

Sociální manipulace a jiné podvody v bankovním sektoru

Bc. Ondřej Smažinka

Diplomová práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav elektroniky a měření

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Bc. Ondřej Smažinka
Osobní číslo:	A23516
Studijní program:	N1032A020003 Bezpečnostní technologie, systémy a management
Specializace:	Bezpečnostní technologie
Forma studia:	Kombinovaná
Téma práce:	Sociální manipulace a jiné podvody v bankovním sektoru
Téma práce anglicky:	Social Manipulation and Other Frauds in the Banking Sector

Zásady pro vypracování

1. Analyzujte historii bankovních podvodů se zaměřením na jejich vývoj a typologii od počátků bankovníctví až po současnost.
2. Identifikujte a klasifikujte různé druhy sociálních manipulací a podvodů v současném bankovním sektoru.
3. Popište moderní techniky útočníků v bankovním sektoru využívající sociální manipulaci.
4. Proveďte analýzu současných obranných mechanismů proti sociální manipulaci v bankovníctví a identifikujte jejich slabiny a zranitelnosti.
5. Prozkoumejte možnosti prevence a osvěty v boji proti sociální manipulaci.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. LIBERTYFUND. A History of Banking in all the Leading Nations. Online. 1896. Dostupné z: <https://oll.libertyfund.org/titles/bulletin-a-history-of-banking-in-all-the-leading-nations-vol-1-u-s-a>. [cit. 2024-10-25]
2. CIALDINI, Robert. Nové zbraně vlivu. Jan Melvil publishing, 2023. ISBN 978-80-7555-181-8.
3. DUBOVECKÁ, Klára. STUDENTS OF THE FACULTY OF SOCIAL STUDIES VS PHISHING ATTACKS: VULNERABILITY OF STUDENTS TO DIFFERENT TYPES OF PHISHING. Bakalářská. Brno: Masarykova univerzita, 2022.
4. Chraňte své peníze před podvodníky. Online. 2023, 2024. Dostupné z: <https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat>. [cit. 2024-10-25]
5. ČNB. Podvody v platebním styku. Online. 2024. Dostupné z: <https://www.cnb.cz/cs/casto-kladene-dotazy/Podvody-v-platebnim-styku/>. [cit. 2024-10-25].

Vedoucí diplomové práce: **prof. Mgr. Milan Adámek, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **29. listopadu 2024**

Termín odevzdání diplomové práce: **30. května 2025**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan



Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 29. listopadu 2024

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že

- odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení diplomové práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – diplomovou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na diplomové práci pracoval samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden jako spoluautor;
- odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne 18.05.2025

podpis autora

ABSTRAKT

Diplomová práce se zabývá historií podvodů, popisuje podvodné metody a také obranné mechanismy. Cílem práce je rozšířit povědomí o podvodech a nabídnout možnosti, jak se před nimi účinně bránit. V rámci praktické části je obsahem práce hloubkový rozhovor s podvedenou ženou, který prozkoumá do hloubky její zážitek s podvodem.

Klíčová slova: podvod, banka, sociální, manipulace

ABSTRACT

The thesis deals with the history of fraud, describes fraudulent methods and also defence mechanisms. The aim of the thesis is to increase the awareness of fraud and to offer ways to effectively defend against it. The practical part of the thesis includes an in-depth interview with a deceived woman to explore in depth her experience with fraud.

Keywords: scam, fraud, bank, social, manipulation

Mé poděkování patří vedoucímu diplomové práce prof. Mgr. Milanovi Adámkovi, Ph.D. za trpělivost, ochotu, profesionalitu a odborné rady, které mi poskytoval při vypracovávání práce.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD.....	11
I TEORETICKÁ ČÁST.....	12
1 PRÁVNÍ HLEDISKO A HISTORIE PODVODŮ	13
1.1 PODVOD Z HLEDISKA LEGISLATIVY.....	13
1.2 HISTORIE.....	14
1.2.1 18. století: Počátky bankovníctví a první podvody	14
1.2.2 19. století: Éra "divokých bank" a finančních krizí.....	15
1.2.3 20. století: Regulace a moderní podvody.....	16
1.3 SOUČASNÝ STAV PODVODŮ V ČESKÉ REPUBLICE	16
2 PODVODNÉ METODY.....	19
2.1.1 Phishing.....	19
2.1.2 Lovescam.....	21
2.1.3 Vishing.....	24
2.1.4 Bazarový podvod.....	25
2.1.5 Falešný bankéř.....	26
2.1.6 Moderní kontext	27
2.1.7 Falešné investice.....	28
3 OBRANNÉ MECHANISMY	30
3.1 PREVENTIVNÍ OPATŘENÍ.....	30
3.2 AKTIVNÍ OPATŘENÍ.....	30
3.2.1 Obezřetnost při sdílení osobních údajů	31
3.2.2 Důkladná kontrola odkazů.....	31
3.2.3 Důkladná kontrola e-mailů.....	32
3.2.4 Důkladná kontrola certifikátů navštěvovaných stránek	32
3.2.5 Kritické vnímání informací	33
3.2.6 Ověřování finančních protistran a recenzí.....	33
3.2.7 Password management.....	34
3.2.8 Vzdělávání	35
3.2.9 Používání anonymizačních nástrojů.....	35
3.3 PASIVNÍ OPATŘENÍ.....	36
3.3.1 Antivirus.....	36
3.3.2 Aktualizace softwaru	37
3.3.3 Používání bezpečných prohlížečů.....	37
3.3.4 Používání bezpečných Wi-Fi sítí	38
3.3.5 Bezpečné platební metody.....	39
4 OBRANNÉ MECHANISMY BANK.....	41
4.1 AKTIVNÍ MECHANISMY	41
4.1.1 Push notifikace	41
4.1.2 Domovská stránka	41
4.1.3 Bezpečnostní přihlašovací metody.....	41

4.1.4	Dvoufaktorové ověření.....	42
4.1.5	Touch iD	42
4.1.6	Face iD.....	42
4.1.7	Další aplikace	43
4.2	PASIVNÍ MECHANISMY	43
4.2.1	Notifikace.....	43
4.2.2	Funkcionality.....	44
4.2.3	Awareness.....	44
4.3	OBRANNÉ MECHANISMY ČESKÉ SPOŘITELNY	44
4.3.1	Aktivní mechanismy	44
4.3.2	Pasivní mechanismy.....	46
II	PRAKTICKÁ ČÁST.....	47
5	NÁVRH ZPRACOVÁNÍ PRAKTICKÉ ČÁSTI.....	48
5.1	VYMEZENÍ VÝZKUMNÉHO PROBLÉMU	48
5.2	HLOUBKOVÝ ROZHOVOR.....	48
5.3	OTÁZKY PRO ROZHOVOR.....	49
5.3.1	Dotazy na respondenta	49
5.4	HYPOTÉZY	51
5.4.1	Samostatné hypotézy.....	52
5.5	HLOUBKOVÝ ROZHOVOR.....	54
5.5.1	Aktéři rozhovoru.....	54
5.5.2	Samotný rozhovor.....	55
5.6	VÝSLEDKY HYPOTÉZ.....	83
	ZÁVĚR.....	86
	SEZNAM POUŽITÉ LITERATURY.....	87
	SEZNAM OBRÁZKŮ.....	91
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	92

ÚVOD

Každý den po celém světě probíhají miliony transakcí. S přechodem finančních transakcí do digitálního světa ale přicházejí ruku v ruce také podvody. Běžné kapsářství, krádeže, podvody a kuplířství nahradily digitální podvody. Dnes již musí být každý návštěvník digitálního světa maximálně obezřetný, zvláště pak, když dojde na manipulaci s osobními údaji nebo penězi. Bankovní svět, který dennodenně chrání své klienty před internetovými podvodníky, obvykle zaujímá roli reagujícího na neustále vyvíjející se podvody. Metody podvodníků se stávají každým dnem více a více sofistikovanými, banky mohou pouze reagovat na nové podvody a snažit se zmírňovat dopady. [1]

Téma sociální manipulace a podvody v bankovním sektoru bylo vybráno proto, že se tomuto tématu autor aktivně věnuje ve svém zaměstnání, i při studiích. Dalším z důvodů je aktuálnost. Podvody na bankovní klienty dosahují ročně astronomických částek v řádech stovek milionů českých korun. Zásadním zlomem, kdy začal počet podvodů prudce narůstat, bylo období pandemie Covid-19. Lidé najednou trávili mnohem více času doma a své finanční záležitosti začali vyřizovat převážně online. Na tento rychlý přesun do digitálního prostředí zareagovaly i firmy – zjednodušily řadu svých procesů a upravily služby tak, aby je klienti mohli pohodlně využívat z domova. [1]

Teoretická část práce se soustředí na vývoj podvodů od jejich historických kořenů až po současnost s důrazem na digitalizaci a její vliv. Podrobně analyzuje různé typy podvodných praktik a způsoby jejich provedení. Dále se zabývá opatřeními, která bankovní sektor přijímá k jejich prevenci, včasnému rozpoznání i minimalizaci škod, jež mohou podvody způsobit.

Praktická část práce se věnuje hloubkovému rozhovoru s osobou, která se stala obětí sociální manipulace. Prostřednictvím tohoto rozhovoru podrobně popisuje svůj osobní zážitek, jenž vyústil v závažnou finanční i emoční ztrátu. [1]

I TEORETICKÁ ČÁST

1 PRÁVNÍ HLEDISKO A HISTORIE PODVODŮ

V této kapitole se v první řadě pojednává o podvodu z hlediska legislativy České republiky. Zároveň je zde rozebrána historie podvodů. Pro příklad demonstrace vývoje podvodů v čase byly vybrány Spojené státy americké. Rozhodl o tom osobní zájem, neboť autor vnímá, že bankovní systém USA ovlivňuje a vždy ovlivňoval bankovní systémy po celém světě.

1.1 Podvod z hlediska legislativy

Podvod je trestný čin neoprávněného zisku bez použití násilí ani jiné fyzické námahy. Je logické, že tento trestný čin je starý jako lidstvo samo. Během času se historie podvádění vyvíjela velmi rychle. Postupně začalo docházet i k organizovanému podvádění několika aktéry ve skupině. Lidé vnímali podvod jako jednoduchou lest sloužící k rychlému obohacení sebe sama, bez použití násilí, které by mohlo potenciálně ohrozit i útočníka i oběť. Zde je poměrně značná šance, že pokud je lest dobře promyšlena, pak potenciální oběť může zjistit, že byla podvedena až dávno potom, co se útočník i oběť rozloučí. [2]

Trestný čin podvodu zabírá široké spektrum počínání a několik zvláštních druhů. Protože podvody začaly v historii čím dál zásadněji ovlivňovat hospodářství, vznikla potřeba subjektů právní moci tento čin označit jako trestný a jednoznačně ho specifikovat. Brzy pak vznikly kategorie podvodů, které známe dodnes jako jsou podvody pojistné, úvěrové, či dotační. [2]

Podvod. § 209: „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, bude potrestán:

- Odnětím svobody až na dvě léta, zákazem činnosti nebo propadnutím věci.“
- Odnětím svobody na šest měsíců až tři léta bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 a byl-li za takový čin v posledních třech letech odsouzen nebo potrestán.
- Odnětím svobody na jeden rok až pět let nebo peněžitým trestem bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 větší škodu.
- Odnětím svobody na dvě léta až osm let bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1 jako člen organizované skupiny,

- spáchá-li takový čin jako osoba, která má zvlášť uloženou povinnost hájit zájmy poškozeného,
- spáchá-li takový čin za stavu ohrožení státu nebo za válečného stavu, za živelní pohromy nebo jiné události vážně ohrožující život nebo zdraví lidí, veřejný pořádek nebo majetek, nebo způsobí-li takovým činem značnou škodu.
- Odnětím svobody na pět až deset let bude pachatel potrestán, způsobí-li činem uvedeným v odstavci 1 škodu velkého rozsahu, nebo
- spáchá-li takový čin v úmyslu umožnit nebo usnadnit spáchání teroristického trestného činu, trestného činu financování terorismu (§ 312d) nebo vyhrožování teroristickým trestným činem (§ 312f).
- Příprava je trestná. [3]

1.2 Historie

Historie bankovních podvodů je bohatá a sahá až do vzniku prvních bankovních systémů. V průběhu staletí se podvody vyvíjely a přizpůsobovaly novým technologiím a finančním systémům. Pro příklad vývoje bankovních podvodů byly vybrány Spojené státy. Historie podvodů ve Spojených státech je velmi rozmanitá a udávala trendy po celém světě. [4]

1.2.1 18. století: Počátky bankovníctví a první podvody

Studium tohoto období ukazuje, jak důležitá je transparentnost, regulace a dohled nad finančními institucemi pro prevenci podvodů a ochranu veřejnosti před finančními ztrátami. Zkušenosti z 18. století poskytují cenné poznatky pro pochopení současných výzev v oblasti bankovních podvodů a potřeby efektivního regulačního rámce. [4]

V 18. století se bankovní sektor ve Spojených státech teprve formoval a byl poznamenán řadou podvodných praktik, které často vycházely z nedostatečné regulace a absence jednotného měnového systému. V tomto období vznikaly různé finanční instituce, které mnohdy operovaly bez dostatečného kapitálového zajištění a transparentnosti. [4]

Jedním z příkladů byla praxe vydávání nekrytých bankovek. Jednotlivé banky emitovaly vlastní měnu bez adekvátního krytí ve zlatě či stříbře. Tato situace vedla k častým podvodům, kdy veřejnost přijímala bankovky, které neměly reálnou hodnotu, což způsobovalo finanční ztráty a podkopávalo důvěru v bankovní systém. [4]

Dalším problémem byla absence jednotného dohledu nad bankovními institucemi. Mnohé banky vznikaly s cílem rychlého zisku a nebyly schopny dostát svým závazkům vůči klientům. Tato situace vedla k častým bankrotům a finančním krizím, které měly negativní dopad na ekonomiku a společnost jako celek. [4]

V reakci na výše zmíněné problémy začaly postupně vznikat snahy o regulaci bankovního sektoru a zavedení jednotných pravidel pro fungování finančních institucí. Nicméně, cesta ke stabilnímu a důvěryhodnému bankovnímu systému byla dlouhá a plná překážek. [4]

1.2.2 19. století: Éra "divokých bank" a finančních krizí

Druhá polovina 19. století byla v americkém bankovníctví charakteristická rychlým růstem, ale také naprostým chaosem v oblasti regulace a prudkým nárůstem podvodných praktik. Tato éra, často označovaná jako období tzv. „divokých bank“ (wildcat banking), byla zcela typická tím, že vznikaly desítky až stovky menších bank, které fungovaly zcela bez jednotných pravidel a často bez dostatečného finančního zajištění. [4]

Hlavní problém spočíval v tom, že každá státní banka měla právo vydávat vlastní bankovky, jejichž krytí nebylo nijak systematicky kontrolováno. Lidé tak často dostávali do rukou prakticky bezcenné peníze, jejichž reálná hodnota závisela výhradně na důvěryhodnosti dané instituce. Některé banky navíc vznikaly jen s cílem zbohatnout na důvěře obyčejných lidí – záměrně sídlily v těžko přístupných oblastech, kde se dalo očekávat, že držitelé bankovek je nikdy nepřijdou vyměnit za skutečné peníze. Šlo o cílené zneužívání systému, který ještě nepočítal s centrálním dohledem. [4]

Výsledkem těchto praktik byly opakované krize – například v letech 1837, 1857 nebo 1873. Tyto otřesy byly často doprovázeny spekulacemi na trhu s půdou nebo železnicí, což jen prohlubovalo důsledky podvodného chování v bankovníctví. Mnoho lidí přišlo o úspory, banky krachovaly v řetězových reakcích a celá ekonomika upadala do recese. [4]

Zkušenosti z tohoto období ukázaly, že samoregulace v bankovníctví zkrátka nefunguje. Právě na konci 19. století se proto začíná formovat silnější státní dohled a úvahy o potřebě vytvořit centrální bankovní instituci. Historie této doby se tak stává klíčovou pro pochopení, proč je dnes bankovní sektor pod tak přísnou kontrolou. [4]

1.2.3 20. století: Regulace a moderní podvody

Ve 20. století prošel americký bankovní sektor zásadními změnami, které byly často vyvolány rozsáhlými podvody a finančními krizemi. Tyto události nejen otřáslы důvěrou veřejnosti v bankovní instituce, ale také vedly k významným reformám a zavedení nových regulačních mechanismů. [4]

Jedním z prvních významných incidentů byla Panika roku 1907, známá také jako „Krise bankéřů“. Tato krize byla spuštěna neúspěšným pokusem o manipulaci s akcemi společnosti United Copper Company, což vedlo k dominovému efektu bankovních krachů a masovým výběrům vkladů. Absence centrální banky a nedostatečný dohled nad finančními institucemi umožnily šíření paniky, která nakonec vyústila ve vytvoření Federálního rezervního systému v roce 1913. [4]

Ve 20. a 30. letech se objevily nové formy podvodů, které využívaly důvěry investorů a nedostatečné regulace. Například Charles Ponzi vytvořil známé Ponziho schéma, které slibovalo vysoké výnosy z arbitráže mezinárodních poštovních kupónů, ale ve skutečnosti šlo o klasický pyramidový podvod. Jeho činnost vedla k obrovským ztrátám pro tisíce investorů a ukázala na potřebu přísnějšího dohledu nad investičními aktivitami. [4]

Velká hospodářská krize v roce 1929 odhalila další slabiny bankovního systému. Mnoho bank selhalo kvůli špatným investicím a spekulacím, což vedlo k masovým výběrům vkladů a dalšímu prohloubení ekonomické krize. V reakci na tuto situaci byl přijat Glass-Steagallův zákon, který oddělil komerční a investiční bankovníctví, a byla zřízena Komise pro cenné papíry a burzy (SEC), aby dohlížela na finanční trhy a chránila investory. [4]

V 80. a 90. letech došlo k deregulaci finančního sektoru, což vedlo k novým formám podvodů a zneužívání. Například krize spořitelů a úvěrních družstev (S&L crisis) byla částečně způsobena podvodnými praktikami a špatným řízením rizik, což vedlo k bankrotu mnoha institucí a nákladům pro daňové poplatníky ve výši stovek miliard dolarů. V reakci na tyto události byly zavedeny nové regulační orgány a zákony, které měly za cíl zvýšit transparentnost a důvěru ve finanční systém. [4]

1.3 Současný stav podvodů v České republice

Situace v České republice je více než znepokojivá, od tzv. „covidových let“, kdy se obrovská část podvodníků přesunula z ulic do digitálního světa. V půlce roku 2023 se společnost

Avast rozhodla zmapovat nárůst kybernetických hrozeb a hrozeb ze strany „kyberšmejdů“.

[5]

Kybernetické hrozby v Česku se od „covidových let“ dramaticky zvýšily. Ve druhém čtvrtletí roku 2023 vzrostl počet podvodů oproti prvnímu kvartálu o alarmujících 81 %. Podobný trend byl zaznamenán i na Slovensku, kde nárůst činil 57 %. Pro srovnání, celosvětový průměrný růst těchto útoků dosáhl pouze 24 %, což naznačuje, že střední Evropa je cílem podvodníků více než jiné části světa. [5]

Ačkoliv způsoby útoků mohou být různé, jejich účel se nemění – podvodníci se snaží připravit oběti o peníze nebo je přimět k prozrazení citlivých údajů. Kyberzločinci stále častěji využívají psychologické manipulace namísto tradičních metod šíření škodlivého softwaru. Tento vývoj znamená, že kromě technických bezpečnostních opatření je klíčové také zvyšovat povědomí veřejnosti o podvodných praktikách. Zatímco dříve podvodníci věnovali velké úsilí o okrádání obětí v běžném světě, od roku 2021 nastal velký odklon těchto podvodníků směrem do světa digitálu. Podvodníci totiž zjistili, že digitální svět je pro ně mnohem bezpečnější místo. Nejen, že když podvodník vytáhne na oběť nůž na ulici riskuje, že na obou stranách dojde k nějakému velmi vážnému zranění, ač původním záměrem bylo například pouze zastrašit, aby oběť bez zbytečných řečí okolo pouze odevzdala peněženku, či šperk, podvodník zároveň riskoval i problémy na své straně, například to, že se oběť bude bránit a zraní podvodníka, nebo by mohlo úplně stačit, kdyby oběť podvodníka jednoduše poznala. Podvodník sám sebe vystavuje velkému riziku už jen tím, že se snaží zahalit svůj obličej. Podvodníci proto zjistili, že digitální svět je pro ně mnohem bezpečnější místo. Nejen, že vytáhne-li podvodník na oběť na ulici nůž, tak riskuje zranění na obou stranách, ale také to, že bude poznán a odhalen. Podvodník sám sebe vystavuje velkému riziku už jen tím, že se snaží zahalit svůj obličej. Zato v prostředí internetu, není náročné stát se anonymním a velmi obtížně odhalitelným. Stejným způsobem došlo k vývoji na straně podvodníků, kteří již digitální svět okupovali. Dříve věnovali velké úsilí k vytváření různých algoritmů, k prolamování hesel nebo rozesílání virů potenciálním obětem a v dnešní době také v mnohem větší míře používají sociální manipulaci jako nástroj k dosažení svých cílů. [39]

Další velkou hrozbou je vytváření falešných webových stránek. Může se jednat o podvodné sbírky, falešné investiční platformy nebo klamavou reklamu, která láká na neexistující produkty a služby. Mezi nejrychleji rostoucí typy podvodů patří falešné seznamky, jejichž počet se ve druhém čtvrtletí meziročně zvýšil o 39 %. [5]

Phishing nadále zůstává jedním z nejrozšířenějších podvodů a ve druhém čtvrtletí tvořil 25 % všech kybernetických hrozeb. Zároveň roste i počet smishingových útoků – tedy phishingu prostřednictvím SMS zpráv. Podvodníci těží z toho, že lidé mají tendenci textovým zprávám důvěřovat a často bez rozmyšlení otevírají odkazy, které SMS zpráva obsahuje. [5]

V roce 2024 server peníze.cz přišel k velice zajímavým statistikám. Banky v roce 2023 evidovaly celkem 69 685 online útoků na klienty. Jednalo se o případy, kdy se podvodníkovi podařilo proniknout do internetového či mobilního bankovníctví, zneužít platební kartu nebo vylákat platbu. Podle České bankovní asociace se počet těchto útoků oproti předchozímu roku ztrojnásobil. [6]

Celková částka, o kterou podvodníci připravili banky a jejich klienty, dosáhla v roce 2023 výši 1,35 miliardy korun. Průměrná finanční ztráta na jednoho podvedeného klienta činila 19 357 korun. Během roku se tato částka postupně snižovala – v prvním pololetí byla přibližně 22 tisíc korun, zatímco ve druhém klesla na 19 tisíc korun. Největší zaznamenaná individuální škoda, kterou podvodníci za celou dobu sledování kybernetických podvodů Českou bankovní asociací způsobili, činila 15 milionů korun. Zatímco banky zaznamenaly téměř 70 tisíc online útoků, policejní statistiky uvádějí „pouze“ 19 592 případů kybernetických podvodů, což představuje meziroční nárůst o 5,5 %. Tento rozdíl podle České bankovní asociace vzniká hlavně proto, že mnoho obětí podvodu se rozhodne neohlásit incident policii a nepodává trestní oznámení. [6]

Podle policie se Česká republika potýká s bezprecedentním nárůstem online kriminality. Policie vyřeší pouze 15,4 % zločinů v kyberprostoru. [7]



Obrázek 1 Počty registrovaných skutků

(zdroj: [8])

2 PODVODNÉ METODY

V této kapitole byly popsány všechny podvodné metody, které se v současné době vyskytují a slouží podvodníkům k okrádání lidí. Pohledy a přístupy k podvodnému jednání se napříč světem poměrně zásadně liší. Zároveň lze konstatovat, že rozlišování podvodů je dnes již zastaralou praktikou. Podvodníci totiž jen zřídka použijí při pokusu o okradení oběti pouze jednu z podvodných metod. Velmi často se dnes setkáváme spíše s kombinací těchto podvodů, kdy podvodníci například nalákají potenciální oběť pomocí tzv. phishingu na lákavou nabídku a poté se oběť již chycenou na prvotní podnět snaží podvést pomocí techniky zvané vishing, tedy podvod skrz hovor. Toto kombinování je přirozenou reakcí podvodníků na snahu bank, antivirů a dalších o preventivní, či aktivní opatření proti podvodníkům. Nyní si představíme detailně ty nejznámější podvodné metody. [10]

2.1.1 Phishing

Phishing je podvodná metoda, kterou lze považovat za jednu z nejzákladnějších a nejstarších ve světě bankovních podvodů. Je to kybernetický útok, který má za cíl z oběti vytáhnout citlivé údaje. [40]

2.1.1.1 Původ slova

Slovo phishing vzniklo z dokumentu „System Security: A hacker's perspective“, v češtině „Bezpečnost systému: Pohled hackera“, od autorů Jerryho Felixe a Chrise Haucka. Zde můžeme najít první zmínku o slově phishing. Slovo phishing jako takové pochází z anglického slova „fishing“, neboli rybaření. Lze zde spatřit jasnou analogii, kde rybář, v našem případě podvodník nahazuje udičku a čeká, až se na ní chytí ryba, v našem případě oběť. Takto phishing funguje, jedná se o pasivní podvod, kdy často hromadně podvodníci nahazují udičky pomocí podvodných e-mailů, SMS zpráv, nebo podvodných webových stránek. [11]

2.1.1.2 Použití

Dříve se takový phishing objevoval převážně v e-mailové komunikaci. Byly to takové ty typické e-maily, které se nám snažily například předat informaci, že zemřel nějaký náš dálný příbuzný a zanechal nám dědictví v řádu několika stovek milionů dolarů. Tyto e-maily ovšem pořád chodí i přes to, že dnes jsou již techniky podvodníků daleko sofistikovanější. [40]

2.1.1.3 Současný stav

Dnes již registrujeme zásadní posun v podvádění pomocí phishingu. Velmi často dochází totiž ke kombinaci mezi phishingem a dalšími podvodnými metodami. Setkáváme se běžně s podvodnými e-maily, sms zprávami, nebo podvodnými weby, které mají za úkol nalákat potenciální oběť. Tyto e-maily, SMS zprávy, nebo podvodné weby dnes bývají velmi dobře a profesionálně zpracovány. Existuje již jen velmi málo metod, jak takovou phishingovou zprávu odhalit. U podvodného e-mailu jsou to zásady jako pečlivá kontrola odesílatele, jeho adresy atd. Často jsme se dříve setkávali například s pravopisnými chybami, nadměrným používáním velkých písmen a podobných, to je minulostí. Jednou z nejdůležitějších zásad je neklikat na odkazy, které podezřelý e-mail obsahuje, to by mohlo vést k předání citlivých informací podvodníkovi, nebo ještě hůře ke stažení škodlivého softwaru do počítače.

Dalším z kanálů, které podvodníci používají k phishingu jsou SMS zprávy. Často to bývají falešné odkazy s textem, kde se například podvodníci vydávají za policii a chtějí zaplatit pokutu za rychlost; falešný bankéř, který upozorňuje na nedoplatek a posílá falešný odkaz na stránku banky anebo třeba různé podvodné SMS zprávy z ministerstev. Zde

dochází k již zmíněné kombinaci mezi phishingem a dalšími podvodnými metodami. Typicky oběti přijde SMS zpráva s falešným textem a odkazem. [9]

1.5.1.5 Konkrétní podvod

Jedním z typických phishingů je falešná SMS od Policie. Oběť se zrovna vrací z dovolené a je si vědoma toho, že po cestě několikrát překročila maximální povolenou rychlost. Je třeba poznamenat, že neexistují důkazy o tom, že podvodníci jsou schopni zjistit, zda se daná oběť skutečně vracela z dovolené, nebo je to pouze náhoda, takzvané zmiňované nahození udičky. Oběť v únavě a vlastním vědomí, že skutečně povolenou rychlost překročila neváhá a otevírá podezřelý odkaz. Zde se objeví na falešné stránce policie, která je téměř neprůstředná, všechny odkazy fungují, vizuální stránka také odpovídá originálu. Jediné, čeho se v tuto chvíli může oběť chytit, je podezřelý název webové stránky, nebo certifikát stránky. Ovšem zde jsou dva problémy. Pokud klient podlehl sociální manipulaci a je přesvědčen, že koná správně, je téměř vyloučeno, že by si šel zkontrolovat certifikát stránky. Druhý problém je, že klient právě užívá mobilní telefon, kde při prohlížení webové stránky lze uvidět název stránky až po přejetí prstem na nejvyšší možnou pozici na stránce, tehdy se teprve odkaz zobrazí a je možné si všimnout něčeho podezřelého. Na této velmi dobře zpracované webové stránce Policie ČR se nachází odkaz do internetového bankovníctví, aby došlo k zaplacení pokuty za překročení maximální povolené rychlosti. Jedná se opět o falešnou stránku, kterou lze jen velmi těžko odhalit. Oběť zadá své údaje sloužící k přístupu do internetového bankovníctví a typicky se ukáže nějaká chybová hláška, že se přihlášení nezdařilo a aby se klient pokusil přihlásit později. Nicméně v této chvíli již oběť předala své přihlašovací údaje do internetového bankovníctví podvodníkům. Ti mají nyní přístup a mohou si procházet internetové bankovníctví oběti, jak se jim chce. Naštěstí se již banky dokážou bránit alespoň tak, že zamezí odvod peněz podvodníkovi nutnou autorizací, kterou může provést pouze klient s vlastní bezpečnostní metodou k autorizaci platby. V tuto chvíli do hry vstupuje podvodník, který oběť telefonicky kontaktuje a vydává se za bankéře banky. Upozomí klienta na podezřelé pohyby v jeho internetovém bankovníctví a po nátlaku ho přesvědčí, aby své peníze vyvedl do domnělého bezpečí, tedy na účet podvodníka. [9]

2.1.2 Lovescam

Lovescam, nebo někdy také nigerijský podvod, je další ze známých a běžných podvodných metod. Jedná se o sociální manipulaci, která nefunguje jako phishing na pasivní bázi tedy nahazování udičky, ale na bázi aktivní manipulace. [9]

2.1.2.1 Původ slova

Lovescam, Romance scam, nigerijský podvod, to jsou synonyma vystihující sociální manipulaci, která vznikla už dávno před internetem. První zmínky o tomto podvodu pocházejí ze začátku 80. let, kdy chodily poštou podvodné dopisy, například od údajného majitele nigerijské petrolejové firmy, nebo třeba amerického vojáka v nesnázích, který prosí o pomoc. Už tehdy tento podvod měl první úspěchy a podvodníci posílající tyto dopisy se učili a vyvíjeli v sociálním manipulování s oběťmi. [12]

2.1.2.2 Použití

Podvodník typicky přes sociální síť kontaktuje svou potenciální oběť a naváže s ní kontakt, který nemusí být nutně milostný. Technik pro vyvolání emocí je mnoho, může to být například vyvolání lítosti nad smyšlenou politováníhodnou situací podvodníka, nebo to bývá situace, kdy se podvodník vydává za amerického vojáka, který uvízl ve válečné oblasti a nutně potřebuje peníze, aby se mohl dostat domů za svou rodinou. Jindy se zase podvodník vydává za majitele obří korporace, jehož peníze jsou v nesnázích a nutně potřebuje, aby oběť poslala peníze. Podvodník slíbí lukrativní podíl, díky kterému oběť přesvědčí. Další z technik je navázání intimního kontaktu s obětí. Podvodník oběti píše hezké a líbivé zprávy, snaží se navázat sblížení a navodit důvěru a poté ve správný moment požádá oběť o zaslání peněz kvůli náhlému problému, například fiktivnímu vážnému onemocnění a nutnosti peněz na náročný zákrok. Obvykle pak podvodníci v případě nespokojenosti oběti přejdou z milostných zpráv k nátlaku, výhrůžkám, nebo vydírání. Z tohoto vzoru je patrné, že podvodníci cílí na lidské emoce, jako jsou chťič, láska, strach a lítost. Zatímco ostatní podvodné metody cílí na lidský chťič nebo zmatení, přesvědčení v rychlosti, kdy oběť díky nepozornosti nechtěně klikne na špatný odkaz a zadá citlivé údaje na nesprávné místo, lovescam je v tom sociálním hledisku zákeřnější. Zatímco podvody jako vishing, phishing, falešný bankéř, nebo podvodné investice probíhají v řádu hodin, lovescam může trvat řádově i několik let. Podvodníci často ze zemí třetího světa používají propracované psychologické metody, které postupně na oběť aplikují. Podvodníci osloví svou potenciální oběť a pak se na ní upnou. Nedají své oběti spát a píšou ji třeba několik hodin denně, hledají jakoukoliv slabinu na oběti, ale přitom jsou maximálně slušní a zdvořilí. Při každodenním psaní se snaží s osobou sblížit a dát jí pocit, že bez podvodníka nemohou dál fungovat. Stanou se nezbytnou součástí života oběti. Pak jen stačí, aby si v sobě potenciální oběť nesla nějakou bolest,

nějaké nevyplněné místo, zkrátka nějakou slabinu. Podvodník se na toto místo upne a postupně se pokouší tohle slabší místo v životě oběti vyplnit. Často se setkáváme i s tím, že se tým vyškolených bankéřů na klientském pracovišti snaží oběti vysvětlit, že se právě stala obětí finančního podvodu, nicméně oběť odmítá uvěřit a nechává se dále podvádět. Sledujeme zde pocity zklamání, nevěřícího a následného obviňování banky, že vlastně ona je ta špatná a snaží se zamilované oběti pokazit to co tak dlouho hledala a konečně našla. Velmi důležité je také této osobě po prozření nabídnout patřičnou péči, neboť tento zážitek může obyčejného člověka silně zasáhnout a zanechá to v něm doživotní trauma. To je základní a zároveň obrovsky zásadní rozdíl mezi lovescamem a jakýmkoliv jiným podvodem. Lovescam nejen, že trvá klidně několik let, ale následky tohoto zážitku mohou být pro lidskou osobnost drtivé. I samotná rekonvalescence z tohoto zážitku může trvat dalších několik let a co hůře, oběť se s tím nemusí smířit do konce života. Oběti se po rozkřiknutí této události stávají obětní posměchu, nepochopení, odsouzení. Samotná oběť pak cítí velký stud o tom dále hovořit a zároveň samozřejmě nesmíme opomenout fakt, že tato oběť mimo to ještě dost možná přišla o obrovskou část finančních prostředků, ne-li celoživotních úspor. [9]

2.1.3 Vishing

Vishing je podvodnou metodou, která je dnes velmi moderní. Jedná se vlastně o phishing, ale pomocí hlasu. Probíhá, ať už běžnou telefonní linkou, nebo dnes často skrz sociální sítě, např. WhatsApp. Zásadním rozdílem mezi vishingem a phishingem je kromě kanálu, kterým tento podvod probíhá, také samotné provedení. Ten zásadní rozdíl je, že vishing nelze dělat pasivně, ale aktivně. Jedinou možností, kdy lze takzvaně nahazovat udičku je případ, kdy vishing neprovádí reálná osoba, nýbrž podvodníky naprogramovaný automat, který automaticky vytáčí čísla a voicebot vede hovory s lidmi, kdy se například voicebot vydává za známou instituci. [9]

2.1.3.1 Původ slova

Vishing, známý také jako hlasový phishing nebo voice phishing, je forma phishingového podvodu, která využívá telefonní hovory a techniky sociálního inženýrství. Výraz vznikl složením slova phishing a voice, nyní tedy voice phishing, neboli vishing. [13]

2.1.3.2 Použití

Vishing se v praxi používá často v kombinaci s jinými podvodnými metodami. Typicky s phishingem anebo také s tzv. „number spoofingem“. Number spoofing je podvodná metoda, při které se podvodníkům podaří volat potenciálním obětem tak, aby oběť viděla na displeji svého telefonního zařízení tel. číslo známé instituce. To může oběť zmást a co hůř, také utvrdit v tom, že volá skutečně s tím, s kým volat chce. Samotný podvod v kombinaci těchto tří metod může vypadat například tak, že oběť otevře podvodný e-mail, který se tváří jako upozornění od banky na podezřelou aktivitu na klientově internetovém bankovníctví. Oběť ve strachu neváhá a klikne na podvodný odkaz, který ji odkáže na falešné stránky banky a nechá zde klienta zadat citlivé údaje do internetového bankovníctví. Klient zadá údaje a poté obdrží hovor z podvodného telefonního čísla, které se na první pohled tváří naprosto legitimně, jako číslo z banky. Na druhé straně hovoru je ovšem podvodník, který se představí jako bankéř a upozorní oběť na podezřelé transakce na jeho účtu. Velmi cynické je to, že ve chvíli, kdy se podvodníkům povede tzv. number spoofing, tedy že jejich telefonní číslo vypadá skutečně úplně stejně jako číslo bankovní instituce, tento falešný bankéř může klidně oběť upozornit na podvody na internetu a poprosí oběť, aby si zkontrolovala, že skutečně hovoří s bankou pomocí čísla banky, které oběť může nalézt na internetu. Tím dojde k tolik potřebnému utvrzení, které má za následek obrovský průšvih. Oběť nyní cítí důvěru k podvodníkovi, a navíc strach o své finance. Podvodný bankéř dá své oběti na výběr:

Bud' může okamžitě všechny své finance poslat na nový bezpečný účet, nebo o všechny své peníze přijde. Oběť pak neváhá a odesílá na domnělý bezpečný účet všechny finance které má na účtu k dispozici a ignoruje všechna bezpečnostní opatření banky. [9]

2.1.4 Bazarový podvod

Jedná se o další ze série častých podvodů, se kterými se běžně setkáváme. Podvodníci spoléhají na to, že se potenciální oběť chytí na podvodné stránky, nebo nabízí na bazarech zboží, které následně zákazník nikdy neobdrží. Efektivnější způsob bazarového podvodu je však situace, kdy se podvodník spojí s obětí s původním zájmem o nějaký produkt na známých bazarových portálech a následně nabídne oběti podvodný odkaz se záminkou zaplacení částky za dovoz, vedoucí do falešného bankovníctví, kde opět tak jako u phishingu oběť dobrovolně odevzdá údaje do svého internetového bankovníctví. [9]

2.1.4.1 Původ slova

Slovo „bazar“ má svůj původ v perštině, konkrétně ve výrazu *bāzār*, a předpokládá se, že vzniklo ze staršího pahlavského výrazu *baha-char* (بهاچار), což lze volně přeložit jako „místo cen“. Z Persie se tento pojem postupně rozšířil nejprve do arabského světa a později do celé oblasti Blízkého východu. [14]

Dnes se varianta tohoto slova v různých podobách vyskytuje v celé řadě jazyků – například v arabštině a urdštině jako بازار, v kurdštině rovněž jako *bazar*, což znamená tržiště. V albánštině, bosenštině a turečtině se používá podoba *pazar*, zatímco v asámštině se zapisuje jako বজাৰ (*bôzar*), v bengálštině jako বাজার a v odštině jako ବଜାର. V bulharštině a makedonštině se pak objevuje jako *nazap*, a v kyperské řečtině existuje výraz *pantopoula*. [14]

2.1.4.2 Použití

Bazarový podvod je sofistikovaná podvodná technika využíváná v online prostředí, kde jsou nakupující a prodávající propojeni přes různé bazary a platformy pro prodej zboží. Tento typ podvodu obvykle spojuje různé taktiky manipulace a klamavého jednání, aby se podvodníkovi podařilo získat peníze nebo zboží od nic netušících obětí. Scénář může začít třeba tak, že podvodník na online bazaru umístí atraktivní inzerát s velmi lákavou cenou nebo s tvrzením, že zboží je ve skvělém stavu a omezeném množství, což má oběť motivovat k rychlému rozhodnutí. Oběť, která na nabídku odpoví, je pak vystavena sérii manipulací ze strany podvodníka, který se často vydává za poctivého prodejce nebo kupujícího. [9]

V případě, že podvodník předstírá roli prodejce, může oběti navrhnout rychlou platbu předem, například s odůvodněním, že je o zboží velký zájem, a pokud oběť rychle nepošle peníze, někdo jiný zboží koupí. Oběť, obvykle ve strachu, že přijde o výhodnou koupi, peníze převede a doufá, že brzy obdrží objednaný produkt. Poté, co podvodník peníze obdrží, však veškerá komunikace náhle ustane a zboží se nikdy nedočká. Podvodníci často využívají anonymní nebo dočasné e-mailové adresy a telefonní čísla, která po uskutečnění podvodu jednoduše deaktivují, čímž oběti znemožní jakýkoliv další kontakt a reklamaci. [9]

Podvodníci mohou používat i sofistikovanější techniky, například falešná potvrzení o platbě, kdy oběť obdrží „důkaz“ o přijetí platby, který je však podvodným dokumentem. Často se jedná o falešnou potvrzovací stránku nebo e-mail, který napodobuje vzhled skutečných bankovních či platebních služeb, což dodává podvodnímu jednání důvěryhodnost. Oběť, která uvěří, že peníze skutečně dorazily, zboží odesílá, aniž by zjistila, že žádná platba nikdy neproběhla. V některých případech podvodníci odkazují oběť na falešné platební portály nebo přesměrovací odkazy, které vypadají jako známé platební brány, což vytváří iluzi, že transakce je autentická. [9]

Další variantou bazarového podvodu je, že podvodník předstírá zájem o zakoupení zboží, které oběť nabízí. Tvrdí, že zboží chce rychle koupit, aniž by jej osobně viděl a obvykle tvrdí, že zboží je určeno „pro rodinného příslušníka“ nebo „přátele v zahraničí“. V tomto případě podvodník žádá oběť o zaslání zboží na adresu, která je obvykle mezinárodní nebo komplikovaná na ověření. Nabízí falešné potvrzení o převodu peněz nebo používá falešné e-maily s instrukcemi k provedení transakce, která ve skutečnosti nikdy neproběhne. Pokud oběť zboží odešle, zjistí, že žádná platba nikdy nebyla uskutečněna a její snaha získat zpět zboží či peníze je marná. [9]

K obraně proti bazarovým podvodům je nezbytné používat bezpečné platební metody, ověřovat identitu protistrany a zvolit důvěryhodnou prodejní platformu. Ostražitost a ověřování detailů, jako je například historie prodejce nebo reference ostatních kupujících, mohou oběti ušetřit spoustu peněz a nepříjemností. [9]

2.1.5 Falešný bankéř

Falešný bankéř je vlastně takovým poddruhem vishingu. Jedná se konkrétní vishing, zaměřený přímo na bankovní sektor. Falešným bankéřem se rozumí osoba, která se vydává za bankéře, nebo pracovníka v komunikačním středisku jedné z bank. Klient se nejdříve stává obětí pomyslné nahozené udičky ve formě phishingu, což může být například

podvodná hromadná SMS zpráva, na kterou klient klikne a zde pod záminkou například doplatku za clo zadá své bezpečnostní údaje sloužící k přihlášení do internetového bankovníctví. Předá tak útočnickovi citlivé údaje, které mu postačí pro přihlášení do internetového bankovníctví klienta. Nicméně v tuto chvíli ještě podvodník nemůže autorizovat platby bez klientova souhlasu. Nyní volá falešný bankéř, který se představí jako pracovník banky a vysvětlí klientovi, že zaznamenal na jeho účtu podezřelé transakce a že pravděpodobně došlo k podvodu. V tu chvíli se podvodník vlastně staví do role jakéhosi zachránce klientových peněžních prostředků. Bohužel nic netušící klient ve strachu uposlechne podvodných pokynů falešného bankéře, který klienta nabádá, aby urychleně své prostředky zachránil tím, že je převede na jiný (podvodný) účet, který mu falešný bankéř nadiktuje. Je to celé opět otázka krátkého času, nátlaku ze strany falešného bankéře a hra na emoce, při kterých klient ve strachu bez rozvahy své peníze odešle na cizí účet, čímž o své finanční prostředky, jimiž na svém bankovním účtu disponoval navždy přijde. [9]

2.1.5.1 *Původ slova*

Slovo „falešný“ pochází ze staroslovanského *falěšb*, odvozeného z latinského *fallacia*, což znamená klam nebo lest. Tento význam se dobře hodí k popisu osoby, která klame ostatní tím, že se vydává za někoho, kým není. Slovo „bankéř“ je zase odvozeno z italského *banca*, což znamená lavice nebo stůl, u kterého probíhaly finanční transakce. [15][16]

2.1.6 Moderní kontext

Dnešní „falešní bankéři“ využívají techniky sociálního inženýrství, aby přiměli oběti odhalit citlivé údaje, jako jsou přístupové kódy, čísla účtů nebo hesla. Tato podvodná metoda vzešla v maximální aktuálnost hromadným přesunem lidí do digitálního světa, a to příchodem Covidu 19. Podvodníci se při komunikaci odvolávají na bezpečnostní důvody, čímž vzbuzují u obětí pocit naléhavosti. [9]

S rozvojem kyberkriminality a phishingových útoků se termín „falešný bankéř“ stal širším označením pro všechny podvodníky, kteří zneužívají identitu bankovních institucí. Tento fenomén je dnes celosvětovým problémem, na který reagují banky i legislativa prostřednictvím osvěty, bezpečnostních protokolů a technologických řešení. [9]

Pojem „falešný bankéř“ tak zůstává aktuální a odráží jednu z nejstarších forem podvodů – zneužití důvěry ve finanční instituce. [9]

2.1.7 Falešné investice

Falešné investice jsou dalším z mnoha problémů hromadné migrace lidstva do digitálního světa. Oběť takové falešné investice se nechá snadno zlákat na myšlenku rychlého zisku velkého obnosu peněz. Tomu výrazně přispívá absence kritického myšlení. Podvodníci mnohdy používají k nalákání svých obětí falešnou reklamu s tváří někoho mediálně známého, kdo je finančně movitý a vzbuzuje u lidí důvěru. V současné době se snaží osobnosti upozornovat na to, že jejich tvář může být zneužita ve prospěch falešného investování, nicméně i tak je tento typ podvodu silně populární a z hlediska podvodníků také velmi úspěšný. Podvodníci se rychle vyvíjejí a dokážou vytvořit i podvodné internetové investiční platformy, které vypadají naprosto věrohodně, a dokonce nabídnou podváděné osobě náhled na to, jak se jeho finance zhodnocují. Ovšem až ve chvíli, kdy se oběť pokusí své vydělané peníze z podvodného investičního portálu vybrat, zjistí tvrdou realitu. [9]

2.1.7.1 Původ slova

Slovo *investment* původně vůbec nesouviselo s penězi. Na začátku znamenalo třeba obléknutí ceremoniálního roucha nebo převzetí nějakého úřadu. Až později začalo znamenat vojenské obklíčení a pak taky finanční vklad. První obchodní významy se objevily v 17. století, když lidé začali vkládat peníze do společností, jako byla Východoindická. Časem se to rozšířilo na obecné investování – tedy vložit peníze s nadějí, že se z toho něco vydělá. [17]

2.1.7.2 Použití

Podvodné investice jsou v praxi neřídka kombinovány s dalšími podvodnými metodami, například s phishingem či falešnými reklamami na sociálních sítích. Typicky jsou spojeny s tzv. „spoofingem identity“, což je metoda, kdy podvodníci vytvoří falešnou investiční platformu nebo webovou stránku, která se tváří jako legitimní investiční společnost. Tyto podvodné stránky působí velmi profesionálně, protože kopírují vzhled a branding známých finančních institucí, což oběti může zmást a utvrdit v dojmu, že jednájí se skutečnou společností. [9]

Podvod obvykle začíná lákavou nabídkou, která se objeví například ve formě reklamy na internetu nebo zprávy v e-mailu či na sociálních sítích. Nabídka slibuje vysoké a rychlé zhodnocení investic do atraktivních oblastí, jako jsou kryptoměny, startupy nebo zelené technologie. Oběť, motivována vidinou snadného zisku, klikne na odkaz v reklamě, který ji

přesměruje na podvodnou stránku. Zde je vyzvána k registraci a vložení prvního vkladu na svůj „investiční účet“. [9]

Jakmile oběť provede vklad, podvodníci ji mohou kontaktovat prostřednictvím telefonátu nebo e-mailu, kde se představí jako zástupci investiční společnosti, pod falešnými jmény či s fiktivními tituly. Telefonát se tváří profesionálně, podvodníci používají odborný jazyk a oběti ukazují falešné výpisy z investičních účtů, které ukazují zisk. To oběť utvrzuje v tom, že její peníze rostou a často ji motivuje k dalším vkladům. [9]

Co je obzvlášť cynické, podvodníci někdy dokonce oběti varují před jinými podvodnými investicemi, aby si získali její důvěru. Oběti mohou být dokonce vyzvány k ověření, že jednájí s legitimní společností – například kontrolou, zda adresa webu nebo kontaktní údaje odpovídají údajům dostupným na internetu. Podvodníci tak vytvoří iluzi bezpečí, která oběť přesvědčí o pravosti celé operace. [9]

Výsledkem je, že oběť pokračuje v zasílání peněz na podvodné účty, aniž by si uvědomila, že všechny vložené prostředky jsou nenávratně ztraceny. V okamžiku, kdy se oběť rozhodne peníze vybrat nebo investici ukončit, podvodníci přestanou komunikovat a celá „společnost“ zmizí. Tento typ podvodu zanechává oběti nejen finančně zničené, ale i emocionálně traumatizované. [9]

3 OBRANNÉ MECHANISMY

Tato kapitola se zaměřila na obranné mechanismy a způsoby, jak se chovat na internetu, aby se minimalizovala šance stát se obětí podvodníků. Kapitola se zaměřila jak na pasivní, tak aktivní opatření. V druhé části kapitoly byly rozebrány obranné mechanismy, kterými se snaží své klienty chránit vybraná banka, konkrétně Česká spořitelna.

3.1 Preventivní opatření

Chovat se dnes na internetu obezřetně je důležitější než kdy dříve. Prostředí internetu je dnes plné všemožných nástrah, kolikrát tvářících se naprosto nevinně. A to nemusí nutně být jen podvod, ale procházení dnešního internetu vyžaduje i určitý odstup a kritické vnímání každé informace, kterou si zde přečteme. Člověk se musí z velké části spolehnout jen a jen na své kritické myšlení. V nepředstavitelné nevýhodě jsou starší lidé, kteří nemají nikoho, kdo by jim vysvětlil, jak se v digitálním světě správně chovat. Doba jde velmi rychle dopředu a tito lidé často mají pocit, že nestíhají s touto dobou jít, nicméně nemají tak úplně na výběr, instituce totiž velmi tvrdě tlačí na paperless iniciativy a pokouší se běžné denní styky s klienty přesouvat do digitální podoby. Jedna věc je, že se mladé generace na digitální svět adaptují daleko rychleji, přesto školství tuto dobu také úplně nereflektuje. Ve společnosti často rezonuje téma toho, proč školství u nás dostatečně nevzdělává mladé lidi finanční gramotnosti, stejně tak by pravděpodobně mělo reflektovat problémy kritického uvažování na internetu, správného nakládání s podávanými informacemi a také důsledně zvažovat každé přihlášení, finanční transakce a nakládání s citlivými a zneužitelnými informacemi.

3.2 Aktivní opatření

Jak se aktivně bránit proti nástrahám dnešního digitálního světa? Tato opatření vyžadují vědomou činnost uživatele. Jsou to postupy, na které je třeba myslet při nakládání s informacemi, při nákupu na internetu, zkrátka při každém použití vlastních citlivých dat a při finančních transakcích.

3.2.1 Obezřetnost při sdílení osobních údajů

Je důležité být opatrný při sdílení citlivých údajů jako jsou adresa, telefonní číslo, číslo sociálního pojištění nebo platební informace. Tyto údaje by neměly být sdíleny s neznámými osobami nebo na veřejných platformách. Sociální sítě jsou výborným nástrojem pro komunikaci, ale také představují rizika. Uživatelé často sdílejí více osobních informací, než je nutné, což může usnadnit útočníkům přístup k vašim účtům nebo jiným citlivým údajům. [18]

Fotografie pořízené chytrými telefony obsahují GPS souřadnice, které mohou prozradit místo, kde byla fotografie pořízena. Proto je důležité být opatrný při sdílení fotografií na sociálních sítích a používat funkce, které tyto údaje odstraní před sdílením. [18]

3.2.2 Důkladná kontrola odkazů

Důkladná kontrola odkazů je zásadní pro zajištění bezpečnosti při procházení internetu. Odkazy mohou skrývat nebezpečné hrozby, jako jsou phishingové útoky, malware nebo ransomware, které mohou vést k vážným bezpečnostním problémům, včetně krádeže osobních údajů nebo finančních ztrát. [19]

Je důležité být obezřetný při klikání na odkazy, zvláště pokud pocházejí z neznámých zdrojů. Jedním ze způsobů, jak zkontrolovat bezpečnost odkazu, je použití nástrojů pro kontrolu odkazů. Tyto nástroje analyzují URL a hlásí, zda je bezpečný nebo nebezpečný. [19]

Dalším krokem je kontrola URL před kliknutím. Je potřeba ověřit odkaz ke zjištění skutečné URL adresy, zda odpovídá očekávanému zdroji. Uživatel by měl také používat zabezpečené protokoly, jako je "https", které zajišťují šifrování dat při přenosu. Zkrácené odkazy mohou být zvláště nebezpečné, protože skrývají skutečnou adresu URL. V takovém případě je dobré použít funkce jako je preview, nebo nástroje, které odhalí cílovou stránku. [19]

Implementace robustních bezpečnostních opatření, jako je dvoufázové ověření a používání antivirových programů, může také pomoci chránit před nebezpečnými odkazy. Je důležité být vždy skeptický vůči neznámým odkazům a nikdy neotevírat podezřelé odkazy zvláště v e-mailech nebo zprávách od neznámých odesílatelů. [19]

3.2.3 Důkladná kontrola e-mailů

Důkladná kontrola e-mailů je zásadní pro zajištění bezpečnosti a ochrany před kybernetickými hrozbami. E-maily jsou často cílem phishingových útoků, ransomwaru a dalších typů kybernetických útoků, které mohou vést k vážným bezpečnostním problémům včetně krádeže osobních údajů nebo finančních ztrát. [20]

Je důležité být obezřetný při procházení e-mailů, zvláště těch, které pocházejí z neznámých zdrojů. Jedním ze způsobů, jak zkontrolovat bezpečnost e-mailů, je pozorné prohlížení hlaviček e-mailů a těla zprávy. Hlavičky e-mailů mohou prozradit, zda e-mail pochází z legitimního zdroje nebo zda je to pokus o phishing. Dále je důležité ověřit adresu odesílatele, protože útočníci často používají podobné domény, aby oklamali příjemce. [20]

Dalším krokem je kontrola příloh a odkazů. Přílohy mohou obsahovat škodlivý kód, který se aktivuje po otevření a odkazy mohou vést na falešné stránky určené k získání citlivých informací. Je žádoucí používat antivirové programy k prohledání příloh a nikdy neotevírat odkazy z podezřelých e-mailů. [20]

3.2.4 Důkladná kontrola certifikátů navštěvovaných stránek

Důkladná kontrola certifikátů navštěvovaných stránek je zásadní pro zajištění bezpečnosti a ochrany před kybernetickými hrozbami. Certifikáty SSL/TLS jsou klíčové pro ověření identity webové stránky a zajištění šifrované komunikace mezi uživatelem a serverem. [21]

Je důležité být obezřetný při návštěvě stránek a kontrolovat, zda mají platný certifikát SSL/TLS. Tento certifikát je obvykle indikován ikonou zámku v adresním řádku prohlížeče. Pokud je certifikát platný, znamená to, že komunikace mezi uživatelem a webovou stránkou je šifrovaná a chráněna před odposlechem nebo zneužitím dat. [21]

Je nutné ověřovat také datum platnosti certifikátu. Pokud je certifikát vypršený nebo neplatný, může to znamenat, že stránka není bezpečná nebo že je certifikát falešný. Některé prohlížeče automaticky varují před stránkami s neplatnými nebo vypršenými certifikáty, ale je důležité být aktivní a kontrolovat tyto informace samostatně. [21]

Dále je důležité ověřit vydavatele certifikátu. Legitimní stránky obvykle používají certifikáty od renomovaných certifikačních autorit, jako je GlobalSign nebo DigiCert. Pokud je certifikát vydán neznámou nebo podezřelou autoritou, může to být známkou nebezpečné stránky. [21]

3.2.5 Kritické vnímání informací

Kritické vnímání informací je zásadní dovednost v dnešním světě, kde je k dispozici obrovské množství dat a informací. Je důležité naučit se rozlišovat mezi spolehlivými a neověřenými zdroji, aby se předešlo dezinformacím a chybným závěrům. [22]

Je důležité být obezřetný při konzumaci informací z médií, sociálních sítí a dalších zdrojů. Dále je nutné správně posoudit zdroj informací a zvážit jeho důvěryhodnost. Zkoumáme, zda informace jsou podporovány důkazy nebo zda jsou založeny na spekulacích. V neposlední řadě je důležité sledovat, zda informace nejsou zkreslené nebo zaujaté. [22]

Dalším krokem je ověření informací přes více zdrojů. Pokud je určitá informace prezentována pouze v jednom zdroji, je vhodné ji ověřit u dalších důvěryhodných zdrojů. To pomáhá odhalit případné nesrovnalosti nebo dezinformace. [22]

Implementace kritického myšlení při vnímání informací může také pomoci chránit před manipulací a propagandou. Je důležité být skeptický vůči informacím, které vypadají příliš dobře (nebo špatně) na to, aby byly pravdivé, nebo které vyvolávají silné emoce bez dostatečných důkazů. [22]

Vzdělávání uživatelů o kritickém myšlení je také klíčové. Pravidelné školení může pomoci uživatelům rozpoznat neověřené nebo zaujaté informace a naučit se, jak se jim vyhnout. Organizace by měly podporovat kritické myšlení a vést své zaměstnance k tomu, aby vždy zvažovali více zdrojů a důkazů před přijetím informací za pravdivé. [22]

Kritické vnímání informací je zásadní pro udržení informované a zodpovědné společnosti, kde jsou rozhodnutí založena na spolehlivých datech a důkazech. [22]

3.2.6 Ověřování finančních protistran a recenzí

Ověřování finančních protistran a recenzí je zásadní pro zajištění bezpečnosti a důvěry v obchodní vztahy. V dnešní době, kdy je trh plný nabídek od různých firem je důležité prověřit důvěryhodnost potenciálních partnerů a ověřit pravost recenzí. [23]

Je také vhodné navštívit národní soudní rejstříky nebo registry dlužníků, aby se získaly základní informace o společnosti, jako jsou registrační údaje a historie změn ve vlastnické struktuře. Kontrola finančních výsledků, jako jsou rozvahy, výkazy zisku a ztráty finančních poměrových ukazatelů, umožňuje posoudit finanční situaci společnosti. Nástroje pro úvěrovou analýzu, jako jsou platformy EURODEBT.eu nebo Malcom Finance, nabízejí

komplexní hodnocení rizik spolupráce s danou společností. Hledání názorů a referencí o firmě na internetu může poskytnout cenné rady ohledně pověsti společnosti. [23]

Při ověřování recenzí je důležité dbát na transparentnost. Nová pravidla pro e-shopy vyžadují, aby vysvětlovaly, jak zajišťují pravost recenzí. Pokud neověřují recenze, musí to uvést. Zveřejňování falešných spotřebitelských recenzí nebo doporučení je zakázáno a může vést k sankcím. Prodávající musí být transparentní ohledně způsobu ověřování recenzí, aby spotřebitelé věděli, zda jsou recenze autentické. [23]

Implementace těchto opatření může pomoci chránit před nekalými obchodními praktikami a zajišťovat bezpečné obchodní vztahy. Je důležité být aktivní při ověřování finančních protistran a recenzí, aby se předešlo potenciálním rizikům. [23]

3.2.7 Password management

Správa hesel je zásadní pro zajištění bezpečnosti a ochrany osobních údajů v digitálním světě. S rostoucím počtem online účtů je důležité mít robustní systémy pro generování, ukládání a správu hesel. [24]

Je nutné vytvářet silná a jedinečná hesla pro každý účet. Silná hesla by měla být dlouhá, minimálně 16 znaků a měla by obsahovat kombinaci velkých a malých písmen, číslic a speciálních znaků. Používání heslových frází, které jsou snadno zapamatovatelné, ale obtížně uhodnutelné je také doporučeno. [24]

Dalším krokem je použití šifrování pro ochranu hesel. Šifrování zajišťuje, že i když jsou hesla ukradena, zůstanou nečitelná pro útočníky. Implementace dvoufázového ověření (2FA) přidává další vrstvu zabezpečení, protože i když je heslo prolomeno, útočník bude potřebovat další ověřovací faktor pro přístup k účtu. [24]

Používání heslových manažerů je klíčové pro bezpečné ukládání a správu hesel. Tyto nástroje generují a ukládají komplexní hesla, takže uživatelé si potřebují pamatovat pouze jedno hlavní heslo pro přístup ke všem účtům. Heslové manažery, jako jsou LastPass nebo KeePass, nabízejí šifrované úložiště a automatické vyplňování hesel, což zjednodušuje používání silných hesel. [24]

Je také důležité pravidelně aktualizovat hesla a sledovat aktivitu na účtech, aby se předešlo neoprávněnému přístupu. Nikdy nezprístupňovat svá hesla jiným osobám, protože to může vést k bezpečnostním rizikům. [24]

Implementace robustních bezpečnostních opatření, jako je centralizovaná správa hesel a technologie pro prevenci běžných hesel, může dále posílit bezpečnost. Vzdělávání uživatelů o bezpečných praktikách správy hesel je také zásadní pro udržení informované a zabezpečené digitální komunity. [24]

3.2.8 Vzdělávání

Vzdělávání o bezpečnosti na internetu je zásadní pro zajištění bezpečnosti a ochrany uživatelů v digitálním světě. Je důležité začít u dětí a mládeže, aby se naučily rozpoznávat online hrozby, chránit své soukromí a bezpečně komunikovat na internetu. [25]

Vzdělávání by mělo být přizpůsobeno věku a vývojovému stádiu studentů. Základní školy mohou začít s jednoduchými koncepty, jako je rozpoznání nebezpečí a ochrana osobních údajů. Střední školy mohou prohloubit znalosti o online hrozbách, jako jsou phishingové útoky a kyberšikana, a naučit studenty, jak bezpečně používat sociální sítě a chránit své online profily. [25]

Na úrovni středních škol a vysokých škol je důležité zaměřit se na sofistikovanější témata, jako jsou kybernetické útoky, ochrana dat a zodpovědné používání technologií. Studenti by měli být schopni kriticky posuzovat informace a rozpoznávat nebezpečné stránky nebo e-maily. [25]

Vzdělávání by mělo být integrováno do celoškolního přístupu, který zahrnuje učitele, rodiče a komunitu. Projekt EVOLVE a další iniciativy nabízejí materiály pro rozvoj digitální gramotnosti a bezpečného chování online. Programy jako Be Internet Awesome od Googlu poskytují učitelům nástroje pro výuku digitální bezpečnosti a občanství. [25]

Je také důležité zapojit rodiče a pečovatele do procesu vzdělávání, aby mohli podporovat děti v jejich online aktivitách a pomáhat jim rozvíjet kritické myšlení a digitální gramotnost. Vzdělávání by mělo být interaktivní a zahrnovat role-playing, hry a videa, aby studenti lépe pochopili online rizika a naučili se, jak se jim vyhnout. [25]

3.2.9 Používání anonymizačních nástrojů

Jednou z nejznámějších anonymizačních technologií je síť Tor. Tor funguje jako decentralizovaná síť serverů, které si předávají požadavky, aby skryly skutečnou IP adresu uživatele. Díky tomu je téměř nemožné určit, kdo přistupuje k jakým informacím. Prohlížeč Tor je založený na Firefoxu a obsahuje doplňky jako HTTPS Everywhere a NoScript, které dále zvyšují bezpečnost. [26]

Další možností jsou anonymizační VPNky, které šifrují váš internetový provoz a mění vaši IP adresu. Tyto služby jsou efektivní pro ochranu před sledováním poskytovatelem internetových služeb nebo jinými třetími stranami. Některé VPNky, jako je ExpressVPN, jsou speciálně navrženy pro použití s Tor a nabízejí pokročilé bezpečnostní funkce. [26]

Proxy servery jsou další možností pro anonymizaci, ale jsou méně bezpečné než VPNky a Tor. Používají se k přeposílání požadavků, aby skryly IP adresu, ale často ohrožují soukromí uživatelů. [26]

Vzdělávání uživatelů o bezpečném používání anonymizačních nástrojů je klíčové. Je důležité pochopit, že žádný nástroj nemůže garantovat absolutní anonymitu, ale může výrazně snížit riziko sledování a úniku osobních údajů. [26]

3.3 Pasivní opatření

Nyní se práce přesouvá k pasivním opatřením, která se zaměřují na strategie a techniky, jež nás pomáhají chránit před kybernetickými hrozbami bez aktivního zásahu. Tyto pasivní metody jsou zásadní pro vytváření robustní obrany proti kybernetickým útokům a zajišťují kontinuální bezpečnostní pokrytí i v situacích, kdy nejsou k dispozici aktivní bezpečnostní týmy nebo když je nutno minimalizovat lidskou intervenci. [27]

Pasivní opatření zahrnují implementaci bezpečnostních systémů, jako jsou firewally, síťové detektory a antivirové programy, které automaticky monitorují a reagují na potenciální hrozby. Tyto systémy jsou navrženy tak, aby fungovaly na pozadí, aniž by vyžadovaly přímou lidskou kontrolu, a poskytují tak nepřetržitou ochranu proti kybernetickým útokům. [27]

3.3.1 Antivirus

Antivirové programy používají různé metody k detekci hrozeb, včetně metody tzv. signature-based detection, která porovnává soubory s databází známých malware znaků, behavior-based detection, která sleduje podezřelé chování, a metoda tzv. heuristic-based detection, která identifikuje nové, dosud neznámé hrozby. Všechny zmíněné metody umožňují antivirovým programům účinně chránit před známými i novými typy malware. [28]

Moderní antivirové programy nabízejí real-time protection, což znamená, že neustále monitorují systém na podezřelou aktivitu a automaticky blokují nebo odstraňují detekované hrozby. Kromě ochrany proti malware, antivirové programy také chrání před spamem a

škodlivými webovými stránkami, které mohou infikovat počítač prostřednictvím phishingových útoků nebo falešných reklam. [28]

Implementace antivirového softwaru je zásadní pro malé i velké podniky, protože zajišťuje ochranu citlivých dat a zabraňuje finančním ztrátám způsobeným kybernetickými útoky. Kromě toho antivirové programy často poskytují další bezpečnostní funkce, jako jsou správci hesel nebo virtuální privátní sítě, které dále zvyšují bezpečnost uživatele. [28]

3.3.2 Aktualizace softwaru

Aktualizace softwaru je zásadní součástí kybernetické bezpečnosti, protože zajišťuje opravu zranitelností a chyb v softwarových aplikacích, které by mohly být zneužity útočníky. Tyto aktualizace často obsahují bezpečnostní aktualizace, které opravují známé slabiny a zabráňují útokům, které by mohly vést k úniku dat nebo ovládnutí systému. [29]

Je důležité pravidelně aktualizovat operační systémy, prohlížeče a další aplikace, aby se minimalizovalo riziko zneužití známých zranitelností. Útočníci totiž často cílí na starší neaktualizované verze softwaru díky znalosti jejich slabin. Ty jsou v novějších verzích postupně opravovány. [29]

Aktualizace softwaru také často přináší nové bezpečnostní funkce a vylepšení. Ty mohou pomoci chránit před novými typy hrozeb, např. aktualizace prohlížečů mohou zahrnovat lepší ochranu proti phishingovým útokům nebo vylepšené šifrování. [29]

Implementace automatizovaných aktualizčních procesů může pomoci zjednodušit údržbu softwaru a zajistit, že všechny systémy jsou aktuální a chráněné. Organizace by měly mít jasnou strategii pro aktualizaci softwaru, která zahrnuje pravidelné kontroly a instalaci bezpečnostních aktualizací. [29]

3.3.3 Používání bezpečných prohlížečů

Používání bezpečných prohlížečů je zásadní pro ochranu osobních údajů a zajištění bezpečnosti během procházení internetem. Moderní prohlížeče nabízejí řadu bezpečnostních funkcí, které rovněž pomáhají chránit před kybernetickými hrozbami, jako jsou phishingové útoky, malware a sledování online aktivit. [30]

Jedním z nejbezpečnějších prohlížečů je Tor Browser. Ten skrývá IP adresu uživatele a šifruje procházení stránek, aby znesnadnil sledování online aktivit. Další bezpečnou

možností je Brave Browser, který blokuje sledovací skripty a reklamy, čímž chrání soukromí uživatelů. [30]

Prohlížeče jako Firefox a Chrome také nabízejí robustní bezpečnostní funkce, mezi které patří automatické blokování nebezpečných stránek a pravidelné bezpečnostní aktualizace. Tyto prohlížeče často zahrnují také rozšíření, která mohou dále posílit bezpečnost, jako je HTTPS Everywhere nebo uBlock Origin. [30]

Stejně jako u operačních systémů, i prohlížeče je potřeba pravidelně aktualizovat, aby se minimalizovalo riziko zneužití známých zranitelností. Používání bezpečných prohlížečů je klíčové pro ochranu citlivých informací a zajištění bezpečného používání internetu. [30]

3.3.4 Používání bezpečných Wi-Fi sítí

Používání bezpečných Wi-Fi sítí je zásadní pro ochranu osobních údajů a zajištění bezpečnosti při online aktivitách. Bezpečné Wi-Fi sítě jsou chráněny silným šifrováním a robustními bezpečnostními protokoly, které znesnadňují neoprávněný přístup k uživatelským datům. [31]

Jedním z nejdůležitějších kroků k zabezpečení Wi-Fi sítě je použití moderních šifrovacích protokolů, jako je WPA3 nebo alespoň WPA2 s šifrováním AES. Tyto protokoly poskytují robustní ochranu proti útokům a zajišťují, že data přenášená přes síť jsou šifrována a chráněna před odposlechem nebo zneužitím. [31]

Dalším krokem je změna výchozích nastavení routeru, včetně názvu sítě (tzv. SSID) a hesla pro administraci. Tyto údaje by měly být jedinečné a silné, aby se předešlo snadnému prolomení hesla útočníky. Filtrování MAC adres může být další vrstvou ochrany, ale není stoprocentně spolehlivé, protože útočníci mohou použít techniku spoofingu. [31]

Pravidelné aktualizace routeru jsou také klíčové pro udržení bezpečnosti sítě. Výrobci pravidelně vydávají aktualizace, které opravují zjištěné bezpečnostní nedostatky a zlepšují celkový výkon zařízení. [31]

Při používání veřejných Wi-Fi sítí je důležité být obezřetný a používat VPN, aby se vytvořilo šifrované spojení mezi zařízením a VPN serverem. Toto zajišťuje, že i když se připojíte k nebezpečné síti, vaše komunikace zůstane chráněna. [31]

3.3.5 Bezpečné platební metody

Jednou z nejbezpečnějších platebních metod jsou kreditní karty, které nabízejí ochranu proti neoprávněným transakcím a umožňují snadné zrušení karty v případě ztráty nebo krádeže. Mnohé kreditní karty také poskytují dvoufázové ověření. To vyžaduje další ověřovací faktor, jako je SMS kód nebo biometrická autentizace pro dokončení transakce. [32]

Další bezpečnou možností jsou digitální peněženky, dnes nejznámější je Apple Pay, Samsung Pay nebo Google Pay, které šifrují platební informace a používají tokenizaci čísel karet, aby chránily skutečné údaje o kartě. Tyto služby také často vyžadují biometrickou autentizaci, jako je otisk prstu nebo rozpoznání obličeje, pro ověření transakcí. [32]

Platební brány, jako jsou PayPal nebo Stripe, nabízejí další vrstvu zabezpečení tím, že oddělují platební informace od prodejce. Tyto služby často zahrnují pokročilé bezpečnostní funkce, jako je monitorování transakcí a automatické odhalování podezřelé aktivity. [32]

Je důležité používat pouze důvěryhodné platební služby a vždy kontrolovat, zda je stránka zabezpečena protokolem HTTPS, aby se zajistilo šifrování dat během transakce. [32]

3.4 Slabiny zabezpečení

Pokud analyzujeme, jak banka chrání své klienty, je na místě také konstatovat oblasti, které buď banka chrání nedostatečně, špatně, nebo z jakéhokoliv důvodu není možné tyto oblasti pokrýt. Základní nevýhodou bank v boji proti podvodníkům je zejména fakt, že jejich role je v drtivé většině pouze reakční. To znamená, že podvodníci jsou ti, kteří jsou vždy první, kteří přijdou s novou metodou podvodu, s novými nápady, jak okrádat lidi a banka může pouze a jen reagovat.

Kde banky pravděpodobně budou muset v budoucnu směřovat své úsilí je umělá inteligence. Dá se předpokládat, že vzestup AI bude znamenat také jeho plošné zneužívání ke zločinným účelům, například k zakládání podvodných stránek, k rozesílání podvodných SMS zpráv a podobně. Co může být ještě větší hrozbou je tzv. VoiceAI (AI vytvořené pomocí hlasu), kdy podvodníci budou schopni napodobovat hlas příbuzných obětí a tím tak přesvědčit oběť k předání citlivých údajů. Již nyní vznikají první deepfake videa a fotografie, která lze jen sotva rozlišit od reálných fotografií a lze předpokládat, že tento trend bude pokračovat a tato podvodná videa a fotografie se budou pouze a více zdokonalovat.

Další z oblastí, kterou zkrátka téměř nelze pokrýt, jsou lidské emoce. Velmi často se setkáváme s tím, že klient je tak zmanipulován v podvodu, že pokládá banku, která se ho

snaží zastavit ve svém jednání jako tu špatnou stranu, která ho vlastně chce připravit o super finanční příležitost v případě falešných investic. Dále paku lovescamu, jak již práce popisuje ve své praktické části, která ukazuje, že lidské emoce jsou opravdu silná zbraň.

4 OBRANNÉ MECHANISMY BANK

V této sekci se práce zaměřuje na jednotlivé mechanismy, které banky v České republice aktivně využívají. Tyto mechanismy jsou rozděleny na aktivní a pasivní.

4.1 Aktivní mechanismy

Aktivní mechanismy, které využívá bankovní sektor v České republice, jsou to metody, jak aktivně klienta chránit a upozorňovat na aktuální rizika.

4.1.1 Push notifikace

Existuje několik způsobů, jak povzbudit zákazníky k posílení své bezpečnosti. Pokud je v aplikaci k dispozici bezpečnostní panel, je nejjednodušší zasílat push notifikace o všech relevantních funkcích. Tyto notifikace mohou sloužit jak pro informace o nejružnějších bezpečnostních trendech, tak například personalizované notifikace pro klienta o tom, že by si měl v blízké době aktualizovat heslo, stáhnout nejnovější aktualizaci aplikace, nebo to může být například zpráva o jeho finanční kondici. [33]

4.1.2 Domovská stránka

Domovská stránka podobně jako push notifikace slouží jako prostor, kde se dá informovat klienta o nejnovějších bezpečnostních trendech, podvodných metodách, nebo personalizovaných zprávách klientovi. Domovská stránka má výhodu, že klientovi může nabídnout obsáhlejší text, například i s obrázky. Nicméně klient si toto upozornění přečte až po autorizovaném přihlášení do aplikace. To je nevýhoda oproti push notifikaci, kterou si klient může přečíst v horní liště telefonu kdykoliv, když jej používá, kdekoli v telefonu. Banky mohou používat na své domovské stránce takzvaná pop-up okna, kde se klientovi po přihlášení do internetového bankovníctví objeví obrazovka s informacemi, které mohou jak textem, tak obrázky a výraznými barvami vzbudit v klientovi potřebu si informace přečíst, zároveň formou pop-up oken má banka možnost si vynutit interakci, kdy je nutné, aby klient stiskl nějaké tlačítko, jinak mu pop-up okno nezmizí. [10]

4.1.3 Bezpečnostní přihlašovací metody

V této sekci práce rozebírá konkrétní bezpečnostní metody, které banky nabízí klientům k přihlášení do internetového bankovníctví. Tyto metody slouží jako ochrana před vniknutím podvodníků na cizí bankovní účet za účelem odcizení finančních prostředků.

4.1.4 Dvoufaktorové ověření

Dvoufaktorové ověření (2FA) při přihlášení do internetového bankovníctví je bezpečnostní mechanismus, který výrazně zvyšuje úroveň ochrany uživatelských účtů před neoprávněným přístupem. Proces vyžaduje, aby uživatel při přihlašování prokázal svou identitu dvěma nezávislými způsoby, což minimalizuje riziko zneužití účtu i v případě kompromitace přihlašovacích údajů. [34]

První faktor, který se používá, je něco, co uživatel zná, tedy například heslo nebo PIN. Toto je standardní způsob ověření identity, který je sám o sobě zranitelný vůči různým druhům útoků, jako je phishing nebo keylogging. Proto se k zabezpečení přidává ještě druhý faktor. [34]

Druhý faktor je založen na něčem, co uživatel vlastní nebo čím je. Nejčastěji se jedná o jednorázový kód zasláný na mobilní telefon prostřednictvím SMS, generovaný speciální aplikací (např. Google Authenticator) nebo potvrzený pomocí biometrických údajů, jako je otisk prstu nebo rozpoznání obličeje. Tento kód je obvykle časově omezený a platí pouze několik desítek sekund. [34]

4.1.5 Touch iD

Touch ID je biometrická technologie vyvinutá společností Apple, která umožňuje uživatelům ověřovat svou identitu pomocí otisku prstu. Tento způsob ověření se často používá při přihlášení do internetového bankovníctví nebo při autorizaci plateb, což výrazně zvyšuje bezpečnost celého procesu. [35]

Princip fungování Touch ID spočívá ve snímání otisku prstu pomocí speciálního senzoru zabudovaného v tlačítku zařízení, například v domovském tlačítku iPhoneu nebo na bočním tlačítku novějších modelů. Po přiložení prstu senzor pořídí vysoce kvalitní obrázek otisku, který je následně porovnán s otisky uloženými v bezpečném úložišti zařízení, tzv. Secure Enclave. Tento způsob zajišťuje, že otisky prstů nejsou nikdy ukládány na vzdálených serverech ani synchronizovány s cloudovými službami. [35]

4.1.6 Face iD

Face ID je pokročilá biometrická technologie vyvinutá společností Apple, která umožňuje ověření identity uživatele prostřednictvím rozpoznávání obličeje. Tato metoda se využívá jak pro přihlašování do internetového bankovníctví, tak pro autorizaci plateb a dalších citlivých operací, což přispívá k výraznému zvýšení bezpečnosti i pohodlí uživatelů. [36]

Technologie Face ID funguje na principu projekce a analýzy tisíců neviditelných bodů na tváři uživatele, které jsou následně převedeny do detailní trojrozměrné mapy. Tento sken je porovnáván s daty uloženými v zabezpečeném úložišti zařízení, známém jako Secure Enclave. Důležité je, že tato data nikdy neopouštějí zařízení a nejsou přenášena na vzdálené servery nebo do cloudových úložišť, což minimalizuje riziko zneužití. [36]

Použití Face ID v internetovém bankovníctví nabízí vysokou úroveň ochrany, protože technologie dokáže rozlišit pravou tvář uživatele i od sofistikovaných pokusů o podvod, jako jsou fotografie, masky nebo jiné repliky. Face ID je navrženo tak, aby se přizpůsobovalo drobným změnám ve vzhledu uživatele, například při nošení brýlí nebo růstu vousů, což zajišťuje jeho spolehlivost v běžném používání. [36]

4.1.7 Další aplikace

Sekundární aplikace, jako je George Klíč od České spořitelny nebo ČSOB Smart klíč, představují moderní způsob dvoufaktorového ověřování, který zvyšuje bezpečnost při přihlašování do internetového bankovníctví a autorizaci finančních operací. Tyto aplikace fungují na principu generování jednorázových kódů nebo potvrzování transakcí prostřednictvím notifikací na mobilním zařízení uživatele. [37]

Při přihlašování do internetového bankovníctví je po zadání uživatelského jména a hesla uživateli zaslána žádost o autorizaci přímo do aplikace George Klíč nebo ČSOB Smart klíč. Uživatel následně transakci potvrdí buď zadáním svého PIN kódu, biometrickým ověřením, jako je otisk prstu či rozpoznání obličeje, nebo kombinací těchto metod. Tím je dosaženo výrazně vyšší úrovně zabezpečení, protože pro úspěšné přihlášení je nutný přístup nejen k přihlašovacím údajům, ale i k fyzickému zařízení s nainstalovanou aplikací. [37]

4.2 Pasivní mechanismy

Mezi pasivní prvky ochrany, které banky využívají patří například upozornění, která banky zasílají svým klientům skrz komunikace, push notifikacemi, emaily, nebo SMS zprávami. Jsou to automatická upozornění, nebo informativní zprávy, mající za účel ubezpečit klienta, že postupuje správně nebo upozornit na neobvyklé aktivity.

4.2.1 Notifikace

Notifikace mohou sloužit jako upozornění například na neobvyklý pokus o přihlášení. Tato funkcionality, kterou banky používají funguje na principu alertů. Alerty vyhodnocují, zda se

do internetového bankovníctví nesnaží přihlásit zařízení, které se ještě nikdy na tento účet nepřihlašovalo, nebo také vyhodnocuje, zda se zařízení nenachází na neobvyklém místě, například mimo Evropu. [33]

4.2.2 Funkcionalita

Některé bankovní aplikace využívají funkcionalit, které upozorňují podobně jako na neobvyklá přihlášení také na neobvyklé platby. Často se setkáváme například s funkcionalitou, kdy si bankovní aplikace pamatuje převody, které již byly v historii účtu uhrazeny. Ta pak také upozorňuje klienta ve chvíli, kdy odesílá své peníze na účet, na který ještě v historii žádné peníze neposílal. [10]

4.2.3 Awareness

Banky se snaží také hojně své klienty edukovat o nejnovějších podvodech, nebo podvodných mechanismech, aby své klienty chránily. Edukace může probíhat všemi kanály, jako jsou SMS zprávy, push notifikace, nebo e-maily. Banky tak posílají edukativní obsah klientům ve formě zpráv, naučných videí, nebo například gamifikovaným obsahem ve formě kvízů, nebo testovacích her, které ukážou, jak moc je klient proti podvodům odolný. Bohužel tyto metody nemají příliš velký dopad, neboť klientovi buď padají do spamu na e-mailové platformě, nebo je to pro něj ve chvíli kdy otevírá internetové bankovníctví za účelem převodu nějakých finančních prostředků spíše přítěž, kterou instinktivně řeší zmáčknutím křížku. [10][9]

4.3 Obranné mechanismy České spořitelny

V této kapitole se práce zaměří na obranné mechanismy, které používá pro ochranu svých klientů největší banka v České republice, a sice Česká spořitelna. Česká spořitelna byla vybrána, protože má nejvíce klientů v České republice a také proto, že je autor práce jejím zaměstnancem.

4.3.1 Aktivní mechanismy

Aktivní mechanismy banky jsou specifické procesy, technologie a opatření, které banka proaktivně implementuje a provozuje za účelem ochrany klientů před podvodnými aktivitami. Narozdíl od pasivních opatření, aktivní mechanismy fungují nepřetržitě a jejich cílem je předcházet, detekovat a reagovat na podezřelé nebo neautorizované aktivity v reálném čase. [10]

4.3.1.1 Volá ČS

Tato funkcionality chrání klienty České spořitelny před již rozebranou podvodnou metodou falešný bankéř. Ač by se to na první pohled nemuselo zdát, toto opatření klienta chrání před několika dalšími podvody, neboť ta paralela mezi falešným bankéřem a dalšími podvody, jako jsou phishing, falešné investice a další, je evidentní. Klient obdrží telefonát a po přijetí se na druhé straně ozve „Dobrý den, Česká spořitelna“, jenže kdo klientovi zaručí, že se na druhé straně hovoru skutečně nachází bankéř České spořitelny? Tento obranný mechanismus funguje tak, že klientovi, který obdrží telefonát ze skutečné České spořitelny se na liště displeje jeho telefonu objeví push notifikace z aplikace George, která klienta informuje o tom, že skutečně hovoří se správným člověkem. [10]

4.3.1.2 Ověření bankéře

Ověření bankéře funguje na podobném principu jako „Volá ČS“, cílem je klienta ubezpečit, že skutečně hovoří s bankéřem České spořitelny. Rozdíl je ovšem v tom, že jde o hovor klienta do banky, nikoliv naopak. Klient ve svém internetovém bankovníctví George může vyvolat hovor s klientským centrem České spořitelny a může si tak být jistý, že nevolá podvodníkovi. Na první pohled by to mohlo vypadat jako zbytečná funkcionality, protože si klient může jednoduše dohledat telefonní číslo přímo na stránkách České spořitelny, nicméně to už dnes nemusí být tak jednoduché, protože podvodníkům stačí založit webové stránky velmi podobné, nebo i téměř nerozeznatelné od stránek České spořitelny a pomocí předplacení reklamy na Google, se klientovi může zobrazit tato podvodná stránka dříve než ta oficiální. Pak se může jednoduše stát, že klient zavolá na číslo podvodníků a domnívá se, že hovoří s Českou spořitelnou. [10]

4.3.1.3 Podezřelé platby

Česká spořitelna se snaží chránit své klienty i při platebním styku. Je to vlastně poslední šance klienta zastavit před tím, než odešle své peníze podvodníkovi. Mechanismus detekuje, zda platba, kterou klient odesílá není ničím podezřelá. Pokud vyhodnotí, že ano, klientovi se objeví při autorizaci platby červená výstražná obrazovka, která jej varuje, že platba, kterou se snaží odeslat se zdá být podezřelá. V tu chvíli je cílem, aby si klient v klidu promyslel, zda skutečně nedělá hloupost. Na této obrazovce se také zobrazí informativní a edukativní obsah, který klientovi říká, jaké všechny podvodné metody se klientům dějí a aby si rozmyslel, zda se právě nestal obětí jedné z nich. [10]

4.3.1.4 Bezpečnostní metody

Jedná se o mechanismy, které chrání klienta před neoprávněným vstupem cizího člověka do klientova internetového bankovníctví. Nyní jsou to metody heslo + SMS anebo ověření pomocí Touch iD, nebo Face iD. Tyto metody jsou již rozebrány v sekci výše. [10]

4.3.2 Pasivní mechanismy

Na rozdíl od aktivních mechanismů nejsou pasivní mechanismy navrženy tak, aby automaticky identifikovaly a reagovaly na hrozby v reálném čase. Jejich síla spočívá ve vytváření bezpečného prostředí a snižování rizika prostřednictvím pravidel a technologií, které jsou implementovány při návrhu systémů a produktů. [10]

4.3.2.1 Bezpečnostní web

Bezpečnostní web České spořitelny slouží jako taková wikipedie všech podvodů a metod, jak se proti nim bránit. Klient si tam může pročíst veškeré podvodné trendy, včetně ilustrací a velkého množství edukativního obsahu. [10]

4.3.2.2 Awareness

Česká spořitelna vyrábí obrovské množství edukativního obsahu, ať už jsou to články v médiích, na bezpečnostním webu, nebo také webináře a reklamy. Velmi často se účastní jako sponzor velkých akcí, kde upozorňuje edukativním způsobem pomocí her na všechny možné bezpečnostní trendy. [10]

4.3.2.3 Eset NetProtect GO

Česká spořitelna ve spolupráci se společností Eset vytvořila mobilní aplikaci, která má za úkol klienta chránit při používání internetu. Každou stránku, kterou klient navštíví, na základě bezpečnostních mechanismů a algoritmů vyhodnocuje, zda tato stránka nemůže být něčím nebezpečná. Pokud má klient aplikaci na pozadí aktivní a aplikace detekuje nebezpečný obsah, stránku zablokuje a klientovi na ní zamezí přístup. Dále pak aplikace kontroluje všechny odkazy, na které klient kliká, ať už je to na internetu, nebo třeba v e-mailu, či SMS zprávě. Tím přímo chrání klienta před nebezpečným podvodem a sice phishingem. [10]

II PRAKTICKÁ ČÁST

5 NÁVRH ZPRACOVÁNÍ PRAKTICKÉ ČÁSTI

Praktická část se věnuje hloubkovému rozhovoru. Záměrem hloubkového rozhovoru je detailně probrat s podvedenou osobou její zkušenost s internetovým podvodníkem. Hloubkový rozhovor byl veden se ženou, která se zapletla do podvodné metody „Love scam“ a stala se obětí sociální manipulace, která ji ve finále připravila o několik tisíc euro a k tomu také způsobila trauma na celý život. S podvedenou paní se autor dostal do styku na facebookové stránce, která se zabývá love scamem a sice se jednalo o stránku „Americký voják – romantický podvod“, kde si uživatelé navzájem sdílí své zkušenosti a snaží se tak navzájem chránit před nástrahami tohoto nelítostného sociálního podvodu.

5.1 Vymezení výzkumného problému

Všemožné různé podvodné metody byly rozebrány již v teoretické části práce. Pro praktickou část byla vybrána jedna podvodná metoda, se kterou se bankovní sektor často potýká a která častou znamená nejen významné finanční úniky, ale také poměrně velké psychologické trauma. To je vlastně také zásadní rozdíl mezi romantickým podvodem a jinými podvodnými metodami. Základní domněnkou autora totiž je, že pokud se člověk omylem „uklikne“, přehlédne, nebo ho zkrátka podvodník přistihne při nepozornosti, může to znamenat citelnou finanční ztrátu a ve většině případů i traumatizující zážitek. Protože lovescam je hra na lidské emoce a trvání jednoho podvodu je několikanásobně delší než u jiných metod, tak byl lovescam vyhodnocen jako ideální pro rozebrání do praktické části a také pro hloubkový rozhovor.

5.2 Hloubkový rozhovor

Hloubkový rozhovor je jednou z nejefektivnějších metod kvalitativního výzkumu. Tato metoda umožňuje získat detailní vhled do zkušeností, postojů a emocí respondenta, což je zvláště důležité při zkoumání citlivých témat, jako je lovescam. [38]

Na rozdíl od standardizovaných dotazníků nebo strukturovaných rozhovorů, hloubkový rozhovor poskytuje prostor pro flexibilitu a spontánnost. To je klíčové, protože umožňuje respondentovi vyjádřit se vlastními slovy a tempem, což často vede k odhalení nečekaných souvislostí nebo aspektů zkoumaného jevu. V kontextu mého výzkumu o romantických podvodech je tato flexibilita neocenitelná, neboť každý příběh oběti je jedinečný a často emocionálně náročný. [38]

Při přípravě na hloubkový rozhovor byl kladen důraz na vytvoření vhodné atmosféry a důvěry. Je potřeba si uvědomit, že respondent bude sdílet velmi osobní a často bolestivé zkušenosti, proto je zásadní, aby se cítil bezpečně a respektovaně. To zahrnuje nejen výběr klidného a soukromého prostředí pro rozhovor, ale také vlastní přípravu na empatické a neodsuzující naslouchání. Pro hloubkový rozhovor byla zvolena forma komunikace tykáním, aby byla atmosféra co možná nejuvolněnější. Před samotným rozhovorem proběhlo několik rozhovorů s podvedenou respondentkou nad jejím zážitkem, tím pádem byla atmosféra mezi oběma stranami již z dřívějška důvěrnější. [38]

Pro rozhovor byly připraveny základní okruhy témat a klíčové otázky, zároveň ale bylo nutné si ponechat dostatek prostoru pro spontánní reakce na výpovědi respondenta. Tato strategie umožňuje udržet focus rozhovoru na výzkumné otázky, zároveň však dává respondentovi svobodu vyjádřit se k aspektům, které považuje za důležité. [38]

Autor práce si uvědomuje, že hloubkový rozhovor klade vysoké nároky na komunikační a analytické dovednosti. Zároveň však věří, že právě tato metoda umožní získat unikátní a hluboké porozumění fenoménu lovescamu z perspektivy těch, kteří jím byli přímo zasaženi. Porozumění je klíčové pro vytvoření efektivních strategií prevence a podpory obětí romantických podvodů. [38]

5.3 Otázky pro rozhovor

Pro hloubkový rozhovor bylo připraveno hned několik otázek, které mají za úkol rozkrýt celý příběh a podrobně rozebrat všechny sociální aspekty, metody a techniky, které se podvodník pokoušel na podvedené použít. Zároveň bylo dbáno na sestavení dotazů tak aby bezpečně rozkryly odpovědi na všechny hypotézy.

5.3.1 Dotazy na respondenta

V hloubkovém rozhovoru byly zodpovězeny tyto dotazy:

5.3.1.1 Úvodní část – kontext a důvěra

- Můžete mi, prosím, říct něco o sobě? V jakém pracujete odvětví, v jakém jste rodinném vztahu?
- Jak jste se dostala do kontaktu s osobou, která vás podvedla? (např. sociální sítě, e-mail, seznamka...)

- Jakým způsobem Vás podvodník kontaktoval? Co byla taková ta první zpráva, která rozpoutala následnou konverzaci?
- Jak je to dlouho, co k podvodu došlo?
- Jakým jazykem jste spolu komunikovali?
- Jak dlouho celková interakce s podvodníkem trvala?
- Co vás na této osobě nejvíce zaujalo?
- Bylo něco, co ve vás od začátku vzbuzovalo důvěru?
- Jak často jste spolu přicházeli do kontaktu?
- Popište mi, prosím, jak probíhala běžná konverzace mezi vámi.
- Jaký vztah se podvodník snažil navázat? Spíše důvěrný, přátelský, nebo například i intimní?
- Jak jste vnímala podvodníka? Jak moc byl váš vztah k němu důvěrný?
- Měla jste někdy nějaké pochybnosti o tom, kdo sedí na druhé straně obrazovky?

5.3.1.2 Průběh podvodu

- Jak dlouho trvalo, než došlo k první žádosti o peníze?
- Jaké důvody podvodník uváděl pro žádost o peníze? (např. lékařská péče, návrat domů, clo...)
- Jak jste se cítila v momentě, kdy vás požádal o peníze?
- Bylo to pro vás překvapivé, nebo jste to vnímala jako logické pokračování vztahu?
- Přemýšlela jste tehdy o možnosti, že by mohlo jít o podvod? Pokud ano, co vás nakonec přesvědčilo, že podvodník mluví pravdu?
- Byli ve vašem okolí lidé, kteří vás varovali? Jak jste na jejich rady reagovala?
- Jaká byla vaše motivace k zaslání peněz? Cítila jste například tlak, strach, empatii?
- Používal na vás podvodník praktiky sociální manipulace? Nátlak, vydírání atd..
- Jaký objem peněz jste podvodníkovi zaslala? (Nemusíte odpovídat, pokud je vám to nepříjemné)

- Popište prosím, jak moc byla zásadní Vámi zasláná částka pro Váš domácí rozpočet

5.3.1.3 *Odhalení podvodu a následky*

- Kdy a jak jste si uvědomila, že jste byla podvedena? Co bylo tím zlomovým okamžikem?
- Jak jste se cítila poté, co jste zjistila pravdu? Jaké emoce u vás převládaly?
- Podnikla jste nějaké kroky poté, co jste zjistila, že jste se stala obětí podvodu? (např. nahlášení policii, pokus o získání peněz zpět...)
- Svěřila jste se někdy s podvodem někomu z vašich blízkých?
- Jaká byla reakce vašeho okolí, když jste o tom mluvila? Setkala jste se s pochopením, nebo spíše s kritikou?
- Jak se cítíte teď, když o této zkušenosti semnou hovoříte?
- Jak vás tato zkušenost ovlivnila do budoucna? Máte teď jiný přístup k online komunikaci?
- Podnikáte nyní nějaká preventivní opatření, pro Vás, nebo Vaše okolí?
- Zajímáte se nyní více o problematiku podvádění?
- Popište prosím, zda tento zážitek pro vás byl spíše emocionální, nebo u vás převládal spíše smutek nad finanční ztrátou?
- Myslíte si, že byste se mohla ještě někdy stát obětí nějakého sociálního podvodu?

5.3.1.4 *Reflexe a poučení*

- Když se na to podíváte zpětně, vidíte nějaké varovné signály, které jste tehdy přehlédla?
- Co byste dnes poradila lidem, kteří by se mohli ocitnout v podobné situaci?
- Myslíte si, že se o těchto typech podvodů mluví dostatečně? Pokud ne, jaké formy prevence by podle vás mohly pomoci?

5.4 Hypotézy

Hypotézy jsou klíčovým prvkem při přípravě hloubkového rozhovoru. Na rozdíl od kvantitativního výzkumu, kde hypotézy slouží k statistickému testování, v kvalitativním

přístupu hypotézy pomáhají udržet směr a strukturu rozhovoru. Hypotézy pro hloubkový rozhovor jsou rozděleny na několik oblastí:

- Respondent – Díky dřívější komunikaci obě strany nevstupovaly tak úplně do neznáma, a proto také autor práce mohl přesněji předpokládat, s jakou osobou bude kvalitativní rozhovor prováděn.
- Kontext – Daná problematika rozebíraná v rozhovoru zapadá do kontextu bankovních podvodů a sociálních manipulací.
- Problém – Hypotézy byly vytvořeny tak, aby rozkryly povahu podvodu.

5.4.1 Samostatné hypotézy

Pro potřebu hloubkového rozhovoru bylo vytvořeno celkem osm hypotéz.

Podvodník je z Afriky a vydával se za amerického vojáka

Jedná se o běžnou taktiku lovescamu. Podvodníci, kteří se zabývají lovescamem mnohdy pochází z afrických zemí, nejčastěji to jsou celá centra podvodníků, která se nacházejí v Nigérii, nebo v Ghaně. To je samozřejmě z velké části dáno politickou a ekonomickou situací v zemi, kdy je to pro běžného občana poměrně snadná cesta k zisku velmi slušného objemu financí anebo také mohou být lidé pracující v těchto centrech k této práci nuceni, i toho jsme již byli svědky v televizních novinách při rozkrývání sítí těchto podvodných center. Dalším ze zásadní důvodů, proč jsou většinou místem tohoto podvodného centra země třetího světa je místní legislativa. Ta je upravena většinou tak, že čeští policisté a složky zabývající se podvody nemají pravomoci, jakkoliv pracovat na území těchto zemí, které často nezvládají samy efektivně bojovat proti tomuto organizovanému zločinu.

Podvedenou našel náhodou na sociální síti Facebook

Jednou z běžných strategií podvodníků pro navazování nových kontaktů je náhodné rozesílání žádostí o přidání do přátel. Tuto žádost většinou doprovází nějaká zpráva, ve které často stojí hned nějaká žádost. Podvodníci poté čekají, až se některá z potenciálních obětí chytí a na žádost odpoví. Následně se snaží podvodník svou oběť velmi rychle přesměrovat na jinou platformu, neboť zde na Facebooku hrozí podvodníkovi odhalení a následné odstranění profilu po opakovaném nahlašování ostatními uživateli. Podvodník proto velmi rychle na svou oběť naléhá, aby se jejich konverzace přesunula na platformy jako jsou WhatsApp, Telegram, nebo Hangout.

Podvodník se pokusil s nějakým emociálně zabarveným důvodem oběti namluvit, že potřebuje poslat peníze

Velmi často taktika podvodníka spočívá v metodě navázat s obětí důvěrnější konverzaci. Jakmile má podvodník pocit, že mu oběť důvěřuje a že se mu povedlo navázat buď silně přátelský nebo dokonce partnerský vztah po internetu, postupně přichází s prvními žádostmi o peníze. Můžou to být například žádosti o peníze na zaplacení cla se slibem, že ihned, jak obdrží peníze, které se z různých důvodů někde zdržely, své oběti je vrátí. Nebo prosba o peníze, které by podvodníka osvobodily z jeho fiktivní mise v Afghánistánu. A k těmto prosbám podvodník používá sociální manipulace. Nejdříve zdůrazní pozitiva, které z transakce oběti vyplynou jako je bohatství a podobně. Pokud ovšem na tuto hru oběť nepřistoupí, začne podvodník používat nátlak. Nejdříve předstírané zklamání a smutek ze zjištění, že ho vlastně oběť nemá ráda a pokud ani to nepomůže, podvodník začne s vydíráním například pomocí obětí zaslaných fotografií.

Podvodník psal s viditelnými překlepy a bylo jednoduše poznat, že šlo o cizince

Podvodníci z afrických zemí míří zejména na potenciální oběti z Evropy, tudíž pro svou komunikaci musí využívat internetových překladačů, které nejsou dokonalé a dříve nebo později je zřejmé, že na druhé straně počítače sedí cizinec. Je to jeden z prvních a nejjednodušeji poznatelných znaků, že jde o podvod.

Předpokládám, že se při rozhovorech projeví, že podvodník je méně vzdělaný člověk, který se v zemi třetího světa uchýlil k nekalé praxi snadného finančního obohacení

Tato hypotéza se opírá zejména o fakt, že podvodné sítě mají svá sídla zpravidla v zemích třetího světa. Předpokladem je, že pro lidi zde žijící je to snadný příjem, za poměrně málo vynaloženého úsilí a nedělá jim morální problém okrádat ostatní. Je potřeba ale nezapomenout na takové podvodníky, kteří jsou vlastně také oběťmi, které naletěly například na falešný inzerát slibující lukrativní práci, kterou jsou nakonec nuceni pomocí vydírání nedobrovolně vykonávat.

Podvodník se snažil s obětí navázat i intimní vztah, za cílem následného vydírání prostřednictvím erotických fotografií.

Jak již bylo uvedeno, podvodník se snaží se svou obětí navázat silně přátelský, nebo milostný vztah z důvodu, aby si k němu oběť vytvořila silnou citovou vazbu a také proto, aby zjistil dostatek informací, které by případně mohl proti oběti použít jako prostředek k vydírání v případě, že by oběť odmítla poslat podvodníkovi peníze.

Předpokládám, že se oběť do podvodníka zamilovala a tato emoce ji přiměla zaslat podvodníkovi své finance.

I toto již bylo výše zmíněno. Hypotéza předpokládá, že oběť, se kterou byl proveden hloubkový rozhovor, byla do podvodníka zamilovaná, a to byl ve finále hlavní důvod, proč mu své peníze zaslala.

Podvedená osoba si odnáší ze střetu s podvodníkem velmi silnou emotivní zkušenost, kterou hodnotí jako horší, než finanční ztrátu

Touto hypotézou předpokládám, že lovescam se vyznačuje na rozdíl od ostatních podvodů mimo jiné také tím, že zanechá v oběti velmi silnou emotivní zkušenost, nebo trauma, které následně oběť vyhodnotí, jako horší než celkovou finanční ztrátu.

5.5 Hloubkový rozhovor

Rozhovor probíhal na platformě MS Teams. Pro záznam bylo použito nahrávání v telefonu a v platformě Teams zároveň, pro případnou korekturu, kdyby jedno, nebo druhé nahrávání nezachytilo některé odpovědi respondentky. K nahrávání jsem byla taky použita funkce přepis, nastavená na slovenštinu, neboť respondentka je ze Slovenska. Rozhovor byl veden formou tykání, aby byla respondentka uvolněnější a trochu z ní upadla nervozita. Respondentka si přála, aby její identita zůstala anonymní. Jméno Lena je smyšlené. Respondentka také souhlasila s obsahem hloubkového rozhovoru, který ji byl zaslán s dostatečným předstihem před tím, než byl uskutečněn samotný rozhovor. Následně byl přepis zkompletován, a protože nebyl úplně dokonalý, některé pasáže byly doplněny po poslechu nahrávky. Odpovědi respondentky byly přeloženy do češtiny. Forma odpovědí i styl byl zachován a překlad je tak 1:1.

5.5.1 Aktéři rozhovoru

Pro pochopení rolí v hloubkovém rozhovoru je nezbytné představit oba aktéry, kteří se hloubkového rozhovoru účastní.

5.5.1.1 Ondřej

Ondřej je autor diplomové práce, a zároveň moderátor hloubkového rozhovoru. Obsah rozhovoru byl diskutován s vedoucím práce. K tvorbě rozhovoru byly použity také zkušenosti nabyté v zaměstnání, kde měl autor práce již několikrát možnost účastnit se hloubkového rozhovoru s podvedenými klienty jako moderátor.

5.5.1.2 *Lena*

Lena je respondent tohoto hloubkového rozhovoru. Je to žena ze Slovenska, v době, kdy k podvodu došlo, měla přibližně 45 let. Stala se obětí lovescamu a přišla tak o nižší tisíce eur a zároveň také, jak sama popisuje, o něco uvnitř sebe.

5.5.2 Samotný rozhovor

O: Ahoj Leno. Vítám tě tady na schůzce, mockrát děkuji, že sis na mě udělala čas a věnovala mi svou důvěru. Velmi si vážím toho, že jsi ochotna o svém opravdu silném příběhu mluvit a pomoci této diplomové práci. Rád bych ze začátku řekl něco málo o sobě: Jmenuji se Ondřej Smažinka, studuji bezpečnostní technologie na Fakultě aplikované informatiky ve Zlíně. Svým nadšením pro bezpečnost jsem se dostal do týmu Klientské bezpečnosti na centrále České spořitelny v Praze, kde se každý den věnujeme podvedeným klientům a snažíme se dělat preventivní i aktivní opatření, jak tyto klienty chránit před „kyberšmejdý“. Díky tomu jsem se rozhodl propojit svou práci se studiem pomocí tématu o sociálních manipulacích na bankovních klientech. Byl bych rád, kdyby tato práce sloužila jako osvěta, jako shrnutí a popis jednotlivých podvodů a metod, které podvodníci používají a zároveň poukázat na zákeřnost a vynalézavost podvodníků, která nám každým dnem dokazuje, že pod vedeným může být opravdu kdokoliv z nás.

L: Sdílím tvůj názor a plně souhlasím se vším, co jsi řekl a hodnotím to v principu už jen z toho důvodu, že mám hodně času na sledování této situace a možná i hodně zkušeností, nejen s tím, že se to stalo mě, ale že to také řeším v práci. Takže souhlasím.

O: Ano. Rád bych ještě aby zazněla pravidla tohoto rozhovoru. Dohodli jsme se společně pro lepší atmosféru a také proto, že spolu již komunikujeme delší dobu, že si budeme tykat. Zároveň jméno Lena je fiktivní a tvá identita zůstane naprosto anonymní. Před rozhovorem jsem ti poslal všechny otázky, které ti dnes položím a ty jsi s nimi souhlasila a souhlasila jsi i s tím, že tyto otázky budou obsahem praktické části mé diplomové práce.

L: Ano, souhlasím.

O: Moc děkuji. Tak teď bych tě teda poprosil, jestli bys mohla krátce popovídat něco o sobě.

L: Nebudu uvádět své jméno, ale pracuji ve stejném prostředí jako ty, tedy jako bankovní pracovník už 20 let. Je mi 50 let. Mám plnohodnotnou rodinu – dvě děti, manžela a všechno, co k tomu patří, včetně zvířat a spousty starostí. Práce mě hodně vytěžuje, ale rodinu mám kompletní, nikdo mi nechybí. Necítím se osamělá ani opuštěná.

Pokud by jedním z důvodů, proč někdo začne komunikovat s neznámým člověkem měla být samota, pak to rozhodně nebyl můj případ. Myslím si, že kdybych to měla stručně vyhodnotit, nikdy bych neřekla, že mi něco chybí. Mám všechno. A přesto...

Přijala jsem to – ne jako výzvu, i když zpětně to tak vlastně hodnotím. Byla to výzva. Byla jsem schopná pustit do svého života někoho, koho jsem neznala. A mám za sebou tuto zkušenost – ten člověk mě nejen zmanipuloval, ale i podvedl. A stalo se to.

O: Jak si se vlastně dostala do kontaktu s tou osobou, která tě podvedla, co byl ten spouštěč, a kdy to bylo?

L: Pracuji dlouhodobě v bance a jsem do své práce opravdu hodně ponořená. Už dlouhou dobu působím jako bankovní specialista na hypoteční úvěry.

Práce tvoří asi polovinu mého života a jsem jí zcela podřízená. Lidé obvykle oddělují soukromí a práci, ale u mě se to naprosto prolíná. V době, kdy mi přišla ta zpráva, jsem pracovala jako vždy.

Ta zpráva přišla od člověka, kterého jsem neznala, přes Messenger. Nebyla to žádost o přátelství, ale přímo zpráva v duchu: „Omlouvám se, že narušuji vaše soukromí. Našel jsem váš profil a dostal jsem doporučení od svého známého, abych vás oslovil s žádostí o pomoc při hledání bydlení.“

V té době jsem Facebook ani Messenger moc nepoužívala. Věděla jsem, že existují, ale nebyly součástí mého života. Na Facebook jsem se podívala maximálně jednou za tři měsíce, jen abych viděla, co dělají moji kolegové a přátelé. Jinak mě to nezajímalo.

Messenger jsem téměř neovládala a neznala jsem žádná jeho rizika. Všechny zprávy, které mi tam přicházely, jsem ignorovala a pokud jsem s někým komunikovala, tak jen s rodinou nebo blízkými kolegy.

Najednou mi ale přišla zpráva od neznámého člověka, který žádal o pomoc v rámci mé práce. Vzala jsem to jako pracovní záležitost – někdo potřeboval pomoci s bydlením a dostal na mě doporučení od jiného klienta. Proto si mě dovolil oslovit. Zpráva byla napsaná slovensky, ale působila, jako by byla vytvořená překladačem.

O: Jakože tam byly gramatické chyby?

L: Nebyly tam žádné závažné gramatické chyby. Ta zpráva byla dobře formulovaná, takže jsem v ní žádnou chybu nenašla. Byla velmi zdvořilá, ale bylo znát, že byla napsaná překladačem – hlavně proto, že mi ten člověk tykal.

Byla jsem si téměř jistá, že to není Slovák a že nerozumí tomu, jak u nás funguje tykání a vykání. Překladač z angličtiny tohle nerozlišuje, takže zpráva byla v slovenštině, ale hned od začátku mi tykal.

Brala jsem to tak, že jde o člověka, který potřebuje mou odbornou pomoc a dostal na mě kontakt od nějakého spokojeného klienta. Proto jsem na to pracovně zareagovala – odpověděla jsem mu, že to není problém a ať mi napíše, co přesně potřebuje. Ráda mu pomůžu.

O: Ještě mě zajímá, možná abychom pochopili mechanismus toho oslovování kyberšmejdů, on neposlal žádost o přátelství, že?

L: Neposlal.

V té době jsem neměla moc zkušeností s tím, jak zjistit, kdo to je a co za tím stojí. Takže jsem si samozřejmě prohlédla jeho profil.

Na profilové fotce byl jen nějaký ptáček sedící na louce s květinami. Kromě toho tam byly možná ještě dvě další fotky, obě s přírodní tematikou. Nebyla tam žádná osobní fotografie, jen příroda. Nic, co by o tom člověku něco konkrétního prozrazovalo.

Jeho jméno bylo uvedeno jako Viliam David, ale když jsem se na to podívala blíž, viděla jsem, že to bylo napsáno „Dawit“ s dvojitým „W“. Už podle toho mi bylo jasné, že jde o cizince.

O: Zajímá mě ještě, zda jsi nějak více pátrala po tom profilu, neboť někdy jsou ty znaky podvodného profilu patrné, například velmi málo přátel, či úplně nový profil na Facebooku.

L: Z toho profilu se nedalo nic zjistit. V době, kdy jsem si ho prohlížela, jsem ani nevěděla, co přesně mám hledat nebo jak by to mělo vypadat. Jen jsem chtěla zjistit, jestli se na některé fotce objeví něco, co by mi pomohlo.

Myslím, že u jedné ze dvou fotek byl komentář. Napsala ho nějaká žena, která byla Němka. Když jsem si ji pak později prohlédla blíže, zjistila jsem, že i ona pracuje v bankovníctví.

Postupem času mi došlo, že měl přesně vytipované spektrum lidí, na které se zaměřoval. To jsem ale zjistila až později.

Když jsem se tím začala více zabývat, začala jsem hledat další chyby a přemýšlela jsem, co všechno ještě můžu zjistit. Postupně mi to začalo dávat větší smysl. Nakonec mi došlo,

že šlo o uměle vytvořený profil přesně za tímto účelem – cíleně zaměřený na ženy pracující v bankovníctví. To byl jeho způsob vyhledávání obětí.

Definitivně jsem to pochopila až ve chvíli, kdy jsem se ho během jednoho rozhovoru zeptala, proč jeho příspěvek lajkovala nějaká Němka. Jakmile jsem na to poukázala, ten příspěvek okamžitě smazal. Už si asi všiml, že něco sleduji, že po něčem pátrám.

Je pravda, že jsem se mu asi po týdnu pokusila poslat žádost o přátelství. On mi předtím říkal, že mi ji nemůže poslat, že mu to nejde. Tak jsem to zkusila já – a také mi to nešlo. Měl to zablokované.

O: Ještě mě zajímá pro kontext, kdy jste si začali psát, jak je to dlouho?

L: Oslovil mě někdy v únoru 2021.

Na jeho zprávu jsem, ale zareagovala až přibližně po třech týdnech. Jelikož jsem Facebook ani Messenger aktivně nepoužívala, vůbec jsem nesledovala, co mi tam přichází. Jen občas jsem se podívala.

Když jsem tu zprávu objevila, byla už asi tři týdny stará. Teprve tehdy jsem na ni odpověděla.

O: Dobrá, vraťme se, prosím, k té vaší konverzaci. Jak jsi reagovala na tu zprávu od podvodníka?

L: Pamatuji si, že jsem tu zprávu našla ráno, těsně před odchodem do práce. Jen jsem krátce odpověděla v duchu: „Mrzí mě, že odpovídám tak pozdě, ale pokud mě stále potřebujete, dejte mi vědět, co přesně chcete.“

Odpověď přišla téměř okamžitě. Jakmile jsem dorazila do práce, už jsem od něj měla zprávu. Psala jsem mu slušně ve slovenštině a vykala mu, on také komunikoval slovensky. Bylo mi jasné, že přesně ví, komu píše – věděl, z jaké jsem země i co dělám. Můj profil nebyl uzamčený, a tak bylo snadné zjistit, že pracuji v bance a specializuji se na úvěry.

Ráno jsem mu tedy jen napsala, že nebudu mít čas dlouho si psát, protože mě čeká porada a hned poté pracovní povinnosti. Pokud mu neodpovím hned, ať se nezlobí. Řekl, že to chápe, ale přesto mě okamžitě začal bombardovat zprávami. Když jsem do pár minut neodpověděla, posílal další a další, dokud jsem znovu nenapsala, že mám klienta a opravdu nemohu reagovat.

V průběhu dne pochopil, že nebudu odpovídat okamžitě a ustoupil. Jen se zeptal, kdy končím v práci. Odpověděla jsem, že kolem šesté večer. Přesně v šest už mi psal, jestli jsem doma a mám čas na psaní. Neodpověděla jsem asi půl hodiny a už mi přišly další zprávy: Proč neodepisuji, proč se mu nevěnuji.

Nakonec jsem mu napsala, že jsem si jen četla zprávy o aktuálním dění, a proto jsem si nevšimla, že mi píše. Od té chvíle bylo jasné, že chce komunikovat neustále – a pokud neodpovím, bude posílat zprávy tak dlouho, dokud mu neodepíšu. Jako by testoval, jak dlouho vydržím neodpovídat.

Po hodině jsem mu konečně napsala, že už mám čas a zeptala se, co potřebuje. Nejdřív se představil – kdo je, proč mi píše. Tvrdil, že není Slovák, ale cizinec, a že má kolegy, kteří se bavili o možnosti žít na Slovensku. Prý ho ta myšlenka zaujala natolik, že se rozhodl zjistit, zda by se k nám mohl přestěhovat.

Řekl, že jeho rodiče byli Slováci, kteří kdysi emigrovali do Ameriky, kde se on narodil. Momentálně je na misi v Afghánistánu jako voják americké armády, ale brzy půjde do důchodu. Prý slíbil své matce, že se jednou vrátí na Slovensko, a proto teď hledá dům, kam by se mohl po odchodu z armády přestěhovat.

Zpočátku to celé působilo jako běžná pracovní záležitost. Říkal, že nepotřebuje úvěr, ale spíš někoho, kdo by mu pomohl najít vhodnou nemovitost. Tvrdil, že na mě dostal kontakt od jednoho ze slovenských vojáků, kteří s ním byli na misi v Afghánistánu a že o mně tento voják mluvil velmi dobře.

Přistupovala jsem k tomu profesionálně. Řekla jsem mu, že mám rodinu, dvě děti, práci a jsem dost vytížená. Nemohla jsem trávit celé hodiny psáním, ale zpočátku jsem to stále vnímala jako pracovní komunikaci. V mé branži platí, že pokud se klient neobslouží, najde si jiného poradce. Proto jsem mu odpovídala i v čase, kdy jsem měla volno.

Ale postupně jsem si začala všímat, že komunikace není úplně standardní. Každé ráno mi psal kolem páté nebo půl šesté, což znamenalo, že mě budil. Psali jsme si do devíti, kdy jsem začínala pracovat. Pak přestal, ale večer znovu navázal kolem šesté a konverzace trvala často až do jedenácti. Denně jsme si vyměnili obrovské množství zpráv.

Postupně jsem si uvědomila, že nejde jen o pracovní záležitost. Spíš mě vtahoval do nekonečné konverzace a nechtěl přijmout, že mám i svůj vlastní život.

O: A o čem jste si tak běžně povídali, co bylo náplní vašich konverzací?

L: Tím, že se to občas prolínalo s tím, že jsem se ho ptala, jakou má představu o tom bydlení, co by přesně chtěl, tak mi vyprávěl o sobě, o své rodině. Vyšlo z něj, že má syna, který byl přibližně ve věku mého syna, v té době asi 14 let. Měli jsme společné zájmy, ptala jsem se ho, co jeho chlapec dělá, jak tráví čas. Potom mi vyprávěl o své manželce, která zemřela při autonehodě, když jela na den svých narozenin s dcerou do obchodního domu. Měla tragickou nehodu a obě zahynuly. On to nesl velmi těžce.

Postupně mi vyprávěl o své rodině. O rodičích moc ne, spíš to bylo povrchní, ale zmínil, že jeho rodiče zahynuli, když mu bylo 13 let a že ho dali do dětského domova. Poté byl umístěn do internátní školy, a nakonec ho adoptovala nějaká rodina. Ta rodina měla dceru, se kterou se později oženil. Jeho noví rodiče byli vojáci a on sám se stal vojákem, i když to nebyla jeho volba, spíš musel respektovat rodinnou tradici.

Vyprávěl mi také o své kariéře, jak se stal vojákem, jak to pro něj bylo těžké, protože to nebyla jeho volba, ale rodinná povinnost. A nakonec mi prozradil, že po ukončení vojenské kariéry chce žít na Slovensku, protože jeho rodiče byli Slováci a slíbil matce, že se tam vrátí.

Zpočátku to celé vypadalo jako pracovní záležitost, pomáhat mu s bytem, ale postupně se to začalo měnit v osobní komunikaci. Během našich rozhovorů jsem zjistila, že jsem mu věnovala čím dál více času. Psal mi každý den, ráno i večer, bez přestávky. Každý den mě budil a psal, dokud jsem nešla do práce. Pak jsme komunikovali až do večera, když jsem měla volno. Bylo to opravdu hodně intenzivní.

O: Rád bych se zaměřil na ten sociální aspekt, zajímá mě důvod, proč jsi vlastně přistoupila na tu jeho hru, proč jsi mu neustále odpovídala, i když takhle naléhal, zajímalo by mě, jestli jsi měla pocit, že třeba jsi postrádala v životě něco, co ti on dával.

L: Můžu říct, že to asi fungovalo takhle zhruba první tři týdny, že on neustále psal a já, i když jsem to necítila, jsem z nějaké slušnosti a taky z takového hm, jak to říct, nechtěla mu říct, že nemám čas, měla jsem pocit, že prostě musím odpovédět. I když mě to bavilo, bylo to pro mě zajímavé, protože najednou jsem byla v kontaktu s někým, kdo je v úplně jiné zemi, v nějakém vojenském konfliktu a všechno, co jsem o tom viděla. A teď jsem měla možnost mít někoho, kdo mi o tom může povědět víc, co se třeba už nezveřejňuje. Zajímalo mě to, jsem zvědavý člověk.

A postupně se to vyvinulo do takového přátelství. Po těch prvních dvou, třech týdnech jsem neměla pocit, že mi lže. Jen jsem měla pocit, že velmi naléhá a tlačí na to, kolik času

mu musím věnovat. Až později jsem pochopila, že to bylo součástí izolace, abych neměla čas na nic jiného než být s ním. Abych se odpojila od svých zájmů, přátel a rodiny. Snažil se mě izolovat a udělat tu vazbu silnou. Ale vždy to bylo velmi slušné. Když komunikuješ s cizincem, zvažuješ, jaká je jejich mentalita, co pro ně něco znamená, jak fungují. Já jsem vždy rozlišovala a byla schopná si uvědomit, že to je jiná mentalita než naše. Byla jsem tak slušná, že jsem mu nedokázala říct, že se odmlčím nebo že ho budu ignorovat. Nikdy bych si to nedovolila, protože jsem to brala jako něco, co si nemohu dovolit. Cítila jsem, že musím odpovědět, abych mu neublížila, aby to nevnímal jako neslušnost.

To byly ty první momenty. V těch prvních dvou, třech týdnech jsem si začala všimnout, že píše něco slovensky, ale nebylo to úplně logické, chyběla tam slova, která překladač nedokázal přeložit. A protože jsem věděla, že je Američan, řekla jsem mu několikrát, že nerozumím, co mi píše, a že mi to může napsat v angličtině, abych to lépe pochopila. Tak mi napsal anglicky a já jsem pochopila, co mi chtěl říct. Poté mi řekl, že dobře rozumím anglicky, protože zvládám jeho angličtinu a že mu nevadí, když píšu slovensky, protože si to rychle přeloží. Vzhledem k tomu, že jeho rodiče byli Slováci, měl nějaké základy slovenštiny a nějaké věci si pamatoval. Navíc teď ho i jeho slovenská jednotka učila a tímto způsobem se s nimi spřátelil. Říkal, že chce pokračovat v učení slovenštiny, a proto mu vyhovuje, když píšu slovensky, protože se tím učí.

Mně se líbilo, když psal anglicky, protože jsem hned rozuměla, nemusela jsem se trápit s tím, co vlastně chce, na co se mě ptá. Tak jsme se domluvili, že přestane používat překladač, i když bylo pro něj těžké přiznat, že ho používá. Nejdříve mi tvrdil, že to je jeho způsob psaní, ale já jsem nebyla hloupá. Když jsem viděla, jak mi občas napsal větu v angličtině, protože jsem ho poprosila, protože jsem nerozuměla, co chce, dala jsem ji do překladače a přesně jsem viděla, jak to překladač přeložil. Přeložil to naprosto stejně, jak mi napsal on, takže jsem věděla, že používá překladač. Měli jsme skoro stejný překladač, který překládal stejně hloupě. Tak jsem mu řekla, že přece nepoužívá překladač, že mi má psát rovnou anglicky, bude to rychlejší a lépe pochopím, co chce. Nakonec na to přistoupil a po dvou až třech týdnech jsme začali komunikovat hlavně anglicky, ale i slovensky.

Komunikace byla velmi rychlá. On pravděpodobně zkopíroval text do překladače, přeložil to a odpověděl mi vždy na míru. Nešlo o žádné kopírované fráze nebo jednoduché věty, byly to normální odpovědi, které byly vytvořeny konkrétně pro mě, takže v té době ještě nepoužíval žádné zjednodušené odpovědi pro rychlou komunikaci. Odpovědi byly adresné.

O: A v tu chvíli už jsi začala pochybovat?

L: Začala jsem pochybovat o tom, jestli mi vůbec říká pravdu a jestli to, co mi říká, je vůbec možné, zhruba ve třetím týdnu. Už jsem si všimla, že některé odpovědi byly jako kdyby z jiného úhlu pohledu, že nebyly vždy stejné. Viděla jsem, že se to lišilo od předchozí odpovědi, ale v nějakém základním smyslu to bylo podobné. Začala jsem zpětně hledat, jestli se stala ta událost, o které mi vyprávěl. Zapnula jsem si všechny zprávy, které šly dostat z Afghánistánu. Minutové zprávy – znamená to, že jsem měla aplikaci, která posílala okamžité zprávy, co se tam děje, co se stalo. Porovnávala jsem to s tím, co mi říkal, a protože jsme mluvili hodiny, on toho stihnul hodně vyprávět. Bylo možné zjistit, že ta osoba, která mi ráno něco řekla, se večer vyjádřila jinak, nebo si nepamatovala, že jsme o tom mluvili už ráno. Tím mi vlastně signalizoval, že to není ta stejná osoba, s kterou jsme si povídali.

O: Wow, takže chceš říct, že s tebou komunikovaly dvě osoby zároveň?

L: Hm, ano.

A tedy zhruba po třech týdnech jsem samozřejmě řekla svým kolegům, co se mi stalo. Říkala jsem, že mám na lince někoho, kdo se tváří, že je americký voják a že je v Afghánistánu a píše mi. Moji kolegové byli mladí a řekli: „Proboha, přestaň, to je podvod!“ Ale nezdálo se mi to jako podvod, protože jsem nevěděla, že teď existuje takový podvod.

Vysvětlili mi, o co jde a já jsem si v té chvíli hned do Googlu vyhledala „americký voják“, a už mi vyběhly zprávy o tom, jak probíhá tento typ podvodu. Jak některé ženy byly nachytané tím, že jim někdo tvrdil, že je americký voják, a pak po nich požadoval peníze za výkupné nebo za dovolenou nebo za něco jiného. Všechno to bylo o penězích a byl to jen předstíraný příběh.

Začala jsem se tedy dál vzdělávat, jak to funguje v americké armádě, jaké tam mají hodnosti a kolik asi tito vojáci vydělávají, protože to je veřejná informace. Všechno se dá zjistit. On se mě v těch prvních dnech také hned ptal, co dělám, kolik vydělávám, jak dlouho jsem v práci, protože potřeboval vědět, kolik mám času, velmi ho zajímalo, kolik vydělávám.

Snažil se mě kategorizovat, jestli jsem bohatá, nebo zda jsem normálně vydělávající člověk, snažil se zjistit mou finanční situaci.

Byly tam takové otázky. Neptal se mě přímo, zda mám úspory nebo kolik jich mám, ale ptal se na to, kolik vydělávám a co všechno stojí život na Slovensku. Řekl mi také, kolik

vydělává on, co všechno mu armáda platí, jak se armáda stará o jeho syna, kde je umístěný, že má všechno zařízené v internátní škole, že armáda platí všechno, co potřebuje.

Poté vlastně řekl, že nic nepotřebuje, protože je v Afghánistánu a všechno mu platí americká armáda. Bylo to očekávání, zjišťování mé finanční a rodinné situace. Snažil se zjistit, jaké mám záliby, jaké barvy se mi líbí, jakou hudbu poslouchám, jaké knihy čtu, které filmy mám ráda. Hledal něco, co bychom měli společného. Testoval mě, aby věděl, o čem se mnou může dál mluvit. V podstatě se snažil, abych se zaměřila jen na něj a odpojila se od okolí, abych už trávila čas pouze s ním, abych neměla čas bavit se s někým jiným. Chtěl mi poskytnout všechno, co mám ráda.

O: Takže jsi měla pocit, jako by se z něj stával tvůj přítel.

L: Ano, přesně tak, v té chvíli jsem to cítila tak, že jsme přešli z pracovního vztahu do něčeho osobního, že se stáváme přáteli, že o sobě víme hodně. A když jsme už věděli hodně o sobě, začalo to přecházet na trošku emočnější úroveň. On měl všechno, co potřeboval, byl spokojený, ale i přesto nebyl šťastný. Chyběla mu rodina a chyběla mu žena jako taková.

Snažil se mě napojit na to, že mě chce mít jako nějakou oporu. Já jsem však pořád tvrdila a trvala na tom, že mám všechno, co potřebuji. Mám svou rodinu, mám tu lidi, které mám ráda, a nepotřebuji v podstatě žádné věci, které by mi zalepily nějaké trhliny v životě.

Ale zároveň se mi s ním dobře povídalo. On přijal to, že je můj přítel, a protože jsem o své rodině řekla vše, i to, že v mé skutečné rodině nemám žádné bratry ani bratrance, prostě žádné muže, řekl mi, že v tomto režimu, pokud chci, bude můj bratr.

Takže jsme se dohodli, že se můžeme bavit v této sféře, že on je můj bratr a já jeho sestra. Tak jsem to odsouhlasila.

O: On tedy přijal roli bratra. A nesnažil se navázat i nějaký intimní kontakt? Víš domnívám se, že podvodníci se snaží také často z obětí vytáhnout citlivé fotografie, pomocí kterých by mohli svou oběť vydírat

L: Ne. Ze začátku vůbec ne. Všechno to probíhalo velmi slušně. On jen zjišťoval, co mi chybí v životě a asi na základě toho, co jsem mu řekla, zjistil, že mi chybí bratr, protože jsem ho nikdy neměla, tak se hned nabídl, že by on mohl být mým bratrem na dálku, že by ho mohl nahradit.

Ptal se, jestli ho jako bratra přijmu a jestli ho přijmu, až přijede na Slovensko, jestli bych pro něj mohla být součástí jeho rodiny, ale v takovém vztahu, že on by byl bratr a já sestra. A takto jsme pokračovali zhruba tři měsíce.

Není to, že by chtěl něco víc. Nešlo o nic jiného. Bylo to o tom, že čím více o sobě budeme vědět, tím silnější to pouto mezi námi bude. Ale stále to bylo v rovině bratr a sestra, nic víc.

O: Takže jestli to chápu správně, váš vztah se tím stával čím dál důvěrnějším a ty jsi byla více a více otevřená v tom, co jsi mu byla ochotna o sobě prozradit?

L: Ano, ale to bylo opravdu, jak z reálného života. On o mně věděl hodně, skutečně věděl některé detaily. Pověděla jsem mu nějaké historky, co se mi staly, třeba na střední škole a byly to věci, které byly i vtipné. Smáli jsme se, prostě zjišťoval, jaký jsem typ člověka.

Dělal si vlastně takový průzkum toho, co mi v životě chybí, jak mě může více připoutat, co mám ráda. A přesně věděl, co mi chybí, a to mi také dával. Čím dál tím víc. Jednoduše zjistil, v jaké situaci se nacházím, co potřebuji, a to mi dával.

Ale nebylo to jen tak, že by mi dal nějaké běžné přátelství nebo chvilkové zážitky. On mi dával mnohem víc. Snažil se vybudovat tak pevné pouto, že z něj už by nešlo jen tak vyskočit. Snažil se vyplnit všechny díry v mém životě, které jsem mu odhalila, že existují.

On totiž přesně ví, po čem jít. Umí dát přesně to, co člověk potřebuje a udělá to tak, že to naplní jeho potřeby. A najednou máš pocit, že máš něco, co jsi nikdy neměl. Takto asi fungují.

O: Rozumím. Zajímalo by mě, když se ještě trochu vrátím k tomu, jak jsi nakousla, že tě kolegové v práci varovali, tak jak se v tobě bila ta důvěra a zároveň ty pochybnosti?

L: Tohle se stalo zhruba ve třetím týdnu, kdy jsem začala víc zjišťovat o amerických vojácích. Tehdy jsem zjistila, že mi neříkal úplně pravdu o své hodnotě, protože ta hodnota, kterou mi řekl, ve skutečnosti vůbec neexistovala. Tak jsem se ho zeptala, aby mi to vysvětlil. Neřekla jsem mu, že jsem to zjišťovala, jen jsem chtěla vědět, co mi na to odpoví. A už jsem si začala vytvářet jakýsi "šuplík", do kterého jsem si ukládala poznatky o tom, že mi nedává správné odpovědi a nechce se o tom dál bavit, protože na to nemá odpověď, kterou bych uznala.

Tím jsem si byla jistá, že něco není v pořádku. Samozřejmě kolegové mi řekli, že existuje způsob, jak tento podvod funguje, že už není ničím výjimečným, když někdo tvrdí,

že je americký voják a že to jsou často podvodníci. Tak jsem se rozhodla kontaktovat svého kamaráda, který pracuje na policii na kriminálce. Řekla jsem mu, co se děje, že si píšu s někým, kdo tvrdí, že je americký voják v Afghánistánu. Můj kamarád, policista, mi okamžitě řekl, že mám přestat s ním psát, ale pokud mi to nevadí, ať si s ním dál píšu, ale ať mu nic neposílám, protože to je podvod. Řekl mi, že to jsou nejspíš podvodníci z Nigérie a že se tímhle způsobem baví. A měl pravdu. "Nic mu neposílej," varoval mě.

Tak jsem si to zapamatovala. O pár dní později jsem mu napsala: "Když jsi tak přesvědčený, že si píšu s podvodníkem, proč mi tedy nedáš nějakého policistu, který to může prozkoumat? Měl by přece být schopný zjistit, kdo je ten člověk, s kým si píšu. Vždyť by ho měli najít přes digitální stopy, ne?" Ale odpověděl mi, že se tím nezabývají. Nikdo nemá čas se tímto zabývat, že to není tak organizované, jak bych si myslela a že to mám prostě nechat být. Doslova mi řekl, že nemá čas na takové věci. Byl to můj kamarád, ale místo pomoci mi řekl, že není možné, aby to někomu přidělil, že na to nemají kapacity.

Tak jsem zjistila, že to musím vyřešit sama. Už jsem ho chtěla odhalit. Chtěla jsem vědět, co za tím je.

Od té chvíle jsem byla na vázkách. Čím dál víc jsem si byla jistá, že mám na druhé straně podvodníka, ale líbil se mi. Měla jsem ho ráda, byla to zábava, bavilo mě si s ním psát. Bylo to pro mě něco nového a nevěděla jsem, jak s tím přestat. Po těch třech týdnech mi poslal zprávu, na základě, které jsem mu řekla: "Víš co, tímhle mi lžeš. Nesnáším podvody a lži, když jsi mi teď takhle zalhal, nevím, jestli s tebou chci dál psát." A on na to odpověděl: "Dobře, tak si přestaneme psát," nebo něco v tom smyslu. A pak byl klid.

Ale přišly Vánoce. A já nevím, co mě k tomu vedlo, ale napsala jsem mu: "Přeji ti příjemné Vánoce, doufám, že jsi v pořádku." A on se po týdnu znovu ozval a začal mi psát. Takhle došlo k prvnímu takovému výpadku komunikace, když jsem ho poprvé obvinila ze lži.

O: Zajímá mě tedy, co tě přimělo k tomu, mu napsat znovu, byl to stesk?

L: Stále jsem nad tím přemýšlela, co za tím vším vlastně je. Co s tím mám dělat? Pokud je to normální člověk, tak to nějak zjistím. A pokud je to podvodník, taky na to přijdu a udělám vše pro to, abych mu v tom zabránila. Chtěla jsem prostě zjistit, co za tím vším skutečně je. A zároveň, i když jsem si byla skoro jistá, že něco není v pořádku, nechtěla jsem o něj přijít jako o člověka, o přítele. Bylo to opravdu zvláštní. Na jednu stranu mě to nelákalo, ale na druhou stranu mi chyběl.

Bylo mi smutno, že už jsem s ním přestala komunikovat. A přitom jsem měla stále v hlavě otázku, kde je pravda a co je vlastně skutečné. Tak jsem se rozhodla, že mu napíšu na Vánoce. Poslala jsem mu takový pozdrav a on se ozval. Jakmile se ozval, zase jsme si začali psát dál.

O: Jasně, rozumím. Zeptám se tedy, jak dlouho to trvalo, než se poprvé odhodlal dotknout otázky financí, tedy, kdy se tě poprvé zeptal, zda mu nějaké peníze nepošleš?

L: Asi po dvou měsících, když jsme obnovili naši konverzaci, jsem už začala pokládat testovací otázky a chtěla jsem odpovědi na některé věci, které jsem si už sama selektovala. Snažila jsem se zjistit, jestli mi říká pravdu, nebo jestli mi lže. Začala jsem si to ověřovat.

V té době, kdy jsem mu napsala, se v Americe prezident Biden rozhodl ukončit misi v Afghánistánu, ačkoliv se měla původně ukončit až o rok později. Bylo to velké oznámení, že se americké vojenské jednotky do září toho roku stáhnou zpět domů. Napsala jsem mu o tom na Velikonoce a on mi odpověděl, že má pro mě skvělou zprávu. Podle něj Biden oznámil, že vojáci budou zpátky doma už v září a že se nemám bát, že se nic nestane, že už jen musím vydržet do září.

Tento vývoj mu ale moc nevyhovoval. Vysvětlil mi, že politici říkají něco jiného, než jaká je skutečnost a že on a ostatní vědí víc než my. Říkal, že situace v Afghánistánu je stále velmi nebezpečná, že talibanci čím dál více útočí a že nějaké výbuchy a smrt vojáků už nejsou ve zprávách, protože jsou to tajné informace. Snažil se u mě vyvolat pocit, že je v ohrožení, že se mu může něco stát a že možná ani do září v zemi nevydrží.

Pak mi řekl, že pokud mi na něm záleží, měla bych něco udělat, abych mu pomohla a aby mohl být dřív doma než v září. Zeptala jsem se ho, co bych mohla pro něj udělat. Vysvětlil mi, že jako rodinný příslušník mohu napsat žádost na nějaký e-mail, aby ho předčasně uvolnili ze služby a pustili ho zpátky domů. Odpověděla jsem, že nikdy nebudu nic psát, jednak to nemám ráda a jednak se vůbec necítím na to, abych psala nějaké americké vojenské instituci, nebo je měla žádat, aby ho poslali domů.

Začal na mě tlačit, že ho nemám ráda, že mu nechci pomoci a že si myslel, že mu budu chtít pomoci, že naše přátelství je silné. Postupně začal používat jemný nátlak a pokoušel se mě vydírat tím, že se ptal, jestli se o něj vůbec nebojím. Co když do září nezvládne vydržet a něco se stane? Co když tam zahyne, a já ho tam nechám?

Řekla jsem mu, že vojáci to mají těžké, ale musí vydržet. Že nepláčou a že na to byli trénováni. Ale on stále tlačil na moje city, že doufal, že ho mám ráda, že mi na něm záleží, a že bych mu měla pomoci.

Pak přišel s návrhem, že mi ten e-mail napíše on. Pošle mi ho a já ho jen pošlu na jinou e-mailovou adresu, kde se postará o to, aby ho uvolnili nebo poslali na dovolenou. Tím by vyřešil vše za mě, protože já prý neovládám jazyk a nevím, komu píšu.

Věděla jsem už tehdy, že se jedná o podvod, protože jsem si na internetu nastudovala, jak takový podvod obvykle funguje. Bylo to typické pro americký vojenský podvod. Zjišťovala jsem, že po žádosti, kterou bych mu poslala, bych obdržela odpověď, že ho prostě nepošlou domů, pokud nezaplatím nějaké poplatky za administrativu a náhradu za dobu, kterou by měl strávit doma.

A tak jsem testovala, co se stane, jestli mi opravdu přijde odpověď, jakou jsem si přečetla na internetu a jestli je to celé opravdu podvod. Každý krok, který jsem udělala, jsem testovala podle toho, co jsem si nastudovala a všechno sedělo.

Nakonec mi přišla odpověď, měla jsem pravdu. Poplatky byly stanovené a já měla zaplatit, pokud jsem chtěla, aby ho pustili domů. Každá zpráva jen potvrdila, že na druhé straně je podvodník. A přesto jsem pokračovala. Byla jsem zvědavá, co se stane dál.

O: Ale v tom momentě jsi ještě žádné peníze neposílala, že?

L: Ne. Ten e-mail jsem poslala na tu organizaci asi po dvou měsících, kdy už jsem souhlasila, že ho pošlu. Do té doby po mě nechtěl žádné peníze a ještě, než jsem ten e-mail odeslala, jsem mu řekla, že pokud mi přijde odpověď, že mám zaplatit nějaké poplatky, tak tím pádem končíme. Nebudu s ním dál komunikovat. On mě ale přesvědčoval, že mi taková odpověď nepřijde, že buď ho uvolní do důchodu, nebo ho pošlou na dovolenou. Já jsem měla napsat e-mail tak, že ho potřebuji v mé zemi z rodinných důvodů, dědictvého řízení nebo něco podobného. Tímto způsobem jsem se ho snažila dostat zpátky domů na několik dní, jako kdyby šlo o volno pro vojenské účely.

Souhlasila jsem tedy a on mi poslal e-mail, který měl být v té struktuře, jak jsem ho měla poslat dál. Já jsem si ten e-mail přeložila a upravila. Napsala jsem, že jsem sestřenicí toho vojáka a že kvůli rodinným záležitostem potřebujeme, aby se zúčastnil nějaké rodinné záležitosti na Slovensku, protože je potřeba vyřešit nějaké dědictví. Takto jsem to napsala a e-mail poslala.

Po nějaké době mi přišla odpověď z organizace, která mi napsala, že pokud chci mít svého manžela doma, musím zaplatit tolik a tolik. V tu chvíli jsem se už začala smát, protože to, co jsem dostala, bylo přesně to, co jsem si přečetla ve všech těch člancích a zprávách, které jsem studovala. On ani nebyl schopný si přeložit ten upravený e-mail, který jsem mu poslala. Odpověděl mi naprosto mimo, úplně neadekvátně, jako kdyby vůbec nečetl, co jsem napsala.

Bylo mi jasné, že mluvím s podvodníkem, a to nejen na té straně, která mi poslala odpověď, ale i na té, která mi e-mail napsala. Byli to zjevní podvodníci, a navíc i velmi nešikovní. Ani si nedali tu námahu přeložit to, co jsem napsala. Tak jsem byla ještě víc přesvědčená, že na druhé straně jsou jen podvodníci. Už mě to ani neštvalo, spíš jsem to brala jako další důkaz, že jde o podvod. Byla to jako další "žhavá jehla" do mého přesvědčení, že jsem je dostala.

Pokračovala jsem v tom tak, že jsem napsala: "Tak, jestli tohle je v pořádku, tak pojďme hrát tuto hru." Vzala jsem to jako výzvu a řekla si, že uvidím, co se bude dít dál. A on mi na to odpověděl: "Pojď." V té chvíli už jsem si byla jistá, že mají nalinkované určité scénáře, kterých se vždy drží. Kdykoliv někdo vybočí, snaží se ho zpátky dostat na tu původní cestu, protože jakékoliv vybočení je pro ně nepřijatelné.

Navíc mě to bavilo, já jsem se normálně bavila, víš? Ale chtěla jsem ho dostat, tam už jen o to ho dostat.

O: Mohla bys, prosím, uvést kolikrát se tě pokusil požádat o peníze, než jsi to udělala doopravdy?

L: Několikrát. Potom se scénáře začaly měnit. Nejprve mi řekli, že mám zaplatit 4800 €, aby ho pustili na rodinnou záležitost, tedy na dovolenou. To jsem odmítla, řekla jsem, že nic nezaplatím, protože tolik peněz nemám. A chtěla jsem vědět, kde přišel na tuto sumu.

On tomu nerozuměl, takže jsem se ho zeptala, kdo mě nacenil na tuto částku. Pokud jsem se správně dočetla ve všech těch zprávách o podvodech, tak částky byly nižší, třeba 2000 nebo 2300 €, ale proč mi přišla částka 4800 €? Kdo to takto nacenil?

On zase začal tvrdit, že nerozumí a pokračoval po svém. Řekla jsem si: "Dobře, pojďme si hrát, pokračujme dál." Celou dobu jsem byla odhodlaná přijít na to o čem jde a zjistit, kdo je na druhé straně. Tak jsem se začala obracet na naše banky, prosila jsem je, aby mi pomohly, abych zjistila, odkud ty e-maily přicházejí. Chtěla jsem zjistit, z jaké země jsou. V podstatě

mi nikdo nechtěl pomoci, každý mi řekl, že mám zkusit hledat na internetu, kde najdu video návody.

V těch návodech se psalo, jak poslat e-mail tak, že po jeho otevření o tom dostanu okamžitě oznámení a také informace o tom, z jaké země přišel. Každý mi dával jen návody, ale nikdo mi skutečně nepomohl. Sama jsem to nedokázala udělat, nebyla jsem tak zručná. A když jsem si prohlížela videa, jak to udělat, jak vytvořit e-mail, aby ho otevřel a já dostala informaci o jeho poloze, už jsem začala narážet na problém, protože všechna videa byla v angličtině a já už v dalších krocích ztrácela kontrolu. Nedokázala jsem to vytvořit. Rozhodla jsem se tedy, že si někoho najdu, kdo mi s tím pomůže. Na chvíli jsem to odložila a nechtěla se tím dál zabývat. Chtěla jsem se soustředit na to, abych ho neodřízla, aby mi nevypadl z linky a já ho mohla dál udržet v kontaktu.

Od té doby jsem s ním mluvila čím dál víc. Začal se mi dostávat pod kůži.

O: Kdy nastal ten zlom a ty peníze jsi mu skutečně zaslala?

L: Takže poté, co jsem odmítla zaplatit těch 4800 €, přišel s novou taktikou. Řekl mi, že se mi asi dva dny neozve, protože byl vyslán na speciální misi s důležitým posláním. Pokud by se mi do dvou dnů neozval, znamenalo by to, že je mrtvý.

Začala jsem pomalu chápat, o co tu jde. A skutečně – celé dva dny se neozval. Přesně po dvou dnech a hodině se najednou znovu ozval. Řekl mi, že se z mise vrátil, byl postřelen, ale úkol splnili na výbornou. Dokonce dostali odměnu od afghánské vlády za záchranu několika členů vládní rodiny před Talibanem. Tvrdil, že za to dostal 3 miliony dolarů v kufříku, ale že je potřebuje dostat do bezpečí, protože jinak by mu je někdo ukradl nebo by prostě zmizely.

Pokračoval ve své hře a oznámil mi, že mi pošle balík s penězi. Snažila jsem se ho od toho odradit – říkala jsem mu, že žádný balík nechci, že u sebe jeho peníze mít nebudu a nemůžu je ani chránit, protože jde o obrovskou sumu. Bránila jsem se a snažila se ho přesvědčit, aby se o nic takového nepokoušel. On ale dál používal různé manipulační taktiky a snažil se mě přesvědčit, že to prostě musí poslat.

V tu chvíli už jsem věděla, že jde o podvod. Přečetla jsem si o něm a bylo mi jasné, že balík bude údajně zadržen celní správou a po mně budou chtít poplatky. Řekla jsem mu, že mu nedám žádné osobní údaje ani adresu, dokud nesplní jeden test. Chtěla jsem si ověřit, jestli se opravdu nachází na místě, na kterém tvrdí, že je. Požádala jsem ho, aby mi dokázal,

že se v jeho blízkosti vyskytuje Slovák, konkrétně někdo z oblasti Košic nebo Prešova. Řekla jsem mu, že pokud správně odpoví na mou otázku, uvěřím mu.

Mezitím jsem si nachystala malý test. Vzala jsem několik šarišských slov a zjistila, že automatické překladače je neumí správně přeložit. Vybrala jsem taková slova, která překladače buď zařazovaly mezi úplně jiné jazyky, nebo je vůbec nedokázaly zpracovat. Pak jsem mu poslala 15 takových výrazů.

O hodinu později mi poslal odpověď – a zvládl to! Z těch 15 slov určil asi 13 správně. V tu chvíli jsem začala o všem pochybovat, zda ho neprávem nepodezřívám.

Nakonec jsem mu tedy dala svou e-mailovou adresu i korespondenční adresu, aby mi mohl poslat balík přes nějakou speciální kurýrní službu. Už jsem se tomu sama smála – představovala jsem si, jak jdu s kufrem plným peněz do banky a pokládám tam tři miliony dolarů. Jak by na to asi moje banka reagovala? V tu chvíli mi to celé připadalo naprosto absurdní.

Samozřejmě, vše dopadlo tak, jak jsem předpokládala. Balík byl „zadržen“ na celnici a po mně chtěli zaplatit clo. Řekla jsem mu, že žádné clo platit nebudu. Pokud věděl, že se platí, měl si peníze nechat a zaplatit to předem sám. Já to za něj dělat nebudu, protože jednak nemám tolik peněz, a hlavně to ani nechci.

Začal mě citově vydírat a tvrdil, že pokud nezaplatím, peníze na celnici zmizí. Odpověděla jsem mu, že se nemusí bát – na celnici se nic neztratí, tam jsou jeho peníze v nejlepší možné úschově. Až opustí armádu, může si je tam vyzvednout. Turecká celnice mu je zatím pohlídá úplně zdarma.

Na chvíli to vzdal, ale pak přišel s další taktikou. Začal mi vyprávět o svém synovi, který je v Americe úplně sám a trápí se. Mají jen jeden den v týdnu, kdy si spolu mohou volat a kvůli časovému posunu je to pro ně oba složité. Prosil mě, jestli bych mu nepomohla, aby měl vlastní počítač, aby s ním mohl komunikovat kdykoli.

Opět šlo o test mé ochoty – tentokrát bylo potřeba poslat 1000,- € učiteli jeho syna na nový počítač. Řekla jsem mu, že ho klidně koupím sama a pošlu přímo na adresu školy. To ale nechtěl.

Začínala jsem být ve zvláštním stavu – chvíli jsem byla stoprocentně přesvědčená, že je podvodník, ale pak jsem zase pochybovala, jestli nejsem paranoidní a neodmítám pomoc někomu, kdo ji skutečně potřebuje. Uvnitř mě se odehrával neustálý boj. Už jsem si začínala

uvědomovat, jak silně mě zmanipuloval a kolik času jsem mu věnovala. Vzniklo mezi námi něco jako podivné pouto, kvůli kterému jsem nebyla schopná ho jen tak odstříhnout.

O: Takže říkáš, že jsi mu ty peníze vlastně poslala proto, že jsi o něj nechtěla přijít, je to tak?

L: Ano, ale také jsem si stanovila určité podmínky. Trvalo přibližně dva týdny, než jsme je vyřešili, ale na žádnou z mých podmínek nakonec nepřistoupil. Nakonec poslední verze dohody byla taková, že bylo potřeba poslat peníze jeho synovi někam do Ameriky na účet nějakého učitele. Ten učitel by za ně koupil počítač, a poté by mi jeho syn poslal fotku s tímto počítačem.

Fotky jeho syna jsem už předtím viděla, protože jsme si během té doby vyměnili několik snímků – jak vypadá jeho rodina, on se synem i samotný syn. On mi také poslal velké množství fotek a stejně tak jsem mu poslala i já své skutečné fotky. Měl dokonce i fotografie mých dětí.

Téměř každý druhý den chtěl vidět, jak vypadám ten den – jak jsem oblečená do práce, jestli tak mohu jít ven, nebo jestli by to mohlo někoho provokovat. Chtěl mít kontrolu nad tím, co si oblékám, a rozhodoval, zda je to „v pořádku“. Neustále chtěl vidět nové fotky, zatímco jeho vlastní zásoba byla omezená – ukradených fotek má jen určitý počet, a tak mi nakonec posílal stále ty samé dokola.

Je pravda, že jsem mu nikdy neposlala žádnou intimní nebo kompromitující fotografii. Byly to vždy jen běžné snímky – například moje tvář, starší fotky z minulosti, třeba z maturity, nebo z různých slavností a karnevalů. Byly to vždy slušné a neškodné fotky.

Chtěl na fotkách vidět, zda jsem smutná, jestli se směji, jestli náhodou nemám opar nebo nejsem nemocná. Snažil se působit dojmem, že mu záleží na mých pocitech – zda jsem šťastná, zda pláču, jestli mě něco bolí a jestli nepotřebuji pomoc.

Neměla jsem problém mu poslat obyčejné fotky, třeba v černém nebo bílém tričku, protože jsem si myslela, že se tím nedá nijak ublížit, ani kdyby to byl podvodník. V té době jsem ještě nevěděla tolik věcí, takže jsem si byla jistá, že takové snímky nelze nijak zneužít a že mi nemohou uškodit. Tehdy mě ani nenapadlo, že by mě s nimi mohl někdo vydírat, protože na nich nebylo nic kompromitujícího.

Celou tu dobu jsem neposlala žádný jiný druh fotografie.

O: Dobře a co se tedy změnilo, že jsi mu potom ty peníze zaslala?

L: Těsně předtím, než jsem se skutečně rozhodla ty peníze poslat, jsme se velmi pohádali. Dohnal mě do stavu zoufalství a vzteku – vyhrožoval mi, že si něco udělá, křičel na mě, že ho nemám ráda, že si na jeho přítelkyni jen hraju, ale ve skutečnosti jí nejsem a že ho vůbec nelituji. Používal různé emocionální manipulace a nátlak, až mě nakonec tak naštvál, že jsem řekla: „Dobře, peníze pošlu. Ale pokud mi nepošleš zpátky fotku svého syna s tím počítačem, tak je to jasný důkaz, že lžeš, a tím naše konverzace končí.“ Byla to pro mě zkouška důvěry.

Nakonec první platba odešla do Ameriky – tisíc eur na účet nějakého muže, který se vydával za učitele. Hned poté začal tlačit, abych mu poslala potvrzení o platbě. Chtěl důkaz, že peníze skutečně odešly z mého účtu. Jenže ty peníze nikam nedorazily, takže jsme je zhruba týden „hledali“. Já jsem mu byla schopná vytisknout i výpis z účtu, aby viděl, že platba proběhla a nebyla vrácena. Jenže on samozřejmě tvrdil, že neumí číst moje bankovní dokumenty, ledaže by si uměl z obrázku zkopírovat text a přeložit ho. Nicméně z výpisu jasně viděl, že tisíc eur skutečně odešlo na daný účet a že transakce byla zaúčtována.

Ty peníze se mi nakonec vrátily zhruba po deseti dnech, protože mezitím došlo k uzavření účtu příjemce. Ukázalo se, že to byl jen nějaký „bílý kůň“. Platba se mi sice vrátila, ale snižená o padesát eur kvůli poplatkům bank. Tak jsem mu oznámila, že peníze se mi vrátily a že už je nikam nepošlu. Jenže on znovu začal naléhat – jeho syn prý pláče, protože počítač chtěl a už se na něj těšil. A jestli mám srdce nechat jeho syna trpět. Začal se mnou manipulovat tím, že pokud odmítnu, jsem hrozný člověk.

Nakonec jsem tedy souhlasila, že peníze pošlu znovu. Jenže tentokrát mi poslal jiné číslo účtu – tentokrát s africkým jménem. Odmítla jsem. Poté mi dal španělský účet – i ten jsem odmítla s tím, že přece americký učitel nemůže mít účet ve Španělsku. Nakonec mi poslal účet, který jsem akceptovala, když mi vysvětlil, že patří nějaké vzdálené příbuzné jiné učitelky, která měla předat peníze dál. Tisíc eur jsem tedy nakonec poslala znovu – a tentokrát dorazily. Potvrdil mi, že peníze přišly a že teď už si jde s učitelem koupit počítač.

Asi po třech až čtyřech dnech mi poslal fotku – chlapce v internátní místnosti, jak drží notebook v ruce a jako by mi mával. Zeptala jsem se ho, kdo tu fotku pořídil, protože podle jeho slov tam děti nemají přístup k mobilním telefonům. Bylo ale zřejmé, že fotka byla pořízena telefonem a odeslána přes WhatsApp. Viděla jsem na ní určité detaily, které mě přesvědčily, že nebyla pořízena tak, jak tvrdil.

Navíc ten chlapec se sice trochu podobal jeho synovi, ale nebyl to on. Dokázala jsem to poznat – nebyla to stejná osoba. Když jsem ho s tím konfrontovala, rozčílil se a tvrdil, že

on přece nejlépe ví, jak vypadá jeho vlastní syn. Začal mě obviňovat, že ho falešně osočuji, protože na fotkách, které mi posílal dříve, bylo dítě sedmileté, zatímco nyní je tomu chlapci čtrnáct. Snažil se mi vnutit pocit viny, že já jsem ta špatná, která mu křivdí.

A tak odešlo prvních tisíc eur a začal kolotoč žádostí o další a další peníze. Snažil se mě přesvědčit, že ho musím „vykoupit“ do důchodu. Já se tomu vyhýbala, odkládala to, ale zároveň jsem byla vnitřně rozpolcená – na jednu stranu jsem si už byla téměř jistá, že je to podvod, ale stále jsem měla pochybnosti. Nechtěla jsem mu ublížit, ale zároveň jsem se nechtěla vzdát toho, co jsme si mezi sebou vybudovali.

Celou dobu jsem jen čekala, až najdu někoho, kdo mi dokáže potvrdit, že je to skutečně podvod. Potřebovala jsem tu jistotu, ale nikdo mi ji neuměl dát. Tak jsem se v tom plácala sama.

O: A ty jsi vlastně svolila ještě jednou k tomu, mu ty peníze poslat, že?

L: Poté trval na tom, že je nutné poslat peníze na jeho důchod. V té době jsem už ale věděla, že o ty peníze s největší pravděpodobností přijdu. Přesto jsem mu nedokázala říct, že je nepošlu a že mu nevěřím. Nedokázala jsem mu vpálit do tváře, že je podvodník a že jsem si tím jistá. Nešlo mi to. Možná kvůli slušnému vychování, možná proto, že se mi přičilo někoho takto obvinít, pokud jsem neměla stoprocentní jistotu.

Snažila jsem se to odkládat a znovu jsem se obrátila na svého známého policistu s otázkou, zda by šlo zjistit, kam ty peníze putují, nebo je zachytit dřív, než dorazí na účet příjemce. Řekl mi, že teoreticky by to mohlo být možné, pokud jsem ochotná to risknout.

Nakonec se ale nestalo nic – nikdo pohyb těch peněz nesledoval a už se mi nikdy nevrátili. V tu chvíli mi bylo jasné, že je konec.

Ty peníze jsem poslala někdy v červenci, tedy přibližně pět měsíců poté, co jsem ho poznala. Celou tu dobu jsem byla v neustálém vnitřním rozporu – chvílemi jsem měla jasno, že je to podvodník a že to musím ukončit, ale vzápětí mě přemohl strach, jaké to bude bez něj.

Asi právě to mělo největší vliv – strašně moc jsem si chtěla namluvit, že to podvod není. Že je skutečný, že ho jen zbytečně podezřívám a že ve skutečnosti jde o zoufalého člověka, který opravdu potřebuje pomoc. Už jsem přestávala rozlišovat, co je pravda a co ne.

O: Cítila si, že jsi na něm tak závislá, že již není cesty zpět, že?

L: Ano. Ty peníze nijak nezasáhly do rodinného rozpočtu, protože jsem je tehdy vybrala ze svého důchodového spoření. Řekla jsem si, že obětuji své úspory, jen abych zjistila pravdu – jestli jsem opravdu tak naivní a naletěla podvodu, nebo zda na druhé straně skutečně stojí člověk, který mě potřeboval a kterého jsem jen neprávem podezřívala.

Potřebovala jsem se sama přesvědčit, jak se situace vyvine a jestli se to časem vyřeší. Ale zároveň jsem věděla, že pokud mu ty peníze nepošlu, tak se mnou už dlouho nezůstane. To bylo víc než jisté.

Celé to směřovalo k tomu, že pokud to neudělám včas, jeho důvěra ve mě skončí a já o něj přijdu. Tehdy mi došlo, že jsem na něm závislá.

O: A to byla vlastně také tvá poslední platba pro něj, že?

L: Ano. Celé to skončilo tak, že tato částka měla být jakési „výkupné“ za jeho návrat domů. Platba odešla, ale pak mi přišel e-mail, ve kterém stálo, že armáda přehodnotila své možnosti a nemůže ho poslat do důchodu. Údajně měl být brzy odvolán do Sýrie, protože byl nepostradatelný, a než se jim podaří najít za něj náhradu, stanovili jeho „hodnotu“ na 50 000 eur.

Aby ho tedy nemuseli poslat do Sýrie a mohli ho ze služby vůbec stáhnout, požadovali dalších 50 000 eur. Jakmile jsem jim poslala 4 800 eur, okamžitě zvýšili částku a chtěli víc. To byl pro mě definitivní konec. Od té chvíle jsem ho už jen záměrně zdržovala. Stalo se to někdy v létě, pravděpodobně v červenci.

Řekla jsem, že tohle je hranice. Nemám už žádné další peníze, nebudu je shánět a ani je neposílám. Ať se děje, co se děje. Byly to poslední peníze, které jsem za něj dala. Pokud ho tedy nepošlou domů, ať mi vrátí zpět to, co jsem zaplatila, a celou žádost ruším. Když se nic z toho, co slíbili, nestalo, ať mi jednoduše vrátí peníze.

Chvíli jsem se snažila vyjednávat, chtěla jsem vidět, jestli je to celé pravda a zda je vůbec skutečný. Pokud by mi peníze vrátili, mohl by to být důkaz důvěry. Ale on mi začal vysvětlovat, že nemá žádnou moc přimět „centrálu“, aby mi peníze poslala zpět. Tvrdil, že oni ho už teď vnímají jako někoho, kdo je v „poloviční výpovědní lhůtě“, že už tam v podstatě končí. Stačí jen doplatit zbývající částku a mohl by odejít do důchodu.

Pořád mě jen manipuloval, měnil podmínky a taktizoval, jak ze mě dostat další peníze. Ale tehdy jsem řekla stop. Moji hranici už překročil. Už nedostane ani korunu.

A od té chvíle mi šlo jen o to, jak ho co nejdéle udržet „na lince“, aby ho někdo mohl vystopovat.

O: Ty ses tedy snažila ho nějak vystopovat, jenže to se nepovedlo, že?

L: Zjistila jsem, že mé vlastní schopnosti na to nestačí, a začala jsem všude možné dohledávat informace o tomto typu podvodu. Hledala jsem na Facebooku, na různých internetových fórech, zkoušela jsem reverzní vyhledávání fotografií, snažila se zjistit, kdo za tím vším stojí. Prostě jsem se pustila do vlastního pátrání.

Takto jsem se dostala do různých skupin, které se specializují na podvody, zejména na ty romantické. Chtěla jsem zjistit, zda někdo nepozná jeho fotografii, kdo by mohl být skutečná osoba za tou tváří. Zajímalo mě i to, jestli on sám ví, že podvodníci zneužívají jeho fotky.

V té době jsem už byla přesvědčená, že na druhé straně je podvodník. Ale přesto jsem ho měla ráda. Postupně se náš vztah změnil – z přátelství, které působilo spíš jako mezi bratrem a sestrou, se to vyvinulo dál. Měl mě rád on, měla jsem ráda já jeho, byli jsme si blízcí.

A pak jsem se začala ptát sama sebe: Koho vlastně mám ráda? Tvář, za kterou se skrýval? Příběh, který mi vyprávěl? Nebo skutečnou osobu, která si se mnou psala a trávila se mnou čas? Bylo evidentní, že mě dokonale poznal – věděl o mně všechno, co jsem mu řekla. Já jsem o něm nevěděla nic, protože hrál svou roli, ale přesto se o mě zajímal. A já si v jednu chvíli myslela, že i on mě má rád, jen mi to nemůže říct, protože by vybočil z té hry, kterou musel hrát.

Na pozadí, ale pořád byla realita – někde tam seděl člověk, který mě musel zmanipulovat, aby ze mě dostal peníze. Ale zároveň bylo znát, že mu na mně záleží. Myslela jsem si, že ten „podvodník“ je možná jen oběť – že ho někdo nutí k tomu, aby vylákal peníze, že má své vlastní problémy a trápení, že je možná i sám v nějaké pasti.

Nešlo jen o soucit, ale i o to, že jsem si říkala, že když už jsem mu poslala poslední peníze, tak tím možná někomu pomohu. A tak jsem si sama pro sebe řekla: „Tohle je poslední charita, kterou v životě udělám.“

Chtěla jsem pochopit, kdo to je. Proč to dělá. A zda by se to dalo nějak zvrátit. Neměla jsem touhu ho zlomit, ale spíš ho pochopit. Přemýšlela jsem, jestli ho nelze nějak „napravit“, ukázat mu, že to, co dělá, je špatné.

Byly to iluze, ideály, nesmysly. Ale já tomu tehdy věřila. A stalo se z toho něco jako závislost.

Hledala jsem každou jeho zprávu. Budila jsem se ráno sama od sebe, přestože normálně dlouho spím, protože jsem věděla, že mi brzy napíše. Celý můj denní rytmus se změnil. Byla jsem schopná nespát, dlouho si psát, trápit se myšlenkami, kdo ten člověk vlastně je a proč to dělá.

A přestože jsem už věděla, že je to celé podvod, nedokázala jsem s tím přestat.

O: Rád bych teď malinko odbočil, zajímá mě, jestli někdo z tvé rodiny něco tušil, neboť ty vlastně popisuješ, že to byl pro tebe i tvůj režim obrovský zásah, tak mě zajímá, zda někdo něco tušil, nebo alespoň viděl, že se něco děje.

L: Můj mladší syn to viděl, protože v té době byl se mnou v pokoji. Byl na mně velmi závislý, spal se mnou v posteli jako dítě, protože byl často nemocný. V noci jsem ho pravidelně kontrolovala, protože trpěl zvláštní chorobou. Manžel se mnou v té době nespál, syn ho v podstatě nahradil a trávil se mnou hodně času.

Viděl, že si s někým píšu, a ptal se, s kým komunikuji. Odpověděla jsem mu jen obecnou informací, že jde o člověka, který potřebuje moji pomoc. Sem tam jsem mu něco drobného řekla, ale v podstatě netušil, o co jde. V té době mu bylo 9 nebo 10 let.

Syn se mnou sdílel moje emoční rozpoložení. Když na mě dolehla únava, smutek nebo frustrace, věděl to. Viděl, že jsem si s někým psala a chápal, že je to pro mě důležité. Starší syn to pravděpodobně také vnímal, ale protože je spíše tichý, neptal se. Občas jsem ho požádala o technickou pomoc, protože hned na začátku se podvodník snažil přesměrovat komunikaci z Facebook Messengeru na jinou platformu, kde by nehrozilo zablokování jeho profilu. Přesměroval mě na Hangouts asi po třech čtyřech dnech. Technicky jsem si s tím nevěděla rady, a tak mě navigoval on.

Když jsem později začala dělat vlastní pátrání a hledala různé způsoby, jak zjistit, odkud mi píše, nebo jak dohledat další osoby zapojené do podvodu, starší syn mi občas pomohl. Měl technické znalosti a chápal, že to nedělám jen tak z rozmaru. Nevypτάval se na důvody, ale pomohl mi. Manžel si pravděpodobně ničeho nevšiml. Ostatní členové rodiny, včetně mých sester, o tom vůbec nevěděli a dodnes to nevědí.

Postupem času jsem začala chápat, jak tento typ podvodu funguje. Pochopila jsem, jak podvodníci navazují kontakty s lidmi, jak je manipulují a jak vylákávají peníze. Nakonec jsem začala pomáhat i jiným.

Nejdříve jsem varovala svou matku. Ukázala mi svůj telefon, vymazala jsem podezřelé zprávy a upozornila ji, aby na ně nikdy neodpovídala. Pak jsem se zapojila do mezinárodní komunity, která se snaží bojovat proti těmto podvodníkům. Pomáháme identifikovat falešné profily, blokovat je a varovat ostatní.

Dlouho jsem se za tuto zkušenost styděla a měla jsem pocit selhání. Teprve postupem času jsem pochopila, že nejsem sama. Když jsem se začala o tuto problematiku zajímat hlouběji, zjistila jsem, že legislativa v různých zemích se velmi liší a že boj proti podvodníkům je složitý. Například v Nigérii a Ghaně existují celé organizované skupiny, které se těmto podvodům věnují jako životnímu stylu. Policie v našich zemích nemá pravomoci zasahovat v zahraničí a mezinárodní spolupráce v těchto případech nefunguje dostatečně efektivně.

Proto je tak důležité, aby se lidé spojili a vzájemně si pomáhali. Sdílení informací je klíčem k tomu, aby se podvody odhalovaly a aby si lidé dokázali ověřit, zda komunikují se skutečnou osobou nebo s podvodníkem.

Můj způsob, jak se s touto zkušeností vyrovnat, je aktivně bojovat proti těmto podvodům a pomáhat ostatním, kteří by se mohli stát oběťmi. A teď si vlastně říkám, že jsem možná zhltnula 5-6 tvých dotazů najednou.

O: Ano, někdy se ti povedlo zhltnout i víc než 6 (smích). Ale to vůbec ničemu nevadí.

L: Dobře, no, takže moje rodina o tom nevěděla.

O: Jak tedy došlo potom k tomu, že si se rozhodla s ním tu interakci ukončit?

L: Ano, ono to vlastně mělo takový vývoj samo o sobě. Už někdy v červenci jsem si řekla, že mu nepošlu ani korunu, protože už bylo víceméně jasné, že je to podvodník. Šlo jen o to ho odhalit nebo nějakým způsobem dostat.

Pak nastal zlom – v Afghánistánu v srpnu došlo k tomu, že se všechny americké vojenské jednotky musely stáhnout, protože Tálibán ovládl zemi. V posledních dvou srpnových týdnech probíhala masová evakuace všech ohrožených osob – informátorů, překladatelů i samotných Afghánců. Celá americká posádka musela odejít. V tu dobu jsem to velmi intenzivně sledovala – každou minutu přicházely zprávy o tom, kdo právě odchází,

kolik letadel odváží lidi pryč, kolik vojáků zůstává, kolik jich bylo nově nasazeno na obranu letiště. Byla to obrovská celosvětová událost.

Můj podvodník se mě, ale snažil přesvědčit, že ho tam zapomněli. Tvrdil, že protože jsem už mezitím zahájila proces jeho odchodu do důchodu, nebyl už oficiálně vojákem, a tak ho tam nechali. To už byl naprostý nesmysl. Bylo vidět, že je v koncích a už neví, jak dál hrát svou hru. Musel improvizovat a od té chvíle to začalo být čím dál trapnější. Já už v tu dobu neměla zájem s ním dál komunikovat – bylo naprosto jasné, že je to celé špatně.

Řekla jsem si ale, že když už jsem to dotáhla až sem, tak ho nenechám jen tak zmizet. Chtěla jsem zjistit jeho pravou identitu a mít nějaké zadostiučinění. Jenže to se nepovedlo, i když jsem ho držela na lince až do února – tedy dalšího půl roku.

Celé to se mnou bylo už jen o tom, že jsem musela ustát tlak a neustále odolávat jeho manipulacím, proč mu nemohu poslat další peníze. Nakonec jsem si vymyslela, že jsem těžce nemocná a hospitalizovaná. Abych si mohla odpočinout a nemusela s ním trávit tolik času, předstírala jsem, že jsem v kómatu. Založila jsem si falešný účet pod jménem svého syna, protože věděl, jak se jmenuje. Jako „můj syn“ jsem mu oznámila, že jsem v nemocnici a že jsem upadla do kómatu. Když jsem se „probrala“, komunikoval dál se mnou i s mým „synem“, což jsem ale byla stále já.

Situace už se pro mě stala neúnosnou. Bylo to psychicky vyčerpávající. Začalo se to podepisovat na mém zdraví – byla jsem neustále unavená, nesoustředěná a nebyla schopná normálně fungovat. Zjistila jsem si mezitím, že podvodníci jako on mají seznamy svých obětí a často je nenechají být ani po odhalení. Neustále je kontaktují, vyhrožují jim, vydírají je nebo se je snaží zmanipulovat k dalším platbám.

Věděla jsem, že se ho nikdy nezbavím, pokud to neukončím radikálně. A tak jsem zinscenovala svou vlastní smrt.

Můj „syn“ mu oznámil, že jsem nemoci podlehla. Podvodník se ještě pokusil získat důkaz – chtěl vidět úmrtní list, fotku hrobu nebo pohřbu. Ale nic nedostal. Můj „syn“ byl nekompromisní, ukončil s ním veškerou komunikaci a odmítl mu poslat cokoli dalšího.

Podvodník se ještě nějaký čas ozýval, snažil se z „mého syna“ dostat peníze alespoň na léky, tvrdil, že je zraněný. Ale neuspěl. Po nějaké době komunikace ustala.

Občas mi ještě přijde nějaká podvodná žádost, ale už jsem se z toho seznamu obětí víceméně vytratila. Přestali mě kontaktovat, protože pro ně už „neexistuji“. Díky tomu mám konečně klid a můžu se soustředit na to, abych pomáhala odhalovat další podobné podvody.

O: Super, ještě bych se tě rád zeptal na to, ty už jsi to vlastně nakousla, jak probíhá nyní ten tvůj boj proti podvodníkům?

L: Moje aktivita začala někdy koncem tohoto léta, když jsem definitivně zjistila, že on je podvodník a že ho potřebuji dostat. Snažila jsem se spojit s různými lidmi a komunitami, které bojují proti tomuto podvodu a mají dostatek informací.

Začala jsem spolupracovat s lidmi, kteří se zaměřovali na nahlašování profilů na Facebooku, dokud je Facebook neodstraní. Tento proces je velmi pracný, protože je nutné opakovaně reportovat jeden profil s informacemi o tom, jak porušuje zásady a proč by měl být z Facebooku odstraněn. Existuje mnoho skupin, které se touto činností zabývají, a oni je reportují, dokud profil nezmizí. Tato aktivita mi však začala zabírat příliš mnoho času, který už jsem i tak neměla, takže jsem se od těchto skupin odklonila a připojila se k mezinárodní komunitě s názvem "Scammhaters United".

Tato komunita vznikla, když jedna žena, která prošla podobným podvodem, začala shromažďovat lidi s podobnými zkušenostmi. Tento podvod ji zasáhl tak silně, že až na letišti, když čekala na svého "miláčka", zjistila, že nikdo nepřijde. Po této zkušenosti začala pátrat, co se stalo. Byla podvedena bez jakýchkoli pochybností o tom, že mluvila s podvodníkem. Tato žena, využívající své zbylé síly, začala spojovat lidi, kteří prošli stejnou zkušeností a shromažďovat informace o tom, jak podvod funguje, kde začíná, kdo ho provádí a jak vypadá reálná tvář podvodníků, kteří se často nacházejí ve velkých skupinách, pracujících v chudých podmínkách. Komunita se snaží zviditelnit podvodníky, aby ostatní lidé, kteří se dostanou do kontaktu s nimi, pochopili, co se děje a odhalili pravdu.

Romantické podvody patří k těm nejkrutějším, protože oběť – ať už žena, muž, nebo dokonce dítě – je celou dobu přesvědčena, že zažívá skutečnou lásku. Až když je podvedena, zjistí, že byla manipulována, což může mít devastující následky. Někteří lidé se z tohoto podvodu nikdy nevzpamatují, ztrácejí nejen peníze, ale i rodinu a někdy i životní smysl. Tyto podvody mění životy a lidé, kteří jsou do nich zapleteni, se stávají troskami, které není snadné opravit.

Když jsem viděla svou vlastní proměnu, uvědomila jsem si, jak těžké to musí být pro lidi, kteří nemají žádné pochybnosti o svých pocitech a věří těmto podvodníkům. Dává mi smysl, že dělám něco, abych těmto podvodníkům zabránila v jejich činnosti.

Naší aktivitou je shromažďování informací a pomoc obětem. Spojujeme se, abychom se pokusili podvody zastavit, zpomalit nebo alespoň informovat lidi, kteří se stali oběťmi. Cílem je pomoci jim uvědomit si, že jsou podvedeni, a pomoci jim opět najít důvěru v sebe a ve svět kolem nich.

Mým úkolem je vyhledávat falešné profily na Facebooku a hlásit je. Spolupracuji s několika lidmi, kteří mají přístup k nástrojům, které Facebook dříve poskytl komunitám, které bojují proti těmto podvodníkům. Tento nástroj umožňuje automatizovaně odstraňovat falešné profily. Ačkoli Facebook v minulosti ukončil přímou spolupráci s těmito skupinami, občas se nám podaří najít způsoby, jak znovu zamezit šíření podvodných profilů.

I když naše snaha může působit jako malá záplata, často pomáhá. Pomohli jsme už mnoha lidem, kteří se díky našim zásahům přesvědčili, že komunikují s podvodníkem, když profil, se kterým komunikovali, zmizel. Takové malé kroky mohou mít velký dopad, protože pomáhají obětem přestat věřit podvodníkům a chrání je před dalším zneužitím.

Ačkoliv je naše činnost slabá v porovnání s celkovou škodou, kterou podvodníci způsobují, víme, že alespoň děláme něco pro to, abychom lidem pomohli. A pokud se nám podaří zachránit alespoň jednoho člověka, má to smysl.

A vím, že máš jednu otázku, co by asi mohlo pomoci nejvíc. Nejlepší je s nimi vůbec nekomunikovat, nepustit si je do života, nepřijímat žádné žádosti.

Platí tu taková zásada: Nepustíš cizího do svého domu, když ho neznáš. Tak proč bys měl přijímat žádost od cizího člověka jako přítele? To není tvůj přítel. Lidé se musí chránit tím, že pustí do svého života jen ty, které opravdu znají, koho mohou reálně oslovit. A ne, pro mě to není jen imaginární osoba. Je to někdo, kdo pro mě nic neznamena, je cizí, takže proč bych ho měla vůbec pustit do svého života? Nepustím ho, nepřijmu, nebudu s ním mluvit, neodpovídat, konec. Blokování znamená žádný kontakt.

V případě tohoto konkrétního romantického podvodu pomáhá jedině toto.

O: Doufám, že tyto cenné rady padnou na úrodnou půdu a třeba někomu, kdo si tohle bude číst pomohou. Dobrá, blížíme se k závěru a mě by ještě zajímalo, zda ve finále bys byla

schopna zhodnotit, co pro tebe bylo vlastně horší? Ten emocionální zážitek, nebo tak finanční ztráta?

L: Ano, nemohu říct, že by mi nebylo líto těch peněz, bylo mi to líto, ale věděla jsem, co dělám, když jsem je dobrovolně poslala někomu cizímu, plně si vědoma svého činu. To je zásadní chyba – poslat peníze někomu, koho neznám. To by nikdy nikdo neměl udělat a já jsem věděla, co dělám, když jsem to poslala. V té chvíli jsem věděla, že ty peníze už nikdy nezískám zpět. Ne, že by mi to nebylo líto, ale tuto ztrátu nepovažuji za ztrátu.

Ale ta emocionální bolest, ta odezva, to, co to se mnou udělalo, kolik mi to vzalo ze života... To je to, co se těžko prožívá. Jakou ztrátu? Cítila jsem, že ta emocionální ztráta mě zasáhla. Z toho se člověk těžko vzpamatovává. Přišla jsem o nějaké peníze, řekněme pár eur, ale to není to, co mě na tom opravdu bolelo. Jak jsem říkala, byla to charita. Nikdy v životě už žádnou charitu neudělám. Mám to za celý život vybrané.

Brala jsem to takto, abych dokázala tuto zkušenost přežít a nezbláznila se z toho. Takto se z toho nezblázním, ale ta emocionální devastace... Pocit pochybností o sobě, co jsem udělala, proč jsem to udělala, jak se ke mně něco takového mohlo dostat, co to se mnou udělalo... Cítila jsem, že něco ve mě zemřelo. Část mě zemřela tou událostí a už se nikdy neprobudí. Ta ztráta tam je a já vím, co jsem dělala. A i přesto to na mně zanechalo tyto stopy.

O: Dobře, mockrát ti děkuji za opravdu vyčerpávající odpovědi. Je to velmi silný příběh, který máš za sebou. Zeptám se tě ještě, jaké máš teď pocity, po tom, co jsi mi celý svůj příběh povykládala?

L: Mnoho pocitů se mi vrátilo zpátky. Víš, člověk se snaží na něco zapomenout, nebo časem něco přestane bolet. Ale teď se mi mnoho z těch pocitů vrátilo zpět a cítím se, jako bych nemohla dýchat. Ne, že bych měla nějaký fyzický problém, ale je to v srdci, ty křeče tam pořád jsou, to cítíš, to se nedá změnit. Už jsem se ale naučila o tom mluvit, i když to bylo na začátku těžké. Přiznat si to, vůbec někomu říct, že jsem mohla být tak hloupá a udělat to. Ano, mohla jsem. Stalo se to a teď se musím naučit o tom mluvit. Takže teď to není tak, že bych odhadovala, co ti mohu říct nebo co ti říct nemohu. To prostě vychází samo ze mě.

Víš, kdyby se to stalo znovu, člověk, naše lidská bytost, ta lidskost stále někde existuje. I když hodně z toho už zmizelo. Lidé už nejsou jako dřív. Důvěra je teď hodně narušená. Obecně nevěříš nikomu. Nevěříš člověku na ulici, který ti omdlel před očima, protože si myslíš, že je opilý a nevíš, že má zdravotní problém. Tak ať se tam válí, já mu nepomůžu.

Ta zlost mezi lidmi je naživo a existuje i v tomto virtuálním prostředí. Existuje určitý stupeň důvěry, ale také extrémní stupeň, kdy věříš člověku na druhé straně úplně všechno, co ti řekne.

Kdyby mi teď někdo řekl, že nutně potřebuje pomoc, protože jeho dítě je těžce nemocné a zda bych mu mohla nějak pomoci, i finančně, určitě bych o tom přemýšlela. Pomoci mu, poslat nějaké peníze na léčbu, protože to dítě trpí. Samozřejmě že vím, že za tím může být podvod, že je to sociální podvod. Takových podvodů je mnoho. Ale i přesto bych byla schopná to udělat, protože to člověčenství v nás zůstává. Zamyslíš se, jestli to, co uděláš, někomu pomůže. A máš z toho dobrý pocit, když dáš třeba jen 10 eur na nemocné děti nebo na cokoliv. Lidé chtějí pomáhat, někdy anonymně, někdy veřejně. Možná někdo to dělá z úplně jiných důvodů, ale myslím si, že ta lidskost v nás ještě zůstává. Jsme schopní znovu skočit do podvodu. A nezastavíš se, prostě pošleš těch 10 korun, pošleš těch 10 eur, protože to někomu může pomoci a tobě to neublíží.

A jsme v době, kdy už existují podvody na jakémoliv téma.

O: To jednoznačně. Ještě by mě zajímalo, teď už opravdu na závěr, jestli si myslíš, že by ses po tomhle zážitku už nemohla nikdy stát obětí podvodu?

L: Myslím, že mohla. Protože si pořád myslím, že v nějakém okamžiku budu mít pocit, že někomu chci pomoci.

Možná to pomůže, možná to bude dobrý skutek. Tohle nedokážu vypnout, prostě bych byla schopná to zopakovat. Ale v tomto konkrétním případě, co se týče romantického podvodu, to už asi nikdy. Už jsem tak zkušená, že to dokážu rozpoznat na první pohled.

A myslím si, že každý druhý člověk je schopný do takového podvodu spadnout, protože každému něco chybí. A když oni zjistí, co ti přesně chybí, na čem ti záleží, tak tě mají. V té chvíli tě mají.

O: Tak dobrá. Leno, já ti mockrát děkuji ještě jednou, za tu všechnu důvěru, kterou jsi mi věnovala, uvědomuji si, že to není vůbec jednoduché, o takové zkušenosti mluvit. Rozumím tomu, že ta zkušenost je obrovsky silná a jsi skvělá, že o ní nejen mluvíš takto otevřeně, ale ještě navíc proti tomu aktivně bojuješ a snažíš se chránit ty, kteří by si potenciálně mohli zažít to samé, za to ti patří můj velký dík a obdiv. Mockrát ti děkuji a měj se krásně. Ahoj

L: Pokud by tě časem napadly nějaké otázky, až to zpracuješ a vlastně zjistíš, že ses na něco ještě nezeptal, klidně to můžeme zopakovat, když řekneš. Já sama ani nevím, co všechno jsem ti vlastně povídala. A také děkuji...

5.6 Výsledky hypotéz

Zde byly rozebrány jednotlivé výsledky hypotéz, které ukázal hloubkový rozhovor

Podvodník je z Afriky a vydával se za amerického vojáka

Z rozhovoru plyne, že když se oběť pokoušela zaslat podvodníkovi své finanční prostředky podruhé, pokusila se tak učinit na účet s adresou ve Spojených státech, což se nepovedlo, nicméně následně se pokusil podvodník nabídnout účet s adresou v Africe, což oběť odmítla. Nakonec se podvodníkovi povedlo peníze získat z účtu Americké banky. Z pokusu podvodníka o nabídnutí afrického účtu bylo usouzeno, že se podvodník opravdu v Africe nachází. Není totiž pravděpodobné, že by si americký podvodník myslel, že africký účet vzbudí v oběti větší dojem bezpečí. Navíc založení bankovního účtu v Africe občanem Ameriky by bylo velmi obtížné. Druhá část hypotézy a sice, že se podvodník vydával za amerického vojáka se potvrdila.

Podvedenou našel náhodou na sociální síti Facebook

Tato hypotéza se potvrdila. Podvodník skutečně kontaktoval podvedenou oběť na sociální síti Facebook. Nicméně i tak byl způsob oslovení poměrně překvapivý. Předpokladem totiž bylo, že podvodník rozešle potenciálním obětem tzv. udičku a bude čekat, jestli se na ni náhodou někdo chytne. To se ovšem nestalo, na místo toho podvodník napsal velmi personalizovanou zprávu, přímo ušitou oběti. To muselo vyžadovat i určitou přípravu, kdy podvodník věděl, čím se oběť živí i odkud pochází.

Podvodník se pokusil oběti namluvit, že potřebuje poslat peníze s nějakým emocionálně zabarveným důvodem

Tato hypotéza se potvrdila. Podvodník skutečně vyzkoušel během dlouhých rozhovorů na svou oběť hned několik emocionálně zabarvených důvodů, proč by mu měla zaslat finanční prostředky. Nejdříve se podvodník pokoušel zahrát na chamtivost. Namluvil oběti, že potřebuje zachránit velmi vysoký žold za své služby v armádě, jenže bohužel kufr s penězi uvízl na hranici v Turecku. Slíbil pak oběti, že pokud zaplatí propuštění skrz hranici, nabídne oběti určitou sumu jako odměnu. Na to ovšem oběť nepřistoupila, a tak se podvodník rozhodl pro jinou metodu. Pokusil se oběti namluvit, že potřebuje peníze za to, že ho pustí

z Afghánistánu. Ve chvíli, kdy se dozvěděl, že oběť opět odmítá, snažil se v ní vyvolat lítost. Namlouval oběti, že pokud to neudělá tak tím vlastně dokazuje, že nemá podvodníka ráda a že dopustí, že tam zemře. Když ani tohle nezabralo, podvodník zahrál na city opět. Nyní tím, že potřebuje koupit počítač pro svého syna, aby spolu mohli komunikovat, protože syn potřebuje tátu a bez počítače spolu nejsou v kontaktu. Na tohle už oběť přistoupila.

Podvodník psal s viditelnými překlepy a bylo jednoduše poznat, že šlo o cizince

Tahle hypotéza se z části nepotvrdila. Skutečně bylo jednoduše poznat, že oběť si dopisuje s cizincem, nicméně tím důvodem nebyly gramatické chyby, ani překlepy, nýbrž absence informovanosti podvodníka o tom, že u nás používáme vykání a tykání. To byl první a patrný náznak toho, že jde o cizince. Další nápovědou byla skladba vět, která mnohdy nedávala správný smysl.

Předpokládám, že se při rozhovorech projeví, že podvodník je méně vzdělaný člověk, který se v zemi třetího světa uchýlil k nekalé praktice snadného finančního obohacení

Tato hypotéza se vůbec nepotvrdila. Ukázalo se naopak, že podvodníci dnes již pracují velmi dobře. Podle výpovědi oběti se ukázalo, že podvodníci perfektně zvládají sociální manipulování s obětí a téměř by se dalo i polemizovat, zda nejsou tímto směrem vzdělání. Další z překvapivých faktů je, že oběť uvedla, že si byla vědoma a několikrát si to i otestovala, že se na ní podvodníci střídali. Oběť se domnívá, že každý z podvodníků podléhá nějaké specifické specializaci a podle tématu se střídají na konverzaci s obětí.

Podvodník se snažil s obětí navázat i intimní vztah, za cílem následného vydírání díky erotickým fotografiím.

Tato hypotéza se nepotvrdila. Oběť uvádí, že jejich vztah byl čistě přátelský, nikoliv intimní. Každopádně pravdou je, že se podvodník pokoušel oběť vydírat i na fotkách, na kterých nebylo nic vyzývavého. Překvapením ovšem zůstává fakt, že se podvodník údajně o zisk intimních fotografií ani jednou nepokusil.

Předpokládám, že se oběť do podvodníka zamilovala a tato emoce ji přiměla zaslat podvodníkovi své finance.

Ani tohle se úplně nepotvrdilo. Z rozhovoru spíše vyplývá, že se oběť upnula na podvodníka v přátelské rovině. Ovšem tak silně, že strach ze ztráty vzájemného kontaktu ji přiměl právě k zaslání peněz neznámo kam.

Podvedená osoba si odnáší ze střetu s podvodníkem velmi silnou emotivní zkušenost, kterou hodnotí jako horší, než finanční ztrátu

Zde se hypotéza naprosto potvrdila. Oběť skutečně uvedla, že celý tento zážitek vnímá jako daleko větší osobní zásah než lítost nad finanční ztrátou. Tohle je typické pro tento typ podvodu a taky základní rozdíl mezi lovescamem a ostatními podvodnými metodami.

ZÁVĚR

Teoretická část se zabývala vymezením podvodu, jeho právním hlediskem a detailně probrala historii bankovních podvodů na příkladu bankovníctví ve Spojených státech. Dále pak teoretická část rozebrala jednotlivé podvodné metody, které jsou dnes nejčastěji používané, vymezila je jako pojem a následně rozebrala praktické použití na příkladech. Dále se pak práce přenesla do konkrétních opatření, která umožní běžnému méně znalému uživateli internetu bezpečně využívat možnosti digitálního světa. V poslední části pak teoretická část popsala metody, kterými banky v České republice chrání své klienty a rozdělila je na aktivní a pasivní. Nakonec byly rozebrány ochranné prostředky proti podvodníkům, které používá Česká spořitelna.

Pro praktickou část práce byl zvolen hloubkový rozhovor s ženou, která se stala obětí podvodného jednání známého jako „lovescam“. Před samotným rozhovorem byly stanoveny výzkumné hypotézy a vytvořena struktura rozhovoru. Praktická část zároveň definuje pojem hloubkového rozhovoru a objasňuje, proč byla tato metoda zvolena jako nejvhodnější pro zkoumání daného problému. Tento podvod trval téměř dva roky a podvedenou paní stál nemalé finanční prostředky, a navíc také značné psychické trauma. Hloubkový rozhovor nabídl detailní náhled do vnímání podvedené a velmi barvitě popsal, jak dokáže být tento podvod neuvěřitelně zákeřný. Běžná veřejnost se na tento podvod často dívá skrze prsty, protože lovescam považuje za něco, na co by přece člověk se zdravým rozumem nenaletěl. Hloubkový rozhovor však nabídl odlišný a mnohem komplexnější pohled na věc. Na rozdíl od běžných podvodů, jako je phishing nebo vishing, které oběť nachytají v momentě krátkodobé nepozornosti, lovescam spoléhá na dlouhodobou sociální manipulaci. Podvodník se dlouhodobě snaží proniknout do života své oběti a zaplnit v jejím nitru prázdnotu, kterou cíleně vyhledává. Po několika měsících, či letech psychického vydírání, naléhání a vyhrožování často oběť nekončí jen bez peněz, ale i s psychickým traumem, kterého se pravděpodobně nezavírá do konce života. A to je zásadní rozdíl mezi lovescamm a ostatními podvody.

SEZNAM POUŽITÉ LITERATURY

- [1] FEDERAL RESERVE BANK OF SAN FRANCISCO. Pandemic Brings Increase in Fraud. Online. 2021. Dostupné z: <https://www.frbsf.org/research-and-insights/blog/sf-fed-blog/2021/11/08/covid-19-pandemic-increase-fraud/>. [cit. 2025-04-12].
- [2] MUNI. *Podvod, jeho druhy a vývoj od roku 1989*. Online. 2011. Dostupné z: https://is.muni.cz/th/ywolq/Text_prace.pdf. [cit. 2025-04-12].
- [3] 25LET KURZYCZ. § 209 paragraf 209. Online. 2024. Dostupné z: <https://www.kurzy.cz/zakony/40-2009-trestni-zakonik/paragraf-209/#paragraf-209H1>. [cit. 2025-04-12].
- [4] THE ONLINE LIBRARY OF LIBERTY. *A History of Banking in all the Leading Nations, vol. I (U.S.A.)*. Online. 2024. Dostupné z: <https://oll.libertyfund.org/titles/bulletin-a-history-of-banking-in-all-the-leading-nations-vol-1-u-s-a>. [cit. 2025-04-12].
- [5] AVAST. *Avast zablokoval v roce 2023 rekordních 10 miliard útoků*. Online. 2024. Dostupné z: <https://blog.avast.com/cs/2020-rok-ve-znameni-fake-news-koronavirovych-podvodu-a-ransomwaru>. [cit. 2025-04-12].
- [6] PENIZE.CZ. *Kaspersky: Pětina kyberútoků v roce 2023 trvala déle než měsíc*. Online. 2024. Dostupné z: <https://www.penize.cz/455555-kaspersky-petina-kyberutoku-v-roce-2023-trvala-dele-nez-mesic>. [cit. 2025-04-12].
- [7] BRNO DAILY. *Police Report Shows Decline In Czech Crime Rate For 2024*. Online. 2025. Dostupné z: <https://brnodaily.cz/2025/01/27/news/police-report-shows-decline-in-czech-crime-rate-for-2024/>. [cit. 2025-04-12].
- [8] MĚŠEC.CZ. *Nechte mě, nebo vás zažalují! Co se odehrává v mysli obětí kyberšmejdu*. Online. 2024. Dostupné z: <https://www.mesec.cz/clanky/nechte-me-nebo-vas-zazaluji-co-se-odehrava-v-mysli-obeti-kybersmejdu/>. [cit. 2025-04-12].
- [9] *Podvody v platebním styku*. Online. 2024. Dostupné z: <https://www.cnb.cz/cs/casto-kladene-dotazy/Podvody-v-platebnim-styku/>. [cit. 2024-10-25].
- [10] ČESKÁ SPOŘITELNA. *Chraňte své peníze před podvodníky*. Online. 2025. Dostupné z: <https://www.csas.cz/cs/o-nas/bezpecnost-ochrana-dat>. [cit. 2025-04-13].

- [11] ESET. *What is Phishing?* Online. 2021. Dostupné z: https://www.eset.com/uk/about/newsroom/blog/what-is-phishing/?srsltid=AfmBOoo4j-QyJa2g54vK3ubYmoZjd7Hc9-6OH_fw7s_6E3FsghgnVkf. [cit. 2025-04-13].
- [12] UNIVERSITY OF NEWCASTLE. *Why are romance scams so powerful?* Online. 2022. Dostupné z: https://www.newcastle.edu.au/data/assets/pdf_file/0009/935298/Hanna-S-Cunha-Article.pdf. [cit. 2025-04-13].
- [13] YUBICO. *What is Vishing?* Online. 2025. Dostupné z: <https://www.yubico.com/resources/glossary/vishing/>. [cit. 2025-04-13].
- [14] QUORA. *What is the origin of the word Bazaar?* Online. 2018. Dostupné z: <https://www.quora.com/What-is-the-origin-of-the-word-Bazaar>. [cit. 2025-05-09].
- [15] ETYMONLINE. *Fake*. Online. 2023. Dostupné z: <https://www.etymonline.com/word/fake>. [cit. 2025-04-13].
- [16] ETYMONLINE. *Banker*. Online. 2023. Dostupné z: <https://www.etymonline.com/word/fake>. [cit. 2025-04-13].
- [17] ETYMONLINE. *Investment*. Online. 2023. Dostupné z: <https://www.etymonline.com/word/fake>. [cit. 2025-04-13].
- [18] BARTVISIONS. *Jak se chránit na sociálních sítích?* Online. 2024. Dostupné z: <https://www.bartvisions.cz/2024/07/jak-se-chranit-na-socialnich-sitich/>. [cit. 2025-04-13].
- [19] SUBROSA. *Understanding the Importance of Link Checker Safety in the World of Cybersecurity*. Online. 2024. Dostupné z: <https://www.subrosacyber.com/en/blog/link-checker-safety>. [cit. 2025-04-13].
- [20] TECHTARGET. *Top 15 email security best practices for 2025*. Online. 2025. Dostupné z: <https://www.techtarget.com/searchsecurity/tip/2019s-top-email-security-best-practices-for-employees>. [cit. 2025-04-13].
- [21] AVAST. *Jak poznám, že je webová stránka bezpečná?* Online. 2018. Dostupné z: <https://blog.avast.com/cs/jak-poznam-ze-je-webova-stranka-bezpecna>. [cit. 2025-04-13].

- [22]PSYCHOLOGYWRITING. *Perception and Critical Thinking*. Online. 2024. Dostupné z: <https://psychologywriting.com/perception-and-critical-thinking/>. [cit. 2025-04-13].
- [23]PENÍZE.CZ. *Konec falešných recenzí. E-shopy musí ukázat, proč jim věřit*. Online. 2022. Dostupné z: <https://www.penize.cz/ochrana-spotrebitele/437599-konec-falesnych-recenzi-e-shopy-musi-ukazat-proc-jim-verit>. [cit. 2025-04-13].
- [24]BEYONDTRUST. *15 Password Management Best Practices*. Online. 2022. Dostupné z: <https://www.beyondtrust.com/blog/entry/top-15-password-management-best-practices>. [cit. 2025-04-13].
- [25]UK SAFER INTERNET CENTRE. *ProjectEVOLVE*. Online. 2025. Dostupné z: <https://saferinternet.org.uk/blog/projectevolve-who-is-it-for-and-how-can-it-help-your-school?>. [cit. 2025-05-09].
- [26]ŽIVĚ. *Jak na internetu surfovat anonymně: osvědčené způsoby na zametení stop*. Online. 2019. Dostupné z: <https://www.zive.cz/clanky/jak-na-internetu-surfovat-anonymne-osvedcene-zpusoby-na-zameteni-stop/sc-3-a-184471/default.aspx>. [cit. 2025-04-18].
- [27]ČESKÁ SPOŘITELNA. *Bezpečné finance: Jak se bránit proti moderním typům podvodů?* Online. 2025. Dostupné z: <https://financnezdravejsi.csas.cz/cs/jsem-v-bezpeci/bezpecne-finance-jak-se-branit-proti-modernim-typum-podvodu>. [cit. 2025-04-18].
- [28]TONERDEPOT. *Proč a který antivirus používat?* Online. 2025. Dostupné z: <https://www.tonerdepot.cz/blog/proc-a-ktery-antivirus-pouzivat>. [cit. 2025-04-18].
- [29]NORTON. *Why you should install software updates and operating system updates today*. Online. 2025. Dostupné z: <https://us.norton.com/blog/how-to/the-importance-of-general-software-updates-and-patches>. [cit. 2025-04-18].
- [30]LIFE24. *Nejbezpečnější webové prohlížeče*. Online. 2022. Dostupné z: <https://www.life24.cz/technologie/nejbezpecnejsi-webove-prohlizece>. [cit. 2025-04-18].
- [31]NORDICTELECOM. *Jak bezpečně používat veřejné Wi-Fi sítě*. Online. 2022. Dostupné z: <https://nordictelecom.cz/novinky/32/>. [cit. 2025-04-18].
- [32]APPLIŠTĚ. *Vzestup mobilních plateb*. Online. 2025. Dostupné z: <https://www.appliste.cz/vzestup-mobilnich-plateb/>. [cit. 2025-05-09].

- [33]RAIFFEISENBANK. *Jak si nastavit upozornění o pohybech na účtu*. Online. 2025. Dostupné z: <https://www.rb.cz/podpora/internetove-a-mobilni-bankovnictvi/nastaveni-notifikaci>. [cit. 2025-04-18].
- [34]MICROSOFT. *Co je dvojúrovňové ověřování?* Online. 2025. Dostupné z: <https://www.microsoft.com/cs-cz/security/business/security-101/what-is-two-factor-authentication-2fa>. [cit. 2025-04-18].
- [35]APPLE. *Správa otisků pro Touch ID*. Online. 2025. Dostupné z: <https://support.apple.com/cs-cz/guide/personal-safety/ipseededc3a8/web>. [cit. 2025-04-18].
- [36]APPLE. *Informace o vyspělé technologii Face ID*. Online. 2025. Dostupné z: <https://support.apple.com/cs-cz/102381>. [cit. 2025-04-18].
- [37]ČSOB. *Aplikace ČSOB Smart klíč*. Online. 2025. Dostupné z: <https://www.csob.cz/lide/ucty/internetove-a-mobilni-bankovnictvi/csob-smart-klic>. [cit. 2025-04-18].
- [38]MUNI. *Hlubkový rozhovor*. Online. 2025. Dostupné z: <https://kisk.phil.muni.cz/100metod/hlubkovy-rozhovor>. [cit. 2025-04-18].
- [39]CIALDINI, Robert. *Nové zbraně vlivu*. Jan Melvil publishing, 2023. ISBN 978-80-7555-181-8.
- [40]DUBOVECKÁ, Klára. *STUDENTS OF THE FACULTY OF SOCIAL STUDIES VS PHISHING ATTACKS: VULNERABILITY OF STUDENTS TO DIFFERENT TYPES OF PHISHING*. Bakalářská. Brno: Masarykova univerzita, 2022.

SEZNAM OBRÁZKŮ

Obrázek 1 Počty registrovaných skutků	19
---	----

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

GPS Global Positioning System

VPN Virtual Private Network

TLS/SSL Secure Socket Layer a Transport Layer Security

URL Uniform Resource Locator

AI – Artificial intelligence