POLICEJNÍ AKADEMIE ČESKÉ REPUBLIKY V PRAZE

Fakulta bezpečnostně právní

Kriminalistické problémy vyšetřování fiktivních bankéřů

Rigorózní práce

Criminalistic problems of investigating fictitious bankers

Rigorous work

AUTOR PRÁCE

Mgr. Tomáš Routa

PRAHA

2024

Čestné prohlášení

Prohlašuji, že předložená práce je mým původním autorským dílem, které jsem vypracoval samostatně. Veškerou literaturu a další zdroje, z nichž jsem čerpal, v práci řádně cituji a jsou uvedeny v seznamu použité literatury.

V Praze, dne 31.05.2024

……

Mgr. Tomáš Routa

ANOTACE

Rigorózní práce z kriminalistického pohledu popisuje podvodná jednání páchaná fiktivními bankéři a jejich metodiku vyšetřování. Práce je rozdělena do čtyř kapitol. V první kapitole je vysvětlena kriminalita fiktivních bankéřů a okruhy, které přímo ovlivňují způsob spáchání. V další části první kapitoly je uveden cíl práce a popis empirického výzkumu. Ve druhé kapitole čtenáři naleznou uveřejněné výsledky z celé terénní činnosti, které jsou podpořeny grafickým vyobrazením a dalšími zjištěnými skutečnostmi. Celá třetí kapitola je věnována kriminalistické metodice vyšetřování fiktivních bankéřů. A poslední kapitola obsahuje závěrečné úvahy autora, které jsou o přijatých opatřeních proti této kriminalitě, náhled na zahraniční řešení a predikce možného dalšího vývoje.

KLÍČOVÁ SLOVA

fiktivní bankéři * metodika * podvod * sociální inženýrství * spoofing * vishing * vyšetřování

ANNOTATION

The rigorous work describes fraudulent acts committed by fictitious bankers and their investigation methodology from a criminalistic perspective. The thesis is divided into four chapters. The first chapter explains the criminality of fictitious bankers and the circuits that directly affect the method of commission. The next section of the first chapter presents the objective of the thesis and a description of the empirical research. In the second chapter, readers will find published results from the entire fieldwork, which are supported by graphical illustrations and other findings. The entire third chapter is devoted to the forensic methodology of investigating fictitious bankers. And the last chapter contains the author's final reflections on the measures taken against this crime, a preview of foreign solutions and predictions of possible future developments.

KEYWORDS

fictitious bankers * methodology * fraud * social engineering * spoofing * vishing * investigation

Obsah

Úvod

Jedním ze základních požadavků kriminalistické praxe je adekvátní odpověď na nové způsoby páchání trestné činnosti. Z kriminalistického pohledu je rigorózní práce komplexně věnována podvodnému jednání páchaného tzv. fiktivními bankéři, které se šíří přibližně od konce roku 2019, distančně a prostřednictvím komunikačních sítí.

Výsledkem této práce je specializovaná metodika, která reaguje na jednu z aktuálních forem trestné činnosti a jejím smyslem není nahradit jinou stávající, ale konkrétně doplnit už existující obecné metodiky. Čtenáři v této práci naleznou typickou metodiku, která je zpracována tak, aby přímo odpovídala současnému kriminalistickému učení.

Počáteční stránky jsou věnovány vysvětlení tématu práce a okruhům, které přímo určují způsob provedení předmětné kriminality.

Záměrně nebyla začleněna všeobecná a teoretická východiska, která by čtenáře zatěžovala a neměla větší informační přínos. Text práce předpokládá jistou odbornost čtenářů, kterým není nutné základní informace opakovaně předkládat. Přesto cítím potřebu některých čtenářů porozumět technické a teoretické stránce, a proto je v práci uvedeno množství relevantních odkazů.

Dále se čtenáři seznámí s výzkumnou činností. Nejdříve je uveden popis celého výzkumu a způsob, jakým byl proveden. Studiem vybraných spisů získané výsledky jsou uvedeny v logických uskupeních, vysvětleny písemnou formou a zpravidla pro přehlednost podpořeny grafickým vyobrazením.

Po výzkumné části je práce už věnována jejímu předmětu, a to je samotná metodika vyšetřování kriminality fiktivních bankéřů.

Práce je uzavřena úvahou nad přijatými opatřeními, zahraničním způsobem boje a budoucím vývojem – evolucí fiktivních bankéřů.

Kromě vlastního terénního výzkumu a zkušeností z dlouholetého vyšetřování kybernetické kriminality v příslušnosti Policie ČR, Územního odboru, SKPV, v obecné rovině rovněž vycházím z odborných publikací, článků a jiných prací, které sepsali odborníci. Zdroje je možné dohledat v seznamu použité literatury.

1 Řešené téma rigorózní práce

1.1 Vysvětlení názvu a problematiky práce

Tématem práce jsou kriminalistické problémy při vyšetřování *fiktivních bankéřů*[1]. Jedná se o kriminalitu, ve které jsou sofistikovaně využívané kombinace metod klamů, manipulací, komunikačních aj. technologií a organizačních prostředků. Řadíme ji do tzv. ostatní kriminality páchané v kyberprostoru s využitím dalších telekomunikačních sítí.

Digitální technika, popř. kyberprostor a mobilní sítě, fiktivním bankéřům slouží jako nástroj k páchání trestné činnosti a prostor k její realizaci. A proto se přímo nejedná o kvalifikovanou (pravou) kybernetickou kriminalitu, do které jsou řazeny trestné činy:

- *Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací*[2],
- *Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat*[3],
- *Neoprávněný zásah do počítačového systému nebo nosiče informací z nedbalosti*[4].

U fiktivních bankéřů se především jedná o distančním způsobem spáchání trestného činu *Podvod*[5]. Je možné, záleží na specifickém postupu a konkrétním počínání pachatele, aby byl doprovázen jednáním, které už ale subsumujeme pod některé shora uvedené trestné činy, popř. dále i trestný čin *Neoprávněné opatření, padělání a pozměnění platebního prostředku*[6].

S ohledem na charakter této kriminality, jedná se zpravidla jen o doprovodnou kvalifikaci (tzn. nepovinnou), byť z trestněprávního hlediska může být doprovodná kvalifikace závažnější.

---

[1] Další možná a častá označení jsou *falešní* nebo *podvodní bankéři*. S těmito názvy se setkáme především ve zpravodajství. Název *podvodní bankéři* se obecně využívá i v kriminalistické praxi.
[2] Zákon č. 40/2009 Sb., *trestní zákoník* v posledním znění, § 230.
[3] Tamtéž, § 231.
[4] Tamtéž, § 232.
[5] Tamtéž, § 209.
[6] Tamtéž, § 234.

Bankovní podvody nejsou žádnou novotou. Jednoduší i propracovanější distanční podvody páchané pod legendou a v zastoupení pracovníků bank byly již dříve. Ovšem případy *fiktivních bankéřů*, jak jsou uvedeny ve smyslu této práce, se objevují od konce roku 2019 s výrazným nástupem v následujících letech, bez ustání až dosud (rok 2024). Jedná se o aktuálně páchanou kriminalitu.

V souhrnu je možno uvést, že fiktivní bankéři využívání tzv. spoofingu a vishingu s dalšími prvky sociálního inženýrství. Dále využívají běžných a veřejně dostupných telekomunikačních služeb a jiných prostředků k navázání kontaktů, softwarových nástrojů nejen k vytváření různých rekvizit a počítačových programů a aplikací k usnadnění páchání, též ke skrytí své činnosti a pozdějšímu maskování výnosů. Pachatelé mají výhradně zištný zájem, přičemž jejich cílem jsou peníze na bankovních účtech. A kriminalitu fiktivních bankéřů je možno řadit do skupiny latentních.

Obecně jsou tyto podvody souhrou techniky, psychologie a organizace.

1.1.1 Vishing a další prvky sociálního inženýrství

Vishing je typem phishingového (kybernetického) útoku, což je jedna z forem sociálního inženýrství. Především spočívá v podvodném telefonním hovoru – tzv. *navolávání*. Vishing je odvozen od anglického sousloví *voice phishing*. A cílem útočníka je získání citlivých informací od oběti, např. jména, rodné číslo, adresy bydliště, číslo bankovního účtu nebo platební karty, přihlašovací fráze, hesla apod.[7]

V případě fiktivních bankéřů je vishing obohacen o další prvky ze sociálního inženýrství. Jedná se především o ovlivňování, a to takové, aby oběť postupovala podle představ a požadavků pachatele. V podstatě hovoříme o vmanipulování do určité situace, např. získání přístupu do zařízení oběti (typicky osobní počítač a mobilní telefon) pomocí programu vzdálené správy[8], odeslání finančních prostředků z bankovního účtu apod. Není vyloučena ani kombinace těchto situací.

[7] Evropská rada a Rada Evropské unie. *Kybernetická bezpečnost: sociální inženýrství*. Online. Dostupné z: https://www.consilium.europa.eu/cs/policies/cybersecurity/cybersecurity-social-engineering/. [cit. 26.01.2024].
[8] Např. aplikace AnyDesk vyvinutá spol. AnyDesk Software GmbH (Německo) nebo aplikace TeamViewer vyvinutá spol. TeamViewer GmbH (Německo).

Navolávání může být prováděno plošně, tj. telefonování na nahodilá či dříve získaná telefonní čísla, nebo cíleně. Pokud je cílené, tak se jedná o zvláštní variantu vishingu, tj. tzv. *spear vishing*. V tomto případě je pachatel do určité míry už seznámen s obětí, ke které přistupuje velmi individuálně a s dopředu připraveným scénářem.[9] Tato forma útoku je lstivější a nebezpečnější. Oběti se obtížněji identifikuje podvodné jednání, a pokud je provedeno správně, tak může zaskočit i obeznámeného a pozorného telefonistu.

U případů fiktivních bankéřů není vyloučena ani varianta obráceného vishingu. Při obráceném je volající oběť, která svým hovorem reagujete na nějaké předešlé upozornění nebo informační sdělení, např. podvodná e-mailová zpráva, SMS apod.

Manipulace a další techniky ze sociálního inženýrství jsou základem komunikace fiktivních bankéřů. Kdo podobné situaci nečelil, tak nepochopí, jak propracovaná a komplexní je především psychologická stránka celého podvodu. Založené jsou na stupňujícím nátlaku a vyvolávání negativních pocitů strachu a úzkosti.

Pachatel v úvodu poleká oběť neoprávněnou událostí spojenou s jejím bankovním účtem nebo jen službou poskytnutou bankou. Překvapivou a naléhavou zprávou vyvolávají pocit stresu a obavy. U oběti dojde k upozadění racionálního uvažování. Informativní dezorientace je dalším krokem k úspěchu. Pachatelé následně oběť zavalí množstvím informací a nutných postupů. Zároveň zdůrazní, že je nutné situaci řešit nyní a bezodkladně, jinak dojde k fatálnímu zneužití bankovního účtu a tím ke značným škodám. Využívají správnou bankovní terminologii a jsou velice dobře připraveni na případné dotazy.

Pachatelé postupují zprvu mírně, slušně až starostlivě. Využívají metod sugesce a asertivní komunikace. Později, pokud to situace vyžaduje a oběť stále více komunikuje obezřetněji, popř. se zdráhá provést nějaké potřebné kroky, přechází do verbální agrese až vyhrožování různými důsledky, např. tím, že banka vyvodí konsekvence z odmítnutého pokračování v hovoru.

[9] SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. vydání. Plzeň: Aleš Čeněk, 2022. ISBN 978-80-7380-849-5, s. 225-227.

1.1.2 Spoofing a VoIP

Fiktivní bankéři se maskují a využívají různých identit. Jednají např. jako úředníci bank, bankovní poradci a bezpečnostní technici. Není žádnou výjimkou využití identit policistů. Identity navíc nemusí být rovnou zcela smyšlené. Použitá jména mohou vycházet ze skutečnosti, čehož využívají a mohou tím navýšit úspěšnost podvodu.

Maskování se provádí, pomineme-li v průběhu hovoru lživé ústní prohlášení volajícího, nahrazením patrných projevů použitého prostředku k navázání komunikace. Tato maskování se označují jako spoofing.

Spoofing je termín používaný v oblasti kybernetické bezpečnosti k popisu techniky, která spočívá v maskování (překrytí) pravé identity. Tzn. věruhodně předstírat potřebnou (důvěryhodnou) identitu nebo původ telekomunikačního a datového provozu.[10] Fiktivní bankéři pomocí spoofingu napodobují ID[11] volajícího, tj. telefonní číslo, a to modifikací parametru *Calling line identification*[12] (zkráceně CLI).

Technika spoofingu je obvykle obohacena o volání přesměrovaná ze zahraničí. K přesměrovaným hovorům pachatelé využívají konfigurovatelné technologie typu *Voice over Internet Protocol*[13] (zkráceně VoIP), případně i připojení k síti Internet pomocí *Virtual private network*[14] (zkráceně VPN).

VoIP mj. umožňuje přenos zdigitalizovaného hlasu z internetové sítě do veřejných sítí ostatních providerů poskytující běžné telekomunikační služby. A pomocí doplňkového softwaru umožnuje upravit telefonní číslo aj. ID volajícího podle vlastního výběru.[15] K prohloubení anonymity jsou tato volání z pravidla vícenásobně předávána (řetězena) přes více zahraničních providerů.

---

[10] KESHAV, Jindal; DALAL, Surjeet a KUMAR SHARMA, Kamal. *Analyzing Spoofing Attacks in Wireless Networks*. New Jersey: IEEE, 2014. ISBN 978-1-4799-4910-6, s. 398-402.
[11] ID je označení pro jednoznačnou identifikaci, popř. individuální nebo unikátní označení.
[12] *Caller ID*. Online. In: Wikipedia. Stránka byla naposledy editována 20.11.2023 v 03:05. Dostupné z: https://en.wikipedia.org/wiki/Caller_ID. [cit. 27.01.2024].
[13] *Voice over Internet Protocol*. Online. In: Wikipedia. Stránka byla naposledy editována 15.01.2024 v 21:38. Dostupné z: https://en.wikipedia.org/wiki/Voice_over_IP. [cit. 27.01.2024].
[14] *Virtual private network*. Online. In: Wikipedia. Stránka byla naposledy editována 19.01.2024 v 07:17. Dostupné z: https://en.wikipedia.org/wiki/Virtual_private_network. [cit. 27.01.2024].
[15] *VoIP phone*. Online. In: Wikipedia. Stránka byla naposledy editována 27.09.2023 v 15:54. Dostupné z: https://en.wikipedia.org/wiki/VoIP_phone. [cit. 27.01.2024].

1.1.3 Fiktivní bankéři v současné praxi

V současné kriminalistické praxi se případy fiktivních bankéřů ustálily do čtyř základních podob (scénářů), které mohou být různě modifikované o použité smyšlené situace, komunikační prostředky, k podpoře podvodu použité rekvizity nebo směřování výnosů.

Jedná se o tyto podoby:

1) Pachatel se vydává za pracovníka bank nebo policistu a náhodně navolává oběti. Pod legendou napadení bankovního účtu a nutnosti ochrany peněz zmanipuluje oběť, aby peníze přeposlala, např. na určené „bezpečné“ účty nebo vložila do automatů na nákup kryptoměn podle QR kódů.
2) Pachatel se vydává za pracovníka bank nebo policistu a cíleně volá vybrané oběti, o které zná alespoň částečné informace (jedná se o spear vishing). Následná situace je obdobná k prvnímu scénáři.
3) Pachatel se vydává za pracovníka bank a náhodně navolává. Obětem oznámí, že je nutno doplnit žádost o úvěr či jiný bankovní produkt, který měla oběť vyžádat. Cílem je oběť zmást tím, že do jejího bankovnictví zřejmě někdo pronikl a produkt na místo ní vyžádal. Oběť je přepojena na spolupachatele, např. bezpečnostního experta, který zajistí ochranu účtu a peněz. Je možné i další zmanipulování oběti a získání půjčky od banky. Následná situace je obdobná k předchozím scénářům.
4) Pachatel se vydává za pracovníka bank a cíleně volá oběti, která není české národnosti. Oběť je dopředu vytipována a komunikace není vedena v českém jazyce. Následná situace je obdobná k předchozím scénářům.

Není podstatné, aby tzv. navolávač vystupoval přímo jako pracovník banky, u které má oběť vedený bankovní účet. Běžně také vystupují jako bezpečnostní nebo expertní pracovníci České národní banky.

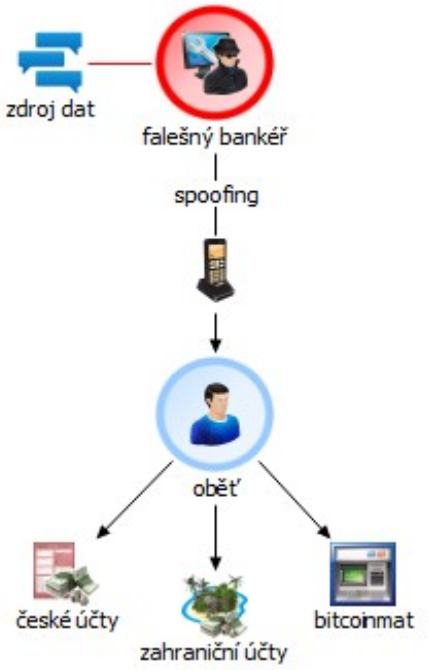
V jednotlivých scénářích mohou být a často jsou využíváni další spolupachatelé, kteří podporují legendu navolávače. Tito spolupachatelé pak vystupují v různých rolích. Typická a častá je role kriminalisty. Ten poskytne oběti lživé informace, o již zahájeném šetření, domlouvá realizaci smyšleného výslechu a z důrazní nutnost spolupráce s bankou, tedy s navolávačem.

Dále mohou být využity již zmíněné nástroje pro vzdálenou správu koncového zařízení uživatele, což je např. mobilní telefon, notebook apod.

Nástroje pro vzdálenou správu pachatelé využívají z více důvodů. Jednak získají přímí vstup do bankovnictví oběti, kde mohou sami kumulovat peníze a provést převody. Dále mohou od bank vyžádat tzv. minutové půjčky s cílem navýšit výnos, získávají další osobní informace a údaje o oběti. A rovněž získávají informace z historie nebo výpisu z účtu, jako jsou jména a další čísla bankovních účtů, které mohou později využít k cílenému útoku na další oběť.

Níže jsou předložena grafická vyobrazení fiktivních bankéřů. Základní a komplexní varianta průběhu. Nutno uvést, že reprezentativně znázorňují průběh jednání fiktivních bankéřů pouze do získání finančních prostředků. Není řešena následná situace při maskování výnosů nebo dalšího pozdějšího počínání.

Obrázek č. 1 – Základní varianta fiktivního bankéře



Zdroj: Vlastní zpracování

Z kriminalistické praxe jsou známi i takové případy, např. kdy k úspěšnému podvodu pachateli (navolávači), který vystupoval jako pracovník banky, postačily dva hovory k výnosu přesahující přes 1.500.000 Kč. Pachatel nejdříve přesvědčil oběť, aby v několika pobočkách banky vybrala veškeré své úspory, pracovníkům

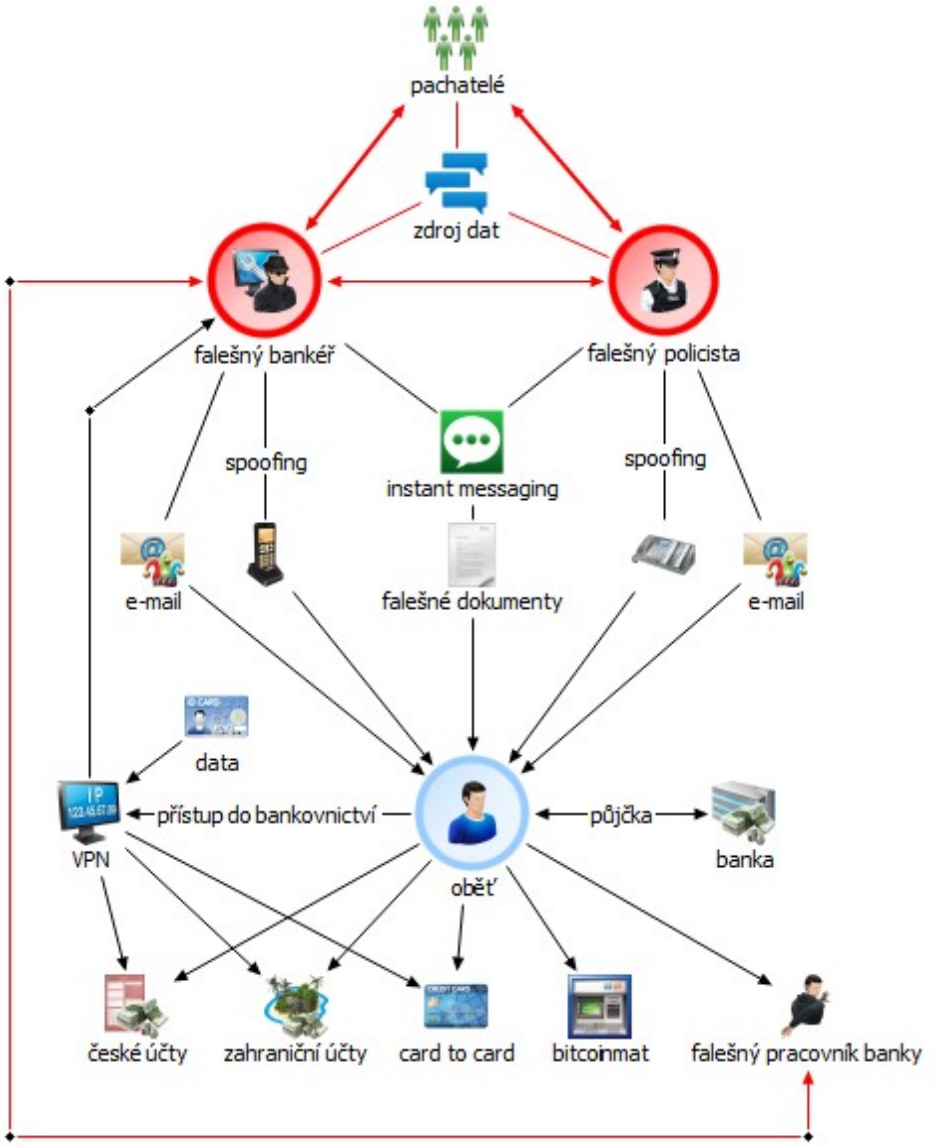
uvedla lživé informace a důvody k výběrům. A následně všechny peníze přeposlala na „bezpečný účet“ (vložila do automatu na nákup kryptoměn).

Takto vcelku jednoduchá, avšak účinná varianta fiktivního bankéře je zobrazena na přiloženém obrázku č. 1 (předchozí strana).

Existují i složité varianty využívající značné množství prostředků. Provedení může být propracované a oběť je sofistikovaně a systematicky manipulována.

Příklad takového podvodu je graficky znázorněn na přiloženém obrázku č. 2.

Obrázek č. 2 – Komplexní varianta fiktivního bankéře



Zdroj: Vlastní zpracování

1.2 Cíle a provedení rigorózní práce

1.2.1 Cíle práce

Cílem této rigorózní práce je vypracování kriminalistické metodiky vyšetřování fiktivních bankéřů.

Kriminalistická metodika musí být založena na zkušenostech vyšetřovací a soudní praxe, a proto jsem nejdříve provedl empirický výzkum, na jehož základě bude vypracována. A dále ji doplním o vlastní zkušenosti z vyšetřování.

Výzkum je rozdělen do dvou částí, a to sběr informací, což je realizováno formou statistického šetření prostřednictvím předpřipravených otázek a dále studia spisů. Studium dopomůže získat další nezbytné informace, které nelze statistiky měřit. Objektem výzkumu jsou informace z vyšetřovacích spisů.

Prostřednictvím studia vyšetřovacích spisů a zodpovězení výzkumných otázek bude následně dosaženo cíle práce.

Čtenářům jen krátce připomenu, že *„metodika vyšetřování je ta část kriminalistické vědy, která odhaluje a zkoumá zákonitosti vzniku stop a zvláštnosti postupů při vyhledávání, zajišťování a využívání stop a zvláštností postupů při vyhledávání, zajišťování a využívání stop, jiných soudních důkazů a kriminalisticky významných informací s ohledem na určitý typ trestného činu a předpokládanou typovou vyšetřovací situaci.“*[16]

Jak bylo výše uvedeno, tak podstatou tvorby metodik je vědecký přístup. Poznatky získané z kriminalistické a soudní praxe budou uspořádány tak, aby jejich zpracování odpovídalo aktuálnímu učení kriminalistické metodiky.

„Každá z metodik vyšetřování jednotlivých druhů trestných činů představuje uspořádaný systém poznatků a doporučení s pevně stanovenou strukturou. Strukturu metodik vyšetřování jednotlivých druhů trestných činů představují následující komponenty:

1. *typová kriminalistická charakteristika dané skupiny trestných činů,*
2. *stopy typické pro daný typ trestných činů,*

[16] NĚMEC, Miroslav et al. *Teorie a metodologie kriminalistiky pro magisterské studium – I. díl. Aktuální problémy kriminalistické teorie*. Praha: ABOOK, 2018. ISBN 978-80-906974-1-6, s. 62.

3. *zvláštnosti předmětu vyšetřování,*
4. *typické podněty k vyšetřování a jejich zvláštnosti,*
5. *typické vyšetřovací situace vyskytující se při vyšetřování daného typu trestných činů,*
6. *typické počáteční úkony a jejich zvláštnosti,*
7. *typové vyšetřovací verze a zvláštnosti vytyčování vyšetřovacích verzí, plánování a organizace vyšetřování,*
8. *zvláštnosti následné etapy vyšetřování,*
9. *zvláštnosti zapojení veřejnosti do vyšetřování.“*[17]

1.2.2 Plán postupu

Rigorózní práci jsem zpracoval na základě níže uvedeného plánu, přičemž tento postup se mi osvědčil už během dřívějších studií a pracích na jiných tématech.

Obsah plánu:

1. úvaha nad teoretickými východisky a následně provedené pilotní šetření (popis pilotního šetření viz subkapitola 1.2.4),
2. editace, doplnění a konečné stanovení výzkumných otázek (přehled otázek viz subkapitola 1.2.5),
3. realizace statistického výzkumu a studium vyšetřovacích spisů (vlastní samostatná terénní práce),
4. analýza, popsání a vysvětlení získaných informací doplněné o vlastní zkušenosti z kriminalistické praxe (viz kapitola 2 a její subkapitoly),
5. vypracování metodiky (viz kapitola 3 a její subkapitoly).

1.2.3 Použité metody

K provedení celého výzkumu a k následnému dosažení cíle práce jsem použil empirické vědecké metody zjišťování faktů a dále zpracování údajů (prvky kvalitativního a kvantitativního hodnocení).

Základní použitá vědecká metoda byla explorace, na kterou jsem navázal analýzou, syntézou, indukcí a dedukcí. Zjištěné informace jsem také podrobil komparaci a deskripci.

[17] Tamtéž, s. 63.

V další části práce jsem hojně využíval generalizace zjištěných informací.

Při zaznamenávání výsledků jsem dále využíval obecně platné matematické postupy (sčítání, odčítání, zaokrouhlení a procentuální výpočty).

1.2.4 Realizace výzkumu

Teorii, která je základem kriminality fiktivních bankéřů, jsem vzal na vědomí v rámci procesu při myšlenkové přípravě na výzkumnou část.

Souhrnně se jedná například o právní úpravu, technické procesy sítě Internet, organizačně-technické možnosti a způsoby evidence Policie ČR, kriminalistické možnosti při prověřování nebo vyšetřování a další. Na tento proces jsem navázal a provedl další zkoumání.

Provedení terénního výzkumu, pro který jsem vybral období od počátku roku 2022 až do konce roku 2023[18], předcházelo pilotní šetření.

Pilotní šetření spočívalo ve vyhodnocení 6 vyšetřovacích spisů (výzkumný vzorek), které byly součástí různých sérií fiktivních bankéřů. Do tohoto šetření jsem vstoupil se základními otázkami, které byly postupně doplňovány o další vhodné, a to podle informací, které bylo možno obecně zjistit a statisticky měřit. V druhé polovině roku 2023 byl seznam otázek uzavřen. Pilotní šetření také přineslo cenné informace následně využité při sestavování procesu výzkumu.

Je nutno čtenářům vysvětlit, že studium spočívalo ve čtení rozhodných písemností z vyšetřovacích spisů (např. výslechy, protokoly o ohledání, protokoly o zvláštních důkazních prostředcích, usnesení o obvinění, obžaloby, soudní rozhodnutí apod.). Tímto jsem především zjišťoval, jakým způsobem se pachatel trestného činu dopustil, průběh vyšetřování a jakým způsobem bylo dosaženo objasnění případu, popř. proč nebylo prověřování úspěšné. Tato zjištění budou zohledněna popisně, bude-li to vhodné jako poznámka k vybrané odpovědi na otázku a dále zobecněna v metodice vyšetřování (viz kapitola 3).

Sběr informací jsem provedl prostřednictvím interního informačního systému Policie ČR. Respektive přes systém *Elektronické trestní řízení* (zkráceně ETŘ)

[18] O důvodech výběru let 2022 a 2023 pro výzkum, také viz subkapitola 2.2, otázka č. 1.

a jeho analyticko-statistickou nástavbu (především byl využit „*komplexní dotaz*“). Obdobně byly vyhledány také případy k celému studiu.

K vyhledávání jsem také využil analyticko-technické funkcionality, tzv. štítků, kterými jsou v rámci ETŘ rovněž označovány případy. Štítky pomáhají rozlišovat různé formy páchání nejen kybernetické kriminality.

Výzkum byl proveden v období od počátku ledna až do konce března roku 2024. Považuji tento údaj rovněž za důležitý, neboť budoucí kontrola výsledků, popř. nově provedené šetření, by mohlo vykazovat jisté odchylky. Především pak ukončené případy z důvodu nezjištění pachatele[19] mohou být později dále rozpracovány (s ohledem na výsledky operativního šetření).

Dotaz do informačního systému Policie ČR obsahoval tato filtrační kritéria:

- *období zaevidování (1. ledna 2022 až 31. prosince 2022),*
- *místo zaevidování (Středočeský kraj),*
- *místo šetření (Středočeský kraj),*
- *štítkové označení (bankéř),*
- *kybernetická kriminalita (v ETŘ označována jako „IT kriminalita“),*
- *ukončené případy*,
- *(závěrečná manuální selekce chybových záznamů).*

Pomocí těchto kritérií jsem získal všechny výsledky. Z výsledků byly odstraněny ty případy, které byly po zaevidování podle příslušnosti postoupeny do jiného kraje ke konání prověřování/vyšetřování (např. z důvodu společného řízení).

Výzkum byl proveden pouze v rámci evidence a území Středočeského kraje, kde byl případ také ukončen. Pokud by byly vzaty v potaz i případy předané mimo Středočeský kraj, mohlo by dojít k ovlivnění výsledků duplicitou kvůli pozdějšímu sloučení.

1.2.5 Výzkumné otázky

Otázky, které jsou uveřejněny na následujících stránkách, obrazně zahrnují přednastavená kritéria, viz předchozí subkapitola, a proto jsou bez dalších

[19] Zákon č. 141/1961 Sb., *o trestním řízení soudním (trestní řád)* v posledním znění, § 159a odst. 5 (nepodařilo se zjistit skutečnosti opravňující zahájit trestní stíhání).

specifikací. Podrobnější vyjádření by otázky jen zahlcovalo informacemi nad míru nezbytně nutnou a omezovalo jejich celkovou přehlednost a srozumitelnost.

Pro potřeby této části výzkumu bylo stanoveno 66 otázek.

Otázky byly uspořádány do šesti skupin a byla stanovena jejich posloupnost následně:

I. přehled případů,
II. způsob provedení,
III. vyšetřování,
IV. pachatelé,
V. oběti,
VI. časové souvislosti.

Znění jednotlivých otázek:

I. přehled případů:

1. Kolik případů bylo celkem evidováno?
2. Kolik případů obsahovalo více dílčích skutků?
3. Kolik skutků bylo dokonaných a kolik v pokusu?
4. Kolik případů bylo objasněno?
5. Kolik skutků bylo zaměřeno na cizince?

II. způsob provedení:

6. Byl proveden předběžný kontakt?
7. Kdo byl původcem prvního hovoru?
8. V jaké denní době pachatel provedl první hovor?
9. Jaká byla četnost hovorů?
10. Jaká byla celková délka hovorů?
11. Jak často byl využíván další komunikační kanál?
12. Jak často bylo využito maskování kontaktu?
13. Odpovídal maskovaný kontakt reálnému?
14. V jaké roli pachatel vystupoval?
15. Jaká legenda byla použita?
16. Bylo využito pomoci spolupachatele?

17. V jaké roli spolupachatel vystupoval?
18. Jakého rázu bylo komunikační vystupování pachatelů?
19. Pokusil se pachatel přesvědčit oběť k půjčce?
20. Podařilo se pachateli získat citlivé údaje oběti?
21. Získal pachatel přístup do internetového bankovnictví oběti?
22. Jakým způsobem pachatel získal přístup do bankovnictví?
23. Jakým způsobem pachatel získal peníze z účtu oběti?
24. U kolika skutků byl výnos směřován do kryptoměn?
25. Bylo využito dalších služeb?
26. Pokračoval pachatel v komunikaci po získání peněz?
27. U kolika skutků pachatel zajistil manipulací odstranění stop nebo jiných informací?
28. Bylo zřejmé, že pachatel dopředu znal nějaké informace o oběti?
29. V jakém okamžiku si oběť uvědomila, že se jedná o podvod?

III. vyšetřování:

30. Jak bylo zjištěno, že byl skutek spáchán?
31. Jaké kriminalistické stopy byly zajištěny?
32. Byly zajištěny jiné soudní důkazy?
33. Zaslechla oběť v pozadí hovorů nějaké zvuky?
34. Jaká byla způsobená škoda v porovnání oběť/Kč?
35. Podařilo se zajistit výnos?
36. Jaká byla výše zajištěného výnosu?
37. V kolika případech zjištěné informace vedly do zahraničí?
38. V kolika případech bylo provedeno mezinárodní šetření?
39. Jaké varianty mezinárodního operativního šetření jsou prováděny?
40. Byla zapojena veřejnost do vyšetřování?
41. Byla zjištěna organizovaná skupina?
42. Jaká byla role známého pachatele v organizované skupině?
43. Jaké bylo zavinění u známého pachatele?
44. Jaké bylo chování pachatele při vyšetřování?
45. Jaký způsob obhajoby pachatel zvolil?
46. Bylo zaznamenáno nějaké ovlivňování svědků/obětí?

47. V kolik případech se pachatel doznal?

IV. pachatelé:

48. Jaké bylo pohlaví pachatele?

49. Jakého věku byl pachatel?

50. Jaké národnosti byl pachatel?

51. Jaké je nejvyšší dosažené vzdělání pachatele?

52. Byl pachatel už dříve trestán?

53. Byl pachatel v době činu zaměstnán?

54. Jakým jazykem pachatel hovořil?

V. oběti:

55. Jaké bylo pohlaví oběti?

56. Jakého věku byla oběť?

57. Jaké národnosti byla oběť?

58. Jakým jazykem oběť hovořila?

59. Jaké je nejvyšší dosažené vzdělání oběti?

60. Byla oběť už dříve cílem kybernetického útoku?

VI. časové souvislosti:

61. Jaká doba uplynula od prvního k poslednímu kontaktu pachatele s obětí?

62. Jaká doba uplynula od zjištění podvodu k oznámení?

63. Jaká doba uplynula od oznámení k zahájení vyšetřování?

64. Jaká doba uplynula od zahájení vyšetřování k podání obžaloby?

65. Jaká doba uplynula od podání obžaloby do soudního rozhodnutí?

66. Jaká doba uplynula od prvního kontaktu do soudního rozhodnutí?

2 Výzkum

2.1 Úvod

V této části práce jsou uveřejněny všechny výsledky z provedeného výzkumu. Výsledky, jak bylo naznačeno v předchozí subkapitole, jsou vhodně doplněny dalšími informacemi ze studia spisů, o jiné zjištěné poznatky a dále mé vlastní zkušenosti z vyšetřování případů fiktivních bankéřů.

V rámci metodiky, která byla zpracována v pozdější části práce (kapitola 3 a její subkapitoly), byla totiž hodnocena i problematika, kterou nelze vysvětlovat pouze na základě statistického šetření. Statistické šetření je nutno primárně brát jako součást celku terénního šetření, které vedle studia vyšetřovacích spisů, přináší především cílené odpovědi o určitých faktorech a měřitelných okolností sledované problematiky.

Několik slov k technickému a organizačnímu uveřejnění výsledků. Získané znalosti byly vysvětleny primárně textovou formou. Výsledky, kde to bylo vhodné, byly podpořeny grafickým vyobrazením.[20] Rovněž jsou uvedeny v přesných počtech zpravidla společně s procentuálním přepočtem (v závorce za výsledky). Procentuální výsledek byl podle obecně platných pravidel zaokrouhlen na celá čísla. A výsledky jsou organizované v tomto pořadí: z roku 2022, z roku 2023, celkové počty a komentář s výjimkami naposledy.

Při studiu výsledků je nezbytné mít na paměti kritéria uvedená v subkapitole 1.2.4, neboť tyto jsou promítnuty v celém tomto terénním šetření.

Konečná suma vyšetřovacích spisů s ohledem na možnosti obsaženého objemu sběrných informací byla vyhodnocena celá a beze zbytku kromě případů, které nebyly dosud uzavřeny. To znamená, že počet případů, ze kterých vycházejí odpovědi na otázky, bude uveden v rámci odpovědi na 1. otázku, pokud u jiné není uvedeno jinak. Nebylo žádnou výjimkou, že některé informace z některých spisů nebyly vůbec zjištěny.

[20] Grafika byla vytvořena pomocí kancelářského editoru od zahraniční společnosti Microsoft, Inc. (USA), tj. Microsoft Office 365 ProPlus 2019 (textový procesor Word).

2.2 Výsledky

I. přehled případů

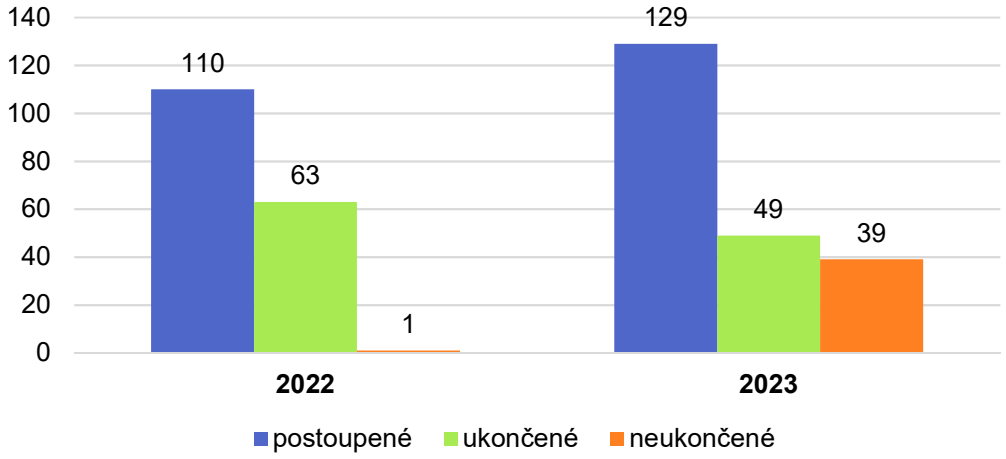
Otázka č. 1: Kolik případů bylo celkem evidováno?

Zodpovězením této filtrační otázky bylo zjištěno, z kolika celkem případů obecně vycházelo terénní šetření.

V roce 2022 bylo v rámci Středočeského kraje evidováno **174** případů fiktivních bankéřů. 110 případů bylo předáno do společnému řízení, popř. předáno podle místní příslušnosti do jiného kraje. Ze zůstatku, tj. 64, bylo ukončeno 63 (98 %) případů. Tudíž část této práce vychází z 63 případů z roku 2022.

V roce 2023 bylo v rámci Středočeského kraje evidováno **217** případů fiktivních bankéřů. 129 případů bylo předáno do společnému řízení, popř. předáno podle místní příslušnosti do jiného kraje. Ze zůstatku, tj. 88, bylo ukončeno 49 (56 %) případů. A další část této práce vychází ze 49 případů z roku 2023.

Graf č. 1 – Kolik případů bylo celkem evidováno?



Zdroj: Vlastní zpracování

Celkem práce vychází ze **112** případů (74 % případů z roků 2022 a 2023).

Roky 2020 a 2021 byly vyloučeny rovnou, a to z toho důvodu, že štítkové označení případů (viz subkapitola 1.2.4) nebylo využito v rámci této kriminality až do konce roku 2022. A vyhledávání by muselo být provedeno jinou analytickou metodou, která by nezaručovala tak přesné výsledky.

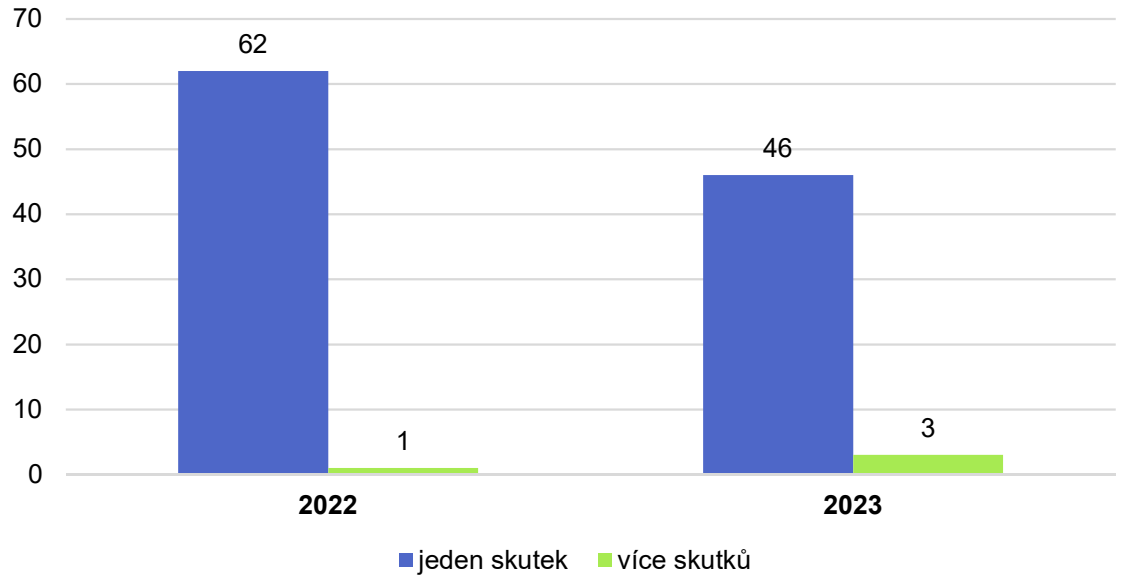
Otázka č. 2: Kolik případů obsahovalo více dílčích skutků?

Hlavním cílem této otázky bylo zjistit, kolik případů obsahuje více dílčích skutků a případě stanovit i jejich počty.

Prověrkou případů bylo zjištěno

- v roce 2022: 62 případů bylo vedeno pro jeden skutek. A 1 případ byl veden pro více skutků. Bylo to celkem 5 dílčích skutků. Dohromady to bylo 67 skutků.
- V roce 2023: 46 případů bylo vedeno pro jeden skutek. A 3 případy byly vedeny pro více skutků. Respektive 1 případ obsahoval 2 a 2 obsahovaly stejně po 5 dílčích skutcích. Dohromady to bylo 58 skutků.

Graf č. 2 – Kolik případů obsahovalo více dílčích skutků?



Zdroj: Vlastní zpracování

Celkem tedy bylo 108 případů vedeno pro jeden skutek a 4 případy byly vedeny pro více dílčích skutků. 112 případů obsahovalo 125 skutků.

Z ostatních krajů bylo postoupeno 9 dílčích skutků a 4 byly zaevidovány už v rámci Středočeského kraje.

Ačkoliv v rámci Středočeského kraje byly vedeny série, tak se jednalo jen o menší do 5 dílčích skutků. Ze své praxe jsem však obeznámen s tím, že v rámci jiných

KŘ jsou vedeny rozsáhlé série s desítkami i stovkami dílčích skutků. To potvrzuje i ta skutečnost (viz otázka č. 1), že 239 dílčích skutků (dohromady za rok 2022 a 2023) bylo postoupeno mimo Středočeský kraj. Postoupení byla zpravidla provedena na základě koordinačních pokynů o společném řízení Úřadu služby kriminální policie a vyšetřování Policejního prezidia České republiky (zkráceně ÚSKPV).

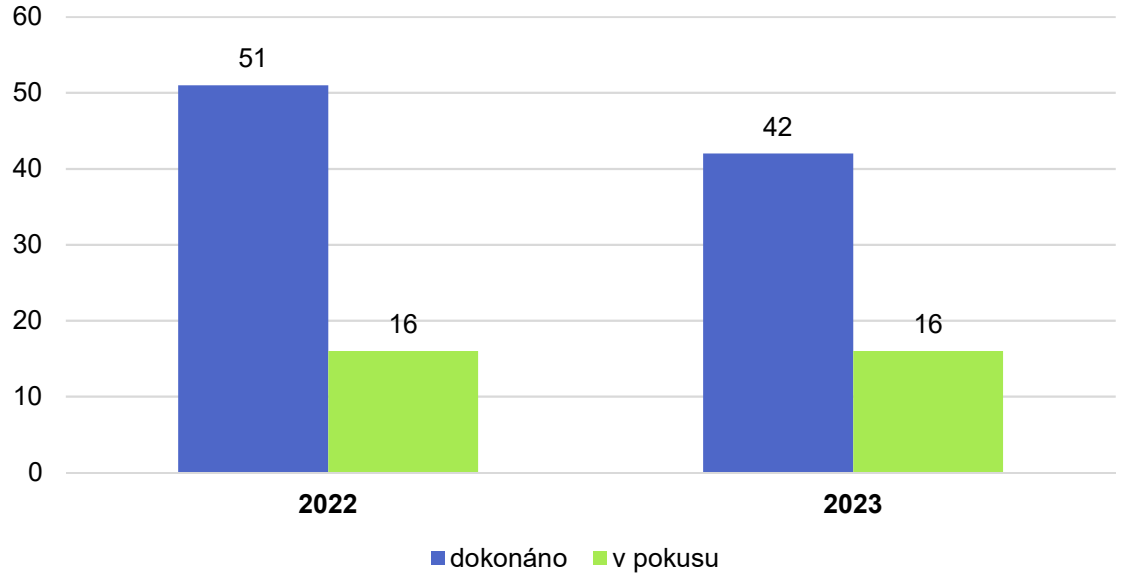
Otázka č. 3: Kolik skutků bylo dokonaných a kolik v pokusu?

Podstatou odpovědi na tuto otázku bylo zjištění, jaká je míra úspěšnosti pachatelů dokončit svá podvodná jednání. Úspěšnost byla hodnocena podle způsobené materiální škody – pachatel získal peníze, což je jejich primární cíl.

Vývojové stádium bylo u skutků

- v roce 2022: 51 (76 %) dokonaných a 16 (24 %) v pokusu,
- v roce 2023: 42 (72 %) dokonaných a 16 (28 %) v pokusu.

Graf č. 3 – Kolik skutků bylo dokonaných a kolik v pokusu?



Zdroj: Vlastní zpracování

Celkem pachatelé byli úspěšní u 93 (74 %) a neúspěšní u 32 (26 %) skutků.

Čtenářům je nutné vysvětlit, že nezdar pachatele nebyl zapříčiněn jen pozorností oběti nebo nesprávně provedeným jednáním, avšak i šťastnou náhodou.

Z vyšetřovací praxe je znám i takový případ, kdy oběť byla připravena značnou sumu vložit do automatu na nákup kryptoměn, avšak nakonec k tomu nedošlo, neboť baterie v mobilním telefonu oběti byla už vybitá po dlouhém hovoru. Oběť, která byla důchodového věku a která nezískala od pachatele další dostatečné informace, jak provést vložení a na jaká místa peníze poukázat, odcestovala do banky. A v bance byla poučena o tom, že se jednalo o podvod.

Otázka č. 4: Kolik případů bylo objasněno?

Otázka stejně jednoznačná, jako jsou bohužel zjištěné výsledky.

V roce 2022 nebyl objasněn ani jeden z 63 (0 %) případů.

V roce 2023 rovněž nebyl objasněn ani jeden ze 49 (0 %) případů.

Celkem byla nulová (0 %) objasněnost.

Bez grafického vyobrazení.

Čtenářům připomenu, že 40 případů (celkem za rok 2022 a 2023) je stále šetřeno, avšak zásadní průlom ve výsledcích zde neočekávám. Valná část neukončených případů byla také zběžně prostudována a po jejich ukončení výsledky nebudou vybočovat od už uzavřených.

Na drastické míře neobjasněnosti se podepisují pachateli vhodně využívané anonymizační technické prostředky a mezinárodní charakter případů (o tomto později, viz otázka č. 37, str. 60 této práce).

Zdárně vyřešených případů není mnoho ani v rámci ostatních KŘ. Na tomto místě je možno uvést, že kriminalisté z KŘ Vysočina úspěšně vyřešili případ fiktivních bankéřů z roku 2021, který obsahoval až **803 dílčích skutků** se škodou okolo 200 miliónů korun.[21]

V rámci této otázky nebyly vzaty v potaz případy vzniklé pozdějším vyčleněním, ve kterých bylo prověřováno, popř. i vyšetřováno, podezření z legalizace výnosu z trestné činnosti bez ohledu na zavinění. V případě nedbalosti se zpravidla jedná o osoby, jejich bankovní účty byly zneužity k převodům, přičemž těmto převodům

[21] DIVIŠOVÁ, Jana. Falešný bankéř – zase. *POLICISTA*. 2024, č. 1, s. 28-29. ISSN 1211-7943.

často v omylu i vypomáhaly. U úmyslné legalizace se jedná o osoby napojené na pachatelé, kterým vypomáhají např. tím, že pomocí tokenů platebních karet vybírají peníze z bankomatů nebo přímo přebírají hotovost od obětí. Tyto osoby se občas daří identifikovat a vyšetřovat.

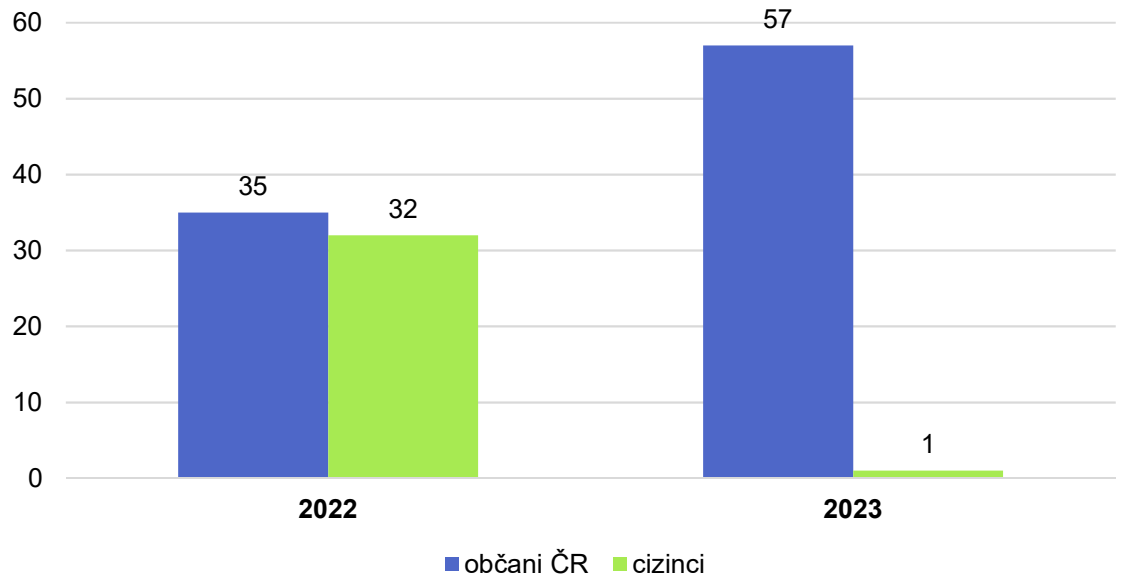
Otázka č. 5: Kolik skutků bylo zaměřeno na cizince?

Smyslem poslední otázky z první otázkové skupiny bylo zjistit, na jaké obyvatelé s ohledem na jejich národnost se pachatelé zaměřují.

Zaměření

- v roce 2022 u 35 (52 %) skutků bylo proti občanům České republiky a 32 (48 %) proti občanům s cizí příslušností;
- v roce 2023 u 57 (98 %) skutků bylo proti občanům České republiky a 1 (2 %) proti občanovi s cizí příslušností.

Graf č. 4 – Kolik skutků bylo zaměřeno na cizince?

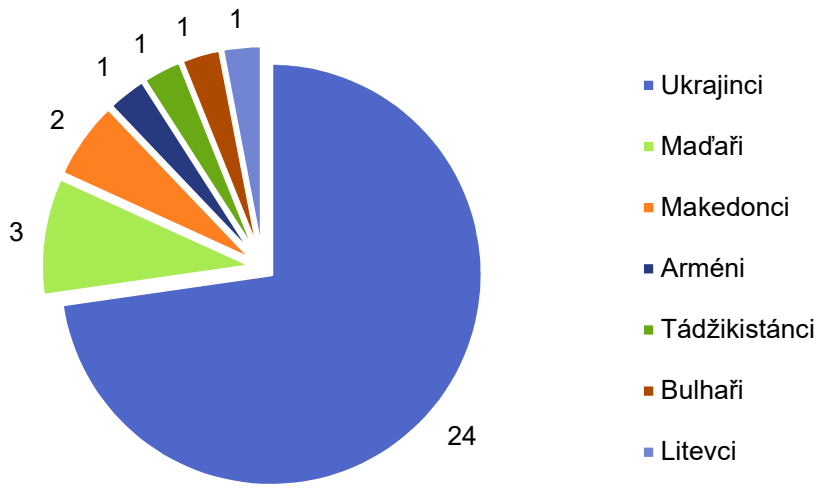


Zdroj: Vlastní zpracování

Celkem 92 (74 %) skutků bylo proti občanům České republiky a 33 (26 %) proti občanům s cizí příslušností.

U cizinců se především jednalo o občany Ukrajiny (24x), Maďarska (3x), Severní Makedonie (2x), Arménie (1x), Tádžikistánu (1x), Bulharska (1x) a Litvy (1x).

Graf č. 5 – Národnost cizinců



Zdroj: Vlastní zpracování

II. způsob provedení

Otázka č. 6: Byl proveden předběžný kontakt?

Není to tak časté u případů fiktivních bankéřů, že by byl proveden kontakt před podvodným hovorem. V praxi se ale objevovaly poznatky o tom, že oběť obdržela např. e-mailovou zprávu s informacemi o fiktivní službě, popř. SMS s potvrzením o provedené fiktivní platbě. Následoval hovor pachatele, který už jako pracovník banky uvedl, že „banka“ zjistila neoprávněnou platbu.

V podstatě se jedná o způsob, jak podpořit legendu a zvýšit úspěšnost podvodu. Není vyloučena ani varianta, že v SMS zprávě nebo v jiném psaní bude uvedeno kontaktní telefonní číslo a výzva s tím, že následný hovor má provést sama oběť (kdo provedl první hlasový kontakt je uvedeno v odpovědi na další výzkumnou otázku).

V rámci této otázky není řešena problematika tzv. phishingu. Tedy jednání, jehož cílem je především v textové formě vylákat osobní, přihlašovací nebo jiné citlivé

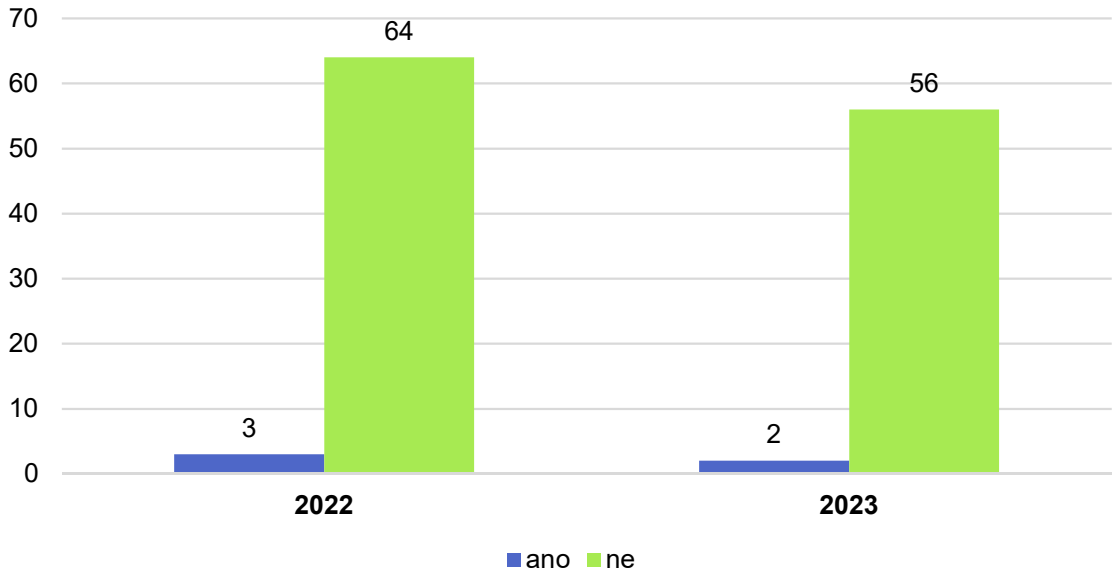
údaje. Na začátku této otázky zmíněné e-mailové a SMS zprávy přímo souvisely s později provedeným podvodným hovorem a s případem fiktivního bankéře.

Cílem této v pořadí 6. otázky bylo tedy zjistit, jestli a jak často pachatelé před podvodným hovorem kontaktují své budoucí oběti.

U skutků bylo zjištěno, že

- v roce 2022 3 (4 %) oběti obdrželi e-mailové zprávy (2x) a SMS (1x). A u ostatních 64 (96 %) skutků nebylo těchto kontaktů zjištěno.
- v roce 2023 2 (3 %) oběti obdrželi e-mailovou zprávu (2x). A u ostatních 56 (97 %) skutků nebylo těchto kontaktů zjištěno.

Graf č. 6 – Byl proveden předběžný kontakt?



Zdroj: Vlastní zpracování

Celkem byl předběžný kontakt proveden u 5 (4 %) skutků. U 120 (96 %) skutků nebylo od obětí zjištěno tohoto jednání pachatelů.

Otázka č. 7: Kdo byl původcem prvního hovoru?

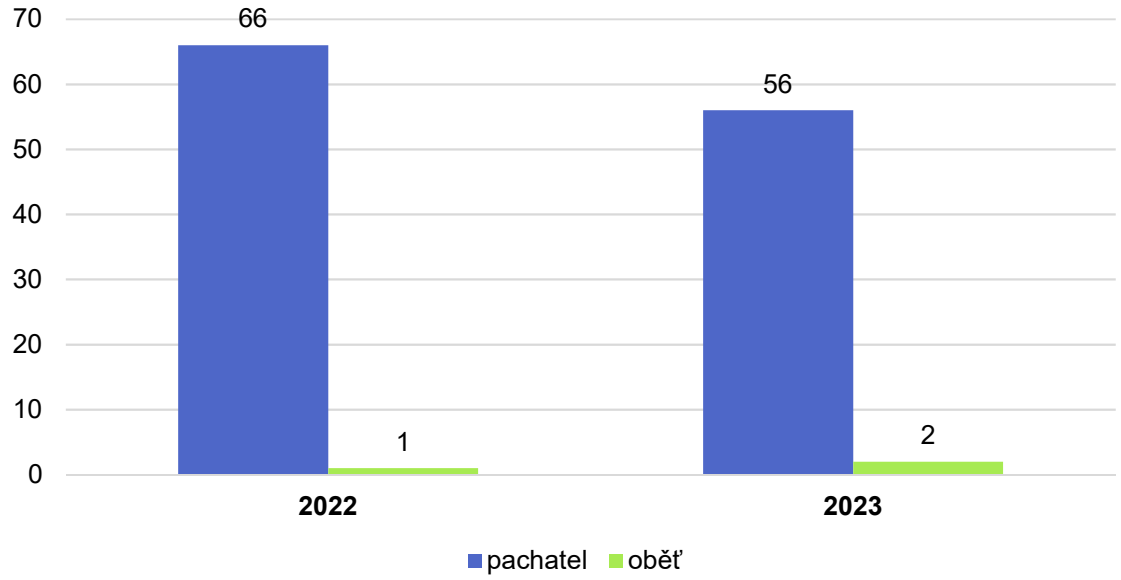
V rámci této jednoduché otázky bylo cílem zjistit, kdo první provedl hlasový hovor, tedy jestli pachatel, nebo sama oběť.

Tato otázka má návaznost na předchozí a do určité míry odráží i její výsledky.

První hlasový kontakt provedl

- v roce 2022 u 66 (99 %) skutků sám pachatel a u 1 (1 %) skutku to byla oběť, která reagovala na SMS zprávu;
- v roce 2023 u 56 (97 %) skutků opět sám pachatel a u 2 (3 %) skutků to byli oběti, které obě reagovali na e-mailové zprávy.

Graf č. 7 – Kdo byl původcem prvního hovoru?



Zdroj: Vlastní zpracování

Celkové výsledky jsou takové, že u 122 (98 %) skutků první hovor provedl pachatel. A u 3 (2 %) skutků to byla oběť.

Otázka č. 8: V jaké denní době pachatel provedl první hovor?

Smyslem této otázky bylo zjistit, v jakém čase pachatelé svým obětím nejčastěji volají. Stanovené možnosti použité pro odpovědi na tuto otázku odrážejí běžné rozdělení denní doby, tj.:

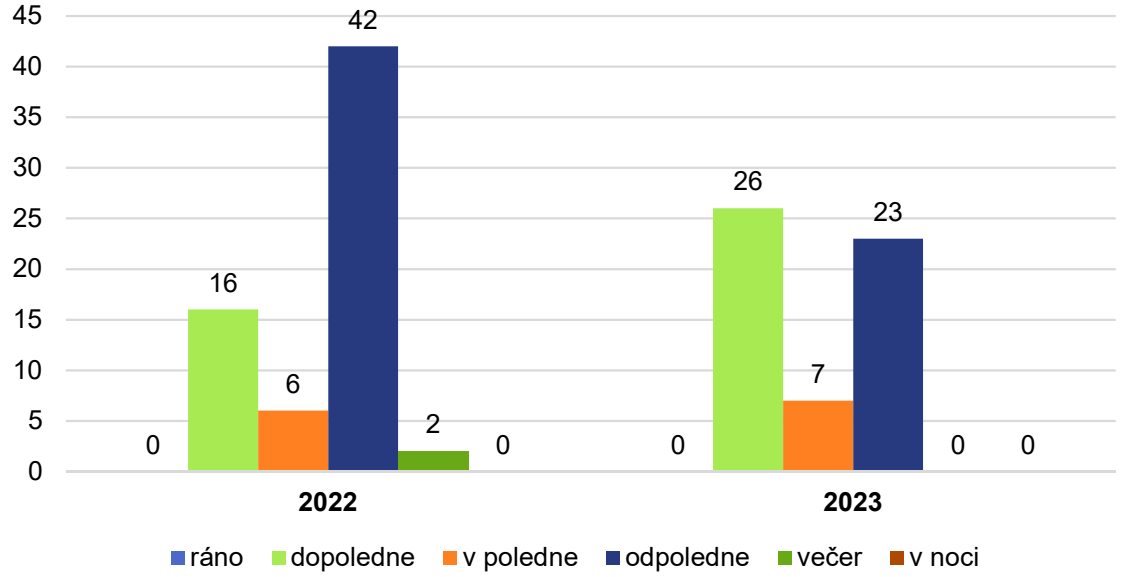
- ráno (6-8 hodin),
- dopoledne (8-12 hodin),
- v poledne (12 hodina),
- odpoledne (12-18 hodin),
- večer (18-22 hodin),
- noc (22-6 hodin).

Odpověď je z 66 skutků z roku 2022 a z 56 skutků z roku 2023, což odpovídá výsledkům z předchozí otázky (dohromady 122).

Pachatelé uskutečnili první hovor

- v roce 2022: 16x dopoledne (24 %), 6x v poledne (9 %), 42x odpoledne (64 %) a 2x večer (3 %). Ráno a v noci nebyl proveden žádný hovor.
- V roce 2023: 26x dopoledne (46 %), 7x v poledne (13 %), 23x odpoledne (41 %). Večer, v noci a ráno nebyl proveden žádný hovor.

Graf č. 8 – V jaké denní době pachatel provedl první hovor?



Zdroj: Vlastní zpracování

Celkem bylo provedeno 42 (34 %) hovorů dopoledne, 13 (11 %) v poledne, 65 (53 %) odpoledne a 2 (2 %) večer. Ráno a v noci nebyl zaznamenán hovor.

Většina dopoledních hovorů byla blíže k poledni a také nemalá část odpoledních. Další poměrně velká část odpoledních hovorů byla provedena okolo 15 hodiny.

Podvody fiktivních bankéřů vyžadují zpravidla čas, a to i několik hodin (viz otázky č. 10 a 61, str. 32 a 73 této práce). Pro některé podvodné variace jsou nutné otevřené banky a dostupnost dalších služeb. A tak hovory uskutečňují v takové době, aby plně využili použitou legendu, postup a usnadnili si podmínky k získání peněz.

Otázka č. 9: Jaká byla četnost hovorů?

Odpovědí na tuto otázku bylo zjištěno, kolik celkem bylo provedeno hovorů mezi pachatelem a obětí.

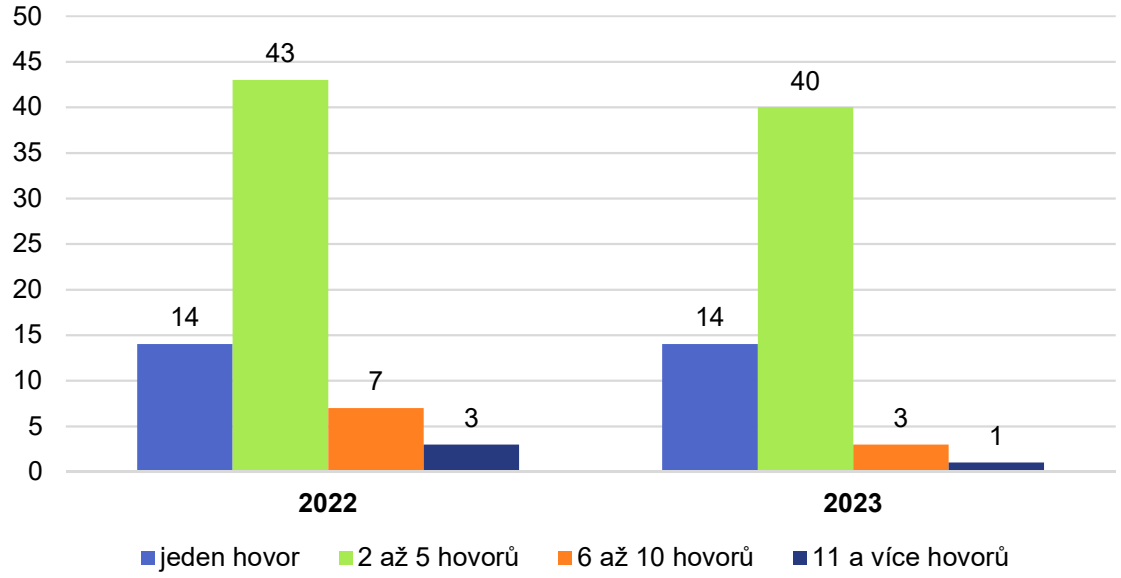
S ohledem na výsledky byly stanoveny skupiny, a to v těchto počtech:

- 1 hovor,
- 2 až 5 hovorů,
- 6 až 10 hovorů,
- 11 a více hovorů.

Četnost hovorů byla následující

- v roce 2022: 14x jeden hovor (21 %), 43x 2-5 (64 %), 7x 6-10 (11 %) a 3x 11 a více hovorů (4 %);
- v roce 2023: 14x jeden hovor (24 %), 40x 2-5 (69 %), 3x 6-10 (5 %) a 1x 11 a více hovorů (2 %).

Graf č. 9 – Jaká byla četnost hovorů?



Zdroj: Vlastní zpracování

Celková četnost hovorů byla: 28x jeden hovor (22 %), 83x 2-5 (67 %), 10x 6-10 (8 %) a 4x 11 a více hovorů (3 %).

Pachatelé zpravidla mají snahu provést méně hovorů, které ale jsou dlouhotrvající. Po prvotním navolání následuje telefonát, ve kterém už probíhá systematická manipulace. Pro pachatele je nežádoucí, aby oběť hovor ukončila a zjišťovala informace, provedla ověření pravosti hovorů nebo jiných skutečnosti. Více hovorů se zpravidla provede v případě, že cílem pachatele je peníze vložit do automatů na nákup kryptoměn, nebo vyšlou oběť do banky pro převzetí bankovní půjčky či jen pro výběr peněz z účtu.

Je možné setkat se také s tím, že pachatelé důrazně žádají, aby oběť při přerušení hovoru s nikým dalším nehovořila a nikomu nevěřila. Utváří k tomu i část legendy, ve které naznačují, že pachatelé mají kontakty v bance a ti mohou zmařit záchranu peněz.

Otázka č. 10: Jaká byla celková délka hovorů?

V rámci odpovědi na tuto otázku jsem se snažil stanovit, jaká byla celková doba hovoru mezi pachatelem a obětí. Respektive jak dlouho dohromady trvala veškerá hlasová komunikace, i když bylo více telekomunikačních spojení. Jedná se o čistý čas vzájemných hovorů.

V rámci této otázky není tedy řešeno, po jakou dobu pachatel udržoval navázaný kontakt s obětí (=celková doba od prvního hovoru až do doby posledního hovoru). To bylo řešeno v rámci otázky č. 61 (časové souvislosti).

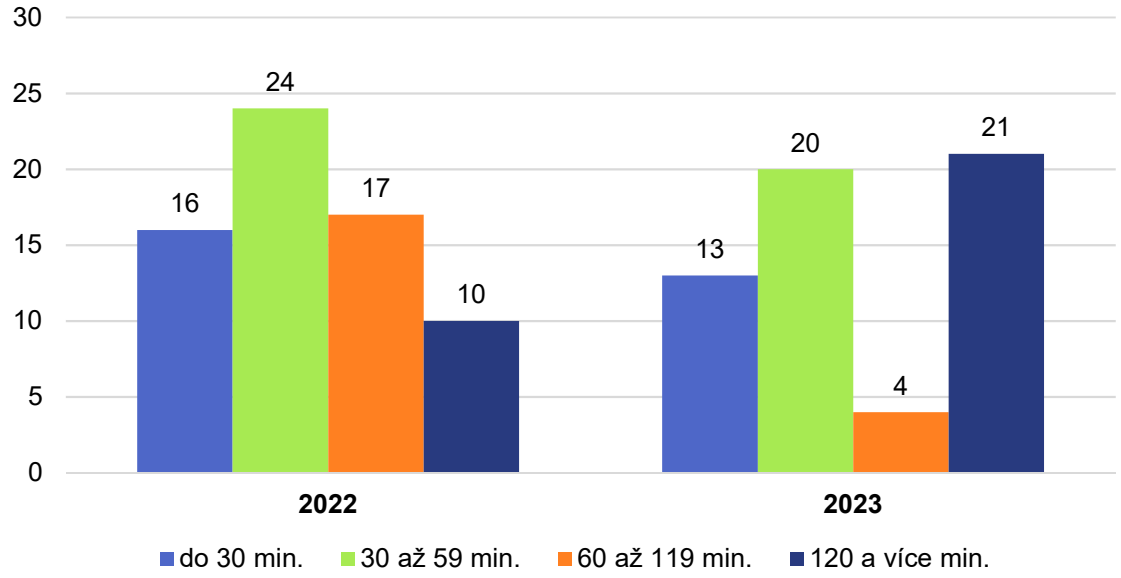
Rovněž i zde byly pro přehlednost stanoveny skupiny, a to v těchto časech:

- do 30 minut,
- 30 až 59 minut,
- 60 až 119 minut,
- 120 a více minut hovoru.

Délka hovorů byla následující

- v roce 2022: 16x do 30 minut (24 %), 24x mezi 30-59 (36 %), 17x mezi 60-119 (25 %) a 10x 120 a více minut (15 %);
- v roce 2023: 13x do 30 minut (22 %), 20x mezi 30-59 (35 %), 4x mezi 60-119 (7 %) a 21x 120 a více minut (36 %).

Graf č. 10 – Jaká byla celková délka hovorů?



Zdroj: Vlastní zpracování

Celkem byla délka hovorů následující: 29x do 30 minut (23 %), 44x mezi 30-59 (35 %), 21x mezi 60-119 (17 %) a 31x 120 a více minut (25 %).

V 5 případech bylo zjištěno, že vzájemné hovory trvaly až 5 hodin. Ve všech těchto skutcích se jednalo o oběti důchodového věku a jednalo se o variantu fiktivního bankéře, kde peníze byly vkládány do automatů na nákup kryptoměn.

Z výsledků je patrné, že délka hovorů není pachatelům na škodu, a to pokud oběť zcela podlehla fikci, plní pokyny pachatele a vše směřuje k získání peněz.

Otázka č. 11: Jak často byl využíván další komunikační kanál?

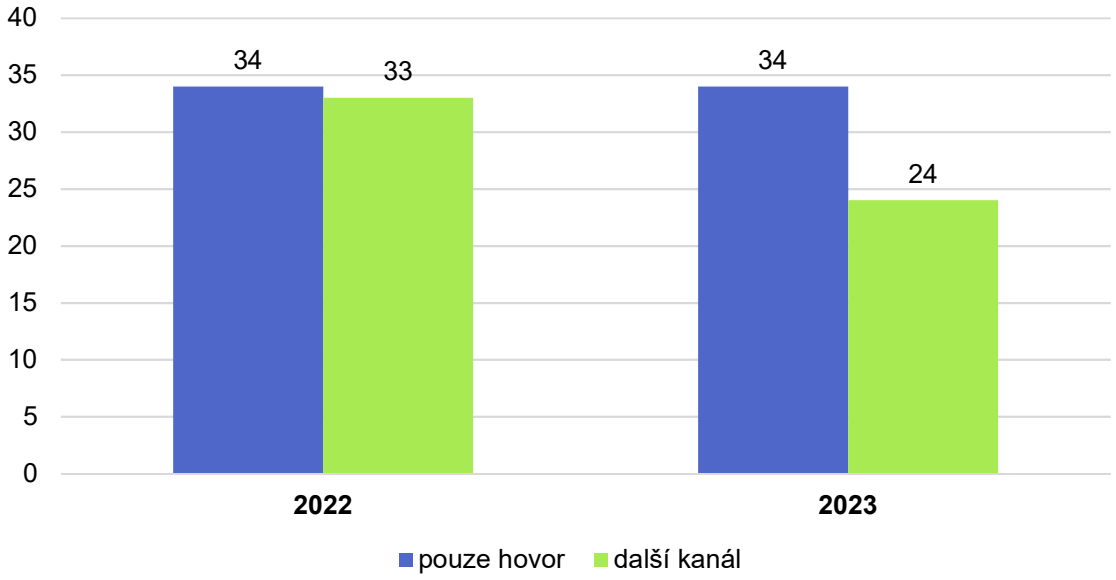
Pachatelé fiktivních bankéřů vyjma hovorů využívají i další komunikační služby. Jedná se především o e-mailové zprávy a služby typu instant messaging (aplikace pro okamžité zasílání zpráv a multimédií). Otázkou bylo, jak často vedle hlasových hovorů tyto služby využívají.

Další komunikační kanály byly využity

- v roce 2022 u 33 z 67 (49 %) skutků a u ostatních, tj. 34 (51 %) skutků, byl proveden jen hlasový hovor,

- v roce 2023 u 24 z 58 (41 %) skutků a u ostatních, tj. 34 (59 %) skutků, byl proveden jen hlasový hovor.

Graf č. 11 – Jak často byl využíván další komunikační kanál?



Zdroj: Vlastní zpracování

Celkem bylo u 57 (46 %) skutků využito dalších komunikačních služeb a u 68 (54 %) nikoliv.

Pachatelé prostřednictvím e-mailů a komunikačních aplikací zasílají obětem dokumenty k podpoření fikce, čísla bankovních účtů pro zaslání peněz nebo QR kódy obsahující kryptoměnové adresy. Obecně služby typu instant messaging umožnují i hlasové hovory. Šetřením bylo zjištěno, že je-li to nutné i tuto funkci pachatelé využívají.

Otázka č. 12: Jak často bylo využito maskování kontaktu?

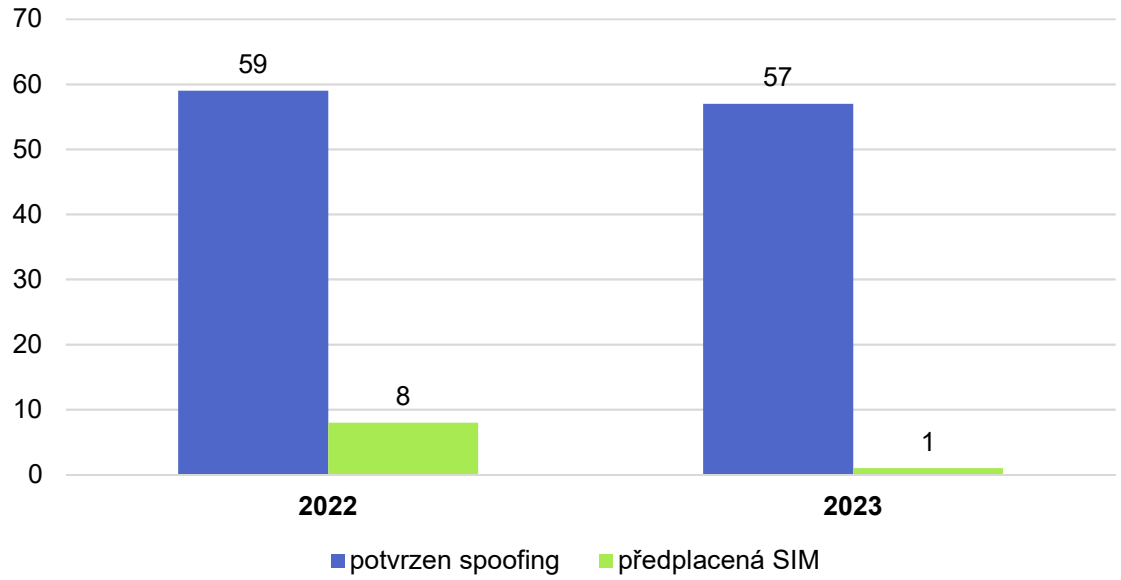
Pachatelé případů fiktivních bankéřů běžně využívají spoofingu a cílem této otázky bylo zjistit reálnou četnost.

V rámci této otázky nebylo vzato jako maskování využití předplacené (anonymní) SIM karty použité v koncovém zařízení. Předplacenou SIM není možné brát jako maskování, i když není znám její uživatel.

Spoofing byl zjištěn

- v roce 2022 u 59 (88 %) skutků a u 8 (12 %) skutků nikoliv (využito předplacené SIM),
- v roce 2023 u 57 (98 %) skutků a u 1 (2 %) skutku nikoliv (také využito předplacené SIM).

Graf č. 12 – Jak často bylo využito maskování kontaktu?



Zdroj: Vlastní zpracování

Celkem byl spoofing využit u 116 ze 125 skutků (93 %).

Skutečnost, že pachatelé případů fiktivních bankéřů využívají překrytého volání, apriori neznamená, že se vyhýbají volání prostřednictvím SIM. Předplacené SIM používají např. pro datová připojení k síti Internet a pro instant messaging.

Otázka č. 13: Odpovídal maskovaný kontakt reálnému?

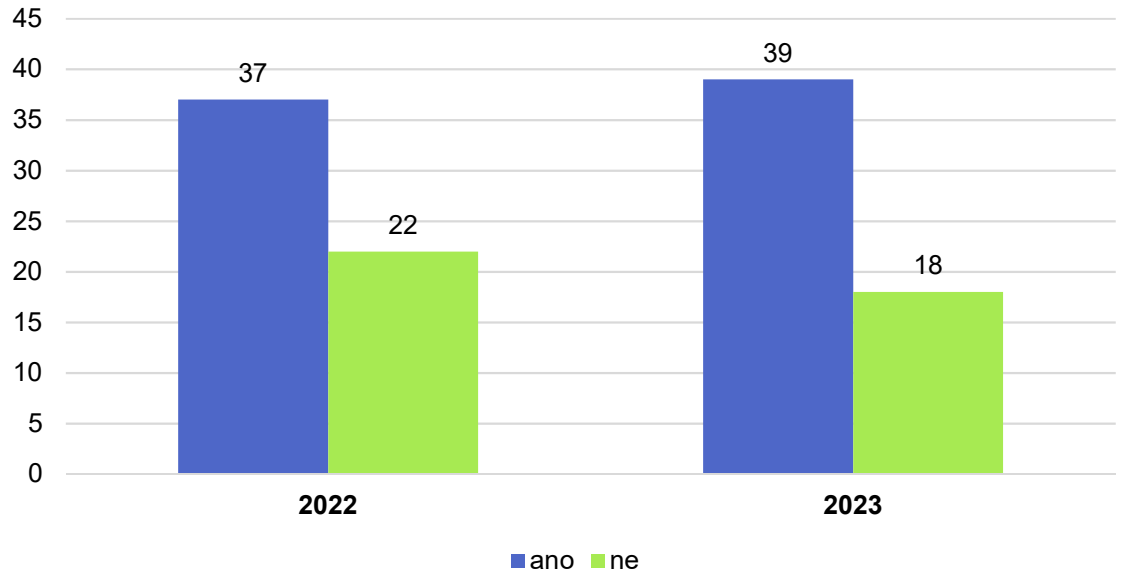
Smyslem této navazující otázky k přechozí bylo stanovit, jak často maskovaný kontakt odpovídá telefonním číslům běžně používaných bankami a Policií České republiky.

Odpověď je z 59 skutků z roku 2022 a z 57 skutků z roku 2023, což odpovídá výsledkům z předchozí otázky (dohromady 116).

Maskovaný kontakt

- v roce 2022 odpovídal reálnému číslu 37x (63 %) a 22x (37 %) nikoliv,
- v roce 2023 odpovídal reálnému číslu 39x (68 %) a 18x (32 %) nikoliv.

Graf č. 13 – Odpovídal maskovaný kontakt reálnému?



Zdroj: Vlastní zpracování

Celkem odpovídalo číslo reálnému u 76 (66 %) skutků a neodpovídalo u 40 (34 %) skutků.

Použitá napodobená čísla nebo čísla přímo odpovídající kontaktům bank a Policii České republiky byly využity spíše u skutků, kde byla oběť české národnosti. U cizinců a skutků, kde nebylo využito podobnosti s reálným číslem, byla zpravidla využívána různá čísla začínající standardně 6 a 7, v běžném devítimístném formátu a s předvolbou +420.

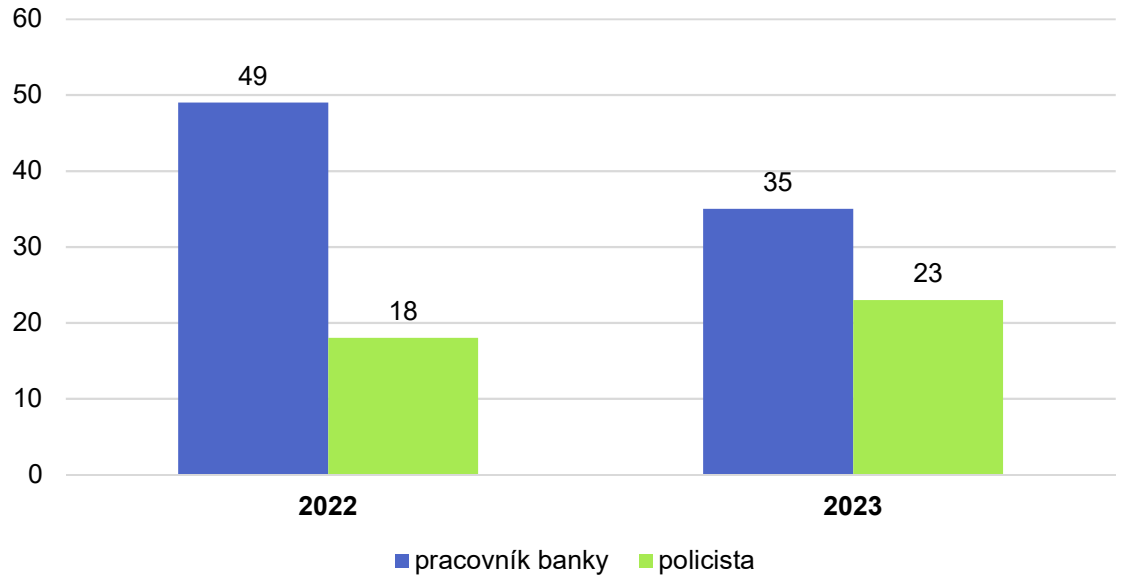
Otázka č. 14: V jaké roli pachatel vystupoval?

Pro potřeby této otázky byly role zobecněny jen na dvě, a to *pracovník banky* a *policista*. O roli pracovníka banky se jednalo, pokud se pachatel představil, např. jako osobní bankéř, bezpečnostní pracovník banky, vedoucí pobočky, bankéř České národní banky, bankovní asistent apod. V případě role policisty byla využívána nejčastěji podoba kriminalista a vyšetřovatel.

Pachatel se představil

- v roce 2022 jako pracovník banky u 49 (73 %) skutků a jako policista u 18 (27 %) skutků,
- v roce 2023 jako pracovník banky u 35 (60 %) skutků a jako policista u 23 (40 %) skutků.

Graf č. 14 – V jaké roli pachatel vystupoval?



Zdroj: Vlastní zpracování

Celkem byla role pracovníka banky využita 84x (67 %) a 41x (33 %) policisty.

Role policistů, jako iniciátora podvodného hovoru, byla využívána spíše u případů, kde oběť nebyla české národnosti.

Otázka č. 15: Jaká legenda byla použita?

Pachatelé podvodů fiktivních bankéřů využívají různé legendy, které bylo možno uspořádat do těchto situací:

- neoprávněné transakce nebo platby kartou,
- napadení bankovního účtu hackery,
- podezřelé akce v internetovém bankovnictví,
- neoprávněná žádost o úvěr,
- ověření služby banky a informace k půjčce,

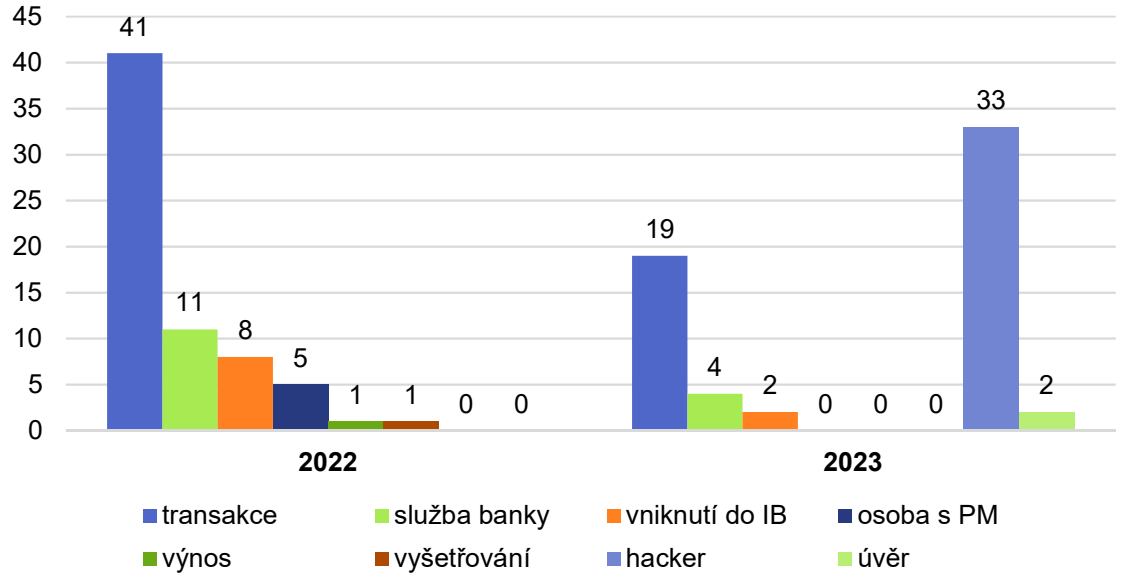
- podezřelá osoba v bance využívající plnou moc,
- zaslání výnosu z investic,
- policejní vyšetřování ve spojení s účtem oběti.

Uvedený soupis legend není konečný. S těmito jsem se ale setkal při provedení tohoto terénního šetření. Použití kombinace legend není vyloučeno.

Použitá legenda

- v roce 2022: 41x neoprávněná transakce nebo platba kartou (61 %), 11x ověření bankovní služby (16 %), 8x vniknutí do internetového bankovnictví (12 %), 5x osoba v bance s plnou mocí (7 %), 1x výnos z investic (2 %) a 1x vyšetřování policie (2 %);
- v roce 2023: 33x napadení účtu hackery (57 %), 19x neoprávněná transakce nebo platba kartou (33 %), 4x ověření bankovní služby (7 %) a 2x neoprávněná žádost o úvěr (3 %).

Graf č. 15 – Jaká legenda byla použita?



Zdroj: Vlastní zpracování

Celkem bylo využito: 60x neoprávněná transakce nebo platba kartou (48 %), 33x napadení účtu hackery (26 %), 15x ověření bankovní služby (12 %), 8x vniknutí do internetového bankovnictví (6 %), 5x osoba v bance s plnou mocí

(4 %), 2x neoprávněná žádost o úvěr (2 %), 1x výnos z investic (1 %) a 1x vyšetřování policie (1 %).

Použitá legenda je dále podporována požadavky pachatelů, např. apel, aby oběť po domnělé záchraně peněz kvůli odstranění digitálního viru uvedla svůj přístroj do továrního natavení. Těmito požadavky podporují věrohodnost situace a oběti přicházejí o informace, které pak mohly být prospěšné při vyšetřování.

Otázka č. 16: Bylo využito pomoci spolupachatele?

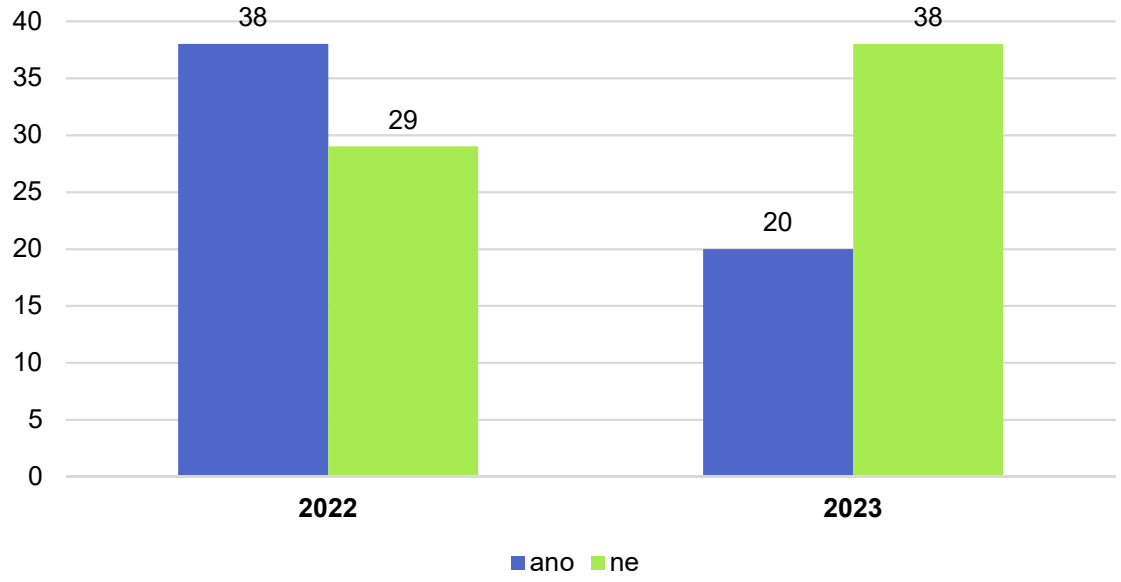
Existence spolupachatele je využívána podle potřeby a do určité míry je ovlivněna použitou legendou. Spolupachatel především vypomáhá utvrzovat pravdivost legendy a s manipulací oběti. Není vyloučeno, že spolupachatel je de facto osoba, která provedla navolání a následně je hovor předán osobě realizující fikci.

V rámci této otázky bylo tedy cílem zjistit, jak často byla využívána přítomnost spolupachatele.

Spolupachatel byl využit

- v roce 2022 u 38 z 67 (57 %) skutků,
- v roce 2023 u 20 z 58 (34 %) skutků.

Graf č. 16 – Bylo využito pomoci spolupachatele?



Zdroj: Vlastní zpracování

Celkem byl spolupachatel využit u 58 ze 125 (46 %) skutků.

Otázka č. 17: V jaké roli spolupachatel vystupoval?

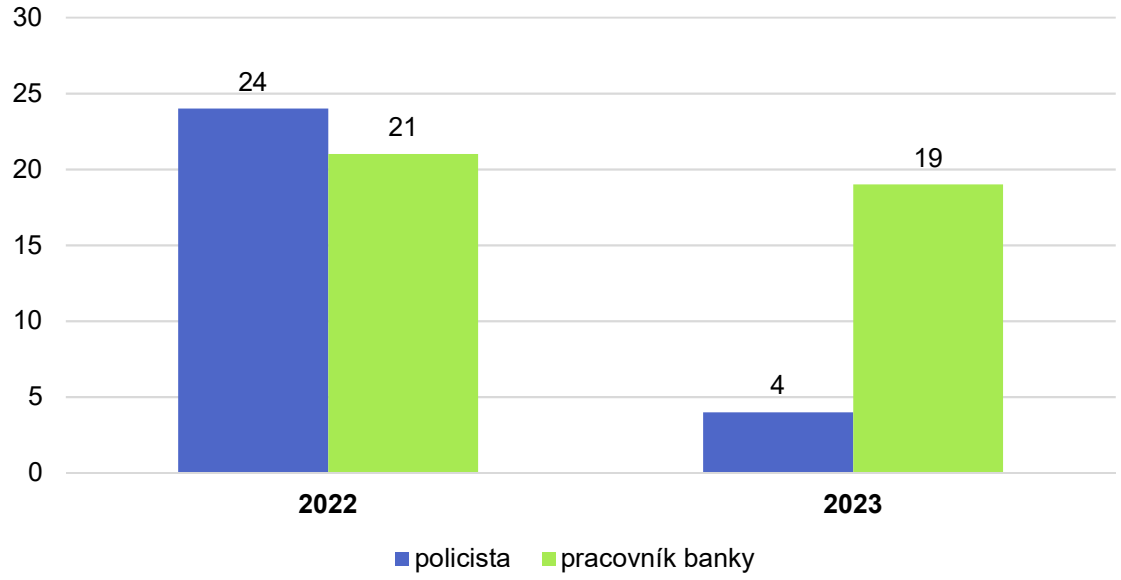
Tato navazující otázka na předchozí pracuje jen se skutky, u kterých bylo využito spolupachatele. V rámci 10 skutků bylo zjištěno, že bylo využito více než jednoho spolupachatele. Tito pak vystupovali v různých rolích. Role jsou de facto totožné s těmi, které byly představeny pod otázkou č. 14.

V roce 2022 bylo 45 a v roce 2023 bylo 23 spolupachatelů (dohromady 68).

Spolupachatelé vystupovali

- v roce 2022 21x jako pracovníci bank (47 %) a 24x jako policisté (53 %). U 7 případů bylo více spolupachatelů (zpravidla dva pracovníci banky a jeden policista).
- V roce 2023 19x jako pracovníci bank (83 %) a 4x jako policisté (17 %). U 3 případů bylo více spolupachatelů (opět dva pracovníci banky a jeden policista).

Graf č. 17 – V jaké roli spolupachatel vystupoval?



Zdroj: Vlastní zpracování

Celkem spolupachatelé vystupovali 40x jako pracovníci bank (59 %) a 28x jako policisté (41 %).

Role se zpravidla obracela. Pokud v úvodu první volal jako pracovník banky, tak druhý vystupoval jako policista a obráceně.

V případě využití více rolí pracovníků bank, tak obecně v rámci prvního hovoru je oběť vystrašena smyšlenou situací. Hovor je předán *expertnímu pracovníkovi banky*, který už buduje fikci a systematicky manipuluje s obětí. A vyžaduje-li to situace pro utvrzení fikce, je navíc proveden hovor s fiktivním policistou.

Otázka č. 18: Jakého rázu bylo komunikační vystupování pachatelů?

Odpovědí na tuto otázku se odchýlím od nastoleného standartu uveřejnění výsledků. Zjištění budou jen popisná.

Terénní šetření dostatečně prokázalo, že komunikační vystupování pachatelů je ze začátku zdvořilé a přiměřené k situaci. Pokud oběť jedná podle požadavku pachatele, tak se vystupování téměř nemění. V případě, že oběť začne projevovat opatrnost nebo odpor ke krokům žádaných pachatelem, dochází ke změně vystupování. A vyvine se až do verbální agrese, přičemž nátlak je podpořen vyhrožováním s různými důsledky z nespolupráce, které buďto vyvodí banka nebo policie.

Odmítnutí kroků ze strany oběti muže aktivovat jinou variantu předpřipraveného scénáře. Pachatel v roli bankéře vysvětlí důsledky a zatím pozastaví komunikaci s tím, že vše uvede policii. Následuje hovor fiktivního policisty, který se snaží oběti domluvit a vysvětluje nutnost spolupráce s bankéřem.

Systematicky zvyšující se nátlak s později gradujícím vyhrožováním jsou klíčové komunikační faktory těchto podvodů.

V situacích, ve kterých oběť nezaváhá, nepodlehne slovní agresi a razantně odmítne spolupráci už ze začátku, tak pachatelé ukončují veškerou komunikaci.

Otázka č. 19: Pokusil se pachatel přesvědčit oběť k půjčce?

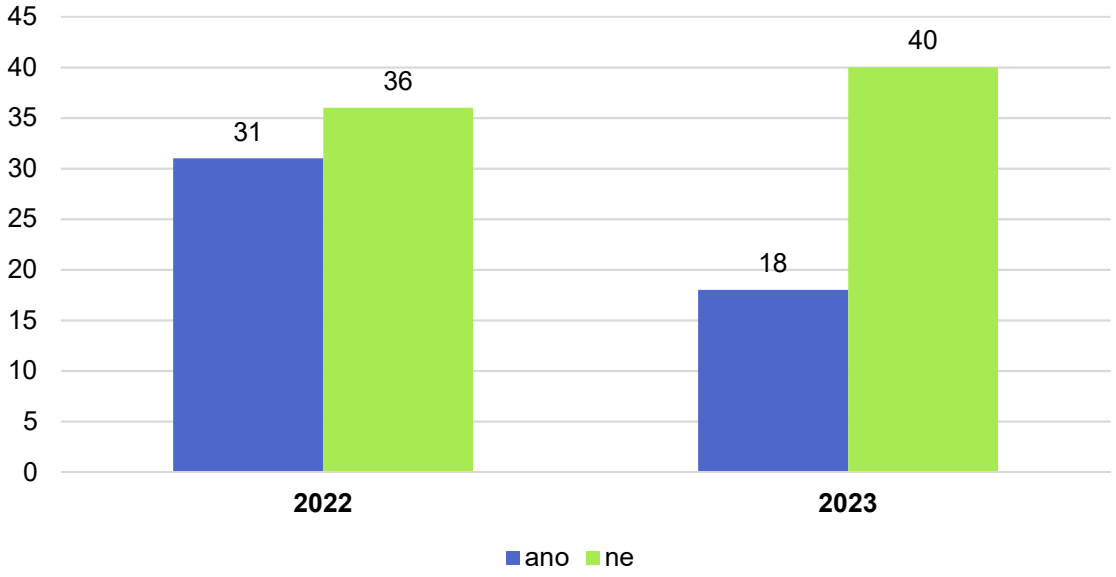
Z vyšetřovací praxe je známo mnoho případů, ve kterých si oběť na pokyn pachatele musela sjednat půjčku (úvěr). Pachatel to vysvětlil tím, že při napadení bankovního účtu neznámou osobou, ona sama půjčku nemůže vyžádat a dojde k zablokování této možnosti, a tím škoda nevnikne. Důvod proč pachatelé tak činí

je snadný. Navyšují tímto potencionální výnos, neboť peníze na účtu společně s penězi z půjčky pak oběti například předávají na určené účty nebo do automatů na nákup kryptoměn.

Pachatel požadoval, aby oběť získala maximální výši předschválené půjčky

- v roce 2022 u 31 z 67 (46 %) skutků,
- v roce 2023 u 18 z 58 (31 %) skutků.

Graf č. 18 – Pokusil se pachatel přesvědčit oběť k půjčce?



Zdroj: Vlastní zpracování

Celkem bylo zjištěno, že požadavek pachatele na vzetí půjčky byla provedena u 49 ze 125 (39 %) skutků.

Žádost o půjčku byla zpravidla provedena jen u případů s obětí české národnosti. A to z důvodů, že cizinci nemají tak často předschválené půjčky a navíc banky u cizinců obvykle provádějí kontrolní hovory, čímž by mohlo dojit k ohrožení fikce.

Otázka č. 20: Podařilo se pachateli získat citlivé údaje oběti?

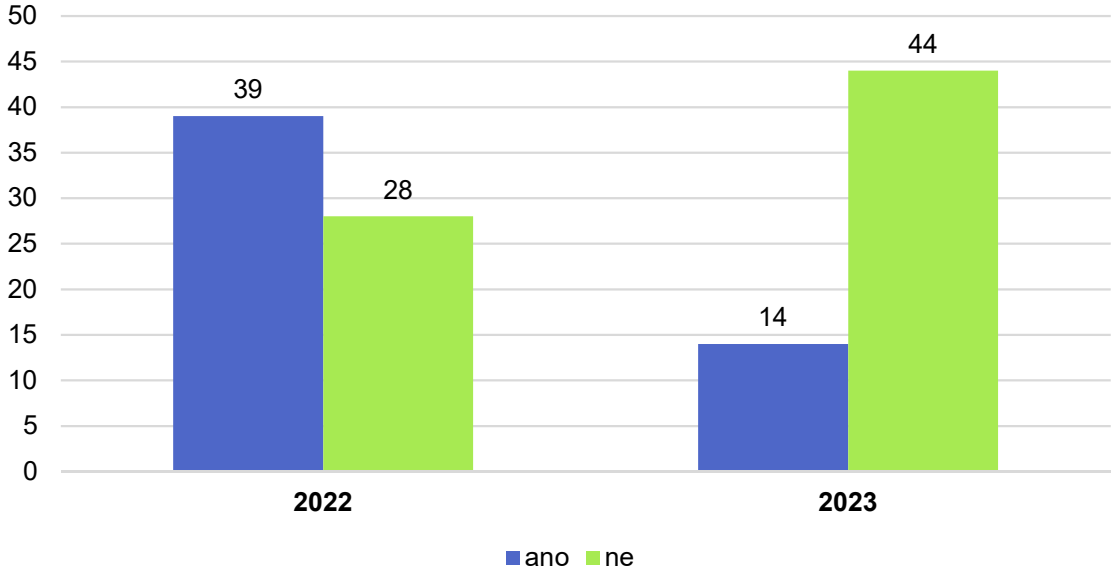
Hlavním cílem pachatelů je získání peněz z bankovních účtů. Vedlejším je získání dalších informací, které lze později využít.

V rámci této otázky bylo zjišťováno, jak úspěšní pachatelé byli při získávání osobních údajů o oběti (jména, datum narození, rodné číslo apod.) a dalších rozhodných bankovních informací, např. o platební kartě, přihlašovací informace do internetového bankovnictví atd.

Pachatel úspěšně získal citlivé údaje

- v roce 2022 u 39 z 67 (58 %) skutků,
- v roce 2023 u 14 z 58 (24 %) skutků.

Graf č. 19 – Podařilo se pachateli získat citlivé údaje oběti?



Zdroj: Vlastní zpracování

Celkem bylo zjištěno, že pachatelům se podařilo u 53 ze 125 (42 %) skutků získat citlivé údaje oběti.

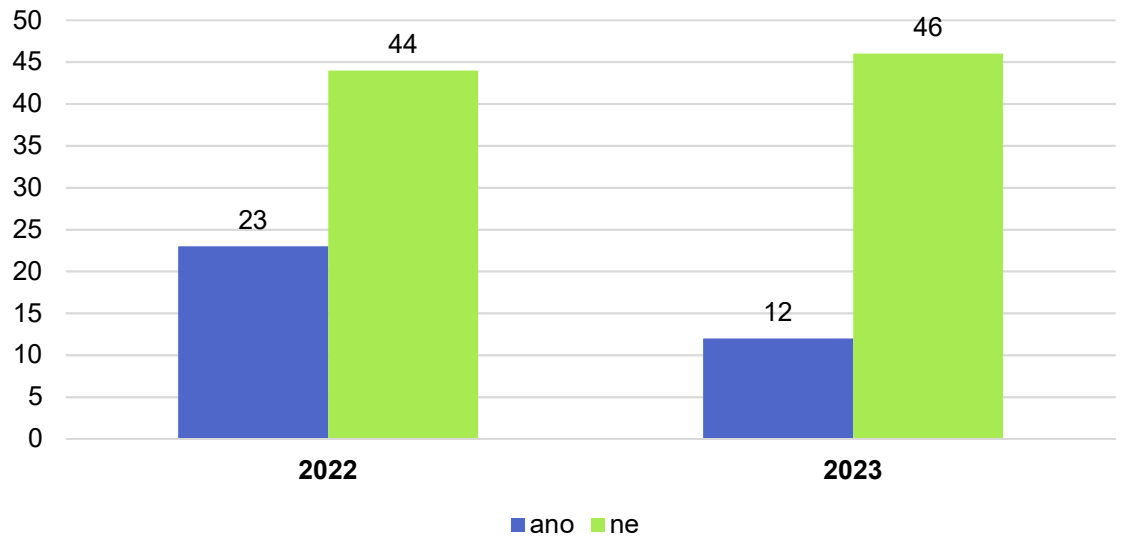
Otázka č. 21: Získal pachatel přístup do internetového bankovnictví oběti?

Získání přístupu do bankovnictví oběti umožní pachatelům provádět celou řadu neoprávněných akcí nebo cíleněji směřovat oběť a navyšovat zisk.

Pachatel úspěšně získal přístup do bankovnictví oběti

- v roce 2022 u 23 z 67 (34 %) skutků,
- v roce 2023 u 12 z 58 (21 %) skutků.

Graf č. 20 – Získal pachatel přístup do internetového bankovnictví oběti?



Zdroj: Vlastní zpracování

Celkem bylo zjištěno, že pachateli se podařilo u 35 ze 125 (28 %) skutků získat přístup do internetového bankovnictví oběti.

Otázka č. 22: Jakým způsobem pachatel získal přístup do bankovnictví?

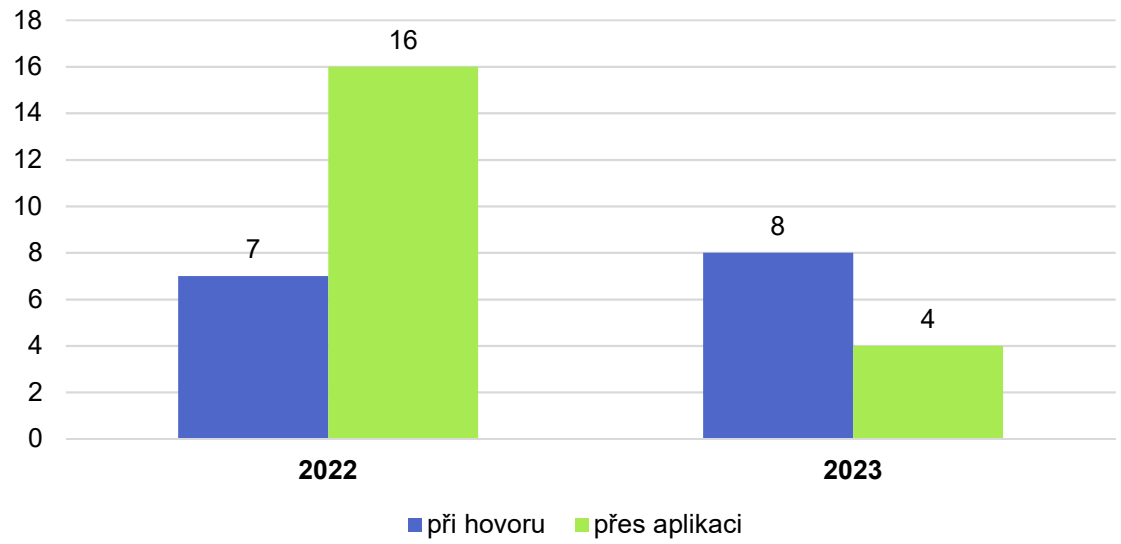
Smyslem této navazující otázky na předchozí bylo zjistit, jakým způsobem se pachateli podařilo získat přístup do internetového bankovnictví oběti.

Odpověď vychází z 23 skutků z roku 2022 a z 12 skutků z roku 2023, což odpovídá výsledkům z předchozí otázky (dohromady 35).

Pachatel získal přístup

- v roce 2022 u 7 (30 %) skutků tak, že oběť svá celá přihlašovací data uvedla při telefonním hovoru a u 16 (70 %) skutků to bylo prostřednictvím aplikace pro vzdálenou správu;
- v roce 2023 u 8 (67 %) skutků tak, že oběť svá celá přihlašovací data uvedla při telefonním hovoru a u 4 (33 %) skutků to bylo prostřednictvím aplikace pro vzdálenou správu.

Graf č. 21 – Jakým způsobem pachatel získal přístup do bankovnictví?



Zdroj: Vlastní zpracování

Celkem bylo zjištěno, že pachateli se podařilo získat přístup tak, že 15x je vyzradila oběť při hovoru (43 %) a 20x získal přístup po přesvědčení oběti k instalaci aplikace pro vzdálenou správu (57 %).

Aplikace pro vzdálenou správu se využívala jak u osobních počítačů a notebooků, tak i u mobilních telefonů. Využívány jsou běžně dostupné a bezplatné verze aplikací, které umožňují snadné používání bez nutnosti registrace.

Dále bylo zjištěno, že aplikace pro vzdálenou správu byla v roce 2022 využívána spíše u cizinců. V roce 2023 tomu už tak nebylo.

Otázka č. 23: Jakým způsobem pachatel získal peníze z účtu oběti?

Otázkou je řešena situace počátečního získání peněz ze zdrojového účtu oběti, a to bez ohledu na to, například jak jsou v případech řetězení účtů získávány až z navazujícího účtu (cíl výnosu bezprostředně po skutku je řešen až v dalších otázkách).

Odpověď vychází z 51 skutků z roku 2022 a ze 42 skutků z roku 2023 (dohromady 93), což odpovídá výsledkům z otázky č. 3 (tzn. dokonané skutky – škoda vznikla).

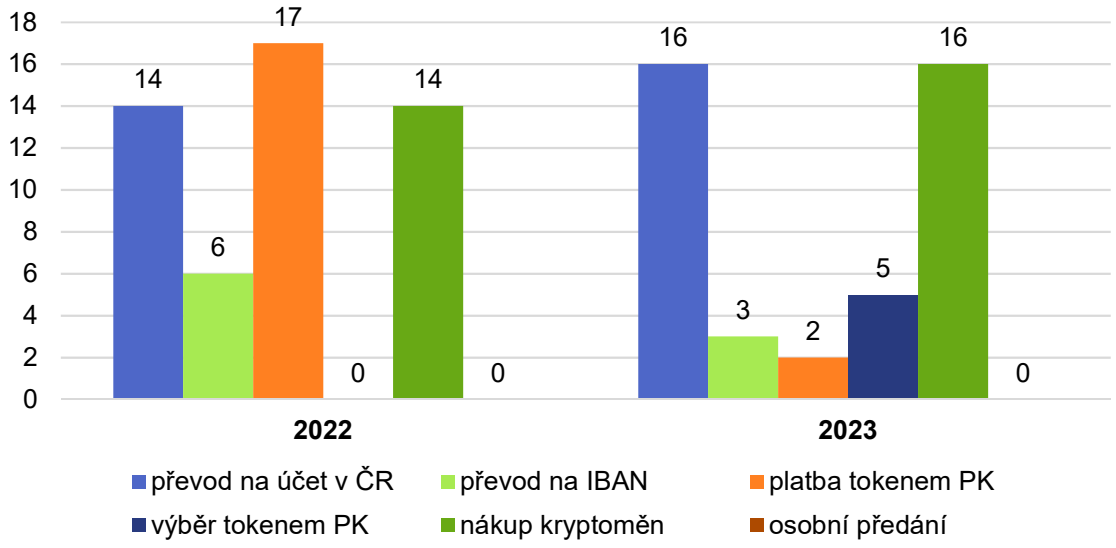
Pachatelé podvodů fiktivních bankéřů peníze z účtu získávají různými způsoby:

- převodem na účet v České republice,
- převodem na účet v zahraničí,
- platba pomocí tokenu platební karty,
- výběr peněz z bankomatu pomocí tokenu platební karty,
- obětí provedený výběr peněz z účtu a nákup kryptoměn,
- obětí provedený výběr peněz z účtu a předání prostředníkovi.

Peníze z účtů byly získány

- v roce 2022: 17x byla provedena platba pomocí tokenu platební karty (33 %), 14x byl obětí proveden výběr peněz z účtu a nákup kryptoměn (28 %), 14x byl proveden převod na účet v ČR (28 %) a 6x byl proveden převod na účet v zahraničí (11 %);
- v roce 2023: 16x byl proveden převod na účet v ČR (38 %), 16x byl obětí proveden výběr peněz z účtu a nákup kryptoměn (38 %), 5x byl proveden výběr peněz z bankomatu pomocí tokenu platební karty (12 %), 3x byl proveden převod na účet v zahraničí (7 %) a 2x byla provedena platba pomocí tokenu platební karty (5 %).

Graf č. 22 – Jakým způsobem pachatel získal peníze z účtu oběti?



Zdroj: Vlastní zpracování

Celkem bylo zjištěno, že nejčastěji bylo využito převodu na účet v ČR a obětí provedený výběr peněz z účtu a nákup kryptoměn, tj. oba způsoby 30x (2x 32 %). Dále u 19 (21 %) skutků byla provedena platba pomocí tokenu platební karty. U 9 (10 %) byl proveden převod na účet v zahraničí. A u 5 (5 %) výběr peněz z bankomatu pomocí tokenu platební karty.

Převody peněz na české účty jsou zpravidla provedeny pro potřeby řetězení účtů, které je využíváno ze dvou důvodů. Jednak pachatel kumuluje peníze na jednom ze zpřístupněných účtů, třeba i z jiného podvodu, odkud jsou následně odčerpány. A jednak pro případné pokračování v dalším útoku, ve kterém je využito převodu k dokreslení použité legendy u další oběti (zde se může jednat o spear vishing). V obou situacích se v podstatě jedná o mezikrok a peníze jsou z následných účtů použity k nákupu kryptoměn. Použité zahraniční účty jsou zpravidla obchodní účty společností, které se věnují obchodování s kryptoměnou. Není vyloučeno, že se jedná o osobní účty cizinců a v tomto případě je situace obdobná k českému účtu. Anebo se jedná o účty založené na zneužité nebo fiktivní totožnosti.

Platba kartou je běžně provedena pomocí zahraniční platební brány a směřuje k zahraničnímu obchodníkovi, přičemž nejčastěji je to opět směnárna kryptoměn. Můžeme se setkat i s tím, že platba byla použita k nákupu v e-shopu. Výběr peněz přes bankomat pomocí tokenu platební karty je proveden v případě, že pachatel sám (pokud měl zajištěn přístup do bankovnictví) nebo ve spolupráci s obětí získal token platební karty. Výběry jsou následně provedeny z běžných bankomatů.

Často využívaný způsob získání peněz přes oběť, která je sama vloží do automatu na nákup kryptoměn je velmi zvláštní. V podstatě oběti jsou fatálně pod vlivem pachatele, zcela plní veškeré jeho pokyny, a ačkoliv peníze mají po výběru u sebe, tedy v bezpečí, jsou schopné je vložit do automatu, jehož jediný účel je nákup kryptoměn.

Způsob získání peněz tím, že oběť na pokyn pachatele vybere peníze z banky a následně je fyzicky předá prostředníkovi (na ulici poblíž banky), není tak častý a patří mezi zvláštní způsoby po celkovém zmanipulování, avšak je pro budoucí vyšetřování velmi důležitý. De facto se jedná o jediný známý fyzický kontakt oběti se členem skupiny pachatelů.

Otázka č. 24: U kolika skutků byl výnos směřován do kryptoměn?

Tato otázka v podstatě navazuje na předchozí a odpověď vychází z 51 skutků z roku 2022 a z 37 skutků z roku 2023 (dohromady 88). Oproti předchozí otázce bylo odečteno 5 skutků, ve kterých byl proveden výběr peněz z bankomatu pomocí tokenu platební karty.

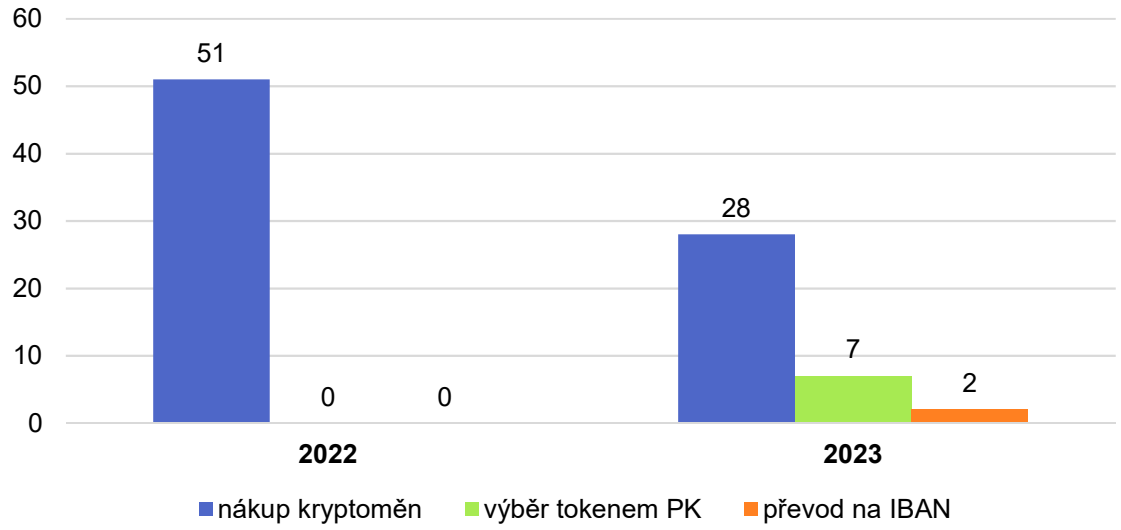
Nákup kryptoměn je možno považovat za maskování výnosu. V současné době je kryptoměna právně, ve smyslu speciality, neregulována.

Otázkou tedy je, jak často byla u podvodů fiktivních bankéřů využívána kryptoměna jako způsob počátečního ukrytí výnosu.

U skutků z roku 2022 bylo zjištěno, že všech 51 (100 %) výnosů končilo nákupem kryptoměn.

U skutků z roku 2023 bylo zjištěno, že 28 (76 %) výnosů končilo nákupem kryptoměn, 7 (19 %) výnosů bylo po kumulaci vybráno přes bankomat pomocí tokenu platební karty z navazujícího účtu (po převodu z účtu původní oběti) a 2 (5 %) výnosy směřovaly na bankovní účty v zahraničí, které byly založeny na zneužité identity.

Graf č. 23 – U kolika skutků byl výnos směřován do kryptoměn?



Zdroj: Vlastní zpracování

Celkem bylo zjištěno, že 79 z 88 (90 %) výnosů končilo v kryptoměně.

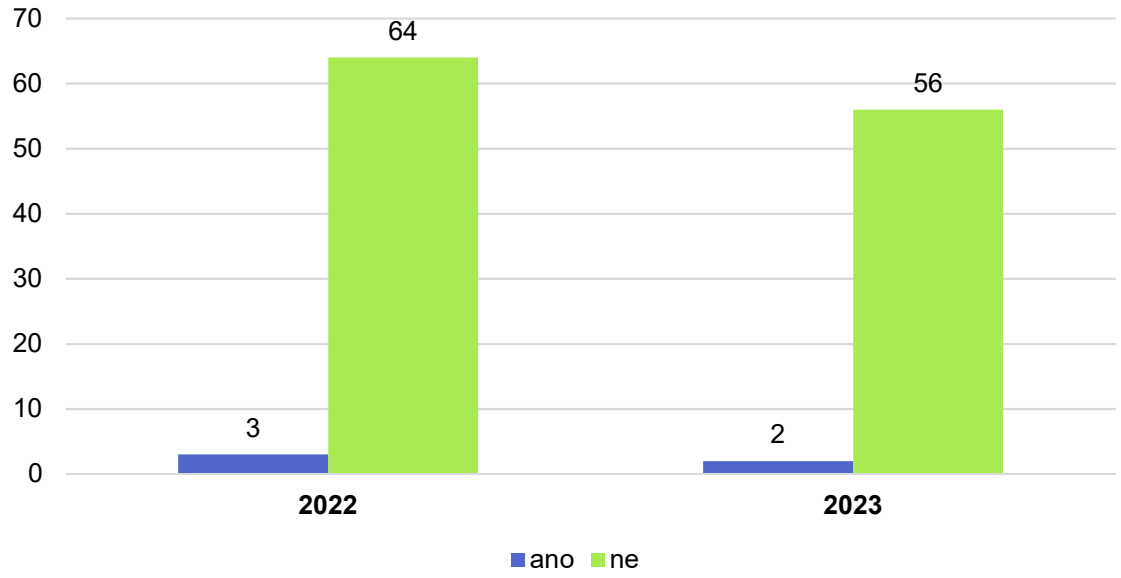
Otázka č. 25: Bylo využito dalších služeb?

Z vyšetřovací praxe jsou známy případy, ve kterých pachatel využívá běžně dostupných služeb, které sjednává pro oběť. Jedná se především o využití TAXI služby, kterou zajistí oběti nemající možnost, jak jinak si zjednat přepravu do místa nákupu kryptoměn.

Pachatel zajistil oběti službu

- v roce 2022 u 3 z 67 (5 %) skutků a jednalo se o TAXI službu.
- v roce 2023 u 2 z 58 (3 %) skutků a opět se jednalo o TAXI službu.

Graf č. 24 – Bylo využito dalších služeb?



Zdroj: Vlastní zpracování

Celkem pachatel zajistil oběti přepravu TAXI službou v 5 ze 125 (4 %) skutků.

Jiných služeb nebylo zjištěno.

Otázka č. 26: Pokračoval pachatel v komunikaci po získání peněz?

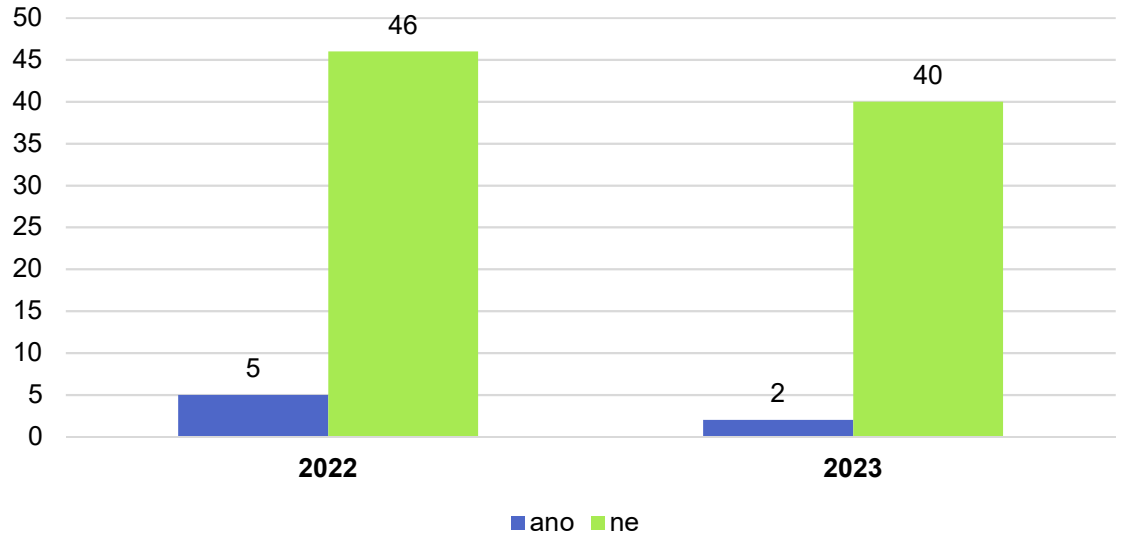
Pokračování v komunikaci po získání peněz bylo buďto za účelem oddálení oznámení, vydírání nebo získání jiné výhody tzn. pro získání dalších informací.

Odpověď opět vychází z 51 skutků z roku 2022 a ze 42 skutků z roku 2023 (dohromady 93) – tzn. dokonané skutky.

Pachatel pokračoval v komunikaci

- v roce 2022 u 5 z 51 (10 %) skutků. U 4 skutků to bylo za účelem získání další informací. A 1 komunikace vedla až k vydírání oběti.
- V roce 2023 u 2 ze 42 (5 %) skutků. U obou to bylo za účelem získání další informací.

Graf č. 25 – Pokračoval pachatel v komunikaci po získání peněz?



Zdroj: Vlastní zpracování

Celkem pachatel pokračoval v komunikaci u 7 z 93 (8 %) skutků.

Uvedené vydírání spočívalo v tom, že pachatel po získání peněz (výběrem z bankomatu pomocí tokenu platební karty) sám sebe v komunikaci před obětí demaskoval a požadoval další osobní informace (fotokopie dokladu totožnosti a řidičského průkazu). S tím, že po jejich obdržení peníze vrátí. Oběť fotokopie poskytla a pachatel své slovo nedodržel. Komunikace byla ukončena.

Otázka č. 27: U kolika skutků pachatel zajistil manipulací odstranění stop nebo jiných informací?

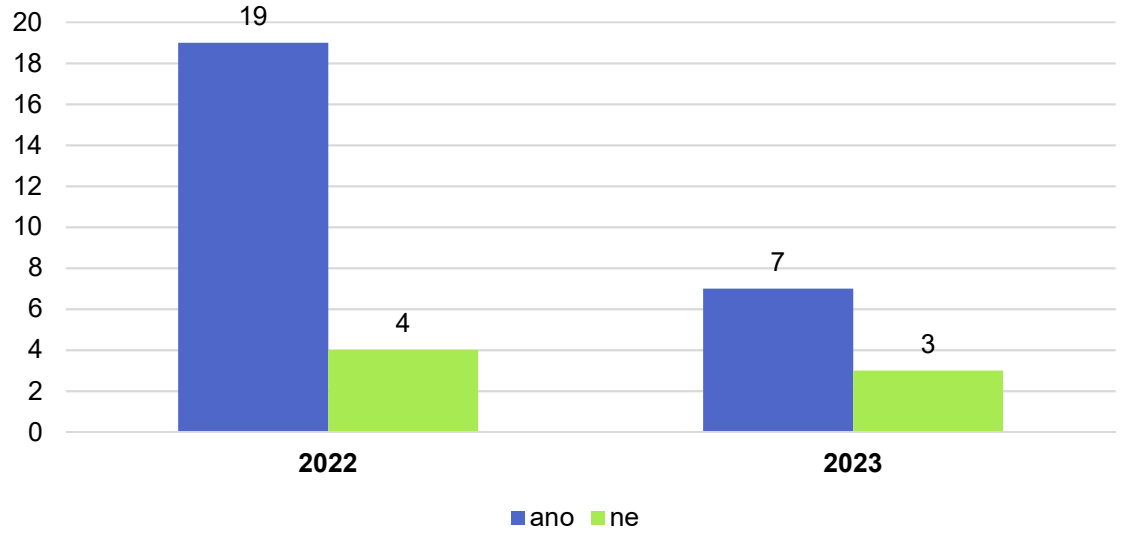
Jsou známi případy, ve kterých např. oběť nemohla poskytnout žádnou textovou komunikaci (provedenou přes aplikace instant messaging). A to z toho důvodu, že pachatel po získání peněz oběť nasměroval k tomu, že je nutné komunikaci odstranit. A oběť tak učinila.

Odpověď vychází z 33 skutků z roku 2022 a z 24 skutků z roku 2023 (dohromady 57), u kterých bylo zjištěno využití dalších komunikačních kanálů (viz odpověď na otázku č. 11).

Pachatel žádal odstranění komunikace

- v roce 2022 u 23 z 33 (70 %) skutků. U 19 to bylo úspěšné.
- V roce 2023 u 10 z 24 (42 %) skutků. A u 7 to bylo úspěšné.

Graf č. 26 – U kolika skutků pachatel zajistil manipulací odstranění stop nebo jiných informací?



Zdroj: Vlastní zpracování

Pachatel se snažil u obětí odstranit komunikaci celkem u 33 z 57 (58 %) skutků. A podařilo se mu úspěšně ovlivnit 26 z 33 (79 %) obětí, které odstranění provedli.

U všech 33 skutků byla snaha zaměřena na odstranění textové komunikace nebo jen zaslaných QR kódů pro načtení kryptoměnových adres. Cílem pachatele je co nejvíce zpomalit nebo znemožnit šetření.

Možno k tématu doplnit, že k neúmyslné likvidaci informací a stop se občas přidávají také skuteční pracovníci bank, kteří obvykle jako první hovoří s obětí. Pracovníci z bezpečnostních důvodů doporučují například z mobilního telefonu smazání aplikací, které pachatel vyžádal k nainstalování, a tím dojde ke ztrátě digitálních informací/stop.

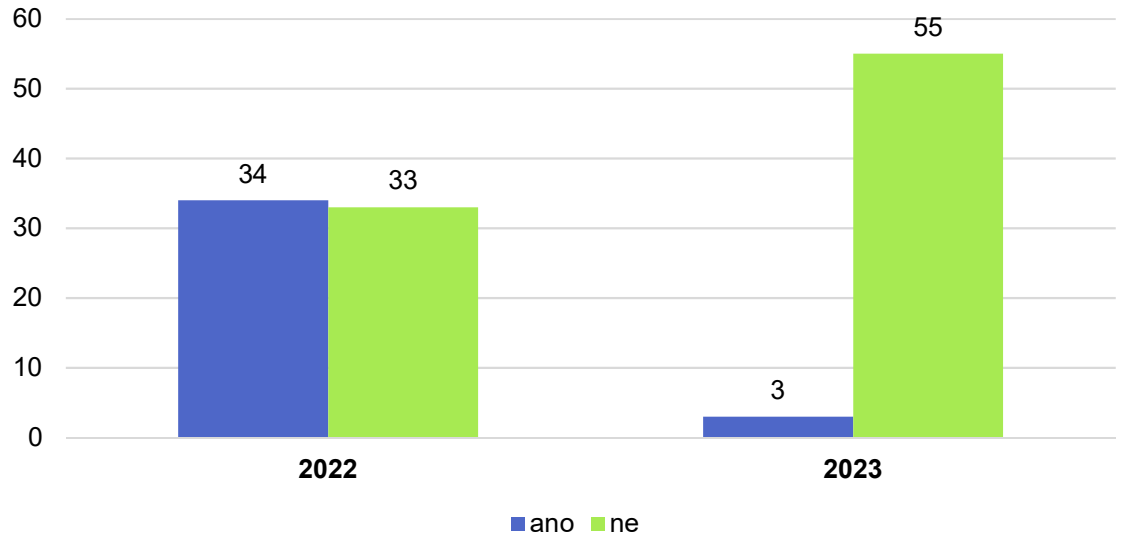
Otázka č. 28: Bylo zřejmé, že pachatel dopředu znal nějaké informace o oběti?

Smyslem této otázky bylo zjistit, jak často je využíváno cíleného útoku, tzv. spear vishingu.

Pachatel byl dopředu obeznámen s nějakým atributem oběti

- v roce 2022 u 34 z 67 (51 %) skutků,
- v roce 2023 u 3 z 58 (5 %) skutků.

Graf č. 27 – Bylo zřejmé, že pachatel dopředu znal nějaké informace o oběti?



Zdroj: Vlastní zpracování

Pachatel dopředu znal informace o oběti celkem u 37 ze 125 (30 %) skutků.

Zde je nutno uvést, že 32 z 34 skutků z roku 2022 a 1 z 3 skutků z roku 2023 byly zaměřeny na cizince. Všichni cizinci používali české telefonní číslo (+420). Je tedy patrné, že pachatel byl obeznámen s tím, že volá na české číslo osobě s určitou cizí národností. A proto jsou tyto případy zařazeny do cíleného útoku.

U zbylých, tedy 4 skutků z obou let, pachatel oběť oslovil správným celým jménem. Z toho u 2 skutků pachatel krom jména znal i datum narození.

Podvody fiktivních bankéřů jsou zpravidla dobře připravené. Existují náznaky, že obětem pachatelé mohli volat už dříve, třeba i půl roku předem, jako pracovníci bank s běžným marketingovým dotazem na klienty. A pokud pachatelé už znají

datum narození, během hovoru postačí položit dotaz na koncovku rodného čísla, např. z důvodu ověření klienta. Následně budou obeznámeni už s celým rodným číslem. Toho pak mohou využít k cílenému útoku a k přesvědčení oběti.

Otázka č. 29: V jakém okamžiku si oběť uvědomila, že se jedná o podvod?

Závěrečnou otázkou z druhé otázkové skupiny bylo zjišťováno, při jaké situaci nebo za jakých okolností si oběť uvědomila, že se jednalo o podvodný hovor.

Odpovědí na tuto otázku se opět odchýlím od nastoleného standartu uveřejnění výsledků. Zjištění budou jen popisná.

Pro potřeby odpovědi bylo nutné provést zobecnění situací, které oběti uváděli, přičemž zdrojové údaje byly velmi různorodé.

Podle výsledků bylo stanoveno, že oběti si uvědomili podvodná jednání:

- bezprostředně po provedení převodů,
- bezprostředně po vložení peněz do automatů pro nákup kryptoměn,
- před vložením peněz do automatů pro nákup kryptoměn (pokus),
- po skutku při hovoru se známým/členem rodiny,
- při hovoru s pachatelem (zpravidla pokus),
- při hovoru se skutečným pracovníkem banky (zpravidla po skutku),
- po skutku po obdržení zprávy z banky do bankovní aplikace,
- po obdržení SMS zprávy (zpravidla po skutku),
- dodatečně (typicky uvědoměním si podivnosti situace, např. po nedovolání na tel. čísla fiktivního bankéře).

Shora uvedeným výčtem nejsou vyloučeny další možnosti, avšak v rámci mnou provedeného šetření jiné nebyly zjištěny.

Stálo za povšimnutí, že banky zareagovaly na podvody fiktivních bankéřů a častěji identifikovaly „podivnější pohyby na účtech“, které se odchylovaly od běžného využívání klientem. Rovněž více kontaktovali své klienty a hovorem ověřovali důvody nestandartních transakcí.

III. vyšetřování

Otázka č. 30: Jak bylo zjištěno, že byl skutek spáchán?

Podstatou této úvodní otázky k vyšetřování bylo zjistit, jak se policejní orgán dozvěděl o tom, že byl spáchán trestný čin v souvislosti s podvodem fiktivního bankéře.

Po prostudování spisových materiálů, které byly vybrány pro toto terénní šetření, bylo zjištěno, že všechny skutky, tj. 125 z let 2022 a 2023, byly oznámeny obětmi.

Bez grafického vyobrazení.

Otázka č. 31: Jaké kriminalistické stopy byly zajištěny?

Jak je z otázky patrné, tak bylo zjišťováno, jaké klasické kriminalistické stopy byly zajištěny při prověřování případů.

Pro potřeby této otázky nebyly vzaty k úvaze paměťové stopy.

Kriminalistické stopy byly zajištěny

- v roce 2022 u 3 z 67 (5 %) skutků. Podařilo se zajistit audionahrávku hlasu pachatele (1/skutek). Tedy byly zajištěny 3 objekty pro audioexpertizu.
- V roce 2023 u 1 z 58 (2 %) skutků. I zde se podařilo zajistit audionahrávku hlasu pachatele. Tzn., byl zajištěn 1 objekt pro audioexpertizu.

Celkem se podařilo zajistit stopy u 4 ze 125 (3 %) skutků. Byly to 4 audionahrávky hlasu pachatele.

Jednalo se o spontánní nahrávky telefonátů, které pořídili sami oběti pomocí automatické aplikace v mobilním telefonu, kterou měli už předinstalovanou.

Bez grafického vyobrazení.

Otázka č. 32: Byly zajištěny jiné soudní důkazy?

Odpovědí na tuto otázku se opět odchýlím od nastoleného standartu uveřejnění výsledků. Zjištění budou opět jen popisná.

Ze spisových materiálu vyšlo najevo, že bylo zajištěno velké množství tzv. jiných soudních důkazů. Obecně se zejména jednalo:

- evidenční záznamy z telekomunikační činnosti (datový i telefonní provoz),
- evidenční záznamy o využití sítě Internet,
- evidenční záznamy k SIM a IMEI,
- evidenční záznamy k uživatelským účtům,
- bankovní záznamy a protokoly,
- textová komunikace,
- digitální písemnosti,
- jiné obrazové materiály zpracované digitálně (např. obrázek),
- kamerové záznamy.

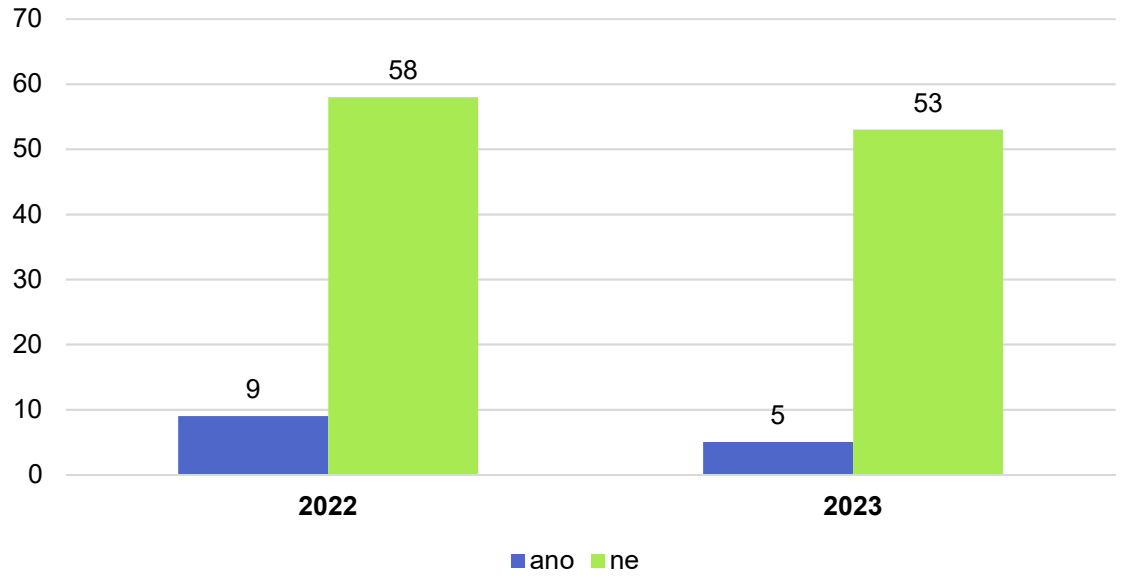
Otázka č. 33: Zaslechla oběť v pozadí hovorů nějaké zvuky?

V rámci této otázky bylo cílem zjistit, zda oběti v pozadí hovorů zaslechli další zvuky nebo hlasy, které mohou mít svůj účel.

Oběti zmiňovali v pozadí hovorů další zvuky/hlasy

- v roce 2022 u 9 z 67 (13 %) skutků,
- v roce 2023 u 5 z 58 (9 %) skutků.

Graf č. 28 – Zaslechla oběť v pozadí hovorů nějaké zvuky?



Zdroj: Vlastní zpracování

Celkem bylo zjištěno, že oběti zaslechli další zvuky/hlasy u 14 ze 125 (11 %) skutků.

Oběti shodně uvedli, že zaslechli zvuky/hlasy dalších hovorů, přičemž se mělo jednat o jiné osoby provádějící podobný hovor. Zmiňovali podobu tzv. call centra. Z vyšetřovací praxe je známo, že hovory v pozadí mohou skutečně být od dalších aktuálně realizovaných podvodů. Ovšem jsou i případy, při kterých zvuky v pozadí jsou uměle dotvořené k hovorům a utváří kulisu. A to právě pro vytvoření dojmu call centra.

Otázka č. 34: Jaká byla způsobená škoda v porovnání oběť/Kč?

Primárním cílem podvodů fiktivních bankéřů je získání peněz z bankovních účtů obětí, a proto jsem se v rámci této další otázky rozhodl zjistit, jaká je obvyklá škoda v poměru na jednu oběť.

Odpověď opět vychází z 51 skutků z roku 2022 a ze 42 skutků z roku 2023 (dohromady 93) – tzn. dokonané skutky.

Peněžní částky byly zaokrouhleny na tisíce.

Pro potřeby této otázky byly stanoveny skupiny peněžních škod:

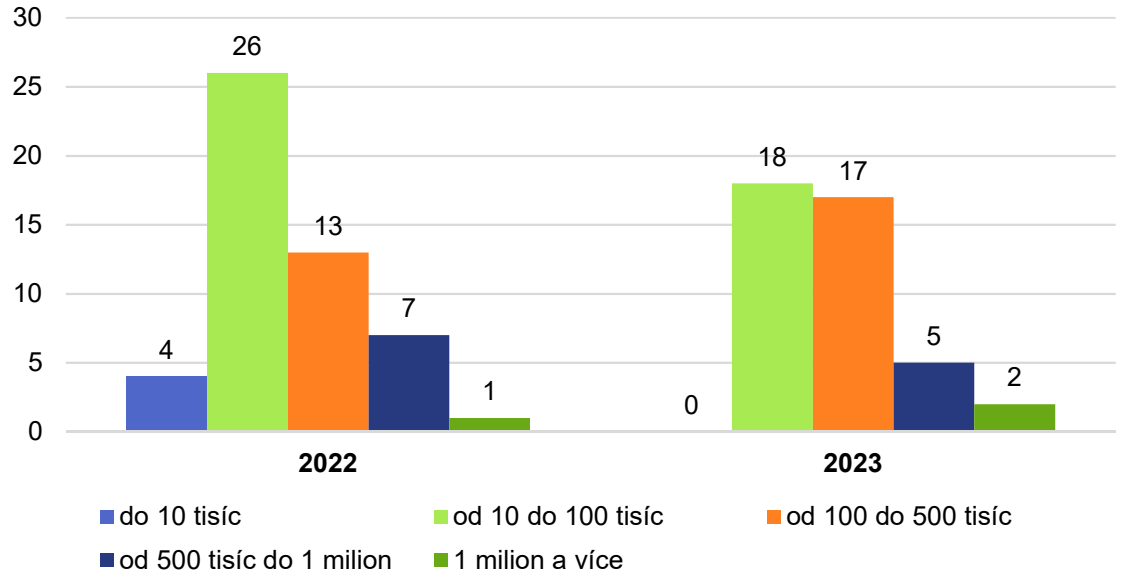
- do 9.999 Kč,
- od 10.000 do 99.999 Kč,
- od 100.000 do 499.999 Kč,
- od 500.000 do 999.999 Kč,
- 1.000.000 a více.

Pokud byl bankovní účet veden v cizí měně (nejčastěji EURO a USD), škoda byla přepočítána do Kč.

U skutků z roku 2022 bylo zjištěno, že u 4 (8 %) byla škoda do 9.999 Kč, u 26 (51 %) byla škoda do 99.999 Kč (z toho 19 skutků bylo blíže k horní hranici), u 13 (25 %) byla škoda do 499.999 Kč (z toho 8 skutků bylo blíže k dolní hranici a 5 skutků bylo blíže k horní hranici), u 7 (14 %) byla škoda do 999.999 Kč (všechny okolo 800.000 Kč) a u 1 (2 %) byla škoda přes 1.000.000 Kč (přesně 1.300.000 Kč).

U skutků z roku 2023 bylo zjištěno, že u 18 (43 %) byla škoda do 99.999 Kč (z toho 12 skutků bylo okolo 50.000 Kč), u 17 (40 %) byla škoda do 499.999 Kč (rovnoměrně v rámci této skupiny škod), u 5 (12 %) byla škoda do 999.999 Kč (z toho 4 skutky byly blíže k 500.000 Kč) a u 2 (5 %) byla škoda přes 1.000.000 Kč (okolo 1.050.000 a 1.150.000 Kč).

Graf č. 29 – Jaká byla způsobená škoda v porovnání oběť/Kč?



Zdroj: Vlastní zpracování

Celkově bylo zjištěno, že peněžní škoda v poměru na jednu oběť byla

- 4x do 10.000 Kč,
- 44x do 100.000 Kč,
- 30x do 500.000 Kč,
- 12 x do 1.000.000 Kč
- 3x přesahovala 1.000.000 Kč.

Celkem způsobená škoda u všech 93 skutků byla okolo 24 milionů Kč.

Průměrná škoda je okolo 250.000 Kč/oběť.

Otázka č. 35: Podařilo se zajistit výnos?

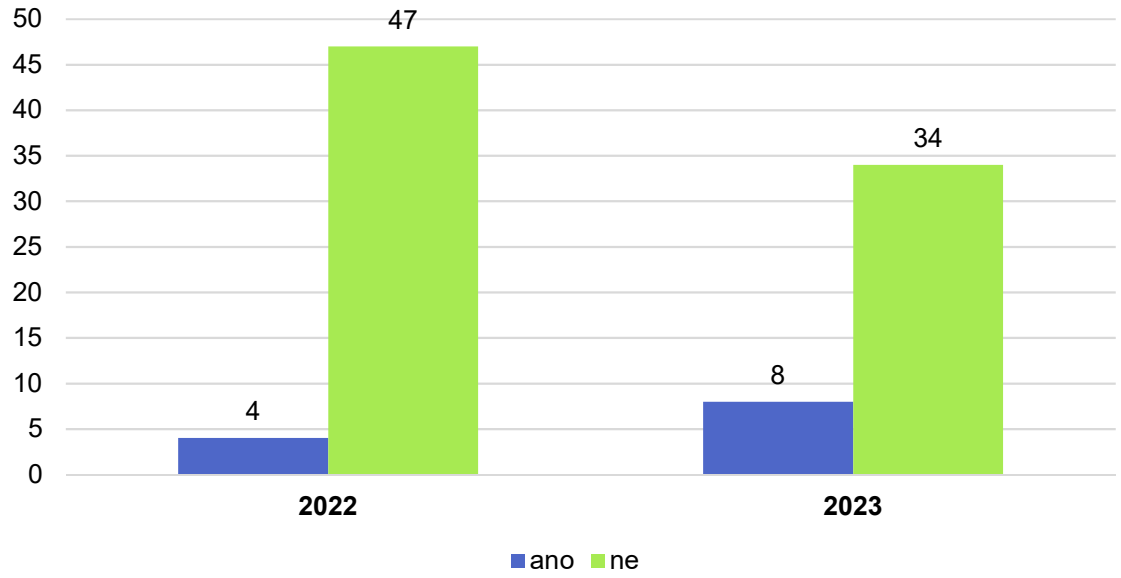
Touto navazující otázkou na předchozí bylo cílem zjistit, jak často bylo provedeno úspěšné zajištění peněz po oznámení skutku, a to bez ohledu na výši zajištěné částky – to bude předmětem další otázky.

Odpověď opět vychází z 51 skutků z roku 2022 a ze 42 skutků z roku 2023 (dohromady 93).

Po oznámení se podařilo zajistit výnos, nebo alespoň jeho část

- v roce 2022 u 4 z 51 (8 %) skutků,
- v roce 2023 u 8 ze 42 (19 %) skutků.

Graf č. 30 – Podařilo se zajistit výnos?



Zdroj: Vlastní zpracování

Celkem se podařilo zajistit výnos nebo část výnosu u 12 z 93 (13 %) skutků.

Nezdar při zajišťování peněz není způsoben tím, že by policejní orgán neprovedl potřebný postup[22], ale z toho důvodu, že v době oznámení jsou peníze zpravidla už mimo dosah, tzn., jsou buďto vybrány pomocí tokenu platební karty, odkloněny

[22] Zákon č. 141/1961 Sb., *o trestním řízení soudním (trestní řád)* v posledním znění, § 79a.

do zahraničí nebo do kryptoměn. A v těchto případech je velmi složité až téměř nemožné účinně provést zajištění výnosu.

Výnos byl zajišťován pouze na bankovních účtech vedených u bank v České republice. A ačkoliv lze také za určitých podmínek provést zajištění kryptoměn, tak v prostudovaných spisech to nebylo zjištěno.

Otázka č. 36: Jaká byla výše zajištěného výnosu?

Touto přímo navazující otázkou na předchozí bylo už přesně zjišťováno, jaká výše výnosu v poměru ke způsobené škodě byla zajištěna.

Odpověď vychází ze 4 skutků z roku 2022 a z 8 skutků z roku 2023, což odpovídá výsledkům z předchozí otázky (dohromady 12).

Výnos byl zaokrouhlen na tisíce a zajištěná částka v případě nutnosti na stovky.

U výnosů z roku 2022 bylo zjištěno, že se podařilo zajistit 2x celý a 2x jeho část:

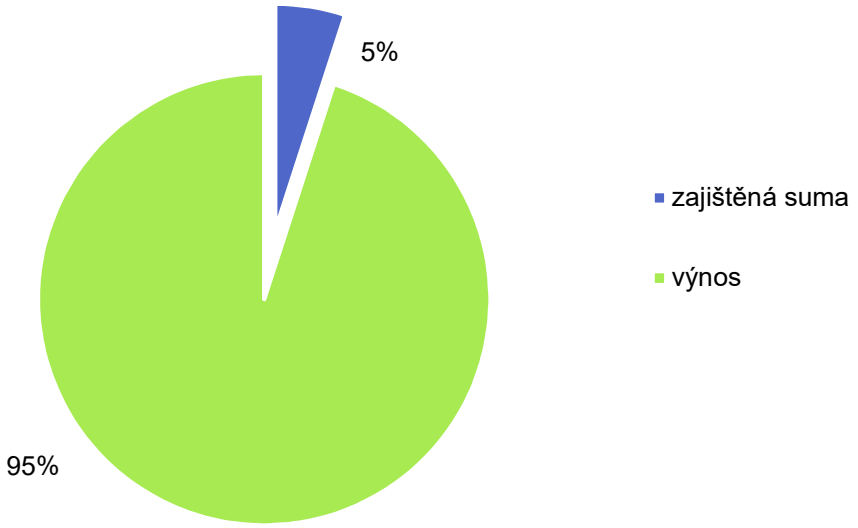
- u škody 290.000 Kč byla zajištěná celá tato částka (100 %),
- u škody 110.000 Kč byla zajištěná celá tato částka (100 %),
- u škody 100.000 Kč byla zajištěná částka 2.000 Kč (2 %),
- u škody 85.000 Kč byla zajištěna částka 60.000 Kč (71 %).

U výnosů z roku 2023 bylo zjištěno, že se podařilo zajistit jen jejich části:

- u škody 950.000 Kč byla zajištěná částka 665.000 Kč (70 %),
- u škody 240.000 Kč byla zajištěna částka do 1.000 Kč (do 1 %),
- u škody 240.000 Kč byla zajištěna částka do 500 Kč (do 1 %),
- u škody 225.000 Kč byla zajištěná částka do 100 Kč (do 1 %),
- u škody 200.000 Kč byla zajištěná částka 50.000 Kč (25 %),
- u škody 150.000 Kč byla zajištěná částka do 200 Kč (do 1 %),
- u škody 150.000 Kč byla zajištěná částka do 100 Kč (do 1 %),
- u škody 90.000 Kč byla zajištěná částka 36.000 Kč (40 %).

Celkem se podařilo zajistit okolo 1.214.900 Kč ze souhrnného přibližného výnosu 24 milionů Kč, což představuje přibližně 5 % z výnosů.

Graf č. 31 – Jaká byla výše zajištěného výnosu?



Zdroj: Vlastní zpracování

Zajištěné částky byly buďto na zneužitých účtech pachatelem ponechané zbytky peněz nebo se jednalo o peníze, které pachatel nestihl odklonit z důvodu blokace účtu ze strany banky (dočasné opatření po zjištěné neobvyklé aktivitě).

Otázka č. 37: V kolika případech zjištěné informace vedly do zahraničí?

V rámci této otázky bylo cílem zjistit, jak často jsou podvody fiktivních bankéřů zahraničního charakteru.

Po prostudování spisových materiálů, které byly vybrány pro celé terénní šetření, bylo u všech případů, tj. 112 z let 2022 a 2023, zjištěno skutečností vedoucích do zahraničí.

Zahraničí informace byly o využívání telekomunikačního a datového provozu, bankovních účtů, kryptoměnových služeb, obchodů, e-shopů, sociálních a jiných sítí a totožností.

Bez grafického vyobrazení.

Otázka č. 38: V kolika případech bylo provedeno mezinárodní šetření?

V předchozí otázce bylo zjištěno, že všech 112 případů bylo s mezinárodním charakterem. Cílem této navazující otázky bylo pak zjistit, v kolika případech bylo provedeno mezinárodní šetření.

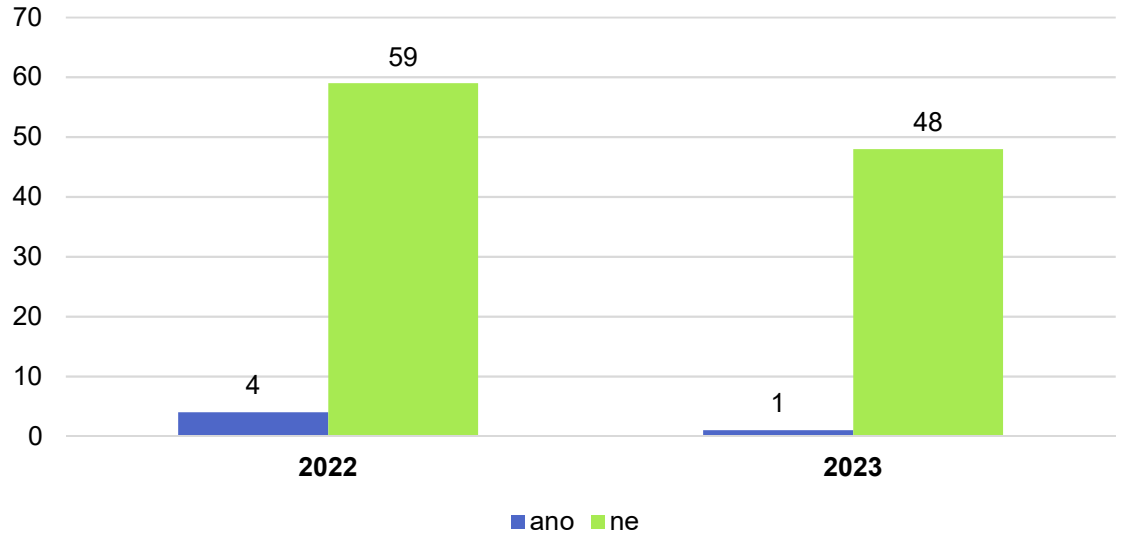
Pro potřeby této otázky mezinárodním šetřením rozumíme:

- Mezinárodní právní pomoc[23] (dále jen „MPP“),
- Evropský vyšetřovací příkaz[24] (dále jen „EVP“).

Mezinárodní šetření bylo provedeno

- v roce 2022 u 4 z 63 (6 %) případů. Konkrétně se vždy jednalo o EVP.
- V roce 2023 u 1 ze 49 (2 %) případů. Opět se jednalo o EVP.

Graf č. 32 – V kolika případech bylo provedeno mezinárodní šetření?



Zdroj: Vlastní zpracování

Celkem bylo zjištěno, že u 5 ze 112 (4 %) případů bylo provedeno mezinárodní šetření, a to formou EVP. MPP nebyla využita.

[23] Zákon č. 104/2013 Sb., *o mezinárodní justiční spolupráci ve věcech trestních* v posledním znění, část třetí, hlava I.
[24] EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady 2014/41/EU ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech. Online. In: *Úřední věstník Evropské unie*. 2014, L 130/1, s. 1-36. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32014L0041. [citováno 06.03.2024].

Otázka č. 39: Jaké varianty mezinárodního operativního šetření jsou prováděny?

Touto navazující otázkou bylo zjišťováno, jaké všechny způsoby jsou využívány pro operativní šetření v cizině.

Odpovědí na tuto otázku se opět odchýlím od nastoleného standartu uveřejnění výsledků. Zjištění budou opět jen popisná.

Mezinárodní operativní šetření je v rámci Policie ČR prováděno velmi často. Je využíváno více cest, kterými je možno získat, ověřit nebo vyvrátit informace. Cesta je zpravidla aplikována podle dřívějších zkušeností a aktuálně dohodnutých způsobů výměny informací.

Není vyloučeno a praxe to mnohdy vyžaduje, že bude využito více cest pro potřeby zjištění stejné informace.

V rámci studia spisových materiálů bylo zjištěno, že nejčastěji je využíváno služeb *Útvaru zvláštních činností* (zkráceně ÚZČ). ÚZČ se v rámci Policie ČR stalo kontaktním místem pro celou řadu zahraničních subjektů (zpravidla postupem podle § 8 a 88a tr. řádu).

Dalšími významnými subjekty pro mezinárodní operativní šetření jsou elitní složky Policie ČR, jako je *Národní centrála proti organizovanému zločinu* (zkráceně NCOZ) a *Národní centrála proti terorismu, extremismu a kybernetické kriminalitě* (zkráceně NCTEKK), které představují kontaktní místa pro vybrané mezinárodní společnosti.

Velmi často je využíváno služeb *Ředitelství pro mezinárodní policejní spolupráci* (zkráceně ŘMPS) a jejich prostřednictvím je zpravidla také prováděna spolupráce s Europolem, Interpolem, se společnými centry, styčnými důstojníky a výjimečně s dalšími spolupracujícími státními orgány.

Realizace vlastního šetření v cizině, které provádí sami zpracovatelé případů, je v posledních letech na vzestupu. Tato šetření jsou u zahraničních subjektů v podstatě na bázi dobrovolnosti při plnění společného cíle, což je boj proti kybernetické kriminalitě.

K vlastnímu šetření je zpravidla využívána e-mailová korespondence. A dále specializovaná kontaktní místa, například velmi zdařilá iniciativa KODEX[25] (www.kodexglobal.com), což je internetová platforma, která umožňuje oficiální, spolehlivou a bezpečnou výměnu informací mezi společnostmi a státními orgány.

V souhrnu je možno uvést, že pro cestu operativního šetření je využíváno těchto kanálů:

- spolupráce s ÚZČ,
- spolupráce s NCOZ nebo NCETKK,
- spolupráce s ŘMPS,
- spolupráce se společným centrem a styčným důstojníkem,
- spolupráce s Europolem nebo Interpolem,
- uzavřené kooperační platformy,
- vlastní operativní šetření.

Otázka č. 40: Byla zapojena veřejnost do vyšetřování?

O případy kybernetické kriminality není mezi širší veřejností zas takový zájem. Kriminalita virtuálního světa je často veřejně prezentována jen jako zajímavost, upozornění nebo předmět k další edukaci. A pokud už je veřejnost do vyšetřování zapojena, tak zpravidla pro účely pátrání po totožnosti pachatele. Není však vyloučeno, že by veřejnost mohla být zapojena i pro potřeby vyhledávání dalších obětí.

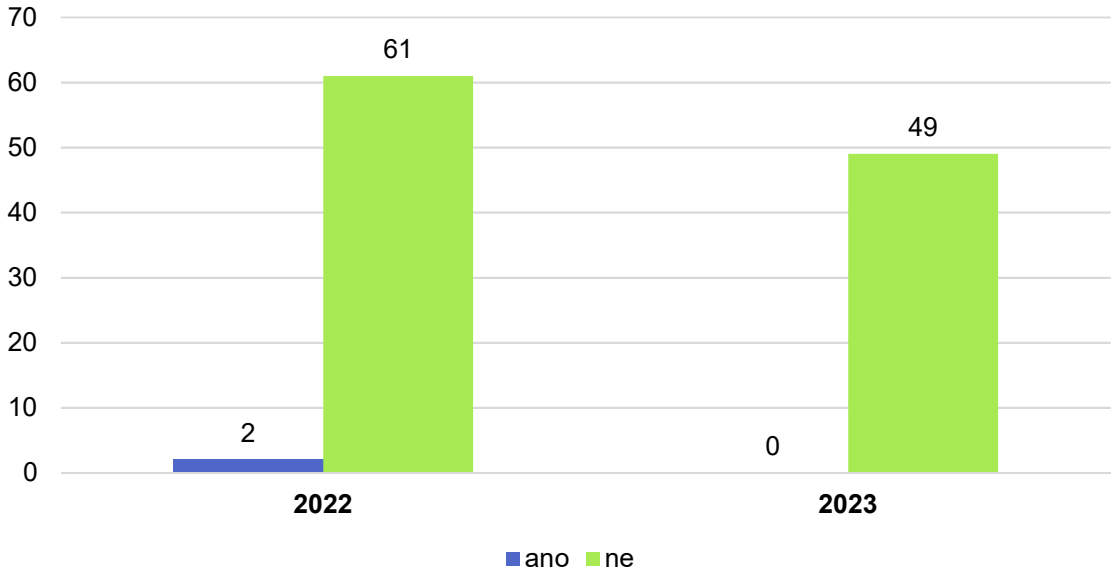
Zapojením veřejnosti do vyšetřování pro potřeby této otázky bylo myšleno, např. pátrání po totožnosti neznámé osoby, jejíž fotografie byla uveřejněná.

Veřejnost byla zapojena

- v roce 2022 u 2 z 63 (3 %) případů. A to skutečně zveřejněním fotografií osob provádějící výběr z bankomatů. Cílem bylo identifikovat totožnost osob.
- V roce 2023 nebylo zjištěno, že by byla veřejnost zapojena do vyšetřování.

[25] Provozovatel je spol. Kodex, Inc., se sídlem P.O. Box 270769, 444 E 3 rd Street, Boston, MA 02127, USA.

Graf č. 33 – Byla zapojena veřejnost do vyšetřování?



Zdroj: Vlastní zpracování

Celkem bylo zjištěno, že u 2 ze 112 (2 %) případů byla veřejnost zapojena do vyšetřování.

Ačkoliv to nebylo přímo smyslem této otázky je na místě uvést, že v rámci několika případů bylo provedeno informování veřejnosti. Jednalo se o poskytnutí informací o existenci případů, způsobu provedení a možností, jak se bránit. V podstatě se jednalo o prevenci a edukaci veřejnosti, jak bylo uvedeno v úvodu této otázky.

Otázka č. 41: Byla zjištěna organizovaná skupina?

Otázka č. 42: Jaká byla role známého pachatele v organizované skupině?

Otázka č. 43: Jaké bylo zavinění u známého pachatele?

Otázka č. 44: Jaké bylo chování pachatele při vyšetřování?

Otázka č. 45: Jaký způsob obhajoby pachatel zvolil?

Otázka č. 46: Bylo zaznamenáno nějaké ovlivňování svědků/obětí?

Otázka č. 47: V kolik případech se pachatel doznal?

S ohledem na výsledky z případů, ze kterých vychází toto celé terénní šetření, nebylo možno odpovědět na připravené otázky č. 41 až 47.

Z formálního důvodu níže uvedu krátký popis předmětu vynechaných otázek:

- otázka č. 41: dopustila se činu organizovaná skupina, popř. byla v průběhu vyšetřování zmapována a popsána její struktura;
- otázka č. 42: jaké postavení zjištěná osoba zastávala v rámci struktury organizované skupiny, proti které bylo vedeno trestní řízení;
- otázka č. 43: z pohledu trestního práva stanovení zavinění u osoby, proti které bylo vedeno trestní řízení;
- otázka č. 44: cílem bylo popsat, jak se projevoval během vyšetřování;
- otázka č. 45: cílem bylo popsat, jak se projevoval v návaznosti na ZTS;
- otázka č. 46: cílem bylo popsat, jestli se snažil ovlivnit výpovědi osob;
- otázka č. 47: cílem bylo popsat, za jakých okolností se k činu doznal.

IV. pachatelé

Otázka č. 48: Jaké bylo pohlaví pachatele?

Otázka č. 49: Jakého věku byl pachatel?

Otázka č. 50: Jaké národnosti byl pachatel?

Otázka č. 51: Jaké je nejvyšší dosažené vzdělání pachatele?

Otázka č. 52: Byl pachatel už dříve trestán?

Otázka č. 53: Byl pachatel v době činu zaměstnán?

Také zde ze stejných důvodů nebylo možno odpovědět na otázky č. 48 až 53.

Opět formální a nezbytný krátký popis předmětu vynechaných otázek:

- otázka č. 48: statistické stanovení pohlaví pachatelů,
- otázka č. 49: statistické stanovení věku pachatelů,
- otázka č. 50: statistické stanovení národnosti pachatelů,
- otázka č. 51: statistické stanovení vzdělanosti pachatelů,
- otázka č. 52: statistické stanovení recidivy u pachatelů,
- otázka č. 53: statistické stanovení zaměstnanosti pachatelů.

Otázka č. 54: Jakým jazykem pachatel hovořil?

Z výslechů obětí bylo možno u pachatelů stanovit alespoň, jakým jazykem hovořili během telefonních hovorů. Pro potřeby této otázky jsou jako pachatelé vzaty všichni bez ohledu na jejich role a zapojení.

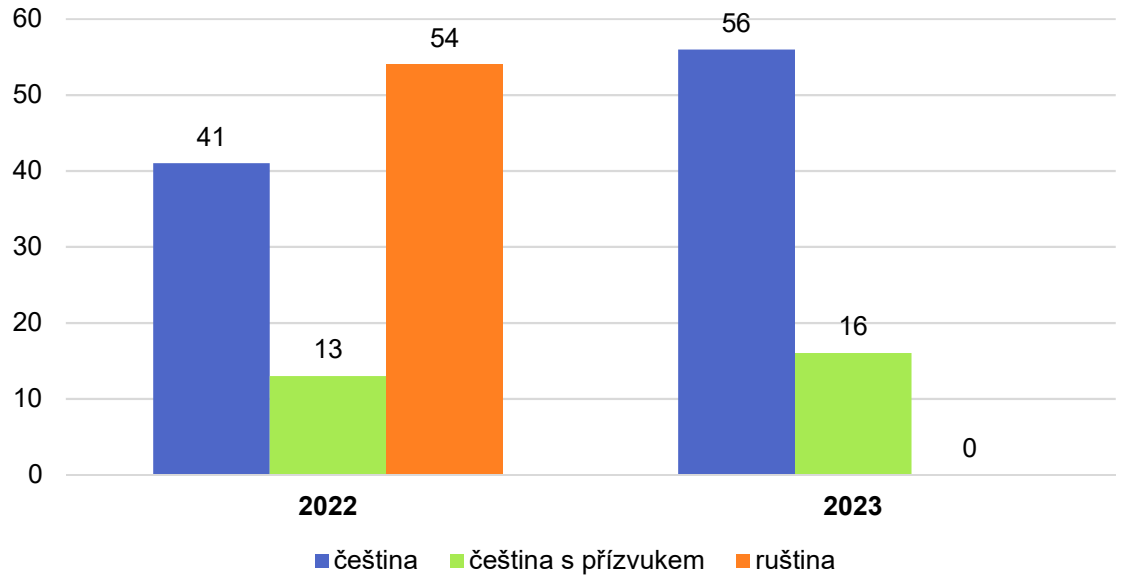
Odpověď vychází ze 108 osob z roku 2022 a ze 72 osob z roku 2023 (dohromady 180), což odpovídá společným výsledkům z otázky č. 1, 16 a 17 (pachatelé v rolích pracovníků bank a policistů).

Nutno uvést, že v počtech nemusejí být výsledky správné. Některé skutky mohly být spáchány stejnými pachateli, avšak jsou prověřovány samostatně. De facto dochází k navýšení (duplicitě) zde uvedených počtů osob, i když se jednalo o stejné. Přesto v poměrech lze očekávat relevantní hodnoty.

Pachatelé hovořili

- v roce 2022: Českým jazykem u 54 (50 %) skutků a Ruským jazykem také u 54 (50 %) skutků. 13 z 54 (24 %) osob hovořících Českým jazykem mělo silný přízvuk.
- V roce 2023: Českým jazykem u všech 72 (100 %) skutků. 16 ze 72 (22 %) osob mělo silný přízvuk.

Graf č. 34 – Jakým jazykem pachatel hovořil?



Zdroj: Vlastní zpracování

Celkem bylo zjištěno, že 126 (70 %) osob hovořilo česky a 54 (30 %) osob hovořilo rusky. Z česky hovořících osob mělo 29 (23 %) znatelný přízvuk.

K přízvuku bylo uváděno, že se vždy jednalo o východoevropský typ.

Oběti ve výsleších, především pak oběti Ukrajinské národnosti, občas uváděli, že pachatelé často během hovorů hovořili střídavě rusky a ukrajinsky.

V. oběti

Odpovědi na všechny otázky z této skupiny vychází z 67 skutků z roku 2022 a z 58 skutků z roku 2023 (dohromady 125).

Pro potřeby této sady otázek byla jako oběť vzata pouze osoba, která vedla hovor s pachatelem.

Nebyly vzaty k úvaze osoby, které se staly návaznými poškozenými, například z toho důvodu, že bankovní účet je veden pro dvě osoby a peníze jsou součástí společného jmění, dále pojišťovny apod.

Otázka č. 55: Jaké bylo pohlaví oběti?

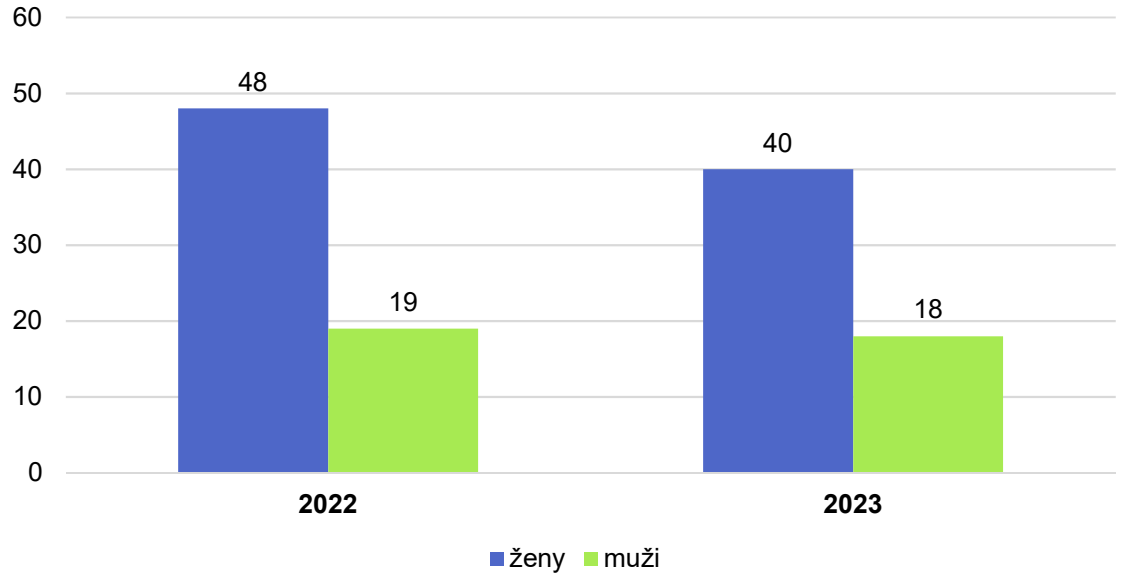
První otázkou v rámci obětí bylo statistické určování jejich pohlaví.

Obětmi bylo

- v roce 2022 48 (72 %) žen a 19 (28 %) mužů,
- v roce 2023 40 (69 %) žen a 18 (31 %) mužů.

Z prostorových důvodů je graf umístěn na následující stránce.

Graf č. 35 – Jaké bylo pohlaví oběti?



Zdroj: Vlastní zpracování

Celkem bylo zjištěno, že obětmi bylo 88 (70 %) žen a 37 (30 %) mužů.

Otázka č. 56: Jakého věku byla oběť?

Navazující otázka na osobu oběti byla věnována statistickému určování věku.

Pro potřeby této otázky byly stanoveny věkové skupiny, a to v tomto uskupení:

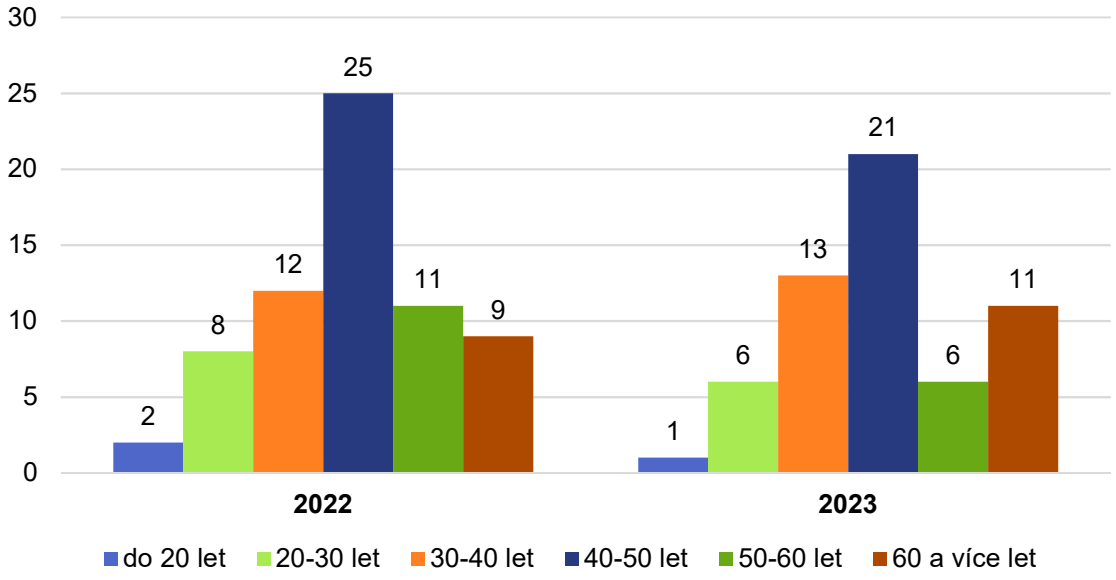
- do 20 let,
- 20-30 let,
- 30-40 let,
- 40-50 let,
- 50-60 let,
- 60 a více.

Oběti byli ve věku

- v roce 2022: 2 (3 %) do 20 let, 8 (12 %) do 30 let, 12 (18 %) do 40 let, 25 (37 %) do 50 let, 11 (17 %) do 60 let a 9 (13 %) obětem bylo více než 60 let;

- v roce 2023: 1 (2 %) do 20 let, 6 (10 %) do 30 let, 13 (22 %) do 40 let, 21 (36 %) do 50 let, 6 (11 %) do 60 let a 11 (19 %) obětem bylo více než 60 let.

Graf č. 36 – Jakého věku byla oběť?



Zdroj: Vlastní zpracování

Celkem bylo zjištěno, že 3 (2 %) oběti byli ve věku do 20 let, 14 (11 %) do 30 let, 25 (20 %) do 40 let, 46 (37 %) do 50 let, 17 (14 %) do 60 let a 20 (16 %) obětem bylo více než 60 let.

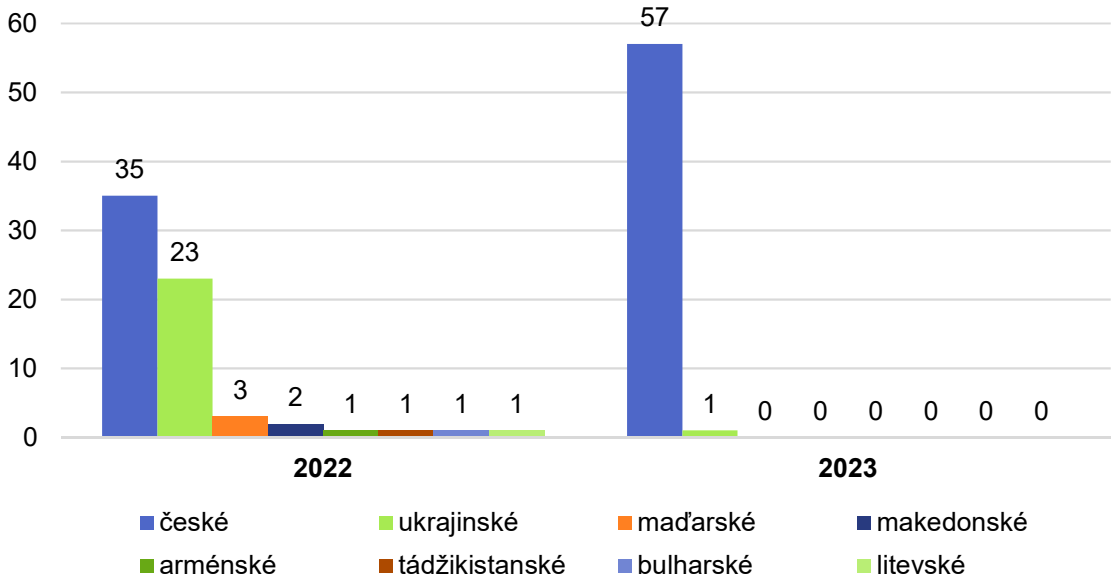
Otázka č. 57: Jaké národnosti byla oběť?

Třetí otázka o obětech byla věnována statistickému určování národnostní příslušnosti.

U obětí byla zjištěna národnost a bylo určeno

- v roce 2022: 35 (51 %) Čechů, 23 (34 %) Ukrajinců, 3 (4 %) Maďaři, 2 (3 %) Makedonci a po jedné oběť z Arménie (2 %), Tádžikistánu (2 %), Bulharska (2 %) a Litvy (2 %);
- v roce 2023: 57 (98 %) Čechů a 1 (2 %) Ukrajinec.

Graf č. 37 – Jaké národnosti byla oběť?



Zdroj: Vlastní zpracování

Celkem bylo obětmi 92 (73 %) Čechů, 24 (19 %) Ukrajinců, 3 (2 %) Maďaři, 2 (2 %) Makedonci a po jedné oběť z Arménie (1 %), Tádžikistánu (1 %), Bulharska (1 %) a Litvy (1 %).

Otázka č. 58: Jakým jazykem oběť hovořila?

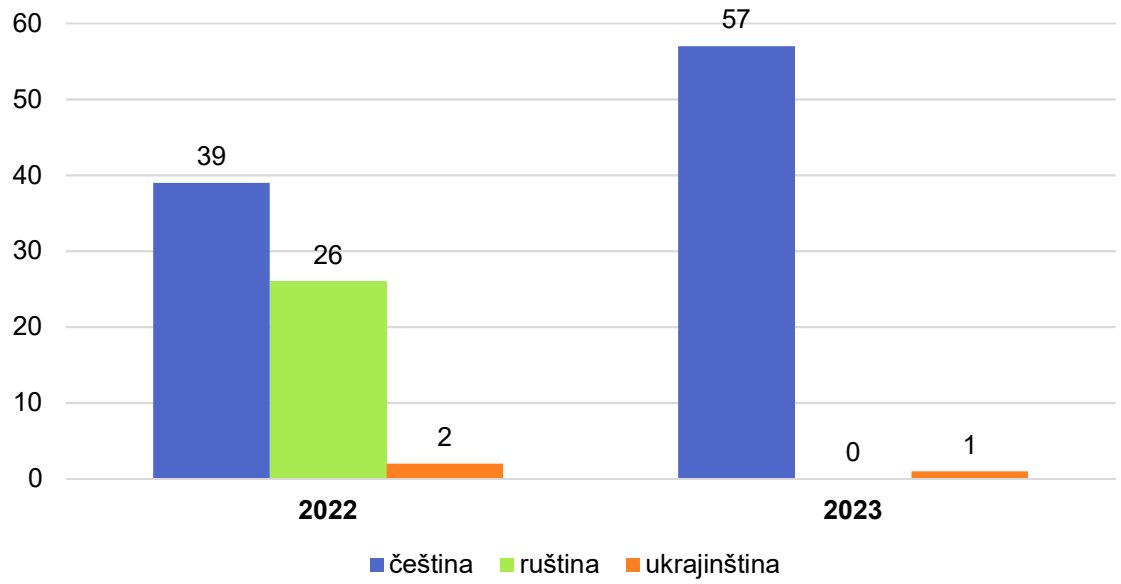
Další otázka k obětem byla věnována statistickému určování jazyku, kterým oběť hovořila během hovoru s fiktivním bankéřem.

Oběť během činu hovořila

- v roce 2022: 39x češtinou (58 %), 26x ruštinou (39 %) a 2x ukrajinštinou (3 %),
- v roce 2023: 57x češtinou (98 %) a 1x ukrajinštinou (2 %).

Z prostorových důvodů je graf umístěn na následující stránce.

Graf č. 38 – Jakým jazykem oběť hovořila?



Zdroj: Vlastní zpracování

Celkem oběti při hovoru s pachatelem využívali 96x češtinu (77 %), 26x ruštinu (21 %) a 3x ukrajinštinu (2 %).

Nutno uvést, že s ohledem na výsledky byla zkoumána znalost češtiny u cizinců. Ze spisových materiálu (především z výslechů) bylo zjištěno, že českým jazykem hovořil 1 Maďar, 1 Bulhar a 2 Makedonci. Všichni čtyři dlouholetí obyvatelé České republiky.

Pro pořádek uvádím, že 21 Ukrajinců hovořilo s pachatelem Ruským jazykem. Ovládali oba jazyky. Ostatní 3 Ukrajinci uvedli, že hovořili Ukrajinským jazykem, avšak vzájemně si dostatečně rozuměli.

Otázka č. 59: Jaké je nejvyšší dosažené vzdělání oběti?

Předposlední otázka věnovaná obětem byla o statistickém určování jejich dosaženého vzdělání.

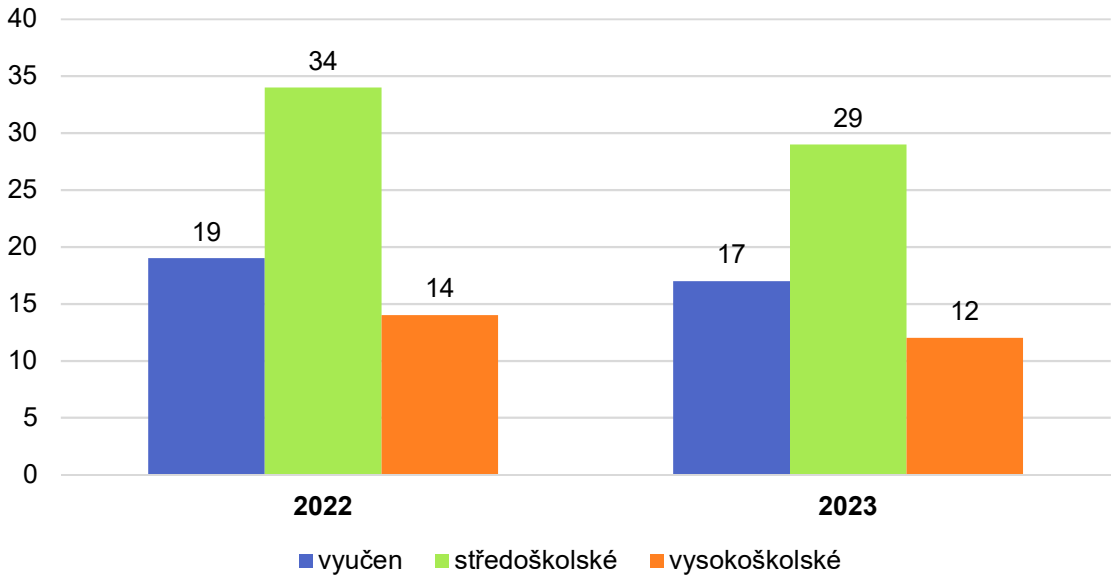
Pro potřeby této otázky byly stanoveny jen 3 skupiny vzdělání, a to:

- vyučen,
- středoškolské,
- vysokoškolské.

Dosažené vzdělání u obětí

- v roce 2022: 34 (51 %) obětí mělo středoškolské vzdělání, 19 (28 %) bylo vyučeno a 14 (21 %) mělo vysokoškolské vzdělání;
- v roce 2023: 29 (50 %) obětí mělo středoškolské vzdělání, 17 (29 %) bylo vyučeno a 12 (21 %) mělo vysokoškolské vzdělání.

Graf č. 39 – Jaké je nejvyšší dosažené vzdělání oběti?



Zdroj: Vlastní zpracování

Celkem mělo 63 (50 %) obětí středoškolské vzdělání, 36 (29 %) obětí bylo vyučeno a 26 (21 %) obětí mělo vysokoškolské vzdělání.

Otázka č. 60: Byla oběť už dříve cílem kybernetického útoku?

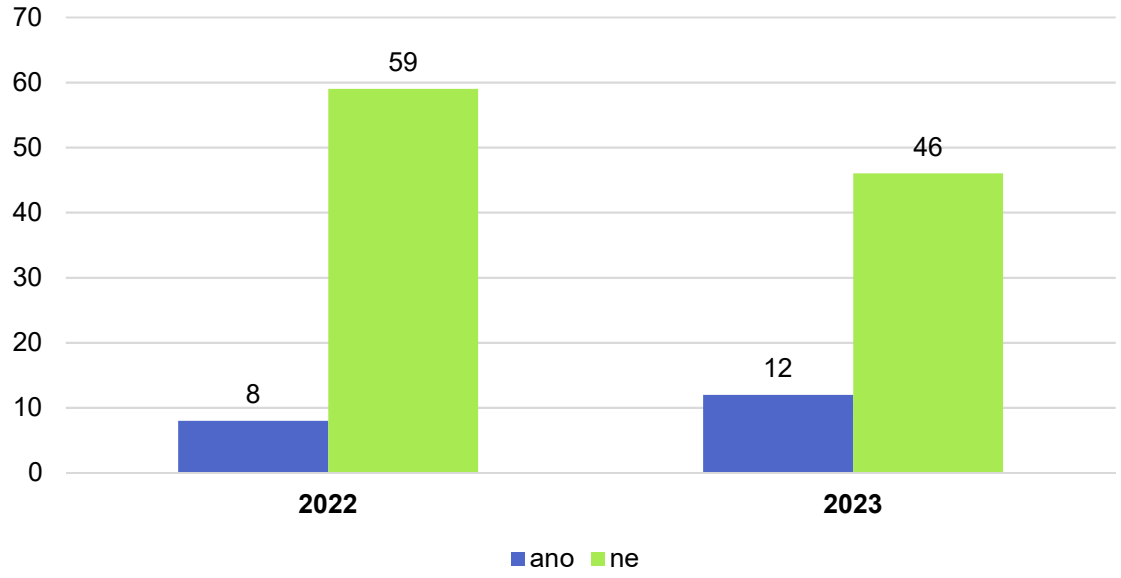
Poslední otázka o obětech je zrcadlem k recidivě u pachatelů, tedy jejím smyslem bylo zjistit, zda oběť už dříve byla cílem kybernetického útoku.

Pro potřeby této otázky byly vzaty k úvaze jen ty skutky, které už oběť dříve oznámila, respektive byly evidované Policií ČR.

Cílem kybernetické kriminality v minulosti bylo

- v roce 2022 8 z 67 (12 %) obětí,
- v roce 2023 12 z 58 (21 %) obětí.

Graf č. 40 – Byla oběť už dříve cílem kybernetického útoku?



Zdroj: Vlastní zpracování

Celkem bylo už dříve obětmi kybernetické kriminality 20 ze 125 (16 %) obětí.

Osoba, která podlehla, je pro pachatele zajímá a kontakty na ní si často předávají, tedy je možné, že bude proti ní veden jiný druh kybernetického útoku, navíc cílený. Bohužel v praxi se ukazuje, že někteří se stávají obětmi opakovaně.

VI. časové souvislosti

Otázka č. 61: Jaká doba uplynula od prvního k poslednímu kontaktu pachatele s obětí?

Smyslem této otázky bylo zjistit, po jakou dobu pachatel udržoval navázaný kontakt s obětí. Nejedná se tedy o čistý čas vzájemných hovorů. To bylo řešeno v rámci otázky č. 10. Zde je řešena celková doba, která je počítána od prvního hovoru a trvala až do doby posledního hovoru/jiného kontaktu.

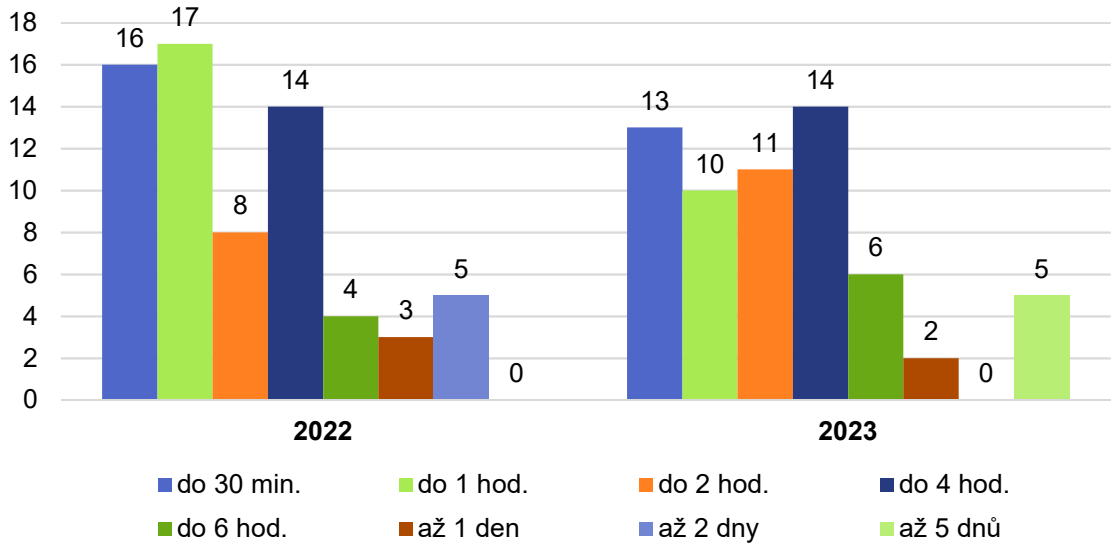
U skutků bylo zjištěno

- v roce 2022: 16x kontakt nepřesáhl 30 minut (24 %), 17x trval do 1 hodiny (25 %), 8x byl mezi 1-2 hodinou (12 %), 14x byl mezi 2-4 hodinou (21 %),

4x byl mezi 4-6 hodinou (6 %), 3x trval až den (4 %) a 5x trval až 2 dny (8 %);

- v roce 2023: 13x kontakt nepřesáhl 30 minut (22 %), 10x trval do 1 hodiny (17 %), 11x byl mezi 1-2 hodinou (19 %), 14x byl mezi 2-4 hodinou (24 %), 6x byl mezi 4-6 hodinou (10 %), 2x trval až den (4 %) a 2x trval až 5 dnů (4 %).

Graf č. 41 – Jaká doba uplynula od prvního k poslednímu kontaktu pachatele s obětí?



Zdroj: Vlastní zpracování

Celkem bylo zjištěno, že navázaný kontakt mezi pachatelem a obětí 29x nepřesáhl 30 minut (23 %), 27x trval do 1 hodiny (22 %), 19x byl mezi 1-2 hodinou (15 %), 28x byl mezi 2-4 hodinou (22 %), 10x byl mezi 4-6 hodinou (8 %), 5x trval až den (4 %), 5x trval až 2 dny (4 %) a 2x trval až 2 dny (2 %).

Zpravidla u kontaktů do 30 minut trvání se jednalo o pokus, kdy oběť nebyla oklamána a nepřistoupila na požadavky pachatele.

Na druhou stranu skutky, které trvaly několik dnů, jsou zajímavé tím, že po celou dobu oběť byla systematicky manipulována, plně důvěřovala pachateli a nenabyla jakéhokoliv podezření.

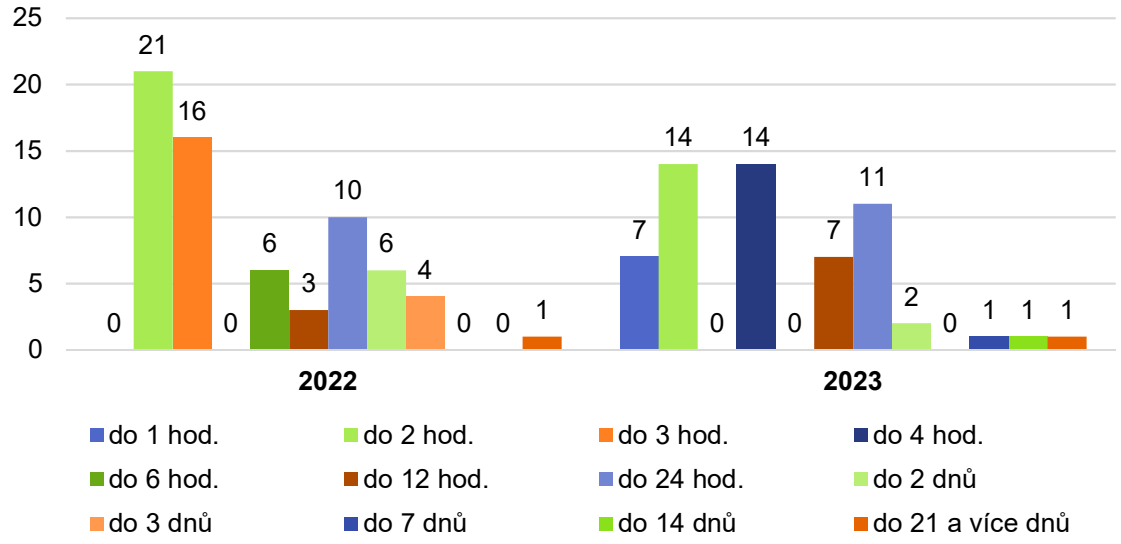
Otázka č. 62: Jaká doba uplynula od zjištění podvodu k oznámení?

V pořadí druhou otázkou z časových souvislostí bylo zjišťováno, jak dlouho trvalo, než oběť provedla oznámení o skutečnostech nasvědčující tomu, že byl spáchán trestný čin.

Oznámení bylo učiněno

- v roce 2022: 21x do 2 hodin (31 %), 16x do 3 hodin (24 %), 6x do 6 hodin (9 %), 3x do 12 hodin (5 %), 10x do 24 hodin (15 %), 6x do 2 dnů (9 %), 4x do 3 dnů (6 %) a 1x oznámení bylo učiněno až po měsíci – přesně 35 dnů (1 %);
- v roce 2023: 7x do 1 hodiny (12 %), 14x do 2 hodin (24 %), 14x do 4 hodin (24 %), 7x do 12 hodin (12 %), 11x do 24 hodin (19 %), 2x do 2 dnů (3 %), 1x do 7 dnů (2 %), 1x do 14 dnů (2 %) a 1x do 21 dnů (2 %).

Graf č. 42 – Jaká doba uplynula od zjištění podvodu k oznámení?



Celkem bylo zjištěno, že doba od zjištění k oznámení byla 7x do 1 hodiny (5 %), 35x do 2 hodin (28 %), 16x do 3 hodin (13 %), 14x do 4 hodin (11 %), 6x do 6 hodin (5 %), 10x do 12 hodin (8 %), 21x do 24 hodin (17 %), 8x do 2 dnů (6 %), 1x do 5 dnů (1 %), 4x do 3 dnů (3 %), 1x do 14 dnů (1 %), 1x do 20 dnů (1 %) a 1x oznámení bylo učiněno až po 35 dnech (1 %).

U cizinců a u nezdařených skutků byla doba k oznámení nejdelší. A některá oznámení byla učiněna až poté, co to u svých klientů vymohla banka.

Otázka č. 63: Jaká doba uplynula od oznámení k zahájení vyšetřování?

Otázka č. 64: Jaká doba uplynula od zahájení vyšetřování k podání obžaloby?

Otázka č. 65: Jaká doba uplynula od podání obžaloby do soudního rozhodnutí?

Otázka č. 66: Jaká doba uplynula od prvního kontaktu do soudního rozhodnutí?

Také ze stejného důvodu, který je uveden na str. 64 této práce, nebylo možno odpovědět na otázky č. 63 až 66.

Opět krátký formální popis předmětu vynechaných otázek:

- otázka č. 63: cílem bylo změřit čas od oznámení/zjištění trestného činu do zahájení vyšetřování,
- otázka č. 64: cílem bylo změřit čas od zahájení vyšetřování do podání obžaloby,
- otázka č. 65: cílem bylo změřit čas od podání obžaloby do soudního rozhodnutí,
- otázka č. 66: cílem bylo změřit celkový čas od prvního kontaktu mezi pachatelem a obětí až do případného soudního uzavření případu.

2.3 Shrnutí

Zpracovaným výzkumem bylo získáno velké množství jednoznačných informací, které mají o předmětné kriminalitě značnou vypovídající hodnotu. Stanovený cíl výzkumu byl splněn.

Dále je nutno konstatovat, že nulová objasněnost neumožnila využít celou řadu předpřipravených otázek, které měly návaznost na osobu pachatele. A proto v okruhu této části problematiky budu vycházet jen ze znalostí, které jsem získal při vyšetřování této problematiky a ze skutečností, které jsou prezentovány v rámci pravidelných operativních skupin k problematice kybernetické kriminality.

Některá zjištění plynoucí z výzkumu jsou velmi důležitá, jak pro budoucí metodiku, tak pro znalost reálných okolností. Vyjma nulové objasněnosti, která je zdrcující, je to také výše úspěšně zajištěného výnosu. Ta byla pouze okolo 5 % z odcizených 24 milionů. Je to především způsobeno tím, že až 90 % výnosů bylo směřováno do kryptoměn, které jsou značně anonymní a velmi obtížně se trasují. U 28 % případů pachatel získal přístup do bankovnictví. Dále je zajímavá ta skutečnost, že pachatel maskované telefonní číslo vydával za pravé u 76 (66 %) skutků a u 40 (34 %) skutků číslo vůbec neodpovídalo. Krom jiného to znamená, že pachatel k úspěšnému provedení nutně nepotřebuje číslo banky nebo policie.

Výsledky a informace z celého terénního výzkumu budou použity jako podklad pro následně zpracovanou metodiku.

3 Metodika vyšetřování fiktivních bankéřů

Kriminalistická metodika vyšetřování fiktivních bankéřů je úzce specializovaná a kombinovaně dceřiná především k metodice vyšetřování obecných podvodů, dále k metodice vyšetřování organizované a kybernetické kriminality.

3.1 Kriminalistická charakteristika

Kriminalita fiktivních bankéřů je ryze majetková trestná činnost podvodného charakteru, typicky páchaná mezinárodně v trestné součinnosti a větších sériových možností.

Obecně je zaměřena proti komukoliv, kdo je oprávněný uživatel bankovního účtu s internetovým přístupem. Páchána je distančním způsobem pomocí telefonní, digitální a další techniky. A cílem jsou peníze uložené na bankovních účtech.

Získávání peněz probíhá buďto zprostředkovaně pomocí zmanipulovaných obětí, které jsou oklamáni a jednají v omylu ve prospěch pachatelů nebo po získání od obětí rozhodných informací a přístupů k internetovému bankovnictví peníze odkloní sami pachatelé. Kombinace není vyloučena.

Povahou je tato kriminalita latentní, a to zpravidla až do doby, než ji oznámí oběť, avšak ta může být ovlivněna studem a skutek může vyjít najevo až se značným odstupem, popř. nemusí být nikdy zjištěn.

Podvody fiktivních bankéřů, pokud se zaměříme na podstatu, jsou výsledkem důsledné kooperace tří stránek, které se vzájemně podporují, a je to stránka:

a) technická,
b) psychologická,
c) organizační.

Ad a) Technická stránka zejména zahrnuje technologickou vybavenost, využité komunikační prostředky a služby, způsob k přístupu do sítě Internet, způsoby zamezeni vzniku digitálních (kybernetických) stop a způsoby získávání peněz.

Ad b) Do psychologické stránky je možno obecně zařadit způsob navázáni kontaktu s obětí, získání jejího zájmu, způsob vedení hovoru, budování systematické manipulace, verbální působení a další metody přesvědčování.

Ad c) Organizační stránka především obsahuje správné využívání technických znalostí, zajištění zázemí a prostor k realizaci, organizaci osob, přeshraniční kriminální spolupráci, získávání nutných pomocníků, utajení činnosti a získávání informací pro páchání trestné činnosti.

Podvodný charakter této trestné činnosti je z trestněprávního pohledu přímo definován trestným činem *Podvod*[26], kterého se dopustí kdokoliv, *„kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou, …“*[27]

Trestný čin podvodu je u kriminality fiktivních bankéřů primární skutkovou podstatou a je běžně doprovázen další kvalifikací, která odráží specifický způsob provedení konkrétního skutku. Jedná se především o trestné činy *Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací*[28] a *Neoprávněné opatření, padělání a pozměnění platebního prostředku*[29]. Vyloučená není další doprovodná kvalifikace.

Z hlediska zavinění se jedná o úmyslné jednání.

S ohledem na výši způsobené škody (do 10.000 Kč[30]) není vyloučené, že skutek bude hodnocen jako tzv. *přestupek proti majetku způsobený podvodem*[31]. Samozřejmě to je možné jen za předpokladu, že nebyl doprovázen jednáním, které je možno subsumovat pod shora uvedené další trestné činy.

U legalizátorů, kteří jednali vědomě (pachatel využil jejich dohodnuté pomoci), je obvyklá kvalifikace *Legalizace výnosů z trestné činnosti*[32] a situačně opět trestný čin *Neoprávněné opatření, padělání a pozměnění platebního prostředku*.

U legalizátorů, kteří jednali nevědomě (zpravidla pachatelem ve vyvolaném omylu, respektive byli součástí řetězce podvodného jednání), po naplnění skutkové

[26] Zákon č. 40/2009 Sb., *trestní zákoník* v posledním znění, § 209.
[27] Tamtéž, § 209 odst. 1.
[28] Tamtéž, § 230.
[29] Tamtéž, § 234.
[30] Tamtéž, § 138 odst. 1 písm. a).
[31] Zákon č. 251/2016 Sb., *o některých přestupcích* v posledním znění, § 8 odst. 1 písm. a) bod 3.
[32] Zákon č. 40/2009 Sb., *trestní zákoník* v posledním znění, § 216.

podstaty (s ohledem na větší škodu, minimálně 100.000 Kč[33]) je možné jednání kvalifikovat jako trestný čin *Legalizace výnosů z trestné činnosti z nedbalosti*[34].

3.1.1 Typické kriminální situace

Komponenty kriminální situace, v níž jsou páchány podvody fiktivních bankéřů, jsou především:

a) **Možnosti a zabezpečení datových a telekomunikačních sítí a služeb**. Vybudované telekomunikační a datové sítě vytvořily nové prostředí – virtuální, do kterého se také přesunula část kriminality. Technika je běžně přizpůsobena k snadnému užívání, a proto zároveň klade nároky, aby nebyla zneužita. Je nutné, aby globální a rychlé šíření nových technologií bylo bezprostředně doprovázeno pochopením obyvatelstva – uživatelů. V České republice je síť Internet veřejně dostupná od roku 1995. Mezi lety 1996-1998 bylo k internetu připojeno jen okolo 5 % obyvatelstva. Přes 50 % obyvatelstva mělo přístup k internetu až po roce 2010. Aktuálně je to okolo 85 %.[35] Digitální gramotnost obyvatelstva, především starších generací, není na takové úrovni. Lidé si často neuvědomují nebezpečí, která nejen internet přináší. Jsou k rizikům slepí a nadmíru důvěřiví. A podceňování nebezpečí a neostražitost v digitálních aj. sítí vede ke značným materiálním a osobnostním škodám.[36] V prostředí internetu *„je největší překážkou anonymita. I dnes má každý člověk stále jedinečnou možnost používat internet anonymně, ví-li, jak na to – jestliže umí maskovat fyzickou polohu svého počítače*.“[37] Obecné možnosti konektivity, které nejsou limitovány vzdáleností, dostupností a využitou technikou, vytvářejí anonymní prostředí, ve kterém je kriminalita úspěšná a velmi skrytá. Je možné se setkat s názorem, že anonymita v sítích je jen iluze.[38] Je používáno přeci techniky, kterou je možno v telekomunikačních sítí jednoznačně identifikovat

[33] Tamtéž, § 138 odst. 1 písm. b).
[34] Tamtéž, § 217.
[35] Český statistický úřad. *Informační společnost v číslech – 2018*. Prezentace. Kapitola C: Jednotlivci. 2018. Dostupné z: https://www.czso.cz/documents/10180/61601892/061004-18_data.zip/669bf930-1b80-4046-9c00-4abdd5ba82b5?version=1.1. [cit. 24.03.2024].
[36] ROUTA, Tomáš. *Kriminalistické problémy vyšetřování podvodných internetových obchodů*. Diplomová práce. Zdeněk KONRÁD (vedoucí práce). Praha: Policejní akademie České republiky v Praze, Fakulta bezpečnostně právní. 2020, s. 58.
[37] GLENNY, Misha. *Temný trh. Kyberzloději, kyberpolicisté a vy*. Oldřich KLIMÁNEK (překladatel). Praha: Argo, 2013. ISBN 978-80-7363-522-0, s. 13.
[38] Např. KOLOUCH, Jan. *Cybercrime*. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8, s. 133.

pomocí IP adres nebo identifikátorů MAC, IMEI, IMSI a jiných individuálních a specifických technických označení. Je možno souhlasit s tím, že techniku nikoliv však bez větších obtíží lze identifikovat, ale jejího uživatele je často problematické ustanovit. Navíc do běžné mobilní sítě je možné přistupovat i z internetu, a to pomocí např. protokolu VoIP (viz subkapitola 1.1.2).

b) **Možnosti a zabezpečení bankovního systému, operací a služeb**. Systém bankovnictví se neustále vyvíjí a reflektuje na požadavky doby. Zjednodušení a zpříjemnění služeb zákazníkům je trendem. Moderní technologie umožnuje bankám vytvářet snadný přístup k bankovním účtům, které si zákazníci sami do značné míry spravují a upravují. Banky tím ale ztrácejí vliv nad bezpečností, neboť co bylo dříve možné jen osobně, je nyní dostupné digitální cestou přes aplikace, např. v tzv. chytrém mobilním telefonu. Avšak tím, že banky umožnily zákazníkům distanční správu účtů, smluvně na ně přesunuli spojená rizika. Je však nutno zdůraznit, že banka nepotřebuje pomoc klienta k ochraně jeho peněz, a pokud klient sám svou činností bance nezmaří jejich ochranu, peníze jsou v bezpečí. Každý majitel účtu je povinen držet v tajnosti svá přístupová hesla a rozhodná data umožňující ovládnout účet nebo platební prostředky. Pachatelé podvodů fiktivních bankéřů využívají nejslabšího dílu bezpečnosti – majitele účtu. Ovlivněním majitele účtu získávají to, co bylo dříve možné jenom přímým vniknutím do banky.

c) **Dostupnost technologií a služeb** napomáhá pachatelům realizovat podvody distančně, získávat různé prostředky a najímat osoby pro dílčí úkoly. Podvody fiktivních bankéřů nejsou zvláště náročné na speciální technickou vybavenost, kterou by bylo obtížné získat. Rovněž technika nevyžaduje zvláštní odbornost a je uživatelsky dostupná. Využívané komunikační služby jsou rovněž běžně přístupné a jsou poskytovány přes internet. Poskytovatelé telekomunikačních služeb, které umožnují anonymní využívání sítí a internetu, nejsou v současné době ničím výjimečným. Pachatelé podvodů navíc mohou získávat prostředky k realizaci, aniž by museli vycestovat do zahraničí a jimi používaná technika, byť je získávána ve větším množství, nevzbuzuje podezření.

d) **Kriminální citlivost, připravenost a vyspělost obyvatelstva**. Podvodná jednání jsou obyčejně ve společnosti rázně odmítána. Tolerance obyvatelstva ke kriminalitě spojené s digitálními sítěmi a internetem ale stoupá a projevuje

se často až nezájmem. Obyvatelé si obvykle neuvědomují, co vše je možné prostřednictvím sítí uskutečnit a jaká rizika a škody lehkomyslným přístupem podstupují. Pachatelé využívají nepřipravenost a neznalost obyvatel a rovněž nahodile situační okolnosti.

e) **Úroveň právních ochran a regulace** je nutná jak z hlediska funkční represe, tak nezbytné účinné prevence. Ochrana obyvatelstva v telekomunikačních sítí před jejich zneužíváním je prioritou s postupující digitalizací.
f) **Trh kryptoměn** a její právní úprava se stává stále důležitějším tématem v kontextu rostoucí popularity a jejich využití v různých oblastech ekonomiky. Základní otázky v této oblasti jsou, zda kryptoměny mohou být považovány za zákonné platidlo a jakým způsobem budou regulovány v rámci jednotlivých právních systémů. V mnoha zemích probíhají aktivní diskuse o vhodném právním rámci pro kryptoměny, včetně otázek týkajících se daní.
g) **Připravenost a vybavenost policejních orgánů**. Kriminalita páchaná v kybernetickém prostoru je velmi dynamická a vyvíjí se společně s novými technologiemi a možnostmi všech komunikačních sítí. Policejní orgány musí na tuto dynamiku adekvátně zareagovat a budovat připravenost a odbornost. Správné využívání lidských zdrojů, znalost technologií a kriminálních postupů je nutnost, bez které nelze účinně bojovat proti jakékoliv kriminalitě.

3.1.2 Typické způsoby páchání

Typické způsoby páchání trestné činnosti fiktivních bankéřů jsou de facto vyjádřeny skutkovou podstatou trestného činu *podvod*[39] a dílem jeho alternativní konstrukce.

Kompletní alternativní vyjádření skutkové podstaty je možno uplatnit v podvodech obecného charakteru, avšak skutek fiktivního bankéře je jednání, které je možné charakterizovat jako aktivní a cílené s postupně gradující fikcí. Pachatel záměrně o sobě uvádí nepravdivé skutečnosti a dále využívá vykonstruovaných lživých situací. S ohledem na typické způsoby páchání fiktivního bankéře lze následně vyloučit alternativy skutkové podstaty trestného činu *podvod*, jako jsou *využije*

[39] Zákon č. 40/2009 Sb., *trestní zákoník* v posledním znění, § 209.

něčího omylu a *zamlčí podstatné skutečnosti*. Způsob páchání je zde jednoznačně vyjádřen v alternativě *uvede někoho v omyl.*

Kriminalita fiktivních bankéřů je tedy primárně páchána formou **uvedení v omyl o osobě pachatele a situaci** s cílem

a) vniknout do bankovního účtu oběti a odčerpat peníze,
b) přesvědčit oběť, aby sama provedla odčerpání peněz.

Sekundárně je typicky páchána za účelem vniknutí do bankovního účtu oběti a následného zneužití účtu

a) k řetězení s dalšími účty (přeposílání výnosů mezi více obětmi),
b) zdroji nových informací,
c) nebo pro potřeby utvoření fikce v rámci dalšího budoucího skutku.

Nelze vyloučit kombinace uvedených možností páchání.

K odčerpání peněz bez ohledu na to, jestli to provedl sám pachatel nebo oběť pod vlivem manipulace, je využíváno více cest:

- bankovní převod na tuzemský účet,
- bankovní převod na zahraniční účet,
- karetní transakce,
- karetní platby,
- výběr peněz z bankomatů,
- vložení peněz do automatu na nákup kryptoměn,
- předání peněz osobě spolupracující s pachatelem (legalizátor).

3.1.3 Typické vlastnosti pachatelů

Vymezit charakteristické vlastnosti pachatelů podvodu fiktivních bankéřů je velmi obtížné, a to nikoli jen z důvodů nedostatečných informací z vyšetřovací praxe.

V úžím vyjádření je pachatelem osoba, která realizuje podvodný hovor s obětí, a proto má určité komunikační předpoklady. Šířeji hovoříme o skupině pachatelů jednající v jisté trestné součinnosti, kteří už mají rozdělené role, a tudíž i rozdílné vlastnosti a jsou na ně kladeny další rozdílné požadavky.

Pachatelství fiktivních bankéřů zpravidla vyžaduje spolupracující skupinu a určitou míru až úplnou organizovanost. Pachatelé navíc využívají přeshraniční propojení, kontakty a spolupráci. Zjištěné minimální skutečnosti z kriminalistické praxe navíc poukazují na to, že někteří pachatelé jsou zapojeny také do dalších typů podvodů páchaných na síti Internet.

U osoby pachatele odbornost není vyloučena, avšak ani není nezbytná. Zběhlost v technologiích, bankovním systému a telekomunikačních sítí je jistou výhodou. Není ani nutný předpoklad zastávaného postavení nebo blízké funkce. Nezbytná je jistá znalost jazyků a určitého prostředí, tzn. států, ve kterém se cílené oběti nacházejí a státu, ze kterého je trestná činnost páchaná.

Zároveň se nejedná o trestnou činnost páchanou výlučně jen cizinci.

Obecně je možno stanovit, že věková hranice pachatelů ani vzdělání zde není zásadní ukazatelem. U části pachatelů je nezbytná výřečnost a schopnost alespoň částečné improvizace a přizpůsobení se nastalé situaci. Výhodou je schopnost získání důvěry, umění manipulací a odhadu osoby. Další část vyžaduje technicky zaměřené typy mající znalosti o technice, sítích, telekomunikacích, o způsobů anonymizace a bankovních postupů. Rovněž osoby se schopností organizovat, získávat spolupachatele, využívat a získávat znalosti mohou mít značné uplatnění.

Není vyloučeno, že pachatelé mohou zastávat více rolí.

Osoba legalizátora, která jednala vědomě s úmyslem pomoci pachateli zastřít výnos, je zpravidla osoba hledající snadný výdělek. Jsou různého věku, spíše mladšího (18-30 let), a vzdělání. Typické je pro ně situační hmotné uspokojení. Z vyšetřovací praxe je známo, že velké zastoupení legalizátorů je z řad cizinců – z východní Evropy.

Obecně je možné pachatele rozdělit do tří skupin s dostatečnou úrovní předpokladu:

- osoby schopné organizace,
- osoby znalé techniky,
- osoby schopné komunikace.

3.1.4 Typické motivy

Typickým motivem podvodu je chamtivost a snadný majetkový prospěch na úkor ostatních. Cílem kriminality fiktivních bankéřů jsou peníze uložené na bankovních účtech obětí a peníze bank, které oběti získají zpravidla předschválenou půjčkou. Výnos je obvykle ukrýván do kryptoměn, které poskytují značnou míru anonymity a zásadním způsobem znesnadňují odčerpání (zajištění). Vyšetřovací praxe zatím poukazuje na to, že tato kriminalita se vyplácí a případné hrozící sankce a tresty nedovedou pachatelé odradit.

3.1.5 Typické vlastnosti obětí

Obětí podvodu fiktivního bankéře může být v podstatě jakákoliv fyzická osoba, která splňuje dva předpoklady. Jednak to je vlastnictví oprávněného přístupu k bankovnímu účtu s právem manipulovat s uloženými penězi. A dále vlastnictví telefonního přístroje.

Nelze vyloučit, že oběť není zároveň poškozená osoba. Nutno uvést, že mohou být poškozeny i právnické osoby, které vlastní peníze na bankovních účtech. Dále to mohou být banky nebo pojišťovny, které kryjí způsobené škody.

V užším pojetí je oběť osoba, která vedla hovor s pachatelem, přičemž nemusí být přímo nepřipravená, lehkomyslná a nadmíru důvěřivá. Obětí se také může stát osoba znalá a schopná rozpoznat podivnost hovoru, která ale je ovlivněna situačními a osobními okolnostmi. Osoba, která je submisivní, snáze ovlivnitelná a psychicky nevyzrálá, popř. i osoba vyššího věku, je snadným cílem manipulací.

Oběti mohou být ovlivněny studem a oznámení skutku nemusí být nikdy učiněno nebo bude provedeno až s odstupem času, třeba po přesvědčení ze strany srozuměné blízké osoby nebo po požadavku banky. Při oznámení a následnému prověřování jsou oběti ochotné a dobře s OČTŘ spolupracují. Mají zpravidla motivaci pomoc dopadnout pachatele.

Z vyšetřovací praxe je známo, že podvodům fiktivních bankéřů jsou náchylnější ženy (přibližně v poměru 2:1). Věk zpravidla není podstatný a zastoupení najdeme v každé věkové kategorii s vyšší účastí osob po 40 roku. Vzdělání rovněž nehraje větší roli. A některé náchylnější a důvěřivější oběti mohou být objektem podvodu opakovaně.

3.2 Typické stopy a další soudní důkazy

Kriminalita fiktivních bankéřů je jedna z typických ostatních kriminalit páchaných v komunikačních sítích. Obvyklé místo činu, kde došlo k střetu oběti s pachatelem, zde nenalezneme. Místem činu je především kybernetický prostor. Zpravidla je možné určit jen místo následku, které je důležité pro stanovení místní příslušnosti. A výjimečně místo, ze kterého byla trestná činnost realizována, přičemž to ale bývá v zahraničí. Dalším místem, kde lze získat stopy, jsou bydliště pachatelů a účastníků trestné součinnosti. Účastníci mohou, hlavně kriminalistická praxe to potvrzuje, přebývat v zemích cílené na oběti.

Z kriminalistické praxe je běžně známo, že lze zajistit jak stopy materiální, tak především stopy paměťové a jiné soudní důkazy. Zpravidla klasické materiální stopy patří mezi poslední, které jsou získávány. Paměťově stopy a jiné soudní důkazy jsou běžně jediným počátečním zdrojem všech informací.

Zvláštní postavení mají tzv. *kybernetické stopy*. Současné kriminalistické učení kybernetickou stopu kategorizuje jako stopu materiální, zachycující vnitřní stavbu odráženého objektu a řazena je do mikrostop.[40] *„Jedná se především o e-maily, digitální fotografie, elektronicky zpracované dokumenty, historie instant message, tabulkové procesory, historie z internetových prohlížečů, databáze, obsah počítačových pamětí (RAM), zálohy počítačových dat aj.“*[41] Současná trestní praxe kybernetické stopy spíše považuje za věcné a listinné důkazy[42]

První kriminalistická stopa, která je běžně zajištěna, je paměťová stopa od oběti. Z počátku se jedná o neobsáhlejší stopu, od které se odvíjí následné šetření.

Oběť podává svědectví o průběhu a způsobu provedení činu, dále o způsobené škodě a o popisu hlasu a akustickém projevu pachatele. Zároveň je oběť zdrojem počátečních jiných soudních důkazů, například: e-mailové zprávy a jiná textová komunikace.

---

[40] PORADA, Viktor a kol. *Kriminalistika. Technické, forenzní a kybernetické aspekty*. Plzeň: Aleš Čeněk, 2016. ISBN 978-80-7380-589-0, s. 170.
[41] NĚMEC, Miroslav et al. *Teorie a metodologie kriminalistiky pro magisterské studium – II. díl. Aktuální problémy kriminalistické praxe*. Praha: ABOOK, 2019. ISBN 978-80-906974-2-3, s. 311.
[42] Zákon č. 141/1961 Sb., *o trestním řízení soudním (trestní řád)* v posledním znění, § 112 odst. 1, odst. 2.

Další paměťové stopy je možné očekávat od pachatelů a dalších osob podílejících se na trestné činnosti.

Klasické kriminalistické stopy je obtížné ze začátku získávat. Vyšetřovací praxe sporadicky zaznamenává případ, ve kterém oběť sama pořídila nahrávku hlasu pachatele. Je to obvykle jediná materiální kriminalistická stopa (typický objekt pro zkoumání v oblasti kriminalistické audioexpertizy), která je zajištěna do doby, než je zjištěno místo, odkud je trestná činnost realizována, popř. bydliště osoby jednající v trestné součinnosti.

Místo realizace této trestné činnosti je zlatým dolem kriminalistických a jiných stop. Je možné zajistit celou řadu klasických materiálních stop (daktyloskopické, trasologické, genetické atd.), jiné předměty jako jsou nástroje k trestné činnosti, další materiály, listiny a kybernetické stopy (v počítačovém, mobilním nebo jiném obdobném systému a na nosičích digitálních dat, tj. přenosné disky, centrální datová úložiště, hard disky, optické disky, řadiče SIM aj.).

Kriminalita fiktivních bankéřů je typická svou sériovou povahou. Pachatelé provádí velké množství dílčích skutků a pro tyto potřeby je nutné množství prostředků. Nebude žádnou výjimkou, že lze v místech realizace trestné činnosti zajistit velké množství telefonní techniky, počítačových sestav aj. digitální techniky, také SIM apod. A to jak aktuálně využívanou techniku, tak odloženou z dřívějších skutků.

Dále je běžné v rámci prověřování a raného vyšetřování zajistit velké množství jiných soudních důkazů, například:

- evidenční záznamy z telekomunikační činnosti (datový i telefonní provoz),
- evidenční záznamy o využití sítě Internet (IP log),
- evidenční záznamy k SIM a IMEI (vzájemné vazby, místa prodeje, způsoby a částky z dobíjení kreditu apod.,
- evidenční záznamy k uživatelským účtům (registr a log z využití),
- bankovní záznamy a protokoly,
- textová komunikace,
- digitální písemnosti,
- jiné obrazové materiály zpracované digitálně,
- kamerové záznamy (z bankomatů a okolních kamerových systémů).

- záznamy o využití dopravních prostředků,
- záznamy z automatické kontroly vozidel.

V pozdější fázi vyšetřování jsou rovněž důležité důkazní materiály představující kriminalistické expertízy, znalecké posudky a jiná odborná zkoumání. Především z oblasti výpočetní techniky při zjišťování obsahu z digitálních nosičů. A využité běžným způsobem mohou být i zvláštní způsoby dokazování[43] (konfrontace atd.).

3.3 Zvláštnosti předmětu vyšetřování

Typické zvláštnosti předmětu vyšetřování, které se v rámci kriminality fiktivních bankéřů pravidelně objevují, jsou:

a) **Ustanovení osob, jejich podíl a popis zločinecké organizované struktury**. Kriminalita přesahující hranice států obvykle bývá páchána formou trestné součinnosti. Přeshraniční charakter stěžuje proces odhalování, objasňování a vyšetřování trestné činnosti, a to bez ohledu na to, jestli se jedná o volnější strukturu zločinecké skupiny nebo přímo o organizovanou skupinu s vnitřním řádem a hierarchií. U kriminality fiktivních bankéřů obvykle nejsou známky o tom, že by byl skutek spáchán přímo organizovanou skupinou. Skutek často bývá proveden ve spolupráci dvou, někdy více osob. Identifikace spolupracující přeshraniční skupiny je složitým procesem a je nutné mezinárodní spolupráce a zapojení více policejních složek. U osob, které přebývají v zemích, které jsou cílené na oběti, je nutné přesně identifikovat jejich funkci a zapojení v rámci trestné součinnosti. Zpravidla to bývají osoby, jejichž bankovní účty slouží k dočasné legalizaci, provádějící výběry peněz z bankomatů pomocí tokenu platební karty nebo získávají další osoby do součinnosti. Problematické je, že tyto osoby nemusí znát ostatní členy a už vůbec nemusí mít povědomí o rozsahu trestné činnosti. Jejich úkoly jsou přesně určené a jejich odměnou jsou promile z výnosů. Naopak na straně odkud je trestná činnost realizována, lze předpokládat výskyt osob s vyšším funkčním zařazením. Tyto osoby zpravidla mají o rozsahu činnosti skupiny už zásadní znalosti a není obtížné je identifikovat. Od ostatních se výrazně odlišují především náplní své činnosti.

[43] Tamtéž, § 104a, 104b, 104c, 104d, 104e.

Dále jsou zde osoby, které provádí samotnou podvodnou činnost – navolávání. Těchto osob bude obvykle více.

b) **Legalizace výnosů z trestné činnosti z nedbalosti**. Jednou ze sekundárních forem páchání této kriminality je získávání zmanipulovaných osob a jejich bankovních účtů pro přesuny peněz. Pachatelé řetězení účtů obětí využívají ke kumulaci peněz. Navíc rychlým přesouváním z účtu na účet snižují rizika jejich zajištění ze strany OČTŘ. Osoby, které provádí transakce na základě pokynů pachatele, byť jednají v omylu a neúmyslně, mohou se dopouštět trestného činu *Legalizace výnosů z trestné činnosti z nedbalosti*[44].

c) **Zkoumání, zda se jedná o individuální nebo dílčí skutek pokračující trestné činnosti**. Zřejmě žádná jiná trestná činnost neumožňuje tak efektivní pokračování jako ta, která je páchaná v kyberprostoru a ostatních mobilních sítí. Počáteční extrémní latentnost umožnuje nerušené vyhledávání dalších obětí a zdokonalování vlastních metod páchání. Policejní orgán se v případě činu spáchaného prostřednictvím sítí musí vždy věnovat otázce, zde se jedná o samotný nebo dílčí skutek pokračující trestné činnosti.

d) **Zkoumání, jaká kriminální metoda byla použitá**. Nejedná se jen o okolnosti, které spáchání trestného činu umožnily, ale především jestli byl použit jeden ze stávajících kriminálních postupů, které už jsou policejnímu orgánu známé, nebo se jednalo o nově zkoušený způsob, ve kterém byly využity nové postupy, techniky a prostředky. Porozumění způsobu provedení je důležité i z pohledu následné prevence.

e) **Vyhledávání a identifikace výnosů**. Vysoké procento výnosů je směřováno do kryptoměn, které jsou využívány pro maskování. V současné době nejsou kryptoměny globálně vyřešeny, a tak není vhodné striktně stanovit postup. Navíc procesy a způsoby těžby informací prochází neustálou proměnou. Možné je jen doporučit využití všech prostředků, které jsou v dané době dostupné, a především využívat stále rostoucí možnosti trasování kryptoměn. Identifikace výnosů je jedna z více cest, kterým policejní orgán může odhalit osoby, které stojí za trestnou činností fiktivních bankéřů.

[44] Zákon č. 40/2009 Sb., *trestní zákoník* v posledním znění, § 217.

Nad rámec uvedených zvláštností je další otázkou reálnost činu. Není vyloučeno, že kriminalita fiktivních bankéřů se může stát krytím k vlastnímu obohacení. Není to rozhodně běžné, spíše jen možné, aby inscenovaný skutek o fiktivním bankéři maskoval jiný podvod – například scénář o domnělé oběti – majitele účtu, který nejdříve získal peníze z půjčky, provedl anonymizovaný vstup do svého bankovnictví a sám peníze odčerpal a ukryl do kryptoměn, přičemž následně oznámil, že byl podveden ze strany neznámé osoby vydávaje se za bankéře. Kvalita provedení takového činu by byla zásadní, neboť absence typických prvků skutku může vést OČTŘ k podezřením.

Ačkoliv se kriminalita fiktivních bankéřů opírá o podvodný charakter, dokazování subjektivní stránky nebude obecně činit větší obtíže, jako tomu je u obecných podvodů, a proto tomu není nutné věnovat pozornost.

3.4 Typické podněty k vyšetřování a jejich zvláštnosti

Z vyšetřovací praxe je známo, že oznámení je typicky provedeno obětí po činu nebo o jeho pokus.

Dále je možné získat informace, že byl spáchán podezřelý čin ve smyslu podvodu s fiktivním bankéřem od zdrojů:

- Finanční analytický úřad (zkráceně FAU),
- bankovní společnosti,
- mezinárodní spolupráce,
- a vlastní zjištění Policie ČR.

Jak bylo výše uvedeno, tak typické a nejčastější oznámení je přímo od oběti. Podnět může být se značnou časovou prodlevou od doby spáchání. To záleží na úspešnosti pachatele a výši způsobené škody. Z počátku poskytnuté informace jsou zpravidla správné a pravdivé, avšak někdy mohou být matoucí, nesprávně vyložené až nepřesné nebo nesprávně vysvětlené až zavádějící, popř, některé skutečnosti si oběť nemusí vůbec vybavit nebo s činem spojit. Především záleží na osobnosti oběti a na schopnosti zpracovat stresové situace. Jde především o technickou stránku podvodu, a pokud si oběť situaci nevybavuje, může nechtěně uvést nesprávné vysvětlení. Naopak některé oběti si nemusí uvědomovat jednoznačnost provedení skutku a budou typicky trvat nad chybou bank a jejich

nedostačujícího zabezpečení. Informace a materiály od obětí zpravidla ze začátku postačí k vytvoření si obrazu o situaci a spáchaném skutku. A později, s ohledem na specifičnost pachatelova jednání, je možné další informace doplnit. Oběti jsou zpravidla nápomocny OČTŘ a mají zájem na dopadení pachatele.

FAU při plnění své funkce finanční zpravodajské jednotky může získat informace o podezřelých aktivitách na bankovních účtech. A v případě že dojde k závěru o okolnostech, že mohlo dojít ke spáchání trestného činu, provede oznámení příslušnému policejnímu orgánu. V těchto případech je nutná finanční analýza bankovních transakcí na zdrojových a cílových účtech s cílem identifikovat, jestli se jedná o účet oběti, která byla k činu zmanipulována nebo se jedná o účet uvědomělého účastníka trestné součinnosti.

Banky typicky v rámci vlastních kontrolních mechanismů analyzují bankovní účty a transakce. A v případě, že zjistí podezřelé aktivity, mohou od majitelů účtů požadovat vysvětlení, popř. provést oznámení policejnímu orgánu s podezřením typicky na legalizaci výnosů z trestné činnosti bez ohledu na zavinění. Další postup je obdobný jako u FAU, a proto není nutné tomuto věnovat další prostor.

Mezinárodní justiční nebo policejní spoluprací lze získat informace o trestné činnosti fiktivních bankéřů v situacích, kdy zahraniční policejní orgán šetřením zjistil informace o trestné součinnosti s mezinárodním přesahem. Informace zpravidla bývají správné a přesné, nicméně je nutné vhodně je doplnit z tuzemských zdrojů. V těchto případech je nutná přeshraniční aktivní spolupráce policejních orgánu a cílit na vytvoření společných vyšetřovacích týmů.

Vlastním zjištěním ze strany policejního orgánu jde především o situace:

a) **Zjištění příjmu peněz na účtu dřívější oběti**. V rámci prověřování případu při pozdějším analytickém vyhodnocení bankovního účtu oběti je možné zjistit příjem, který oběť nedovede vysvětlit, nezná zdroj peněz a také bankovní účet. Následným prověřením je zjištěna osoba – typicky další oběť, která byla rovněž podvedena, avšak dosud oznámení sama neučinila nebo si zatím nebyla vědoma toho, že byla obětí podvodného jednání fiktivního bankéře. Nutno uvést, že dřívější oběť, na jejímž bankovním účtu byla transakce zjištěna, nemusí o transakci skutečně zpočátku vědět. Banky po oznámení provedenou

blokaci internetového bankovnictví a občas nové přístupy uživatel účtu získá po delším časovém odstupu.

b) **Zjištění v rámci prověřování jiného skutku**. Osoby napojené na fiktivní bankéře mohou být zapojeny do dalších podvodů a typicky v rámci odposlechů mohou být zjištěny poznatky o této další trestné činnosti.

c) **Přítomnost osoby u automatu na nákup kryptoměn**. Posledním ale velmi zvláštním typem vlastního zjištění skutku je situace, při které náhodně jdoucí obeznámený policista zjistí přítomnost osoby u automatu na nákup kryptoměn, přičemž osoba možné oběti vzbuzuje dojem zmatenosti nebo přímo udivenosti. Tyto osoby se často od běžných uživatelů těchto kryptoměnových automatů odlišují stářím, sériovým vkládáním velkého objemu peněz nebo neustálým telefonováním, a to s pachatelem, který takto úkoluje oběť. Stává se, že osoby, které jsou osloveni s upozorněním, reagují podrážděně a nepřijímají varování.

3.5 Typické vyšetřovací situace

Typické vyšetřovací situace je možné rozdělit do skupin podle počátečních priorit ve vztahu uplynulé doby od skutku k oznámení, podle znalosti především o osobě pachatele, zapojených osob a prvotních informací o skutku.

a) **Skutek byl spáchán a oznámení bylo provedeno až s odstupem času**. Běžná situace bez ohledu na vývojové stádium, která nevyžaduje nutné rychlé reakce. Postupuje se běžnou cestou s cílem ověřit oznámené skutečnosti, vyhledat nové dostatečné informace a provést nezbytná šetření s cílem ztotožnit pachatele, legalizátory, zajistit výnos a případně identifikovat další oběti.

b) **Skutek byl spáchán v blízké době a je nutná rychlá reakce a aktivní činnost policejního orgánu**. Jedná se zejména o situace s cílem identifikovat bankovní účty nebo využité kryptoměnové adresy, na které byly peníze odkloněny a provést zajištění výnosu. Dále se jedná o ty výjimečné situace, při kterých oběť peníze předala osobně a je nutno provést bezodkladné pátrání. Tato situace je tedy zaměřená na zajišťovací úkony a zjištění totožnosti osob. Záměrně je uvedeno zjištění totožnosti osob, nikoliv zadržení podezřelého. Po identifikaci osoby jednající v trestné součinnosti je zpravidla výhodnější se zadržením vyčkat, to však záleží na aktuálních situačních

okolnostech, a případně před zadržením upřednostnit provedení operativně pátracích úkonů (typicky sledování osob a odposlechy), zmapovat možná propojení a zajistit si počáteční informace k výchozímu popisu struktury skupiny pachatelů.

c) **Jsou známy kusé informace, které je nutno ověřit**. Tato počáteční situace vychází ze skutečnosti, že mohou být zjištěny skutkové okolnosti jako čas, místo (bankovní účty) a možná peněžní škoda, avšak není známa osoba oběti ani pachatele. Je nezbytné provést šetření a doplnit nutné informace s cílem ověřit spáchání skutku. V případě, že bude zjištěno, že se nejedná o podezření z trestného činu, případ bude založen.

Podle situačních okolností jsou tedy typické prvotní vyšetřovací situace následující:

- skutek se stal a pachatel není znám,
- skutek se stal a je nutné pátrat po horké stopě,
- skutek se stal, je známa osoba legalizátora a není znám pachatel,
- podezřelá situace, není známa oběť ani pachatel.

Podvody fiktivních bankéřů jsou mladou stále vyvíjející se kriminalitou, navíc velmi úspěšnou, a přesto z toho mála dosavadní vyšetřovací praxe lze po zahájení trestního stíhání vymezit situace:

- obviněný doznává trestnou činnost i případné zapojení a postavení v rámci zjištěné formy trestné součinnosti,
- obviněný částečně doznává trestnou činnost, odmítá sdělené postavení v rámci popsané formy trestné součinnosti,
- obviněný odmítá trestnou činnost a také případnou formu trestné součinnosti,
- obviněný účelově vypovídá,
- obviněný odmítá vypovídat.

Negativní vyšetřovací situace, které mohou nastat z důvodu odmítajícího postoje obviněného, musí být řešeny aktivní vyšetřovací činností společně s využíváním všech dostupných zákonných prostředků. Typickým prostředkem je snaha získat

a využít spolupracujícího obviněného[45], který musí významně přispět k objasnění zločinu spáchaného v organizované součinnosti.

3.6 Typické počáteční úkony a jejich zvláštnosti

Počáteční úkony a jiná přijatá opatření jsou typická pro jakýkoliv okruh kriminality. Jejich pořadí, význam a způsob provedení se běžně odvíjí od situačních okolností případu a nelze kategoricky stanovit jejich pořadí. Pouze je možné je typově uvést, neboť jejich provedení lze v průběhu prvotních etap vyšetřování očekávat.

Obecně je nutno lpět na včasnosti, důvodnosti a zákonnosti prováděných úkonů.[46]

Typické úkony, které je nutno provádět spěšně, jsou zajišťovacího charakteru, tj. zajištění osob, výnosu, kybernetických stop, dalších časem omezených důkazů a digitálních dat, což je v případech páchaných v kyberprostoru a mobilních sítí běžné.

Souhrn všech typických opatření:

- provedení výslechů obětí, případných svědků a možných podezřelých,
- provedení předložení nebo vydání věcí důležitých pro trestní řízení,
- provedení prohlídek,
- provedení ohledání veřejně dostupných kybernetických dat a soukromých dat s umožněným přístupem uživatele,
- využívání operativně pátracích prostředků,
- zajištění tzv. data freezingu[47],
- zajištění podezřelých,
- zajištění materiálů od obětí,
- zajištění kriminalistických stop a jiných soudních důkazů,
- zajištění nástrojů a výnosů z trestné činnosti,
- zajištění kamerových záznamů,
- zajištění evidenčních a registračních informací,
- zajištění bankovních informací,
- zajištění provozních a lokalizačních informací,

[45] Zákon č. 141/1961 Sb., *o trestním řízení soudním (trestní řád)* v posledním znění, § 178a.
[46] Tamtéž, § 157.
[47] Dočasná ochrana digitálních dat před samovolným nebo automatizovaným odstraněním.

- zajištění odborných a expertních vyjádření, využívání konzultací,
- zajištění typických podkladů k posouzení finančních poměrů osob,
- zajištění ostatních nezbytných procesních písemností,
- zajištění analytického vyhodnocení,
- předání informací, zveřejnění a prevence,
- spolupráce s dalšími organizačními složkami státu a se specializovanými součástmi Policie ČR,
- spolupráce mezinárodní a justiční,
- vyhledávání a využívání metodik,
- vyhledávání doporučení a pokynů k postupu od ÚSKPV.

Výslech oběti je typicky zaměřen na zodpovězení všech kriminalistických otázek s důrazem na průběh skutku, využité komunikační prostředky a použité personálie pachatele. Znalost průběhu skutku je nesmírně důležitá, neboť lze odvodit, jaká forma způsobu provedení byla využita a případně identifikovat nové postupy pachatelů. Informace o využitých komunikačních prostředcích jsou zase důležité pro počáteční šetření, zajišťování stop a trasování hovorů. Personálie a údaje o pachateli, např. použitá jména, telefonní čísla, přezdívky v komunikačních aplikací, e-mailové adresy atd., jsou samozřejmě vylhaná a není třeba je nějak zvláště ověřovat. Jejich přínos je spíše pro vyhledávání dílčích skutků.

Výslechem oběti rovněž musí být zjištěn popis pachatelova hlasového projevu. Použitý jazyk, nářečí, přízvuk a jiná hlasová specifika.

Dále je vhodné při výslechu zjistit, jestli pachatel o oběti dopředu neznal už nějaké informace. Personálie oběti jsou často zjistitelné po internetu, přes různé sociální sítě, kde je oběť aktivní, z uniklých databází atd. Avšak je rovněž možné, že oběť byla pachatelem kontaktována už dříve. Například pod záminkou reklamního marketingu, přičemž vhodně zvolenými otázkami pachatel získal nezbytné další údaje.

Od oběti je dále nutné správně zajistit veškeré materiály, které vznikly v souvislosti s případem, přepisy textové komunikace aj. další data, která vznikla. Dále je nutno provést u oběti ohledání věci a zajistit tzv. metadata v mobilním nebo počítačovém systému, která vznikla při používání aplikací a komunikací. Získání souhlasu oběti

k prolomení tzv. bankovního tajemství[48] je rovněž neméně důležité. A dále souhlas k zajištění telekomunikačních dat[49] o provozu telefonního čísla oběti.

Bankovní zpráva se souhlasem oběti zpravidla obsahuje informace o transakcích, výběrech peněz, o vloženém novém zařízení a jeho aktivaci, vytvořených tokenů platebních karet atd. Záznamy o internetovém využití bankovnictví jsou obvykle nepoužitelné, zaleží ale na specifickém postupu pachatele, přičemž v případě použití aplikací pro vzdálenou správu, jsou zaznamenané IP adresy oběti, respektive koncového zařízení, které oběť použila. Pachatele totiž pomocí aplikace vzdálené správy přes zařízení oběti vstupuje do bankovnictví.

Telekomunikační záznamy o provozu při činu použitého telefonního čísla oběti jsou nesmírně důležité a provedeným šetřením u poskytovatele mobilních služeb je možné získat nezbytné telekomunikační informace o využití telefonních čísel pachatele, popř. zjistit, jestli bylo použito maskování ID volajícího. V tomto případě následným trasováním se lze pokusit zjistit směřování hovoru – zdroj.

Zajišťování výnosů na bankovních účtech a zamrazení kryptoměn jsou úkony, které by měly být jedny z počátečních. Ačkoliv nemusí být případ zdárně vyřešen, tak trestná činnost by se neměla vyplácet a je nezbytné se pokusit získat nazpět veškeré odcizené prostředky.

Metadata, textové komunikace, digitální písemnosti a jiné počítačem zpracované informace, pokud je to možné, je nutné získat v originální podobě. V případech, ve kterých není možné získat originální data, jsou přípustné kopie. Z technických důvodů je přípustné provádět i snímky. Zajištění dat musí být provedeno takovým způsobem, aby zvolená cesta neumožnovala později rozpory.

Všechna zajištěná data a digitální informace musí být navíc opatřena pečetí. V praxi se běžně využívá hashovacích algoritmů[50], které v digitálním prostředí zastávají funkci podpisu a garantují pravost, nezměněnost a originalitu zajištěných dat.

[48] Zákon č. 21/1992 Sb., *o bankách* v posledním znění, § 38.
[49] Zákon č. 141/1961 Sb., *o trestním řízení soudním (trestní řád)* v posledním znění, § 88a odst. 4.
[50] Nejčastěji je využíván algoritmus SHA-256 a MD5. Nejsou vyloučené jiné.

V kriminalistické praxi jsou v případech rozsáhlejších sérií vydávány ze strany ÚSKPV koordinační pokyny, ve kterých je popsán způsob provedení, dále znaky umožňující případné společné šetření a základní pokyny k počátečním úkonům a opatřením.

3.7 Typové vyšetřovací verze a organizace vyšetřování

3.7.1 Vyšetřovací verze

U kriminality fiktivních bankéřů je zpravidla vycházeno z předpokladu, že skutek byl reálně spáchán, a proto je možno běžně stanovit následující verze.

a) **Verze o počtu pachatelů**. Jedná se o základní předpoklad u spáchaného skutku a s ohledem na počáteční informace je už možné předběžně stanovit, zda pachatel jednal sám, což není běžné, nebo v nějaké trestné součinnosti a případě kolik přibližně osob je do trestné činnosti zapojeno a jaká je jejich organizovanost.
b) **Verze o počtu skutků**. Je možné očekávat, že pachatel neskončí u jednoho skutku a bude v trestné činnosti pokračovat. Pomocí zjištěných personáliích o pachateli, které při činu použil, je možné následnou analytickou činností prověřit, zda se jednalo o dílčí skutek pokračující trestné činnosti.
c) **Verze o pobytu a pohybu pachatele**. U trestné činnosti páchané distančně prostřednictvím komunikačních sítí je vždy možné vytyčit verze o pobytu pachatele, respektive jestli je jeho pohyb vnitrostátní, zahraniční nebo zahrnuje oboje možnosti.
d) **Verze o členech organizované skupiny**. V situacích, ve kterých je podezření, že skutek byl spáchán organizovanou skupinou, je možné vytyčit verze o tom, jestli zlončická skupina začlenila osoby, které podobnou trestnou činnost v minulosti realizovaly, nebo se jedná o nově zformovanou z osob nemající trestní minulost. Kombinace není vyloučena.
e) **Verze o podvodném propojení**. Z kriminalistické praxe je de facto známo, že u případů páchaných přes síť Internet a mobilní sítě, jsou různé variace podvodů nějakým způsobem propojené (např. přes legalizátory) a mohou je páchat stejné osoby. Po zjištění základních skutkových okolností je vhodné pokusit se stanovit, zda se jedná o pachatelé specializující se na bankovní distanční podvody nebo je jejich kriminální činnost různá.

f) **Verze o typovém způsobu provedení**. Ze způsobu provedení musí policejní orgán vždy odvodit, jestli použitá kriminální metoda je známa, nebo se jedná o nový způsob, popř. jaké k tomu bylo využito technologie nebo zneužitých prostředků, jaké slabiny v opatřeních byla obejita, jak se ovlivňují a jaká šetření umožnují. A jaké jsou možnosti obrany.

3.7.2 Organizace vyšetřování

Organizace vyšetřování u typické kriminality fiktivních bankéřů je obvykle nutná jen v situaci, ve které je vyšetřována série trestné činnosti nebo je plněno více úkolů v zahraničí.

Spisový rozsah případu může být značný až extrémní a je dopředu nutné stanovit cíle, které je potřeba vyšetřováním naplit. Cílům musí odpovídat přijatý plán, který je reálný a také uskutečnitelný. Musí být stanoveny jednotlivé úkoly a určeni pracovníci, kteří je budou plnit. Není vyloučeno, že některé plánované úkony mohou být provedeny i dožádáním jiného úvaru.

Součástí organizace je nutná, jak spolupráce více specializovaných složek Policie ČR, tak i aktivní účast státního zastupitelství, které musí být jednak srozuměno s postupem vyšetřování a dále s jeho vytyčeným cílem, a to mj. kvůli úkonům prováděných v zahraničí.

Mezinárodní spolupráce při provádění obtížných a náročných úkonů může vyústit až do vytvoření společného vyšetřovacího týmu dvou nebo více dotčených států. Na území České republiky vyšetřovací tým vede státní zástupce vykonávající dozor.[51]

V případech vyšetřování mezinárodní zločinecké organizace je nutné dopředu znát právní úpravu a okolnosti, při kterých se úkony realizují. A obecně je dobré, aby vyšetřovatel předpokládal budoucí vývoj a pružně přizpůsoboval prováděné operativní a vyšetřovací úkony ve spolupráci s dozorujícím SZ.

[51] Zákon č. 104/2013 Sb., *o mezinárodní justiční spolupráci ve věcech trestních* v posledním znění, § 73 a § 185.

3.8 Zvláštnosti následné etapy vyšetřování

Obecně u kriminality páchané v kyberprostoru a mobilních sítí je doporučeno, aby realizaci a vedení úkonů především prováděl vyšetřovatel, který má potřebnou odbornost anebo alespoň elementární znalosti o okruzích problematiky.

Reálné obtíže, které vznikají jsou zpravidla v důsledku mezinárodního charakteru této trestné činnosti a tím spojeného získávání informací ze zahraničí a provádění úkonů v zahraničí.

Je nutno zdůraznit, že většina kriminalistických úkonů a postupů a jejich provedení v rámci vyšetřování fiktivních bankéřů nijak více nevybočuje od vysokého standardu, který je napříč celou kriminalistickou činností a používanými konkrétními metodikami vyšetřování. A proto není nutné všechny úkony znovu popisovat.

Kriminalita fiktivních bankéřů je sice speciálním typem provedení podvodu, avšak je možno odkázat na většinu vyšetřovacích úkonů, jako je například přibrání znalce, do obecných metodik, které jsou o vyšetřování všeobecných podvodů, dále o organizované a kybernetické kriminalitě.

Zmíněný znalec je sice velmi důležitou osobou mj. v rámci kriminality fiktivních bankéřů, avšak jeho účast je zpravidla obdobná k účasti v obecné metodice vyšetřování kybernetické kriminality.[52]

Pozornost proto bude v nezbytném rozsahu věnována pouze osobě svědka a obviněného.

3.8.1 Svědek

Primární osoba svědka je zpravidla osoba oběti a té byla už věnována pozornost v rámci subkapitoly 3.6 (typické počáteční úkony). Jen krátce shrnu, že osoba oběti poskytuje informace o průběhu skutku, jednání pachatele anebo pachatelů a o projevů pachatele. Zpravidla je to jediná osoba, která vyjma obviněného, byla součástí trestné činnosti. A její paměťovou stopu je nutno kompletně vytěžit.

[52] Např. NĚMEC, Miroslav et al. *Teorie a metodologie kriminalistiky pro magisterské studium – II. díl. Aktuální problémy kriminalistické praxe*. Praha: ABOOK, 2019. ISBN 978-80-906974-2-3, s. 319-322.

Sekundární osoba svědka je typicky specialista v oblasti, který poskytuje znalosti o technické a technologické stránce podvodu, jako jsou skutečnosti o bankovním systému, operacích a zabezpečení. Dále specialista vypovídající o možnostech, funkčnosti a operacích komunikačních sítí atd.

Osoba svědka v postavení specialisty na problematiku je velmi důležitou osobu v těch případech, kdy obviněný nespolupracuje nebo byla odstraněna technická výbava a další nástroje k trestné činnosti, které by běžným znaleckým zkoumáním mohly některé tyto otázky zodpovědět.

3.8.2 Obviněný

Obecné provedení výslechu u obviněného nevybočuje, je prováděn s ohledem na jeho postavení v systému zločinecké struktury a nutné je se více zaměřit:

- na technickou stránku, využité prostředky, jakým způsobem byly získány a způsob využívání sociálního inženýrství,
- způsob anonymizace v sítích,
- podíl účastníků trestné součinnosti a jejich zapojení,
- způsob využívání zahraničních kontaktů,
- způsob krytí výnosů a identifikace výnosů,
- identifikaci dalších obětí,
- a na zapojení do dalších podvodných aktivit.

3.9 Zvláštnosti zapojení veřejnosti do vyšetřování

Transparentnost s ohledem na zákonnou neveřejnost přípravné fáze trestního řízení a zapojení veřejnosti do vyšetřování jsou stále významnější otázky.

Všeobecně je známo, že veřejnost podle typu kriminality reaguje velmi odlišně. Kyberkriminalita je vnímána spíše méně negativně, i když se především jedná o podvodná jednání, která jsou jinak velmi citlivá témata. Dehonestace a další prvky sekundární viktimizace jsou v případech kyberkriminality velmi časté.

U případů fiktivních bankéřů je možno zapojení veřejnosti rozdělit na dvě části.

V první části zapojení veřejnosti se jedná o využití obyvatelstva jednak k pátrání po totožnosti pachatelů, například pomocí fotografie osob, které provedly výběr peněz z bankomatů. A dále při pomoci s vyhledáváním dalších obětí.

Ve druhé části už cílíme na prevenci a máme na mysli edukaci s upozorněním obyvatelstva na způsob páchání trestné činnosti. Je velmi důležité srozumitelně vysvětlovat podstatu základu způsobu provedení trestné činnosti a pokusit se ochránit další potencionální oběti, tedy zmírnit budoucí následky.

Boj proti podvodům fiktivních bankéřů je ale nutný realizovat na více frontách. Po technické stránce jsou už upravována pravidla používání bankovních účtů, jsou přidávána ochranná opatření a v rámci možností omezována překrytá volání atd. (viz 4. kapitola).

Výsledky terénního šetření ukazují na to, že spoofing sice slouží jako maskovaní a ztěžující opatření pachatelů pro případné dohledávaní hovoru, ale i když použitý kontakt neodpovídá bance nebo policii, jsou úspěšní. Přes všechna organizační a technická opatření je proto důležitá dlouhodobá vzdělávací kampaň a osvěta obyvatelstva, protože pouze oběti tuto kriminalitu umožňují. Majitel účtu je jediný, vyjma banky, který plné ovládá účet, provádí uživatelská nastavení a mění limity a pravidla využívání platebních prostředků. Pachatel, který ovládne oběť, ovládne bankovní účet. A tím jsou všechna technická a bezpečnostní opatření zmařena.

Téměř denně je možné se setkat s různými upozorněním bank, policie aj. institucí. Jsou medializované případy různých podvodů. Využívány jsou různé přenosové kanály, od televizního zpravodajství, novinové a internetové články, newslettery až po články na sociálních a trendových sítích. Otázkou je proč to není účinné?

Je patrné, že širší obyvatelstvo není dostatečně připraveno a nemá dostatečné povědomí o tom, jak fungují mobilní sítě, o existenci prostředků, které umožnují měnit informace o hovoru atd. A také o systému bank, které zásadně nemusí mít součinnost klienta k ochraně peněz.

Konkrétní způsoby prevence jsou například informační sdělení na automatech určených k nákupu kryptoměn, zdařilá bankovní kampaň nazvaná „Volač a Klikač okrádají Česko“[53] nebo vzdělávací kampaň #nePINdej![54], informační upozornění při používání bankovních aplikací apod.

[53] Prezentována je ČSOB, a. s., se sídlem Radlická 333/150, 150 57 Praha 5, IČ: 00001350.
[54] Prezentována je Českou bankovní asociací, se sídlem Italská 69 (Budova Churchill II), 120 00 Praha 2, IČ: 45772193.

4 Závěrečné úvahy

4.1 Opatření

Stejně důležité jako je postavit pachatele před spravedlnost, je nutno znemožnit nebo znesnadnit páchání budoucí trestné činnosti. Některá opatření byla mj. proti kriminalitě fiktivních bankéřů už přijata.

Opatření je možné rozdělit na:

a) informační (např. upozornění a vzdělávání obyvatelstva),
b) technická (např. ochrana mobilních sítí a bankovního systému),
c) organizační (typicky kooperace zainteresovaných institucí, aktivní přístup k vyhledávání a potírání kriminality).

Ad a) Informační opatření byla de facto popsána více už v přechozí subkapitole 3.9, a proto jim zde nebude věnována další pozornost.

Ad b) Technická opatření telekomunikačních společností jsou na bázi samoregulace s cílem identifikovat (zahraniční) spoofing, např. implementací technologie STIR/SHAKEN (dále viz níže) nebo vytvářet tzv. blacklist, a tedy následného potlačení spojení podvodných hovorů.

Je však nutno postupovat opatrně, neboť opatření mohou narážet na povinnost plynoucí z telekomunikačního zákona propojit všechna spojení.

Podezřelé hovory jsou typicky takové, kdy například telefonní číslo reprezentující běžnou pevnou linku České republiky volá z ciziny. Anebo podle geolokačních dat identifikovaný hovor z České republiky, který ale je přepojen přes zahraničního operátora.[55]

Technologie STIR/SHAKEN byla vyvinuta ve spolupráci mezi telekomunikačními společnostmi, vládními úřady a regulačními orgány k boji proti telefonním podvodům. Standard je označovan jako *Secure Telephone Identity Revisited*

[55] Český telekomunikační úřad. *ČTÚ pomůže výrazně omezit spoofing: Mnoho podvodných hovorů už nebude spojeno*. Online. Dostupné z: https://ctu.gov.cz/tiskova-zprava%3A-ctu-pomuze-vyrazne-omezit-spoofing%3A-mnoho-podvodnych-hovoru-uz-nebude-spojeno. [cit. 01.04.2024].

(zkráceně STIR) a *Signature-based Handling of Asserted information using toKENs* (zkráceně SHAKEN).

Tato technologie pracuje tak, že poskytuje mechanismus pro ověření identity volajícího, který umožňuje operátorům telefonního hovoru označit volání jako legitimní nebo potenciálně nebezpečné. To se děje pomocí digitálního podpisu, který je vytvořen uživatelem nebo operátorem volání a ověřen opačnou stranou prostřednictvím certifikátu.

STIR/SHAKEN pomáhá eliminovat podvodná navolávání a zvýšit důvěru v sítě.[56]

Bankovní instituce krom masivní informační kampaně zavádí analyticko-technická opatření, která např. spočívají v automatizované kontrole bankovních účtů. Pokud systém vyhodnotí, že transakce nebo výběry jsou nestandardní, může dojít k pozastavení účtu a bankovní úředník provede ověření u majitele účtu. Dalším typickým opatřením je postupné zavedení dvoufázového ověření při vstupu do internetového bankovnictví a při provedení transakce.[57]

Ad c) Organizační opatření jsou především reprezentována proaktivním přístupem proti kybernetické kriminalitě, jejího aktivního vyhledávání a potírání.

V rámci České republiky vznikla pracovní skupina složená ze zástupců Policie ČR, bankovní asociace, Českého telekomunikačního úřadu, asociace provozovatelů mobilních sítí, dalších odborníků a bezpečnostních specialistů, za účelem předávání informací, informování o postupů pachatelů a vypracování a stanovení možností, jak omezit jejich činnost a ochránit obyvatele.

4.2 Zahraničí

Problematikou spoofingu se samozřejmě potýkají i zahraniční policejní orgány, banky a telekomunikační společnosti. Bohužel zatím není ustanovena žádná plošná strategie, ani v rámci Evropské unie, a státy reagují různě. Jsou to spíše

[56] Federal Communications Commission. *Combating Spoofed Robocalls with Caller ID Authentication*. Online. Dostupné z: https://www.fcc.gov/call-authentication. [cit. 01.04.2024].
[57] Metro. *Spořitelna do boje proti kyberšmejdům nasadila speciální klientský tým*. Online. Dostupné z: https://www.metro.cz/protext/sporitelna-do-boje-proti-kybersmejdum-nasadila-specialni-klientsky-tym.A230906_105000_metro-protext_air. [cit. 06.04.2024].

universální opatření plošného charakteru. Na výsledky se vyčkává a v současné době není jisté, která strategie je správná.

Například Evropská unie přijala opatření mj. k boji proti spoofingu, které obecně zahrnují:

1. Směrnice EU o síťové a informační bezpečnosti (NIS Directive)[58]. Směrnice stanovuje povinnosti pro poskytovatele digitálních služeb a provozovatele kritické infrastruktury v oblasti ochrany proti kybernetickým hrozbám, včetně spoofingu.
2. Nařízení GDPR[59]. Obecné nařízení o ochraně osobních údajů obsahuje ustanovení o zpracování osobních údajů v rámci kybernetických útoků, opět včetně spoofingu.
3. Spolupráce s členskými státy a mezinárodními organizacemi. Evropská unie spolupracuje s členskými státy a mezinárodními organizacemi, jako je *Organizace pro hospodářskou spolupráci a rozvoj* (zkráceně OECD) nebo *Mezinárodní telekomunikační unie* (zkráceně ITU), na opatřeních proti kybernetickým hrozbám.
4. Finanční podpora a výzkum. Evropská unie poskytuje finanční prostředky a podporuje výzkum v oblasti kybernetické bezpečnosti, aby posílila schopnost členských států bojovat proti spoofingu a dalším kybernetickým hrozbám.[60]

Opatření států Evropské unie proti vishingovým podvodům v bankovnictví se mohou v podrobnostech lišit, ale obecně se dají uvést následující:

[58] EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Online. In: *Úřední věstník Evropské unie*. 2016, L 194/1, s. 1-30. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32014L0041. [citováno 01.04.2024].
[59] EVROPSKÁ UNIE. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Online. In: *Úřední věstník Evropské unie*. 2016, L 119/1, s. 1-88. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679. [citováno 01.04.2024].
[60] European Commission. *EU anti-fraud measures*. Online. Dostupné z: https://commission.europa.eu/strategy-and-policy/eu-budget/how-it-works/annual-lifecycle/implementation/anti-fraud-measures_en. [cit. 01.04.2024].

1. Informační kampaně. Většina států Evropská unie provádí informační kampaně zaměřené na osvětu veřejnosti o rizicích vishingových podvodů a jak se jim vyhnout.
2. Spolupráce mezi bankami a bezpečnostními orgány. Banky spolupracují s bezpečnostními orgány a sdílí informace o vishingových podvodech, aby byly rychle odhaleny a zastaveny.
3. Technologická opatření. Banky investují do technologií, které jim pomáhají detekovat podezřelé transakce a podvodné telefonické hovory.
4. Dvoufázové ověření. Většina bank zavádí dvoufázové ověření transakcí, což zvyšuje bezpečnost účtů a brání vishingovým podvodům.
5. Spolupráce se zahraničními partnery. Vzhledem k tomu, že vishingové podvody mohou být koordinovány mezinárodně, státy Evropská unie spolupracují se zahraničními partnery a sdílí informace o podvodech.
6. Legislativní opatření. Některé státy Evropská unie přijímají legislativní opatření, která zvyšují tresty za provádění vishingových podvodů a zlepšují ochranu obyvatelstva.[61]

Například německé banky přijímají různá opatření proti vishingovým podvodům v bankovnictví a snaží se chránit své klienty před ztrátou finančních prostředků. Mezi tyto opatření patří:

1. Posílení bezpečnostních systémů a technologií pro identifikaci a ověření klientů při provádění bankovních transakcí.
2. Poskytování školení a osvěty klientům o rizicích vishingových podvodů a způsobech, jak se jim vyhnout.
3. Zavedení dvoufázové autentizace pro přístup k bankovním účtům a provádění transakcí.
4. Monitorování podezřelých aktivit na bankovních účtech a rychlá reakce v případě podezřelých transakcí.
5. Spolupráce s dalšími bankami a institucemi v rámci sdílení informací o vishingových podvodech a společného boje proti nim.

[61] European Commission. *Cybersecurity Policies*. Online. Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies. [cit. 06.04.2024].

6. Poskytování bezpečnostních tipů a rad klientům, jak chránit své bankovní účty a osobní údaje před vishingovými podvody.[62]

A němečtí telekomunikační operátoři rovněž podnikají různá opatření k ochraně před spoofingem. Patří mezi ně:

1. Implementace technologií, jako je STIR/SHAKEN, které umožňují ověření identity volající strany a udržují celý telekomunikační proces transparentní.
2. Monitoring síti a detekce podezřelých aktivit, jako je velké množství neidentifikovaných hovorů s různými mezinárodními čísly.
3. Aktivní sledování a analýza hovorů s podezřelými vzory chování nebo doporučenými varovnými známkami spoofingu.
4. Poskytování nástrojů a služeb pro zákazníky, které jim umožňují filtrovat nežádoucí hovory a blokovat neznámá čísla
5. Spolupráce s jinými telekomunikačními operátory a orgány činnými v trestním řízení k identifikaci a potrestání pachatelů spoofingu.[63]

Všechna tato, byť některá zatímní opatření, mají za cíl ochránit občany Evropské unie před kybernetickými hrozbami, včetně spoofingu, a zvýšit bezpečnost digitálního a mobilního prostředí v Unii.

Je patrné, že přijatá opatření Evropské unie a států Unie jsou velmi podobná těm, které přijímají instituce a orgány České republiky.

4.3 Predikce

S rostoucí informovaností obyvatel, regulací a ochranou telekomunikačních sítí, dojde nutně i k evoluci podvodů fiktivních bankéřů.

Samozřejmě typické a známé způsoby páchání fiktivních bankéřů úplně nevymizí. Pachatelé je zřejmě ale budou využívat ve vlnách, jako tomu je například u případů podvodů s falešnými doktory, vojáky apod. (což je typická variace tzv. nigérijských dopisů). U těchto skutků je možné pozorovat, že pachatelé provedou určitou sérii podvodů a po informační reakci ze strany policie a médií, po které lze očekávat

[62] Crowdstrike. *Was ist ein Vishing-Angriff?* Online. Dostupné z: https://www.crowdstrike.de/cybersecurity-101/vishing/. [cit. 02.04.2024].
[63] Bundesnetzagentur. *Manipulation von Rufnummern*. Online. Dostupné z: https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Manipulation/start.html. [citováno 02.04.2024].

větší obezřetnost obyvatel, činnosti na nějakou dobu zanechají. A po opadnutí zájmu a dočasné situační osvěty, opět provedou útok.

Dále je možné se domnívat, že v budoucnu bude jednak více cílených útoků a jednak budou více zapojeny bankovní a komunikační aplikace. A také se nabízí využití uměle inteligence, která přináší nové možnosti.

Cílené útoky jsou extrémní hrozbou, neboť pokud jsou správně provedeny, dokážou způsobit značné škody u jinak ostražitých a znalých obyvatel. Technická opatření sice mohou zmírnit škody, avšak pokud je oběť zcela pod vlivem pachatele, sama provede kumulaci peněz a jejich předání, nelze tomu technikou zabránit. Pomocí umělé inteligence je už nyní možné věrně napodobit hlas a s jeho pomocí bude možné provést další variace cílených útoků.

Využívání dalších podvodných aplikací pro bankovní podvody fiktivních bankéřů je už nyní možné v prvních náznacích v kriminalistické praxi sledovat.

Podle zatímních informací pachatel předběžně kontaktuje oběť například SMS zprávou, do které s vhodnou legendou umístí internetový odkaz na podvodné stránky. Oběť podle pokynů vyplní bankovní přístup, čímž ho pachateli předá. Pachatel následně z bankovnictví získá potřebné informace a provede hovor s obětí. Během hovoru s vhodnou legendou, např. o napadení účtu, využije informace už z přístupného bankovnictví, aby oběť zdárně přesvědčil. Zmanipuluje ji k nainstalování podvodné aplikace a dále přiložení platební karty k telefonu. Tato aplikace umožnuje načítat rozhodná data z karty pomocí technologie NFC, která je bezprostředně poté přenáší do zařízení pachatele – bude se jednat typicky o mobilní telefon, se kterým zřejmě spolupachatel už bude připravený u peněžního automatu. Komunikace mezi aplikacemi je obousměrná a peněžní automat registruje použití fyzické karty. Pachatel pomocí aplikace nebo hovorem dále získá od oběti potřebný PIN.

Je možné, že komunikační aplikace, typu instant messaging, vytlačí používané běžné hovory. Pokud tedy budou samoregulační opatření mobilních operátorů na vysoké úrovni a znemožní podvodná volání. V rámci těchto aplikací opatření mobilních operátorů nebudou funkční, neboť k spojení je využívána datová síť.

Závěr

Cílem této rigorózní práce bylo vytvořit typickou kriminalistickou metodiku na téma vyšetřování podvodů tzv. fiktivních bankéřů, která je řazena mezi ostatní trestnou činnost páchanou v kyberprostoru a mobilních sítí.

Domnívám se, že cíl práce jsem splnil.

Počáteční text práce byl věnován vysvětlení tématu a blízkým okruhům, které mají na téma zásadní podíl. Bez těchto základních informací by se práce neobešla a získala tím na potřebné hloubce. Nechybí ani zobecněné příklady ze současné kriminalistické praxe.

Následoval teoretický základ terénního šetření s důkladným popisem výzkumných fází, po kterém byly uvedeny všechny výsledky z rozsáhlého výzkumu. Jen krátce připomenu, že výzkum se opírá o 112 uzavřených případů z roku 2022 a 2023 vedených v rámci celého Středočeského kraje. Nezbytný dostatek informací, který byl získán, následně dopomohl k tvorbě předmětné kriminalistické metodiky, ve které jsou promítnuté i mé zkušenosti a další zjištěné poznatky z kriminalistické praxe.

Považuji za vhodné uvést, že v roce 2022 byly skutky téměř z poloviny zaměřeny na cizince – především na Ukrajince. Je pravděpodobné, že to bylo ovlivněno vojenským konfliktem a značnou uprchlickou migrací. Pachatelé jednoduše využili zmatků a situační neznalost migrujících osob. V předchozích letech byli cizinci cílem jen ojediněle, jako tomu je v roce 2023. Další výsledky z terénního šetření přinesly sice už očekávaná, avšak i tak překvapující zjištění. Všechny zkoumané případy byly neobjasněny a souhrnný zajištěný výnos se pohybuje jen okolo 5 % z 24 milionů.

Extrémní míra úspěšnosti pachatelů unikat spravedlnosti a získávat značný zisk přispívá a podněcuje je k další pokračující trestné činnosti, kterou se nedaří potírat ani zatím uspokojivě omezit.

Kriminalistická metodika vyšetřování byla zpracována s důrazem na praktičnost a reálnost situace, ve které se tato kriminalita nachází, a to s ohledem na možnosti

rigorózní práce. Metodika byla zpracována tak, aby odpovídala kriminalistickému učení, tj. od charakteristiky až po zapojení veřejnosti do vyšetřování.

Závěrečný text práce pojednává o opatřeních, zahraničním způsobu boje proti předmětné kriminalitě a také je uvedena prognóza, jak se v blízké době mohou podvody fiktivních bankéřů dále vyvíjet.

V současné době už sledujeme první náznaky upraveného způsobu páchání. Jsou využívány nové podvodné bankovní aplikace, kterými se pachatelé snaží obcházet zabezpečení bank. A bude také zajímavé sledovat možnosti zapojení umělé inteligence do budování manipulace.

Domnívám se, že tato rigorózní práce a výsledky, které obsahuje, budou přínosné pro teoretickou, tak i praktickou činnost. A ačkoliv to nebylo počátečním záměrem, může se také stát zdrojem poznání starších a dalších studentů Policejní akademie České republiky v Praze. Hlavní přínos této práce očekávám v její využitelnosti pro vyšetřovací praxi. A výsledky z terénního šetření mohou být zdrojem k dalším pracím.

Boj proti kriminalitě fiktivních bankéřů, respektive přímo proti praktikám zneužívání maskovaných hovorů a zneužívání osob majitelů bankovních účtů k obcházení bankovního zabezpečení, je veden na více frontách. Nově zaváděná technická opatření, např. samoregulace mobilních operátorů, kontrolní mechanismy bank, dlouhodobé vzdělávací kampaně a osvěta obyvatelstva, budou na tuto kriminalitu mít jistě vliv. Otázkou je, jestli více na straně případných obětí, anebo na straně zločineckých skupin, které se rychleji přizpůsobí a vyvinou nové postupy.

Podvodná jednání v komunikačních sítích se neustále vyvíjí a mění v souladu s technologickými pokroky a bezpečnostními opatřeními. Zločinci se neustále snaží najít nové způsoby, jak zneužít důvěru uživatelů, získat citlivé informace nebo peníze.

Bylo by velmi pošetilé se domnívat, že je možné kriminalitu v sítích zcela vymýtit. Je však nutné ji účinně omezit a trestat.

Seznam použité literatury

Monografie

- GLENNY, Misha. *Temný trh. Kyberzloději, kyberpolicisté a vy*. Oldřich KLIMÁNEK (překladatel). Praha: Argo, 2013. ISBN 978-80-7363-522-0.
- KESHAV, Jindal; DALAL, Surjeet a KUMAR SHARMA, Kamal. *Analyzing Spoofing Attacks in Wireless Networks*. New Jersey: IEEE, 2014. ISBN 978-1-4799-4910-6.
- KOLOUCH, Jan. *Cybercrime*. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8.
- KONRÁD, Zdeněk; NĚMEC, Miroslav a NOVOTNÝ, František. *Vybrané otázky teorie a praxe výslechu*. Praha: Policejní akademie České republiky v Praze, 2008. ISBN 978-80-7251-294-2.
- NĚMEC, Miroslav. *Kriminalistická taktika pro policisty a studenty policejní akademie České republiky*. Praha: ABOOK, 2017. ISBN 978-80-906974-09.
- NĚMEC, Miroslav et al. *Teorie a metodologie kriminalistiky pro magisterské studium – I. díl. Aktuální problémy kriminalistické teorie*. Praha: ABOOK, 2018. ISBN 978-80-906974-1-6.
- NĚMEC, Miroslav et al. *Teorie a metodologie kriminalistiky pro magisterské studium – II. díl. Aktuální problémy kriminalistické praxe*. Praha: ABOOK, 2019. ISBN 978-80-906974-2-3.
- PORADA, Viktor a kol. *Kriminalistika. Technické, forenzní a kybernetické aspekty*. Plzeň: Aleš Čeněk, 2016. ISBN 978-80-7380-589-0.
- PORADA, Viktor. *Kriminalistika: technické, forenzní a kybernetické aspekty*. 2. aktualizované a rozšířené vydání. Plzeň: Aleš Čeněk, 2019. ISBN 978-80-7380-741-2.
- ROUTA, Tomáš. *Kriminalistické problémy vyšetřování podvodných internetových obchodů*. Diplomová práce. Zdeněk KONRÁD (vedoucí práce). Praha: Policejní akademie České republiky v Praze, Fakulta bezpečnostně právní. 2020.
- SMEJKAL, Vladimír. *Kybernetická kriminalita*. 3. vydání. Plzeň: Aleš Čeněk, 2022. ISBN 978-80-7380-849-5.

❖ STRAUS, Jiří a kol. *Kriminalistická technika*. 3. rozšířené vydání. Plzeň: Aleš Čeněk, 2013. ISBN 978-80-7380-409-1.

Časopisecké články

❖ DIVIŠOVÁ, Jana. Falešný bankéř – zase. *POLICISTA*. 2024, č. 1, s. 28-29. ISSN 1211-7943.

Zákonná úprava

❖ EVROPSKÁ UNIE. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). Online. In: *Úřední věstník Evropské unie*. 2016, L 119/1, s. 1-88. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R0679. [citováno 01.04.2024].
❖ EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady 2014/41/EU ze dne 3. dubna 2014 o evropském vyšetřovacím příkazu v trestních věcech. Online. In: *Úřední věstník Evropské unie*. 2014, L 130/1, s. 1-36. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32014L0041. [citováno 06.03.2024].
❖ EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Online. In: *Úřední věstník Evropské unie*. 2016, L 194/1, s. 1-30. Dostupné z: https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32014L0041. [citováno 01.04.2024].
❖ Zákon č. 21/1992 Sb., *o bankách* v posledním znění.
❖ Zákon č. 40/2009 Sb., *trestní zákoník* v posledním znění.
❖ Zákon č. 104/2013 Sb., *o mezinárodní justiční spolupráci ve věcech trestních* v posledním znění.
❖ Zákon č. 141/1961 Sb., *o trestním řízení soudním (trestní řád)* v posledním znění.
❖ Zákon č. 251/2016 Sb., *o některých přestupcích* v posledním znění.

Interní akty řízení

- Pokyn policejního prezidenta č. 103/2013 ze dne 28. května 2013*, o plnění některých úkolů policejních orgánů Policie České republiky v trestním řízení* v posledním znění.
- Pokyn policejního prezidenta č. 40/2022 ze dne 28. února 2022, *o opatřeních kybernetické bezpečnosti* v posledním znění.
- Rozkaz ředitele Krajského ředitelství policie Středočeského kraje č. 108/2022 ze dne 19. září 2022, *kterým se zřizuje pracovní skupina 14 odbor KYBER* v posledním znění.

Webové stránky a elektronické zdroje

- Bundesnetzagentur. *Manipulation von Rufnummern*. Online. Dostupné z: https://www.bundesnetzagentur.de/DE/Vportal/TK/Aerger/Faelle/Manipulation/start.html. [citováno 02.04.2024].
- *Caller ID*. Online. In: Wikipedia. Stránka byla naposledy editována 20.11.2023 v 03:05. Dostupné z: https://en.wikipedia.org/wiki/Caller_ID. [cit. 27.01.2024].
- Crowdstrike. *Was ist ein Vishing-Angriff?* Online. Dostupné z: https://www.crowdstrike.de/cybersecurity-101/vishing/. [cit. 02.04.2024].
- Česká bankovní asociace. *Češi a kyberbezpečnost 2024*. Online. Dostupné z: https://cbaonline.cz/cesi-a-kyberbezpecnost-2024. [cit. 06.04.2024].
- Český telekomunikační úřad. *ČTÚ pomůže výrazně omezit spoofing: Mnoho podvodných hovorů už nebude spojeno*. Online. Dostupné z: https://ctu.gov.cz/tiskova-zprava%3A-ctu-pomuze-vyrazne-omezit-spoofing%3A-mnoho-podvodnych-hovoru-uz-nebude-spojeno. [cit. 01.04.2024].
- Český statistický úřad. *Informační společnost v číslech – 2018*. Prezentace. Kapitola C: Jednotlivci. 2018. Dostupné z: https://www.czso.cz/documents/10180/61601892/061004-18_data.zip/669bf930-1b80-4046-9c00-4abdd5ba82b5?version=1.1. [cit. 24.03.2024].

- Evropská rada a Rada Evropské unie. *Kybernetická bezpečnost: sociální inženýrství*. Online. Dostupné z: https://www.consilium.europa.eu/cs/policies/cybersecurity/cybersecurity-social-engineering/. [cit. 26.01.2024].
- European Commission. *EU anti-fraud measures*. Online. Dostupné z: https://commission.europa.eu/strategy-and-policy/eu-budget/how-it-works/annual-lifecycle/implementation/anti-fraud-measures_en. [cit. 01.04.2024].
- European Commission. *Cybersecurity Policies*. Online. Dostupné z: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies. [cit. 06.04.2024].
- Federal Communications Commission. *Combating Spoofed Robocalls with Caller ID Authentication*. Online. Dostupné z: https://www.fcc.gov/call-authentication. [cit. 01.04.2024].
- Metro. *Spořitelna do boje proti kyberšmejdům nasadila speciální klientský tým*. Online. Dostupné z: https://www.metro.cz/protext/sporitelna-do-boje-proti-kybersmejdum-nasadila-specialni-klientsky-tym.A230906_105000_metro-protext_air. [cit. 06.04.2024].
- Národní úřad pro kybernetickou a informační bezpečnost*. Upozornění na vishing zneužívající identitu bankovních institucí*. Online. Dostupné z: https://nukib.gov.cz/cs/infoservis/hrozby/1705-upozorneni-na-vishing-zneuzivajici-identitu-bankovnich-instituci/. [cit. 06.04.2024].
- *Virtual private network*. Online. In: Wikipedia. Stránka byla naposledy editována 19.01.2024 v 07:17. Dostupné z: https://en.wikipedia.org/wiki/Virtual_private_network. [cit. 27.01.2024].
- *Voice over Internet Protocol*. Online. In: Wikipedia. Stránka byla naposledy editována 15.01.2024 v 21:38. Dostupné z: https://en.wikipedia.org/wiki/Voice_over_IP. [cit. 27.01.2024].
- *VoIP phone*. Online. In: Wikipedia. Stránka byla naposledy editována 27.09.2023 v 15:54. Dostupné z: https://en.wikipedia.org/wiki/VoIP_phone. [cit. 27.01.2024].

Seznam použitých obrázků

Seznam použitých grafů

Seznam použitých zkratek

ČR – Česká republika

CLI – Calling Line Identification

ETŘ – Elektronické trestní řízení

EU – Evropská unie

EVP – Evropský vyšetřovací příkaz

FAU – Finanční analytický úřad

GDPR – General Data Protection Regulation

IBAN – International Bank Account Number

ID – Identity Document (v překladu přeneseně také *identifikační údaj*)

IP – Internet Protocol

IT – Informační technologie

IMEI – International Mobile Equipment Identity

IMSI – International Mobile Subscriber Identity

ITU – International Telecommunication Union

KŘ – Krajské ředitelství

NCOZ – Národní centrála proti organizovanému zločinu

NCTEKK – Národní centrála proti terorismu, extremismu a kybernetické kriminalitě

NFC – Near Field Communication

NIS – Network And Information systems

MAC – Media Access Control

MPP – Mezinárodní právní pomoc

OČTŘ – orgán činný v trestním řízení

OECD – Organisation for Economic Co-operation and Development

PIN – Personal Identification Number

PK – platební karta

QR – Quick Response

RAM – Random Access Memory

ŘMPS – Ředitelství pro mezinárodní policejní spolupráci

SHAKEN – Signature-based Handling of Asserted information using toKENs

SIM – Subscriber Identity Module

SKPV – Služba kriminální policie a vyšetřování

SMS – Short Message Service

STIR – Secure Telephone Identity Revisited

SZ – státní zástupce

ÚSKPV – Úřad služby kriminální policie a vyšetřování

ÚZČ – Útvar zvláštních činností

VoIP – Voice over Internet Protocol

VPN – Virtual Private Network