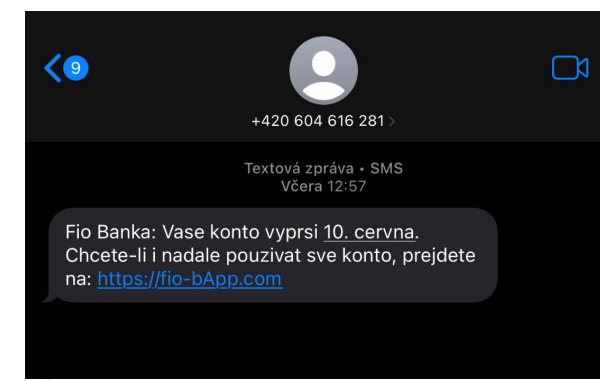
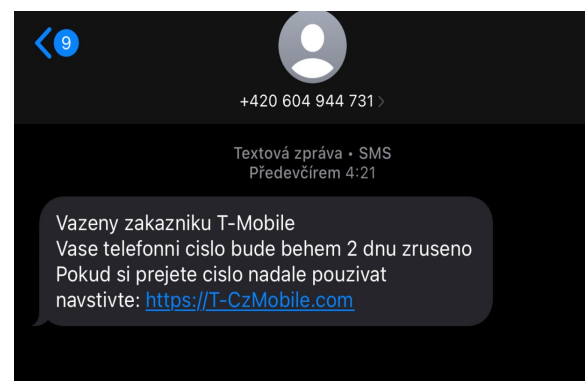
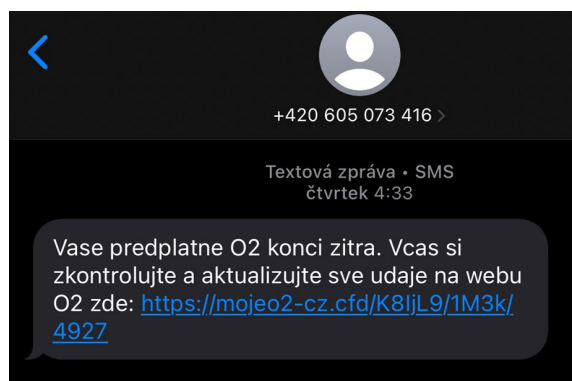
Podvodník napodobí známou firmu či instituci a pod záminkou platby vyláká přihlašovací nebo karetní údaje.

Podvodné zprávy napodobují banky, úřady, přepravní společnosti nebo obchodní platformy a prostřednictvím odkazu získávají:

- přístupy do bankovníctví;
- kompletní údaje o platební kartě;
- autorizační a ověřovací kódy.

NEJČASTĚJŠÍ ZÁMINKY:

neprovedená platba, aktualizace bezpečnostních údajů, pokuta, doplatek za dopravu či clo nebo vrácení peněz.



PROČ JSME DNES ZRANITELNĚJŠÍ?



KOMERČNÍ
BANKA

Žijeme v informačním prostředí plném tlaku a rozptýlení.

INFORMAČNÍ OBEZITA přetěžuje náš mozek – a zvyšuje naši zranitelnost.



INFORMAČNÍ OBEZITA



Denně jsme vystaveni tisícům zpráv, notifikací, reklam, příspěvků.



Informace jsou dostupné 24/7 a v reálném čase.



Počet kanálů, ze kterých na nás informace proudí, neustále roste.



Odhady: denně jsme vystaveni 6 000–10 000 marketingovým sdělením.



Výsledek: náš mozek je přetížený a má méně kapacity na rozmyšlené rozhodování.



NÁŠ MOZEK MÁ LIMIT

Vědomě zpracujeme

120 ± 20

informací za sekundu.

Do vědomí se dostane

5–9

informací za sekundu.



ZBYTEK NÁŠ MOZEK FILTRUJE.

Automaticky, rychle a bez našeho vědomí. Využívá k tomu zkratky (heuristiky).



AŽ 95 % ROZHODNUTÍ DĚLÁME NA AUTOPILOTA.

Rychle, automaticky, bez námahy. Skvělé pro každodenní život. Rizikové v nečekaných situacích.



CO TO S NÁMI DĚLÁ



MENTÁLNÍ PŘETÍŽENÍ

mozek je unavený a hledá nejjednodušší cestu.



SNÍŽENÁ POZORNOST

hůř se soustředíme, snadněji něco přehlédneme.



ZÚŽENÉ VNÍMÁNÍ

nevidíme širší kontext ani varovné signály.



VYŠŠÍ NÁCHYLNOST K CHYBÁM

rozhodujeme rychle, bez ověření.



VYŠŠÍ STRES A ÚZKOST

trvalá pohotovost oslabuje naše duševní zdroje.



NÁŠ MOZEK JE SKVĚLÝ SLUHA, ALE VE SVĚTĚ PŘETÍŽENÍ SE SNADNO STANE ZRANITELNÝM.



KLÍČ JE ZPOMALIT, OVĚŘIT A PORADIT SE.

INVESTIČNÍ PODVODY

48 %

**Ze všech případů
platebních podvodů**

v 1. pololetí 2026

JAK POZNAT INVESTIČNÍ PODVOD:

Falešný poradce slibuje vysoké výnosy, buduje dlouhodobou důvěru a ukazuje smyšlené zhodnocení investice.

Falešný investiční poradce oběť zpravidla kontaktuje telefonicky a přesvědčuje ji k: prvnímu, často nízkému vkladu; instalaci aplikace pro vzdálený přístup; postupnému posílání dalších peněz.

PŘI POKUSU O VÝBĚR PENĚŽ:

podvodník požaduje další „daně“ a „poplatky“. Oběť nezíská výnos ani původní investici.

NOVÁ PLATFORMA UMOŽŇUJE ZÍSKAT OD 14 000 KORUN
ZAREGISTRUJTE SE A ZÍSKEJTE PŘÍSTUP K PLATFORMĚ

Image of a man holding a smartphone displaying a fake bank app with transactions like 'Komerční banka +14.900 CZK' and 'Převod prostředků -1.300 CZK'.

ZJISTĚTE SI VÍCE

VAŠE INVESTICE 6.000 Kč
MĚSÍČNÍ PŘÍRŮBEK 70.000 Kč

SCHVÁLENO VLÁDOU

KAŽDÝ OBYVATEL ČESKA KTERÝ KOUPI BALÍK AKCIÍ CEZ ZA 6.000 Kč

DOSTANE 70.000 Kč MĚSÍČNĚ

[Navštívit stránku](#)

ČEZGroup spouští novou platformu
ČEZGroup nyní umožňuje každému Čechovi stát se akcionářem

Reklama • Vlára net-invest

Immediate Rise

Vydělávejte 20656 AŽ 47836 KORUN ČESKÝCH DENNĚ
s nejinteligentnějším kryptografickým softwarem na světě

Form fields: Vaše jméno, Vaše příjmení, Tvůj e-mail, Vaše telefonní číslo

[Zaregistrujte se nyní](#)

Marek Dospiva
Nadatel "Přítelka (Investment)"

Ján Kraus
slavný historik

"Poslední tento projekt za jeden z nejpopulárnějších a nejrozsáhlejších investičních projektů. Má přesvědčení bylo vyvoláno po prostudování a odborných technologií. Ti týdně po objevení tohoto systému jsem investoval 1,5 mil. Kč a nyní dráhně rostl dva 70.000 Kč" - svědčí v rozhovoru.

Tuto platformu používám již několik let. Všem doporučuji, aby se zaregistrovali ještě dnes, aby zbyla možnost. Myslím, že z toho budou mít prospěch všichni v České republice.

BÍLÍ KONĚ = MONEY MULES

MONEY MULE =

člověk, přes jehož účet podvodníci převádějí nebo vybírají peníze vědomě i nevědomě

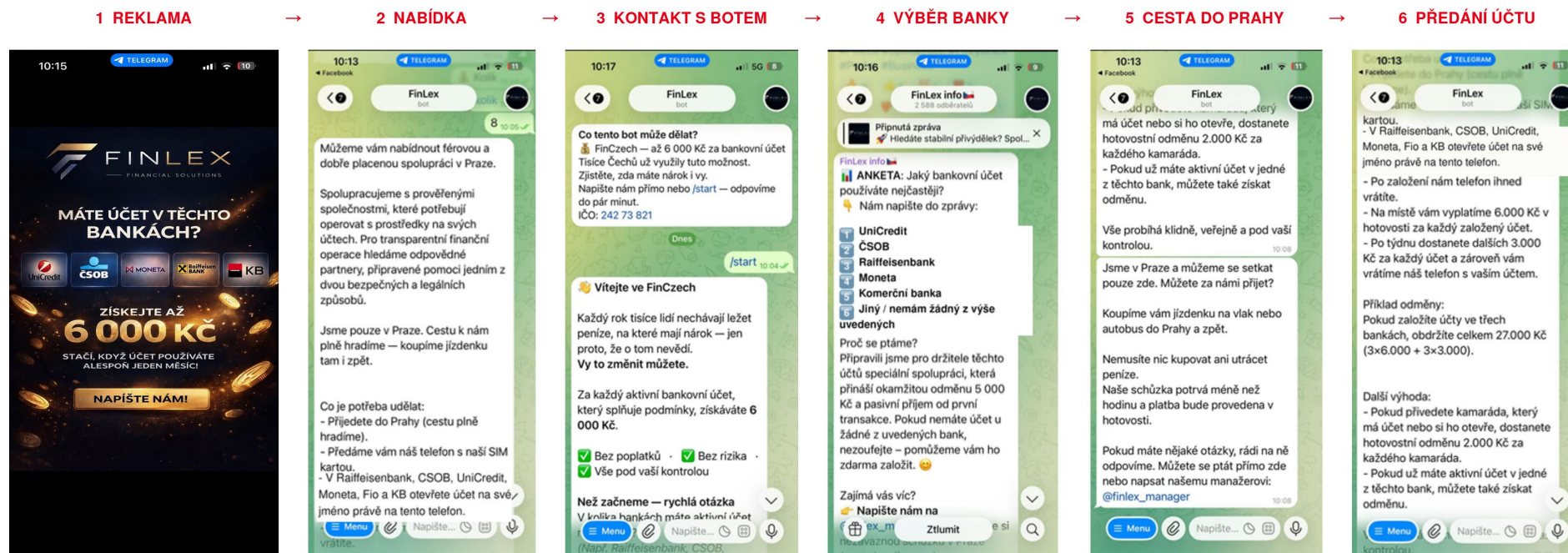
JAK HO PODVODNÍCI ZÍSKAJÍ:

Nejčastěji prostřednictvím nabídky snadného přivýdělku nebo brigády na sociálních sítích.

DŮSLEDKY PRO MAJITELE ÚČTU:

hrozí mu trestní stíhání za praní peněz, povinnost nahradit způsobenou škodu a případně i odnětí svobody.

JAK PROBÍHÁ NÁBOR BÍLÉHO KONĚ



HOTOVOST

PŘEDÁNÍ HOTOVOSTI „KURÝROVI“

Podvodník vydává výběr za záchranu peněz. Oběť přesvědčí, aby hotovost sama vybrala a předala cizímu člověku.

VAROVNÝ SIGNÁL:

požadavek vybrat hotovost a předat ji „kurýrovi“.

JAK PODVOD PROBÍHÁ?

1. FALEŠNÝ HOVOR
Volající se vydává za banku, ČNB nebo policii.
2. STRACH A NÁTŁAK
Tvrdí, že účet je napadený a peníze je nutné okamžitě „zachránit“.
3. VÝBĚR HOTOVOSTI
Oběť dostane instrukce i připravené vysvětlení pro pracovníky banky.
4. PŘEDÁNÍ „KURÝROVI“
Peníze odevzdá cizímu člověku na parkovišti, ulici či jiném veřejném místě.
5. PENÍZE MIZÍ
Hotovost končí u podvodníků a šance na její získání zpět je minimální.



KDYŽ JSME PŘETÍŽENÍ, FUNGUJÍ ZKRATKY MYSLI

Náš mozek chce šetřit energii a rozhoduje rychle.
Podvodníci toho využívají.

1

AUTORITA

Důvěřujeme autoritám
a odborníkům.

Jak to funguje:

Máme vrozenou tendenci
poslouchat autoritu.

PŘÍKLAD:

„Volá banka / policie,
musí to být pravda.“

2

KONZISTENTNOST

Máme tendenci být
konzistentní se svými
předchozími kroky.

Jak to funguje:

Malý krok vytvoří závazek
pokračovat.

PŘÍKLAD:

„Už jsem ověřil / potvrdil,
tak musím pokračovat.“

3

SOCIÁLNÍ SCHVÁLENÍ

Řídíme se tím, co dělá
většina nebo co je
společensky přijímané.

Jak to funguje:

Předpokládáme, že ostatní
vědí, co je správné.

PŘÍKLAD:

„Když to dělají ostatní,
bude to správné.“

4

AVERZE KE ZTRÁTĚ

Bojíme se ztratit víc než
se těšíme na zisk.

Jak to funguje:

Strach ze ztráty nás tlačí
k rychlému rozhodnutí.

PŘÍKLAD:

„Ztratím peníze / účet,
když neudělám hned.“

5

KONFIRMAČNÍ ZKRESLENÍ

Neradi se mýlíme a rádi si
potvrzujeme svá přesvědčení.

Jak to funguje:

Všímáme si hlavně informací,
které potvrzují to, čemu už
věříme.

PŘÍKLAD:

„Našel jsem recenzi /
článek, který to potvrzuje,
tak je to pravda.“

6

NEDOSTATEK ČASU (NALÉHAVOST)

Pod tlakem času přecházíme
do rychlého, automatického
rozhodování.

Jak to funguje:

Není čas na rozmyšlenou,
jednáme impulzivně.

PŘÍKLAD:

„Máte 10 minut, jinak
bude váš účet zablokován.“



ZKRATKY NÁM POMÁHAJÍ KAŽDÝ DEN.

ALE VE STRESU A POD TLAKEM NÁS MOHOU DOVÉST K CHYBĚ.



**ZASTAVTE SE. OVĚŘTE. PORAĎTE SE.
KLÍČ JE ZPOMALIT.**

REZERVACE UBYTOVÁNÍ

“PLATBA NEPROŠLA“

nejčastější záminka

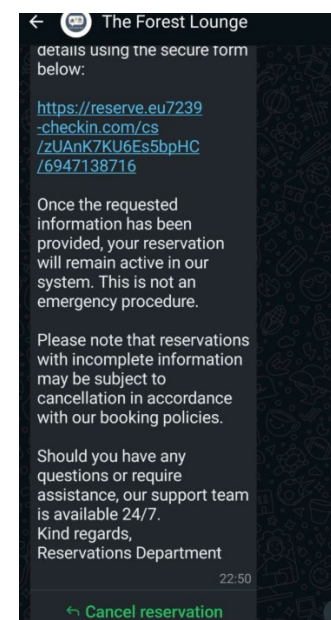
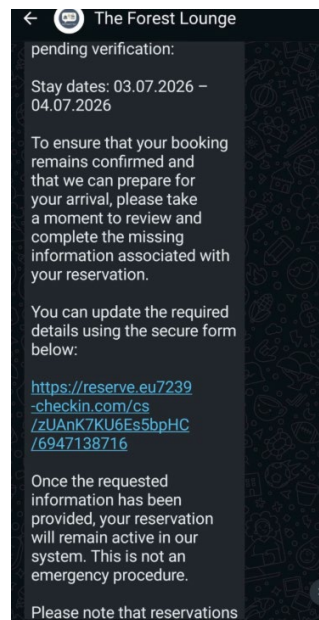
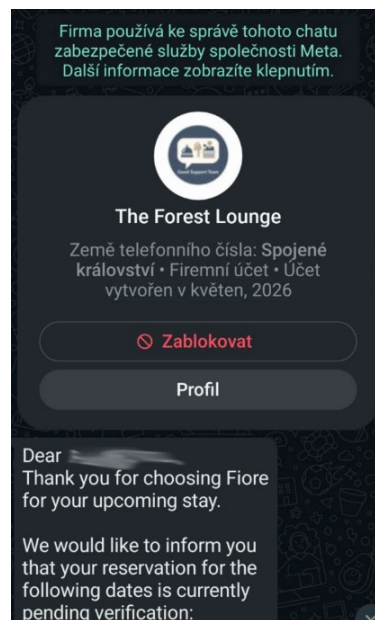
JAK PODVOD POZNAT:

Zpráva zná detaily skutečné rezervace, tlačí na rychlou reakci a odvádí hosta mimo oficiální aplikaci nebo web.

Podvodníci se vydávají za ubytování nebo zákaznickou podporu rezervační platformy. Hosty kontaktují e-mailem, přes SMS, WhatsApp nebo přímo v interním chatu platformy.

VAROVNÉ SIGNÁLY:

odkaz mimo oficiální doménu platformy;
tlak na okamžitou platbu;
požadavek zadat údaje ke kartě znovu.



PODVODNÁ APLIKACE – NFC RELAY ATTACK

„PŘILOŽTE KARTU K TELEFONU“

zdánlivé „ověření“ karty

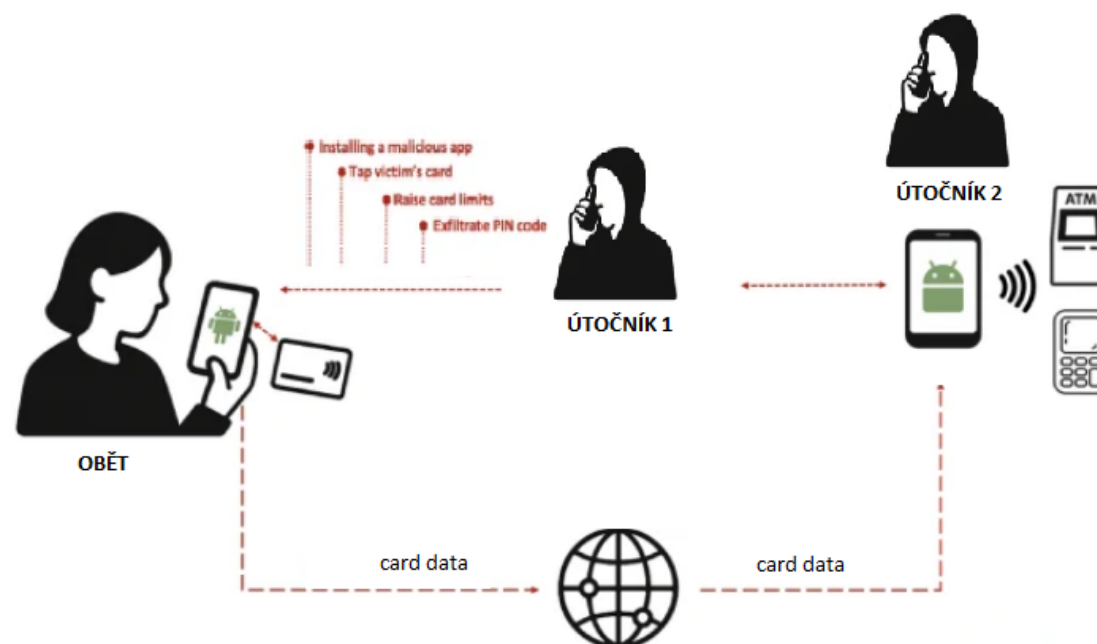
JAK PODVOD POZNAT:

Volající požaduje instalaci aplikace z odkazu, přiložení fyzické karty k telefonu a zadání PINu.

Falešná bezpečnostní aplikace funguje jako „červí díra“: údaje z přiložené karty okamžitě přenese do zařízení útočníka.

JAK PODVOD PROBÍHÁ:

FALEŠNÝ HOVOR → INSTALACE APLIKACE → PŘILOŽENÍ KARTY A ZADÁNÍ PINU → PŘENOS KARETNÍCH ÚDAJŮ → VÝBĚR NEBO PLATBA



JAK SE PODVODU BRÁNIT

KÓD V SMS NENÍ OVĚŘENÍ BANKÉŘE

ani když jej pošle údajná
banka nebo policie

SKUTEČNÉ OVĚŘENÍ:

Probíhá výhradně v
aplikaci KB+ nebo KB Klíč,
kde klient vidí jméno
bankéře a čtyřmístný
kontrolní kód.

OVĚŘTE VOLAJÍCÍHO

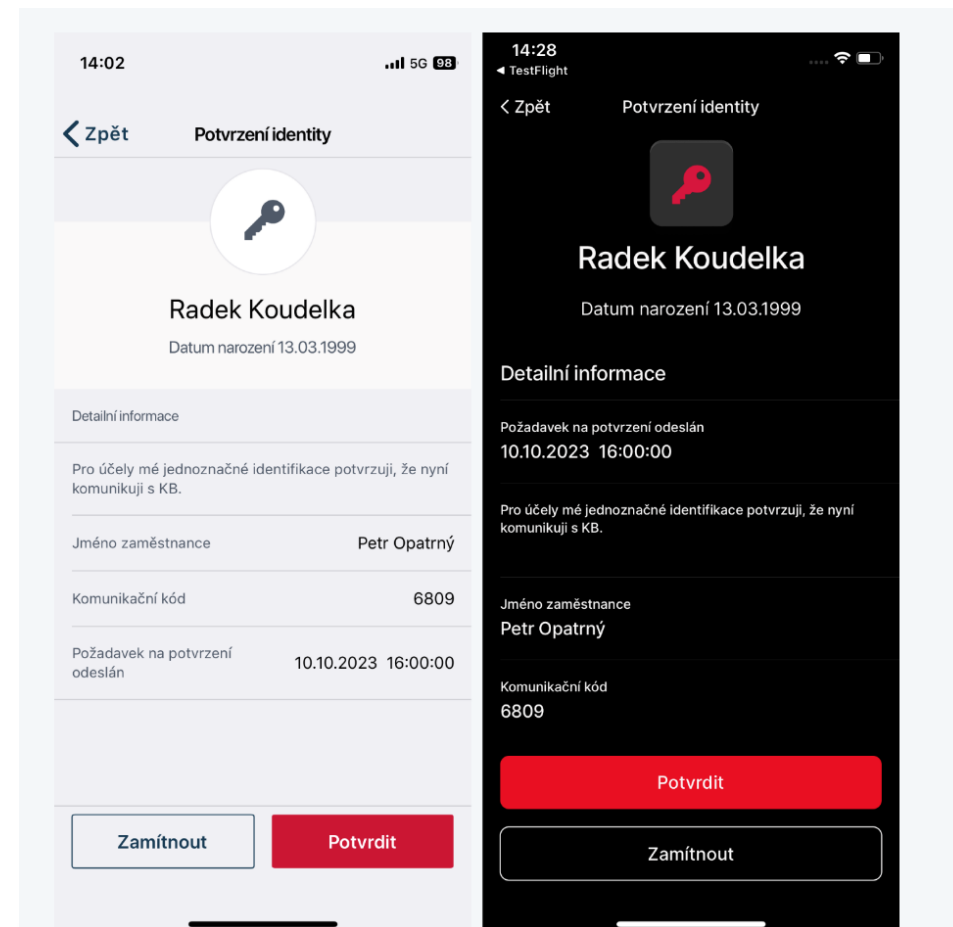
Přímo v aplikaci KB+ nebo KB Klíč.

NEINSTALUJTE APLIKACI Z ODKAZU

Aplikace stahujte pouze z oficiálních
obchodů.

NEPŘIKLÁDEJTE KARTU K TELEFONU

Na pokyn volajícího nikdy nezadávejte
PIN.



WHATSAPPOVÉ PODVODY

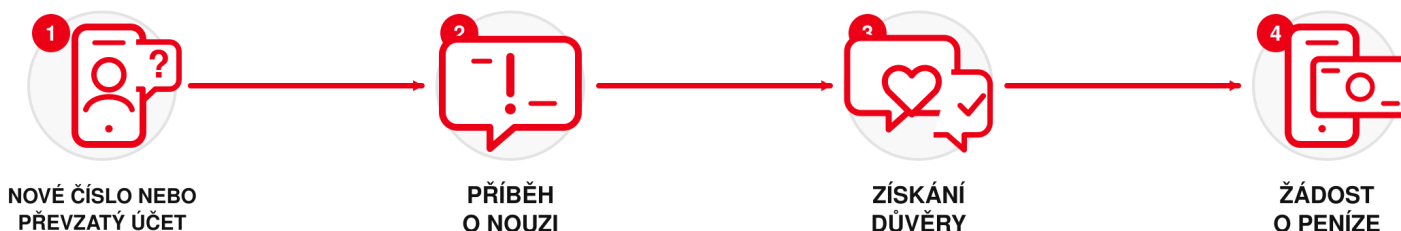
NOVÉ ČÍSLO NEBO PŘEVZATÝ ÚČET

Podvodník se vydává za dítě, příbuzného nebo jiného známého.

JAK PODVOD PROBÍHÁ:

Po získání důvěry přichází naléhavá žádost o peníze.

Zpráva může přijít **z nového čísla i ze skutečného profilu**, který útočník převzal.



WHATSAPPOVÉ PODVODY

JEDEN HOVOR

může celý podvod zastavit

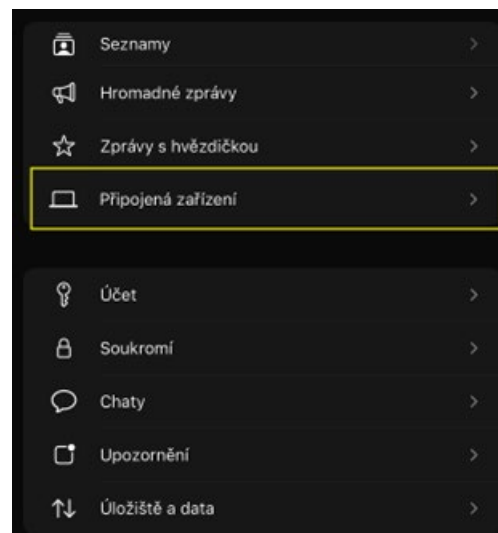
JAK SE BRÁNIT:

Žádost ověřte mimo původní konverzaci.

OVĚŘTE, KDO VÁM SKUTEČNĚ PÍŠE

- zavolejte blízkému na původní známé číslo;
- neposílejte peníze pouze na základě zprávy;
- v aplikaci WhatsApp kontrolujte **Nastavení** → **Propojená zařízení**;
- všechna neznámá zařízení ihned odhlaste.

Neodpovídejte pouze ve stejné konverzaci. Identitu ověřte jinou cestou.



4 P, KTERÁ VÁS OCHRÁNÍ

Když jsme přetíženi, mozek reaguje rychle. Dejte si pauzu a **přepněte správně.**

1 PAUZA ZASTAVTE SE.



NÁDECH – VÝDECH
Zklidněte tělo i mysl.
Nereagujte okamžitě.
Zpomalte.
Dejte si pár vteřin.

- Zpomalte. Nespěchá to.
- Nereagujte okamžitě.
- Dejte si alespoň pár vteřin.
- Emoce a tlak podvodníků jsou nástroje manipulace.

2 PROMYSLI PŘEPNĚTE Z EMOCIONÁLNÍHO RYCHLÉHO MYŠLENÍ DO RACIONÁLNÍHO POMALÉHO MYŠLENÍ.



KLÍČOVÉ OTÁZKY:

Co se po mně chce
a proč zrovna teď?
Dává to smysl?
Jaké mohou být důsledky?
Jednal/a bych stejně, kdybych měl/a
o hodinu (nebo dvě) více času?



PŘEPÍNEJTE VĚDOMĚ.

Spěch je zbraň podvodníků.
Klid je vaše výhoda.

3 PROVĚŘ OVĚŘTE INFORMACE.



OVĚŘUJTE JINÝM KANÁLEM.

Nikdy ne přes odkaz, telefon
ani kontakty, které vám poslali.

- Zkontrolujte informace z více zdrojů.
- Kontaktujte instituci oficiálním způsobem (web, aplikace, ověřené číslo).
- Neověřujte přes odkazy v SMS, e-mailech nebo zprávách.

4 POKRAČUJ TEPRVE TEĎ JEDNEJTE.



POKUD SI NEJSTE JISTÍ, POŽÁDEJTE O POMOC.

Není to slabost,
ale projev síly a rozvahy.

- Teprve nyní se rozhodněte.
- Pokud si nejste jisti, poraďte se s někým, komu důvěřujete.
- Raději ověřte dvakrát než litujte.



PAUZA. PROMYSLI. PROVĚŘ. POKRAČUJ.

ČTYŘI KROKY, KTERÉ VÁM MOHOU UŠETŘIT VELKÉ ZTRÁTY.



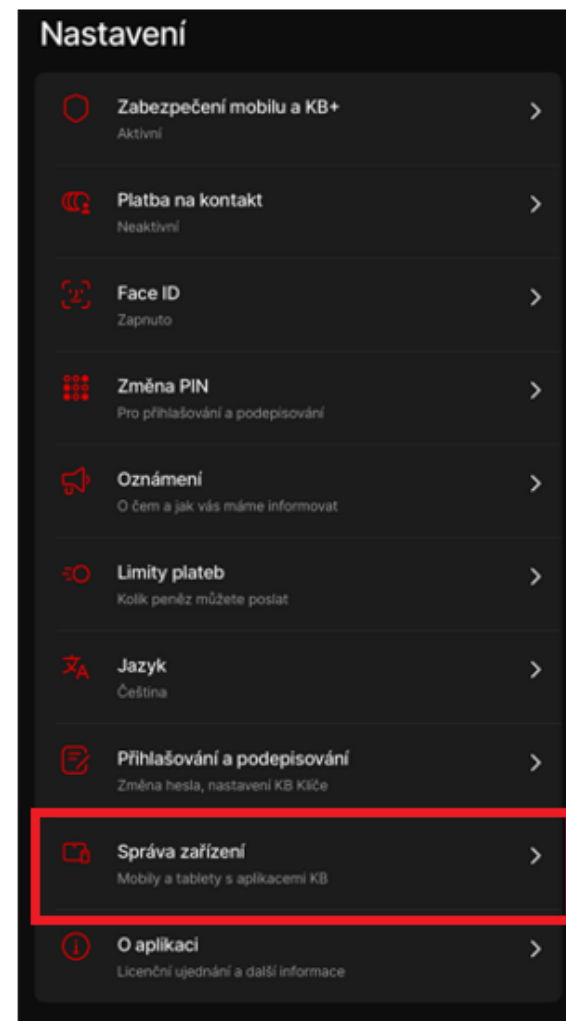
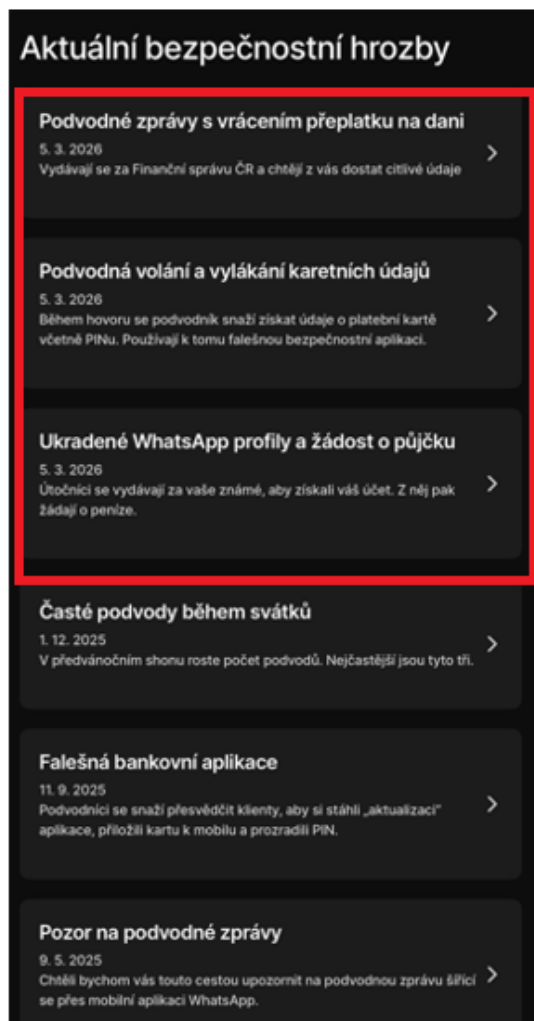
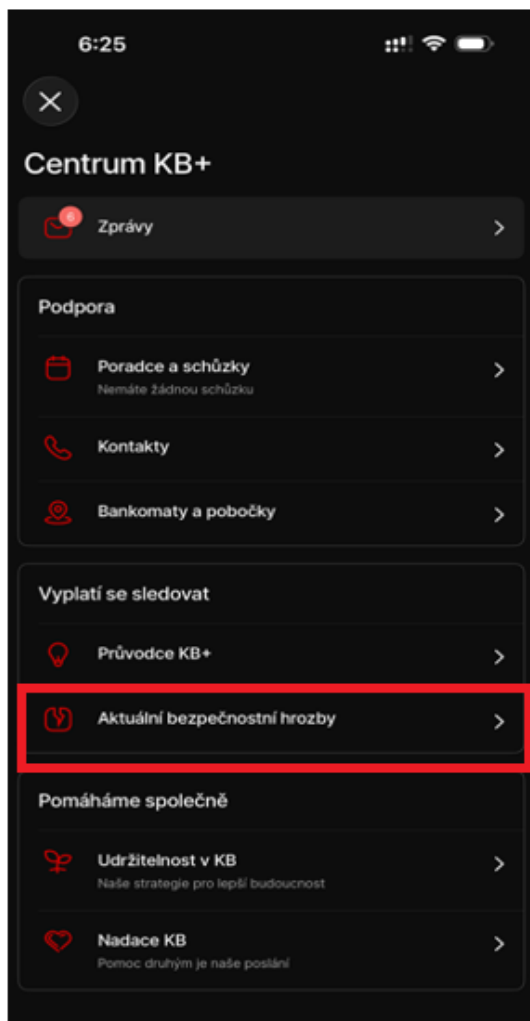
**KLIDNÉ ROZHODNUTÍ
JE VAŠE NEJLEPŠÍ OCHRANA.**

Tipy a rady

1. **Zastavte se a zamyslete se.** Proč by někdo dal hodně peněz za málo práce? Chovala by se daná instituce tímto způsobem? Jak byste se zachovali ve fyzickém světě – dali byste klíče od svého bytu nebo své úspory člověku, kterého neznáte?
2. Vždy **ověřujte s kým voláte** pomocí bankovní aplikace
3. Pamatujte bankéř / doručovací služby / prodávající / kupující **nepotřebuje znát vaše citlivé údaje** (všechna čísla z karty nebo přístupy a hesla do bankovníctví). Pokud někdo platí vám, stačí mu číslo účtu.
4. Ujistěte se, **že potvrzujete přihlášení nebo platíte správnému příjemci správnou částku** ve správné měně. A jestli to tak opravdu chcete vy, ne příjemce. Pamatujte, že příchozí platby se nikdy nepotvrzují.
5. **Investujte jen přes oficiální investiční portály**, osobní bankéře nebo internetové bankovníctví.
6. Vždy vstupujte do internetového bankovníctví, do klientských zón firem nebo na stránky úřadů pouze z oficiálních stránek dané instituce, ne prostřednictvím náhodného odkazu z vyhledávačů.
7. **Budte obezřetní. Neklikejte a nezažívejte své citlivé údaje** (všechna čísla z karty nebo přístupy a hesla) do odkazů, které vám přišly prostřednictvím SMS, chatu nebo e-mailu.
8. Nikdy **neinstalujte program pro vzdálený přístup** (např. AnyDesk, TeamViewer, SupRemo) do PC / mobilu / tabletu. Protistrana si pak ve vašem zařízení může dělat, co chce, bez vašeho vědomí.
9. **Navštivte oficiální stránky** dané společnosti a informace si ověřte tam. Neověřujte informace na telefonním čísle / e-mailu, které vám cizí osoba předala v SMS nebo nadiktovala po telefonu..
10. **Vyhledejte si recenze** společnosti i dané telefonní číslo na internetu na více místech, nespolehejte jen na stránky konkrétní firmy. Čím více hodnocení, tím lépe
11. Vždy si protistranu a informace, které vám tvrdí, **ověřte více způsoby**. Pokud máte jakékoliv pochybnosti, obraťte se na banku.
12. **Instalujte si aplikace pouze z oficiálních obchodů** (pro iOS <https://www.apple.com/cz/app-store/>, pro Android <https://play.google.com/store/apps>).
13. **Poradte se se svými blízkými.**



Tipy a rady – KB podpora



Tipy a rady na léto - cestování s kartou

1. Pokud vybíráte z bankomatu (zejména v exotických destinacích) **pozor na případnou „pomoc“ v podobě náhodného kolemjdoucího**, který ochotně bude pomáhat při výběru.
2. **Používejte kartu výhradně bezkontaktně** a nezapomínejte vždy schovávat při zadávání svůj PIN.
3. DCC – Dynamic currency conversion – pokud bankomat nebo platební terminál nabízí konverzi měn, tak doporučujeme nepotvrzovat a **vždy volte platbu v místní měně**.
4. Poplatky za výběr na bankomatech „surcharge“ – **pozor na bankomaty, které k výběru přidávají svůj vlastní poplatek**.
5. Dopředu si **ověřte přijímání debetních a kreditních karet**. Zejména u autopůjčoven a hotelů se můžete setkat s preferencí právě kreditních karet.
6. **Doporučujeme mít dvě karty** (jednu vždy záložní na hotelu v trezoru včetně hotovosti), případně využívat kartu v chytrých zařízeních.
7. **Doporučujeme mít i částečnou hotovost** pro případ, že budete potřebovat zaplatit drobnosti (parkování, občerstvení, toalety apod.)
8. Peníze **nikdy nesměňujte s neznámými lidmi na ulici**.
9. **Zapište číslo, na které můžete zavolat v případě odcizení karty** nebo jakékoli jiné nouzové situace
10. Před odjezdem si **zkontrolujte dobu vypršení platnosti karty** a nastavené limity.
11. **Nahrajte si kartu do svého mobilního zařízení** a využívejte mobilní platby / výběr
12. **Nahlaste nám vaši cestu.**



**BUDOUCNOST
JSTE VY  KB**