ČBA & ČIIA – setkání auditorů finanční oblasti

Praktické bankovní zkušenosti s aktuálními kybernetickými útoky na klienty bank

Praha / 1. června / 2023

JUDr. Petr Barák,
Vedoucí operačních rizik, Air Bank a.s. / člen skupiny PPF,
Předseda KBFB ČBA

I banku můžete mít rádi

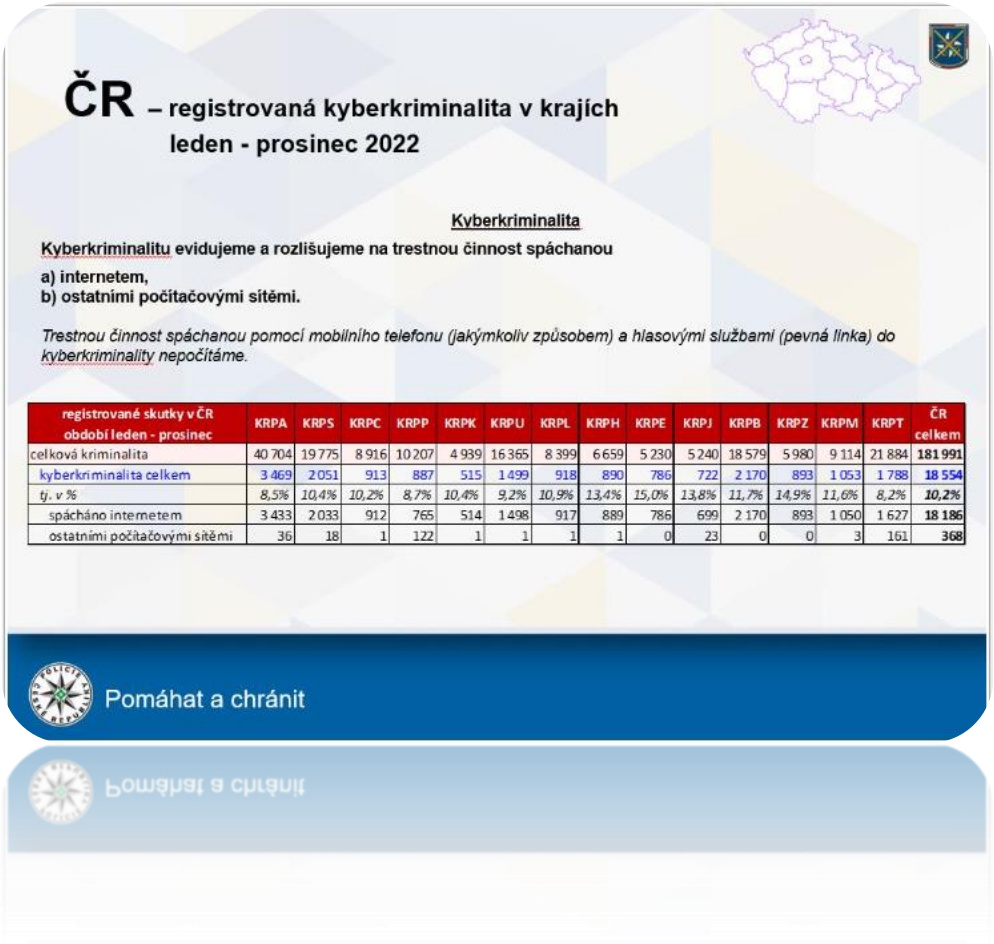
k / interní

Typy kybernetických útoků

- Hacking (kreditní karty)
- Znepřístupnění služby (DoS, DDoS)
- **Krádež identity** (úvěrové podvody)
- Šíření viru
- Počítačový vandalismus
- Kybernetický terorismus
- **Online podvody** (reverzní bazarové podvody)
- Softwarové pirátství
- Padělání / injektáž / webových stránek
- Škodlivý kód
- Malware
- **Phishing**
- **Vishing**
- Spam
- **Spoofing**
- Hanobení na sociálních sítích
- …

Co nám říkají fakta

V oblasti podvodů páchaných v online prostředí se stále setkáváme s provázanou **sériovou trestnou činností**, která je ve většině případů navázána na legalizaci **skrze nastrčené „legalizátory“ pocházející z post sovětských republik.** K náborů dochází zpravidla skrze sociální sítě s **nabídkou výhodného přivýdělku** v oblasti kryptoměn. Častými případy jsou stále **podvodné nabídky investování, podvodné obvolávání** pod různými legendami a napadení bankovního účtu. Podvodné, tzv. **„topované reklamy“,** spočívající v zaplacení reklamy ve vyhledávačích, která směřuje na, **spoofovanou, webovou stránku** tvářící se jako regulérní stránka banky. Dále stále zaznamenáváme případy tzv. **reverzních inzertních podvodů** a od srpna roku 2022 se setkáváme s **podvodnými SMS** zprávami, které se tváří jako odeslané od **Ministerstva práce a sociálních věcí**, kdy je cílem pachatele vylákat z oběti přístupové údaje do bankovnictví a ty následně zneužít. Již tradičně byl v prosinci zaznamenán nárůst tzv. „**vánočního phishingu“**, tedy podvodných e-mailů a SMS zpráv s legendou o **doplacení zásilky**, opět s cílem zejména vylákat citlivé bankovní údaje a tyto zneužít.



ČR – registrovaná kyberkriminalita v krajích
leden - prosinec 2022

Kyberkriminalita

Kyberkriminalitu evidujeme a rozlišujeme na trestnou činnost spáchanou

a) internetem,
b) ostatními počítačovými sítěmi.

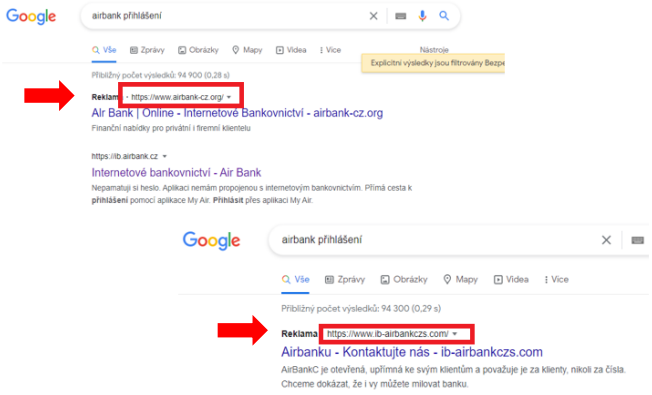
Trestnou činnost spáchanou pomocí mobilního telefonu (jakýmkoliv způsobem) a hlasovými službami (pevná linka) do kyberkriminality nepočítáme.

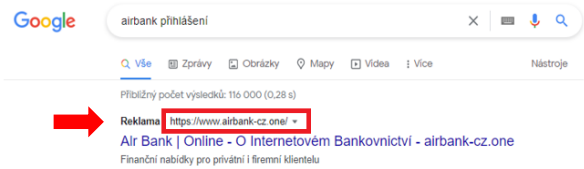
registrované skutky v ČR období leden - prosinec	KRPA	KRPS	KRPC	KRPP	KRPK	KRPU	KRPL	KRPH	KRPE	KRPJ	KRPB	KRPZ	KRPM	KRPT	ČR celkem
celková kriminalita	40 704	19 775	8 916	10 207	4 939	16 365	8 399	6 659	5 230	5 240	18 579	5 980	9 114	21 884	**181 991**
kyberkriminalita celkem	3 469	2 051	913	887	515	1 499	918	890	786	722	2 170	893	1 053	1 788	**18 554**
tj. v %	*8,5%*	*10,4%*	*10,2%*	*8,7%*	*10,4%*	*9,2%*	*10,9%*	*13,4%*	*15,0%*	*13,8%*	*11,7%*	*14,9%*	*11,6%*	*8,2%*	***10,2%***
spácháno internetem	3 433	2 033	912	765	514	1 498	917	889	786	699	2 170	893	1 050	1 627	**18 186**
ostatními počítačovými sítěmi	36	18	1	122	1	1	1	1	0	23	0	0	3	161	**368**

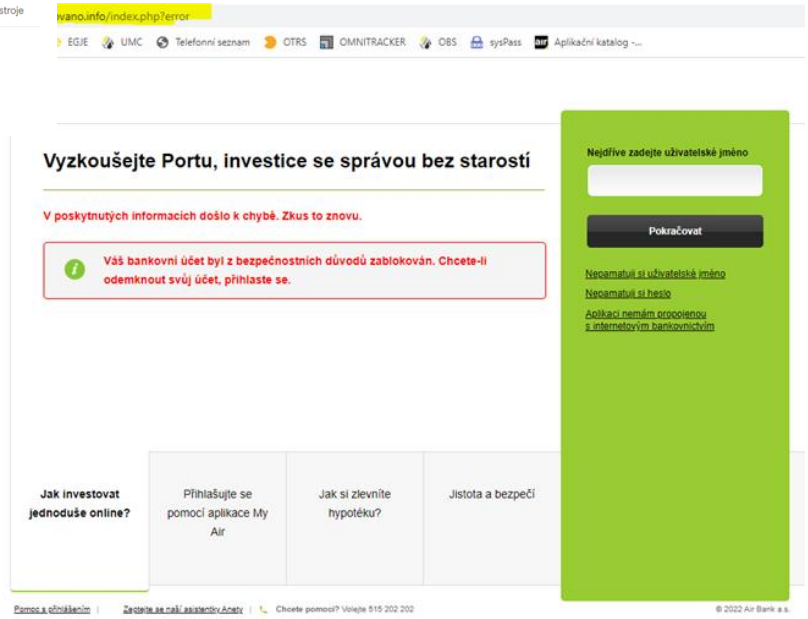
Pomáhat a chránit

Banky evidují v roce 2022 počty kybernetických útoků na své klienty v řádech několikanásobně vyšších.

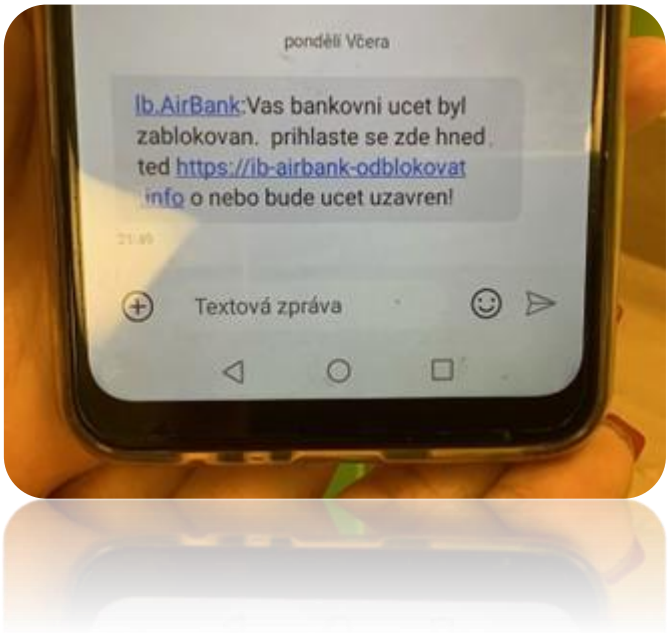
Phishing – typické projevy

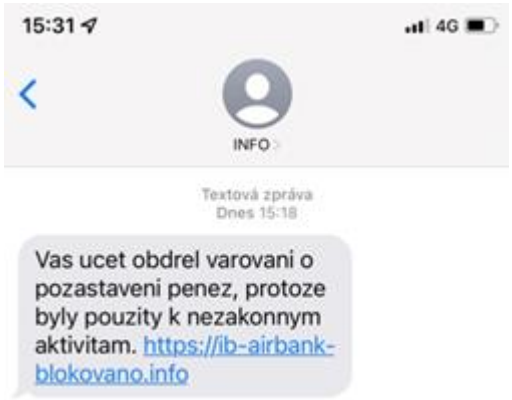


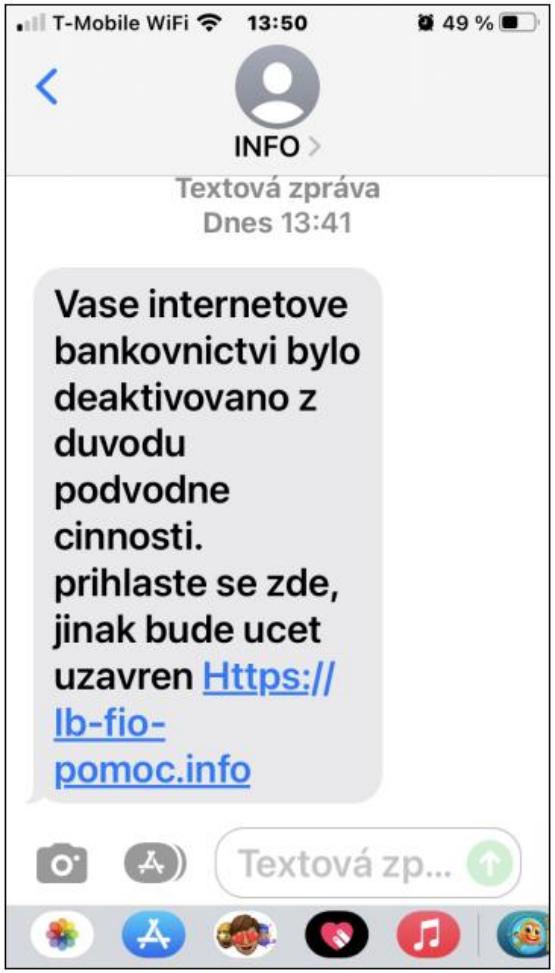




Smishing – typické projevy







Vishing – typické projevy ve veřejném prostoru

lešná soutěž imitující facebookové stránky Zoo Praha

Slíbil balík s pokladem. Naletěla jste, stopla banka ženu žádající o další úvěr

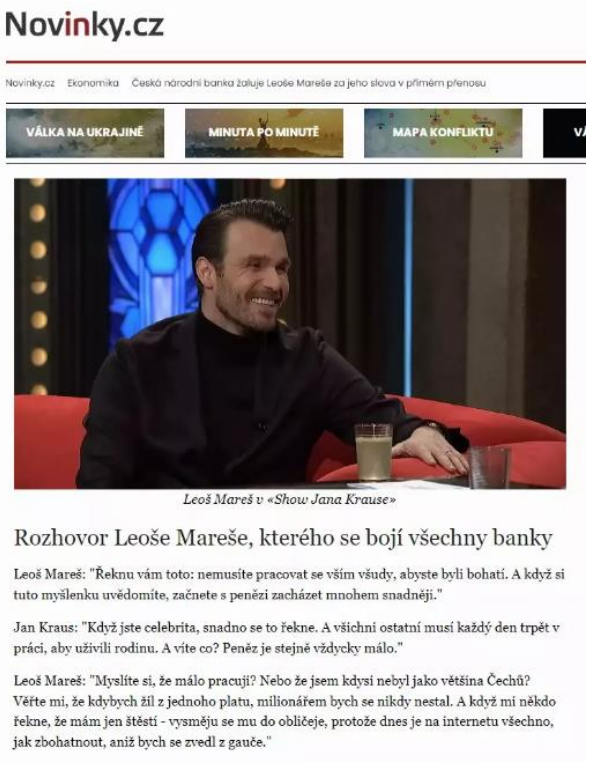
13. 4. 2023, 14:24
Jakub Bartosz

Další z nekončící série podvodů, za kterými jsou báchorky anonymních známostí z internetu, kterým lidé uvěří a pošlou jim nemalé peníze, vyšetřují policisté na Hodonínsku. Žena naletěla údajnému německému lékaři, toho času na Ukrajině. Slíbil šperky a milion dolarů v zásilce, kterou ale prý zadrželi celníci v Litvě. Vyplacení neexistujícího balíku stálo ženu 900 tisíc korun.

Žena ze Zlínska myslela, že soutěží s kamarádkou o večeři. Na účtu jí zbylo sotva na jednu

23. 5. 2023, 11:10 – Zlín
Jakub Bartosz

Měla to být soutěž o večeři, na kterou měla jít s kamarádkou, ve finále ženě zmizelo z účtu čtvrt milionu a zůstatek činil 143 korun. Další podvod, kdy lidé pošlou zcela neuváženě někomu cizímu osobní údaje k platební kartě, vyšetřují kriminalisté na Zlínsku.



Leoš Mareš v «Show Jana Krause»

Rozhovor Leoše Mareše, kterého se bojí všechny banky

Leoš Mareš: "Řeknu vám toto: nemusíte pracovat se vším všudy, abyste byli bohatí. A když si tuto myšlenku uvědomíte, začnete s penězi zacházet mnohem snadněji."

Jan Kraus: "Když jste celebrita, snadno se to řekne. A všichni ostatní musí každý den trpět v práci, aby uživili rodinu. A víte co? Peněz je stejně vždycky málo."

Leoš Mareš: "Myslíte si, že málo pracuji? Nebo že jsem kdysi nebyl jako většina Čechů? Věřte mi, že kdybych žil z jednoho platu, milionářem bych se nikdy nestal. A když mi někdo řekne, že mám jen štěstí - vysměju se mu do obličeje, protože dnes je na internetu všechno, jak zbohatnout, aniž bych se zvedl z gauče."

Investiční podvody

9:50 čt 25. 5. oenotheraceae.com 75 %

CEZ spolecne s vladou zahajuje mezinarodni investicni project. Investujte do Ceské energetika a vydelavejte od 50.000 Kč mesicne.

Illustrative photo. | Photo: Shutte

ČTK
Aktualizováno 25 Květen 2023, 07:47

Mezinárodní platforma ČEZ je určena speciálně pro občany, kteří se chtějí podílet na investicích na mezinárodním trhu, je navržena tak, aby pomohla obyčejným lidem vyrovnat se s velkými investory, kteří díky svému obrovskému kapitálu vydělávají miliony. Jedinecnost platformy CEZ spociva v tom, zeiss 5 500 Kč můžete začít investovat a vydělávat své první peníze.

I minimální investice může poskytnout pasivní příjem 60 000 Kč měsíčně, protože systém analyzuje samotný trh. Platforma je přístupná pouze jednotlivcům, aby se zabránilo monopolu. Díky tomu může každý investovat do energetických zdrojů země a získat z ní vysoké dividendy.Platforma v současné době funguje ve 20 zemích, včetně České republiky

OFICIÁLNÍ STRÁNKY

Jak tento projekt funguje?

Hlavním rysem projektu ČEZ je 100% ziskovost. Investiční projekt je navržen tak, že při prodeji elektřiny platforma automaticky vypočítá zisk každého investora a odešle jej na svůj vlastní účet. Uživatel nemusí mít určité dovednosti pro práci se zdrojem, protože platforma je plně automatizovaná. Ponecháním kontaktů na oficiálních stránkách získáte osobního manažera, který vysvětlí, jak vše funguje.

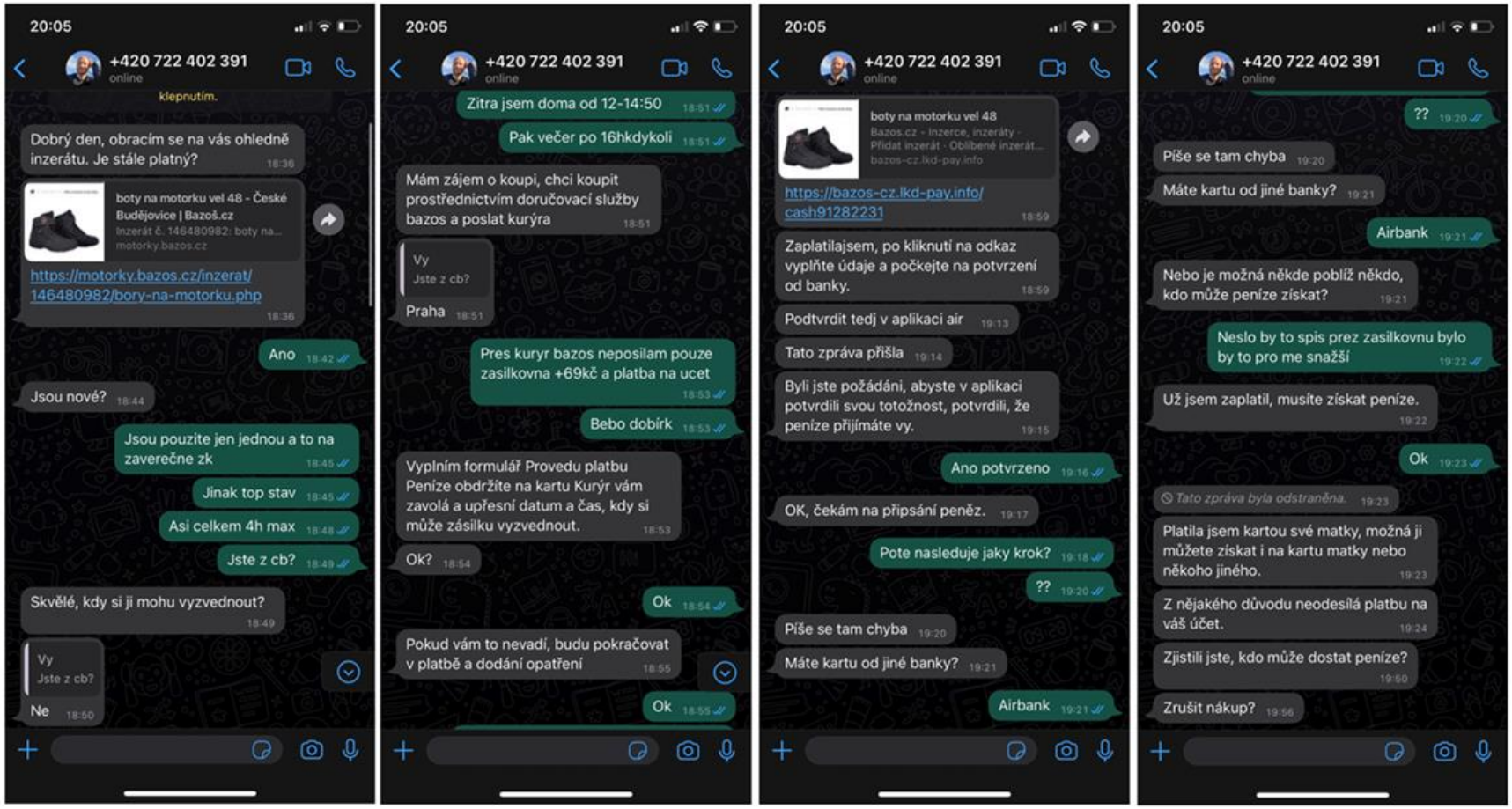
ZAREGISTROVAT

ČEZ vám dal možnost začít s minimálními investicemi, které vám umožní vidět efektivitu p
p
měite na paměti, že výše očekávaného příjmu závisí přímo na vašem počátečním vkladu.

OFICIÁLNÍ STRÁNKY

ČEZ
6 To se mi líbí stránky

Podvodný bazarový prodej (Vinted, Aukro, S-Bazar…)



Spoofing – falešný bankéř

Spoofing – falešný bankéř

Aktuální scénáře legalizace výnosů z kybernetické kriminality přes klienty bank

1. Ukrajinská mula

Trestná činnost: vědomá Legalizace výnosů z trestné činnosti

Zdrojová trestná činnost: Phishing/Vishing (podvodné investice, bazarový phishing, prozrazení přihlašovacích údajů do sběrače)

Výskyt: výrazně od 2021, akcelerace od 4/2022

2. Balkánská mula

Trestná činnost: vědomá Legalizace výnosů z trestné činnosti

Zdrojová trestná činnost: Phishing (falešné stránky banky, bazarový phishing, smishing typu ČSSZ – soc. dávky typu příspěvek na bydlení, příspěvek na dítě,….)

Výskyt: výrazněji od 2022

3. Investor

Trestná činnost: nevědomá Legalizace výnosů z trestné činnosti

Zdrojová trestná činnost: investiční vishing

Výskyt: výrazněji od 2021

4. Podvodný prodej zboží/služeb

Trestná činnost: Podvod + nevědomá legalizace výnosů z trestné činnosti

Zdrojová trestná činnost: Podvod

Výskyt: dlouhodobý

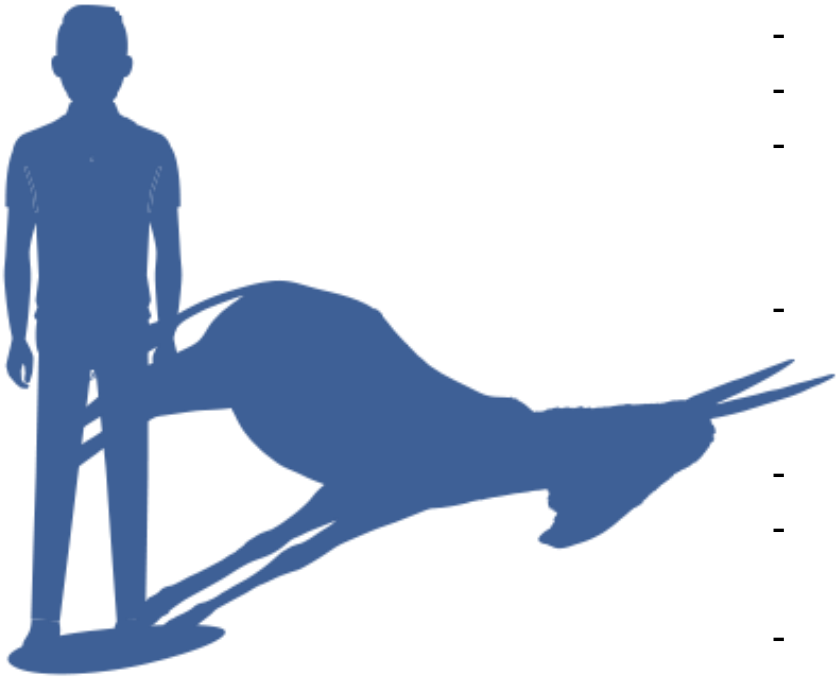
5. Fraud romance

Trestná činnost: Podvod, nevědomá Legalizace výnosů z trestné činnosti

Zdrojová trestná činnost: Podvod

Výskyt: dlouhodobý

Money Mula - Nejčastější způsob legalizace



Charakteristické znaky:

- 89 % těchto klientů se rekrutuje z Ukrajiny, Uzbekistánu…
- 76% do 35 let,
- 69% s korespondenční adresou v Praze,
- 49% as více než 100% nárůstem přihlášení do MA/IB za posledních pět dní před příchodem peněz
- 65% klientů kde je počet dní od zaktivnění nové RS do zapojení k legalizaci menší než 30 dní (median = 39),
- Často příjemce sociální / uprchlické dávky
- Vzestupná sekvence plateb od stejné osoby v jiné bance (bez předchozí transakční historie)
- Navyšování limitů krátce před nebo po příchozích platbách
- Maximální využití OKAP
- Příchozí i odchozí transakce / hotovostní výběry / jsou prováděny téměř ve stejném čase
- Předchozí minimální transakční historie
- …

Money Mula – typický transakční scénář

Zaúčtování Provedení	Typ Kód transakce	Název Číslo účtu / debetní karty	Detaily	Částka CZK
27.04.2023 27.04.2023	Příchozí úhrada	Klient XY příchozí platba z účtu v jiné bance		5 000,00
27.04.2023 27.04.2023	Příchozí úhrada	Klient XY příchozí platba z účtu v jiné bance		45 000,00
27.04.2023 27.04.2023	Příchozí úhrada	Klient XY příchozí platba z účtu v jiné bance		49 000,00
27.04.2023 27.04.2023	Příchozí úhrada	Klient XY příchozí platba z účtu v jiné bance		51 000,00
27.04.2023 27.04.2023	Příchozí úhrada	Klient XY příchozí platba z účtu v jiné bance		49 000,00
27.04.2023 27.04.2023	Příchozí úhrada	Klient XY příchozí platba z účtu v jiné bance		49 000,00
27.04.2023 27.04.2023	Příchozí úhrada	Klient XY příchozí platba z účtu v jiné bance		52 000,00

IN / instantní platby
Čas: 10:46 - 11:25

02.05.2023 27.04.2023	Výběr hotovosti	MoneyMula hotovostní výběr s PK	Bankomat: CESKA SPORITELNA, A.S. MOSTECKA 40, PRAHA 1, 11800, CZE	-5 000,00
02.05.2023 27.04.2023	Výběr hotovosti	MoneyMula hotovostní výběr s PK	Bankomat: CESKA SPORITELNA, A.S. MOSTECKA 40, PRAHA 1, 11800, CZE	-45 000,00
02.05.2023 27.04.2023	Výběr hotovosti	MoneyMula hotovostní výběr s PK	Bankomat: CESKA SPORITELNA, A.S. MOSTECKA 40, PRAHA 1, 11800, CZE	-49 000,00
02.05.2023 27.04.2023	Výběr hotovosti	MoneyMula hotovostní výběr s PK	Bankomat: CESKA SPORITELNA, A.S. MOSTECKA 40, PRAHA 1, 11800, CZE	-51 000,00
02.05.2023 27.04.2023	Výběr hotovosti	MoneyMula hotovostní výběr s PK	Bankomat: CESKA SPORITELNA, A.S. MOSTECKA 40, PRAHA 1, 11800, CZE	-49 000,00
02.05.2023 27.04.2023	Výběr hotovosti	MoneyMula hotovostní výběr s PK	Bankomat: CESKA SPORITELNA, A.S. MOSTECKA 40, PRAHA 1, 11800, CZE	-49 000,00
02.05.2023 27.04.2023	Výběr hotovosti	MoneyMula hotovostní výběr s PK	Bankomat: CESKA SPORITELNA, A.S. MOSTECKA 40, PRAHA 1, 11800, CZE	-52 000,00

OUT / hotovostní výběry
Čas: 10:48 – 11:28

Kontrola klienta – aneb co klient to „právník“

„K vaší zprávě:
Odkazujete se na § 9 z.č. 253/2008 Sb. znění. K tomu uvádím, že banka může provést kontrolu klienta před uskutečněním obchodu. Rozhodně banka nemůže nejprve odepsat peníze z účtu klienta a následně odešlé peníze zadržet na svém účtu a následně požadovat po klientovi doklady ke kontrole.

Odkazujete na odst. 7 § 9 a povinnosti dle tohoto ustanovení jsem dostál, protože jsem vaší bance sdělil všechny informace k původu peněz, které jsem si vložil na účet. V případě hotovosti z mých úspor neexistují doklady k původu peněz, když jde o moje naspořené finance. Cit. ustanovení neuvádí nic, že bych byl povinen bance vydávat nějaké čestné prohlášení, které by toto nahrazovalo. Mnou učiněné čestné prohlášení je to samé, jako když vaší bance do zprávy napíšu, že jde o moje úspory.

Upozorňuji vás, že když jsem zadal příkaz k úhradě jinému subjektu na úhradu částky 400 tis. Kč, tento obchod nepodléhá žádné kontrole banky z hlediska cit. zákona, protože jde o převod mezi účty klientů, které jsou identifikovatelné. Navíc jsem v příkazu uvedl poznámku, z jakého titulu peníze na účet příjemce zasílám.

Jde-li o vklady peněz, které jsem na svůj účet uskutečnil, při žádném vkladu jsem nepřekročil limit pro hotovostní platby, navíc jsem se při vkladu identifikoval. Vaše banka nemá žádné oprávnění, aby mé vklady v daný den nebo v jiné období sumarizovala a aby z toho bezdůvodně vyvozovala existenci nějakých rizikových faktorů podle zákona o legalizaci výnosů z trestné činnosti. K také dodávám, že z peněz, které jsem si 22.5. na svůj účet vložil, jsem včera 23.5. vybral částku 100 tis. Proč by měla být zrovna částka 400 tis. Kč poukazovaná bezhotovostně podezřelou, mi není zřejmé.

Vzhledem k tomu, že mi vaše banka bezdůvodně a protiprávně zadržuje peníze, opětovně vaši banku vyzývám, aby mi buď připsala zpět částku 400 tis. Kč na můj účet (tj. částku, která je nyní "ve vzduchu" někde u vaší banky, nebo aby okamžitě provedla zadanou platbu.“

Výzvy

- Regulatorní změny
- Technologická inovace a digitalizace (změna chování a požadavky klientů, např. na tzv. „chytrá řešení“ vs ochrana identity včetně té bankovní)
- Kybernetická bezpečnost (bezpečnost fin. prostředků, citlivých dat / důvěra a soukromí)
- Nástup IA / etická dilemata (otázky odpovědnosti, rozhodování založeného na algoritmech, transparentnosti a důvěryhodnosti technologií)
- Schopnost rozpoznání reálného světa od virtuálního (např. deepfakes)
- Nové informace a schopnost jejich efektivního / zákonného / využití
- Změna chování útočníků (sociální inženýrství
- …

Riziko zneužití

Bank iD

Riziko zneužití

Kim Kardashian - Deepfake

Bez spolupráce to nepůjde

Děkuji za pozornost

JUDr. Petr Barák
Vedoucí Oddělení řízení operačních rizik a AML
E-mail: petr.barak@airbank.cz
Mobil: +420 602 621 965