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

BAKALÁŘSKÁ PRÁCE

PODVODY PÁCHANÉ V KYBERNETICKÉM PROSTORU MÍŘENÉ PROTI SENIORŮM V ČESKÉ REPUBLICE

Autorka práce: Veronika Tomková, DiS.

Studijní program: Bezpečnostně právní činnost

Forma studia: kombinovaná

Vedoucí práce: JUDr. Milan Kocík, MBA, LL.M.

Katedra: katedra právních oborů a bezpečnostních studií

2025

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Veronika Tomková

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

Název bakalářské práce: Podvody páchané v kybernetickém prostoru mířené proti seniorům v České republice

Název bakalářské práce v anglickém jazyce: Fraud Committed in Cyberspace Targeting Seniors in the Czech Republic

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce: JUDr. Milan Kocík, MBA, LL.M.

Datum zadání bakalářské práce: říjen, 2024

Cíl bakalářské práce:
Hlavním cílem bakalářské práce je zhodnocení nejčastěji využívaných metod a znaků kriminálního jednání v kybernetickém prostoru, jimiž pachatelé manipulují s obětmi.
Vedlejším cílem bakalářské práce je stanovení jednotlivých preventivních opatření pro snížení počtu kybernetických útoků mířených proti seniorům.

Student: Veronika Tomková	30.10.2024 *datum*	 *podpis*
Vedoucí práce: JUDr. Milan Kocík, MBA, LL.M.	8.11.2024 *datum*	 *podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	2.12.2024 *datum*	 *podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	9.12.2024 *datum*	 *podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	10.12.2024 *datum*	 *podpis*

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

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně, na základě vlastních zjištění a s použitím odborné literatury i 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 vedoucího 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 vedoucímu své bakalářské práce JUDr. Milanu Kocíkovi, MBA, LL.M., za cenné rady, připomínky a metodické vedení práce.

ABSTRAKT

TOMKOVÁ, V. Podvody páchané v kybernetickém prostoru mířené proti seniorům v České republice. České Budějovice: Vysoká škola evropských a regionálních studií, 2025. 68 s. Vedoucí bakalářské práce: JUDr. Milan Kocík, MBA, LL.M.

Klíčová slova: kybernetická kriminalita, podvody, senioři, prevence, kybernetické útoky

Tato bakalářská práce se zaměřuje na problematiku podvodů, které jsou páchány v kybernetickém prostoru na seniorech v České republice. Senioři představují jednu z nejzranitelnějších skupin, jelikož obecně mají nedostatek technické znalosti a povědomí o kybernetických hrozbách. Cílem práce je analyzovat nejčastější strategie a metody, které pachatelé využívají k manipulaci s oběťmi, a identifikovat včasná opatření pro snížení rizika kybernetických útoků.

V teoretické části je vysvětlen pojem kyberkriminalita, jsou zde charakterizovány hlavní aspekty kybernetických podvodů a popsány faktory, které přispívají k jejich páchání. Také jsou zkoumány účast pachatelů a specifika seniorské populace v kontextu kybernetické kriminality. Praktická část obsahuje analýzu dvou reálných případových studií, které zobrazují různé podvodné praktiky. Na základě těchto kazuistik jsou navržena zásadní doporučení pro zvýšení ochrany seniorů před kybernetickou kriminalitou. Práce přináší ucelený pohled na aktuální hrozby, kterým senioři v kybernetickém prostoru čelí, a zdůrazňuje význam prevence, osvěty a právního rámce jako klíčových opatření proti kybernetickým podvodům.

ABSTRACT

TOMKOVÁ, V. Fraud Committed in Cyberspase Targeting Seniors in the Czech Republic. České Budějovice: The College European and Regiolan Studies, 2025 68 pgs. Supervisor: JUDr. Milan Kocík, MBA, LL.M.

Key words: cybercrime, fraud, seniors, prevention, cyber attacks

This bachelor 's thesis focuses on the issue of fraud commited in cyberspace against seniors in the Czech Republic. Seniors represent one of the most vulnerable groups, as they generally lack technical knowledge and awareness of cyber threats. The aim of the thesis is to analyze the most common strategies and methods used by perpetrators to manipulate victims and to identify early measures to reduce the risk of cyber attaks.

The theoretical part explains the concept of cybercrime, characterizes the mail aspects od cyber fraud, and describes the factors contributing to its occurrence. It also examines the role of perpetrators and the specifics of the senior population in the context of cybercrime. The practical part contains an analysis of two real case studies that illustrate different fraudulent practices. Based on these case studies, key recommendations are proposed to enhance the protection of seniors agains cybercrime. The thesis provides a comprehensive view of the current threats that seniors face in cyberspace and highlights the importance of prevention, awareness, and legal frameworks as key measures against cyber fraud.

Obsah

Úvod

V současné době zažíváme období intenzivního technologického rozvoje, který proniká do všech oblastí našich životů a mění způsoby, jak pracujeme, komunikujeme a trávíme volný čas. Většina lidí používá technologie nejen pro práci, ale také v domácím prostředí, kde nám usnadňují běžné činnosti. Díky takovému pokroku dnes můžeme využívat internet, který propojuje svět prostřednictvím počítačů, tabletů, chytrých telefonů i dalších zařízení. Internet přinesl nové možnosti, od komunikace a sdílení informací až po digitální služby, které nahrazují dřívější metody, jako jsou psaní dopisů či osobní schůzky. V dnešní době můžeme komunikovat s lidmi na druhé straně zeměkoule nebo si zajistit služby, které dříve vyžadovaly osobní účast.

Ačkoliv technologie přináší nespočet výhod, jejich rychlé šíření má také své stinné stránky. Digitalizace nám poskytuje možnosti, ale také přináší nové formy kriminality, zejména v oblasti kybernetického prostoru. Podvodníci a zločinci dnes využívají moderní zařízení a digitální prostor k nekalým účelům, aby se obohatili na úkor obětí. Pomocí různých technik se dokážou dostat do počítačů běžných uživatelů a zneužít jejich důvěru i informace pro vlastní zisk.

Obzvláště zranitelnou skupinu v této souvislosti představují senioři, kteří v digitálním prostředí často nemívají tolik zkušeností a povědomí o možných hrozbách. Mnozí z nich se s internetem setkali až v pozdějším věku a chybí jim základní dovednosti nebo instinktivní schopnost rozpoznat nebezpečí, na které mohou v online prostředí narazit. Porozumění těmto problémům a včasná identifikace mechanismů, jimiž podvodníci působí na své oběti, ty mohou být krokem ke zlepšení ochrany seniorů a posílení jejich pocitu bezpečí při používání moderních technologií.

V teoretické části se bakalářská práce věnuje základním pojmům kybernetické kriminality, dále nejčastějším druhům kybernetických podvodů mířených proti seniorům v České republice a také typologii pachatelů i jejich obětí. V neposlední řadě se práce věnuje příčinám kybernetických podvodů, prevenci podvodů na internetu a vyšetřováním kybernetických podvodů.

Praktická část se věnuje analýze dvou reálných případových kazuistik. Pomocí těchto kazuistik budou identifikovány vzorce jednání jak pachatelů, tak obětí a následně navržena preventivní opatření.

1 Cíl a metodika bakalářské práce

Hlavním cílem předkládané bakalářské práce je zhodnocení nejčastěji využívaných metod a znaků kriminálního jednání, jimiž pachatelé manipulují s oběťmi.

Vedlejším cílem této bakalářské práce je stanovení jednotlivých preventivních opatření ke snížení počtu kybernetických útoků mířených proti seniorům.

Tématem této bakalářské práce je problematika kybernetických podvodů zaměřených na seniory v České republice. Vzhledem k rapidnímu rozvoji digitálních technologií, přístupu k internetu a rozšiřování online služeb se kyberkriminalita stává stále aktuálnější a složitější. Senioři, jakožto zranitelná skupina obyvatel, se mnohdy stávají snadným cílem pachatelů, kteří využívají jejich nedostatečných technických znalostí i důvěřivosti.

Teoretická část práce se zaměřuje na základní definice a vysvětlení klíčových pojmů. Základem této části je literární rešerše, přičemž zde se vycházelo z odborné literatury, mimo jiné i z důvěryhodných internetových zdrojů. Tato část má za cíl poukázat na složitost daného tématu a poskytnout přehled o vývoji kybernetických hrozeb i současných podvodných taktik.

Metodika práce se zaměřuje na deskriptivní a komparativní analýzu. Kazuistiky reálných případů kybernetických útoků na seniory budou analyzovány s důrazem na společné rysy těchto případů, což umožní identifikaci hlavních znaků kriminálního jednání. Tato metoda poskytne empirický základ pro vypracování efektivních preventivních opatření. Zdroje budou analyzovány s cílem poskytnout ucelený pohled na současnou situaci a vyvodit konkrétní závěry a doporučení. Dále se práce zaměří na prevenci a ochranu seniorů před kyberkriminalitou, přičemž budou uvedeny možné strategie vzdělávání, osvěty a technické ochrany. Součástí budou rovněž doporučení na základě analýzy reálných případů kyberútoků, která budou sloužit jako model pro preventivní opatření, která by mohla vést ke snížení počtu kyberútoků mířených na seniory.

2 Teoretická východiska kyberkriminality

Kybernetická kriminalita, často zkráceně označovaná jako kyberkriminalita, v dnešní době představuje rozmáhající se a závažný problém, který významně zasahuje do bezpečnosti jednotlivců i společnosti jako celku. Kyberkriminalita má dopad nejen na běžné uživatele digitálních technologií, ale také zaměstnává orgány činné v trestním řízení, které se zaměřují na identifikaci i stíhání internetových podvodníků a hackerů. Kdybychom se měli zamyslet nad počátky kyberkriminality, lze předpokládat, že její základy se datují od příchodu prvního počítače. Ačkoliv tyto počítače nebyly na současné technologické úrovni, někteří odborníci by mohli považovat za počátek kyberkriminality právě výše uvedenou dobu, zatímco jiní by její začátek stanovili až do období významnějšího technického rozvoje[1].

Kybernetická kriminalita je specifická také tím, že se často prolíná s jinými druhy kriminality. Například ekonomickou, bankovní nebo majetkovou kriminalitu lze v současnosti páchat prostřednictvím počítačových systémů. V takovém případě můžeme hovořit o trestné činnosti s prvky kybernetické kriminality, jako jsou neoprávněný přístup do počítačových systémů nebo neoprávněná manipulace s daty, což je v českém právním systému zakotveno v § 230 zákona č. 40/2009 Sb.[2]

První známý případ spadající výhradně do kategorie počítačové kriminality lze datovat do 70. let, kdy pracovník úřadu důchodového zabezpečení, nespokojený se svou prací, úmyslně poškodil záznamy na magnetických páskách pomocí magnetu, když obsluhoval samočinný počítač LEO 326. Tímto činem se snažil u automatizovaného počítače na zpracování důchodové agendy vyvolat havarijní stav a vyřadit jej z provozu, což mělo za následek, že zařízení nestačilo plnit svůj denní plán. Tímto jednáním ohrozil včasnou výplatu u zhruba 40 000 starobních, invalidních, vdovských a sirotčích důchodů. Úřad důchodového zabezpečení v Praze musel v té době vynaložit částku 1 001 229 Kč na odvrácení hrozících škod, pachateli byl uložen trest podle § 97 odstavce 3 Tr. Z., a to odnětí svobody v trvání 10 let[3].

První trestné činy spojované s kybernetickým prostorem měly podobu sabotáží. Tyto útoky páchali především zaměstnanci, kteří chtěli tímto způsobem poškodit svého

[1] ZAVRŠNÍK, A. Kyberkriminalita. Wolters Kluwer, 2017. 148 s. ISBN 978-80-7552-759-2.
[2] SMEJKAL V. Kybernetická kriminalita, Plzeň: Aleš Čeněk, 2015. 636 s. ISBN 978-80-7380-501-2.
[3] Ibid.

zaměstnavatele, a také reformátoři, kteří tímto činem vyjadřovali nesouhlas s politickou situací. Historicky prvním počítačovým útokem byl incident z 19. století, kdy byl poškozen tkalcovský stroj, řízený děrnými štítky. Josef Jacquard, jakožto vynálezce tohoto stroje, tak nevinně přispěl k prvním zaznamenaným útokům na automatizované systémy[4].

Ve srovnání s minulostí, kdy byly počítače spíše luxusem a sloužily převážně ve firemních a vládních institucích, je nyní situace zcela jiná. Podle statistik byl roce 2023 počítač běžnou součástí 82 % českých domácností a připojení k internetu mělo přibližně 87 % z nich. Po celém světě podle Mezinárodní telekomunikační unie využívalo internet v roce 2023 zhruba 67 % populace, což je více než dvojnásobek v porovnání s rokem 2013. Tyto údaje ukazují, jak rychle se internet a digitální technologie staly nezbytnou součástí každého života[5].

Pokud se zaměříme na starší populaci, můžeme vidět, že i mezi seniory uživatelů internetu neustále přibývá. V roce 2010 mělo k internetu přístup pouze 13 % osob starších 65 let, avšak do roku 2023 tento podíl stoupl na 52 %. Ještě významnější nárůst je patrný ve skupině osob 55 až 64 let, kde internet v roce 2010 používalo 42 % lidí, ovšem v roce 2023 to bylo již 91 %[6]. Tento vzestupný trend poukazuje na skutečnost, že internet se stává běžným nástrojem komunikace, informací i zábavy napříč všemi generacemi. Z těchto čísel můžeme usuzovat, že podvodníci a hackeři se budou snažit využívat svých schopností k nekalým praktikám a cíleně útočit na méně schopné jedince využívající počítač, kteří se na internetu pohybují, což bývá obzvláště pro osoby pokročilého věku rizikové.

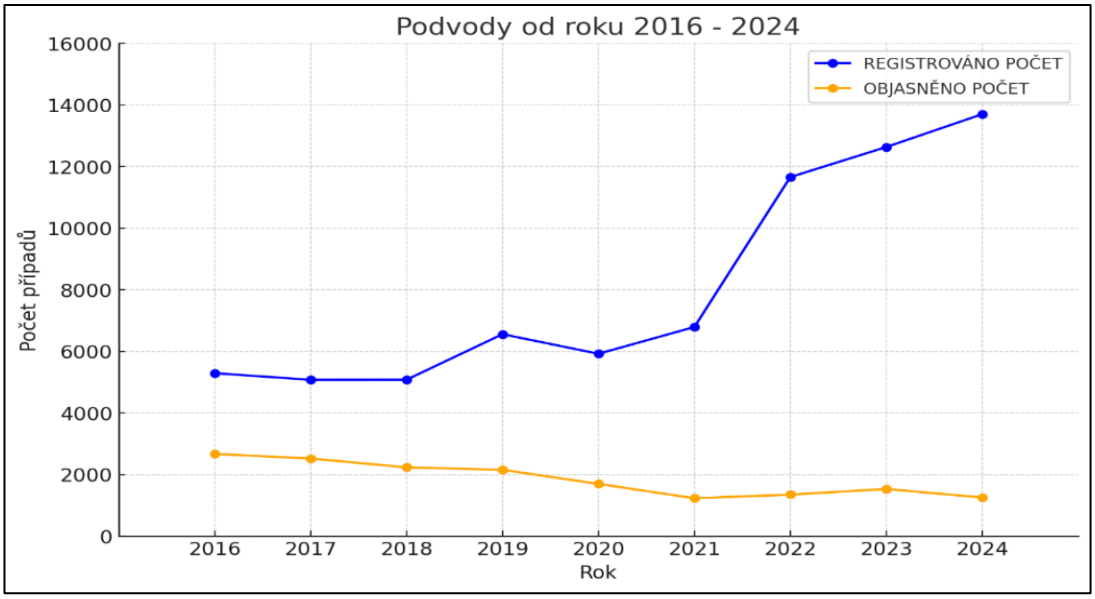
Policie ČR v rámci svých kompetencí řeší kybernetickou kriminalitu především jako podvod podle § 209 zákona č. 40/2009 Sb., kdy na základě statistik můžeme vidět postupný nárůst počtu podvodů od roku 2016 do současnosti.

[4] YONAZI, J. J., SEDOYEKA, E., ARIWA, E., EL-QAWASMEH, E. e-Technologies and Networks for Development. Heidelberg: Springer, 2011. 366 s. ISBN 978-3-642-22729-5.
[5] ČESKÝ STATISTICKÝ ÚŘAD, Informační technologie v domácnostech a mezi jednotlivci [online] poslední aktualizace 02.02.2024 [cit. 2024-05-11] Dostupné z: https://www.czso.cz/csu/czso/domacnosti_a_jednotlivci)
[6] Ibid.

Tabulka 1: Statistika kybernetické kriminality v České republice[7]

ROK	REGISTROVÁNO	OBJASNĚNO	OBJASNĚNO V PROCENTECH
	POČET	POČET	tj. v % (objasněnost)
2016	5 289	2 667	50,4
2017	5 074	2 518	49,6
2018	5 077	2 230	43,9
2019	6 556	2 151	32,8
2020	5 920	1 693	28,6
2021	6 789	1 228	18,1
2022	11 658	1 345	11,5
2023	12 634	1 527	12,1
2024	13 701	1 253	9,2

Graf 1: Podvody v rámci kybernetické kriminality



Zdroj: vlastní zpracování podle statistiky Policie ČR

Z grafu je patrné, že podvodů v České republice v letech 2016 až 2024 stále přibývá, přičemž nejvýraznější růst nastal v roce 2021. To souvisí především s rozvojem

[7] POLICIE ČESKÉ REPUBLIKY, Statistiky kriminalita [online]. [cit. 2025-03-05]. Dostupné z: https://policie.gov.cz/statistiky-kriminalita.aspx

internetových podvodů. Naopak počet objasněných podvodů je relativně stabilní a spíše se snižuje, což může být důsledkem například zvýšeného počtu případů, ale také složitějšího dokazování a odhalování pachatelů v online prostředí.

Kybernetická kriminalita zahrnuje široké spektrum trestné činnosti, která využívá moderní technologie k poškození jednotlivců, organizací či institucí. Rozvoj digitálních technologií přináší stále nové formy kybernetických hrozeb. Zatímco dříve byly útoky zaměřeny především na firmy a státní instituce, v posledních letech se kyberzločinci soustředí stále častěji na individuální uživatele, zejména na ty, kteří jsou v online prostředí méně zkušení. Tato skutečnost se týká především starší generace, která je vůči některým typům podvodů zranitelnější. Proto je potřeba preventivních opatření a vzdělávání uživatelů v oblasti kybernetické bezpečnosti důležitější než kdy dříve.

2.1 Pojem kybernetická kriminalita

Pojmy jako kybernetická kriminalita, kybernetický útok či kyberprostor patří dnes mezi běžně používané, nicméně pro lepší pochopení této problematiky je třeba se v nich důkladně orientovat. Pro kybernetickou kriminalitu, někdy označovanou zkráceně jako kyberkriminalita, neexistuje jedna pevně stanovená definice. Přesto ji můžeme chápat jako jednání, které využívá moderní technologie a zaměřuje se na neoprávněné nebo nemorální aktivity, často s cílem získat neoprávněné výhody.

Ministerstvo vnitra ČR definuje kyberkriminalitu jako *„trestnou činnost, v níž určitým způsobem figuruje počítač jako technické a programové vybavení (včetně dat) nebo některé jeho komponenty, případně více počítačů propojených do sítě, a to buď jako předmět této trestné činnosti (kromě případů, kde jsou považovány za movité věci), nebo jako prostředí či nástroj trestné činnosti“*[8]. Tato definice poukazuje na to, že počítač může být buď samotným cílem, nebo nástrojem trestné činnosti.

Z pohledu Policie ČR je kybernetická kriminalita chápána jako *„trestná činnost, která je páchána v prostředí informačních a komunikačních technologií, včetně počítačových sítí“*[9]. V Evropské unii je kyberkriminalita obecněji definována jako *„nemorální a neoprávněné jednání, které zahrnuje zneužití nebo změnu dat získaných*

[8] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY Základní definice, vztahující se k tématu kybernetické bezpečnosti [online] Praha, 2009 [cit. 2024-11-04] Dostupné z: cyber_vyzkum_studie_pojmy.pdf
[9] POLICIE ČESKÉ RUPUBLIKY Kyberkriminalita [online] [cit. 2024-11-04] Dostupné na WWW: https://www.policie.cz/clanek/kyberkriminalita.aspx

prostřednictvím informačních a komunikačních technologií nebo jejich úpravu"[10]. Tato definice se zaměřuje na zásah do integrity a důvěrnosti dat, což je základní prvek většiny kybernetických útoků.

Z těchto definic lze vyvodit, že kyberkriminalita zahrnuje široké spektrum aktivit, které jsou zaměřeny na zneužití technologických systémů nebo jejich obsahu a které jsou klasifikovány jako trestné činy. Kyberkriminalita bývá často zaměňována s pojmy počítačová či internetová kriminalita. Tyto pojmy je však nutné rozlišovat, neboť každý se vztahuje k jinému prostředí a spektru aktivit. Počítačová kriminalita zahrnuje trestnou činnost odehrávající se v prostředí počítačových systémů bez nutnosti připojení k internetu. Internetová kriminalita se naopak zaměřuje na činy, které probíhají výhradně na internetu. Kybernetická kriminalita tedy představuje širší koncept, který zahrnuje jak internetové, tak počítačové trestné činy, a vztahuje se na veškeré aktivity v rámci kyberprostoru, tedy na všechny digitální a technologické procesy i nástroje. Je proto důležité tyto termíny rozlišovat, neboť v literatuře bývají často zaměňovány a nesprávně označovány jako synonyma[11].

Toto široké spektrum různých definic je důležité proto, že kybernetická kriminalita neustále mění svou podobu s tím, jak se technologie vyvíjí. Zatímco v počátcích šlo o napadení prvních počítačových systémů, dnes se kybernetické útoky zaměřují nejen na počítače, ale také na chytré mobilní telefony, internetové účty, chytré domácnosti a různá zařízení napojená na internet. Kybernetická kriminalita se postupně vyvinula z počítačové kriminality, jak ji definuje autor Smejkal ve své knize Počítačové právo. Nejenže se tak zvyšuje počet kybernetických útoků, ale i jejich rozmanitost a technická sofistikovanost. Tento vývoj klade vysoké nároky na ochranu uživatelů i bezpečnostních složek, které se zabývají prevencí a vyšetřováním kybernetické kriminality[12].

Kyberkriminalita se tak stává jednám z velkých bezpečnostních problémů, které ovlivňují všechny oblasti našeho života, proto je nezbytné rozvíjet svou erudovanost jednotlivých typů a mechanismů v tomto odvětví kriminálního jednání, jejichž

[10] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY Základní definice, vztahující se k tématu kybernetické bezpečnosti [online] Praha, 2009 [cit. 2024-11-04] Dostupné z: cyber_vyzkum_studie_pojmy.pdf

[11] MinisterstvoVnitraCR, In: Youtube.cz [online] datum vydání 04.08.2022 [cit. 2024-11-05] dostupné na WWW: https://www.youtube.com/watch?v=4_dFiDX4vpQ

[12] SMEJKAL, V., SOKOL, T., VLČEK, M. Počítačové právo. Praha: C. H. Beck, 1995. 264 s. ISBN 80-7179-009-5.

prostřednictvím dochází k útokům na různé cílové skupiny, zejména pak na zranitelnější populaci, jako jsou senioři.

2.2 Pojem kybernetický prostor

Kybernetický prostor, známý též jako kyberprostor, je jedním z dalších důležitých pojmů současné digitální doby, přičemž jeho definice zůstává nejednoznačná. První zmínky o kybernetickém prostoru pocházejí z roku 1982, kdy toto slovo poprvé použil autor William Gibson v povídce Burning Chrome, a následně ve svém slavném románu Neuromancer z roku 1984. W. Gibson, představitel žánru kyberpunk (subžánr science fiction, který je zasazen do futuristického prostředí a charakterizuje jej kombinace společenské spodiny a pokročilé technologie[13]), který ve své knize popisoval budoucnost, kde svět funguje prostřednictvím elektronické interakce, a potřeboval jednoduché a výrazné označení pro tento prostor. Tak vznikl pojem „cyberspace“ neboli kyberprostor, který se používá dodnes. W. Gibson v něm viděl prostředí, kde lidé interagují s technologiemi a vstupují do virtuálních světů, což se brzy stalo nejen představou, ale i realitou[14].

V současné době chápeme kyberprostor jako virtuální a abstraktní prostředí, kde dochází ke komunikaci a interakci globálně ve světě. Představuje prostředek, který propojuje počítačové systémy na celém světě a umožňuje výměnu informací, komunikaci a přenos dat. Do kyberprostoru se vstupuje například prostřednictvím internetového připojení či bezdrátových sítí, jako je Wi-Fi. Uživatelé se v něm mohou pohybovat, komunikovat a sdílet obsah. Kyberprostor lze vnímat jako nehmotnou vrstvu nad reálným světem, která je tvořena miliardami propojených zařízení, která spolu vytváří síť umožňující nepřetržitý tok informací mezi jednotlivými uživateli, institucemi a organizacemi.

Viditelný web (anglicky Surface web) je ta část kyberprostoru, kterou spíše znají běžní uživatelé. Skládá se z indexované webové stránky, která je nejčastěji přístupná prostřednictvím prohlížečů. Kyberprostor můžeme přirovnat k takzvanému ledovci, na kterém se větší část uživatelů pohybuje jen ve viditelné části, přičemž o hlubších vrstvách nemá povědomí. Pro typického uživatele internet znamená především tuto viditelnou část,

[13] WIKIPEDIE, Kyberpunk [online] poslední aktualizace 13.10.2024 [cit. 2024-11-05] Dostupné z: https://cs.wikipedia.org/wiki/Kyberpunk

[14] ZLATUŠKA, J. Kyber není kybernetika, Vesmir.cz [online] poslední aktualizace 03.11.2016 [cit. 2024-11-06] Dostupné z: https://vesmir.cz/cz/casopis/archiv-casopisu/2016/cislo-11/kyber-neni-kybernetika.html

nazývanou Surface web. Pod touto silnou vrstvou se nachází Deep web, obsah, který není zařazen do běžných vyhledávačů, a proto také vyžaduje netypický přístup. Pod touto vrstvou se ještě nachází další web, zvaný Dark web. Ten je dostupný jen prostřednictvím specifických sítí, například Tor. Tento prostor je spojován hlavně s anonymitou a nelegálními aktivitami, avšak jeho využívání může mít i legální účely, jako je například soukromí. Velká část uživatelů si kyberprostor přestavuje pouze jako Surface web, a neuvědomuje si, že jde o hlubší součást internetu[15].

Kyberprostor vznikl souběžně s internetem a od té doby se rozvíjí s novými technologiemi, které mu dodávají další rozměry. Přestože je kyberprostor nehmotný, má skutečný dopad na reálný svět. Příkladem toho může být ochrana soukromí, bezpečnostní otázky či komunikace. Stal se tak prostorem, kde probíhá obrovské množství aktivit, které by dříve byly možné jen fyzicky, případně by nebyly uskutečnitelné vůbec. Kyberprostor se také stal místem, kde je vyžádáno aktivní opatření k zajištění ochrany uživatelů. Díky dynamickému rozvoji technologií a širšímu využívání internetu se kyberprostor stal nepostradatelným prostředím pro moderní společnost, zároveň však i místem, kde dochází k bezpečnostním narušením, jako jsou kybernetické útoky, krádeže dat či jiné formy kybernetické kriminality[16].

Kybernetický prostor zahrnuje jak veřejnou část internetu, která je přístupná většině uživatelů, tak i neveřejné či uzavřené systémy, například v rámci vládních institucí nebo podniků, které jsou chráněny a zabezpečeny proti neoprávněnému přístupu. Tato rozmanitost vytváří prostředí s potenciálem pro rozvoj, inovace i zneužití, což činí kyberprostor jak nástrojem pro pokrok, tak oblastí, kde je potřeba zajistit odpovídající ochranu před různými hrozbami.

2.3 Pojem kybernetický útok

Dalším důležitým pojmem k pochopení problematiky kybernetické kriminality je kybernetický útok, často zkráceně označovaný jako kyberútok. Ten nastává v situaci, kdy se jednotlivci nebo skupiny pokoušejí proniknout do našeho počítačového systému prostřednictvím internetu. Kyberútok je tedy možné definovat jako *„pokus o anonymní nabourání a neoprávněný přístup k počítači, výpočetnímu systému, počítačové síti nebo*

[15] KOLOUCH, J. Cybercrime. Praha: CZ.NIC, 2016. 524 s. ISBN 978-80-88168-15-7.
[16] ZELINKA, I. Kybernetický prostor – nástrahy, úskalí a hrozby, Národní centrum průmyslu 4.0 [online] [cit. 2024-11-06] Dostupné z: https://www.ncp40.cz/aktuality/kyberneticky-prostor-nastrahy-uskali-a-hrozby

jiné počítačové technologii s úmyslem způsobit škodu, např. deaktivovat počítač, odcizit nebo zničit data a informace, použít prolomený počítačový nebo informační systém ke spuštění dalších útoků, ovládnout výpočetní prostředí nebo infrastrukturu apod.“[17].

Jak se uvádí v knize Bezpečnost informačních systémů, podle zákona o kybernetické bezpečnosti se v kybernetickém prostoru odehrávají různé typy útoků:

- kyberterorismus v případě, že cílem nebo nástrojem útoku teroristů je informační nebo telekomunikační systém,
- kybernetická válka v případě ohrožení cizím státem,
- kybernetická kriminalita v případě, že se jedná o kriminalitu v klasickém pojetí jakožto promyšlenější druh trestné činnosti, často prováděný v rámci organizovaného zločinu[18].

Intenzita a dopad kyberútoku často závisí na tom, jak dobře je náš systém zabezpečen. V posledních letech kyberútoky získaly na sofistikovanosti a představují stále větší hrozbu nejen pro seniory a běžné uživatele, ale také pro celé národní systémy a globální bezpečnost. Útočníci zdokonalují své techniky, aby jejich činy zůstaly co nejdéle skryté, což znemožňuje jejich včasné odhalení.

Různé formy kyberútoků, které se neustále vyvíjejí, zahrnutí například šíření malwaru (škodlivého softwaru, který poškozuje nebo zneužívá počítače), phishing (podvodné získávání citlivých informací pomocí falešných zpráv nebo stránek[19]), útoky typu DDoS (útok, který zahlcuje server nebo síť, čímž ji vyřadí z provozu[20]), ransomware (škodlivý software, který šifruje soubory a požaduje výkupné[21]) a další způsoby, jak manipulovat a zneužívat informace. Tyto metody jsou navrženy tak, aby útočníci mohli obejít stávající bezpečnostní opatření a získat tak přístup k citlivým datům nebo kontrolu nad systémy. Kybernetické útoky se vyznačují tím, že využívají slabin jak v technologiích, tak v lidských návycích, což často vede k vážným finančním ztrátám, poškození pověsti a ohrožení soukromí.

[17] Legislativa.cz, Kybernetický útok (kyberútok). Definice, typy, následky a prevence [online] poslední aktualizace 13.09.2022 [cit. 2024-11-07] Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok

[18] SMEJKAL, V., SOKOL, T., KODL, J. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Aleš Čeněk, 2019 s. 378 s. ISBN 978-80-7380-765-8.

[19] WIKIPEDIE, Phishing [online] poslední aktualizace 13.10.2024 [cit. 2024-05-11] Dostupné z: https://cs.wikipedia.org/wiki/Phishing

[20] WIKIPEDIE, Denial of service [online] poslední aktualizace 16.12.2024 [cit. 2025-02-07] Dostupné z: https://cs.wikipedia.org/wiki/Denial_of_service

[21] WIKIPEDIE, Ransomware [online] poslední aktualizace 06.02.2025 [cit. 2025-02-07] Dostupné z: https://cs.wikipedia.org/wiki/Ransomware

V současnosti útoky zaznamenávají vzestup a kyberzločinci se neustále snaží vylepšovat své metody. Kybernetické útoky se stávají čím dál rafinovanější a jejich dopady se prohlubují. To je důvod, proč jsou prevence a vzdělávání v oblasti kybernetické bezpečnosti důležité, zvláště u zranitelnějších skupin, jako jsou senioři, kteří často nemívají dostatečné technické znalosti, a mohou se tak snadno stát terčem útoků.

3 Druhy kyberkriminality se zaměřením na seniory

Jak již bylo naznačeno v podkapitole výše, kybernetických útoků existuje celá řada a jde o takovou trestnou činnost, která se stále rozvíjí. V současné době můžeme rozlišovat dvě základní oblasti páchání kybernetické kriminality. První je takzvaná ICT-kyberkriminalita, která je páchána přímo s využitím počítače, notebooku, tabletu či jiných technologických zařízení. Pod tento pojem se řadí kybernetické útoky typu ransomware, phishing, trojské koně a mnohé další. Takové útoky častokrát využívají zranitelnosti v softwaru nebo neopatrnost uživatelů k získání neoprávněného přístupu k citlivým datům či finančnímu prospěchu pachatelů[22].

Druhá oblast zahrnuje ostatní kybernetickou kriminalitu, kterou můžeme definovat jako jiný druh kriminality, jenž se však projevuje v online prostoru. Zde můžeme řadit například trestné činy mravnostního charakteru, například vydírání, sexuální online násilí a další druhy, které mají podobnou formu. Tyto trestné činy často kombinují tradiční kriminální prvky s využitím moderních technologií, čímž se zvyšuje jejich dosah a také anonymita pachatelů. Některé trestné činy, které jsou páchány prostřednictvím moderních technologií, jako jsou počítače, ve velké míře cílí přímo na seniorskou populaci. Senioři se na internetu setkávají s různými formami nástrah, které se snaží využít jejich nižší míru digitální gramotnosti, důvěřivosti či neznalost moderních technologií. S rozvojem digitalizace ve společnosti se tyto formy kriminality stávají stále sofistikovanějšími, což klade zvýšené nároky na preventivní opatření a osvětu zaměřenou právě na tuto zranitelnou skupinu obyvatelstva[23].

3.1 Phishing – podvodné e-maily

Phishing patří mezi nejčastější formy podvodů, jejichž cílem je vylákání citlivých údajů od seniorů, jako jsou čísla platebních karet nebo přístupy do internetového bankovnictví. Může se také jednat o manipulaci vedoucí ke stažení škodlivého softwaru.

Typický scénář phishingového útoku spočívá v tom, že senior obdrží podvodný e-mail, který ho vyzývá k ověření svého bankovního účtu zadáním osobních údajů. Pokud tak učiní, pachatelé získají přístup k těmto citlivým informacím a následně převedou

[22] POLICIE ČESKÉ REPUBLIKY, Kyberkriminalita [online]. [cit. 2025-03-12]. Dostupné z: https://policie.gov.cz/clanek/kyberkriminalita.aspx

[23] JIROVSKÝ, V. Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. 288 s. ISBN 978-80-247-1561-2.

finanční prostředky na jiné účty. Výsledkem je, že senior může přijít o značnou část svých úspor, nebo dokonce o veškerou finanční hotovost[24].

Phishingové útoky se často šíří nejen prostřednictvím e-mailů, ale i videí či sociálních sítí. Pachatelé rozesílají falešná oznámení, která napodobují notifikace například o nových přátelích, komentářích či jiných aktivitách na sociálních sítích. Nebezpečí těchto zpráv spočívá v jejich vysoké míře věrohodnosti, jelikož se vizuálně velmi podobají skutečným oznámením. Tyto falešné zprávy obvykle obsahují odkazy, na které je uživatel vyzván kliknout a následně zadat své citlivé údaje, zejména přihlašovací údaje k bankovním účtům. Odkazy mohou vést na podvodné webové stránky, které věrně kopírují vzhled oficiálních stránek bank nebo jiných institucí, a jak bylo již výše uvedeno, tyto zadané údaje se následně okamžitě dostávají do rukou pachatelů[25].

Pro pachatele je tvorba falešných stránek a podvodných zpráv poměrně jednoduchá, díky dostupnosti šablon a návodů na internetu se tyto techniky stále zdokonalují.

3.2 Smishing – podvodné SMS

Dalším z běžně se vyskytujících podvodných jednání je smishing, což je podvod spojený se zasíláním falešných textových zpráv. Cílem těchto zpráv je vyvolat u příjemce dojem takové situace, která ho přiměje k rychlému a neuváženému jednání. Nejčastěji se v těchto zprávách objevují informace o nevyzvednuté zásilce na poště, oznámení o výhře v soutěži o velkou hotovost nebo o hodnotném předmětu. Odesílatel těchto zpráv může mít telefonní číslo, které je velmi podobné oficiálním číslům banky, pošty, úřadů nebo jiných důvěryhodných institucí a doručovacích služeb. Tento podvodný trik zvyšuje věrohodnost zprávy a snižuje šance, že příjemce zprávu identifikuje jako podvodnou. V některých případech obsahují tyto esemesky i webový odkaz, který po rozkliknutí přesměruje uživatele na falešnou stránku. Na této stránce jsou poté požadovány citlivé osobní údaje, jako jsou čísla bankovních účtů, PIN-kódy nebo údaje o platebních kartách.

[24] KYBERTEST, Podvodné e-maily (phishing) [online]. [cit. 2025-12-03]. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu/phishing-podvodne-e-maily

[25] Citace: DONÁT, J., TOMÁŠEK, J. Právo v síti: Průvodce právem na internetu. C.H.Beck, 2016. 352 s. ISBN 978-80-7400-610-4.

Jakmile se osoba na takovou stránku dostane a zadá zde své údaje, podvodníci je mohou zneužít k finančnímu obohacení[26].

Cílem těchto podvodných praktik je vždy získání finančního prospěchu. Senioři se bohužel stávají častými oběťmi smishingu, jelikož mívají větší důvěru v komunikaci prostřednictvím textových zpráv.

Podvodníci též často využívají specifických časových okamžiků, kdy je oběť více zranitelná. Například v povánočním období, kdy lidé mohou ztratit přehled o svých objednávkách a mohou snadněji podlehnout falešným oznámením o zásilkách.

3.3 Vishing – podvodné telefonáty

Dalším z velice častých a velmi nebezpečných druhů podvodů je vishing, taktéž známý jako voice phishing. Tento podvod je doopravdy velmi zákeřný, jelikož oběť komunikuje přímo s podvodníkem, který se může vydávat za bankéře, policistu nebo jinou důvěryhodnou osobu. Cílem vishingu je vyvolat u oběti pocit důvěry, popřípadě i strachu, což podvodníkům umožňuje s obětí manipulovat.

Komunikace obvykle začíná tak, že se podvodník představí jako bankéř, finanční poradce, policista nebo jiná veřejně známá osoba, a její identitu, kterou podvodník zneužívá, lze snadno ověřit. V další fázi podvodník informuje oběť, že její bankovní účet byl napaden, nebo že některý z jejích příbuzných naléhavě potřebuje pomoc. Někdy se snaží oběť přesvědčit, že jí nabídne velmi výhodnou investici, nebo že může získat velkou částku z investic. Situace je podvodníky navržena tak, aby podněcovala oběť buď k pocitu ohrožení, nebo naopak k chamtivosti, což vede k tomu, že důvěřivý člověk odevzdá podvodníkům peníze nebo citlivé údaje. Pachatelé tohoto typu podvodu se na své jednání pečlivě připravují. Začínají tím, že si shromažďují informace o oběti, což jim umožňuje působit přesvědčivěji. Získají nejen základní informace, jako jsou jméno, příjmení, datum narození a adresa, ale v některých případech mohou disponovat i fotokopií občanského průkazu oběti anebo jiného identifikačního dokladu. Tato důvěryhodná informace pomáhá podvodníkovi vytvářet pocit autenticity a důvěryhodnosti[27].

[26] KYBERTEST, Podvodné SMS (smishing) [online]. [cit. 2025-12-03]. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu/smsishing-podvodne-sms-zpravy

[27] KYBERTEST, Podvodné telefonáty údajných bankéřů, policistů či investičních poradců (vishing) [online]. [cit. 2025-12-03]. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu/vishing-podvodne-telefonaty

Podvodníci při tomto druhu podvodu využívají techniku tzv. spoofingu. Jde o program umožňující skrýt skutečné telefonní číslo a místo něj zobrazit číslo, které vypadá jako oficiální číslo banky, policie či jiné instituce. Pokud oběť zareaguje a zavolá zpět na toto číslo, spojí se s oficiální institucí, jejíž číslo na displeji vidí.

3.4 Podvodné m-platby

M-platba neboli mobilní platba je způsob platby, který funguje podobně jako platba platební kartou. Rozdíl však spočívá v tom, že při platbě kartou se peníze strhávají přímo z bankovního účtu. U m-platby je však částka odečítána z předplaceného kreditu nebo z měsíčního tarifu, který má oběť u svého mobilního operátora.

Pro podvodníky představuje m-platba výhodu, jelikož při jejím využívání od oběti není třeba získávat údaje o platební kartě, ale stačí jednorázový kód, který je zaslán prostřednictvím mobilního operátora. Tento kód pak slouží pro ověření platby. Podvodníci se snaží získat telefonní číslo oběti, které je pro tento podvod důležité. Pokud má osoba, kterou chtějí podvést, profil na sociálních sítích, mohou se do něj pokusit nabourat, a to buď přímo, nebo prostřednictvím různých metod získání přístupu k jejím kontaktům. Jakmile podvodníci mají telefonní číslo oběti, zadávají ho do platební brány a vybírají jako možnost platby právě m-platbu. Aby platba mohla proběhnout, musí provozovatel platební brány verifikovat transakci prostřednictvím kódu, který je odeslán na zadané telefonní číslo. Podvodník tedy následně kontaktuje oběť, která mu poskytla své telefonní číslo, a žádá ji o zaslání tohoto ověřovacího kódu. Jakmile oběť kód pošle, podvodník využije tuto informaci k provedení platby a strhne z jejího kreditu nebo tarifu požadovanou částku[28].

Tento typ podvodu je velmi nebezpečný, protože oběť nemusí mít povědomí o tom, že byla podvedena, dokud neobdrží výpis, kde zjistí neautorizovanou platbu.

3.5 Bazarové podvody

Bazarové podvody se staly relativně novou, ale velmi oblíbenou taktikou podvodníků. Setkat se s tímto druhem podvodu může v současnosti prakticky kdokoli, kdo má přístup k počítači a internetu. S rozvojem online platforem pro nákup a prodej

[28] KYBERTEST, Podvodné m-platby [online]. [cit. 2025-12-03]. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu/podvodne-m-platby

zboží bývají takové podvody stále častější. Zpravidla mívají za cíl získat citlivé údaje oběti nebo přímo její finanční prostředky.

Podvodníci začínají tím, že reagují na inzeráty, které obsahují nabídky prodeje zboží. Z inzerátu si obvykle opatří e-mailovou adresu nebo telefonní číslo prodávajícího a následně jej kontaktují. Tento kontakt může probíhat prostřednictvím různých komunikačních aplikací, jako jsou WhatsApp, Messenger nebo jiné obdobné platformy, kde se vydávají za zájemce o koupi zboží. V průběhu této komunikace podvodník postupně navádí oběť k tomu, aby uhradila poplatek za přepravu zboží, který by měl zajišťovat kupující, tedy podvodník. Tento poplatek bývá obvykle vybírán prostřednictvím falešné platební brány, která je zřízena tak, aby vypadala jako oficiální web dopravce. Prodávající, tedy oběť, obvykle obdrží odkaz na tuto nepravou platební bránu, která vypadá důvěryhodně. Po kliknutí na odkaz je oběť požádána o vyplnění svých citlivých údajů, jako jsou informace o platební kartě, přístupové údaje do online bankovnictví, včetně hesla a bezpečnostního kódu zaslaného prostřednictvím autorizační SMS. Podvodníkovi takto získané údaje umožní převést peníze z bankovního účtu oběti na jiný účet, čímž oběť připraví o většinu finančních prostředků, případně dokonce o všechny[29].

3.6 Podvodné mobilní aplikace a udělení oprávnění k aplikacím

Senioři kromě počítačů stále častěji využívají chytré telefony, které jim usnadňují přístup k internetu, a otevírají se tak nové možnosti komunikace a zábavy. Během svého „brouzdání“ po internetu se však mohou setkat s nabídkami, které na první pohled mohou vypadat jako užitečné aplikace nebo aktualizace. Méně zkušený uživatel, zvláště pak senior, si může nechtěně stáhnout malwarem infikovanou aplikaci nebo aktualizaci z neoficiálních obchodů s aplikacemi nebo z podezřelých webových stránek.

Tyto škodlivé aplikace s sebou mohou přinést řadu nebezpečí, mezi která patří například sledování aktivit uživatele, krádež osobních údajů či přístup k citlivým informacím. Některé aplikace mohou také vyžadovat vysoká oprávnění, která se sice mohou jevit neškodně, ale ve skutečnosti mohou představovat riziko. Mezi taková

[29] KYBERTEST, Bazarové podvody [online]. [cit. 2025-12-03]. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu/bazarove-podvody

oprávnění se může řadit například souhlas s nahráváním telefonických hovorů, přístup k fotoaparátu, textovým zprávám a dalším funkcím telefonu[30].

Podpisem těchto oprávnění může být neúmyslně umožněno podvodníkovi získat citlivé údaje, jako jsou přihlašovací údaje do online bankovnictví, obcházení dvoufázového ověření nebo přístup k potvrzovacím SMS-kódům. Takové informace mohou být použity k finančním podvodům, krádežím nebo jiným nelegálním aktivitám[31].

3.7 Podvodné e-shopy a webové stránky

V dnešní době představuje nakupování přes internet běžnou součást života. Taková forma nákupu je pohodlná, rychlá a přehledná, často také nabízí výhodnější ceny ve srovnání s těmi v kamenných prodejnách. Tyto faktory činí z online nakupování atraktivní záležitost i pro seniory, kteří hledají jednoduchý způsob, jak si pořídit různé zboží za dobrou cenu z pohodlí svého domova. Bohužel, právě nízké ceny mohou být klamavé a výsledek takového nákupu může být pro seniora nepříjemný.

Podvodníci využívají tohoto trendu a snaží se nalákat seniory na falešné e-shopy, ale i na napodobeniny oficiálních stránek bank či dalších institucí. Takové stránky mohou vypadat téměř identicky, což obětem může ztížit odhalení podvodu. Mnohdy se jedná o lákavé nabídky, jako jsou neuvěřitelné slevy, výhry v soutěžích nebo jinak atraktivní nabídky, které mají za cíl vzbudit zájem a nalákat oběť k návštěvě webové stránky. Pokud se oběť pokusí na takovou stránku dostat, může se například stát, že URL-adresa webu bude zneužita k přesměrování oběti na falešnou stránku, která vypadá jako legitimní e-shop. Dalším nebezpečím je stažení škodlivého malwaru, který může infikovat počítač či mobilní telefon. Tento malware může ukrást citlivé údaje, šifrovat soubory a následně podvodník může požadovat výkupné za jejich zpřístupnění. V případě, že jde o podvodné stránky bank, podvodníci se často zaměřují na získání přístupových údajů k internetovému bankovnictví. Jejich cílem je vylákat hesla, čísla účtů a další citlivé informace, které mohou následně využít k finančním podvodům[32].

[30] KYBERTEST, Podvodné mobilní aplikace a udílení oprávnění k aplikacím [online]. [cit. 2025-12-03]. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu/podvodne-mobilni-aplikace-a-udileni-opravneni-k-aplikacim
[31] Ibid.
[32] KYBERTEST, Podvodné e-shopy a webové stránky [online]. [cit. 2025-12-03]. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu/podvodne-e-shopy-a-webove-stranky

4 Typologie pachatelů trestné činnosti v kyberprostoru a jejich motivace

V obecné rovině se podle trestního zákoníku (§ 22 odst. 1 TrZ) *„pachatelem rozumí osoba, která svým jednáním naplnila znaky skutkové podstaty trestného činu nebo jeho pokusu či přípravy, je-li trestná“*[33]. V případě trestní odpovědnosti za spáchání trestného činu je stanoveno, že pachatelem je fyzická osoba, která svým jednáním naplnila všechny znaky trestného činu a v době jeho spáchání dovršila patnáctý rok svého věku[34], u mladistvé osoby podle zákona č. 218/2003 Sb. § 5 je dáno, že její čin musí být protiprávní a zároveň je schopna ovládat své jednání[35].

Podle autora Vladimíra Smejkala můžeme speciálně v oblasti kyberkriminality očekávat, že se pachatelé budou rekrutovat nejen z řad osob mladistvých (tedy těch, kdo v době spáchání provinění dovršili 15. rok a nepřekročili 18. rok svého života), ale i osob, které nedovršily věk 15 let. Vzhledem k rostoucí penetraci počítačů a počítačových sítí, včetně připojení k internetu, ale i v této oblasti dochází k posunu a věkové rozložení pachatelů trestné činnosti se zplošťuje[36].

Konkrétní popis podvodníků na internetu je velmi složitý, jelikož vysoká míra anonymity umožňuje pachatelům snadno uniknout spravedlnosti. Obecně však můžeme říct, že pachatele bychom mohli rozdělit do dvou skupin. Hackeři, kteří mívají buď velmi dobrou znalost internetového prostředí a častokrát vynikají v rychlém programování nebo jsou experti ve využívání konkrétního programu, anebo amatéři, pro které je hacking pouze prostředkem a technologie jim umožní dosažení jejich cíle. Taková osoba útočí na špatně zabezpečené osobní údaje, kreditní karty či naivní lidi, jako bývají senioři. Znalosti amatérů jsou ve srovnání s hackery výrazně omezené. Hlavní motivaci pro amatéry představuje především finanční zisk. K méně častým motivačním pohnutkám mohou patřit i chuť škodit nebo msta.

[33] ČESKO. ZAKONYPROLIDI, Trestní zákoník - § 22 [online]. [cit. 2025-12-15]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[34] ČESKO. ZAKONYPROLIDI, Trestní zákoník - § 25 [online]. [cit. 2025-12-15]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
[35] ČESKO. ZAKONYPROLIDI, Zákon o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže) č. 218/2003 Sb. [online]. [cit. 2025-12-15]. Dostupné z: https://www.zakonyprolidi.cz/cs/2003-218
[36] SMEJKAL, V. Kybernetická kriminalita. 3 vydání. Plzeň: Aleš Čeněk, 2022 s. ISBN 978-80-7380-849-5.

Dříve byl mezi oběma skupinami jeden zásadní charakteristický rys. Jak hackeři, tak amatéři vynikali vysokou mírou inteligence. Tento rys však v průběhu let zanikl. Je to dáno tím, že technologie bývají mnohonásobně vyspělejší, než tomu bylo dříve. Díky tomu i průměrně zdatný člověk je schopen v internetovém prostředí vytvořit větší množství internetových stop. Takovými stopami se rozumí tvorba podvodných internetových stránek, zasílání škodlivých e-mailů, změna hlasu či vizáže osoby přes aplikace a mnoho dalších.

Pokud bychom svou pozornost měli zaměřit na hackera, tento pojem bývá velmi zkreslený. Většina lidí se domnívá, že hacker je osoba, která pouze škodí. Toto tvrzení však není pravdivé a obecně lze hackery řadit do dvou základních skupin[37]:

Hackeři *„jsou osoby, které s nadšením programují, dokonce je programováním posedlý, anebo dává přednost praktickému programování před teoretickými úvahami o programování. Jsou to osoby, které vynikají v rychlém programování nebo jsou experty ve využívání konkrétního programu[38]“*.

Crackeři jsou osoby, *„jejichž prvotním cílem je zneužití hackerských metod, většinou pro finanční zisk. Do této skupiny je však možno zařadit i individua zneužívající internet a technologie pro vandalismus, teroristické aktivity, finanční podvody a další nelegální činnosti“[39]*.

Názvy hackeři a crackeři můžeme též vykládat jako etičtí a neetičtí hackeři, které samo o sobě definuje, kdo je kladně a kdo negativně vnímán společností. Toto dělení bývá často vykládáno jako tzv. kloboukové dělení. Zde rozlišujeme tři kategorie:

White hat hackers neboli hackeři s bílým kloboukem či etičtí hackeři jsou osoby, které vynikají v oblasti počítačové bezpečnosti a mají hluboké znalosti o fungování systémů. Jejich cílem je identifikovat zranitelnosti a slabiny v systémech s cílem poskytnout vlastníkům systémů informace a doporučení, jak je opravit. Pracují většinou pro organizace, které je najímají jako součást bezpečnostních týmů[40].

[37] JIROVSKÝ, V. Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. 288 s. ISBN 978-80-247-1561-2.
[38] Ibid.
[39] Ibid.
[40] Certifikace Manažerských Systémů.cz, Kdo je etický hacker a co je jeho prací [online] [cit. 2024-12-27]. Dostupné na WWW: https://www.cems-cz.com/blog/534-kdo-je-eticky-hacker-a-co-je-jeho-praci

Black hat hackers neboli hackeři s černým kloboukem jsou hackeři provádějící nelegální aktivity, jako jsou krádež dat, špionáž, vydírání, sabotáž nebo poškozování počítačových systémů za účelem osobního prospěchu nebo škody. Takové osoby ignorují veškerá pravidla a zákony pro ně nehrají žádnou roli. Jsou známí právě pro své škodlivé jednání na internetu[41].

Gray hat hackers neboli hackeři se šedým kloboukem představují jakýsi střed mezi White hat hackery a Black hat hackery. Provádějí nelegální aktivity, ale často s dobrými úmysly, jako je varování vlastníků o zranitelnostech v jejich systémech. Mohou také požadovat peníze nebo jinou kompenzaci za poskytnutí informací o zabezpečení[42].

Dá se říct, že toto jsou základní skupiny hackerů, ale existuje celá řada dalších specifických skupin v rámci kybernetického prostředí. Každý typ hackera má své vlastní charakteristiky, motivace a etické normy, které určují jejich chování v kybernetickém prostředí.

Jestliže svou pozornost zaměříme na hlavní motivaci, jak je uvedeno výše, tou bývá především finanční zisk. Tato motivace je však jednou z mnoha, které mohou pachatele pobízet k páchání trestné činnosti v online prostoru. Podle knihy Kybernetická kriminalita autora Vladimíra Smejkala se najdou i jiné motivy, které se mohou také kombinovat:

- pocit převahy nad vyšší institucí, například zaměstnavatelem, policií, veřejností,
- pocit beztrestnosti, neodhalitelnosti, pocit intelektuální převahy,
- kompenzace své vlastní nespokojenosti s prací, vzdělávacím systémem, osobním životem, překonání svého pocitu nedostatečnosti,
- snaha o získání určitých výhod,
- touha po dobrodružství,
- politické motivy (politický odpor)[43].

[41] Certifikace Manažerských Systémů.cz, Kdo je etický hacker a co je jeho prací [online] [cit. 2024-12-27]. Dostupné na WWW: https://www.cems-cz.com/blog/534-kdo-je-eticky-hacker-a-co-je-jeho-praci
[42] Ibid.
[43] SMEJKAL, V. Kybernetická kriminalita. 2. vydání. Plzeň: Aleš Čeněk, 2018. 934 s. ISBN 978-80-7380-720-7.

Tato rozmanitost motivů ukazuje, že kybernetická kriminalita zahrnuje velké množství pohnutek, které mohou být jak osobní, tak ideologické.

4.1 Kriminogenní faktory umožňující páchání kybernetické trestné činnosti

Kriminogenními faktory rozumíme takové faktory, které přispívají ke vzniku a také k samotnému šíření kybernetické kriminality. Nejvýznamnější faktor představuje vysoká míra anonymity na internetu. Anonymitou se rozumí určitý stav, kdy osoba, která používá služby v online prostoru, není při užívání viditelná[44]. Lze říct, že její skutečná identita spojená s jejími digitálními aktivitami zůstává skryta. Hlavní cíl je především zůstat těžko identifikovatelný pro ostatní uživatele, poskytovatele služeb či případné podvodníky. Tohoto stavu je možné docílit například skrýváním IP-adres (tedy čísla, které jednoznačně identifikuje síťové rozhraní v počítačové síti[45]), šifrovaných komunikačních kanálů (tzv. tajná/skrytá komunikace) či vytváření online persony pomocí pseudonymů[46].

Dalším významným prvkem, který přispívá ke vzniku a šíření kybernetické kriminality, je snadná dostupnost technologií. V minulosti bylo zapotřebí hlubokých znalostí ke spáchání kybernetického podvodu, v současnosti však, s nástupem umělé inteligence a automatizace, je vytvoření škodlivých a podvodných prostředků mnohem jednodušší. Díky tomu přibývá kybernetických zločinů a podvodníci mohou provádět sofistikované útoky s minimální vynaloženou snahou. Též vzniká velké množství manipulativních technik za účelem získání citlivých informací či finančních prostředků. Tyto techniky se nazývají sociální inženýrství, které pracuje se strachem obětí, vytváří na oběť nátlak, využívá zvědavosti, naléhavosti nebo chamtivosti obětí. Útočníci místo složitého prolomení bezpečnostních systémů využívají lidskou psychologii. Pachatelé využívající tuto techniku bývají označováni jako sociotechnikové. Jejich cílem je přesvědčit oběť, aby udělala něco, co může pachateli přinést profit, nebo poskytla citlivé informace. Takový pachatel se snaží o to, aby oběť nepoznala, že byla zneužita[47]. Metody

[44] KLIMEK, L., ZÁHORA, J., HOLCR, K. Počítačová kriminalita v europskych súvislostech. Praha: Wolters Kluwer, 2016. 448 s. ISBN 978-80-8168-538-5.
[45] WIKIPEDIE, IP adresa [online]. poslední aktualizace 09.12.2024 [cit. 2024-12-27]. Dostupné z: https://cs.wikipedia.org/wiki/IP_adresa
[46] RYCHLOST.CZ. Anonymita na internetu: Je možné zůstat opravdu neviditelný? [online]. [cit. 2024-12-27]. Dostupné z: https://rychlost.cz/clanek/2024-10-anonymita-na-internetu-je-mozne-zustat-opravdu-neviditelny
[47] ŠULC, V. Kybernetická bezpečnost. Plzeň: Aleš Čeněk, 2018. 147 s ISBN 978-80-7380-737-5.

sociálního inženýrství, jako jsou phishing, smishing, vishing, jsou podrobněji přiblíženy v kapitole výše.

Kriminogenních faktorů existuje velké množství, proto následuje výčet několika z nich:

- snížená možnost dopadení – vysoká míra anonymity ztěžuje identifikaci a dopadení pachatele,
- rychlost kriminálního jednání – útoky jsou velmi rychlé a pachatel je schopen převést velké množství peněz v krátké době,
- nedostatečné zabezpečení uživatelů – užití slabých hesel, neaktualizace zařízení,
- nízká vymahatelnost práva – právní systém je opožděn za vývojem technologií,
- psychologické faktory – chybovost uživatelů,
- vzestup kybernetických prostředků – množství nových hrozeb a nových podvodů v prostředí internetu,
- nedostatečné vzdělání uživatelů v oblasti kybernetické bezpečnosti – podceňování situací a hrozeb,
- decentralizované finanční měny/systémy – vznik digitální měn, jako jsou kryptoměny.

Kriminogenní faktory tvoří komplexní soubor příčin, díky nimž je pachatelům usnadněno páchat trestnou činnost v online prostředí. Tato kombinace faktorů ukazuje, že boj s kybernetickou kriminalitou je náročný a vyžaduje neustálou adaptaci právních, technologických i preventivních opatření.

5 Senioři jako cílová skupina kyberkriminality a charakteristika seniorské populace

V průběhu života nás ovlivňuje řada faktorů, které formují naše chování, vnímání světa a schopnost adaptace na nové situace. Mezi tyto faktory patří vzdělání, rodinné zázemí, sociální prostředí, přátelské vazby, kulturní zvyklosti a také doba, ve které žijeme. Významnou roli v tomto procesu sehrává i věk, který s sebou přináší nejen životní zkušenosti, ale také různé fyzické i psychické změny. Tyto změny ovlivňují způsob, jakým jedinec reaguje na nové neznámé situace, sociální výzvy, dokonce i na nové technologie.

Osoby, které dosáhnou určitého věku, označujeme za seniory. Tato skupina tvoří početně rostoucí část populace, což je důsledek prodlužující se průměrné délky života a zlepšení zdravotní péče. Termín „senior“ však není jednoznačně definován. Z hlediska sociologie se za seniory obvykle považují osoby ve věku 60 let a starší. Z čistě společenského pohledu bývají senioři často vnímáni jako jedinci, kteří ukončili svou aktivní pracovní kariéru a odešli do důchodu[48].

V době, kdy osoba dosáhne seniorského věku, může na sobě zaznamenávat řadu změn. Přibývá různých nemocí, zdravotních obtíží, komplikací i dalších životních potíží. Kromě zhoršujícího se zdraví se senioři setkávají se sociálními problémy, jako jsou osamění, přílišná důvěřivost či naivita. Mnoho seniorů touží po uznání a respektu, chtějí být vnímáni jako plnohodnotní členové společnosti, kteří mají stále co nabídnout. Tato potřeba být aktivní a zapojený může vést k tomu, že se senioři pouštějí do nových činností, včetně používání moderních technologií, kde však mohou narazit na své limity. V důsledku této snahy o adaptaci se mohou stát zranitelnějšími a náchylnějšími k podvodům, ať už v reálném světě, nebo v online prostředí. Senioři si většinou bývají vědomi své slabosti a zranitelnosti, snaží se však o její eliminaci. Pokud nastane situace, kdy by taková osoba měla pomoc vyhledat, dostává se do stavu utajování problému. To je způsobeno pocitem vlastní viny a snahou o vyloučení pocitu vlastní neschopnosti.

Jestliže se oprostíme od reálného světa, kde seniora může přepadnout pachatel na ulici, vydírat jej, zneužívat jeho slabosti a důvěřivosti, a nahlédneme do virtuálního světa, zjistíme, že na seniory zde číhá řada pastí. Tuto skupinu obyvatelstva do velké míry

[48] PRIMASENIOR. Od kdy je člověk senior? [online]. [cit. 2025-01-12]. Dostupné z: https://www.primasenior.cz/od-kdy-je-clovek-senior/

charakterizuje omezená digitální gramotnost, která je dána především nedostatkem přístupu k moderním technologiím v jejich mládí. Dnešní senioři žili v době, kdy byly nejrůznější technologie v počátcích svého vývoje a ceny takovýchto přístrojů dosahovaly astronomických výšin. Technologie byly drahé a bývaly považovány spíše za luxusní zboží než za běžný nástroj každodenního použití. Tento historický kontext působí na digitální gramotnost dnešních seniorů. Omezená digitální gramotnost je jedním z klíčových faktorů zvyšujících zranitelnost seniorů.

Je však důležité zmínit, že existují i další faktory, které zvyšují zranitelnost seniorů ve virtuálním prostředí. Jak již bylo zmíněno výše, přílišná důvěřivost a nedostatek podezíravosti zvyšují míru ohrožení této skupiny občanů. To je důvod, proč senior snáze uvěří podvodným e-mailům, reklamám nebo žádostem o poskytnutí osobních informací, či si takového jednání nemusí být ani vědom. Selhání může být i na straně samotného zabezpečení elektroniky. Mnoho seniorů nemá softwarové a bezpečnostní aktualizace, případně nemají ve svých technologických zařízeních tyto nástroje vůbec instalovány. Taková nedbalost může znamenat zvýšené riziko kybernetických útoků a bezpečnostní chyby mohou zůstat neopravitelné. Senioři také mohou mít omezené povědomí o tom, jak chránit své soukromí v online prostředí. Časté a volné sdílení osobních informací na sociálních sítích nebo na jiných online platformách může zvýšit riziko identitních krádeží a dalších forem kybernetických útoků. Také existence různých typů zařízení a aplikací může pro seniory představovat zmatek a ztížit jim orientaci v digitálním prostředí. Různé platformy mohou vyžadovat odlišné postupy, což může pro seniory představovat komplikace.

Rizika nemusíme hledat pouze za technologiemi, ale můžeme je nalézt i v samotném vlivu stárnutí. Jak bylo popsáno výše, i fyzické omezení seniora do velké míry ovlivňuje a může se podepsat na jeho chování v digitálním prostředí. Vlivem fyzických nebo psychologických faktorů mohou být senioři méně odolní vůči manipulaci na internetu. Fyzická omezení spojená s přibývajícím věkem, jako jsou problémy se zrakem či třes rukou, mohou představovat překážky při používání technologií s malými obrazovkami nebo klávesnicemi. To může vést k chybným kliknutím na nesprávné odkazy nebo nechtěné stahování nebezpečných souborů. Postupem času senioři mívají problémy s pamětí a kognitivními schopnostmi, což jsou vlivy, které směřují k podceňování rizik, dále pak k obtížím při identifikaci podvodů nebo samotných

podvodníků figurujících na internetu. U starších jedinců hrozí zhoršená orientace na internetu, s čímž souvisí i jejich rizikový pohyb ve virtuálním prostředí[49].

Velkým a důležitým tématem je i nedostatek podpory a vzdělání v oblasti moderních technologií. Mnozí senioři nenacházejí dostatečnou podporu ze strany své rodiny nebo komunity, ve které se nachází. To může ovlivňovat jejich schopnost se chránit před kybernetickými hrozbami. Také samotný nedostatek vzdělávání a informací o rizicích kyberkriminality může vést k rizikovému chování na internetu. Senioři buď o výukových programech, které podporují jejich znalosti v oblasti moderních technologií, vědí, jen je ovšem nevyužívají ze strachu či pocitu nepotřebnosti, anebo ani nemají povědomí o tom, že takové programy existují.

5.1 Viktimologie na internetu, kdy obětí je senior

Viktimologie je obor, který se zabývá studiem obětí trestné činnosti a dalších traumatizujících událostí, mezi které patří i páchání trestné činnosti na internetu. V posledních letech se viktimologie stále více zaměřuje na problematiku kybernetického zločinu a jeho dopady na zranitelné skupiny, jako jsou senioři. Internetová viktimologie zkoumá různé formy kybernetických hrozeb, které byly popsány v kapitole výše, a které postihují starší občany. Tyto hrozby následně analyzuje, určuje jejich důsledky a možnosti prevence. Důsledky se rozumí například finanční ztráty, kdy senioři mohou přijít o veškeré své úspory, nebo mohou být kvůli podvodům na internetu zadluženi. Dále se může jednat o psychické dopady, kdy senioři ztrácí důvěru jak v internetové prostředí, tak v lidi a pocit, že se stali oběťmi internetového podvodu, může mít vážné psychické dopady, včetně úzkostí a depresí[50].

S viktimologií se pojí další pojmy, a to viktimizace a viktimnost. Tato dvě pojmosloví jsou sice různá, ale vzájemně propojená v oblasti viktimologie. U viktimizace se jedná o proces, kdy fyzická osoba, v tomto případě senior, se stává obětí[51]. Zatímco u viktimnosti můžeme hovořit o určité disponovanosti nebo pravděpodobnosti stát se obětí trestného činu[52]. K tomu mohou přispívat různé faktory, přičemž jedním z nich je

[49] CIMRMANNOVÁ, T., Zápisky z předmětu Vybrané sociální problémy a metody sociální práce (2019), nepublikováno, Evangelická akademie – Vyšší odborná škola a střední odborná škola
[50] WIKIPEDIE, Viktimologie [online]. poslední aktualizace 25.12.2023 [cit. 2025-01-12]. Dostupné z: https://cs.wikipedia.org/wiki/Viktimologie
[51] WIKIPEDIE, Viktimizace [online]. poslední aktualizace 25.12.2023 [cit. 2025-01-12]. Dostupné z: https://cs.wikipedia.org/wiki/Viktimizace
[52] SLOVNÍK CIZÍCH SLOV. Viktimnost [online]. [cit. 2025-01-12]. Dostupné z: https://slovnik-cizich-slov.abz.cz/web.php/slovo/viktimnost

stáří. Ovšem těchto faktorů je mnohem více a se zmiňovaným stářím se mohou prolínat i jiné faktory související se stářím. Může se například jednat o fyzické či psychické hendikepy, které seniora ovlivňují v chování v digitálním prostoru, a jiné.

Výše zmíněná viktimizace prochází několika fázemi, které jsou primární, sekundární a terciální. Primární viktimizace je přímo způsobena internetovým útokem. V této fázi oběť, v tomto případě senior, čelí okamžitému nebezpečí, které má za následek například finanční ztráty nebo vznik psychických traumat v důsledku podvodného jednání. Tento první kontakt s trestným činem je pro seniory obzvlášť náročný, neboť nejenže přicházejí o své úspory, ale také zažívají silný šok, který může mít dlouhodobé nebo trvalé následky. Finanční ztráty mohou vážně ohrozit jejich životní úroveň, zatímco psychické trauma může způsobit dlouhodobé ztráty důvěry v ostatní a v internetové prostředí[53].

Sekundární viktimizace se projevuje výhradně v rovině psychické nebo emoční. Tato fáze následuje po spáchání skutku a týká se především požitků oběti v reakci na událost. Sekundární viktimizaci mohou nezáměrně způsobit jak okolí oběti, tak i osoby zapojené do trestního řízení. Například nesprávně provedený výslech, kdy je oběť neúměrně vystavena stresu, nebo pokud se s ní jedná neempaticky. Podobně může sekundární viktimizaci vyvolat i pachatel, který se snaží zastrašit seniora, aby měl strach o celé věci hovořit s úřady, nebo mu vyhrožuje dalšími trestnými činy, pokud bude chtít činit určité kroky k nápravě[54].

Poslední fázi představuje terciární viktimizace, která nastává po primární i sekundární fázi. V této fázi je senior zasažen tak hluboce, že není schopen se opětovně začlenit do běžného života. Jeho životní rytmus je narušen, obvykle bývá stále pohlcován strachem a obavami, že se stane opět obětí. Může se cítit ztracený a neschopný čelit každodenním význam, což může mít vážný dopad na jeho sociální vztahy i celkovou pohodu. V takových stavech je pro oběť důležité vyhledat odbornou pomoc, aby se mohl začít uzdravovat jak psychicky, tak i sociálně a znovu se začlenit do společnosti.

Viktimologie je důležitým oborem pro porozumění procesům, kterými oběti trestné činnosti procházejí. Výzkum viktimologie přispívá k lepší identifikaci zranitelných jedinců a pomáhá přizpůsobit právní, sociální a psychologickou pomoc tak,

[53] HOLOMEK, J., Viktimologia. Plzeň: Aleš Čeněk, 2013. 166 s. ISBN 978-80-7380-446-6
[54] Ibid.

aby byla co nejefektivnější. V kontextu seniorů, kteří se často stávají cílem kybernetických podvodů i dalších trestných činů, je výzkum viktimologie nezbytný pro identifikaci a eliminaci rizikových faktorů, které je činí zranitelnými.

6 Příčiny kybernetických podvodů na seniorech

Příčinou, proč se senioři stávají častým terčem kybernetických útoků, je nemálo a vzájemně se prolínají. Může se jednat o již zmíněnou nedostatečnou digitální gramotnost, důvěřivost na straně seniora a sociální izolaci, nedostatečnou ochranu osobních údajů či zneužívání strachu a mnoho dalších. Tyto příčiny podle Úřadu služby kriminální policie a vyšetřování Policejního prezidia České republiky můžeme rozdělit na tři hlavní kategorie. Jedná se o příčiny na straně nabídky, příčiny na straně poptávky a příčiny dané vývojem situace[55].

6.1 Příčiny na straně nabídky

Příčinami na straně nabídky se rozumí takové příčiny, které vytváří pachatelé za účelem svého zisku. Pachatel či skupina pachatelů se zaměřují na pocity strachu nebo chamtivosti seniora. Jsou založeny například na velmi kvalitně zpracovaných prezentačních a ilustrativních materiálech, které mají přesvědčit seniora o výhodnosti nabídky i možnosti pravidelného a vysokého zhodnocení úspor. Nebo jej naopak přesvědčit o tom, že jeho finanční prostředky mohou být nenávratně ztraceny, pokud senior nezačne pachatele poslouchat. Může se jednat například o prezentaci naskenovaného občanského průkazu nebo osobních údajů. Pachatelé si vybírají zranitelné oběti, kterými častokrát bývají senioři, které jsou do schémat kybernetických podvodů lákány pod příslibem vysokého a pravidelného zhodnocení prostředků, pokud své prostředky chtějí zhodnocovat[56].

Aby měl příběh, který pachatel své oběti předříkává, úspěch, musí být zjevně výhodnější než nabídky legitimních poskytovatelů finančních služeb. Aby toho podvodníci dosáhli, slibují obětem vysoké garantované zisky, které se zpravidla pohybují o několik procent výše než běžné výnosy od legitimních poskytovatelů finančních služeb. Tato tvrzení podvodníků mohou být podpořena výše zmiňovanými materiály, které bývají pečlivě propracované. Mezi takové materiály se mohou řadit fiktivní grafy či data bez jakékoli provázanosti s realitou. Senioři vzhledem ke své důvěřivosti častokrát uvěří v jejich pravdivost a s příslibem zaručených zisků vkládají peníze do rukou podvodníků,

[55] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY Analytický materiál k problematice investičních podvodů [online] 19.12.2023 [cit. 2025-01-15] Dostupné v systému Policie ČR ETŘ
[56] Ibid.

aniž by o podvodu měli tušení. Podvodníkům nahrává fakt, že regulované a legitimní subjekty musí uvádět, že minulé výnosy nejsou zárukou výnosů budoucích. Takového faktu podvodníci využívají ve svůj prospěch, jelikož toto omezení pro ně samotné samozřejmě neplatí[57].

Další výhodou, kterou podvodníci v kyberprostoru získávají, je jeho nehmotná povaha. Nákup hmotných statků je pro seniory přirozenější a snazší, jelikož kupovaný předmět lze různými způsoby prokázat, ověřit, osahat, a především jej vidět před sebou. Hmotnými statky můžeme rozumět suroviny, nemovitosti a jiné. Pokud se senioři rozhodnou pro nákup v kyberprostoru, většinou se setkají s akciemi či kryptoměnami, které z velké části ověřit nemohou nebo nevědí, jak to učinit. Zároveň velké množství obětí postrádá detailní znalost dané problematiky, a nezbývá jim tudíž nic jiného než se spoléhat na důvěru v odbornost a dobré úmysly pachatelů.

Jak již bylo zmíněno výše, pachatelé se také zaměřují na strach, který se v seniorech snaží vyvolat. Protože si senioři z velké části neumějí informace na internetu správně ověřovat, dostávají se často do svízelných situací. Pachatel si připraví povídání například o napadení jejich bankovního účtu a za pomoci pečlivě připraveného plánu i materiálů s osobními informacemi se snaží seniora zmanipulovat a přimět ke krokům, které byl sám neučinil, a především jim častokrát nerozumí.

6.2 Příčiny na straně poptávky

Takovými příčinami se rozumí ty, které vytváří nevědomky samotné oběti kybernetických podvodů. Současní senioři vyrůstali v době, kdy spoření bylo důležitou součástí jejich života, především proto, aby se měli lépe. V dnešní době je spoření pomalu nahrazováno investicemi, do kterých se starší populace lidí fungujících na internetu také snaží proniknout. Lidé všeobecně přirozeně tíhnou ke zhodnocování svých úspor a mají touhu mít dostatek finančních prostředků. Bohužel se však snaží najít takové způsoby zhodnocení svých úspor, které jsou co nejjednodušší, a častokrát právě toto jednání bývá nejrizikovější. Základním problémem u takového jednání bývá nedostatek jak finanční, tak digitální gramotnosti i dalších znalostí potřebných pro vyhodnocení reálnosti a samotné rizikovosti podvodné nabídky. Mnozí ze seniorů jsou v investování laici, kteří si myslí, že zbohatnutí u podobných nabídek je zaručené. Důsledkem této situace je touha

[57] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY Analytický materiál k problematice investičních podvodů [online] 19.12.2023 [cit. 2025-01-15] Dostupné v systému Policie ČR ETŘ

obětí lákavé nabídky rychlého a bezpracného zbohatnutí využít. Osoby v takových chvílích prožívají tzv. fear of missing out, ve zkratce FOMO, což je pojem, který do češtiny můžeme přeložit jako strach, že něco zmeškáme[58].

Často se také stává, že pokud již senior má nějaké prostředky investované a pachatelé jej nechávají v domnění, že se jeho prostředky zhodnocují, například posíláním falešných grafů s vývojem ceny, dochází tak k vytváření důvěry v produkt, který následně mohou doporučit dále, a to jak přátelům, tak rodině. Samozřejmé je, že pokud takovou osobu podvodníci znovu kontaktují, nemá problém poskytnout další finanční hotovost. Toho podvodníci využívají do té doby, dokud to jde. Než senior odhalí pravdu a začne být podezíravý, mohou uplynout nejen měsíce, ale i celé roky a škoda může mezitím dosáhnout statisíců, v některých případech dokonce i milionů korun.

Dalším z mnoha faktorů, které zvyšují počet obětí kybernetických podvodů, je důvěra v doporučení určitých autorit. Tomu můžeme rozumět tak, že senior v rámci komunikace s přáteli může uvěřit podvodu, kterému věří jeho dobrý přítel, nebo dokonce rodina. Toto ohrožení ovšem vůbec nemusí souviset pouze s okruhem blízkých lidí, ale podvodníci již využívají pokročilé umělé inteligence, díky které mohou vytvářet obrázky a videa, na kterých se vyskytují jejich oblíbení politici, herci, zpěváci a jiné veřejně známé tváře, kteří poukazují na výhodnou a zaručenou investici, jež je v samotném důsledku podvodná. Takto doporučený produkt může být oběťmi bezvýhradně přijímán bez kritického zvážení jeho možných nedostatků a rizik[59].

6.3 Příčiny dané vývojem situace

Vlivem opatření zavedených v souvislosti se šířením pandemie onemocnění covid-19 došlo u velkého množství lidí jak k většímu rozsahu úspor, například na základě zrušené či odložené spotřeby statků ve formě dovolených, kulturních či sportovních aktivit, tak ke změně spotřebního chování, které se vyznačovalo větší opatrností a tvorbou úspor vzhledem k menší předvídatelnosti budoucí situace ve společnosti.

V nedávné době, konkrétně v období let 2022 a 2023, v České republice vyvstal problém s vysokou mírou inflace, která se blížila 20 %. Tento jev zapříčinil zvýšení cen všech komodit v zemi, včetně surovin a služeb. Stav, ve kterém se občané České

[58] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY Analytický materiál k problematice investičních podvodů [online] 19.12.2023 [cit. 2025-01-15] Dostupné v systému Policie ČR ETŘ
[59] Ibid.

republiky nacházeli, měl negativní dopad na peněženky lidí, včetně jejich úspor a případného zhodnocení naspořených peněz. Proto lidé začali hledat jiné, a především rizikové způsoby zhodnocení a uchování hodnoty peněz. Zde však mnozí naráželi na své vědomosti v oblasti investic a zhodnocení úspor. Mnohdy neuvážené nakupování něčeho, čemu lidé nerozuměli, vedlo k nevratným ztrátám již tak znehodnocených peněz trvajícími inflačními tlaky. Takový vývoj situace byl velmi příznivý pro podvodníky, jelikož málokterá společnost byla schopna nabídnout vyšší úroky oproti inflaci. Pro podvodníky však žádný limit neexistuje a garantovaný výnos 30 % a vyšší byl interpretován ve většině podvodných nabídek[60].

Vysoká míra inflace nebyla jedinou příčinou rozrůstající se kybernetické kriminality. Velký pokrok zaznamenávaly investice v online prostředí, a to především kryptoměny. Nejznámější kryptoměna Bitcoin se začala poprvé ve větším měřítku šířit k běžným uživatelům v roce 2017, kdy se jeho hodnota přehoupla přes 1 000 dolarů. Od té doby popularita Bitcoinu stoupá, a to především díky velké volatilitě, která vedla k velkým ziskům některých lidí. Zprávy o této kryptoměně i jejím růstu zaplavovaly a stále zaplavují internet, což v lidech vzbuzuje touhu po rychlém zbohatnutí a vede k neuváženému nakládání s penězi[61].

Na základě těchto faktorů můžeme shrnout, že vývoj situace byl a stále je v některých svých aspektech pro pachatele kybernetických podvodů spíše příznivý, přičemž lze očekávat vznik nových metod či postupů k oklamání důvěřivých osob a zneužívání jejich identit.

[60] MINISTERSTVO VNITRA ČESKÉ REPUBLIKY Analytický materiál k problematice investičních podvodů [online] 19.12.2023 [cit. 2025-01-15] Dostupné v systému Policie ČR ETŘ
[61] Ibid.

7 Prevence a ochrana seniorů před kyberkriminalitou

S přibývající kriminalitou páchanou na internetu přibývá i zájmů (především ze strany orgánů, např. Policie ČR) o zvýšení prevence a zároveň ochrany před kybernetickými podvodníky. Prevence je opatření zaměřené na předcházení záporným jevům a jejich následkům. Tento pojem se často používá v souvislosti se zdravím, sociální problematikou nebo kriminalitou. Prevence se zaměřuje na minimalizaci rizik a jejich následků, přičemž je ve většině případů považována za účinnější než řešení již vzniklých problémů. Důležitým aspektem prevence je podněcování pozitivního vývoje v daném odvětví, avšak její účelnost je ovlivněna sociálními, ekonomickými a behaviorálními aspekty. Prevence se dělí podle obsahu a cílové skupiny.

❖ Členění podle obsahu:

- primární prevence – soustředí se na preventivní opatření zamezující vzniku škodlivých jevů, například očkování ve zdravotnictví nebo vzdělávání se v oblasti kriminality,
- sekundární prevence – zaměřuje se na rychlé odhalení problémů v prvotním stadiu, například může jít o diagnostické programy nebo identifikaci nejistého chování,
- terciární prevence – orientuje se na potlačení důsledků již vzniklého problému a podnět k návratu normálního stavu, například může jít o rehabilitace u onemocnění či opětovné začlenění pachatelů trestné činnosti.

❖ Členění podle cílové skupiny (adresátů):

- globální prevence – míří na celou populaci, například celonárodní kampaně o kyberbezpečnosti,
- selektivní prevence – zaměřuje se na rizikové skupiny, jako jsou senioři, kteří bývají častými oběťmi internetových podvodů,
- indikativní prevence – soustředí se na jedince, kteří v minulosti byli tímto negativním jevem zasaženi, například pomocí terapie pro oběti kriminality[62].

K tomu, abychom mohli kvalitně rozebrat a interpretovat preventivní opatření publiku, je dobré si uvědomit, že taková preventivní aktivita by měla být přiměřená věku

[62] ENCYCLOPEDIE SOCIÁLNÍCH VĚD. Prevence [online]. [cit. 17. 3. 2025]. Dostupné z: https://encyklopedie.soc.cas.cz/w/Prevence

příjemců, kterým je informace předávána. V případě, že příjemcem je mladší dítě, snaha by měla být spíše obecného charakteru. Tím je myšleno přenesení informace o důležitosti bezpečného hesla na internetu, sdělování osobních informací prostřednictvím internetu, fungování na sociálních sítích i při jiných aktivitách. Jedná-li se o děti staršího věku, bývá vhodné sdělit informace podrobnější – např. o sextingu, online podvodech, kyberšikaně a jiných. Pokud bychom měli sdělit informace seniorovi, je užitečné je zacílit na druhy a specifika podvodného jednání v kyberprostoru, na manipulaci ze strany podvodníků, bezpečné využívání internetu apod.[63]

Aby se prevence stala efektivním prostředkem, měla by být soustavná a dlouhodobá. Jestliže se jedná o prevenci krátkodobou nebo jednorázovou, existuje velká pravděpodobnost, že se osoba může stát obětí podvodného jednání na internetu. To bývá například u seniorů zapříčiněno zhoršenou pamětí nebo tím, že vznikají stále nové podvodné triky, které jsou podvodníky praktikovány, přičemž senior netuší, že se jedná o podvodnou praktiku. Dlouhodobost pomáhá seniorovi vštěpovat si do paměti nové poznatky, díky kterým může snáze rozpoznat klamavý přístup podvodníků. Seniorům je také vhodné věci ukazovat interaktivně s velkou mírou zapojení v rámci diskusí, práce ve skupinách či představením skutečných příběhů jiných seniorů. Prevence by seniory neměla děsit, ale naopak jim ukazovat správnou cestu a návod, jak se chovat v prostředí kybernetického prostoru[64].

Jeden z využívaných prostředků pro zvýšení erudovanosti seniorů představují přednášky. Tyto bývají většinou zajišťovány odborníky na kybernetickou bezpečnost nebo zástupci orgánů činných v trestním řízení a zaměřují se na různé aspekty kybernetické bezpečnosti. Tím se rozumí identifikace kybernetických hrozeb, ochrana osobních údajů, bezpečné chování v online prostředí a bezpečnostní postupy pro ochranu před kyberútoky. Přednášky nemusí být zaměřeny pouze na cílovou skupinu, jako jsou senioři, ale také na veřejnost či firmy nebo školy. Přednášky všeobecně slouží ke zvýšení povědomí o kybernetických hrozbách a poskytnutí konkrétních doporučení s nástroji pro ochranu. Konkrétně se senioři na přednáškách učí ověřování důvěryhodnosti webových

[63] Úvod do sociální práce s mládeží ohroženou elektronickým násilím a kriminalitou, organizováno Národním centrem bezpečnějšího internetu, certifikát, 2015.
[64] CIMRMANNOVÁ, T. Zápisky z předmětu Vybrané sociální problémy a metody sociální práce (2019), nepublikováno, Evangelická akademie – Vyšší odborná škola a střední odborná škola

stránek či e-mailů, tvorbě silných hesel a důležitosti rozmanitosti hesel pro každý účet zvlášť nebo nepodceňování aktualizací ve svých zařízeních[65].

Kromě přednášek jsou v rámci prevence k dispozici různé webové stránky a online zdroje, jež se zaměřují na bezpečné fungování na internetu. Takové stránky slouží k poskytování cenných a užitečných rad, nástrojů a upozornění, které pomáhají seniorům se lépe a efektivněji orientovat v kyberprostoru. Webové stránky dále mohou obsahovat školení a workshopy zaměřené na kyberbezpečnost, které pomáhají seniorům lépe porozumět problematice a naučí je konkrétním postupům vedoucím k ochraně. Webové stránky též mohou obsahovat různé aktuality, zaměřené na informace o nejnovějších kyberhrozbách nebo fóra či poradenské a podpůrné služby, kde se senioři mohou obrátit na odborníky ohledně konzultací a podpory v případě dotazů nebo problémů týkajících se kyberbezpečnosti. Webové stránky vytváří různé neziskové organizace, soukromé společnosti, vzdělávací instituce nebo vládní agentury, jako jsou ministerstva, úřady a jiné. Webové stránky mají za cíl poskytnout seniorům prostředky a znalosti k tomu, aby mohli bezpečněji využívat internet a chránit se před kybernetickými hrozbami i podvodníky na internetu.

Pro seniory, avšak nejen pro ně vznikají nejrůznější tituly knih, které mají za úkol edukovat seniory v používání počítačů i dalších přístrojů. Jednou z takových publikací je například kniha s názvem Internet pro seniory autora Josefa Pecinovského, která učí seniory, jak se správně orientovat na internetu, nakupovat v online prostředí, komunikovat na internetu i mnohé další. Podobnými tituly jsou např. stejnojmenná kniha „Internet pro seniory“ Miroslava Šance nebo „Komunikace na počítači pro seniory“ autorů Mojmíra Krále a Davida Krále. Všechny knihy jsou napsány tak, aby senior měl možnost jim porozumět a aby si z nich něco odnesl[66].

Dále vznikají stále nové programy na ochranu počítače a jeho komponentů. Ty chrání uživatele před stahováním škodlivých programů nebo kliknutím na škodlivé webové stránky. Mezi takové programy řadíme různé antivirové programy, které mají za cíl detekci a odstranění škodlivých softwarů, jako jsou viry, červi či trojské koně. Dále existují antimalwarové programy, které se specializují na odhalování a odstranění spywarů (podobají se špionům, kteří tajně sbírají informace a následně je odesílají

[65] Ibid.
[66] CIMRMANNOVÁ, T. Zápisky z předmětu Vybrané sociální problémy a metody sociální práce (2019), nepublikováno, Evangelická akademie – Vyšší odborná škola a střední odborná škola

pachateli) či ransomwarů (jedná se o škodlivý software, který vyhrožuje obětem, že pokud nezaplatí určitou částku, jejich data nebo systémy budou trvale zničeny, případně že přístup k nim bude zablokován).

Důležité však je seniory učit aktualizaci softwaru, neboť její pravidelnost může zabránit zranitelnosti operačního systému počítače, a také využívání silných hesel, která seniora mohou chránit před zneužitím dat v počítači.

K sice opomíjeným preventivním opatřením, majícím ale pro většinu seniorů nesmírný význam, patří vliv rodiny a přátel. Senioři rádi komunikují a v případě nesnází se mohou obrátit na své blízké okolí. Významná je zde role rodiny a přátel, kteří mohou seniora podporovat a pomáhat mu ve fungování na internetu. Důležité je dát seniorovi pocit, že v tom není sám a není ostuda, že něco neví. Pokud se senior ocitne v situaci, kdy na druhé straně telefonu má podvodníka, kterému argumentuje, že se poradí s dcerou, synem či jinou blízkou osobou, může tak předejít podvodnému jednání[67].

7.1 Vyšetřování kyberkriminality zaměřené na seniory a její právní ukotvení v České republice

Vyšetřování je základním prvkem pro odhalování podvodníků působících na internetu. Takovým vyšetřováním se z hlediska kybernetické kriminality zabývá kriminalistika. Ta na základě svých metod a postupů zkoumá trestné činy v oblasti kyberkriminality, způsoby jejich spáchání, typologii pachatelů i jejich obětí a další faktory, které napomáhají dopadení pachatelů i jejich spravedlivému potrestání. Takové metody jsou výsledkem práce kriminalistů, jejich pomocí jsou odhalovány nové metody a postupy pachatelů.

Kybernetických útoků existuje celá řada a lze se zde setkat s velkou variabilitou jejich provedení. Pachatelé za sebou v drtivé většině nezanechávají žádné hmatatelné stopy, a proto bývá jejich dopadení nezřídka velmi komplikované, až nemožné. Kriminalisté musí rychle a pružně reagovat na nově vzniklé podvody na internetu a neustále se v této oblasti vzdělávat. Dalo by se říci, že se jedná o neustálý koloběh, kdy pachatelé vymýšlejí nové a nové postupy pro svůj zisk, což ztěžuje práci kriminalistům, odhalujícím trestnou činnost na internetu. Další velký problém představuje složitost informačních systémů. Obecně je digitální technika čím dál pokročilejší a pachatelé

[67] CIMRMANNOVÁ, T. Zápisky z předmětu Vybrané sociální problémy a metody sociální práce (2019), nepublikováno, Evangelická akademie – Vyšší odborná škola a střední odborná škola

bývají častokrát velmi vzdělaní v oblasti výpočetní techniky i programování. Kriminalisté musí pružně reagovat na tok nových informačních systémů a vynaložit snahu na jejich rozklíčování. Výhodou pachatelů bývá i snadná likvidace případných stop. To je věc, která kriminalistům opět ztěžuje práci a snižuje pravděpodobnost dopadení pachatele.

Odhalování takových trestných činů, které se na internetu vyskytují, bývá velmi obtížné, a především dlouhodobé. Taková práce vyžaduje specifické znalosti, touhu po dopadení a neustálé rozšiřování svých znalostí. Policie se proto snaží vytvářet týmy speciálně proškolených kriminalistů, kteří mohou snadněji šlapat na paty pachatelům. Pokud se policisté při výkonu své práce setkají s osobou, která oznámila kybernetický podvod, je důležité, aby se postupovalo co nejrychleji. Kriminalisté se poté snaží pracovat maximálně efektivně, aby pachatel měl co nejméně času na zahlazení všech stop, pokud ovšem tak neučinil již v průběhu páchání protiprávního jednání. Policisté se při vyšetřování a prověřování kybernetických útoků i podvodů snaží vytvářet různorodé plány a postupy, jak nejrychleji zabránit převodu peněz, a zároveň jak zabránit pachateli v dalším klamavém jednání. To je však velmi složité, jelikož způsobů páchání takovéto trestné činnosti existuje celá řada a v průběhu času vznikají nové a nové techniky. Podle knihy „Kyberkriminalita a právo“ autorů Tomáše Gřivny a Radima Polčáka se plán vyšetřování dělí na dvě základní části.

První z nich zahrnuje pozorování, shromažďování a vyhodnocování informací. V rámci této části kriminalisté prověřují určité skutečnosti, například jakým způsobem došlo k protiprávnímu jednání. Také je v této části důležité určit, kdo se na konkrétním případu bude podílet. Druhá část již může zahrnovat domovní prohlídku, zajišťování počítačových stop, ohledání místa činu, výslech obviněného a svědků i další postupy[68].

Při vyšetřování musí kriminalisté také počítat s možností, že pachatel nemusí být sám, ale může se jednat o organizovanou skupinu, která se skládá z vysoce inteligentních lidí. Takové skupiny se snaží o co největší anonymitu a povětšinou mají ve skupině zavedena taková opatření, aby se minimalizovalo riziko jejich odhalení. Takové skutečnosti velmi protahují práci kriminalistů, v mnoha případech ji až znemožňují. Důležité tedy je sestavit takový tým profesionálů, kteří budou schopni rozklíčovat myšlenkové pochody pachatelů. Členové takového týmu musí dodržovat pravidla stanovená vedoucím pracovníkem, který se stará především o celkový postup

[68] GŘIVNA, T., POLČÁK, R. Kyberkriminalita a právo. Praha: Auditorium, 2008. 220 s. ISBN 978-80-903786-7-4.

vyšetřování. Vedoucí pracovník stanoví úkoly, které mají být provedeny, a taktéž to, kdo a kdy je provede. Rovněž dohlíží na kontrolu provedení jednotlivých zadaných úkolů. Mezi jeho úkoly patří též plánování dalšího postupu ve vyšetřování. Cílem nejrůznějších vyšetřovacích postupů je zajištění co největšího množství důkazních materiálů, potřebných k dokazování viny určitým osobám. Mezi důkazní materiál můžeme řadit výpovědi obviněného a svědků, znalecké posudky, věci a listiny důležité pro trestní řízení a jiné. Také samotný počítač pachatele a veškeré datové nosiče mohou být důkazním prostředkem[69].

Dokazování viny podvodníkům za pomoci důkazních materiálů je náročné a existuje zde jistá rozmanitost samotných důkazů. Může se jednat o výpisy volaných čísel, odeslané zprávy, podezřelá vyhledávání na internetu, textové dokumenty uložené v počítači i jiné prostředky dokazující vinu podvodníkovi. Dojde-li k dopadení pachatele či pachatelů, jedním z nejdůležitějších důkazních prostředků bývá právě výslech, jehož cílem je dosáhnout doznání, nebo alespoň získání potřebných informací k dalšímu vyšetřování. Kriminalisté se na takový výslech musí dostatečně připravit, sestavit plán, jakým způsobem budou podezřelého vyslýchat, a také sepsat řadu otázek, na které budou chtít znát odpovědi[70].

Každý výslech má tři fáze, mezi které řadíme úvod, monolog a dialog. Během úvodu dochází k ověření, že před kriminalistou sedí ta osoba, kterou chce vyslýchat. Dále kriminalisté o osobě zjistí další identifikační data. Vyslýchaný je řádně poučen a uvádí, že je se vším srozuměn. Následuje monolog, kdy během této fáze uvede vyslýchaný všechny skutečnosti, které o projednávané věci ví. Kriminalista během monologu vyslýchanému nevstupuje do řeči. Tato fáze je důležitá hned z několika důvodů. Kriminalista může sledovat nejen obsah toho, co mu vyslýchaný uvádí, ale také může sledovat řeč těla, která mu může napovědět, kdy se pro vyslýchaného stává monolog nepříjemným a kdy lže. Poslední fázi představuje dialog, který vede kriminalista. V této fázi kriminalista pokládá jednotlivé otázky vyslýchanému a zjišťuje další okolnosti, které v monologu nezazněly, nebo by na ně kriminalista chtěl znát odpověď. Kriminalista se

[69] GŘIVNA, T., POLČÁK, R. Kyberkriminalita a právo. Praha: Auditorium, 2008. 220 s. ISBN 978-80-903786-7-4.
[70] Ibid.

snaží, aby vyslýchaný odpovídal co nejpřesněji a uváděl takové skutečnosti, které mohou pomoci ve vyšetřování[71].

Používání různých metod vede k úspěšnému vyšetřování kybernetických útoků a podvodů v naší společnosti. Zároveň nové postupy mohou pomoci kriminalistům v odhalování nových podvodů, které by zůstaly neobjasněné. Jak již bylo zmíněno výše, odhalování kybernetických útoků je dlouhodobé a náročné. Kriminalisté musí pružně reagovat na každou prošetřovanou událost a snažit se z každé situace vytěžit maximum. Bez úspěšného vyšetřování budou pachatelé více a více klamat důvěřivé občany, jelikož se jedná o profitabilní činnost, která je umocněna vysokou mírou diskrétnosti.

[71] DOBSA, J., Zápisky z předmětu Kriminalistika [2023], nepublikováno, Vyšší policejní škola a Střední policejní škola Ministerstva vnitra v Praze

8 Případové kazuistiky kyberútoků

Na místní, popřípadě obvodní oddělení Policie České republiky přicházejí osoby s problémy různého druhu, ve kterých se snaží najít pomoc orgánu policie. Často se jedná o delikty, jako jsou krádeže, vloupání, násilí, výtržnictví či jiné trestné skutky. V posledních letech se však policie stále častěji setkává s případy kybernetických podvodů, které mnohdy mívají pro oběti vážné následky.

Tato praktická část práce se zaměřuje na dvě konkrétní případové kazuistiky, které si kladou za cíl ilustrovat, jakým způsobem podvodníci postupují v rámci páchání kybernetických podvodů. Důraz je kladen nejen na analýzu jejich taktik a metod, ale i na následky, se kterými se oběti potýkají, jako jsou finanční ztráty či psychické a sociální následky.

Cílem této praktické části je poskytnout komplexní pohled na problematiku kybernetických útoků zaměřených na seniory. Na základě vybraných případových studií, získaných v rámci výkonu služby na místním oddělení Policie České republiky, budou shrnuta doporučení pro prevenci těchto trestných činů.

V souladu s ochranou osobních údajů byly jména i další identifikační údaje v rámci této práce změněny.

8.1 Případová studie vybraného reálného útoku č. 1 a dopad na oběť

V posledních letech dochází k nárůstu kybernetické kriminality, což potvrzují i četná oznámení obětí. Jednou z nich se stala i 63letá Zuzana Nováková, která se dostavila na místní oddělení Policie ČR v Čakovicích. Paní Zuzana vyrůstala v rodině s tradičními hodnotami a virtuální svět jí byl dlouhodobě cizí. Přestože vlastnila chytrý mobilní telefon a počítač, používala je pouze na základní úrovni. Ačkoli z médií i od známých věděla o existenci podvodníků, domnívala se, že sama jedná bezpečně a že jí nic podobného nehrozí.

Dne 15. 12. 2023 přibližně ve 13 hodin jí zazvonil telefon. Na druhé straně se ozval mužský hlas, který se představil jako zaměstnanec České spořitelny ze Zlína. Uvedl, že se do tamní pobočky dostavila žena, která se snažila na její občanský průkaz získat půjčku ve výši 240 000 Kč. Tvrdil, že osobně viděl její doklad totožnosti, a proto volá,

aby situaci ověřil. Dále sdělil, že kontakt získal od České národní banky. Muž se představil jako Pavel Černý a dodal, že se jí brzy ozve někdo z její banky – Raiffeisenbank.

Krátce nato paní Zuzaně zavolal údajný zaměstnanec Raiffeisenbank, ten se představil jako pan Tichý. Požádal ji, aby si stáhla aplikaci Viber, jejímž prostřednictvím budou pokračovat v komunikaci. Paní Zuzana ho poslechla a aplikaci si nainstalovala. Pan Tichý jí sdělil, že ji brzy kontaktuje další osoba z bezpečnostního oddělení banky. Tento muž se nepředstavil a okamžitě ji začal zahlcovat informacemi o tom, jak ochránit její finance. Poté ji přepojil na jiného pracovníka, který se představil jako Jonáš. Ten ji instruoval, aby se dostavila do nejbližší pobočky Raiffeisenbank na Černém Mostě a vybrala veškerou hotovost ze svého účtu.

Během cesty i samotného výběru hotovosti byla stále na telefonu s podvodníky, aniž by tušila, že se jedná o podvod. V pobočce vybrala celkem 155 000 Kč. Poté byla instruována k převedení peněz na spořicí účet, odkud částku rovněž vybrala. Podvodník ji neustále varoval, aby nikomu nesdělovala, co dělá, protože by se tím mohla ohrozit bezpečnost jejích financí. Zejména ji odrazoval od informování pracovníků banky, protože mezi nimi údajně mohli být podvodníci napojení na ženu ze Zlína, která se snažila získat půjčku na její doklady.

Po výběru peněz ji podvodník navedl k bitcoinmatu v obchodním centru na Černém Mostě. Tam jí pan Jonáš vysvětlil, že vložené peníze budou dočasně uloženy na bezpečnostním účtu a následující den se jí vrátí zpět na běžný účet. Paní Zuzana nikdy o bitcoinmatu neslyšela, a proto se přesně řídila pokyny. Přes aplikaci Viber jí podvodník zaslal QR-kódy, které naskenovala, a následně do bitcoinmatu vložila celkem 155 000 Kč.

Tím však podvod neskončil. Podvodníci se začali zajímat i o bankovní účet jejího manžela. Pan Jonáš jí sdělil, že i jeho účet může být napaden, a přesvědčil ji, aby převedla i jeho peníze. Paní Zuzana měla k účtu manžela dispoziční právo a věděla, že na něm má 147 000 Kč. Podvodníci ji nasměrovali do nejbližší pobočky České spořitelny, kde celou částku vybrala, a následně ji opět prostřednictvím bitcoinmatu vložila na tzv. bezpečnostní účet. Celkem tak přišla o 302 000 Kč.

Po ukončení hovoru si paní Zuzana začala uvědomovat, že se pravděpodobně stala obětí podvodu, o kterém dosud slýchala pouze z médií. Policii poskytla veškeré

informace, včetně telefonních čísel, odkud jí podvodníci volali. Uvedla, že všichni pachatelé mluvili plynně česky a působili jako mladí lidé. Jediné, co jí a jejímu manželovi zůstalo, byla potvrzení o vkladech do bitcoinmatu. V důsledku této události přišli o všechny úspory a nyní se musí vystěhovat z nájemního bytu v Praze, neboť si již nemohou dovolit platit nájemné.

Tento příběh byl získán výslechem výše uvedené poškozené osoby.

8.2 Případová studie vybraného reálného útoku č. 2 a dopad na oběť

Pan Petr Novák, narozený v roce 1956, pochází z chudé rodiny, kde se pečlivě hlídala každá koruna. Jeho rodiče byli tvrdě pracující lidé a on sám si tuto hodnotu osvojil během svého produktivního věku. Za svůj život si dokázal našetřit dostatečnou finanční rezervu, aby si mohl užívat klidného stáří. Dne 14. června 2023 se pan Novák rozhodl podat trestní oznámení na místním oddělení Policie ČR v Čakovicích, kde uvedl, že se stal obětí kybernetického podvodu.

Vše začalo 28. února 2023, kdy si pan Novák prohlížel novinky na internetu. Na jedné z nejmenovaných stránek na něj vyskočila reklama nabízející investice do kryptoměn. Vzhledem k tomu, že už dříve slyšel o lidech, kteří na tomto typu investic zbohatli, rozhodl se kliknout na odkaz a zkusit štěstí. Na portále nalezl kontakt na společnost, která se měla těmito investicemi zabývat, a ihned ji kontaktoval. Na druhé straně se mu ozvala žena hovořící plynule česky, která se představila jako finanční poradkyně. Působila důvěryhodně a ochotně odpovídala na všechny jeho dotazy. Hovořila o historickém vývoji kryptoměn, spokojených zákaznících i o tom, že investice je rychlá a snadná cesta k vysokému zisku. Pan Novák nikdy předtím neinvestoval a jeho znalosti v oblasti kryptoměn byly minimální. Přesto jej přesvědčila, že jde o zaručený způsob zbohatnutí. Téhož dne byl přepojen na další poradkyni, která mu měla pomoci s převodem peněz. Zaslala mu graf s růstem ceny kryptoměn a vyzvala jej k rozhodnutí, kolik peněz chce investovat. Původně chtěl investovat 10 000 Kč, ale poradkyně jej přesvědčila, aby vložil 30 000 Kč, s argumentem, že větší investice znamená vyšší zisk. Následně jej instruovala, aby navštívil bitcoinmat v obchodním centru Černý Most, kam měl celou částku postupně vložit. Dne 17. března 2023 mu poradkyně telefonicky sdělila, že se jeho investice zdvojnásobila. Zároveň mu doporučila, aby vložil další finanční prostředky pro ještě větší výtěžek. Tímto způsobem byl pan Novák opakovaně vyzýván k dalším vkladům, až nakonec přišel o částku 490 600 Kč, kterou vybíral ze svých úspor

a bankovních účtů. Dne 25. května 2023 poradkyně nabídla novou službu převodu peněz přes kurýrní společnost. Pan Novák souhlasil, předal kurýrovi hotovost 180 000 Kč a věřil, že jeho investice nadále roste. Obrat nastal dne 14. června 2023, kdy pan Novák žádal vyplacení svých prostředků. Poradkyně jej přemlouvala k další investici, ale on trval na svém. Nakonec mu sdělila, že pro výběr peněz musí vložit dalších 30 000 amerických dolarů. To se mu zdálo podezřelé, a proto ještě téhož dne navštívil policii a nahlásil podvod. Přesto dne 25. srpna 2023 opětovně zaslal na účet podvodné společnosti 600 000 Kč, neboť si byl jistý, že firma je legitimní a on se nemůže mýlit. Celkově tak přišel o 1 270 600 Kč.

Případ se stal předmětem policejního šetření, avšak pachatelé zůstávají neznámí. Tento případ ukazuje, jak snadno se mohou senioři stát oběťmi podvodníků a jak důležité je být opatrný při online investicích. Kromě finanční ztráty mohou oběti takových podvodů přijít o stabilitu, důvěru v sebe sama i svůj běžný život.

Tento příběh byl získán výslechem výše uvedené poškozené osoby.

8.3 Analýza případových kazuistik

Na základě výše uvedených případových kazuistik se práce zaměří na jejich analýzu, s cílem nejen identifikovat důvody, které vedly k úspěšnému podvodnému jednání, ale také poskytnout konkrétní doporučení pro prevenci. Pomocí analýzy praktická část práce definuje metody manipulace, které byly využity k získání důvěry oběti, a zároveň poukáže na psychologické a sociální dopady těchto podvodů na zranitelné skupiny osob, jako jsou senioři. Na závěr budou navrženy opatření, která by mohla přispět k ochraně této skupiny osob před podobnými hrozbami.

8.4 Detailní analýza případové kazuistiky č. 1

Modus operandi pachatelů

Využité techniky manipulace vůči oběti

Pachatelé využili techniku sociálního inženýrství, která kladla důraz na vytváření důvěry mezi pachatelem a obětí. Používali manipulace s emocemi a rozhodováním oběti. V rámci manipulace též použili tlak na čas, kdy paní Zuzanu přesvědčili, že její finanční prostředky jsou v bezprostředním ohrožení. Paní Zuzana tak byla vystavena velkému

psychologickému tlaku, který vedl k jejímu impulzivnímu rozhodnutí, jako bylo okamžité převedení finančních prostředků.

Práce s obětí

Pachatelé získali důvěru tím, že se vydávali za zaměstnance důvěryhodných institucí, jako jsou banky Česká spořitelna, Raiffeisenbank či Česká národní banka. Pachatelé také poskytli konkrétní detaily, například jméno pracovníka určité společnosti nebo informace o pokusu o půjčku ze strany cizí osoby. Tyto informace na paní Zuzanu působily věrohodně, což mohlo vést k pocitu legitimity. Následný přechod na aplikaci Viber mohl posílit pocit bezpečí a zároveň myšlenku, že pachatelé skutečně chtějí paní Zuzaně pomoci finanční prostředky ochránit.

Prostředky využité pro realizaci podvodu

- **Telefonát.** Podvodníci využili telefonního hovoru ke sdělení, že existuje problém s účtem paní Zuzany, kdy následovalo vyzvání k nainstalování aplikace.
- **Aplikace Viber.** Šlo o zajištění komunikačního prostředku mezi podvodníky a obětí.
- **Bitcoinmat.** Pachatelé paní Zuzanu navedli k bitcoinmatu, kde prostřednictvím QR-kódů vložila finanční prostředky.
- **Falešné identity.** Podvodníci přijali identitu pracovníků různých institucí (banky, bezpečnostní služby), což v paní Zuzaně vzbudilo dojem důvěryhodnosti.

<u>Profil oběti</u>

Zranitelnost paní Zuzany způsobilo několik faktorů:

- **Technologická neznalost.** Přestože paní Zuzana vlastnila elektroniku, například mobilní telefon či počítač, její znalosti ve věci kybernetické bezpečnosti byly omezené.
- **Důvěřivost.** Jakožto seniorka byla zranitelná vůči těmto podvodům, především když se domnívala, že se jedná o pomoc ze strany autorit.
- **Nedostatek kritického myšlení v krizové situaci.** Paní Zuzana jednala pod tlakem velkého varování a tomuto nátlaku podlehla, aniž by se nad situací zamyslela a ověřila si pravost informací.

- **Povědomí o kybernetické bezpečnosti.** Přestože paní Zuzana měla základní povědomí o některých metodách a praktikách, jakými pachatelé postupují a manipulují v rámci kybernetických podvodů, nedokázala je aplikovat v nastalé situaci.
- **Motivace a reakce během podvodu.** Hlavní motivace paní Zuzany zahrnovala ochranu svých finančních prostředků a zabránění zneužití svého účtu. Pod vyvinutým tlakem začala reagovat na instrukce podvodníků. Paní Zuzana byla motivována strachem z možné ztráty peněz a vnitřním pocitem, že podvodníkům může plně důvěřovat.

Dopad na oběť

- **Finanční ztráty.** Po spáchání podvodu paní Zuzana ztratila důvěru ve finanční instituce a v myšlenku, že je schopna ochránit své finanční prostředky.
- **Ztráta důvěry.** Paní Zuzana ztratila důvěru ve finanční instituce.
- **Existenční problémy.** Finanční ztráta měla za následek existenční problémy, které vyústily v nutnost opustit nájemní byt v Praze.
- **Pocit zahanbení a bezmoci.** Pocity studu z vlastní zranitelnosti, a především z toho, že paní Zuzana byla podvedena.

Právní aspekty

- **Trestný čin.** Jedná se o podvod podle § 209 trestního zákoníku, kdy pachatelé využili lži a podvodné praktiky, aby získali finanční prostředky oběti. Podvodníci jednali v úmyslu získat pro sebe finanční prospěch na úkor důvěřivé oběti, paní Zuzany.
- **Důkazy.** Důkazní materiál má podobu telefonních čísel, z nichž pachatelé volali, konverzace v aplikaci Viber, a také stvrzenek z bitcoinmatu.
- **Kroky podniknuté policií a šance na dopadení pachatelů.** Policie obdržela oznámení a byly jí poskytnuty výše uvedené důkazní materiály, které mohou pomoci k identifikaci pachatelů. Pravděpodobnost dopadení je však vzhledem k velké míře anonymity nízká.

Preventivní opatření

- **Prevence podobných případů.** V tomto případě by prevence měla být zaměřena na vzdělávací programy pro seniory se zaměřením na kybernetickou bezpečnost, informování o rizicích podvodů i to, jak se chránit před neznámými telefonáty a e-maily.
- **Důležitost osvěty a vzdělávání seniorů.** Osvěta je nezbytná pro zvýšení povědomí mezi seniory. Programy, které učí seniory o nebezpečí různých podvodů,

například phishingu, mohou pomoci snížit počet obětí. Kurzy kybernetické bezpečnosti by měly být dostupnější a více zaměřené na praktické rady, jak se podvodům vyhnout, a zároveň by měly umět nastínit, jak takový podvod vypadá.

- **Zlepšení bankovních procesů.** Banky by měly zlepšit ověřovací mechanismy při online transakcích, například zavedením vícefaktorových ověření pro finanční operace, aby se snížila možnost podvodu.

8.5 Detailní analýza případové kazuistiky č. 2

Modus operandi pachatelů

Využité techniky manipulace vůči oběti

Pachatelé využili metody falešného investičního podvodu, který se zakládal na následujících manipulativních taktikách:

- **Využití důvěryhodné identity.** Pachatelé se vydávali za finanční poradce, aby působili profesionálně. Též s obětí hovořili plynně česky, což zvýšilo důvěryhodnost pachatelů.
- **Užití psychologické manipulace.** Pachatelé přesvědčovali oběť, že investice do kryptoměn je snadný způsob rychlého zisku. Prezentovali nepravé grafy a falešné zisky, čímž v oběti vyvolali dojem úspěšné investice.
- **Postupné navyšování vkladů.** Po prvním vkladu pachatelé využili principu „sunk cost fallacy“ (tzv. klam ztracených nákladů), kdy oběť nechce přijít o již investované peníze, a proto investuje dále.
- **Vytváření nátlaku a falešných příležitostí.** Pachatelé předstírali růst investice a tlačili oběť k dalším vkladům. Nabídka kurýrní služby k předání hotovosti měla zamezit možnosti zpětného vystopování platby.

Práce s obětí

Pachatelé používali odbornou terminologii, odkazovali se na fiktivní „spokojené zákazníky“ a podpořili důvěryhodnost falešnými grafy. Nechali oběť na počátku dosáhnout „falešného zisku“, čímž ji utvrdili v tom, že investice funguje. Neustále byli s obětí v kontaktu a budovali vztah založený na zdánlivé profesionalitě i ochotě pomoci.

Prostředky využité pro realizaci podvodu

- **Internetová reklama.** Získání pozornosti oběti prostřednictvím klamavé investiční nabídky.
- **Telefonická komunikace.** Profesionálně vedené hovory se snahou manipulovat a přesvědčit oběť.
- **Bitcoinmat.** Anonymní a nevratný způsob převodu finančních prostředků.
- **Kurýrní služba.** Osobní převzetí hotovosti, což znemožnilo zpětné sledování platby.

Profil oběti

Co způsobilo zranitelnost oběti?

- Nedostatečné povědomí o kybernetických podvodech a rizicích spojených s investicemi do kryptoměn.
- Psychologický efekt předchozích investičních úspěchů (falešné výnosy).
- Důvěřivost a tendence věřit autoritám, zejména finančním poradcům.
- Přesvědčení, že investice nemůže být podvod.
- Minimální znalosti ohledně fungování kryptoměn a investic.
- Motivace oběti ke zhodnocení úspor a vidina finančního zisku.

Dopad na oběť

- **Finanční ztráty.** Celková ztráta dosáhla částky 1 270 600 Kč, což zásadně ovlivnilo finanční situaci oběti.
- **Ztráta důvěry.** Nejen vůči investičním společnostem, ale i vůči sobě samému a vlastnímu úsudku.
- **Pocit hanby a viny.** Oběť se může obviňovat, že podvod neprohlédla dříve.
- **Existenční problémy.** V závislosti na jeho celkové finanční situaci mohlo dojít ke ztrátě stability a nutnosti omezit životní standard.

Právní aspekty

- **Trestný čin.** Jedná se o podvod podle § 209 trestního zákoníku. Pachatelé mohli jednat jako organizovaná skupina, což zvyšuje závažnost trestu.

- **Důkazy.** Telefonní záznamy a čísla, z nichž podvodníci volali. Záznamy z bitcoinmatu a bankovních transakcí. Svědectví poškozeného a popis kurýra. Případné kamerové záznamy z místa předání finančních prostředků.
- **Kroky podniknuté policií a šance na dopadení pachatelů.** Šetření se zaměřuje na sledování transakcí, ale vzhledem k anonymitě kryptoměnových plateb je šance na dopadení pachatelů nízká. Pokus o identifikaci kurýra.

Preventivní opatření

- **Prevence podobných případů.** Důležitost osvěty seniorů a důsledné informování o rizicích online investic. Dále je důležité klást důraz na kritické myšlení, a to tak, že je třeba seniory naučit ověřování investičních příležitostí. Také je potřeba zajistit lepší regulace reklam.
- **Důležitost osvěty a vzdělávání seniorů.** Důležitost prevence, jelikož většina seniorů nemá dostatečné znalosti o digitálních hrozbách. Dále větší spolupráce s bankami při informování klientů o podezřelých výběrech velkých částek. Též poskytování kurzů a přednášek, které si kladou za cíl zvýšení povědomí seniorů o rizicích investic a kryptoměn.
- **Zlepšení bankovních procesů.** Zpřísnění regulace online investičních platforem a omezení podvodné reklamy. Zavedení bezpečnostních opatření v bankách při podezřelých transakcích seniorů. Možnost zavedení tzv. ochranné lhůty pro podezřelé investiční transakce, kdy by klient měl čas své rozhodnutí přehodnotit.

8.6 Komparace případových kazuistik č. 1 a č. 2

Oba příběhy vykazují jak společné rysy, tak i určité rozdíly, které pomáhají lépe pochopit mechanismus kybernetických podvodů zaměřených na seniory. Tato analýza shrnuje hlavní podobnosti a rozdíly mezi případy a ukazuje na opakující se vzorce, které pachatelé využívají.

Společné znaky obou případů

Cílová skupina – senioři jako zranitelné oběti

- Oběťmi se stali senioři, kteří byli na základě manipulativního jednání přinuceni k nevratnému odeslání finančních prostředků.

- Senioři jsou zranitelnější z důvodu menšího povědomí o kybernetických podvodech, důvěřivosti a absence zkušeností s moderními technologiemi.
- Obě oběti byly finančně zabezpečené a měly našetřené úspory, což pachatelé dokázali využít.

Použité manipulační techniky

- **Důvěryhodná identita.** Podvodníci se v obou případech vydávali za profesionály (bankéře, finanční poradce).
- **Vytvoření falešného pocitu naléhavosti.** Pachatelé nutili oběti k rychlým rozhodnutím pod tlakem (k převodu peněz „co nejdříve“, k nutnosti vložit „poslední částku“, aby investice fungovala).
- **Psychologická manipulace.** Opakované přesvědčování, že oběť investuje správně a že se jí investice vrátí, nebo naopak že své finanční prostředky ochrání.

Použití moderních technologií k podvodu

- **Využití internetu.** Podvodníci navázali první kontakt prostřednictvím reklamy (u případu č. 2) a telefonátu (v případě č. 1).
- **Kryptoměny jako anonymní nástroj převodu.** V obou případech hrály kryptoměny roli při převodu peněz.
- **Telefonní komunikace jako hlavní prostředek manipulace.** Pachatelé s oběťmi pravidelně telefonovali, vytvářeli pocit důvěry a udržovali psychologický tlak.

Postoj obětí k podvodu a jejich reakce

- **Ztráta důvěry až v pozdní fázi.** Senioři si podvod uvědomili až po finančních ztrátách.
- **Snaha získat peníze zpět.** I po zjištění, že byli podvedeni, se stále snažili peníze „zachránit“.
- **Pozdní oznámení na policii.** V obou případech došlo k ohlášení podvodu až po ztrátě velké finanční částky.

Dopady na oběti

- **Finanční ztráty.** Šlo o částky v řádech tisíců až milionu korun.

- **Psychická újma.** Ztráta sebedůvěry, pocity viny a studu.
- **Existenční problémy.** Snížení životní úrovně kvůli ztrátě úspor.

Rozdíly mezi případy

- **Dynamika podvodu.** První případ měl relativně rychlý průběh, stačil k tomu jeden den, zatímco druhý podvod se odehrával několik měsíců a byl založen na postupném navyšování investovaných prostředků.
- **Celková finanční ztráta.** Oběti v obou případech přišly o významné finanční částky, ale paní Zuzana ztratila „jen“ 302 000 Kč, zatímco pan Novák přišel o 1 270 600 Kč.
- **Dopad na oběť.** V prvním případě oběť čelila bezprostřední existenční krizi, neboť přišla o úspory a musela se vystěhovat z bytu. Ve druhém případě byl dopad především psychologický – pan Novák dlouhodobě věřil, že vydělává, a o to horší pro něj bylo zjištění, že přišel o všechny úspory.
- **Přístup obětí k moderním technologiím.** Paní Zuzana používala technologie pouze omezeně, pan Novák sám aktivně investici chtěl.

Opakující se vzorec podvodu

Prvotní oslovení oběti

- Nečekaná nabídka, která vypadá důvěryhodně (falešná investice, ochrana financí).

Vybudování důvěry

- Dlouhé telefonáty s přátelským a profesionálním přístupem.
- Předstírání odbornosti a poskytování „důkazů“ o legitimitě (např. falešné zisky v druhém příběhu).

Počáteční nižší vklady a jejich navyšování

- V prvním případě seniorka nejprve převáděla nižší částky, než byla přesvědčena k vyššímu převodu.
- V druhém případě oběť chtěla investovat 10 000 Kč, nicméně byla přesvědčena ke 30 000 Kč a následně k dalším vkladům.

Vytvoření nátlaku na oběť

- Neustálé telefonáty a psychologický nátlak.
- Využití psychologických triků („musíte jednat rychle“, „investice právě teď roste“).

Požadavek na další vklad jako okamžik prozření

- Oběti si podvod uvědomily ve chvíli, kdy pachatelé požadovali další vysoký vklad (v prvním případě se jednalo o podezřelý přesun financí, ve druhém o nutnost vložit 30 000 amerických dolarů pro výběr „výnosu“).

<u>Doporučení a preventivní opatření</u>

Pro seniory a širokou veřejnost

- Nikdy neposkytovat přihlašovací údaje a neprovádět podezřelé převody.
- Ověřovat informace u oficiálních zdrojů (např. banky, ČNB, Policie ČR).
- Nedůvěřovat nečekaným telefonátům a lákavým investičním nabídkám.
- Informovat rodinné příslušníky o podezřelých hovorech a nabídce investic.

Pro státní orgány a finanční instituce

- Zajistit větší osvětu seniorů o kybernetických podvodech.
- Přísněji regulovat reklamy na investiční platformy a kryptoměnové služby.
- Zavést povinná bezpečnostní opatření u vysokých bankovních převodů seniorů.

Závěr

Taro bakalářská práce se zabývala problematikou kybernetických podvodů v kybernetickém prostoru páchaných na seniorech v České republice. Vzhledem k rostoucímu trendu digitalizace ve společnosti se kybernetická kriminalita stává stále větším problémem a jejími oběťmi se ve velké míře stávají právě senioři. Práce proto byla zaměřena na analyzování nejen základních pojmů souvisejících s kybernetickou kriminalitou, ale také na druhy kybernetických podvodů, se kterými se senioři potýkají.

V teoretické části byly definovány pojmy jako kybernetická kriminalita, kybernetický prostor a kybernetický útok. Též byly nastíněny jejich vývoj a současná podoba. Poté byla rozebrána typologie pachatelů, jejich metody a motivace, jež používají k manipulaci s oběťmi. Pachatelé kybernetických útoků nezřídka využívají techniky sociálního inženýrství, které si zakládá na psychologické manipulaci, vytváření strachu či tlaku na oběť. Tato metoda se ukázala nejúčinnější právě u seniorů, kteří bývají důvěřivější a méně zkušení v rozpoznávání podvodných taktik.

Specifické kapitoly se zaměřily na nejběžnější formy kybernetických podvodů, jako jsou například phishing, vishing, smishing, bazarové a podvodné mobilní aplikace či falešné e-shopy. Tyto metody bývají pravidelně spojovány s využitím technologií, mezi které patří podvodné hovory či e-maily, což následně ztěžuje dopadení pachatele. Starší generace osob proto v této souvislosti představuje specifickou a rizikovou skupinou, poněvadž obvykle nemají dostatek informací o tom, jak se těmto rizikům účinně bránit.

Část práce tvořilo zkoumání příčin kybernetických podvodů na seniorech, která byla rozčleněna na tři hlavní oblasti – příčiny na straně nabídky, poptávky a faktory dané vývojem situace. Studie odhaluje, že mezi hlavními důvody zvyšujícího se počtu kybernetických útoků se řadí nejen inovace a snadný přístup pachatelů k důvěrným údajům, ale také sociální a psychologické prvky. V souvislosti s tím mohou být sociální izolace seniorů, omezená schopnost objektivně posuzovat informace a slabá úroveň digitálních dovedností výrazně prohloubeny.

V praktické části byly zkoumány dvě skutečné studie kybernetických útoků, které odhalily vzájemně se podobající vzorce chování pachatelů i obětí. Tyto kazuistické analýzy umožnily rozpoznat klíčové znaky podvodů a nabídnout návrh pro ochranná opatření. Výsledky ukázaly, že k nejúčinnějším metodám ochrany seniorů náleží osvěta

a edukace, přičemž v jejich rámci je důležité nejen informovat starší osoby o hrozbách, ale taktéž jim poskytnout užitečné rady, jak se kybernetickým podvodům vyhnout.

Na závěr lze konstatovat, že kybernetickou kriminalitu je třeba chápat jako vážnou hrozbu, která si žádá velkou pozornost a přizpůsobení bezpečnostních opatření. Předcházením rizikovým situacím a jejich včasnou identifikací lze zásadně přispět k úbytku počtu obětí mezi seniory. Zásadní role v prevenci u této citlivé skupiny mají rozvoj znalostí seniorů a také zapojení rodiny, bezpečnostních složek i veřejných institucí. Tato činnost nejenže zachycuje aktuální stav kybernetických podvodů zaměřených na starší osoby, ale nabízí i různé metody, jak jejich přítomnost omezit, prostřednictvím odpovídajících opatření a vzdělávání.

V souvislosti s rychlým vývojem kybernetických hrozeb je nevyhnutelné, aby i dále zesilovaly preventivní programy a aby byl kladen větší důraz na legislativní opatření, která by umožnila pachatele kybernetické kriminality účinněji trestat. Rozšíření vědomostí seniorů o hrozbách v kyberprostoru je zásadní pro ochranu jejich financí i osobních údajů.

Seznam použitých zdrojů

Literární zdroje

1. DONÁT, J., TOMÁŠEK, J. Právo v síti: Průvodce právem na internetu. C.H.Beck, 2016. 352 s. ISBN 978-80-7400-610-4.
2. GŘIVNA, T., POLČÁK, R. Kyberkriminalita a právo. Praha: Auditorium, 2008. 220 s. ISBN 978-80-903786-7-4.
3. HOLOMEK, J., Viktimologia. Plzeň: Aleš Čeněk, 2013. 166 s. ISBN 978-80-7380-446-6.
4. JIROVSKÝ, V. Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada, 2007. 288 s. ISBN 978-80-247-1561-2.
5. KLIMEK, L., ZÁHORA, J., HOLCR, K. Počítačová kriminalita v europskych súvislostech. Praha: Wolters Kluwer, 2016. 448 s. ISBN 978-80-8168-538-5.
6. KOLOUCH, J. Cybercrime. Praha: CZ.NIC, 2016. 524 s. ISBN 978-80-88168-15-7.
7. PETROWSKI, T. Bezpečí na internetu pro všechny. Liberec: Dialog, 2014. 248 s. ISBN 978-80-7424-066-9.
8. SMEJKAL, V. Kybernetická kriminalita. Plzeň: Aleš Čeněk, 2015. 636 s. ISBN 978-80-7380-501-2.
9. SMEJKAL, V. Kybernetická kriminalita. 2. vydání. Plzeň: Aleš Čeněk, 2018. 934 s. ISBN 978-80-7380-720-7.
10. SMEJKAL, V. Kybernetická kriminalita. 3. vydání. Plzeň: Aleš Čeněk, 2022 s. ISBN 978-80-7380-849-5.
11. SMEJKAL, V., SOKOL, T., KODL, J. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Aleš Čeněk, 2019 s. 378 s. ISBN 978-80-7380-765-8.
12. SMEJKAL, V., SOKOL, T., VLČEK, M. Počítačové právo. Praha: C. H. Beck, 1995. 264 s. ISBN 80-7179-009-5.
13. ŠTĚDROŇ, B. a kol. Právo a umělá inteligence. Plzeň: Aleš Čeněk, 2020. 201 s. ISBN 978-80-7380-803-7.
14. ŠULC, V. Kybernetická bezpečnost. Plzeň: Aleš Čeněk, 2018. 147 s ISBN 978-80-7380-737-5.

15. YONAZI, J. J., SEDOYEKA, E., ARIWA, E., EL-QAWASMEH, E. e-Technologies and Networks for Development. Heidelberg: Springer, 2011. 366 s. ISBN 978-3-642-22729-5.
16. ZAVRŠNÍK, A. Kyberkriminalita. Wolters Kluwer, 2017. 148 s. ISBN 978-80-7552-759-2.

Elektronické zdroje

1. Certifikace Manažerských Systémů.cz, Kdo je etický hacker a co je jeho prací [online] [cit. 2024-12-27]. Dostupné na WWW: https://www.cems-cz.com/blog/534-kdo-je-eticky-hacker-a-co-je-jeho-praci
2. CRYPTOGUIDE, Historie kryptoměn/Kompletní časová osa [online]. Poslední aktualizace 05.04.2024 [cit. 2025-02-01]. Dostupné z: https://cryptoguide.cz/historie-kryptomen-kompletni-casova-osa/
3. ČESKÝ STATISTICKÝ ÚŘAD, Informační technologie v domácnostech a mezi jednotlivci [online]. poslední aktualizace 02.02.2024 [cit. 2024-05-11]. Dostupné z: https://www.czso.cz/csu/czso/domacnosti_a_jednotlivci)
4. ENCYCLOPEDIE SOCIÁLNÍCH VĚD. Prevence [online]. [cit. 17. 3. 2025]. Dostupné z: https://encyklopedie.soc.cas.cz/w/Prevence
5. KYBERTEST, Bazarové podvody [online]. [cit. 2025-12-03]. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu/bazarove-podvody
6. KYBERTEST, Podvodné e-maily (phishing) [online]. [cit. 2025-12-03]. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu/phishing-podvodne-e-maily
7. KYBERTEST, Podvodné e-shopy a webové stránky [online]. [cit. 2025-12-03]. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu/podvodne-e-shopy-a-webove-stranky
8. KYBERTEST, Podvodné m-platby [online]. [cit. 2025-12-03]. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu/podvodne-m-platby
9. KYBERTEST, Podvodné mobilní aplikace a udílení oprávnění k aplikacím [online]. [cit. 2025-12-03]. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu/podvodne-mobilni-aplikace-a-udileni-opravneni-k-aplikacim
10. KYBERTEST, Podvodné SMS (smishing) [online]. [cit. 2025-12-03]. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu/smsishing-podvodne-sms-zpravy

11. KYBERTEST, Podvodné telefonáty údajných bankéřů, policistů či investičních poradců (vishing) [online]. [cit. 2025-12-03]. Dostupné z: https://www.kybertest.cz/nejcastejsi-typy-podvodu/vishing-podvodne-telefonaty
12. Legislativa.cz, Kybernetický útok (kyberútok). Definice, typy, následky a prevence [online]. poslední aktualizace 13.09.2022 [cit. 2024-11-07]. Dostupné z: https://legislativa.cz/zdroje/kyberneticka-bezpecnost/kyberneticky-utok
13. MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, Základní definice, vztahující se k tématu kybernetické bezpečnosti [online]. Praha, 2009 [cit. 2024-11-04]. Dostupné z: https://cyber_vyzkum_studie_pojmy.pdf
14. POLICIE ČESKÉ REPUBLIKY, Kyberkriminalita [online]. [cit. 2025-03-12]. Dostupné z: https://policie.gov.cz/clanek/kyberkriminalita.aspx
15. POLICIE ČESKÉ REPUBLIKY, Statistiky kriminalita [online]. [cit. 2025-03-05]. Dostupné z: https://policie.gov.cz/statistiky-kriminalita.aspx
16. PRIMASENIOR. Od kdy je člověk senior? [online]. [cit. 2025-01-12]. Dostupné z: https://www.primasenior.cz/od-kdy-je-clovek-senior/
17. RYCHLOST.CZ. Anonymita na internetu: Je možné zůstat opravdu neviditelný? [online]. [cit. 2024-12-27]. Dostupné z: https://rychlost.cz/clanek/2024-10-anonymita-na-internetu-je-mozne-zustat-opravdu-neviditelny
18. SLOVNÍK CIZÍCH SLOV, Viktimnost [online]. [cit. 2025-01-12]. Dostupné z: https://slovnik-cizich-slov.abz.cz/web.php/slovo/viktimnost
19. WIKIPEDIE, Denial of service [online]. poslední aktualizace 16.12.2024 [cit. 2025-02-07]. Dostupné z: https://cs.wikipedia.org/wiki/Denial_of_service
20. WIKIPEDIE, IP adresa [online]. poslední aktualizace 09.12.2024 [cit. 2024-12-27]. Dostupné z: https://cs.wikipedia.org/wiki/IP_adresa
21. WIKIPEDIE, Kyberpunk [online]. poslední aktualizace 13.10.2024 [cit. 2024-05-11]. Dostupné z: https://cs.wikipedia.org/wiki/Kyberpunk
22. WIKIPEDIE, Phishing [online]. poslední aktualizace 13.10.2024 [cit. 2024-05-11]. Dostupné z: https://cs.wikipedia.org/wiki/Phishing
23. WIKIPEDIE, Ransomware [online]. poslední aktualizace 06.02.2025 [cit. 2025-02-07]. Dostupné z: https://cs.wikipedia.org/wiki/Ransomware
24. WIKIPEDIE, Viktimizace [online]. poslední aktualizace 25.12.2023 [cit. 2025-01-12]. Dostupné z: https://cs.wikipedia.org/wiki/Viktimizace
25. WIKIPEDIE, Viktimologie [online]. poslední aktualizace 25.12.2023 [cit. 2025-01-12]. Dostupné z: https://cs.wikipedia.org/wiki/Viktimologie

26. ČESKO. ZAKONYPROLIDI, Trestní zákoník - § 22 [online]. [cit. 2025-12-15]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
27. ČESKO. ZAKONYPROLIDI, Trestní zákoník - § 25 [online]. [cit. 2025-12-15]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40
28. ČESKO. ZAKONYPROLIDI, Zákon o odpovědnosti mládeže za protiprávní činy a o soudnictví ve věcech mládeže a o změně některých zákonů (zákon o soudnictví ve věcech mládeže) č. 218/2003 Sb. [online]. [cit. 2025-12-15]. Dostupné z: https://www.zakonyprolidi.cz/cs/2003-218
29. ZELINKA, I. Kybernetický prostor – nástrahy, úskalí a hrozby, Národní centrum průmyslu 4.0 [online]. [cit. 2024-11-06]. Dostupné z: https://www.ncp40.cz/aktuality/kyberneticky-prostor-nastrahy-uskali-a-hrozby
30. ZLATUŠKA, J. Kyber není kybernetika, Vesmir.cz [online]. poslední aktualizace 03.11.2016 [cit. 2024-11-06]. Dostupné z: https://vesmir.cz/cz/casopis/archiv-casopisu/2016/cislo-11/kyber-neni-kybernetika.html

Ostatní zdroje

1. MINISTERSTVO VNITRA ČR. Kybernetická kriminalita [online]. YouTube, 04.08.2022 [cit. 2024-11-05]. Dostupné z: https://www.youtube.com/watch?v=4_dFiDX4vpQ

Seznam zkratek

ČR – Česká republika

FOMO – Fear Of Missing Out (strach, že o něco přejdeme)

Sb. – Sbírka zákonů České republiky

SMS – Shot Message Service (krátká textová zpráva)

Tr. Z. – Trestní zákoník (zákon č. 40/2009 Sb.)

apod. – a podobně

Seznam tabulek a grafů