VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, Z. Ú., ČESKÉ BUDĚJOVICE

BAKALÁŘSKÁ PRÁCE

INVESTIČNÍ PODVODY V KYBERPROSTORU

Autor práce: David Kropík

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Katedra právních oborů a bezpečnostních studií

2026

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú.
Žižkova tř. 1632/5b, 370 01 České Budějovice

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: David Kropík

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Investiční podvody v kyberprostoru

Název bakalářské práce v anglickém jazyce: Investment Fraud in Cyberspace

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce (jméno a příjmení, včetně titulů):
RNDr. Růžena Ferebauerová

Datum zadání bakalářské práce (měsíc, rok): Listopad, 2025

Cíl bakalářské práce:
Cílem bakalářské práce je identifikovat nejčastější formy investičních podvodů v kyberprostoru, charakterizovat jejich mechanismy a na základě výsledků dotazníkového šetření vyhodnotit úroveň informovanosti veřejnosti o těchto rizicích, včetně faktorů, které přispívají k jejich zranitelnosti vůči těmto podvodům.

Student: David Kropík	8.12.2025 *datum*	 *podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	11.12.25 *datum*	 *podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	11.12.2025 *datum*	 *podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	11.12.2025 *datum*	 *podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	20.12.2025 *datum*	 *podpis*

VYSOKÁ ŠKOLA EVROPSKÝCH A REGIONÁLNÍCH STUDIÍ, z. ú. ČESKÉ BUDĚJOVICE

Prohlašuji, že jsem bakalářskou práci vypracoval(a) samostatně, na základě vlastních zjištění a s použitím odborné literatury a materiálů uvedených v seznamu použitých zdrojů.

Prohlašuji, že v souladu s § 47b zákona č. 111/1998 Sb. v platném znění souhlasím se zveřejněním své bakalářské práce v elektronické podobě ve veřejně přístupné části infodisku VŠERS, a to se zachováním mého autorského práva k odevzdanému textu této kvalifikační práce. Souhlasím dále s tím, aby toutéž cestou byly v souladu s uvedeným ustanovením zákona č. 111/1998 Sb. zveřejněny posudky vedoucí(ho) a oponentů práce i záznam o průběhu a výsledku obhajoby kvalifikační práce. Rovněž souhlasím s porovnáním textu mé kvalifikační práce systémem na odhalování plagiátů.

.....

Děkuji vedoucí bakalářské práce RNDr. Růženě Ferebauerové za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

KROPÍK D. *Investiční podvody v kyberprostoru: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2026. 66 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová

Klíčová slova: investiční podvod, kyberprostor, oběť, phishing, útočník, sociální inženýrství

Tato bakalářská práce se zaměřuje na aktuální téma investičních podvodů v online prostředí a jejich dopad na běžné uživatele. Hlavním cílem práce je analyzovat mechanismy těchto podvodů a na základě získaných dat posoudit, nakolik je veřejnost o těchto hrozbách informována. Teoretický základ tvoří rozbor různých forem online investičních podvodů, kde je kladen důraz hlavně na metody sociálního inženýrství, zneužívání jmen známých osobností a vytváření falešných investičních nabídek. Práce se věnuje také právnímu pohledu na věc a důležitosti prevence pro digitální bezpečnost. Praktický přínos spočívá v dotazníkovém šetření, které zjišťovalo, jak jsou respondenti informovaní a nakolik dokážou v reálných situacích rozpoznat hrozby spojené s online investováním. Analýza se soustředí na varovné signály podvodů a na to, jak ostražití jsou lidé při klikání na odkazy nebo reklamy na sociálních sítích. Ze získaných dat vyplývá, že i když lidé o hrozbách teoreticky vědí, jejich skutečné reakce na manipulativní útoky mají stále značné mezery.

ABSTRACT

KROPÍK D. Investment Fraud in Cyberspace: Bachelor Thesis. České Budějovice: The College of European and Regional Studies, 2026. 66 pp. Supervisor: RNDr. Růžena Ferebauerová

Key words: investment fraud, cyberspace, victim, phishing, social engineering, attacker

This bachelor's thesis focuses on the current issue of investment fraud in the online environment and its impact on ordinary users. The main objective of the thesis is to analyze the mechanisms of these scams and, based on the data collected, assess the extent to which the public is aware of these threats. The theoretical foundation consists of an analysis of various forms of online investment fraud, with an emphasis on social engineering methods, the misuse of celebrities' names, and the creation of fake investment offers. The thesis also addresses the legal perspective on the matter and the importance of prevention for digital security. The practical contribution lies in a questionnaire survey that assessed how well-informed respondents are and to what extent they can recognize threats associated with online investing in real-life situations. The analysis focuses on warning signs of fraud and on how vigilant people are when clicking on links or ads on social media. The data reveals that while people are theoretically aware of the threats, their actual responses to manipulative attacks still show significant gaps.

Obsah

Úvod

Investiční podvody v kyberprostoru jsou v posledních letech na vzestupu a představují čím dál častější hrozbu pro běžné uživatele internetu. S tím, jak se online investování stalo dostupným pro širokou veřejnost, se začalo objevovat i velké množství podvodných nabídek, které se tváří jako legitimní příležitosti k získání finančního obnosu. Pachatelé dnes nevyužívají jen technické chyby v systémech bank a dalších institucí, ale hlavně psychologické faktory, jako je například nepozornost, důvěřivost. Kvůli anonymitě v online prostředí je pak velmi těžké tyto peníze získat zpět, což z tohoto tématu dělá vážný problém pro banky i policii.

Útočníci nejčastěji sázejí na metody sociálního inženýrství. Využívají falešné reklamy, nátlak přes telefon nebo zneužívají tváře známých osobností, aby v lidech vzbudili falešný pocit jistoty. Schopnost tyto triky včas poznat je často jedinou cestou, jak o peníze nepřijít. Přestože se o bezpečnosti na internetu mluví v poslední době v médiích často, pohled na skutečné zkušenosti lidí s těmito útoky a na to, jak na ně reálně reagují, ukazuje na přetrvávající nedostatky v ostražitosti, a proto je potřeba se tomuto tématu věnovat hlouběji. Dnešní investování už není jen o akciích, ale zahrnuje i složitější oblasti jako jsou kryptoměny. Podvody se v tomto prostředí neustále mění a přizpůsobují tomu, co je zrovna populární. Proto je důležité sledovat nejen to, jak jsou lidé technicky zabezpečení, ale hlavně to, jak dokážou informace na internetu kriticky vyhodnocovat a zachovat se v takové situaci. Klíčovým prvkem v tomto problému zůstává prevence a ochrana, která v dnešní době nezahrnuje pouze technické zabezpečení, ale především povědomí uživatelů a využívání asistenčních služeb, jako je například kybernetické pojištění.

Teoretická část práce nejprve vymezuje samotný pojem kyberprostoru a důvěru uživatelů v tomto prostředí. Následně definuje základní formy kyberkriminality, jako jsou phishing či vishing, a popisuje profily pachatelů i zranitelnost obětí. Pozornost je také věnována mechanismům sociálního inženýrství, zneužití vzdáleného přístupu a konkrétním druhům investičních podvodů, včetně falešných platforem, kryptoměnových podvodů a zneužívání známých osobností. Teoretický blok uzavírá analýza následků těchto činů, přehled příslušné legislativy v čele s trestním zákoníkem a možnosti prevence i technické ochrany.

Praktická část práce navazuje na teoretické poznatky a prostřednictvím dotazníkového šetření zkoumá, jak respondenti vnímají rizika investičních podvodů.

Šetření zjišťuje intenzitu využívání internetu a typy používaných zařízení, přičemž se dále soustředí na reálné zkušenosti s podezřelými reklamami na sociálních sítích nebo znalost pojmu phishing. Dalším okruhem je analýza přímého oslovení respondentů prostřednictvím podezřelých e-mailů či zpráv a vyhodnocení jejich bezprostřední reakce na nevyžádané online nabídky. Pozornost je věnována také tomu, zda se respondenti aktivně věnují investování a jakým způsobem v praxi ověřují důvěryhodnost platforem, včetně těch, které zneužívají tváře známých osobností. Šetření dále rozebírá schopnost identifikovat varovné signály podvodu a zjišťuje zkušenosti s tímto fenoménem v blízkém okolí. V závěru jsou posouzeny postoje k formám prevence, důvěra v informační zdroje a pocit informovanosti o hrozbách v kyberprostoru

1 Cíl a metodika bakalářské práce

Bakalářská práce se věnuje problematice investičních podvodů v kyberprostoru. Cílem bakalářské práce je analyzovat mechanismy podvodného jednání v online prostředí, zhodnotit úroveň informovanosti o těchto rizicích v závislosti na technické zdatnosti a identifikovat hlavní faktory, které ovlivňují zranitelnost při investování na internetu.

V teoretické části je za pomoci literární rešerše definována kybernetická kriminalita a její specifika. Pozornost je věnována psychologickým aspektům a metodám sociálního inženýrství, jako je nátlak na emoce nebo zneužití autority. Následující kapitoly podrobně rozebírají konkrétní druhy podvodů, od phishingu přes podvody s kryptoměnami až po zneužívání známých osobností a falešné investiční platformy. Součástí teoretické části je také právní úprava kybernetické kriminality v České republice. Teoretickou část uzavírá přehled preventivních opatření, který se zaměřuje na technické zabezpečení, ochranu při vzdáleném přístupu a možnosti kybernetického pojištění.

V praktické části bakalářské práce jsou investiční podvody popsány z hlediska reálné praxe. K dosažení cíle práce bylo provedeno dotazníkové šetření. Dotazník je postaven chronologicky od identifikačních otázek, přes zjišťování využívaných zařízení pro přístup k internetu, až po otázky na praktické zkušenosti s podvody. Jeden z klíčových okruhů šetření zjišťuje, kdy a jak dochází k setkání s podezřelou nabídkou a zda jsou rozpoznány varovné signály. Analýza se dále zaměřuje na to, zda probíhá aktivní investování a jak tato zkušenost ovlivňuje vnímání rizik. Otázky také směřují na rozdíl mezi teoretickou znalostí pojmů a praktickým chováním při ověřování odkazů a reklam na sociálních sítích. Dále je v šetření řešeno, jakým informačním zdrojům je přikládána váha a jaké formy prevence jsou vnímány jako nejúčinnější. Poslední část otázek se věnuje sebehodnocení a víře ve vlastní schopnost rozpoznat podvodný útok.

2 Kyberprostor

Pojem kyberprostor byl poprvé použit americkým spisovatelem Williamem Gibsonem v povídce Burning Chrome z roku 1982 a do širšího povědomí se dostal zejména díky románu Neuromancer. Gibsonovo pojetí kyberprostoru však vycházelo především z oblasti science fiction a odlišovalo se od současného odborného chápání tohoto pojmu. Kyberprostor byl v jeho dílech popisován jako imaginární, vizuálně pojaté prostředí představující metaforu propojení dat a lidské mysli. Současné pojetí kyberprostoru je naproti tomu založeno na reálné technické infrastruktuře a praktickém fungování informačních a komunikačních technologií ve společnosti.[1]

Kyberprostor můžeme vymezit z několika hledisek, které se vzájemně mezi sebou doplňují. Z technického pohledu ho lze chápat jako soubor technologických zařízení, která jsou mezi sebou propojena na různých komunikačních medií. Tato propojení mohou být realizována jak bezdrátově, tak i za pomocí kabelových přenosů, například přes optický kabel. Do kyberprostoru patří rozsáhlé počítačové systémy, servery, směrovače, tak i běžná koncová zařízení, kterými jsou například mobilní telefony, tablety, chytré hodinky a další podobná zařízení. Přístup do kyberprostoru je umožněn za pomocí internetového připojení, které je ve většině případů realizováno bezdrátově.[2]

Toto prostředí je dále možné také vnímat jako virtuální realitu, která nemá stanové žádné hranice, takže nikde nezačíná ani nekončí. Přestože se jedná o nehmotné prostředí, existence kyberprostoru je zcela závislá na materiálních technologiích umístěných ve fyzické formě. Avšak kyberprostor díky rozptýlení jednotlivých hmotných prvků, jako jsou síťové komponenty, počítačové systémy, cloudová úložiště, dokáže fungovat i při částečném poškození této infrastruktury. V případě úplného zničení těchto hmotných prvků by však došlo k nevratnému narušení, nebo zániku kyberprostoru.[3]

Z hlediska fungování jej lze rovněž definovat jako prostor kybernetických aktivit nebo jako prostředí vytvářené informačními a komunikačními technologiemi. Oproti reálnému světu se jedná o specifické prostředí, ve kterém nemůžeme automaticky

[1] LIBICKY, Martin C. In: *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press, 2007, S. 5. ISBN 978-0-511-28535-6.
[2] SMEJKAL, Vladimír. Kapitola 1 Počítače a kybernetická kriminalita – základní pojmy. In: *Kybernetická kriminalita*. 3. rozšířené a aktualizované vydání. Čeněk, 2022, S. 31–39. ISBN 978-80-7380-849-5.
[3] KOLOUCH, Jan a BAŠTA A KOL., Pavel. In: *CyberSecurity*. Praha: CZ.NIC, z. s. p. o, 2019, S. 35. ISBN 978-80-88168-34-8.

předpokládat, že zde budou platit stejná pravidla, jaká platí ve fyzickém prostoru. Z toho důvodu se musela postupně vymezit nová kritéria odpovídající pro kyberprostor, zejména v souvislosti s vymezením právních vztahů.[4]

2.1 Využití Kyberprostoru

Kyberprostor je v současné době pro každého znáš běžnou součástí života a jeho využití je pro většinu uživatelů každodenní samozřejmostí. Slouží především ke komunikaci, sdílení informací a realizaci pracovních i osobních aktivit. Prostřednictvím elektronické pošty, sociálních sítí a různých online platforem je tak umožněn rychlý kontakt mezi lidmi bez ohledu na jejich fyzickou vzdálenost. Velkou roli hraje kyberprostor také v oblasti práce a vzdělávání, kde umožňuje práci z domova, nebo realizace studijních činností v online prostoru.

Vedle komunikace a práce je kyberprostor využíván také k poskytování velké škály digitálních služeb. Mezi tyto služby patří například elektronické obchodování, online služby, veřejné správy nebo využívání digitálních obsahu. Součástí využití kyberprostoru jsou také finanční aktivity, jako je internetové bankovnictví, online platby, nebo online investiční platformy. Díky rostoucí nabídce všech těchto služeb se pro spoustu lidí stává kyberprostor nedílnou součástí života.[5]

2.2 Důvěra uživatelů v kyberprostoru

Dlouhodobé a každodenní používání kyberprostoru má velký vliv na to, jakým způsobem jej uživatelé vnímají a jak se v něm chovají. Postupem času se u části uživatelů vytváří pocit bezpečí a pocit jistoty, a to ovlivňuje jejich míru obezřetnosti v tomto online prostředí. Právě tato důvěra a pocit samozřejmosti může vést k tomu, že uživatelé přestávají věnovat dostatečnou pozornost možným rizikům a méně si ověřují informace či chování online služeb kde se nejčastěji pohybují. V praxi se ukazuje že významnou roli při vzniku bezpečnostních incidentů hraje lidský faktor, a to zejména chyby nepozornost, nebo přílišná důvěra uživatelů. Tyto skutečnosti poté mohou být zneužity k podvodnému jednání, což zvyšuje celkovou zranitelnost uživatelů v kyberprostoru. [6]

---

[4] KOLOUCH, Jan a BAŠTA A KOL., Pavel. In: *CyberSecurity*. Praha: CZ.NIC, z. s. p. o, 2019, S. 35. ISBN 978-80-88168-34-8.

[5] KOLOUCH, Jan a BAŠTA A KOL., Pavel. In: *CyberSecurity*. Praha: CZ.NIC, z. s. p. o, 2019, S. 36. ISBN 978-80-88168-34-8.

[6] KREČ, Luboš. *Bezpečnost firem ohrožují jejich vlastní lidé, v kyberprostoru se vyplatí nulová důvěra, radí etičtí hackeři*. Online. 2021. Dostupné z: https://byznys.hn.cz/c1-66903030-bezpecnost-firem-ohrozuji-jejich-vlastni-lide-v-kyberprostoru-se-vyplati-nulova-duvera-radi-eticti-hackeri. [cit. 2026-01-28].

3 Kyberkriminalia

Pojem kyberkriminalita označuje trestnou činnost, při níž hrají klíčovou roli informační a komunikační technologie. Digitální zařízení, jako jsou počítače, mobilní telefony nebo další prvky informační infrastruktury, zde mohou vystupovat nejen jako nástroj pro páchání trestné činnosti, ale také jako jejich přímí cíl. Nejedná se teda pouze o využití moderních technologií při páchání běžné kriminality, ale o specifickou formu protiprávního jednání, která je spjata s digitálním prostředím.[7]

Jednoznačné vymezení kyberkriminality je v odborné literatuře dlouhodobě považováno za problematické, a to zejména kvůli velké šířce tohoto pojmu, který zahrnuje různé formy jednání. Některé definice jsou vymezovány příliš úzce a nezahrnují všechny relevantní projevy této kriminality, jiné jsou naopak tak obecné, že by bylo možné pod pojmem kyberkriminality zařadit téměř jakýkoliv trestný čin, při němž byl použit počítač, nebo internet. Právě z tohohle důvodu zde neexistuje žádná přímá definice která by tento pojem vymezovala zcela jednoznačně.[8]

Toto prostředí se vyznačuje zejména absencí geografických hranic a vysokou mírou časové dostupnosti. Informace jsou zde přístupné prakticky kdykoliv a odkudkoliv v závislosti na připojení k síti, což má přímý dopad na způsob páchání trestné činnosti. Útočníci tak mohou s relativně nízkými náklady způsobit značné škody a současně využívat prostředí, které významně ztěžuje jejich identifikaci a následné odhalení.[9]

Z hlediska dopadů se jedná o kriminalitu, která může zasahovat nejen na jednotlivé osoby, ale také na velké organizace a veřejné instituce. Její formy se neustále vyvíjejí v návaznosti na technologický pokrok a měnící se způsob používání digitálních technologií. Právě díky této dynamice a schopnosti se přizpůsobit, dělá z kyberkriminality významný bezpečností problém současné společnosti.[10]

[7] ZÁVRŠNÍK, Aleš. In: *Kyberkriminalita*. Právní monografie. Praha: Wolters Kluwer, 2017, S. 1-3. ISBN 978-80-7552-759-2.
[8] ZÁVRŠNÍK, Aleš. In: *Kyberkriminalita*. Právní monografie. Praha: Wolters Kluwer, 2017, S. 1-3. ISBN 978-80-7552-759-2.
[9] GŘIVNA, Tomáš; POLČÁK, Radim a UHLÍŘOVÁ, Kateřina. In: *Kyberkriminalita a právo*. Praha: Auditorium, 2008, S. 30. ISBN 978-80-903786-7-4.
[10]GŘIVNA, Tomáš; POLČÁK, Radim a UHLÍŘOVÁ, Kateřina. In: *Kyberkriminalita a právo*. Praha: Auditorium, 2008, S. 30. ISBN 978-80-903786-7-4.

3.1 Základní formy kyberkriminality

Kyberkriminalita zahrnuje obrovské množství trestných činností, které se liší jak způsobem provedení, tak i cílem útoku. V praxi se tak jedná o zneužití důvěry uživatelů pohybující se v kyberprostoru

3.1.1 Phishing

Phishing je jedna z nejrozšířenějších forem kybernetických podvodů. Jedná se o podvodné jednání, při kterém se snaží útočníci získat od oběti citlivé údaje, jako jsou například přihlašovací údaje, osobní informace nebo údaje k platebním kartám. Základem phishingu je oklamání uživatele za pomocí falešné komunikace, která se tváří jako zpráva od důvěryhodné instituce, nebo osoby, příkladem může být třeba banka, nebo státní organizace.[11]

Nejčastější formou phishingu jsou podvodné e-maily, které uživatele nabádají k tomu, aby provedl nějakou akci, například změnou hesla, nebo potvrzení platby. Tyto e-maily většinou obsahují odkazy, které se tváří jako legitimní stránka, ale ve skutečnosti se jedná pouze o podvodnou stránku vytvořenou podvodníky. Po zadání vašich údajů se většinou nic nestane a vaše přihlašovací údaje, nebo číslo karty získají podvodníci. Vedle e-mailového phishingu se zde vyskytují také další varianty, jako je například smishing, který funguje za pomocí SMS zpráv, nebo vishing který funguje prostřednictvím telefonické komunikace, při níž se útočník vydává například za pracovníka banky, nebo technické podpory. [12]

Úspěšnost phishingových útoků je založené především na lidském faktoru a důvěře uživatelů, kteří běžně používají online komunikační kanály. Útočníci se snaží vyvinout co největší časový tlak a strach, aby snížili ostražitost oběti. Phishing je tak tím pádem jedna z bran k dalším podvodům, zejména k finančním a investičním podvodům.

3.1.2 Vishing

Vishing je metoda, kdy útočník využívá k získání citlivých údajů a financí přímo telefonní hovor. Hlavním rozdílem oproti komunikaci přes e-mail je přímý kontakt, který pachateli umožňuje okamžitě reagovat na dotazy oběti. Útočníci se vydávají za pracovníky banky, policisty nebo technickou podporu. Cílem útočníka je zneužít svého

[11] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. In: *Výkladový slovník kybernetické bezpečnosti*. Páté doplněné a upravené vydání. Praha: Česká pobočka AFCEA, 2022, S. 122. ISBN 978-80-908388-4-0.
[12] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. In: *Výkladový slovník kybernetické bezpečnosti*. Páté doplněné a upravené vydání. Praha: Česká pobočka AFCEA, 2022, S. 122. ISBN 978-80-908388-4-0.

důvěryhodně znějícího hlasu k tomu, aby oběť nadiktovala například potvrzovací kódy, nebo autorizovala platbu.[13]

3.1.3 Spoofing

Základním principem spoofingu je sofistikované maskování identity útočníka, které má v oběti vyvolat falešný pocit bezpečí. Nebezpečí této metody spočívá především v tzv. Caller ID Spoofingu. Útočníci zde využívají bezpečnostní mezery v telefonních sítích k tomu, aby na displeji oběti došlo k zobrazení jakéhokoliv čísla. Nejčastěji se jedná o oficiální linky bankovních institucí, Policie ČR nebo státní správy. Oběť pak nemá důvod k pochybnostem, protože volající působí legitimně. Stejný princip se uplatňuje i v e-mailové komunikaci, kde útočník manipuluje se zprávou tak, aby adresa odesílatele přesně odpovídala firemnímu standardu.[14]

3.1.4 Pharming

Pharming představuje vyšší stupeň hrozby než klasický phishing, a to zejména kvůli své funkci být téměř neviditelný. Zatímco phishingové útoky vyžadují aktivní chybu uživatele, u pharmingu útočí přímo na síťové komunikace. Typicky dochází k manipulaci s DNS záznamy nebo k napadení zranitelných domácích Wi-Fi routerů. Pro uživatele je tento útok prakticky nezjistitelný: do prohlížeče zadá správnou a ověřenou URL adresu své banky, ale systém ho bez jakéhokoliv varování přesměruje na podvržený server. Vzhledem k vizuální identitě falešného webu s originálem je následná krádež přihlašovacích údajů pro útočníka jen otázkou několika sekund.[15]

3.1.5 Podvodné e-shopy a inzeráty

Podvodné e-shopy a inzeráty představují další rozšířenou formu kyberkriminality, se kterou se mohou běžní uživatelé v online prostředí setkat. Smyslem tohoto jednání je přesvědčit oběť o tom, že se jedná o standardní bezpečný obchod.

S rostoucím rozsahem online nakupování se tyto praktiky stávají stále častějšími a zasahují značnou část uživatelů.

[13] HADNAGY, Christopher a FINCHER, Michele. In: *Phishing Dark Waters*. John Wiley & Sons, 2015, s. 27-28. ISBN 978-1-119-18362-4.
[14] HADNAGY, Christopher a FINCHER, Michele. In: *Phishing Dark Waters*. John Wiley & Sons, 2015, s. 25-27. ISBN 978-1-119-18362-4.
[15] GRIMES, Roger A. a JUST, John N. In: *Fighting Phishing: everything you can do to fight social engineering and phishing*. Indianapolis: John Wiley, 2024, S. 36–37. ISBN 9781394249220.

Falešné e-shopy často nabízejí zboží za výrazně nižší ceny, než se běžně udává na trhu, případně prezentují časově omezené akce, které mají u uživatele vyvolat pocit naléhavosti. Po zaplacení produktu však zboží, které uživatel objedná vůbec nepřijde, nebo přijde úplně jiný produkt než měl být uživateli doručen. Dalším znakem takového podvodu je téměř nemožné dohledat kontaktní údaje, nebo nedohledatelné obchodní podmínky, což poté výrazně komplikuje případné vrácení peněz.[16]

Samostatnou skupinu tvoří také podvodné inzeráty, které se objevují na internetových bazarech a inzertních portálech. Útočníci zde mohou vystupovat jak v roli prodávajícího, tak v roli kupujícího. Častým příkladem takového podvodu je, když je oběť vyzvána zaplatit předem, nebo je nucena zadat citlivé údaje na stránku vytvořenou útočníky a slouží k odcizení těchto informací. Dopady těchto podvodů nejsou omezeny pouze na finanční ztráty, ale mohou vést i k dalším formám zneužití, jako jsou například neoprávněné transakce, nebo krádež identity. Anonymita útočníků a častý mezinárodní přesah těchto případů navíc výrazně ztěžují jejich odhalení a následný trestní postih.[17]

3.2 Pachatelé a oběti v kyberprostoru

3.2.1 Profil a motivace pachatelů

Pachatelé kyberkriminality využívají prostředí kyberprostoru především kvůli možnosti působit na dálku a s omezeným rizikem odhalení. Oproti klasické trestné činnosti zde není nutný žádný osobní kontakt s obětí, což v tomto případě umožňuje útočníkům zasahovat velké množství uživatelů bez nutnosti fyzické přítomnosti na místě činu. Právě anonymita a obtížná dohledatelnost patří k hlavním důvodům proč se kyberkriminalita v posledních letech výrazně zvyšuje.[18]

Hlavní motivace pro pachatele bývá finanční zisk, jelikož v kyberprostoru lze dosáhnout vysokého výnosu s malým úsilím. Pachatelé často využívají jednoduché ale efektivní taktiky, díky kterým dokáží oslovit až několik stovek potencionálních obětí v krátkém časovém úseku. Nejedná se však pouze o jednotlivce, ale v dnešní době jsou to i velké organizované skupiny působící na mezinárodní úrovni. Tyto skupiny kombinují

[16] CIALDINI, Robert B. In: *Nové zbraně vlivu*. V Brně: Jan Melvil Publishing, 2023, S. 27–28. ISBN 978-80-7555-181-8.
[17] CIALDINI, Robert B. In: *Nové zbraně vlivu*. V Brně: Jan Melvil Publishing, 2023, S. 27–28. ISBN 978-80-7555-181-8.
[18] KOLOUCH, Jan. In: *CyberCrime*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016, S. 12–14. ISBN 978-80-88168-18-8.

technické prostředky s psychologickými tak, aby měli co největší šanci z potencionálních obětí získat peníze nebo citlivé údaje.[19]

3.2.2 Zranitelnost oběti

Způsob, jakým uživatelé vnímají a využívají kyberprostor, má zásadní vliv na jejich míru zranitelnosti vůči podvodům v kyberprostoru. Každodenní používání digitálních technologií vede u mnoha lidi k tomu, že online prostředí se pro ně stává postupem času jako běžné a důvěryhodné prostředí. Tato rutina však může postupně oslabovat obezřetnost a vést k různých rizikům, která jsou s pohybem v kyberprostoru spojena.[20]

Jeden z dalších faktorů zvyšující riziko, že se uživatel stane obětí kyberkriminality, je nedostatečná kontrola a ověřování informací. V praxi se často objevují situace, kdy uživatelé reagují na nečekané výzvy, aniž by si ověřili jejich pravost. Útočníci těchto situací využívají ve svůj prospěch a záměrně pracují s psychologickými prvky, jako je vyvolání naléhavosti nebo strachu. Lidská chyba, nepozornost a přehnaná důvěra je tak jedním z hlavních důvodů úspěšnosti kybernetických útoků.[21]

[19] KOLOUCH, Jan. In: *CyberCrime*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016, S. 12–14. ISBN 978-80-88168-18-8.
[20]SEDLÁK, Petr a KONEČNÝ, Martin. In: *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021, S. 114-116. ISBN 978-80-7623-068-2.
[21] SEDLÁK, Petr a KONEČNÝ, Martin. In: *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. Brno: CERM, akademické nakladatelství, 2021, S. 114-116. ISBN 978-80-7623-068-2.

4 Mechanismy sociálního inženýrství a lidský faktor v online podvodech

Úspěch moderních kybernetických útoků dnes nestojí pouze na technické vyspělosti škodlivého softwaru, ale především na schopnosti útočníků manipulovat s lidským rozhodováním. Sociální inženýrství v tomto kontextu představuje metodu, která namísto prolamování šifer cílí na zneužití přirozených lidských emocí, jako je důvěřivost, strach nebo vidina rychlého zisku.[22]

4.1 Techniky budování falešné legitimity a autority

V online světě, kde chybí osobní kontakt, je důvěra tím nejdůležitějším a zároveň nejkřehčím článkem. Útočníci si to uvědomují a celý jejich úspěch stojí na tom, že musí oběť během pár minut přesvědčit o své profesionalitě. Snaží se vytvořit dojem, že peníze budou u nich v bezpečí, k čemuž využívají osvědčené triky kombinující psychologii s moderními technologiemi.[23]

Základem bývá naprostá sebejistota při komunikaci. Útočník nevolá jako někdo, kdo zkouší štěstí, ale jako někdo, kdo se v oboru vyzná a o své oběti už něco ví. Často se představuje jako osobní bankéř nebo analytik z prestižní firmy. Aby zněl co nejvíce věrohodně, začne používat odborné termíny, které většina lidí sice zná z doslechu, ale úplně přesně jim nerozumí.[24]

Další částí je vizuální stránka. Podvodníci si dávají hodně práce s tím, aby jejich weby vypadaly totožně, nebo dokonce i lépe, než stránky skutečné banky. Používají ukradená loga známých institucí, falšují různé certifikáty a na stránky umisťují grafy, které se hýbou v reálném čase. Všechno to tak má působit jako obchodní terminál. Pro běžného uživatele internetu je téměř nemožné poznat, že ten krásný web se stejnou adresou je ve skutečnosti pouze podvod vytvořený během několika dnů[25].

Důležitým prvkem celého podvodu je vyvolání pocitu, že v tom oběť není sama. Podvodníci na svých stránkách nebo v reklamách na Facebooku a ostatních sociálních

[22] ESET. Online. Sociální inženýrství. Dostupné z: https://www.eset.com/cz/socialni-inzenyrtsvi-a-bezpecnost-firmy/. [cit. 2026-03-19].
[23] ARTIC WOLF. *What is Social Engineering?* Online. Dostupné z: https://arcticwolf.com/resources/glossary/social-engineering/. [cit. 2026-01-28].
[24] ARTIC WOLF. *What is Social Engineering?* Online. Dostupné z: https://arcticwolf.com/resources/glossary/social-engineering/. [cit. 2026-01-28].
[25] ARTIC WOLF. *What is Social Engineering?* Online. Dostupné z: https://arcticwolf.com/resources/glossary/social-engineering/. [cit. 2026-01-28].

sítích ukazují nespočet spokojených recenzí. Jsou tam fotografie lidí, kteří se usmívají a píší, jak díky této platformě mohli zaplatit hypotéku a další potřebné věci a v některých případech tam přidají i příběh nějaké celebrity. Využití známých osobností v reklamních sděleních tak významně zvyšuje důvěryhodnost podvodu a vede k oslabení přirozené ostražitosti uživatele.[26]

4.2 Mechanismy přímé manipulace

Pokud se podvodníkům úspěšně podaří s obětí vybudovat dobrý první dojem a získají si pozornost, přichází na řadu nejdůležitější část celého procesu, kterou je přímý kontakt útočníka s obětí. Zatímco webové stránky slouží pouze jako prvotní nástroj, telefonický kontakt je primárním nástrojem k psychologickému ovlivnění oběti a vyvolání požadované reakce. Telefonická komunikace poskytuje podvodníkům značnou výhodu, protože na rozdíl od e-mailu umožňuje okamžitě vyvíjet nátlak a nedává oběti prostor pro kritické zhodnocení situace nebo konzultaci s blízkými.[27]

Nejsilnější zbraní, kterou podvodníci při hovoru využívají, je vyvolání pocitu naléhavosti. Nabízená investice je prezentována jako příležitost, která trvá pouze pár minut a už se nikdy nebude opakovat. Útočníci záměrně pracují se strachem z ušlé příležitosti, kdy oběť pod tlakem ztrácí schopnost logického úsudku a začíná jednat impulzivně. Rychlá a sebejistá mluva útočníka má v napadeném vyvolat dojem, že hovoří s expertem, který situaci plně rozumí. K tomuto tlaku se navíc přidává i informační zahlcení, kdy útočník začne předkládat technické detaily o grafech a burze, v nichž se neproškolený uživatel snadno přestává orientovat. Takto přetížený člověk pak snadno začne podléhat tomu, že se spolehne na „zkušeného makléře“, který najednou vystupuje jako zachránce, avšak ve skutečnosti útočník provádí cílenou manipulaci. [28]

S tím také úzce souvisí snaha útočníků udržet oběť na lince za jakoukoliv cenu. Přerušení hovoru a následná konzultace s rodinou nebo přáteli by totiž mohli vést k ukončení celého podvodu. Útočníci se proto snaží udržovat kontakt i hodiny, kdy jejich cílem je oběť psychicky vyčerpat. Finálním krokem této manipulace je pak snaha přimět vystresovanou oběť k instalaci softwaru pro vzdálenou správu, nejčastěji se jedná o

[26] ARTIC WOLF. *What is Social Engineering?* Online. Dostupné z: https://arcticwolf.com/resources/glossary/social-engineering/. [cit. 2026-01-28].
[27] JIROVSKÝ, Václav. In: *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, S. 195-205. ISBN 978-80-247-1561-2.
[28] JIROVSKÝ, Václav. In: *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, S. 195-205. ISBN 978-80-247-1561-2.

program AnyDesk, díky kterému získají útočníci plnou kontrolu nad zařízením a bankovnictvím.[29]

4.3 Zneužití vzdáleného přístupu

Jakmile se útočníkovi podaří oběť v hovoru dostatečně psychicky unavit, přichází na řadu technická část podvodu. Útočníkův cíl je v tuto chvíli získat přímý přístup k bankovnictví oběti, ale tak, aby to pro banku nevypadalo podezřele. K tomu dnes podvodníci nepotřebují žádné složité hackerské nástroje. Stačí jim, když se útočníkům podaří oběť přesvědčit, aby si sama do mobilu nebo počítače nainstalovala program AnyDesk nebo TeamViewer. [30]

Tyto programy jsou samy o sobě kompletně legitimní a běžně se využívají například ve velkých firmách, kde mohou IT technici na dálku spravovat problémy pro firmu. Poté, co uživatel program spustí a nadiktuje útočníkovi přístupový kód, získává druhá strana plnou kontrolu nad plochou, soubory i myší a klávesnicí. Útočník v tu chvíli ovládá zařízení stejně, jako by u něj fyzicky seděl.[31]

Tento moment je pro úspěch podvodu zásadní. Pokud se útočník přihlásí do bankovnictví skrze tento vzdálený přístup, bankovní systémy vidí přihlášení z běžně používaného zařízení a známé IP adresy, což výrazně snižuje riziko zablokování účtu. V této fázi útočník připravuje na pozadí odchozí platby a oběť záměrně rozptyluje grafy zisků, nebo potvrzení o zaregistrování do jejich fiktivních investičních programů. Celý proces je zakončen tím, že útočník požádá oběť, aby potvrdila převod v mobilní aplikaci pod záminkou, že se jedná pouze o testovací vklad nebo aktivaci účtu. Ve skutečnosti tak oběť nevědomky potvrzuje převod svých úspor na účty bílých koní, odkud peníze bleskově mizí na další účty.[32]

---

[29] JIROVSKÝ, Václav. In: *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, S. 195-205. ISBN 978-80-247-1561-2.

[30] ČSOB. Online. Podvod se vzdálenou správou AnyDesk a TeamViewer. Dostupné z: https://www.csob.cz/v-obraze/blog/clanky/podvod-se-vzdalenou-spravou-anydesk-a-teamviewer. [cit. 2026-03-19].

[31] ANYDESK. Online. Jak předejít podvodům přes AnyDesk. Dostupné z: https://www.instaluj.cz/anydesk/jak-predejit-podvodum-pres-anydesk/. [cit. 2026-03-19].

[32] ČSOB. Online. Podvod se vzdálenou správou AnyDesk a TeamViewer. Dostupné z: https://www.csob.cz/v-obraze/blog/clanky/podvod-se-vzdalenou-spravou-anydesk-a-teamviewer. [cit. 2026-03-19].

5 Investiční podvody v kyberprostoru

Investiční podvody v kyberprostoru představují jednu z významných forem online kriminality, která se týká širokého spektra uživatelů. Rozvoj digitálních technologií a snadná dostupnost internetu umožnily vznik nových investičních příležitostí, zároveň však vytvořily také prostor pro zneužívání důvěry veřejnosti. Podvodné nabídky se často tváří jako legitimní investice a využívají moderní online prostředí k oslovení co největšího počtu potenciálních obětí. [33]

Typickým znakem investičních podvodů v kyberprostoru je jejich vysoká míra profesionality a přesvědčivosti. Podvodné reklamy často slibují rychlé a vysoké zhodnocení finančních prostředků. Útočníci využívají graficky propracované webové stránky, smyšlené a falešné recenze. Útočníci k oslovení obětí využívají širokou škálu metod, od graficky propracovaných webových stránek až po sofistikované formy přímého oslovení, jak je podrobně uvedeno v předchozí kapitole o mechanismech manipulace.[34]

Velkou roli v šíření investičních podvodů hraje také lidský faktor. Lidé jsou často motivování vidinou snadného výdělku a pod nátlakem emocí, jako je strach z promarněné příležitosti nebo snaha rychle zlepšit svou finanční situaci. Nedostatečné znalosti v oblasti investování a fungování finančních trhů často vedou k tomu, že oběti nedokáží včas rozpoznat podvod a stanou se obětí podvodníků.

Závažnost investičních podvodů spočívá nejen ve financích ztrátách jednotlivců, ale také v narušení online prostředí jako celku. Tyto podvody jsou tak rozšířené, že přesahují hranice států, což značně komplikuje práci dopadnout podvodníky a provádět následné trestní řízení. Investiční podvody tak představují závažný společenský problém.[35]

[33] ČESKÁ NÁRODNÍ BANKA. *Varování před podvodnými investičními platformami*. Online. 2024. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/ochrana-spotrebitele/upozorneni/Varovani-pred-podvodnymi-investicnimi-platformami/. [cit. 2026-01-28].
[34] ČESKÁ NÁRODNÍ BANKA. *Varování před podvodnými investičními platformami*. Online. 2024. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/ochrana-spotrebitele/upozorneni/Varovani-pred-podvodnymi-investicnimi-platformami/. [cit. 2026-01-28].
[35] POLICIE ČESKÉ REPUBLIKY. *Pozor na podvody na internetu!!!*. Online. 2024. Dostupné z: https://policie.gov.cz/clanek/or-melnik-zpravodajstvi-pozor-na-podvody-na-internetu.aspx. [cit. 2026-01-28].

5.1 Průběh investičních podvodů

Investiční podvody v kyberprostoru mají většinou velmi podobný scénář, který se opakuje bez ohledu na to, zda se nabídka týká levných akcií, kryptoměn nebo jiných finančních prostředků. Celý proces tak lze rozdělit do tří klíčových fází, kdy oběť postupně propadává podvodu.[36]

Prvním krokem tohoto podvodu je propracovaná inzerce na sociálních sítích, která cílí na emoce a přirozenou snahu lidí zajistit se do budoucna. Ve chvíli, kdy uživatel v naději na snadný výdělek zadá své jméno a telefonní číslo, pro útočníky to představuje klíčový moment pro zahájení přímé komunikace. Aby útočníci potlačili pochybnosti, využívají stejný vizuální styl webových stránek, jako například u velkých bankovních institucí. jak je podrobně vysvětleno v kapitole 4.1 [37]

Jakmile oběť zanechá své údaje, následuje telefonát od člověka, co se vydává za osobního bankéře, nebo investičního specialistu, který se snaží působit jako poradce pro získání finančního zisku za pomocí investice. V tomto bodě ještě útočníci nechtějí vybrat celý účet, ale dovést oběť k prvnímu menšímu vkladu. Tento krok slouží zejména k překonání psychologické bariéry. Jakmile člověk pošle první peníze, začne celé věci věřit mnohem více, obzvlášť, když útočníci ukážou na falešných grafech fiktivní zhodnocení vložených prostředků.[38]

Celý podvod vrcholí v ten moment, kdy se oběť pokusí o výběr svých domnělých zisků nebo když odmítá posílat další finanční prostředky. V tento moment útočníci změní svou strategii. Místo slibů o zisku začnou tvrdit, že pro vyplacení peněz je nutné nejdříve uhradit fiktivní poplatky, daně nebo provize. Právě pod touto záminkou, kdy oběť věří, že je už jen krůček od svých peněz, je oběť dotlačena k instalaci programu pro vzdálený přístup, jak je podrobně vysvětleno v kapitole 4.3.[39]

[36] DOVE, Martina. In: *The psychology of fraud, persuasion and scam techniques: understanding what makes us vulnerable*. New York: Routledge, 2025, S. 2-3. ISBN 978-1-003-59025-5.
[37] DOVE, Martina. In: *The psychology of fraud, persuasion and scam techniques: understanding what makes us vulnerable*. New York: Routledge, 2025, S. 2-3. ISBN 978-1-003-59025-5.
[38] DOVE, Martina. In: *The psychology of fraud, persuasion and scam techniques: understanding what makes us vulnerable*. New York: Routledge, 2025, S. 2-3. ISBN 978-1-003-59025-5.
[39] DOVE, Martina. In: *The psychology of fraud, persuasion and scam techniques: understanding what makes us vulnerable*. New York: Routledge, 2025, S. 2-3. ISBN 978-1-003-59025-5.

5.2 Druhy investičních podvodů

5.2.1 Falešné investiční platformy

Klíčovým prvkem těchto podvodů je vytvoření sofistikovaného webového rozhraní, které vizuálně napodobuje legitimní investiční platformy. Uživatel po registraci sleduje fiktivní růst svých investic prostřednictvím grafů a statistik, které jsou však plně pod kontrolou útočníka a neodpovídají reálnému trhu. Tato vizualizace zisků slouží jako psychologický nástroj, který má v oběti upevnit pocit úspěšné investice a motivovat ji k dalším vkladům, přičemž finanční prostředky jsou ve skutečnosti převáděny přímo na účty pachatelů.[40]

Podvodné platformy často zneužívají názvy známých finančních institucí nebo investičních nástrojů k posílení důvěryhodnosti u veřejnosti. Pachatelé navíc využívají lákavé nabídky v podobě bonusových vkladů, které mají u oběti vyvolat pocit výjimečné příležitosti. Celý systém je však uzavřeným mechanismem, který neumožňuje reálné obchodování ani následný výběr zisků. Hlavním cílem je získání maximálního objemu prostředků dříve, než si uživatel uvědomí, že zobrazená data na obrazovce neodpovídají zůstatku na jeho skutečném účtu.[41]

5.2.2 Investiční podvody využívající kryptoměny

V oblasti kryptoměnových podvodů útočníci zneužívají obecného povědomí o existenci digitálních měn v kombinaci s nízkou úrovní technických znalostí uživatelů o principu jejich převodu. Mechanismus podvodu často spočívá v tom, že oběť nejprve převede finanční prostředky na legitimní českou kryptoměnovou burzu, což budí dojem bezpečnosti a legality celé operace a po nákupu dané kryptoměny následuje klíčová fáze útoku, kdy je uživatel pod manipulativním příslibem vysokého zisku přesvědčen k převodu finančních prostředků na privátní peněženku ovládanou útočníkem.[42]

Hlavním rizikem u těchto transakcí je jejich nevratnost. V prostředí kryptoměn neexistuje možnost reklamace nebo stornování příkazu, jako je tomu u běžných bankovních služeb. Po odeslání finančních prostředků na anonymní adresu útočníka se

[40] HOLT, Thomas J.; BOSSLER, Adam M. a SEIGFRIED-SPELLAR, Kathryn C. In: *Cybercrime and digital forensics: an introduction*. Second edition. London: Routledge, 2018, S. 218-223. ISBN 978-1-138-23872-5.
[41] HOLT, Thomas J.; BOSSLER, Adam M. a SEIGFRIED-SPELLAR, Kathryn C. In: *Cybercrime and digital forensics: an introduction*. Second edition. London: Routledge, 2018, S. 218-223. ISBN 978-1-138-23872-5.
[42] POLICIE ČESKÉ REPUBLIKY. *Podvod s investicemi do kryptoměny*. Online. Dostupné z: https://policie.gov.cz/clanek/podvod-s-investicemi-do-kryptomeny.aspx. [cit. 2026-01-29].

tato stávají prakticky nedohledatelnými. Jelikož zde nefiguruje žádná centrální bankovní autorita, která by mohla převod zastavit, bývá ztráta financí v naprosté většině případů trvalá. Orgány činné v trestním řízení navíc narážejí na obtížnou sledovatelnost těchto prostředků, protože pachatelé využívají rozsáhlé sítě peněženek k zakrytí historie těchto transakcí.[43]

5.2.3 Zneužití známých osobností

V České republice představuje tato metoda v současnosti jeden z nejúčinnějších postupů, neboť zneužívá přirozenou důvěru veřejnosti v autority a známé tváře. Podvodníci využívají identitu známých firem, například energetických společností, kterou spojují s tvářemi politiků, jako je prezident Petr Pavel, guvernér centrální banky nebo sportovní legendy, jakou je například Jaromír Jágr. Užití tváří veřejně známých osobností slouží k přenosu jejich autority na podvodný produkt, čímž dochází k oslabení kritického myšlení a vytvoření falešného pocitu bezpečí. Inzeráty jsou prezentovány jako exkluzivní příležitosti k investicím do strategických státních projektů, což vede k potlačení přirozené ostražitosti obětí.[44]

Největším vrcholem této manipulace je pak využití technologie Deepfake. Útočníci pomocí umělé inteligence vytvářejí videa, kde veřejně známé osobnosti promlouvají k divákům přímo prostřednictvím videa, které vypadá jako skutečná reportáž v televizi nebo v internetových zprávách, kde prezident vlastním hlasem a s přirozenou mimikou vysvětluje, jak je nový investiční program výhodný. Pro běžného uživatele, který na takovou reklamu narazí, je téměř nemožné poznat, že jde o digitální podvrh. Celý tento vizuální podvod slouží jen jako návnada, která má oběť přimět k vyplnění kontaktních údajů.[45]

5.2.4 Romantické podvody s investičním prvkem

Tato forma útoku kombinuje psychologickou manipulaci s investičním podvodem. Název “pig butchering” (v překladu porážka prasete) přesně vystihuje strategii útočníků. Strategie spočívá v dlouhodobém budování emoční vazby a vytváření falešné důvěry, což útočníkovi následně umožňuje manipulovat oběť k vysokým

[43] POLICIE ČESKÉ REPUBLIKY. *Podvod s investicemi do kryptoměny*. Online. Dostupné z: https://policie.gov.cz/clanek/podvod-s-investicemi-do-kryptomeny.aspx. [cit. 2026-01-29].
[44] AVAST. *Investiční podvody s lidmi, které nejspíš znáte*. Online. Dostupné z: https://blog.avast.com/cs/investicni-podvody-s-lidmi-ktere-mozna-znate. [cit. 2026-01-29].
[45] AVAST. *Investiční podvody s lidmi, které nejspíš znáte*. Online. Dostupné z: https://blog.avast.com/cs/investicni-podvody-s-lidmi-ktere-mozna-znate. [cit. 2026-01-29].

finančním vkladům. Celý tento proces začíná nenápadně, často náhodnou zprávou na WhatsAppu nebo sociálních sítích, která vypadá jako omyl. Útočníci se snaží pomalu budovat virtuální vztah a předstírají vážný zájem, aby oběť neměla žádné podezření a skutečně podlehla citům útočníka.[46]

Jakmile vznikne citové pouto, útočník začne navádět oběť na falešnou investiční platformu. Aby oběť však definitivně uvěřila, nechá ji na začátku vybrat malý "zisk", což vede k tomu, že oběť uvěří v legálnost celého systému a pošle i své celoživotní úspory. Celý podvod je ukončen tím, když se oběť pokusí o reálný výběr větší sumy peněz. V ten moment se útočník vymlouvá na smyšlené poplatky nebo daně. Jakmile oběť už nemá co poslat, útočník okamžitě zmizí a zablokuje si oběť.[47]

5.3 Známé případy investičních podvodů

5.3.1 OneCoin

Jedním z nejznámějších investičních podvodů v oblasti kryptoměn je projekt OneCoin, který byl spuštěn v roce 2014. Projekt byl prezentován jako nová digitální měna, která měla konkurovat známým kryptoměnám a investorům přinést vysoké zisky. Ve skutečnosti se však nejednalo o skutečnou kryptoměnu, ale o podvodný systém fungující na principu pyramidového schématu. Investoři byli motivováni k nákupu vzdělávacích balíčků, které údajně obsahovaly tokeny této kryptoměny.[48]

Projekt založila bulharská podnikatelka Ruja Ignatova spolu se svými spolupracovníky. Společnost pořádala prezentace a marketingové akce po celém světě, kde propagovala investice do OneCoinu. Investoři byli často přesvědčováni, aby do projektu zapojili také další osoby, což je typický znak pyramidových schémat. Ve skutečnosti však kryptoměna OneCoin nefungovala na veřejném blockchainu a investoři neměli možnost své prostředky reálně obchodovat.[49]

---

[46] O2 CYBERNEWS. *Pig butchering*. Online. Dostupné z: https://o2cybernews.cz/slovnik/pig-butchering. [cit. 2026-02-19].
[47] O2 CYBERNEWS. *Pig butchering*. Online. Dostupné z: https://o2cybernews.cz/slovnik/pig-butchering. [cit. 2026-02-19].
[48] UNITED STATES ATTORNEY'S OFFICE. *Co-Founder Of Multibillion-Dollar Cryptocurrency Scheme "OneCoin" Sentenced To 20 Years In Prison*. Online. 2023. Dostupné z: https://www.justice.gov/usao-sdny/pr/co-founder-multibillion-dollar-cryptocurrency-scheme-onecoin-sentenced-20-years-prison. [cit. 2026-02-19].
[49] UNITED STATES ATTORNEY'S OFFICE. *Co-Founder Of Multibillion-Dollar Cryptocurrency Scheme "OneCoin" Sentenced To 20 Years In Prison*. Online. 2023. Dostupné z: https://www.justice.gov/usao-sdny/pr/co-founder-multibillion-dollar-cryptocurrency-scheme-onecoin-sentenced-20-years-prison. [cit. 2026-02-19].

Podle amerického ministerstva spravedlnosti investovali lidé z celého světa do tohoto projektu více než 4 miliardy amerických dolarů. V roce 2023 byl spoluzakladatel projektu Karl Sebastian Greenwood ve Spojených státech odsouzen k trestu odnětí svobody v délce 20 let za svou roli v tomto podvodném schématu (U.S. Department of Justice, 2023). Případ OneCoin je dnes považován za jeden z největších investičních podvodů v historii kryptoměn.[50]

5.3.2 BitConnect

Dalším známým případem investičního podvodu v oblasti kryptoměn je projekt BitConnect, který fungoval v letech 2016 až 2018. Tato platforma nabízela investorům možnost zhodnotit své prostředky prostřednictvím tzv. „lending programu“. Uživatelé měli nakoupit kryptoměnu BitConnect a následně ji investovat do systému, který údajně využíval automatizovaný obchodní algoritmus generující vysoké zisky. Projekt sliboval investorům velmi vysoké výnosy, které měly být generovány prostřednictvím obchodování na kryptoměnových trzích. Ve skutečnosti však šlo o podvodné schéma založené na principu Ponziho systému. Výnosy starších investorů byly vypláceny z prostředků nových účastníků, což je typický znak tohoto typu finančního podvodu. [51]

Podle amerických úřadů způsobil projekt BitConnect investorům po celém světě škody ve výši přibližně 2,4 miliardy dolarů. Platforma byla nakonec v roce 2018 uzavřena poté, co regulační orgány začaly upozorňovat na její nelegální fungování a nedostatečnou transparentnost. Případ BitConnect je dnes považován za jeden z největších podvodů v historii kryptoměn. [52]

5.3.3 Twitter Bitcoin scam

Dalším známým případem investičního podvodu v kyberprostoru byl tzv. Twitter Bitcoin scam, ke kterému došlo v červenci roku 2020. Při tomto incidentu útočníci získali přístup k několika ověřeným účtům na sociální síti Twitter a následně z nich zveřejnili příspěvky propagující kryptoměnový podvod. V těchto příspěvcích útočníci

[50] UNITED STATES ATTORNEY'S OFFICE. *Co-Founder Of Multibillion-Dollar Cryptocurrency Scheme "OneCoin" Sentenced To 20 Years In Prison*. Online. 2023. Dostupné z: https://www.justice.gov/usao-sdny/pr/co-founder-multibillion-dollar-cryptocurrency-scheme-onecoin-sentenced-20-years-prison. [cit. 2026-02-19].

[51] BDO CANADA. *Fraudsters mask global Ponzi scheme behind deceptive cryptocurrency platform BitConnect*. Online. Dostupné z: https://www.bdo.ca/insights/cryptocurrency-execs-charged-for-2-4-billion-ponzi-scheme. [cit. 2026-02-19].

[52] BDO CANADA. *Fraudsters mask global Ponzi scheme behind deceptive cryptocurrency platform BitConnect*. Online. Dostupné z: https://www.bdo.ca/insights/cryptocurrency-execs-charged-for-2-4-billion-ponzi-scheme. [cit. 2026-02-19].

vyzývali uživatele, aby poslali kryptoměnu Bitcoin na určitou adresu s příslibem, že jim bude zaslaná částka zdvojnásobena. [53]

Mezi napadené účty patřily například účty známých osobností a společností, jako jsou Elon Musk, Barack Obama, Bill Gates, Apple nebo Uber. Díky velkému počtu sledujících působily tyto příspěvky na mnoho uživatelů důvěryhodně a některé osoby na podvod skutečně reagovaly. Během krátké doby tak útočníci získali kryptoměny v hodnotě přibližně 100 000 až 120 000 amerických dolarů. [54]

Vyšetřování později ukázalo, že útočníci využili techniky sociálního inženýrství a získali přístup k interním nástrojům společnosti Twitter, které jim umožnily ovládat účty uživatelů. Celkem bylo kompromitováno více než 100 účtů, přičemž zhruba 45 z nich bylo použito k šíření podvodných zpráv. Tento incident ukázal, jak mohou útočníci využít důvěru veřejnosti ve známé osobnosti a sociální sítě k realizaci investičních podvodů. [55]

5.4 Následky a dopady investičních podvodů

Následky investičních podvodů v kyberprostoru představují komplexní problém, který zdaleka přesahuje pouze oblast přímých finančních ztrát. V momentě, kdy dochází k definitivnímu přerušení komunikace ze strany útočníka, se oběť ocitá v situaci, která má hluboký dopad na její ekonomickou stabilitu i psychosociální integritu.

5.4.1 Finanční a existenční dopady

Cílem útočníků v kyberprostoru je získání maximálního množství finančních prostředků, což pro oběti často znamená závažnou finanční tíseň. Nejedná se pouze o ztrátu krátkodobých úspor, ale mnohdy o celoživotní úspory určené na zajištění bydlení či na stáří. Ztráta těchto prostředků vede k neschopnosti hradit běžné životní náklady, jako je nájemné či pravidelné platby, a k prudkému poklesu životní úrovně.[56]

Závažným aspektem je také skutečnost, že oběti jsou pod nátlakem donuceny k čerpání bankovních úvěrů nebo k půjčkám v rámci rodinných a přátelských vazeb. Uživatel se

[53] MITNICK SECURITY. *The 2020 Twitter Bitcoin Scam*. Online. Dostupné z: https://www.mitnicksecurity.com/blog/2020-twitter-bitcoin-scam. [cit. 2026-02-19].
[54] MITNICK SECURITY. *The 2020 Twitter Bitcoin Scam*. Online. Dostupné z: https://www.mitnicksecurity.com/blog/2020-twitter-bitcoin-scam. [cit. 2026-02-19].
[55] MITNICK SECURITY. *The 2020 Twitter Bitcoin Scam*. Online. Dostupné z: https://www.mitnicksecurity.com/blog/2020-twitter-bitcoin-scam. [cit. 2026-02-19].
[56] POLICIE ČESKÉ REPUBLIKY. *Podvod s investicemi do kryptoměny*. Online. Dostupné z: https://policie.gov.cz/clanek/podvod-s-investicemi-do-kryptomeny.aspx. [cit. 2026-02-19].

tak ocitá v dluhové pasti, kdy kromě ztráty vlastního majetku musí splácet reálné závazky, což má dlouhodobý negativní dopad na jeho finanční stabilitu.[57]

Navrácení neoprávněně vyvedených finančních prostředků je v online prostředí velmi komplikované. Pachatelé využívají vysoké míry anonymity internetu, a především specifických vlastností kryptoaktiv, která umožňují okamžitý přesun finančních prostředků do jiných států. Na rozdíl od standardních bankovních transakcí, u nichž existuje časová prodleva pro případnou blokaci či stornování příkazu, jsou tyto převody nevratné a probíhají v řádu sekund. Pro většinu obětí tato skutečnost znamená definitivní ztrátu finančních prostředků a omezené právní i technické možnosti další obrany.[58]

5.4.2 Vliv podvodu na psychiku oběti

Finanční ztráta představuje pouze jeden scénář dopadu investičního podvodu. Psychologické následky jsou často závažnější, neboť útočníci využívají sofistikované metody psychologického nátlaku a manipulační techniky, které vedou k nekritickému přijetí předložených informací. Jakmile dojde k odhalení podvodu, u oběti se typicky dostavuje stav hlubokého psychického traumatu, provázený pocity selhání v oblasti kritického myšlení.[59]

Dominantním faktorem v této fázi je intenzivní pocit studu. Oběti se často izolují od svého nejbližšího okolí, včetně rodiny a přátel, z obavy ze ztráty sociálního statusu. Strach z negativního hodnocení okolím či z potenciálního zesměšnění vede k tomu, že se poškození uzavírají do sebe a incident zamlčují. Právě tento psychologický mechanismus je hlavní příčinou nízké míry nahlášených případů, neboť oběť preferuje ochranu vlastního soukromí před rizikem opětovného prožívání traumatu v rámci vyšetřovacího procesu.[60]

Konečným důsledkem bývá hluboká nedůvěra k digitálnímu prostředí a moderním technologiím obecně. Poškozený vnímá online prostor jako trvale nebezpečný, což vyvolává rezistenci k dalšímu využívání digitálních služeb. Tato ztráta důvěry má

[57] POLICIE ČESKÉ REPUBLIKY. *Podvod s investicemi do kryptoměny*. Online. Dostupné z: https://policie.gov.cz/clanek/podvod-s-investicemi-do-kryptomeny.aspx. [cit. 2026-02-19].
[58] POLICIE ČESKÉ REPUBLIKY. *Podvod s investicemi do kryptoměny*. Online. Dostupné z: https://policie.gov.cz/clanek/podvod-s-investicemi-do-kryptomeny.aspx. [cit. 2026-02-19].
[59] DOVE, Martina. In: *The psychology of fraud, persuasion and scam techniques: understanding what makes us vulnerable*. New York: Routledge, 2025, S. 2-5. ISBN 978-1-003-59025-5.
[60] DOVE, Martina. In: *The psychology of fraud, persuasion and scam techniques: understanding what makes us vulnerable*. New York: Routledge, 2025, S. 2-5. ISBN 978-1-003-59025-5.

dlouhodobý negativní dopad na ochotu jedince využívat digitální technologie a na jeho schopnost bezpečně se orientovat v kyberprostoru.[61]

[61] DOVE, Martina. In: *The psychology of fraud, persuasion and scam techniques: understanding what makes us vulnerable*. New York: Routledge, 2025, S. 2-5. ISBN 978-1-003-59025-5.

6 Právní aspekty investičních podvodů

Investiční podvody v online prostředí jsou specifické tím, že útočníci kombinují psychologický nátlak s technickými prostředky. Z pohledu českého práva se tak nejedná o jeden samostatný problém, ale o situaci, která zasahuje do několika zákonů současně. Pro kompletní analýzu tohoto tématu je proto nutné sledovat tři základní právní roviny.

Základem je trestní zákoník (zákon č. 40/2009 Sb.), který definuje vinu pachatele a sazby trestů. Důležitý je také zákon o platebním styku (zákon č. 370/2017 Sb.), protože upravuje vztah mezi podvedeným klientem a bankou v otázce odpovědnosti za škodu. Poslední částí tohoto právního rámce je zákon o opatřeních proti legalizaci výnosů (zákon č. 253/2008 Sb.), který řeší kontrolu podezřelých plateb a identifikaci osob. Právě souhra těchto předpisů určuje, jak stát na moderní podvody reaguje.

6.1 Trestní zákoník (Zákon č. 40/2009 Sb.)

Trestní zákoník je v českém právním řádu hlavním nástrojem, podle kterého policie a soudy určují vinu a výši trestu pro pachatele online podvodů. U investičních schémat se v praxi téměř nikdy nejedná o porušení pouze jednoho paragrafu. Útočníci totiž kombinují lhaní, technické nabourání do soukromí i následné zakrývání stop, což vede k takzvanému souběhu několika trestných činů najednou. Z pohledu kriminalistiky lze tento proces rozdělit na tři klíčové oblasti.[62]

6.1.1 Podvod (§ 209)

Tento paragraf tvoří základní kámen pro stíhání investičních podvodů. K jeho naplnění dochází ve chvíli, kdy útočník vědomě uvádí oběť v omyl ohledně budoucích zisků s cílem obohatit sebe nebo jinou osobu na úkor cizího majetku.[63]

U online investic jde typicky o slibování nereálného zhodnocení peněz, které má oběť motivovat k první platbě. Z právního hlediska je zde klíčová výše způsobené škody. Protože u těchto podvodů lidé často přicházejí o částky vyšší než jeden milion korun, hrozí pachatelům výrazně přísnější trestní sazby[64].

[62] ZÁKONY PRO LIDI. Online. Zákon č. 40/2009 Sb. 2009. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40. [cit. 2026-03-19].
[63] ZÁKONY PRO LIDI. Online. Zákon č. 40/2009 Sb. 2009. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40. [cit. 2026-03-19].
[64] ZÁKONY PRO LIDI. Online. Zákon č. 40/2009 Sb. 2009. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40. [cit. 2026-03-19].

6.1.2 Neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému nebo nosiče informací (§ 230)

Zatímco podvod řeší lhaní, tento paragraf se zaměřuje na technické napadení zařízení. U investičních podvodů k jeho naplnění dochází ve chvíli, kdy útočník přiměje oběť k instalaci softwaru pro vzdálený přístup, jako je AnyDesk nebo TeamViewer.[65]

V momentě, kdy pachatel získá nad zařízením kontrolu a začne v něm bez vědomí majitele provádět operace například zadávat platby v internetovém bankovnictví, dochází k neoprávněnému průniku do systému. Tento paragraf je v práci klíčový, protože ukazuje, že útočník neničí jen finance oběti, ale hrubě zasahuje i do jejího digitálního soukromí a bezpečnosti dat.[66]

6.1.3 Legalizace výnosů z trestné činnosti (§ 216)

Tento paragraf řeší snahu pachatelů zakrýt nelegální původ ukradených financí. U investičních podvodů je tato fáze klíčová pro bezpečné vyvedení peněz mimo dosah policie.[67]

K naplnění zákona dochází využíváním sítě tzv. bílých koňů. Jde o prostředníky, kteří poskytují své účty k přeposílání ukradených částek, čímž se snaží zamést stopy mezi útočníkem a obětí. Z právního hlediska je důležité, že stíhán může být i samotný „bílý kůň“, pokud o nelegálním původu peněz věděl, nebo mu to vzhledem k okolnostem mělo být jasné.[68]

6.2 Zákon o platebním styku (č. 370/2017 Sb.)

Tento zákon je klíčový pro vztah mezi podvedeným klientem a jeho bankou. Určuje totiž pravidla pro to, kdy je banka povinna ukradené peníze vrátit a kdy za škodu

[65] ZÁKONY PRO LIDI. Online. Zákon č. 40/2009 Sb. 2009. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40. [cit. 2026-03-19].
[66] ZÁKONY PRO LIDI. Online. Zákon č. 40/2009 Sb. 2009. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40. [cit. 2026-03-19].
[67] ZÁKONY PRO LIDI. Online. Zákon č. 40/2009 Sb. 2009. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40. [cit. 2026-03-19].
[68] ZÁKONY PRO LIDI. Online. Zákon č. 40/2009 Sb. 2009. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40. [cit. 2026-03-19].

odpovídá sám klient. U investičních podvodů, kde hraje roli AnyDesk, je největším problémem pojem „hrubá nedbalost“.[69]

Podle zákona má uživatel povinnost chránit své bezpečnostní prvky, jako jsou hesla a potvrzovací kódy. V momentě, kdy klient dobrovolně nainstaluje software pro vzdálený přístup, dává útočníkovi kontrolu nad svým zařízením i bankovnictvím. Banky takové jednání zpravidla klasifikují jako hrubé porušení bezpečnostních povinností, což jim umožňuje odmítnout odpovědnost za vzniklou škodu. V takovém případě banka za ztrátu neodpovídá a klient nese škodu v plné výši. Právní spory se zde vedou především o to, zda byl útok natolik propracovaný, že jej průměrný uživatel nemohl rozpoznat.[70]

6.3 Zákon o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu (č. 253/2008 Sb.)

Tento zákon, v praxi běžně označovaný jako AML zákon, představuje preventivní rovinu ochrany finančního systému. Jeho hlavním cílem je ztížit podvodníkům cestu k ukradeným penězům a jejich následné „vyprání“. Pro téma investičních podvodů jsou v tomto právním rámci klíčové především mechanismy identifikace klienta a hlášení podezřelých obchodů.[71]

Banky a kryptoměnové burzy mají zákonnou povinnost prověřovat své klienty a sledovat neobvyklé transakce. Pokud systém banky vyhodnotí platbu jako rizikovou – například náhlý převod vysoké částky na zahraniční burzu u klienta, který takové operace nikdy nedělal – může platbu pozastavit a nahlásit ji Finančnímu analytickému úřadu (FAÚ). Tento zákon je tedy nástrojem, který se snaží podvod zastavit dříve, než peníze definitivně opustí kontrolovaný bankovní prostor a zmizí v anonymitě[72]

[69] ZÁKONY PRO LIDI. Online. Zákon č. 370/2017 Sb. 2017. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-370. [cit. 2026-03-19].
[70] ZÁKONY PRO LIDI. Online. Zákon č. 370/2017 Sb. 2017. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-370. [cit. 2026-03-19].
[71] ZÁKONY PRO LIDI. Online. Zákon č. 253/2008 Sb. 2008. Dostupné z: https://www.zakonyprolidi.cz/cs/2008-253. [cit. 2026-03-19].
[72] ZÁKONY PRO LIDI. Online. Zákon č. 253/2008 Sb. 2008. Dostupné z: https://www.zakonyprolidi.cz/cs/2008-253. [cit. 2026-03-19].

7 Prevence a ochrana před investičními podvody

Vzhledem k rostoucí sofistikovanosti kybernetických útoků a neustálému vývoji nových metod sociálního inženýrství se prevence stává nejdůležitějším prvkem ochrany před investičními podvody v kyberprostoru. Efektivní obrana v tomto prostředí vyžaduje komplexní přístup, který nespoléhá pouze na automatizované systémy finančních institucí, ale klade důraz na aktivní roli samotného uživatele, protože právě on je ten nejslabší článek v celém systému. Útočníci totiž neútočí na neprostupná softwarová zabezpečení, ale na lidské emoce, nepozornost a důvěřivost.[73]

7.1 Aktivní prvky zabezpečení v kyberprostoru

Bezpečnost v online prostředí začíná u nastavení základních bariér, které útočníkům zkomplikují přístup k citlivým údajům uživatele. V případě investičních podvodů útočníci velmi často využívají právě podcenění základních bezpečnostních prvků ze strany uživatele. Je proto nutné, aby uživatel spoléhal i na vlastní ochranu a využíval dostupné technické nástroje, než aby pouze spoléhal na ochranu ze strany banky.[74]

7.1.1 Zásady bezpečného používání hesel

Kvalita hesel představuje první úroveň technické ochrany uživatele na internetu. Pro efektivní zabezpečení je v současné době vyžadováno používání silných hesel, které mají minimální délku 12 znaků u běžných uživatelů a 17 znaků u administrátorů. Kombinují se zde velká a malá písmena, číslice a speciální znaky. Základní chybou uživatele je, že používá více stejných hesel pro několik různých služeb najednou, například e-mail, sociální sítě a internetové bankovnictví.[75]

Pokud by totiž došlo k úniku hesel z nějakého méně zabezpečeného portálu, například e-shopu, útočníci mohou získané údaje poté automaticky zkoušet zadávat i do systému finančních institucí. Jako efektivní nástroje ochrany se proto nejvíce využívají správce hesel. Tyto programy umožní generovat a bezpečně uchovávat unikátní a velmi

[73] *ESET*. Online. Kybertest. Dostupné z: https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/kybertest-falesne-stranky-internetoveho-bankovnictvi-cesi-s-jistotou-nepoznaji-podvodne-sms-u-nich/. [cit. 2026-03-04].

[74] *ESET*. Online. Kybertest. Dostupné z: https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/kybertest-falesne-stranky-internetoveho-bankovnictvi-cesi-s-jistotou-nepoznaji-podvodne-sms-u-nich/. [cit. 2026-03-04].

[75] KOLOUCH, Jan a BAŠTA A KOL., Pavel. In: *CyberSecurity*. Praha: CZ.NIC, z. s. p. o, 2019, S. 285-286. ISBN 978-80-88168-34-8.

složitá hesla pro každou službu zvlášť, aniž by si je musel uživatel zapamatovat. Tímto krokem se výrazně sníží riziko, že by útočník odhalil heslo oběti.[76]

7.1.2 Dvoufázové ověření a mobilní klíče

Samotné heslo k ochraně financí v dnešní době nestačí, protože se dá velice snadno ukrást za pomocí phishingu. Proto je standardem dvoufázové ověření. Zatímco správce hesel slouží k bezpečné správě přihlašovacích údajů, mobilní klíče fungují jako druhý nezávislý stupeň ochrany. Správce hesel řeší první krok, kterým je ověření identity uživatele při vstupu do systému, ale mobilní klíč slouží až k finálnímu potvrzení konkrétní platby nebo operace. Tato technologie využívá biometrické prvky, jako je otisk prstu nebo sken obličeje, což je mnohem bezpečnější než SMS kódy, které dokážou útočníci odchytit nebo přemluvit oběť k jejich přeposlaní.[77]

Velkým rizikem může být v této souvislosti metoda, která spoléhá na nepozornost nebo vyčerpání uživatele. Útočník schválně posílá jednu potvrzovací notifikaci za druhou a čeká na moment, kdy to oběť ze zvyku v rychlosti potvrdí, jen aby se takových upozornění mohla zbavit. Právě v tom spočívá nebezpečí. Mobilní klíč je v podstatě digitální podpis každého uživatele a jeho potvrzení dává útočníkovi plnou moc nad transakcí. Základním pravidlem je striktní potvrzování pouze těch operací, které uživatel sám inicioval. I kdyby útočník znal heslo k účtu, stejně by se bez potvrzení na mobilu do systému nedostal.[78]

7.1.3 Kybernetické pojištění a asistenční služby

Dalším prvkem ochrany který se v poslední době stále více prosazuje, je sjednání kybernetického pojištění. Samotný pojistný produkt sice nepředstavuje přímou technickou bariéru proti útoku, slouží však jako účinný nástroj pro zmírnění finančních dopadů v případech, kdy dojde k lidské chybě. Pojišťovny dnes v rámci těchto služeb nabízejí nejen náhradu ukradených peněz, ale také pomoc odborníků při zablokování účtů

[76] ŠTRÁFELDA, Jan. *Heslo*. Online. Jan Štráfelda. Dostupné z: https://www.strafelda.cz/heslo. [cit. 2026-03-04].
[77] IT NETWORK. Online. Lekce 6 - Bezpečné přihlašování – 2FA a vícefaktorové ověřování. Dostupné z: https://www.itnetwork.cz/bezpecnost/bezpecne-prihlasovani-2fa-a-vicefaktorove-overovani. [cit. 2026-03-04].
[78] IT NETWORK. Online. Lekce 6 - Bezpečné přihlašování – 2FA a vícefaktorové ověřování. Dostupné z: https://www.itnetwork.cz/bezpecnost/bezpecne-prihlasovani-2fa-a-vicefaktorove-overovani. [cit. 2026-03-04].

nebo právní poradenství. Pojištění tak funguje jako pojistka, která sice útoku nezabrání, ale výrazně pomůže s následným řešením vzniklé škody. [79]

Pojišťovna v rámci asistenčních služeb zajišťuje například pomoc IT specialistů, kteří prověří koncová zařízení a odstraní případný škodlivý software nebo viry, které tam útočníci mohli zanechat. Součástí pojistného krytí bývá také právní pomoc a asistence při komunikaci s bankovními institucemi či policií, což poškozenému výrazně ulehčuje následné procesy po zjištění incidentu. [80]

7.2 Preventivní opatření při využívání vzdáleného přístupu

Klíčovým pravidlem bezpečnosti je nikdy neposkytovat přístupové údaje k aplikacím jako AnyDesk nebo TeamViewer osobám, které uživatel sám nekontaktoval na základě nějakého požadavku. Legitimní instituce, jako jsou banky nebo technická podpora velkých technologických firem, nikdy nevyžadují instalaci softwaru pro vzdálené ovládání zařízení za účelem „záchrany peněz“ nebo „opravy napadeného účtu“. Pokud se stane, že by osoba na druhém konci požadovala nainstalování a přístup k těmto aplikacím, je nejlepší věc okamžité ukončení hovoru.[81]

Jedna z dalších vrstev ochrany představuje správné nastavení samotného zařízení. Doporučuje se mít funkci vzdálené plochy v operačním systému standardně vypnutou a aktivovat ji pouze v případech, kdy je zásah prováděn pod dohledem důvěryhodného odborníka. V rámci prevence je také nutné sledovat, co si do svého zařízení stahujete a instalovat aplikace pouze z oficiálních ověřených zdrojů. Poslední vrstvu této ochrany pak tvoří správné nastavení samotné aplikace, a to konkrétně manuální potvrzování každého pokusu o připojení přímo na displeji zařízení. Tímto krokem získá uživatel absolutní kontrolu nad tím, co se na jeho zařízení děje.[82]

7.3 Antivirová ochrana a aktualizace softwaru

Posledním důležitým krokem pro ochranu je to, v jakém stavu má uživatel svůj mobilní telefon nebo počítač. Útočníci se totiž neustále snaží najít chyby v operačních systémech, přes které by se do zařízení dostali, i když uživatel neudělá žádnou chybu.

[79] ČSOB POJISTOVNA. Online. Pojištění kybernetických rizik. Dostupné z: https://www.csobpoj.cz/pojisteni/podnikatele-firmy/pojisteni-kybernetickych-rizik. [cit. 2026-03-04].
[80] ČSOB POJISTOVNA. Online. Pojištění kybernetických rizik. Dostupné z: https://www.csobpoj.cz/pojisteni/podnikatele-firmy/pojisteni-kybernetickych-rizik. [cit. 2026-03-04].
[81] POLICIE ČESKÉ REPUBLIKY. Online. AnyDesk je host, který se nezouvá!. Dostupné z: https://policie.gov.cz/clanek/anydesk-je-host-ktery-se-nezouva.aspx. [cit. 2026-03-04].
[82] POLICIE ČESKÉ REPUBLIKY. Online. AnyDesk je host, který se nezouvá!. Dostupné z: https://policie.gov.cz/clanek/anydesk-je-host-ktery-se-nezouva.aspx. [cit. 2026-03-04].

Proto je naprosto zásadní pravidelně instalovat všechny aktualizace, které systém nabízí. Tyto aktualizace nejsou pouze o vizuální stránce, ale také opravují kritické zranitelnosti v systému, kterými by mohl do zařízení proniknout virus nebo podvodná aplikace. [83]

Důležitou roli hraje i antivirový program. Ten dnes neřeší jen klasické viry, ale v reálném čase hlídá, zda se nějaká aplikace na zařízení nechová podezřele a nebo jestli se uživatel nesnaží přihlásit na falešnou stránku banky. Častou chybou uživatelů však je, že na tuto technickou ochranu až moc spoléhají a ztrácejí ostražitost. Značná část uživatelů podceňuje riziko sociálního inženýrství, kdy ani pokročilé technické zabezpečení nedokáže zabránit útoku, pokud dojde k dobrovolnému předání přístupových údajů. Lidský faktor a kritický úsudek uživatele tak zůstávají nejdůležitějším článkem celého řetězce prevence.[84]

[83] MCCARTHY, Linda a WELDON-SIVIY, Denise. In: *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online*. Praha: CZ.NIC, [2013], S. 33-35. ISBN 978-80-904248-6-9.
[84] MCCARTHY, Linda a WELDON-SIVIY, Denise. In: *Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online*. Praha: CZ.NIC, [2013], S. 33-35. ISBN 978-80-904248-6-9.

8 Vyhodnocení dotazníkového šetření k investičním podvodům

Praktická část bakalářské práce vychází z vlastního dotazníkového šetření, které bylo realizováno s cílem analyzovat úroveň povědomí o investičních podvodech. Hlavním záměrem bylo zjistit, jak oslovení respondenti přistupují k vlastní bezpečnosti v digitálním prostředí, jak reagují na podezřelé nabídky a zda jsou seznámeni se základními pojmy z oblasti kybernetické bezpečnosti, jako je například phishing.

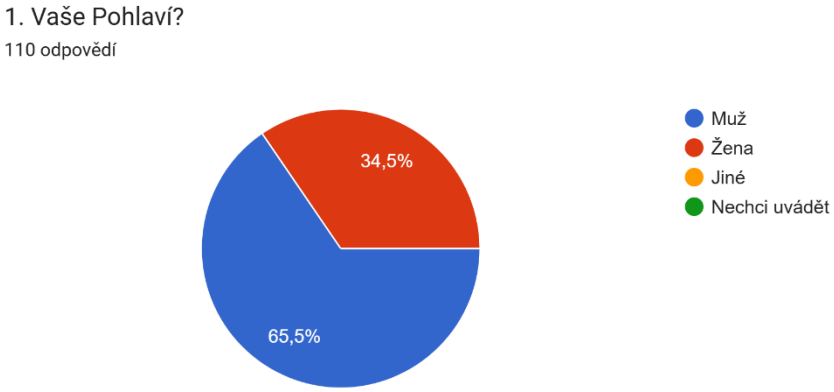
Dotazník byl distribuován v online formě jako anonymní šetření a celkem bylo získáno 110 plnohodnotných odpovědí. Odpovědi těchto respondentů tvoří základ pro následující vyhodnocení. Struktura otázek byla navržena tak, aby mapovala cestu respondentů od základních demografických údajů a technického vybavení přes jejich konkrétní znalosti rizik až po reálné zkušenosti s podvodným jednáním v online prostoru.

Celý výzkum se skládá z 20 otázek zaměřených na klíčové oblasti digitální bezpečnosti. Sleduje se v nich nejen subjektivní pocit informovanosti respondentů, ale také jejich praktické návyky při ověřování investičních platforem a reakce na nevyžádanou komunikaci. Závěrečná část dotazníku se věnuje oblasti prevence a zjišťuje, jaká opatření považují respondenti za nejúčinnější a kterým zdrojům informací důvěřují nejvíce. Data získaná od 110 respondentů jsou v následující části kapitoly znázorněna v grafech a doplněna o stručný komentář s výsledky.

Otázka č. 1

První otázka se zaměřovala na pohlaví respondentů. Největší podíl tvořili muži, kterých bylo celkem 72 (65,5 %). Ženy byly zastoupeny v počtu 38 respondentů (34,5 %) z celkového počtu odevzdaných dotazníků.

Graf 1 Pohlavní respondentů[85]

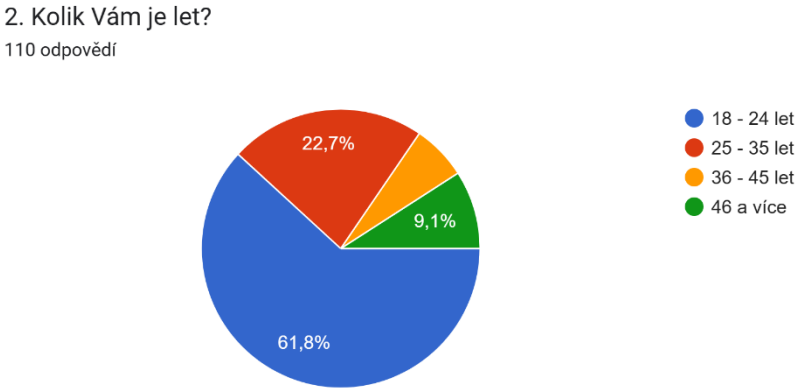


Otázka č. 2

Druhá otázka se zaměřovala na věkové rozložení respondentů. Cílem bylo zjistit, do jakých věkových kategorií se řadí osoby, které na dotazník odpovídaly, a získat tak přehled o zastoupení jednotlivých generací v rámci celého souboru. Z výsledků je patrné, že nejpočetnější skupinu tvoří respondenti ve věku 18–24 let, kterých bylo celkem 68 (61,8 %). Druhou nejzastoupenější kategorií jsou respondenti ve věku 25–35 let v počtu 25 (22,7 %). Skupina respondentů starších 46 let byla zastoupena 10 respondenty (9,1 %) a nejméně početnou skupinu tvořili lidé ve věku 36–45 let, kterých bylo 7 (6,4 %). Tato data potvrzují, že dotazník oslovil primárně mladší generaci uživatelů internetu, která je v online prostředí nejaktivnější.

[85] Vlastní zpracování

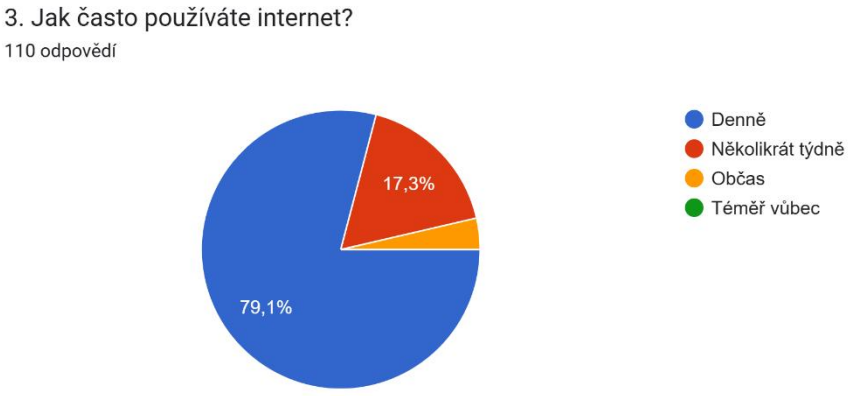
Graf 2 Věk respondentů[86]



Otázka č. 3

Tato otázka zjišťovala, jak často se respondenti pohybují v online prostředí. Častější využívání internetu totiž přirozeně zvyšuje šanci, že respondenti narazí na podvodnou reklamu nebo nabídku. Z výsledků je patrné, že internet denně využívá naprostá většina dotázaných, konkrétně 87 (79,1 %) respondentů. Dalších 19 (17,3 %) respondentů uvedlo, že jsou online několikrát týdně, a pouze 4 (3,6 %) respondenti se k internetu připojují pouze občas. Z dat tedy vyplývá, že téměř všichni respondenti jsou v online prostoru aktivní pravidelně.

Graf 3 Frekvence využívání internetu u respondentů[87]

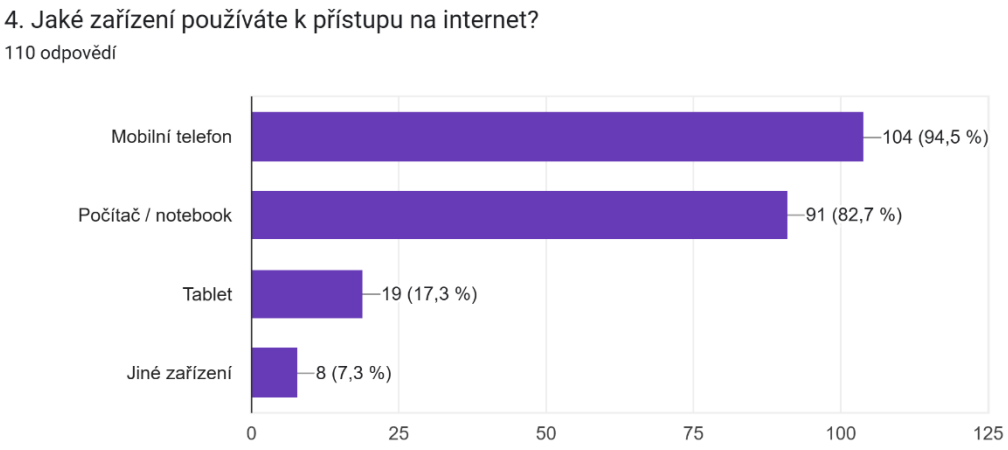


[86] Vlastní zpracování
[87] Vlastní zpracování

Otázka č. 4

Čtvrtá otázka zjišťovala, jakou techniku používají respondenti k připojení na internet. Typ zařízení je důležitý, protože podvodné reklamy nebo falešné aplikace se na každém zařízení mohou zobrazovat úplně odlišně. V této otázce měli respondenti možnost vybrat více odpovědí současně. Z výsledků je patrné, že naprostá většina, konkrétně 104 (94,5 %) respondentů, využívá k přístupu mobilní telefon. Velmi silně je zde zastoupen také počítač nebo notebook, který uvedlo 91 (82,7 %) respondentů. Tablet používá 19 (17,3 %) respondentů a jiné zařízení uvedlo 8 (7,3 %) respondentů. Je tedy zřejmé, že respondenti k přístupu na internet techniku kombinují, ale mobilní telefon s počítačem / notebookem zde jasně dominuje.

Graf 4 Zařízení využívaná respondenty k přístupu na internet[88]

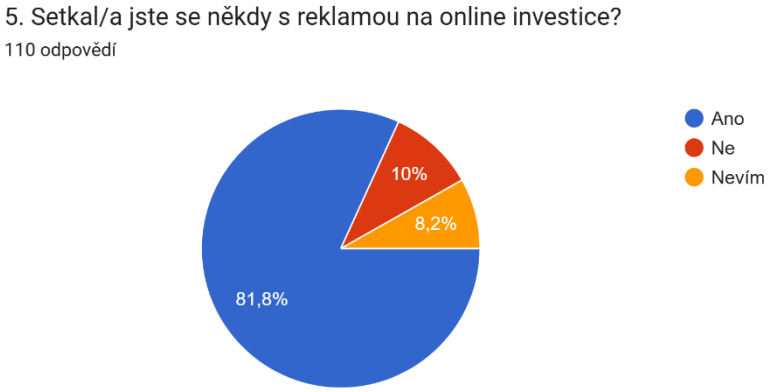


Otázka č. 5

V páté otázce se zjišťovalo, zda mají respondenti s reklamou na online investice osobní zkušenost. Tato otázka měla ověřit, jak často se tyto nabídky v online prostoru objevují. Z grafu vyplývá, že většina, konkrétně 90 (81,8 %) respondentů, se s takovou reklamou již setkala. Záporně odpovědělo 11 (10 %) respondentů a zbývajících 9 (8,2 %) respondentů zvolilo možnost, že neví, zda se s takovou formou někdy setkali. Z výsledků je tedy zřejmé, že naprostá většina respondentů těmto nabídkám v digitálním prostředí běžně čelí a nejedná se pouze o ojedinělé případy.

[88] Vlastní zpracování

Graf 5 Výskyt reklamy na online investice u respondentů[89]



Otázka č. 6

Šestá otázka navazovala na předchozí zjištění a zaměřovala se na to, zda respondenti na zobrazenou investiční reklamu reálně klikli. Tato otázka pomáhá určit míru interakce respondentů s tímto problémem. Celkem 68 (61,8 %) respondentů uvedlo, že na takový odkaz nikdy neklikli. Dalších 22 (20 %) respondentů již v minulosti na takový odkaz kliklo a zbývajících 20 (18,2 %) respondentů uvedlo, že si tuto skutečnost nepamatuje. Z výsledků tedy vyplývá, že i přes vysokou míru zobrazování těchto reklam na ně většina respondentů nekliká. Pětina respondentů na tyto nabídky aktivně zareagovala, což představuje skupinu, která může být více ohrožena investičními podvody.

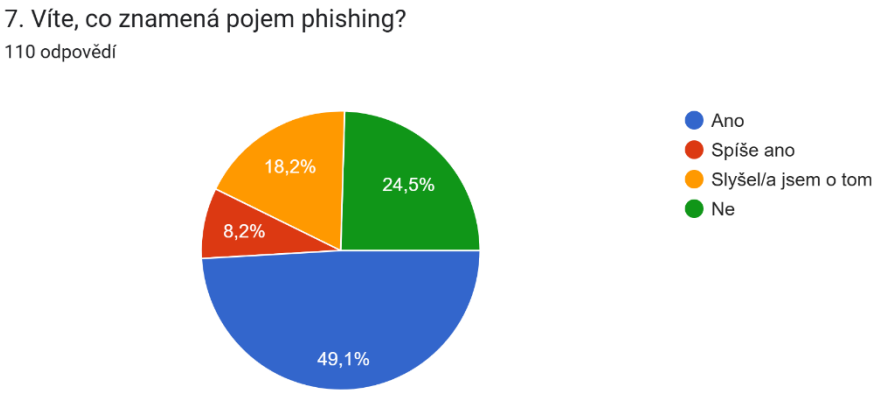
[89] Vlastní zpracování

Graf 6 Reakce respondentů na investiční reklamu na sociálních sítích[90]

Otázka č. 7

V sedmé otázce se zjišťovalo, zda respondenti znají pojem phishing. Tento termín je důležitý, protože se s ním v rámci online podvodů často pracuje. Z výsledků grafu je zřejmé, že největší skupinu tvoří 54 (49,1 %) respondentů, kteří tento pojem znají. Celkem 27 (24,5 %) respondentů uvedlo, že vůbec neví, co tento pojem znamená, a dalších 20 (18,2 %) respondentů o něm už někdy slyšelo. Nejméně početnou skupinu tvoří 9 (8,2 %) respondentů, kteří zvolili možnost „Spíše ano“. Ukazuje se tedy, že i když polovina respondentů ví, o co jde, zbývající část má o této hrozbě jen malé nebo žádné povědomí, což z nich může dělat snadnější cíle pro různé online podvody

Graf 7 Znalost pojmu phishing u respondentů[91]

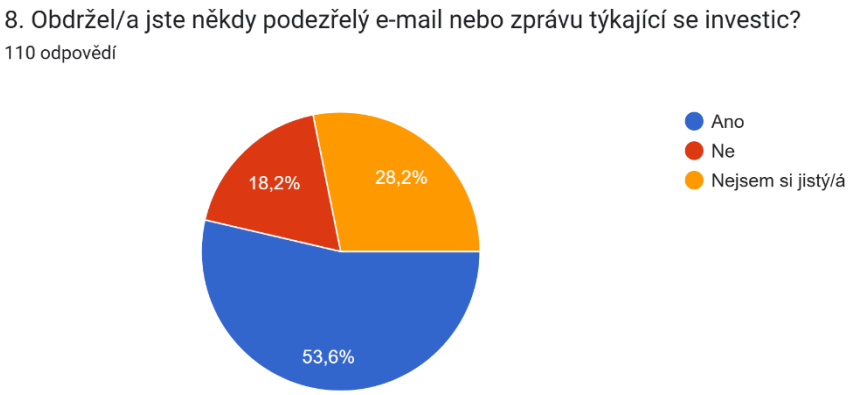


[90] Vlastní zpracování
[91] Vlastní zpracování

Otázka č. 8

Další otázka v dotazníku zjišťovala, zda se respondenti setkávají s podvodnými nabídkami i přímo ve svých soukromých zprávách nebo e-mailových schránkách. To ukazuje na šíření investičních podvodů i mimo veřejné sociální sítě. Z nasbíraných odpovědí vyplývá, že největší část, konkrétně 59 (53,6 %) respondentů, již nějakou podezřelou zprávu ohledně investic obdržela. Celkem 31 (28,2 %) respondentů uvedlo, že si touto skutečností nejsou jisti. Nejméně početnou skupinu tvoří 20 (18,2 %) respondentů, kteří s tímto jevem nemají žádnou zkušenost. Poměrně vysoký počet nerozhodných respondentů může naznačovat, že rozpoznat podvodnou zprávu od té legitimní není v soukromé komunikaci vždy snadné.

Graf 8 Zkušenost respondentů s podezřelými zprávami o investicích[92]

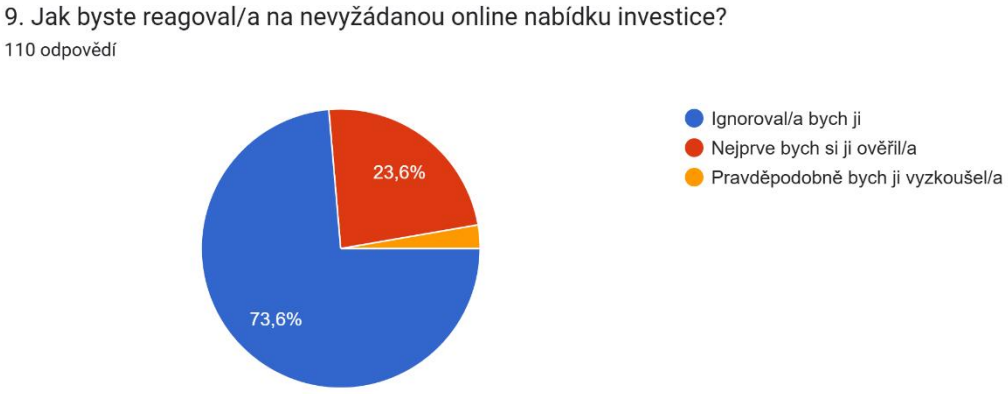


Otázka č. 9

Devátá otázka zjišťovala reakci respondentů na nevyžádané investiční nabídky. Cílem bylo zjistit, jaká je míra obezřetnosti u dotázaných v případě, že jsou přímo osloveni s touto nabídkou. Celkem 81 (73,6 %) respondentů uvedlo, že by takovou nabídku ignorovalo. Dalších 26 (23,6 %) respondentů by si nabídku nejprve ověřilo a pouze malá část, konkrétně 3 (2,7 %) respondentů, by ji pravděpodobně vyzkoušela. Data potvrzují, že i když se s těmito nabídkami setkává velké množství lidí, většina k nim přistupuje s nedůvěrou a uvědomuje si možná rizika.

[92] Vlastní zpracování

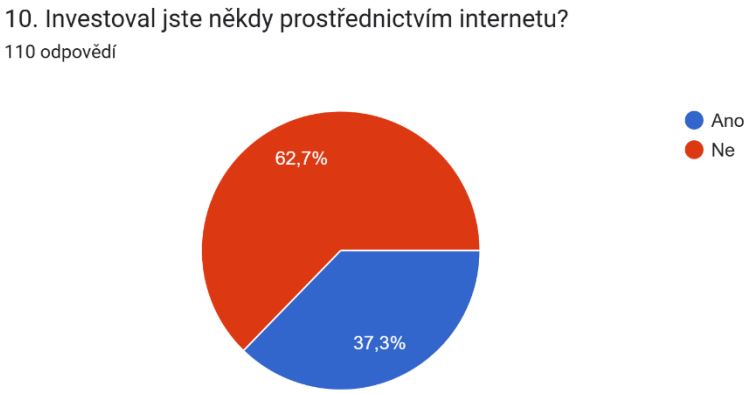
Graf 9 Postoj respondentů k nevyžádaným investičním nabídkám[93]



Otázka č. 10

Cílem desáté otázky bylo zjistit, kolik respondentů má s online investováním reálnou zkušenost. Tyto údaje pomáhají zjistit, jak velká část dotázaných se v tomto prostředí skutečně pohybuje. Z nasbíraných dat vyplývá, že zkušenost s online investicemi má méně než polovina respondentů. Kladně odpovědělo 41 (37,3 %) respondentů, zatímco většinu tvoří skupina 69 (62,7 %) respondentů, která přes internet nikdy neinvestovala. Z výsledků je patrné, že i když se respondenti s nabídkami investic setkávají běžně, k samotnému investování se odhodlá jen menší část z nich. To může naznačovat to, že jsou respondenti vůči těmto nabídkám spíše opatrní.

Graf 10 Zkušenost respondentů s online investováním[94]

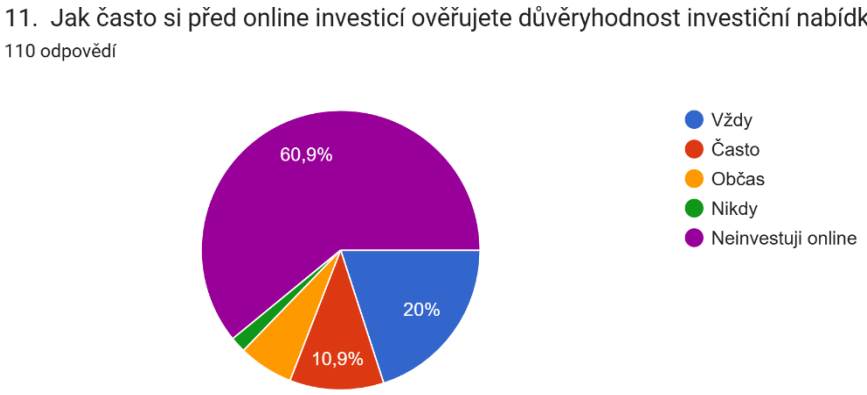


[93] Vlastní zpracování
[94] Vlastní zpracování

Otázka č. 11

Jedenáctá otázka zjišťovala, jak zodpovědně respondenti přistupují k samotnému investování a zda si ověřují, komu své peníze skutečně posílají. Tato data jsou klíčová pro posouzení rizikového chování této skupiny. Z grafu je na první pohled vidět, že největší skupinu tvoří 67 (60,9 %) respondentů, kteří online vůbec neinvestují. Pokud se však zaměříme na tu skupinu, která investiční platformy využívá, tak 22 (20 %) respondentů si nabídku ověřuje vždy a 12 (10,9 %) respondentů tak činí často. Celkem 7 (6,4 %) respondentů si informace ověřuje pouze občas a 2 (1,8 %) respondenti uvedli, že si důvěryhodnost neověřují nikdy. Výsledky tedy ukazují, že i mezi aktivními investory existuje část respondentů, která se kvůli nedostatečnému ověřování může snadno stát obětí podvodu.

Graf 11 Míra ověřování investičních nabídek respondenty[95]



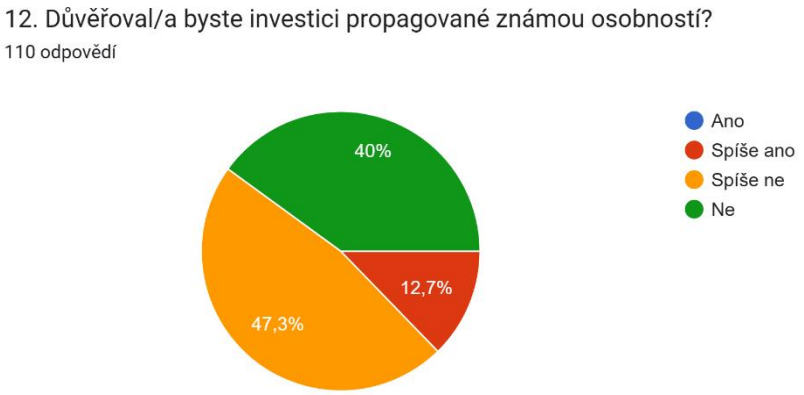
Otázka č. 12

Dvanáctá otázka se zaměřila na vliv známých osobností na rozhodování respondentů. Podvodníci často zneužívají tváře celebrit k tomu, aby u lidí vzbudili falešný pocit důvěry a profesionality nabízené investice. Z odpovědí je patrné, že většina respondentů tomuto typu propagace nepodlehne. Nejpočetnější skupina, konkrétně 52 (47,3 %) respondentů, se přiklání k odpovědi „Spíše ne“ a dalších 44 (40 %) respondentů zvolilo jednoznačnou možnost „Ne“. Naopak 14 (12,7 %) respondentů uvedlo, že by takové investici spíše důvěřovalo. Přestože drtivá většina dotázaných vnímá přítomnost

[95] Vlastní zpracování

celebrity v reklamě skepticky, stále zde existuje necelých 13 % respondentů, kteří by mohli být tímto způsobem manipulace ovlivněni.

Graf 12 Důvěra respondentů v investice propagované známou osobností[96]

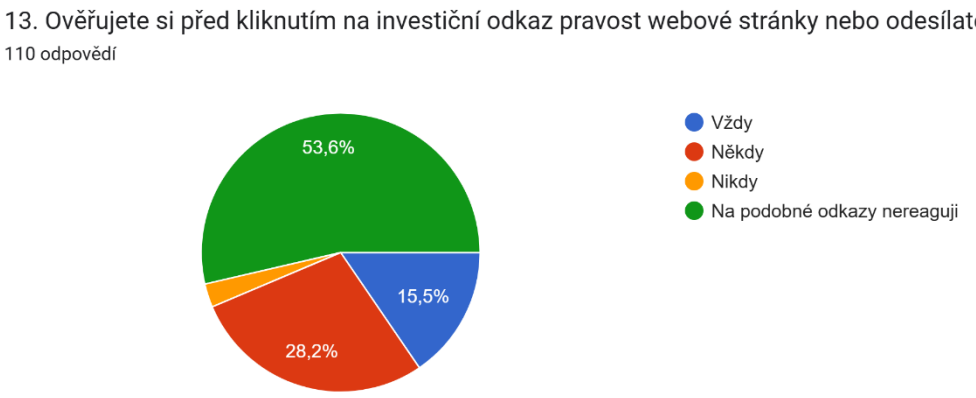


Otázka č. 13

Tato otázka zjišťovala, jak se respondenti chovají ve chvíli, kdy se setkají s konkrétním investičním odkazem. Z výsledků je patrné, že největší část, celkem 59 (53,6 %) respondentů, na podobné odkazy vůbec nereaguje, což představuje nejúčinnější formu obrany. Dalších 31 (28,2 %) respondentů si pravost odkazu ověřuje pouze někdy a 17 (15,5 %) respondentů tak činí vždy. Nejméně početnou skupinu tvoří 3 (2,7 %) respondenti, kteří uvedli, že si informace neprověřují nikdy. Z dat vyplývá, že většina respondentů volí cestu pasivní ochrany a na podezřelé odkazy vůbec nekliká. Pokud se však rozhodnou odkaz otevřít, ne všichni si už následně ověřují, zda je daná stránka nebo odesílatele skutečně pravý.

[96] Vlastní zpracování

Graf 13 Obezřetnost respondentů při otevírání investičních odkazů[97]

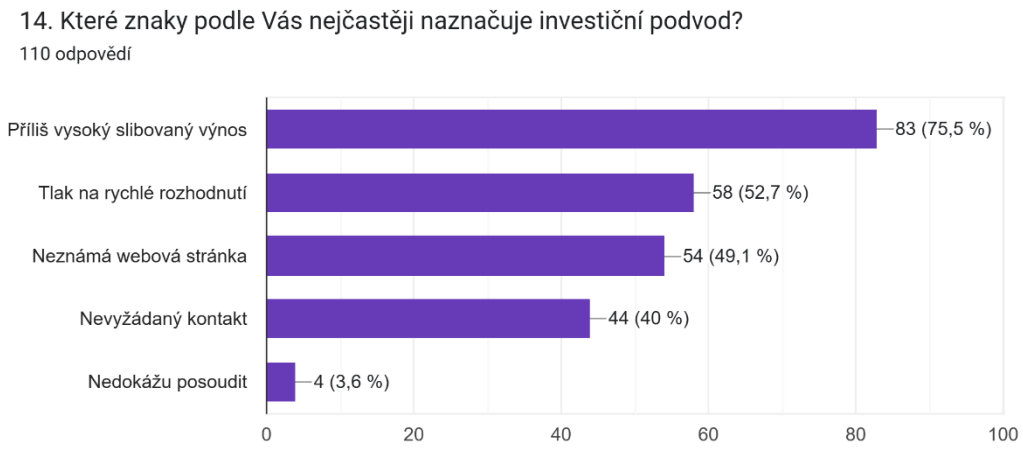


Otázka č. 14

Čtrnáctá otázka byla zaměřena na identifikaci rizikových faktorů, které respondenti považují za klíčové při rozpoznávání podvodných nabídek. Tato otázka umožňovala výběr více odpovědí. Graf jasně ukazuje, že nejčastěji identifikovaným znakem podvodu je pro 83 (75,5 %) respondentů příliš vysoký slibovaný výnos. Jako další významný varovný faktor vnímá 58 (52,7 %) respondentů tlak na rychlé rozhodnutí a 54 (49,1 %) respondentů označilo neznámou webovou stránku. Celkem 44 (40 %) respondentů považuje za varovný znak nevyžádaný kontakt. Pouze 4 (3,6 %) respondenti uvedli, že tyto znaky nedokážou posoudit. Data potvrzují, že většina respondentů si je vědoma základních znaků podvodného jednání, zejména v případech, kdy nabídka slibuje nereálné zhodnocení financí.

[97] Vlastní zpracování

Graf 14 Identifikace rizikových faktorů v investičních nabídkách[98]



Otázka č. 15

Patnáctá otázka zjišťovala, zda mají respondenti reálnou zkušenost s investičními podvody. Získaná data poskytují důležitý pohled na to, jak moc je tato hrozba v současnosti rozšířená v běžném životě respondentů. Z výsledků vyplývá, že největší skupinu tvoří 49 (44,5 %) respondentů, kteří se s investičním podvodem dosud nesetkali. Velmi významným zjištěním však je, že celkem 44 (40 %) respondentů o takovém podvodu ví ze svého blízkého okolí. Osobně se s tímto jevem setkalo 9 (8,2 %) respondentů a zbývajících 8 (7,3 %) respondentů uvedlo, že si touto skutečností nejsou jisti. Celkově to ukazuje, že skoro každý druhý respondent už na investiční podvod narazil, buď se do té situace dostal sám, nebo to musel řešit někdo z jeho okolí.

[98] Vlastní zpracování

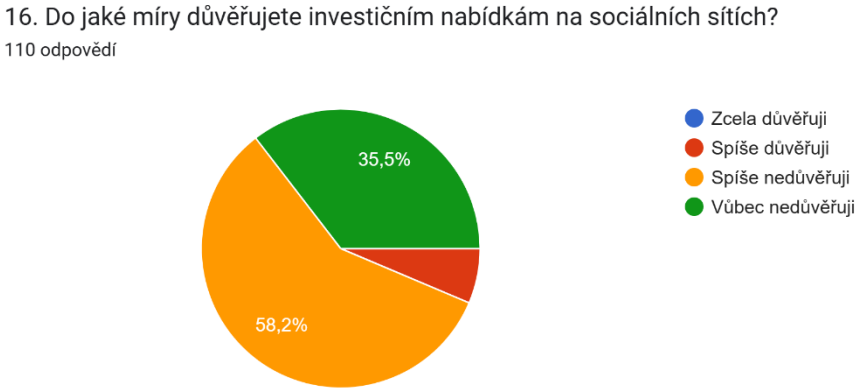
Graf 15 Osobní zkušenosti respondentů s investičním podvodem[99]

Otázka č. 16

Šestnáctá otázka dotazníku zkoumala důvěru respondentů k investicím, které jsou propagovány v prostředí sociálních sítí. Právě tyto platformy totiž podvodníci zneužívají k oslovování potenciálních obětí nejčastěji. Z odpovědí vyplývá, že respondenti jsou k takovým výzvám velmi skeptičtí. Největší skupina, celkem 64 (58,2 %) respondentů, zvolila možnost „Spíše nedůvěřuji" a dalších 39 (35,5 %) respondentů těmto nabídkám nevěří vůbec. Pouze 7 (6,4 %) respondentů vyjádřilo částečnou důvěru. Možnost „Zcela důvěřuji" nevybral žádný z respondentů. Výsledky tak potvrzují, že si naprostá většina respondentů uvědomuje rizika anonymity na internetu a k finančním nabídkám na sociálních sítích přistupuje s velkou rezervou.

[99] Vlastní zpracování

Graf 16 Míra důvěry respondentů v investiční nabídky na sociálních sítích[100]



Otázka č. 17

Tato otázka byla zaměřena na hodnocení účinnosti různých preventivních opatření. Respondenti měli možnost vybrat více odpovědí současně. Výsledky ukazují, že za nejvíce efektivní způsob prevence považuje 74 (67,3 %) respondentů varování od bank a jiných institucí. Druhým nejčastěji voleným opatřením je větší informovanost veřejnosti, kterou označilo 66 (60 %) respondentů. Významnou roli podle dotázaných hraje také vzdělávání v oblasti kybernetické bezpečnosti, které zvolilo 46 (41,8 %) respondentů, a zvýšená opatrnost při pohybu v online prostoru, kterou preferuje 44 (40 %) respondentů. Celkem 38 (34,5 %) respondentů zvolilo možnost vlastního vzdělávání v oblasti financí a přísnější regulaci reklamy na internetu vybralo 34 (30,9 %) respondentů. Pouze 2 (1,8 %) respondenti nedokázali účinnost opatření posoudit. Data ukazují, že respondenti spoléhají především na ochranu ze strany institucí a na celospolečenské vzdělávání.

[100] Vlastní zpracování

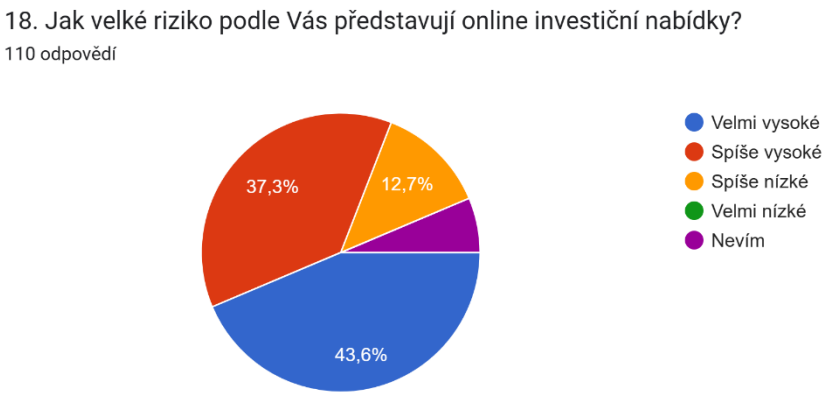
Graf 17 Hodnocení účinnosti preventivních opatření respondenty[101]

Otázka č. 18

Cílem této otázky bylo zjistit, jak respondenti vnímají nebezpečí spojené s investováním v online prostoru. Tato subjektivní reflexe je důležitá pro pochopení toho, nakolik jsou respondenti v digitálním prostředí obezřetní. Odpovědi ukazují, že naprostá většina dotázaných vnímá tyto nabídky jako hrozbu. Největší skupina, konkrétně 48 (43,6 %) respondentů, považuje toto riziko za velmi vysoké a dalších 41 (37,3 %) respondentů ho označilo za spíše vysoké. Celkově tak přes 80 % respondentů přistupuje k online investicím s velkou opatrností. Naopak jako spíše nízké vnímá riziko pouze 14 (12,7 %) respondentů a možnost velmi nízkého rizika nezvolil žádný z dotazovaných. Zbývajících 7 (6,4 %) respondentů nedokázalo situaci posoudit. Získaná data potvrzují, že online investiční nabídky jsou vnímány jako riziková oblast, což dává smysl i vzhledem k předchozím odpovědím o celkové nedůvěře k reklamám na sociálních sítích.

[101] Vlastní zpracování

Graf 18 Postoje respondentů k investičním podvodům[102]

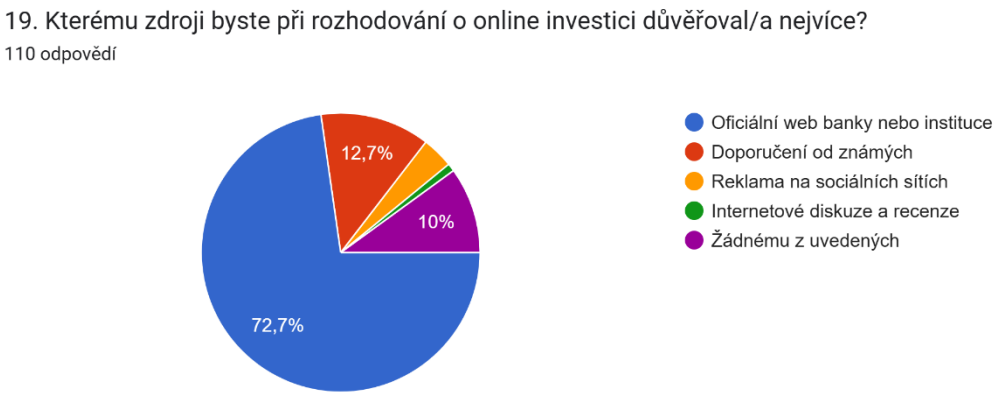


Otázka č. 19

Předposlední otázka zkoumala, kam by se respondenti obrátili pro důvěryhodné informace v případě, že by se rozhodovali o realizaci online investice. Identifikace důvěryhodných zdrojů je klíčová pro to, aby se člověk nenechal zmást falešnými recenzemi nebo komentáři u online investic. Většina, konkrétně 80 (72,7 %) respondentů, by nejvíce důvěřovala oficiálnímu webu banky nebo jiné finanční instituci. Dalších 14 (12,7 %) respondentů by se spoléhalo na doporučení od svých známých a celkem 11 (10 %) respondentů uvedlo, že by nedůvěřovalo žádnému z uvedených zdrojů. Reklamu na sociálních sítích zvolili pouze 4 (3,6 %) respondenti a internetové diskuse či recenze by využil pouze 1 (0,9 %) respondent. Tyto výsledky potvrzují, že respondenti v otázkách financí preferují autoritu zavedených institucí před neověřenými informacemi z internetu. Výsledky ukazují, že v otázkách financí respondenti spoléhají spíše na ověřené instituce než na anonymní zdroje z internetu.

[102] Vlastní zpracování

Graf 19 Důvěryhodnost informačních zdrojů o online investicích u respondentů[103]

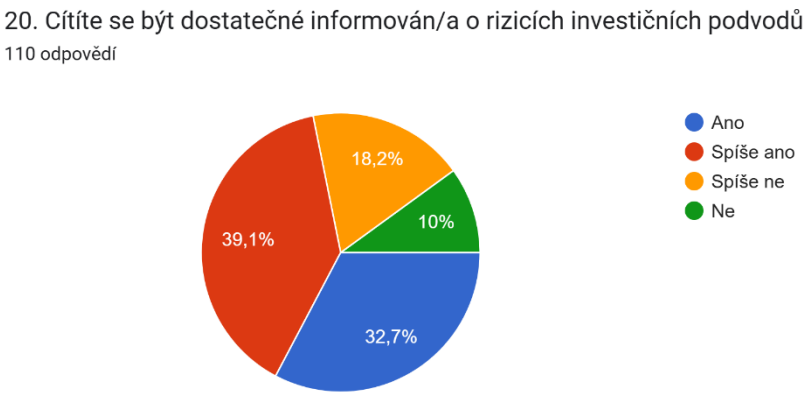


Otázka č. 20

Poslední otázka dotazníku se zaměřila na to, jak respondenti hodnotí svou informovanost o hrozbách spojených s online investicemi. Toto sebehodnocení ukazuje, nakolik si respondenti v online prostoru věří a zda dokážou rozpoznat hrozbu. Výsledky ukazují, že úroveň informovanosti je z pohledu respondentů vysoká. Největší část, celkem 43 (39,1 %) respondentů, se cítí být spíše informována. Dalších 36 (32,7 %) respondentů na otázku odpovědělo jednoznačně ano. To znamená, že více než 70 % respondentů vnímá své znalosti o online podvodech jako dostatečné. Opačný postoj vyjádřilo 20 (18,2 %) respondentů, kteří se cítí být spíše neinformováni, a zbývajících 11 (10 %) respondentů se cítí být neinformováno vůbec. I přes vědomí vysokého rizika, které online investice představují, tak většina respondentů ukazuje značnou důvěru ve své schopnosti rozeznat investiční podvody v online prostředí.

[103] Vlastní zpracování

Graf 20 Míra informovanosti respondentů o investičních podvodech[104]



8.1 Shrnutí výsledků dotazníkového šetření

Z provedeného dotazníkového šetření vyplývá, že respondenti jsou aktivními uživateli internetu, kteří využívají především mobilní telefony a počítače. Jelikož se jedná převážně o mladší generaci, která v dotazníku odpovídala, je jejich orientace v online prostředí na dobré úrovni. Většina respondentů se v minulosti již setkala s podezřelou zprávou nebo e-mailem, což u nich vyvolalo přirozenou opatrnost proti dalším podvodným aktivitám. I když polovina respondentů zná odborné pojmy jako phishing, stále existuje část, která si jejich přesným významem není jistá, ovšem i když respondenti mohou tyto pojmy znát, nezaručuje jim to hned tu nejlepší ochranu. Je důležité vyhodnocovat konkrétní situace, protože pouhá znalost názvu jednotlivých útoků zde nestačí.

Tato zkušenost se přímo promítá do jejich chování vůči investičním nabídkám. Respondenti nemají důvěru k reklamám na sociálních sítích a k investicím, které propagují známé osobnosti či celebrity. Za hlavní varovné signály podvodu považují především nátlak na rychlé rozhodnutí a přísliby nereálně vysokých zisků. Při ověřování informací se respondenti snaží chovat obezřetně a kontrolovat pravost odkazů, ale z výsledků je patrné, že v této oblasti přetrvávají určité nedostatky, které představují zvýšené bezpečnostní riziko. Právě když jsou uživatelé pod tlakem, může jejich obezřetnost při každodenním používání internetu snadno polevit.

V Otázkách týkající se financí a bezpečnosti se respondenti spoléhají téměř výhradně na autoritu bankovních institucí a jejich oficiální webové stránky. Jiné zdroje,

[104] Vlastní zpracování

jako jsou internetové diskuse nebo recenze, pro ně nemají žádnou váhu. V oblasti prevence pak respondenti očekávají aktivnější přístup od institucí, zejména formou včasných varování v bankovních aplikacích a celkového vzdělávání veřejnosti skrze média.

Výsledky šetření tedy potvrzují, že respondenti vnímají online investování jako vysoce rizikové a jsou si vědomi toho, že ani jejich znalosti nejsou neomylné. I přes snahu o individuální ostražitost zůstává pro respondenty klíčovým faktorem bezpečnosti podpora ze strany bank a oficiálních institucí. Celková ochrana uživatelů tak v praxi nezávisí pouze na teorii, ale především na kombinaci včasné informovanosti a důvěry v zavedené instituce.

Závěr

Cílem této bakalářské práce bylo provést analýzu investičních podvodů v online prostředí a na základě realizovaného šetření u respondentů posoudit jejich schopnost těmto hrozbám čelit. Práce se zaměřila na rozkrytí metod, kterými útočníci manipulují své oběti, a na vyhodnocení celkové úrovně digitální gramotnosti a ostražitosti veřejnosti v oblasti online investování.

V teoretické části byla nejprve vymezena problematika kybernetické kriminality s důrazem na psychologické techniky sociálního inženýrství. Byly rozebrány aktuální techniky, jako jsou klamavé reklamy zneužívající tváře známých osobností nebo budování sofistikovaných falešných investičních platforem. Důraz byl kladen také na právní rámec těchto podvodů v České republice a na klíčovou roli prevence, která představuje nejúčinnější způsob ochrany finančních prostředků v digitálním věku.

Praktická část práce byla založena na dotazníkovém šetření, které mapovalo reálné zkušenosti uživatelů s investičními podvody v online prostředí. Z odpovědí respondentů vyplynulo, že naprostá většina využívá internet na denní bázi, a to primárně prostřednictvím mobilních zařízení, přičemž se běžně setkávají s podvodnými nabídkami na internetu nebo skrze podezřelé e-maily. Ukázalo se, že zatímco většina respondentů přistupuje k pohybu v digitálním prostoru zodpovědně a dokázala by identifikovat prvotní varovné signály podvodu, úroveň znalostí se výrazně snižuje v okamžiku, kdy dojde na samotnou odbornou investiční terminologii. Zjištěné skutečnosti vedou k závěru, že technická ochrana samotná nestačí, pokud není podpořena kritickým myšlením a schopností včas identifikovat manipulativní strategie útočníků. Jako nejúčinnější způsob prevence a nápravy pak respondenti označili formy pravidelného varování ze strany bankovních institucí a celkového zvyšování informovanosti široké veřejnosti.

Na základě shromážděných poznatků lze konstatovat, že role vzdělávání a informovanosti je v boji proti online podvodům naprosto zásadní. Správně nastavená prevence může významně posílit odolnost společnosti vůči neustále se vyvíjejícím metodám útočníků.

Seznam použitých zdrojů

Literární zdroje

1. CIALDINI, Robert B. Nové zbraně vlivu. V Brně: Jan Melvil Publishing, 2023. 512 s. ISBN 978-80-7555-181-8.
2. DOVE, Martina. The psychology of fraud, persuasion and scam techniques: understanding what makes us vulnerable. New York: Routledge, 2025. 156 s. ISBN 978-1-003-59025-5.
3. GRIMES, Roger A. a JUST, John N. Fighting Phishing: everything you can do to fight social engineering and phishing. Indianapolis: John Wiley, 2024. 448 s. ISBN 9781394249220.
4. GŘIVNA, Tomáš; POLČÁK, Radim a UHLÍŘOVÁ, Kateřina. Kyberkriminalita a právo. Praha: Auditorium, 2008. 220 s. ISBN 978-80-903786-7-4.
5. HADNAGY, Christopher a FINCHER, Michele. Phishing Dark Waters. John Wiley & Sons, 2015. 192 s. ISBN 978-1-119-18362-4.
6. HOLT, Thomas J.; BOSSLER, Adam M. a SEIGFRIED-SPELLAR, Kathryn C. Cybercrime and digital forensics: an introduction. Second edition. London: Routledge, 2018. 741 s. ISBN 978-1-138-23872-5.
7. JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. Výkladový slovník kybernetické bezpečnosti. Páté doplněné a upravené vydání. Praha: Česká pobočka AFCEA, 2022. 352 s. ISBN 978-80-908388-4-0.
8. JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. 284 s. ISBN 978-80-247-1561-2.
9. KOLOUCH, Jan a BAŠTA A KOL., Pavel. CyberSecurity. Praha: CZ.NIC, z. s. p. o, 2019. 560 s. ISBN 978-80-88168-34-8.
10. KOLOUCH, Jan. CyberCrime. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. 528 s. ISBN 978-80-88168-18-8.
11. LIBICKY, Martin C. Conquest in Cyberspace: National Security and Information Warfare. Cambridge University Press, 2007. 323 s. ISBN 978-0-511-28535-6.
12. MCCARTHY, Linda a WELDON-SIVIY, Denise. Buď pánem svého prostoru: jak chránit sebe a své věci, když jste online. Praha: CZ.NIC, [2013]. 318 s. ISBN 978-80-904248-6-9.

13. SEDLÁK, Petr a KONEČNÝ, Martin. Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru. Brno: CERM, akademické nakladatelství, 2021. 440 s. ISBN 978-80-7623-068-2.
14. SMEJKAL, Vladimír. Kapitola 1 Počítače a kybernetická kriminalita – základní pojmy. Kybernetická kriminalita. 3. rozšířené a aktualizované vydání. Čeněk, 2022. 1166 s. ISBN 978-80-7380-849-5.
15. ZÁVRŠNÍK, Aleš. Kyberkriminalita. Právní monografie. Praha: Wolters Kluwer, 2017. 148 s. ISBN 978-80-7552-759-2.

Elektronické zdroje

1. ANYDESK. Online. Jak předejít podvodům přes AnyDesk. Dostupné z: https://www.instaluj.cz/anydesk/jak-predejit-podvodum-pres-anydesk/. [cit. 2026-03-19].
2. ARTIC WOLF. What is Social Engineering? Online. Dostupné z: https://arcticwolf.com/resources/glossary/social-engineering/. [cit. 2026-01-28].
3. AVAST. Investiční podvody s lidmi, které nejspíš znáte. Online. Dostupné z: https://blog.avast.com/cs/investicni-podvody-s-lidmi-ktere-mozna-znate. [cit. 2026-01-29].
4. BDO CANADA. Fraudsters mask global Ponzi scheme behind deceptive cryptocurrency platform BitConnect. Online. Dostupné z: https://www.bdo.ca/insights/cryptocurrency-execs-charged-for-2-4-billion-ponzi-scheme. [cit. 2026-02-19].
5. ČESKÁ NÁRODNÍ BANKA. Varování před podvodnými investičními platformami. Online. 2024. Dostupné z: https://www.cnb.cz/cs/dohled-financni-trh/ochrana-spotrebitele/upozorneni/Varovani-pred-podvodnymi-investicnimi-platformami/. [cit. 2026-01-28].
6. ČSOB. Online. Podvod se vzdálenou správou AnyDesk a TeamViewer. Dostupné z: https://www.csob.cz/v-obraze/blog/clanky/podvod-se-vzdalenou-spravou-anydesk-a-teamviewer. [cit. 2026-03-19].
7. ČSOB POJISTOVNA. Online. Pojištění kybernetických rizik. Dostupné z: https://www.csobpoj.cz/pojisteni/podnikatele-firmy/pojisteni-kybernetickych-rizik. [cit. 2026-03-04].
8. ESET. Online. Kybertest. Dostupné z: https://www.eset.com/cz/o-nas/pro-novinare/tiskove-zpravy/kybertest-falesne-stranky-internetoveho-bankovnictvi-cesi-s-jistotou-nepoznaji-podvodne-sms-u-nich/. [cit. 2026-03-04].

9. ESET. Online. Sociální inženýrství. Dostupné z: https://www.eset.com/cz/socialni-inzenyrtsvi-a-bezpecnost-firmy/. [cit. 2026-03-19].
10. IT NETWORK. Online. Lekce 6 - Bezpečné přihlašování – 2FA a vícefaktorové ověřování. Dostupné z: https://www.itnetwork.cz/bezpecnost/bezpecne-prihlasovani-2fa-a-vicefaktorove-overovani. [cit. 2026-03-04].
11. MITNICK SECURITY. The 2020 Twitter Bitcoin Scam. Online. Dostupné z: https://www.mitnicksecurity.com/blog/2020-twitter-bitcoin-scam. [cit. 2026-02-19].
12. O2 CYBERNEWS. Pig butchering. Online. Dostupné z: https://o2cybernews.cz/slovnik/pig-butchering. [cit. 2026-02-19].
13. POLICIE ČESKÉ REPUBLIKY. Online. AnyDesk je host, který se nezouvá! Dostupné z: https://policie.gov.cz/clanek/anydesk-je-host-ktery-se-nezouva.aspx. [cit. 2026-03-04].
14. POLICIE ČESKÉ REPUBLIKY. Podvod s investicemi do kryptoměny. Online. Dostupné z: https://policie.gov.cz/clanek/podvod-s-investicemi-do-kryptomeny.aspx. [cit. 2026-02-19].
15. POLICIE ČESKÉ REPUBLIKY. Pozor na podvody na internetu!!!. Online. 2024. Dostupné z: https://policie.gov.cz/clanek/or-melnik-zpravodajstvi-pozor-na-podvody-na-internetu.aspx. [cit. 2026-01-28].
16. ŠTRÁFELDA, Jan. Heslo. Online. Jan Štráfelda. Dostupné z: https://www.strafelda.cz/heslo. [cit. 2026-03-04].
17. UNITED STATES ATTORNEY'S OFFICE. Co-Founder Of Multibillion-Dollar Cryptocurrency Scheme "OneCoin" Sentenced To 20 Years In Prison. Online. 2023. Dostupné z: https://www.justice.gov/usao-sdny/pr/co-founder-multibillion-dollar-cryptocurrency-scheme-onecoin-sentenced-20-years-prison. [cit. 2026-02-19].
18. ZÁKONY PRO LIDI. Online. Zákon č. 40/2009 Sb. 2009. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40. [cit. 2026-03-19].
19. ZÁKONY PRO LIDI. Online. Zákon č. 370/2017 Sb. 2017. Dostupné z: https://www.zakonyprolidi.cz/cs/2017-370. [cit. 2026-03-19].
20. ZÁKONY PRO LIDI. Online. Zákon č. 253/2008 Sb. 2008. Dostupné z: https://www.zakonyprolidi.cz/cs/2008-253. [cit. 2026-03-19].

Seznam tabulek a grafů

Seznam příloh

Přílohy

1. Vaše Pohlaví

- Muž
- Žena
- Jiné
- Nechci uvádět

2. Kolik Vám je let?

- 18–24 let
- 25–35 let
- 36–45 let
- 46 a více

3. Jak často používáte internet?

- Denně
- Několikrát týdně
- Občas
- Téměř vůbec

4. Jaké zařízení používáte k přístupu na internet?

- Mobilní telefon
- Počítač / notebook
- Tablet
- Jiné zařízení

5. Setkal/a jste se někdy s reklamou na online investice?

- Ano
- Ne
- Nevím

6. Klikl/a jste někdy na investiční reklamu na sociálních sítích

- Ano
- Ne
- Nevím

7. Víte, co znamená pojem phishing?

- Ano
- Spíše ano
- Slyšel/a jsem o tom
- Ne

8. Obdržel/a jste někdy podezřelý e-mail zprávu týkající se investic?

- Ano
- Ne
- Nejsem si jistý/á

9. Jak byste reagoval/a na nevyžádanou online nabídku investice?

- Ignoroval/a bych ji
- Nejprve bych si ji ověřil/a
- Pravděpodobně bych ji vyzkoušel/a

10. Investoval jste někdy prostřednictvím internetu?

- Ano
- Ne

11. Jak často si před online investicí ověřujete důvěryhodnost investiční nabídky nebo platformy?

- Vždy
- Často
- Občas
- Nikdy
- Neinvestuji online

12. Důvěřoval/a byste investici propagované známou osobností?

- Ano
- Spíše ano
- Spíše ne
- Ne

13. Ověřujete si před kliknutím na investiční odkaz pravost webové stránky nebo odesílatele?

- Vždy
- Někdy
- Nikdy
- Na podobné odkazy nereaguji

14. Které znaky podle Vás nejčastěji naznačuje investiční podvod?

- Příliš vysoký přínos
- Tlak na rychlé rozhodnutí
- Neznámá webová stránka
- Nevyžádaný kontakt
- Nedokážu posoudit

15. Setkal/a jste se osobně nebo ve svém okolí s investičním podvodem na internetu?

- Ano, osobně
- Ano, ve svém okolí
- Ne
- Nejsem si jistý/á

16. Do jaké míry důvěřujete investičním nabídkám na sociálních sítích?

- Zcela důvěřuji
- Spíše důvěřuji
- Spíše nedůvěřuji
- Vůbec nedůvěřuji

17. Které způsoby prevence investičních podvodů považujete za nejúčinnější?

- Větší informovanost veřejnosti
- Varování od bank a institucí
- Přísnější regulace reklamy
- Vzdělávání o kybernetické bezpečnosti
- Vlastní vzdělávání a zvyšování digitální gramotnosti
- Zvýšená opatrnost na internetu
- Nevím

18. Jaké velké riziko podle Vás představují online investiční nabídky

- Velmi vysoké
- Spíše vysoké
- Spíše nízké
- Velmi nízké
- Nevím

19. Kterému zdroji byste při rozhodování o online investici důvěřoval/a nejvíce?

- Oficiální web banky nebo instituce
- Doporučení od známých
- Reklama na sociálních sítích
- Internetové diskuze a recenze
- Žádnému z uvedených

20. Cítíte se být dostatečně informován/a o rizicích investičních podvodů na internetu?

- Ano
- Spíše ano
- Spíše ne
- Ne