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

BAKALÁŘSKÁ PRÁCE

PHISHINGOVÉ ÚTOKY VŮČI SENIORŮM V OKRESE OPAVA A ROLE POLICIE ČR V JEJICH ODHALOVÁNÍ A PREVENCI

Autor práce: Martin Ligocki, DiS.
Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Vedoucí práce: RNDr. Růžena Ferebauerová
Katedra: Katedra právních oborů a bezpečnostních studií

2026

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: Martin Ligocki
Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Phishingové útoky vůči seniorům v okrese Opava a role Policie ČR v jejich odhalování a prevenci

Název bakalářské práce v anglickém jazyce: Phishing Attacks Against Seniors in the Opava District and the Role of the Czech Police in Their Detection and Prevention

Katedra: Katedra právních oborů a bezpečnostních studií
Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová
Datum zadání bakalářské práce (měsíc, rok): říjen 2025

Cíl bakalářské práce:
Hlavním cílem této práce je vymezit problematiku phishingových útoků zaměřených na seniory v okrese Opava a zhodnotit roli Policie ČR při jejich odhalování a prevenci.
Vedlejším cílem bakalářské práce je na základě dotazníkového šetření vyhodnotit úroveň povědomí seniorů o phishingových hrozbách a navrhnout doporučení, která mohou sloužit Policii ČR i dalším institucím při tvorbě preventivních opatření.

Student: Martin Ligocki, DiS.	31. 10. 2025 *datum*	*podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	6. 11. 25 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	11. 12. 2025 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	11. 12. 2025 *datum*	*podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	20. 12. 2025 *datum*	*podpis*

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

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

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

.....

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

ABSTRAKT

LIGOCKI, M. *Phishingové útoky vůči seniorům v okrese Opava a role Policie ČR v jejich odhalování a prevenci: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2026. 68 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová.

Klíčová slova: kyberkriminalita, phishing, smishing, vishing, IP adresa, phishingové nástroje, vyšetřování, senior

Bakalářská práce se zabývá problematikou phishingových útoků zaměřených na specifickou skupinu seniorů v okrese Opava. V první části bakalářské práce jsou vysvětleny základní pojmy v oblasti kyberkriminality, phishing a jeho specifické metody, jako jsou smishing či vishing. Dále práce poskytuje ucelený přehled o zranitelnosti seniorské populace a preventivních opatřeních, která realizuje Policie ČR a další subjekty v rámci kybernetické bezpečnosti. Součástí práce je i trestněprávní legislativa a procesní postupy Policie ČR při vyšetřování této trestné činnosti. V praktické části práce jsou prezentovány výsledky dotazníkového šetření, jež si kladlo za cíl získat názory a zkušenosti seniorů v okrese Opava s touto problematikou a na jejich základě navrhnout zefektivnění preventivní činnosti v regionu.

ABSTRACT

LIGOCKI, M. *Phishing Attacks Against Seniors in the Opava District and the Role of the Czech Police in Their Detection and Prevention: Bachelor Thesis*. České Budějovice: The College of European and Regional Studies, 2026. 68 pp. Supervisor: RNDr. Růžena Ferebauerová.

Key words: cybercrime, phishing, smishing, vishing, IP address, phishing tools, investigation, senior

The bachelor thesis deals with the issue of phishing attacks targeting a specific group of seniors in the Opava district. In the first part of the thesis, fundamental concepts in the field of cybercrime are explained, along with phishing and its specific methods, such as smishing or vishing. Furthermore, the work provides a comprehensive overview of the vulnerability of the senior population and preventive measures implemented by the Police of the Czech Republic and other entities within the framework of cybersecurity. The thesis also includes criminal legislation and the procedural methods of the Police of the Czech Republic during the investigation of this criminal activity. In the practical part of the work, the results of a questionnaire survey are presented, which aimed to obtain the opinions and experiences of seniors in the Opava district regarding this issue and, based on these findings, to propose more effective preventive activities in the region.

Obsah

Úvod

S dynamickým rozvojem informačních a komunikačních technologií se v posledních desetiletích zásadně proměnil způsob interakce mezi lidmi, přístup k informacím i správa osobních financí. Internet se stal neodmyslitelnou součástí každodenního života, a to napříč všemi generacemi. Zatímco pro mladší generace je pohyb v kyberprostoru přirozeností, pro generaci seniorů představuje online svět nové příležitosti, ale také značná rizika, na která nebyli v průběhu svého aktivního života připravováni.

Právě senioři se v posledních letech stávají jednou z nejvíce ohrožených skupin v oblasti kybernetické kriminality. Důsledky kybernetických útoků na starší občany navíc přesahují rovinu ekonomických ztrát. Ačkoliv jsou finanční škody často fatální a přímo ohrožují existenční jistoty poškozených, neméně závažná je rovina psychologická. Oběti se často potýkají s hlubokým pocitem osobního selhání, ztrátou důvěry ve vlastní schopnosti a následnou stigmatizací ze strany okolí. Tento fenomén vede k postupnému digitálnímu vyloučení, kdy se senioři ze strachu z dalšího napadení zcela stahují z online prostoru, čímž přicházejí o moderní komunikační kanály a prohlubují svou sociální izolaci.

Policie České republiky dlouhodobě sleduje trestné činy v kyberprostoru a z dostupných statistik vyplývá, že počet evidovaných skutků má alarmující vzestupnou tendenci. Tento nárůst je patrný zejména u kyberpodvodů, kam se řadí phishing, smishing či vishing. V současné době se tak kybernetická bezpečnost seniorů stává celospolečenskou výzvou, která vyžaduje koordinovanou součinnost státních orgánů, komerčního sektoru i neziskových organizací. Samotná represe ze strany Policie ČR, byť je nezbytná, nemůže být jediným nástrojem obrany. Důležitým prvkem se stává budování digitální resilience, která propojuje technologické zabezpečení s kritickým myšlením a mediální gramotností. Právě pochopení mechanismů, jakými útočníci manipulují lidským vědomím, a znalost aktuálních trendů v oblasti kybernetického podvodu jsou základními předpoklady pro vytvoření bezpečného prostředí, ve kterém mohou senioři využívat výhody digitálního věku bez neustálého rizika viktimizace.

1 Cíl a metodika bakalářské práce

Hlavním cílem práce je vymezit problematiku phishingových útoků zaměřených na seniory v okrese Opava a zhodnotit roli Policie ČR při jejich odhalování a prevenci. Vedlejším cílem práce je na základě dotazníkového šetření vyhodnotit úroveň povědomí seniorů o phishingových hrozbách a navrhnout konkrétní doporučení, která mohou sloužit Policii ČR i dalším institucím při zefektivňování preventivních opatření v regionu.

Teoreticko-metodická část práce vychází z rešerše aktuálních odborných pramenů, legislativních rámců a statistik týkajících se kybernetické kriminality. Autor v práci kombinuje teoretické vymezení phishingu s analýzou specifické zranitelnosti seniorské populace. Důraz je kladen na faktory, které ze seniorů činí prioritní cíl útočníků, a na systémové postupy Policie ČR při řešení této trestné činnosti.

Součástí empirické části je dotazníkové šetření, jež si klade za cíl zmapovat reálnou situaci v okrese Opava. Pro tyto účely byla zvolena kvantitativní výzkumná metoda formou dotazníkového šetření. Tato metoda byla vybrána pro svou efektivitu při sběru dat od většího počtu respondentů v různých zařízeních pro seniory v okrese Opava a pro možnost následného statistického vyhodnocení získaných údajů. Respondenti byli v úvodu šetření informováni o anonymitě sběru dat, účelu výzkumu a o skutečnosti, že poskytnuté údaje budou využity výhradně pro potřeby této bakalářské práce.

Struktura dotazníku a následná analýza dat byla navržena tak, aby ověřila dvě předem definované hypotézy:

- H1: Většina dotázaných seniorů v okrese Opava se v online prostoru již setkala s podezřelou zprávou (e-mail, SMS), která vykazovala znaky phishingu.
- H2: Senioři jako primární zdroj informací o bezpečnosti na internetu využívají rodinné příslušníky (děti, vnoučata), nikoliv oficiální státní instituce nebo média.

Sběr dat probíhal v období od prosince 2025 do února 2026. Celkem bylo distribuováno 200 dotazníků, přičemž návratnost činila 114 řádně vyplněných tiskopisů. Získaná data byla následně zpracována a výsledky jsou v práci prezentovány formou tabulek a grafů s doprovodným vyhodnocením. Tyto výstupy slouží jako podklad pro

identifikaci mezer v informovanosti a pro formulaci návrhů směřujících ke zvýšení bezpečnosti seniorů v kyberprostoru.

2 Kyberkriminalita

Kyberkriminalitu můžeme z odborného hlediska vymezit jako protiprávní a podvodné jednání osoby nebo skupiny osob, které je konáno prostřednictvím veřejných sítí (internetu), přičemž tyto veřejné sítě slouží jako nástroj k oslovení většího počtu potencionálních obětí, než je tomu při páchání běžných podvodů. Při využití veřejných sítí hraje důležitou roli anonymizace samotného pachatele.[1]

Právní normy jsou v užívání pojmů, které se vážou k trestné činnosti páchané prostřednictvím internetu, často nejednotné. Podle Koloucha[2] bývají v různých odborných pracích i v právních dokumentech často zaměňovány pojmy počítačový trestný čin s počítačovou kriminalitou, kybernetický trestný čin s pojmem kyberkriminalita apod. Správně použitá terminologie však hraje důležitou roli pro vymezení obsahového významu jednotlivých druhů trestné činnosti.

Smejkal ve své publikaci[3] vymezil počítačovou kriminalitu jako páchání trestné činnosti, v níž figuruje počítač jako souhrn hardwarového a softwarového vybavení data nevyjímaje, případně větší množství počítačů samostatných nebo propojených do počítačové sítě, a to buď jako předmět této trestné činnosti, ovšem s výjimkou té trestné činnosti, jejímž předmětem jsou popsaná zařízení jako movité, nebo jako nástroje trestné činnosti. Toto vyjádření však evokuje představu, že počítačová kriminalita se vztahuje pouze na jednání, které využívá osobního počítače a jeho systémů. V současnosti je takovéto označení nedostačující, jelikož pro páchání trestné činnosti využívají pachatelé různé typy zařízení. V soudobé literatuře je proto namísto pojmu počítač užíváno označení informační a komunikační technologie (Information and Communication Technologies, dále jen ICT), popř. trestné činy v ICT, dále pak také computer-related crime a další. V mezinárodní komunikaci je častěji využíváno pojmu kybernetická kriminalita (kyberkriminalita).[4]

Jelikož se informační technologie a jejich využití neustále mění a rozšiřují, nelze pojem kyberkriminalita přesně ohraničit a vymezit. Kyberkriminalita v širším pojetí představuje množinu pro veškerou trestnou činnost, ke které dochází v prostředí informačních a komunikačních technologií. Delikty páchané v rámci této množiny je

[1] KOLOUCH, J. *Cybercrime*. Praha, 2016, s.35.
[2] KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 31-32.
[3] SMEJKAL, V., SOKOL, T.; VLČEK M. *Počítačové právo*. Praha, 1995, s. 99.
[4] GŘIVNA, T, POLČÁK R. *Kyberkriminalita a právo.* Praha, 2008, s. 32.

možno dále třídit a označovat různými pojmy podle různých hledisek.[5] **Mezi nejčastější formy kyberkriminality dle Koloucha[6] patří:**

- neoprávněný přístup k počítačovým systémům,
- krádež a poškozování dat,
- šíření škodlivého softwaru
- kyberpodvody (phishing, scamy, falešné online obchody aj.),
- online stalking a vyhrožování,
- dětská pornografie,
- kybernetické útoky.

Z výše uvedeného vyplývá, že definice kyberkriminality je obtížná a vyžaduje komplexní přístup. Je nutné brát v potaz dynamický vývoj technologií a neustále se měnící modus operandi pachatelů.

2.1 Historie kyberkriminality

Kyberkriminalita má poměrně krátkou, zato velice dynamickou historii. Kořeny sahají do 60. let 20. století. První kyberútoky se zaměřily na mainframy a velké počítačové systémy. Mezi průkopníky patřili hacktivisté (sloučenina slov hacking a activism), kteří zneužívali počítačové systémy zejména pro politické protesty. S rozvojem osobních počítačů v 70. letech 20. století se objevily nové formy útoků a nové hrozby, zejména škodlivé viry a rané formy malwaru. Boom kyberkriminality nastal v 90. letech 20. století v souvislosti s masovou dostupností internetu. Pachatelé začali využívat sofistikovanější nástroje a techniky, objevily se první formy phishingových podvodů, kybernetická špionáž aj.

Počátek 21. století byl charakteristický organizovanou formou kyberkriminality. Do hry vstoupily menší i větší kriminální skupiny a státy začaly rovněž využívat kyberútoky k dosažení různých cílů. Nové formy kyberkriminality (krádež identity, malware aj.) se objevily s rozmachem chytrých telefonů a mobilního internetu. Třetí dekáda 21. století je spojena s hrozbou kyberútoků zejména na kritickou infrastrukturu (elektrárny, nemocnice). Mezi hlavní trendy patří šíření škodlivého softwaru, těžba kryptoměn na cizím zařízení bez souhlasu majitele, šíření falešných audiovizuálních

[5] KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 35.
[6] KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 37-39.

záznamů a mnoho dalšího. Pachatelé neustále modernizují techniky kyberútoků, včetně využití umělé inteligence a strojového učení.

2.2 Vymezení základních pojmů

Kromě vymezení definice a rozdílu mezi počítačovou a kybernetickou kriminalitou, je potřeba v souvislosti s páchání této formy trestné činnosti, vymezit také další pojmy, a to kyberprostor, pachatel, spolupachatel, účastník a oběť.

2.2.1 Internet

Pojem internet, vycházející z anglického spojení interconnected networks, označuje celosvětový systém propojených počítačových sítí. Tato globální infrastruktura integruje lokální sítě, čímž uživatelům zpřístupňuje rozsáhlé spektrum služeb a informačních zdrojů. Kromě okamžitého přístupu k aktuálnímu dění v lokálním i globálním měřítku slouží internet jako platforma pro sebevzdělávání, pracovní činnost, kreativní tvorbu a interaktivní komunikaci. Právě komunikační funkce je klíčovým benefitem, neboť eliminuje geografické bariéry a umožňuje udržování sociálních vazeb bez ohledu na fyzickou vzdálenost. V současnosti tak internet představuje integrální součást každodenního života většiny populace.[7]

2.2.2 Kyberprostor

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) vymezuje kyberprostor jako globální a dynamickou oblast, která je charakterizována vzájemným propojením počítačových, komunikačních a informačních systémů. Jedná se tedy o nekonečnou sdílenou síť počítačů a dalších zařízení. Tato infrastruktura umožňuje neomezený přenos dat a informací. Kyberprostor se stal neodmyslitelnou součástí života, je využíván ve škole, v práci i v osobním životě.

2.2.1 Pachatel

Zákon č. 40/2009 Sb., trestní zákoník (dále jen TrZ) definuje pachatele v § 22 jako osobu, která „svým jednáním naplnila všechny znaky skutkové podstaty trestného činu nebo jeho pokusu či přípravy, je-li trestná. Pachatelem trestného činu je i ten, kdo k provedení činu užil jiné osoby“[8] za podmínek vymezených v § 22 odst. 2 TrZ.

[7] HORSKÁ, B.; LÁSKOVÁ, A. a PTÁČEK, L., V. *Internet jako cesta pomoci: internetové poradenství pro pomáhající profese*. Praha, 2010, s. 18.
[8] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In *Sbírka zákonů, Česká republika.* 2009, částka 11. Dostupné z: <https://app.beck-online.cz>.

Pachatelem trestného činu je tedy fyzická osoba, která splňuje všechny zákonem vymezené znaky, a v době spáchání trestného činu byla schopna posoudit svůj čin a jeho následky (příčetnost), a v době spáchání trestného činu dovršila věk 15 let. Smejkal[9] poukazuje na to, že zejména v oblasti kyberkriminality lze předpokládat, že se pachatelé budou rekrutovat zejména z oblasti mladistvých (15-18 let). Dále uvádí, že s ohledem na věk pachatele se mění také způsob páchání trestné činnosti a motiv. Zjištění motivu je velice důležité jak pro vymezení okruhu podezřelých, tak i pro následnou klasifikaci trestného činu. Pachatelem může být také právnická osoba za podmínek stanovených zákonem č. 418/2011 Sb., Zákon o trestní odpovědnosti právnických osob (dále jen TOPO) a řízení proti nim.

2.2.1 Spolupachatel

TrZ vymezuje také osobu spolupachatele v § 23 takto: „Byl-li trestný čin spáchán úmyslným společným jednáním dvou nebo více osob, odpovídá každá z nich, jako by trestný čin spáchala sama“[10] (spolupachatelé). Spolupachatelé jsou tedy osoby, které se na spáchání trestného činu podílely společně a s úmyslem.

2.2.1 Účastník

Účastníkem na dokonaném trestném činu nebo jeho pokusu je dle § 24 TrZ ten, „kdo úmyslně:

- spáchání trestného činu zosnoval nebo řídil (organizátor),
- vzbudil v jiném rozhodnutí spáchat trestný čin (návodce), nebo
- umožnil nebo usnadnil jinému spáchání trestného činu, zejména opatřením prostředků, odstraněním překážek, vylákáním poškozeného na místo činu, hlídáním při činu, radou, utvrzováním v předsevzetí nebo slibem přispět po trestném činu (pomocník).“[11]

2.2.1 Oběť

TrZ nevymezuje definici oběti, místo toho používá označení poškozený. Oběť je definována v § 2 odst. 2 zákona o obětech trestných činů (dále jen ZOOTČ) takto: “Obětí se rozumí fyzická osoba, které bylo nebo mělo být trestným činem ublíženo na zdraví,

[9] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň, 2015, s. 486.
[10] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In *Sbírka zákonů, Česká republika*. 2009, částka 11. Dostupné z: <https://app.beck-online.cz>.
[11] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In *Sbírka zákonů, Česká republika*. 2009, částka 11. Dostupné z: <https://app.beck-online.cz>.

způsobena škoda nebo nemajetková újma nebo na jejíž úkor se pachatel trestným činem obohatil nebo měl obohatit. ZOOTČ dále v § 2 odst. 4 vymezuje také pojem zvlášť zranitelnou oběť – dítě, senior, fyzicky či mentálně znevýhodněná osoba a další."[12]

Oběti přísluší právo na informace o trestním řízení, na ochranu před druhotnou újmou a také právo obrátit se na specializované organizace.

[12] ČESKO. Zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů). In *Sbírka zákonů, Česká republika*. 2013, částka 20. Dostupné z: <https://app.beck-online.cz>.

3 Phishing jako součást kyberkriminality

Phishing je formou internetového podvodu, při kterém se pachatel snaží získat od potenciální oběti její citlivá data (přihlašovací údaje, údaje ke kreditním kartám), nebo ji rovnou navést k přímému převodu finančních prostředků. Celý útok je založen na důvěřivosti oběti a její časové tísni k ověření pravdivosti a legálnosti.[13] Lance James definuje phishing jako „činnost, kdy je uživateli zaslán padělaný e-mail, který se klamavým způsobem staví do té pozice, že byl odeslán skutečnou finanční institucí ve snaze oklamat příjemce e-mailu tak, aby sdělil své soukromé informace typu čísla platební karty nebo bankovního účtu."[14]

Základním principem phishingu je tedy věrohodné napodobení žádosti o poskytnutí citlivých údajů, nejčastěji formou upozornění zaslaného přes e-mail, SMS, nebo jiné online komunikační prostředky. Zprávy mohou být maskovány tak, aby co nejvíce imitovaly důvěryhodného odesílatele. Součástí těchto podvodných zpráv je zpravidla odkaz, na který má oběť kliknout a který ji přesměruje na stránku dané instituce, kde zadá svá citlivá data. Přesměrování však oběť přesměruje na podvodné stránky pachatele, které jsou k nerozeznání od oficiálních stránek daného subjektu. Pokud oběť zadá svá citlivá data, pachatel je využije ve svůj prospěch.[15]

Rozeznat podvodnou zprávu může být obtížné i pro zkušeného uživatele. **Mezi varovné signály patří:**

- odchylky ve formě e-mailu,
- stylistické a gramatické chyby v textu,
- odlišnosti v doméně dané instituce,
- nezabezpečené odkazy,
- samotný fakt, že daná instituce nikdy od svých uživatelů nepožaduje zadání citlivých údajů tímto způsobem.

Kolouch[16] uvádí, že phishingové útoky je možné provádět i v reálném světě. Ovšem virtuální realita umožňuje pachateli oslovit obrovské množství obětí s minimem námahy. Dále autor přirovnává phishing ke kobercovému bombardování, jelikož cílí na relativně neurčené množství obětí proto, aby měl vyšší naději na úspěch.

[13] INTERNETEM BEZPEČNĚ. *Phishing*. [online]. [cit. 15. 01. 2026]. Dostupné z: <https://www.internetembezpecne.cz/internetem-bezpecne/podvodne-praktiky/phishing/>.
[14] JAMES, L. *Phishing bez záhad*. Praha, 2007, s. 28.
[15] JIRÁSEK, P.; NOVÁK, L.; POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti*. Praha, 2025, s. 137.
[16] KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 246.

Na phishing můžeme dle Koloucha[17] nahlížet jak z širšího, tak užšího úhlu pohledu. Tyto přístupy se neliší podstatou útoku, ale mírou vyžadované interakce. **V širším pojetí** můžeme phishing chápat jako jakoukoli podvodnou aktivitu, která se snaží vylákat od oběti citlivé informace (čísla kreditních karet včetně CVV kódu aj.). Patří sem nejen klasické phishingové e-maily, ale i jiné techniky, jako je spear phishing, smishing, vishing a phishing na sociálních sítích. Základním stavebním prvkem tohoto jednání je vytvoření falešného pocitu důvěry oběti vůči pachateli, manipulace s emocemi a akceptace předem připraveného pachatelova scénáře . Phishing **v užším pojetí** je založen na přímém vyžádání údajů oběti pachatelem, nejčastěji vyplněním formuláře na podvodné stránce.

Phishingový útok můžeme dle Koloucha[18] rozdělit do pěti fází:

1. Fáze plánování, která zahrnuje výběr oběti a metody útoku. V této fázi pachatel vyhodnocuje technické zabezpečení cíle (oběti) a rizika, která mohou být s provedením útoku spojena.

2. Fáze vytváření podmínek, ve které pachatel připravuje technické řešení (datová schránka pro příjem získaných dat, sestavení podvodné zprávy aj.) a vytváří podmínky pro provedení phishingového útoku (seskupení dat o obětech a jejich kontaktní údaje).

3. Fáze vlastního phishingového útoku je zaměřena na rozeslání podvodné zprávy předem připravenému seznamu potencionálních obětí. V této fázi se oběť poprvé setkává s podvodným e-mailem a úspěšnost útoku se odvíjí od informovanosti oběti v rámci phishingové problematiky.

4. Fáze samotného sběru dat je založena na součinnosti oběti, která v prostředí falešné webové stránky zadá a potvrdí svá citlivá data. Tato data jsou automaticky shromážděna a odeslána do datové schránky pachatele.

5. Fáze odčerpání peněžních prostředků zahrnuje činnost pachatele, který využije získaná data k tomu, aby pomocí převodu (zejména na zahraniční účty) odčerpal

[17] KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 246-274.
[18] KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 247-248.

finanční prostředky oběti pomocí různých technik. Tyto odčerpané prostředky se stávají prakticky nevystopovatelnými.[19]

3.1 Historie phishingu

Počátky phishingu datujeme do 70. let 20 století. Autorství pojmu se připisuje Philipovi Zimmanovi, průkopníkovi kryptografie. V tehdejším kontextu se jednalo o fishnet (rybářská síť), metaforu pro shromažďování hesel z nesicherovaných sítí. V 80. letech 20. století pronikl phishing do raných online komunit. V souvislosti s masivním rozvojem internetu v 90. letech 20. století a stoupajícím počtem uživatelů, se phishing stal mnohem rozšířenější formou kybernetických útoků. Pachatelé se v těchto letech zaměřili zejména na zdokonalení technik útoků (využití psychologických triků, manipulace), vzniká cílenější forma zaměřená na specifické osoby a organizace – spear phishing. S nástupem nového milénia se stává phishing globálním fenoménem. Roku 2000 se poprvé objevují útoky s využitím smishingu. Po roce 2010 se otevírají nové možnosti phishingu s využitím sociálních sítí. Dalším přelomovým rokem je rok 2020, kdy s nástupem nových technologií (cloud computing, kryptoměny, mobilní platby) začínají pachatelé využívat nové pokročilé techniky, např. deepfakes (syntetická média, která využívají umělou inteligenci). Phishing se v současnosti (rok 2024) neustále vyvíjí a přizpůsobuje novým technologiím a chování uživatelů. Podvodníci jsou čím dál rafinovanější a jejich útoky mohou být velmi přesvědčivé.

3.2 Trestněprávní ochrana

Snahy o právní regulaci v rámci kyberkriminality (a rámcově phishingu) můžeme vypozorovat již od prvopočátku problémů, které s kyberkriminalitou souvisejí. Jedním z prvních dokumentů, který byl přijat v této oblasti, je Manuál OSN o prevenci a kontrole trestných činů spojených s počítači z roku 2003. Důležitými dokumenty jsou také Úmluva Rady Evropy č. 185, Dodatkový protokol Rady Evropy č. 189 k Úmluvě o kyberkriminalitě a dokumenty EU/ES sloužící k harmonizaci právních úprav při potírání kybernetické trestné činnosti.

V České republice existuje komplexní právní rámec pro boj proti kyberkriminalitě, který zahrnuje jak TrZ, tak i další související zákony:[20]

[19] KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 248.
[20] KOLOUCH, J. *Cybercrime*. Praha, 2016, s. 338.

- Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim
- Zákon č. 141/1961 Sb., o trestním řízení soudním
- Zákon č. 218/2003 Sb., zákon o soudnictví ve věcech mládeže
- Zákon č. 121/2000 Sb., autorský zákon
- Zákon č. 127/2005 Sb., o elektronických komunikacích
- Zákon č. 480/2004 Sb., o některých službách informační společnosti
- Zákon č. 273/2008 Sb., o Policii České republiky
- Zákon č. 89/2012 Sb., občanský zákoník
- Zákon č. 101/2000 Sb., o ochraně osobních údajů
- Zákon č. 14/1993 Sb., o opatřeních na ochranu průmyslového vlastnictví
- Zákon č. 441/2003 Sb., o ochranných známkách
- Zákon č. 527/1990 Sb., o vynálezech, průmyslových vzorech a zlepšovacích návrzích
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce
- Zákon č. 160/1999 Sb., o svobodném přístupu k informacím
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

3.3 Nejčastější formy phishingových útoků

Phishingové útoky se vyskytují v mnoha různých formách s jedním společným jmenovatelem: oklamat oběť a přimět ji k prozrazení citlivých informací nebo provedení akce, která pachateli prospěje. Jednotlivé formy se liší v závislosti na tom, jakým způsobem se pachatel snaží vylákat od oběti citlivé informace. Mezi nejběžnější formy phishingu patří spear phishing, smishing a vishing.

3.3.1 Spear phishing

Spear phishing je založen na stejném principu, jako běžný phishing s tím rozdílem, že je mnohem agresivnější a je vytvořen konkrétní oběti na míru. Pachatel se na něj připravuje mnohem precizněji, cílí na soukromí potencionální oběti a získané informace využije, aby dosáhl svého cíle. Podvodné zprávy jsou postaveny na tom, že přichází od osoby, kterou senior dobře zná, ať už od přátel, či rodinných příslušníků.

Předmětem takovéto žádosti je naléhavá prosba o pomoc, o poskytnutí finančních prostředků aj.[21] Obzvlášť nebezpečnou formou je pak ta, kdy se útočník vydává za osobu na vysoké pozici a žádá přístup k citlivým dokumentům a interním systémům (často podobné technice whalingu).[22]

3.3.2 Smishing

Smishing (spojení slov SMS a phishing) je formou phishingového útoku, který je uskutečňován prostřednictvím SMS zpráv. Pachatel se snaží od potencionální oběti získat citlivé údaje k bankovním účtům, či kreditním kartám. Vyžaduje sdělení a zadání přihlašovacích údajů, hesla, ověření mobilním klíčem, celé číslo karty včetně CVC/CVV kódu, ověření 3D Secure apod.

Princip smishingu spočívá v zaslání SMS zprávy, která se vydává za zprávu bankovní instituce. Součástí této zprávy je odkaz, který příjemce přesměruje na podvodné webové stránky, které jsou k nerozeznání od oficiálních stránek dané instituce.[23]

3.3.3 Vishing

Termín vishing (spojení slov voice a phishing) označuje podvodné telefonáty, prostřednictvím nichž se snaží pachatel získat citlivé údaje od potencionální oběti. Rizikovost tohoto jednání je zejména v tom, že senior je vystaven přímému jednání s pachatelem, který ji zdárně manipuluje. Pachatel je na jednání se seniorem velmi dobře připraven, zná jeho základní údaje (jméno, příjmení, adresu, číslo bankovního účtu) oběti. Díky moderním technologiím si pachatel upraví číslo tak, aby bylo skoro k nerozeznání od čísla napodobované instituce.[24]

Podstatou vishingu je, aby pachatel vzbudil v seniorovi pocit strachu, falešné důvěry a pocitu, že je nutné jednat bez odkladu. Nejčastěji k tomu využívá fiktivní situace související s napadením účtu, podezřelými transakcemi, výhodnými investicemi, ochranou finančních prostředků apod. Při rozhovoru požaduje pachatel po seniorovi sdělení přihlašovacích údajů, ověření identity, čísla platební karty aj.

---

[21] KYBERTEST. *Nejčastější typy podvodů: Phishing, podvodné emaily.* [online]. [cit. 15. 01. 2026]. Dostupné z: <https://www.kybertest.cz/nejcastejsi-typy-podvodu/phishing-podvodne-e-maily>.
[22] ALBRECHT, CH. D. a kol. *Fraud Examination.* 6. vyd. Boston, 2019, s. 591.
[23] KYBERTEST. Nejčastější typy podvodů: *Smishing, podvodné SMS zprávy*. [online]. [cit. 15. 01. 2026]. Dostupné z: <https://www.kybertest.cz/nejcastejsi-typy-podvodu/smsishing-podvodne-sms-zpravy>.
[24] KYBERTEST. *Nejčastější typy podvodů: Vishing, podvodné telefonáty.* [online]. [cit. 15. 01. 2026]. Dostupné z: <https://www.kybertest.cz/nejcastejsi-typy-podvodu/vishing-podvodne-telefonaty>.

4 Postup Policie ČR při prověřování phishingu

Proces prověřování je zahájen podáním trestního oznámení. V praxi je trestní oznámení podáváno nejčastěji na neznámého pachatele. Prvním krokem je zahájení úkonů trestního řízení dle § 158 odst. 3 trestního řádu (dále jen TrŘ), nejčastěji pro přečin podvodu dle § 209 TrZ, přečin neoprávněný přístup k počítačovému systému a neoprávněný zásah do počítačového systému a nosiče informací dle § 230 TrZ a přečin neoprávněné opatření, padělání a pozměnění platebního prostředku dle § 234 TrZ. Dále následuje sepsání úředního záznamu o podaném vysvětlení dle § 158 odst. 6 TrŘ s poškozeným, případně s oznamovatelem.

Následně se dle výpovědi poškozeného provede souhlas s prolomením bankovního tajemství a vyhotoví se usnesení o zajištění výnosů z trestné činnosti dle § 79a odst. 1 trestního řádu, pokud je známo, na jaký bankovní účet vedený u banky v České republice byly finanční prostředky poškozeného odeslány. Po obdržení informací z banky poškozeného se provádí analýza vztahující se k IP adresám, ze kterých neznámý pachatel neoprávněně vstoupil do internetového bankovnictví poškozeného, a dle sdělených informací se zjišťuje, zdali se jedná o dynamickou, či statickou IP adresu a na koho je registrována. Pokud je známo číslo účtu, na který byly finanční prostředky poškozeného odeslány, policejní orgán vyhotoví návrh dle § 8 odst. 2 TrŘ, který zašle příslušnému státnímu zastupitelství, které vydá pokyn bance ke sdělení údajů k majiteli účtu. Je-li známa osoba majitele účtu, je tato vyzvána k podání vysvětlení, zda s osobou poškozeného komunikovala, nebo zda se jedná o dalšího poškozeného v řetězovém trestném činu. Pokud není známo číslo účtu, na který byly finanční prostředky poškozeného odeslány, ke kroku s návrhem na státní zastupitelství není přistoupeno.

V procesu prověřování se dále zjišťují další relevantní informace, které mohou vést k odhalení osoby pachatele (emailové adresy, telefonní čísla, registrace na webových stránkách, sociálních sítích apod.). Jakmile jsou shromážděny veškeré důkazní prostředky proti osobě pachatele (i s negativním výsledkem) a finanční prostředky na účtu příjemce jsou prokazatelně finančními prostředky poškozeného, vydá policejní orgán usnesení dle § 79f odst. 1 TrŘ o zrušení zajištění předmětného účtu a navrácení finančních prostředků poškozenému, případně ponechání finančních prostředků na účtu.

Prověřování této trestné činnosti je nejčastěji ukončeno vydáním usnesení o odložení dle § 159a odst. 5 trestního řádu pro neznámého pachatele, jelikož osoba pachatele se buď skrývá za anonymní IP adresou, či spoofovanými tel. čísly, nebo je

zjištěna IP adresa Ruské federace či Ukrajiny, a pro nízkou škodu poškozeného se nevyžaduje z ekonomických a procesních důvodů mezinárodní spolupráce ke zjištění osoby pachatele.

4.1 IP adresa a postup jejího zjištění

IP adresa funguje jako adresa daného zařízení na internetu. Každé zařízení, které je připojené k internetu, má svou jedinečnou IP adresu. IP adresa se zapisuje pomocí čtyř čísel oddělených tečkami (xx.xxx.x.x), přičemž každé číslo může mít hodnotu od 0 do 255. **Rozlišují se dva hlavní typy IP adres:**

- IPv4 (Internet Protocol version 4): Původní a nejrozšířenější verze, která používá 32bitová čísla.
- IPv6 (Internet Protocol version 6): Nová generace IP adres s 128bitovými čísly, která nabízí mnohem větší prostor pro přidělování adres.

Dále je možné rozdělit IP adresu na veřejnou a soukromou, statickou a dynamickou.

Postup zjištění IP adresy v procesu prověřování se řídí přísnými právními předpisy. **Mezi běžné metody patří:**

- získání IP adresy od poskytovatele internetových služeb (dle § 8 odst. 1 TrŘ, popř. § 88a TrŘ),
- analýza aktivity uživatele, která zahrnuje sledování webových stránek, sledování komunikace s jinými uživateli aj.,
- využití malware,
- získání IP adresy z veřejných zdrojů (např. whois.com).

4.2 Problematika dokazování

Dokazování phishingu v trestním řízení představuje specifickou výzvu, protože phishing je formou kybernetické kriminality, která se zaměřuje na podvodné získávání citlivých informací od uživatelů prostřednictvím podvodných e-mailů, zpráv nebo webových stránek. Smejkal[25] zdůrazňuje fakt, že objekty je možné považovat za důkazy až tehdy, jsou-li akceptovatelné a prokazatelné. Dále autor vymezuje klíčové aspekty

[25] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň, 2015, s. 500.

problematiky dokazování, a to fyzickou vs. logickou přítomnost, čas, čitelnost dat, identifikaci a autentizaci, a v neposlední řadě průkaznost důkazů.

4.2.1 Fyzická vs. logická přítomnost

Virtuální realita (dále jen VR) poskytuje pachatelům mnoho způsobů, jak se anonymizovat, což může být výzvou při dokazování trestné činnosti v tomto prostředí. V rámci VR existují dva hlavní koncepty, které je třeba rozlišit: fyzická přítomnost a logická přítomnost. Fyzická přítomnost se týká skutečného umístění osoby v reálném světě. Při použití VR může být osoba kdekoli, tato přítomnost může být určena pomocí tradičních metod, jako jsou údaje o IP adrese, polohové údaje nebo fyzické vyšetřovací úkony. Logická přítomnost se týká existence a interakce osoby ve virtuálním prostředí, například v online hrách, chatovacích místnostech nebo na sociálních médiích v rámci VR. Osoba může být logicky přítomna v různých virtuálních prostorech současně, přičemž její identita může být skryta nebo anonymizována. Logickou přítomnost může být obtížné vystopovat, jelikož pachatelé mohou používat nástroje pro maskování identity, jako jsou virtuální privátní sítě (VPN), anonymizátory nebo různé účty.

4.2.2 Čas

Dalším aspektem, který znesnadňuje dokazování je určení času. VR je globálním prostředím, ve kterém se mohou uživatelé nacházet v různých časových pásmech po celém světě. Rozdílné časové zóny a nastavení zařízení mohou vést k nesrovnalostem v určení času, což ztěžuje určení přesného časového okamžiku trestného činu. Pachatelé mohou manipulovat s časovými údaji nebo používat falešné časové záznamy k zamaskování svých aktivit. Pro správné určení času trestného činu je často nutné kombinovat časové údaje s událostmi zaznamenanými v různých zdrojích dat. To může zahrnovat analýzu komunikace, pohybu a interakcí v rámci VR a porovnání těchto údajů s časovými záznamy.

4.2.3 Čitelnost dat

Data v kybernetickém prostředí mohou být šifrována nebo kódována, což může znesnadnit jejich čitelnost. Pachatelé mohou používat šifrovací nástroje k ochraně svých komunikací a aktivit před odhalením. Data v prostředí VR a online mohou být uložena v různých formátech, což může zkomplikovat jejich analýzu. Vyšetřovatelé musí být schopni pracovat s různými formáty dat a převádět je do čitelných formátů pro analýzu. Mnoho trestných činů ve VR a kybernetickém prostředí zahrnuje komunikaci

prostřednictvím sociálních sítí nebo aplikací, získání těchto dat je komplikováno právními omezeními (GDPR).

4.2.4 Identifikace a autentizace

Identifikace je proces zjišťování totožnosti osoby. V kybernetickém prostředí se identifikace může provádět na základě IP adres, uživatelských jmen, e-mailových adres, čísla účtu nebo dalších identifikačních údajů. V případě VR se identifikace může týkat virtuálních avatarů, uživatelských účtů a jejich propojení s fyzickými osobami. **Autentizace** je proces ověřování totožnosti osoby, která se snaží přistoupit k systému nebo službě. Tradiční metody autentizace zahrnují uživatelské jméno a heslo, ale v moderním prostředí se využívají také biometrické údaje (např. otisky prstů) nebo dvoufázová autentizace, která v běžném pokusu o nabourání se či odcizení uživatelského účtu může překazit nespočet pokusů.[26] Pachatelé mohou používat anonymizační nástroje, jako jsou VPN (virtuální privátní síť) nebo TOR (software sloužící k anonymizaci internetového připojení), k zakrytí své skutečné identity, což znesnadňuje jejich identifikaci.

4.2.5 Průkaznost důkazů

Aby mohl být pachatel odsouzen, musí být důkazy dostatečné. Aby toto bylo dodrženo, uvádí Smejkal[27] hlavní aspekty, kterým je potřeba se vyhnout:

- nekvalifikované a nejednotné postupy policejních orgánů,
- nedostatečná metodika pro zajištění stop v kyberprostoru,
- zničení stop v průběhu získávání,
- nezachování zkoumaného objektu v původní a nezměněné podobě.

4.3 Metody zajištění peněžních prostředků

V České republice se zajištění peněžních prostředků v trestním řízení řídí trestním řádem (zákon č. 141/1961 Sb., ve znění pozdějších předpisů, dále jen TrŘ). TrŘ stanovuje několik metod, které lze použít k zajištění peněžních prostředků, které by mohly být použity k páchání trestné činnosti nebo k odčinění škody způsobené trestným činem. Mezi nejčastější metody patří zajištění peněžních prostředků na účtu u banky a zajištění náhradní hodnoty.

[26] KOHOUT, R., KARCHŇÁK, R. *Bezpečnost v online prostředí.* Karlovy Vary, 2016, s.15–21.
[27] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň, 2015, s. 502.

4.3.1 Zajištění peněžních prostředků na účtu u banky

Právní úprava zajištění peněžních prostředků na účtech banky (§ 79a odst. 1-5 TrŘ) v trestním řízení představuje klíčový nástroj pro boj proti trestné činnosti. Tento postup umožňuje orgánům činným v trestním řízení účinně zabránit zneužití finančních prostředků pro nelegální účely a zároveň chránit oprávněné zájmy státu a veřejnosti. Nicméně, aby byl tento nástroj efektivní, je důležité, aby byl aplikován v souladu s právními předpisy a s respektem k právům majitelů účtů.

V souladu s platným TrŘ může orgán činný v trestním řízení rozhodnout o zajištění peněžních prostředků na účtu u banky, pokud existuje důvodné podezření, že peníze na účtu jsou spojeny s trestnou činností. Toto zajištění může zahrnovat i peněžní prostředky, které na účet přijdou dodatečně, pokud jsou rovněž spojeny s důvody zajištění. Rozhodnutí policejního orgánu je možné učinit po předchozím souhlasu státního zástupce, pokud se nejedná o naléhavý případ, který nesnese odkladu (§79a odst. 1 TrŘ).

Písemné rozhodnutí o zajištění musí být doručeno bance, u které je účet veden, a poté i majiteli účtu. V rozhodnutí se uvádí číslo účtu a konkrétní peněžní částka, na kterou se zajištění vztahuje. Zajištění se týká peněžních prostředků na účtu v okamžiku doručení rozhodnutí bance, až do výše částky uvedené v rozhodnutí o zajištění. Jakmile je peněžní prostředek zajištěn, je znemožněno jakékoliv nakládání s penězi na účtu až do výše zajištěné částky (§79a odst. 2 TrŘ). Orgán činný v trestním řízení, který rozhodl o zajištění, má povinnost provést všechny nezbytné úkony k výkonu takového rozhodnutí. To zahrnuje kontaktování osob a institucí souvisejících se zajištěnou věcí a koordinaci s dalšími orgány (§ 79a odst.4 TrŘ). Rozhodnutí o zajištění je možné napadnout stížností (§ 79a odst. 5 TrŘ).[28]

4.3.2 Zajištění náhradní hodnoty

Právní úprava zajištění náhradní hodnoty v trestním řízení dle § 79g, TrŘ poskytuje orgánům činným v trestním řízení možnost zajistit hodnoty, které jsou spojeny s trestnou činností. Tento nástroj je důležitý pro efektivní boj proti trestné činnosti a zajištění spravedlnosti. Zároveň je důležité, aby byl tento nástroj používán s respektem k právům osob, které se s ním setkávají. Proto je klíčové, aby postupy zajištění náhradní

[28] ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In *Sbírka zákonů, Česká republika.* 1961, částka 66. Dostupné z: <https://app.beck-online.cz>.

hodnoty byly prováděny v souladu s právními předpisy (§ 79g TrŘ) a s ohledem na individuální situaci dotčených osob.

Zajištění náhradní hodnoty je možné v situaci přesně vymezené v §79g odst. 1 TrŘ, kdy není možné zajistit věc, která je spojena s trestnou činností. V těchto případech lze zajistit náhradní hodnotu, která odpovídá hodnotě (nebo částečné hodnotě) těchto věcí. Při zajištění náhradní hodnoty se postupuje obdobně podle příslušných ustanovení, která upravují zajištění věci spojené s trestnou činností. Tento proces zahrnuje obdobné postupy jako u zajištění původní věci (peněz).

Předseda senátu nebo státní zástupce může na návrh osoby, které byla náhradní hodnota zajištěna, povolit provedení úkonu týkajícího se zajištěné náhradní hodnoty. Toto povolení může být uděleno z důležitých důvodů. Proti rozhodnutí o povolení provedení úkonu je možné podat stížnost, která má odkladný účinek. To znamená, že provedení úkonu bude pozastaveno do vyřízení stížnosti (§ 79g odst. 2 TrŘ).[29]

4.4 Vrácení, vydání a další nakládání s věcmi důležitými pro trestní řízení

Právní úprava vrácení, vydání a dalšího nakládání s věcmi důležitými pro trestní řízení je přesně vymezena v § 80 TrŘ. Poskytuje jasný postup pro zajištění spravedlivého a transparentního nakládání s věcmi, které byly odebrány nebo vydány během trestního řízení.

Věci, které byly vydány nebo odňaty, se vracejí osobám, které je vydaly nebo jim byly odebrány, pokud již nejsou potřebné pro další řízení a nevzniká možnost jejich propadnutí nebo zabrání. Pokud právo na věc uplatňuje jiná osoba, věc se vydá tomu, o jehož právu není pochyb. V případě pochybností se věc uloží do úschovy a osoba, která si na ni činí nárok, je upozorněna, aby svůj nárok uplatnila v občanskoprávním řízení. Pokud byla věc mezitím prodána, nakládá se s částkou za ni strženou podle stejných zásad. Pokud osoba, která má na věc právo, nepřevezme věc přes opakovanou výzvu, bude věc prodána a částka za ni stržená uložena do úschovy soudu. Bezcenná věc se zničí (§ 80 odst. 1 TrŘ). Jestliže hrozí, že se věc, kterou nelze vrátit nebo vydat, zkazí, prodá se a částka za ni stržená se uloží do úschovy soudu (§ 80 odst. 2 TrŘ).

[29] ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In *Sbírka zákonů, Česká republika.* 1961, částka 66. Dostupné z: <https://app.beck-online.cz>.

Rozhodnutí o vrácení a vydání věci, jakož i o uložení do úschovy činí předseda senátu, v přípravném řízení státní zástupce nebo policejní orgán. Proti rozhodnutí je možné podat stížnost, která má odkladný účinek (§ 80 odst. 3 TrŘ).[30]

4.5 Ukončení prověřování

Jak již bylo uvedeno výše, prověřování této trestné činnosti (phishingu) je nejčastěji ukončeno vydáním usnesení o odložení dle § 159a odst. 5 trestního řádu pro neznámého pachatele, jelikož osoba pachatele se buď skrývá za anonymní IP adresou, či spoofovanými tel. čísly, nebo je zjištěna IP adresa Ruské federace či Ukrajiny, a pro nízkou škodu poškozeného se nevyžaduje z ekonomických a procesních důvodů mezinárodní spolupráce ke zjištění osoby pachatele.

[30] ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In *Sbírka zákonů, Česká republika*. 1961, částka 66. Dostupné z: <https://app.beck-online.cz>.

5 Postup Policie ČR při vyšetřování phishingu

Vyšetřování phishingu Policií České republiky se řídí § 160 TrŘ a násl. Postup podle tohoto paragrafu se týká **zahájení trestního stíhání** a obsahuje několik klíčových kroků, které policejní orgán dodržuje při vyšetřování. Postup podle § 160 trestního řádu je klíčovou fází vyšetřování phishingu, kdy se shromažďují důkazy a informace o osobách již obviněných, aby bylo možné přijmout další právní kroky. Osoba se stává obviněnou po vydání usnesení o zahájení trestního stíhání a jejího doručení osobě pachatele. Opis usnesení o zahájení trestního stíhání je třeba doručit obviněnému nejpozději na počátku prvního výslechu a do 48 hodin státnímu zástupci a obhájci (§ 160 odst. 2 TrŘ), pokud si jej obviněný zvolil sám, nebo pokud mu byl ustanoven (nutná obhajoba § 36 TrŘ).[31]

Usnesení o zahájení trestního stíhání je důležitý právní dokument, který vydává orgán činný v trestním řízení při zahájení trestního stíhání proti určité osobě. Usnesení musí obsahovat povinné náležitosti, které zaručují, že obviněná osoba bude správně informována o svých právech a povinnostech, a že bude vyšetřování probíhat v souladu s právními předpisy.

Náležitosti usnesení o zahájení trestního stíhání dle § 160 TrŘ jsou následující:[32]

1. Výroková část:

- obsahuje základní informace o usnesení,
- identifikuje osobu, proti které je zahájeno trestní stíhání, včetně jejího jména, data narození a dalších identifikačních údajů,
- uvádí, z jakého trestného činu je osoba obviněna, s uvedením konkrétních paragrafů trestního zákoníku, které osoba údajně porušila,
- popisuje skutkové okolnosti trestného činu (datum, místo a způsob spáchání trestného činu) i subjektivní složky (úmysl, motiv, jednání pod vlivem omamných látek, v afektu), které mají vliv na posouzení zavinění.

2. Odůvodnění:

- vysvětluje důvody, proč bylo zahájeno trestní stíhání,

[31] ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In *Sbírka zákonů, Česká republika.* 1961, částka 66. Dostupné z: <https://app.beck-online.cz>.
[32] ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In *Sbírka zákonů, Česká republika*. 1961, částka 66. Dostupné z: <https://app.beck-online.cz>.

- uvádí, na základě jakých důkazů nebo informací bylo rozhodnuto zahájit trestní stíhání,
- zdůvodňuje, proč existuje důvodné podezření, že osoba spáchala trestný čin, ze kterého je obviněna.

3. Poučení:

- obsahuje informace o právech obviněné osoby v trestním řízení,
- informuje obviněného o právu na obhajobu a právu zvolit si obhájce,
- zahrnuje poučení o právu vyjádřit se ke všem skutečnostem a navrhnout důkazy,
- informuje o možnosti podat stížnost proti usnesení o zahájení trestního stíhání a o lhůtě pro její podání.

5.1 Výslech obviněného

Výslech obviněného je upraven v § 91 a následujících paragrafech TrŘ a má několik specifických náležitostí, které musí být dodrženy, aby byl výslech veden zákonně a s respektem k právům obviněného.

Náležitosti výslechu obviněného podle TrŘ zahrnují:[33]

- Poučení: před výslechem musí být obviněný poučen o svých právech, zejména o právu nevypovídat a právu na obhájce.
- Právo na obhájce (§ 33 TrŘ), kterého si může obviněný zvolit sám, nebo může požádat o určení obhájce ex offo, nebo se může hájit sám.
- Osobní a majetkové poměry: výše příjmu obviněného, zaměstnání, výdaje obviněného, půjčky, hypotéky, nákladné zájmy, prověření insolvence a exekučních příkazů, vlastnictví hmotných či nehmotných věcí, postoj obžalovaného k uložení případného trestu veřejně prospěšných prací či peněžitého trestu.
- Výslech k dané věci a jeho zaznamenání včetně závěru. Závěrem se rozumí protokol o výslechu obviněného, který je obviněnému přečten nahlas a srozumitelně. Obviněný protokol na závěr stvrdí vlastním podpisem na každé straně protokolu.

[33] ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In *Sbírka zákonů, Česká republika.* 1961, částka 66. Dostupné z: <https://app.beck-online.cz>.

V případě úmyslných trestných činů se z pravidla po provedení protokolu o výslechu obviněného provádějí identifikační úkony, které zahrnují různé metody pro získání a záznam údajů o osobě. Tyto úkony zahrnují biologické odběry, pořizování fotografií, daktyloskopii (otisky prstů) a popis fyzických charakteristik osoby (výška, váha aj.). Shromážděné informace se zaznamenávají do systému Fodagen, což umožňuje efektivnější identifikaci pachatelů a rychlejší nalezení možných podezřelých/obviněných na základě shromážděných dat. Tento proces pomáhá orgánům činným v trestním řízení při vyšetřování a stíhání trestné činnosti.

5.2 Shromáždění znaleckých posudků

Shromáždění znaleckých posudků je jedním z klíčových kroků vyšetřování, který umožňuje orgánům činným v trestním řízení získat odborné názory a informace nezbytné pro rozhodování v dané věci. Orgán činný v trestním řízení může povolat znalce, pokud je to nezbytné pro objasnění skutečností důležitých pro trestní řízení (§ 105 odst. 1 TrŘ)[34]. Znalec je povinen vypracovat znalecký posudek, ve kterém poskytne své odborné stanovisko k otázkám položeným orgánem činným v trestním řízení. Posudek by měl obsahovat podrobné informace o předmětu posouzení, metodách použité analýzy, výsledcích a závěrech znalce (§ 107 TrŘ). Orgán činný v trestním řízení může seznámit obviněného a jeho obhájce s posudkem znalce, aby mohli navrhnout doplňující důkazy nebo klást další otázky. Pokud se znalec nemůže dostavit k výslechu, může být posudek přečten a znalec může být vyzván k dalšímu vysvětlení nebo objasnění svého stanoviska.

5.3 Hodnocení zaměstnavatele

Hodnocení zaměstnavatele pro účely trestního řízení je postup, při kterém může být zaměstnavatel vyzván k poskytnutí informací a záznamů o svém zaměstnanci (obviněném). **Hodnocení zaměstnavatele pro trestní řízení může zahrnovat:**

- poskytnutí pracovního záznamu o výkonu zaměstnance (obviněného), jeho docházce, pracovních úspěších či neúspěších, disciplinárních opatřeních a dalších souvisejících skutečnostech,
- vyjádření k charakteru, povaze a chování obviněného na pracovišti,
- doporučení či hodnocení zaměstnance (slabé a silné stránky).

[34] ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In *Sbírka zákonů, Česká republika*. 1961, částka 66. Dostupné z: <https://app.beck-online.cz>.

Zaměstnavatel by měl s orgány činnými v trestním řízení spolupracovat a poskytnout veškeré potřebné informace v souladu s právními předpisy.

5.4 Zpráva z místa bydliště

Zpráva z místa bydliště je dalším důležitým nástrojem při vyšetřování trestného činu, protože poskytuje orgánům činným v trestním řízení důležité informace o obviněném. Tato zpráva může být využita k získání kontextu a lepšího pochopení pozadí osoby zapojené do trestního řízení.

Zpráva z místa bydliště může obsahovat následující informace:

- sousedské vyjádření (pohled na chování, pověst a rodinné vazby obviněného),
- informace o životním stylu obviněného,
- sociální vazby obviněného (přátelé, osoby stýkající se s obviněným),
- informace o psychickém stavu obviněného a jeho fyzických aktivitách.

5.5 Skončení vyšetřování a prostudování spisu

Podle § 166 TrŘ[35] mají všechny strany trestního řízení právo na prostudování spisu. Toto ustanovení upravuje, kdy a za jakých podmínek mohou obviněný, jeho obhájce, poškozený a další oprávněné osoby získat přístup k vyšetřovacímu spisu. Na možnost prostudovat spis upozorní orgán činný v trestním řízení obviněného, jeho obhájce a poškozeného nejméně tři dny předem (§ 166, odst. 1 TrŘ). Nevyužije-li obviněný, jeho obhájce, poškozený či další oprávněné osoby možnost prostudovat spis, ačkoli byli na tuto možnost řádně a včas upozorněni, učiní o tom policejní orgán záznam do spisu a dále postupuje, jako by k tomuto úkonu došlo (§ 166, odst. 2 TrŘ).

Trestní řád dále vymezuje lhůty pro skončení vyšetřování. Policejní orgán je povinen skončit vyšetřování nejpozději do dvou měsíců od zahájení trestního stíhání, jde-li o věc patřící do příslušnosti samosoudce (§ 167 odst. 1 písm. a) TrŘ), nebo do tří měsíců od zahájení trestního stíhání, jde-li o jinou věc patřící do příslušnosti okresního soudu (§ 167 odst. 1 písm. b) TrŘ).[36] Pokud není vyšetřování ve výše uvedených lhůtách skončeno, musí policejní orgán toto jednání písemně zdůvodnit státnímu zástupci

[35] ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In *Sbírka zákonů, Česká republika.* 1961, částka 66. Dostupné z: <https://app.beck-online.cz>.
[36] ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In *Sbírka zákonů, Česká republika.* 1961, částka 66. Dostupné z: <https://app.beck-online.cz>.

a vymezit lhůtu pro pokračování a ukončení vyšetřování. Státní zástupce může písemným pokynem upravit navrhovaný výčet úkonů i lhůtu pro jejich provedení.

5.6 Návrh na podání obžaloby

Po dokončení vyšetřování a shromáždění důkazů policejní orgán předloží vyšetřovací spis státnímu zástupci s návrhem na podání obžaloby (§ 166 odst. 3 TrŘ). Státní zástupce přezkoumá spis a posoudí, zda jsou důkazy dostatečné pro podání obžaloby soudu.

Návrh na podání obžaloby obsahuje informace o obviněném, trestném činu, ze kterého je obviněn, a důkazech, které jsou k dispozici. Důkazy musí být shromážděny během vyšetřování a musí být dostatečné k prokázání viny obviněného.

Pokud výsledky vyšetřování poskytují dostatečný základ pro postavení obviněného před soud, státní zástupce podá obžalobu a přiloží k ní všechny související spisy a přílohy. Státní zástupce informuje obviněného, jeho obhájce a poškozeného (pokud je známo jejich místo pobytu nebo sídlo) o podání obžaloby. V případě, že je obviněný advokátem, jsou vyrozuměni také ministr spravedlnosti a předseda Advokátní komory. Obžaloba může být podána pouze za čin, pro který bylo zahájeno trestní stíhání podle § 160 TrŘ. Pokud státní zástupce zamýšlí posoudit tento čin jako jiný trestný čin než ten, který posuzoval policejní orgán, musí před podáním obžaloby informovat obviněného a jeho obhájce o zamýšlené změně a zjistit, zda navrhují další vyšetřování s ohledem na tuto změnu (§ 176 TrŘ).

Povinné náležitosti obžaloby dle § 177 trestního řádu:[37]

- označení státního zástupce,
- den sepsání obžaloby,
- jméno a příjmení, datum narození, státní příslušnost a bydliště obviněného,
- zaměstnání obviněného
- hodnost obviněného, pokud se jedná o příslušníka ozbrojených sil a informace o útvaru,

[37] ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In *Sbírka zákonů, Česká republika*. 1961, částka 66. Dostupné z: <https://app.beck-online.cz>.

- žalobní návrh s přesným vymezením skutku, pro který je obviněný stíhán, s uvedením místa, času a způsobu jeho spáchání, popřípadě s uvedením jiných skutečností,
- návrh druhu a výměry trestu, nebo návrh na upuštění od potrestání,
- odůvodnění žalovaného skutku s uvedením seznamu důkazů.

Po podání obžaloby se věc dostává do kompetence soudu, který případ dále projednává a rozhoduje o vině a případném trestu pro obviněného.

6 Zranitelnost seniorské populace v online prostředí

Progresivní digitalizace společnosti integruje informační a komunikační technologie do každodenní rutiny všech generací. Zatímco u mladší populace je digitalizace prakticky stoprocentní, u seniorské skupiny sledujeme kontinuální, avšak pozvolnější nárůst konektivity. Vzhledem k tomu, že dnešní senioři neprošli procesem digitalizace během své školní docházky ani v rané fázi profesního života, vyžadovala adaptace na digitální prostředí značné úsilí a specifický přístup k učení. Navzdory těmto počátečním handicapům internet do života seniorů pronikl natolik, že redefinuje jejich pojetí volného času a otevírá nové možnosti pro seberealizaci, které byly pro předchozí generace seniorů nedostupné.[38]

Zranitelnost seniorů v kyberprostoru je pro jejich **nedostatek technických dovedností** v kombinaci s dalšími faktory značně vysoká. Generace seniorů vyrůstala v době, která podporovala **přirozený respekt k autoritám**, zejména pak k institucím, úředním osobám a bezpečnostním složkám. Útočníci při svém podvodném jednání formou phishingu využívají především strach seniora ze střetu s touto autoritou, apel k poslušnosti a časový nátlak.[39] To vše potlačuje jakékoliv kritické myšlení seniora a vede k tunelovému vidění, kdy se oběť soustředí výhradně na splnění příkazu ve snaze vyhnout se domnělé sankci.

Kromě technologických bariér ovlivňují zvýšenou zranitelnost seniorské populace v kyberprostoru také specifické **psychosociální faktory**. Mezi ty nejvýznamnější řadíme:

- přirozeně vyšší míra důvěřivosti,
- sociální izolace,
- postupný pokles kognitivních funkcí.

Vedle výše uvedeného se útočníci stále častěji zaměřují na zneužití rodinných a interpersonálních vztahů. Tímto způsobem útočník parazituje na silné emocionální vazbě a přirozené potřebě staršího člověka pomoci blízkému v krizové situaci. Mechanismus útoku obvykle spočívá v simulaci naléhavé události, jako je dopravní nehoda či finanční tíseň, do které se měl člen rodiny údajně dostat. Útočník využívá momentu překvapení a vysoké míry stresu, což seniorovi znemožňuje racionální ověření

[38] SAK, P.; KOLESÁROVÁ, K. *Sociologie stáří a seniorů.* Praha, 2012, s. 104.
[39] ČESKÉ DŮCHODY. *Podvody, nástrahy a zákeřnosti na internetu: Vyznejte se v hrozbách pro seniory.* [online]. [cit. 09. 02. 2026]. Dostupné z: <https://ceskeduchody.cz/navody/bezpecne-na-internetu-seniori-podvody-phishing-skodlive-programy>.

identity volajícího. Moderní hrozbu v této oblasti představuje nasazení umělé inteligence, či technologie deepfake, která umožňuje věrnou imitaci hlasu konkrétního příbuzného. Cílem těchto technik je oběť citově paralyzovat a přimět ji k okamžitému převodu finančních prostředků dříve, než stačí situaci konzultovat s okolím.[40]

6.1 Edukace a prevence seniorské populace v kyberprostoru

V éře masivní digitalizace veřejných i soukromých služeb (eGovernment, internetové bankovnictví, elektronické zdravotnictví) se seniorská populace ocitá v paradoxní situaci. Na jedné straně jim technologie nabízejí nástroje k překonání sociální izolace, na straně druhé je vystavují rizikům, na která jejich předchozí životní zkušenost nestačí. Prevence a edukace v této oblasti proto již nemohou být chápány pouze jako izolované předávání technických návodů, ale jako komplexní budování digitální rezilience.

6.1.1 Teoretické vymezení a cíle prevence

Prevenci můžeme definovat jako „souhrn opatření zaměřených na předcházení nežádoucím jevům,“[41] jejichž primárním účelem je eliminace či minimalizace rizik spojených s užíváním informačních a komunikačních technologií. Hlavním cílem prevence v oblasti kyberkriminality je tedy „zabránění trestné činnosti ještě předtím, než k ní dojde.“[42]

V prostředí kybernetické bezpečnosti lze roviny prevence interpretovat následovně:

- **plošná prevence (primární)**, která zahrnuje obecnou osvětu o bezpečném pohybu na internetu, která je určena všem uživatelům bez rozdílu a jejímž cílem je vytvořit prostředí, kde jsou bezpečnostní návyky přirozenou součástí digitální gramotnosti;
- **cílená prevence (sekundární)**, která reaguje na specifické hrozby, kterým čelí konkrétní segmenty populace (v případě seniorů jde o školení

[40] NÚKIB. *Kybernetická bezpečnost: Pomůcka pro seniory*. [online]. [cit. 09. 02. 2026]. Dostupné z: <https://nukib.gov.cz/download/vzdelavani/kurzy/Pomucka-SENIOR.pdf>
[41] MARTANOVÁ, V., B. JANÍKOVÁ, T. DANĚČKOVÁ, et al. *Učební texty ke specializačnímu studiu pro školní metodiky prevence.* Praha, 2007, s. 10.
[42] CHALUPOVÁ, K., ŠTEFUNKOVÁ, M., ŠEJVL, J. *Základy prevence kriminality pro pedagogické pracovníky*. Praha, 2012, s. 11.

zaměřená na konkrétní techniky sociálního inženýrství, které zneužívají jejich důvěřivost či nižší technickou zdatnost);

- **reaktivní prevence (terciární)**, která se soustředí na nápravu škod a práci s osobami, které se již staly obětí kyberpodvodu. Tato fáze je zásadní pro obnovu digitální důvěry a prevenci další viktimizace.[43]

Současná podoba prevence kybernetické kriminality zaměřená na seniorskou populaci v České republice není doménou pouze jednoho sektoru. V souladu s moderními trendy se transformovala do multidisciplinárního modelu, který kombinuje expertní znalosti státních institucí, technologické zázemí bankovního sektoru a terénní zkušenosti neziskových organizací**. Instituce jako NÚKIB a Policie ČR** definují aktuální podoby útoků (např. phishing) a vytvářejí standardizované metodiky. Prevence zde však nepůsobí izolovaně; státní složky poskytují data a odbornou záštitu dalším partnerům, čímž zvyšují legitimitu preventivních sdělení v očích seniorů. **Bankovní sektor** (např. prostřednictvím kybertest.cz) vnáší do prevence prvky interaktivity a praktického nácviku, umožňuje seniorům testovat své reakce v simulovaném a bezpečném prostředí bez rizika reálné finanční ztráty. **Neziskové organizace** se zaměřují na srozumitelnost informací, což je zásadní pro překonávání mezigeneračních bariér a pocitu digitálního vyloučení seniora.

6.1.2 Gerontagogické přístupy v prevenci phishingu

Vzdělávání seniorů v oblasti kybernetické bezpečnosti, konkrétně v ochraně proti phishingu, vyžaduje respektování základních principů obecné gerontagogiky. Edukace v seniorském věku není pouhým předáváním informací, ale procesem, který musí brát v úvahu biologické, psychologické a sociální aspekty stárnutí.

Kalnický[44] uvádí, že pro seniora je zásadní, aby vzdělávání nebylo pouze pasivní teorií. Učení musí být postaveno na konkrétních a smyslově vnímatelných podnětech. V kontextu phishingu se jedná o praktickou analýzu podvodných e-mailů, kde se senior učí rozpoznávat varovné signály (špatná čeština, podezřelá doména) přímo na příkladech z praxe. Dále zdůrazňuje, že edukace seniora musí být v souladu se životními zkušenostmi jedince a jeho aktuálními potřebami. Efektivní metodou je zde přirovnání phishingových útoků k tradičním podvodům, což seniorům usnadňuje pochopení mechanismu manipulace v kyberprostoru. Je nezbytné rovněž vzít v úvahu individuální vzdělávací

[43] CHALUPOVÁ, K., ŠTEFUNKOVÁ, M., ŠEJVL, J. *Základy prevence kriminality pro pedagogické pracovníky.* Praha, 2012, s.15–16.
[44] KALNICKÝ, J. *Obecná gerontagogika.* Opava, 2019, s. 12-31.

možnosti seniorů a jejich specifické tempo učení. Při prevenci phishingu to znamená nespěchat na výsledek, ale umožnit seniorovi opakovanou interakci s materiály, dokud si nevybuduje dostatečnou sebedůvěru v odhalování hrozeb. Vzdělávání seniorů plní i významnou socializační funkci. Skupinová výuka o kyberhrozbách pomáhá seniorům sdílet negativní zkušenosti s podvody, čímž se snižuje jejich pocit stigmatizace a izolace, která z nich často činí snadnější cíle.

7 Praktická část

Praktická část bakalářské práce je založena na vlastním výzkumném šetření, které se zaměřuje na aktuální hrozby v oblasti kybernetické bezpečnosti. Hlavním záměrem je analyzovat úroveň digitální gramotnosti a schopnost kritického posouzení rizik spojených s phishingovými útoky u seniorů. Vzhledem k rostoucí sofistikovanosti podvodných technik je nezbytné identifikovat slabá místa v orientaci této populace, aby bylo možné definovat efektivní preventivní opatření.

Konkrétně je tato část práce zaměřena na zmapování a analýzu úrovně povědomí o phishingu u seniorů v okrese Opava, přičemž se zaměřuje na klienty a návštěvníky domovů pro seniory, klubů seniorů a denních stacionářů. Cílem tohoto šetření je získat relevantní data, která poslouží k hlubšímu porozumění potřebám a zkušenostem této specifické věkové skupiny v daném regionu.

Pro účely empirického šetření byla zvolena kvantitativní výzkumná metoda, realizovaná formou anonymního dotazníkového šetření. Samotný sběr dat probíhal v časovém rozmezí od prosince 2025 do února 2026. Pro zajištění dostatečné průkaznosti bylo do vybraných zařízení v okrese Opava distribuováno celkem 200 dotazníků v tištěné podobě. Tento způsob distribuce byl zvolen s ohledem na specifika cílové skupiny, aby byla zajištěna maximální přístupnost a srozumitelnost pro všechny respondenty.

Účastníci byli v úvodu šetření ujištěni o naprosté anonymitě svých odpovědí a o tom, že poskytnuté údaje budou využity výhradně pro potřeby této bakalářské práce. Z celkového počtu distribuovaných dotazníků se jich vrátilo 114 řádně vyplněných, což představuje 57% návratnost. Tento výsledný vzorek tvoří zkoumaný soubor, který je následně podroben analýze. Získaná data jsou zpracována a interpretována pomocí statistických metod, přičemž pro přehlednou vizualizaci klíčových zjištění jsou v textu využity grafy a tabulky.

7.1 Stanovené hypotézy

H1: Většina dotázaných seniorů v okrese Opava se v online prostoru již setkala s podezřelou zprávou (e-mail, SMS), která vykazovala znaky phishingu.

H2: Senioři jako primární zdroj informací o bezpečnosti na internetu využívají rodinné příslušníky (děti, vnoučata), nikoliv oficiální státní instituce nebo média.

7.2 Vyhodnocení dotazníku

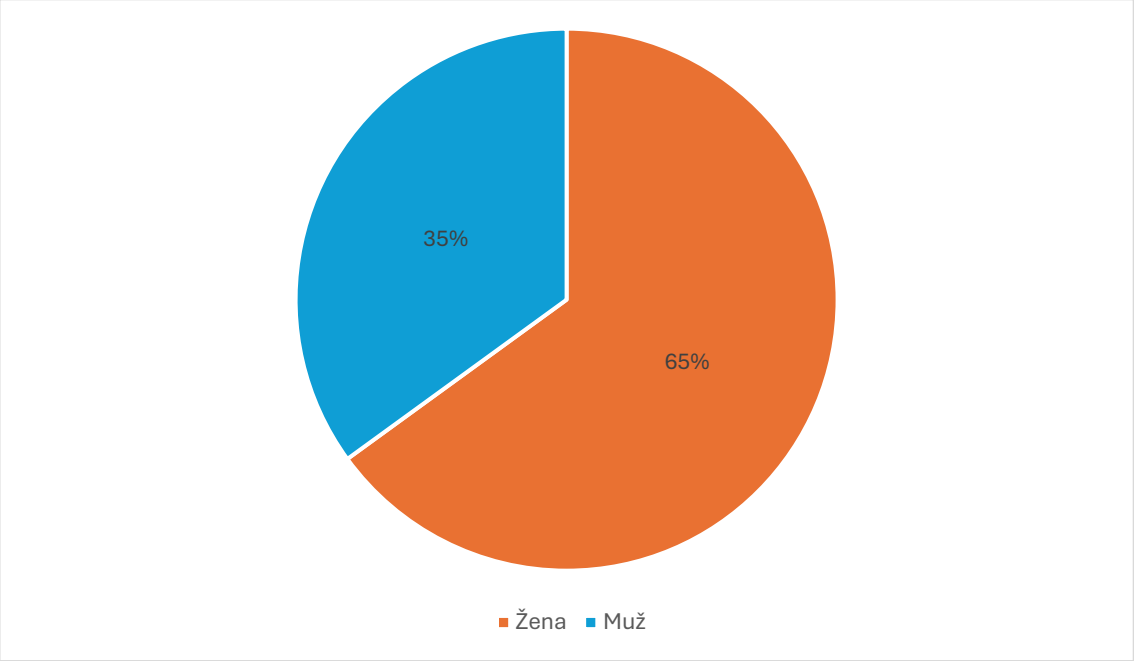
Níže jsou podrobně rozebrány odpovědi na jednotlivé otázky dotazníku, které slouží jako podklad pro následné potvrzení či vyvrácení stanovených hypotéz.

7.2.1 Pohlaví respondentů

Tabulka 1: Otázka dotazníku č. 1: Pohlaví[45]

Možnost	Počet odpovědí	Zastoupení respondentů v %
Žena	74	65
Muž	40	35

Graf č. 1: Otázka dotazníku č. 1: Pohlaví[46]



Zastoupení respondentů podle pohlaví vykazuje převahu žen, které tvoří 65 % zkoumaného vzorku. Na základě tohoto zastoupení však není možné jednoznačně určit, jak pohlaví ovlivňuje povědomí o phishingu nebo zranitelnost vůči němu, protože výsledky mohou být ovlivněny složením návštěvníků seniorských zařízení v okrese Opava, kde šetření probíhalo.

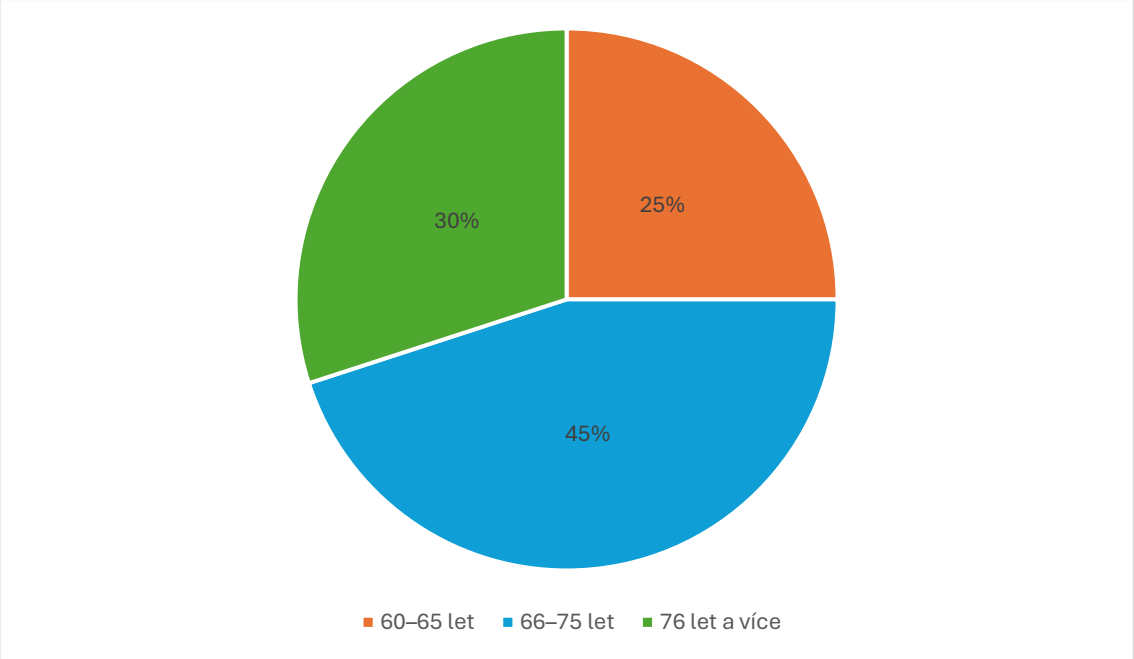
[45] Vlastní zpracování.
[46] Vlastní zpracování.

7.2.2 Věk respondentů

Tabulka 2: Otázka dotazníku č. 2: Věk[47]

Možnost	Počet odpovědí	Zastoupení respondentů v %
60–65 let	28	25
66–75 let	52	45
76 let a více	34	30

Graf č. 2: Otázka dotazníku č. 2: Věk[48]



Z hlediska věkového složení je nejvíce zastoupena skupina respondentů ve věku 66–75 let (45 %). Na základě tohoto rozložení lze usuzovat, že zájem o online prostor je u seniorů v okrese Opava přítomen napříč různými fázemi postproduktivního věku, přičemž výsledky mohou být ovlivněny aktuální mírou soběstačnosti a ochotou zapojit se do šetření v daných zařízeních.

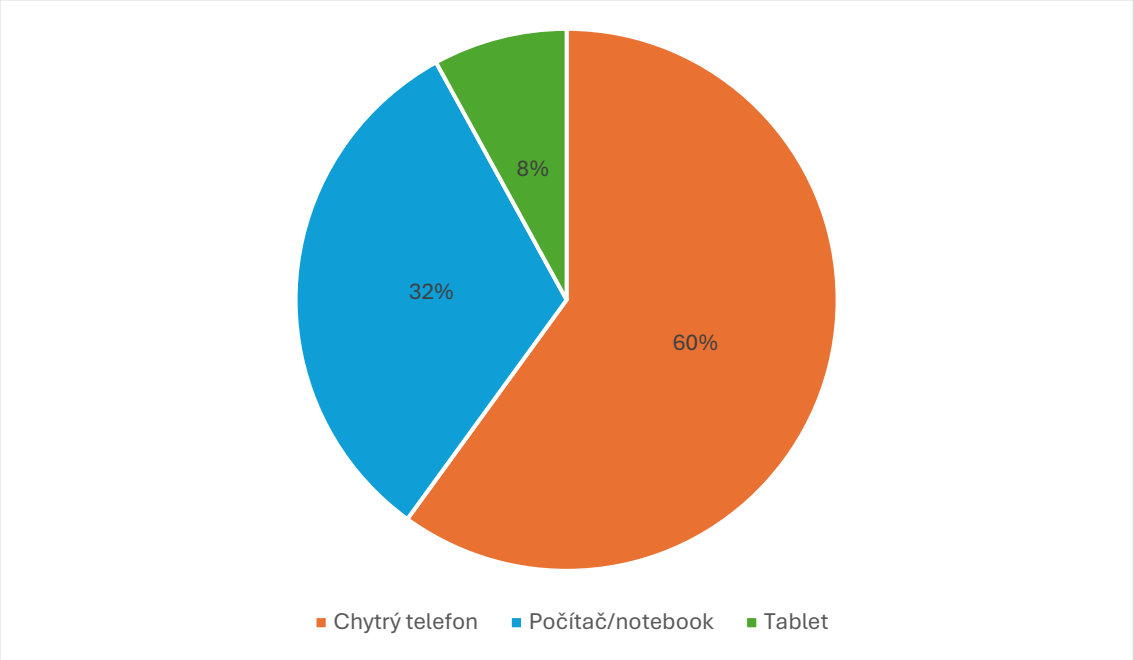
7.2.3 Používané zařízení k přístupu na internet

Tabulka 3: Otázka dotazníku č. 3: Jaké zařízení nejčastěji používáte k přístupu na internet?[49]

Možnost	Počet odpovědí	Zastoupení respondentů v %
Chytrý telefon	68	60
Počítač/notebook	36	32
Tablet	10	8

[47] Vlastní zpracování.
[48] Vlastní zpracování.
[49] Vlastní zpracování.

Graf č. 3: Otázka dotazníku č. 3: Jaké zařízení nejčastěji používáte k přístupu na internet?[50]



Z hlediska preferovaného hardwarového vybavení dominuje u respondentů chytrý telefon (60 %). Na základě tohoto zjištění lze usuzovat, že senioři preferují mobilitu, což však definuje i vektor možného ohrožení skrze mobilní komunikaci. Tato koncentrace na smartphonech naznačuje, že preventivní kampaně by se měly zaměřit především na bezpečnost v mobilním prostředí.

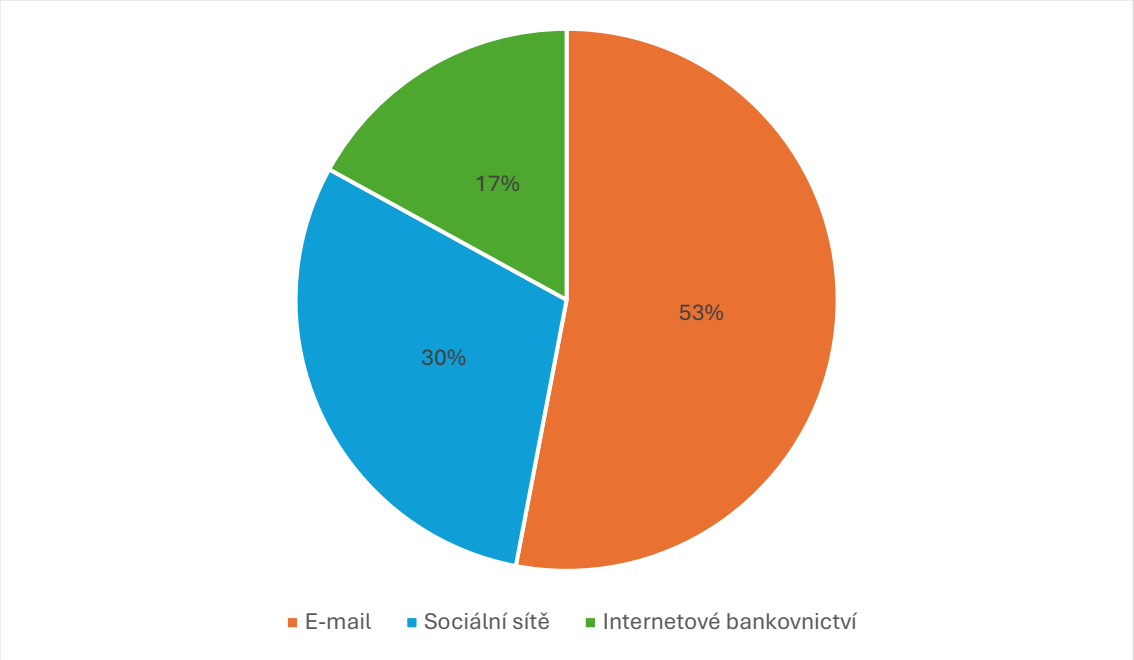
7.2.4 Využívané služby na internetu

Tabulka 4: Otázka dotazníku č. 4: Které služby na internetu využíváte?[51]

Možnost	Počet odpovědí	Zastoupení respondentů v %
E-mail	60	53
Sociální sítě	34	30
Internetové bankovnictví	20	17

[50] Vlastní zpracování.
[51] Vlastní zpracování.

Graf č. 4: Otázka dotazníku č. 4: Které služby na internetu využíváte?[52]



Dominantní službou v online aktivitách seniorů v okrese Opava zůstává elektronická pošta (e-mail), kterou jako svou primární aktivitu označilo 53 % dotázaných. Na základě těchto dat je zřejmé, že e-mailová komunikace představuje pro tuto věkovou skupinu stěžejní komunikační kanál, což ji však zároveň činí hlavním cílem pro phishingové kampaně a podvodné zprávy. Zastoupení sociálních sítí (30 %) a internetového bankovnictví (17 %) pak dotváří profil digitálního chování seniorů a poukazuje na nezbytnost zacílit bezpečnostní vzdělávání nejen na ochranu soukromí, ale také na zabezpečení finančních transakcí.

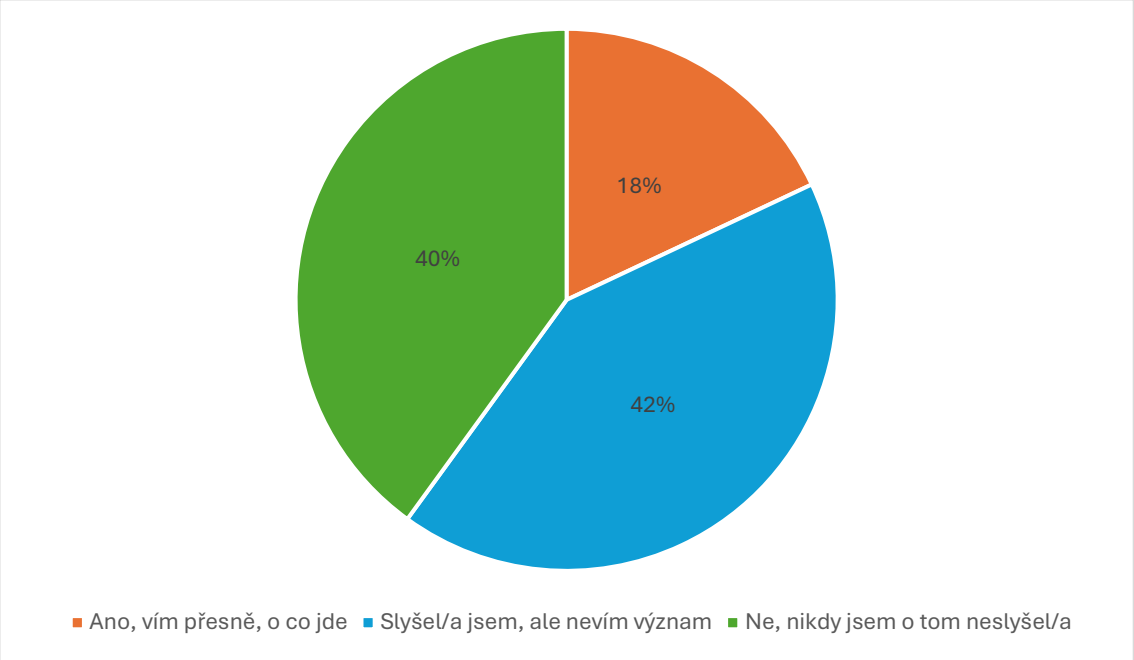
7.2.5 Znalost termínu "phishing"

Tabulka 5: Otázka dotazníku č. 5: Slyšel/a jste někdy termín "phishing" (podvodné zprávy lákající údaje)?[53]

Možnost	Počet odpovědí	Zastoupení respondentů v %
Ano, vím přesně, o co jde	21	18
Slyšel/a jsem, ale nevím význam	48	42
Ne, nikdy jsem o tom neslyšel/a	45	40

[52] Vlastní zpracování.
[53] Vlastní zpracování.

Graf č. 5: Otázka dotazníku č. 5: Slyšel/a jste někdy termín "phishing" (podvodné zprávy lákající údaje)?[54]



Z analýzy povědomí o odborné terminologii vyplývá, že pouze 18 % respondentů má přesnou představu o tom, co termín phishing znamená. Na základě těchto dat lze konstatovat, že u seniorů v okrese Opava převažuje neznalost nebo pouze povrchní povědomí o tomto pojmu, což může v praxi oslabovat jejich schopnost včas identifikovat sofistikovanější podvodné kampaně. Tato skutečnost podtrhuje význam edukačních aktivit, které by se neměly zaměřovat pouze na praktické rady, ale také na vysvětlení základních pojmů, čímž se zvýší celková digitální gramotnost a ostražitost seniorů v online prostředí.

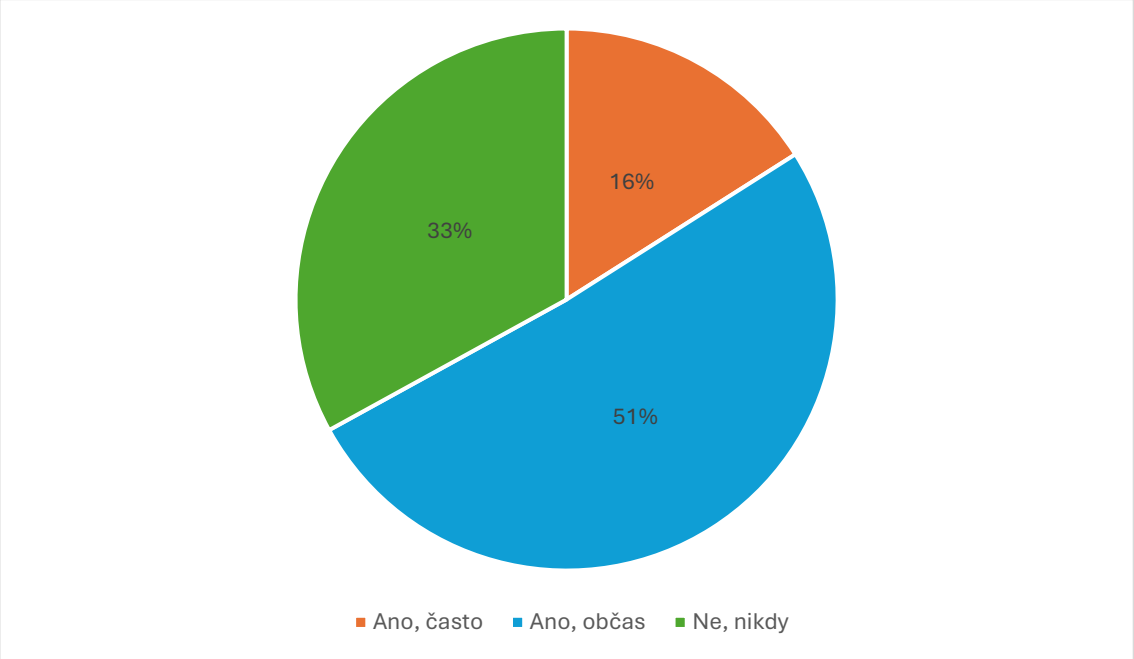
7.2.6 Zkušenost s podezřelou zprávou

Tabulka 6: Otázka dotazníku č. 6: Obdržel/a jste někdy podezřelý e-mail nebo SMS (např. výzva k doplatku, zablokovaný účet v bance, výzva k zaslání peněz rodinnému příslušníku aj.)?[55]

Možnost	Počet odpovědí	Zastoupení respondentů v %
Ano, často	18	16
Ano, občas	58	51
Ne, nikdy	38	33

[54] Vlastní zpracování.
[55] Vlastní zpracování.

Graf č. 6: Otázka dotazníku č. 6: Obdržel/a jste někdy podezřelý e-mail nebo SMS (např. výzva k doplatku, zablokovaný účet v bance, výzva k zaslání peněz rodinnému příslušníku aj.)?[56]



Získaná data ukazují, že zkušenost s pokusem o kybernetický podvod je mezi seniory v okrese Opava velmi rozšířená, neboť celkem 67 % respondentů (součet odpovědí „Ano, často“ a „Ano, občas“) potvrdilo přijetí podezřelé zprávy. Na základě těchto výsledků lze konstatovat, že kyberkriminalita zacílená na starší populaci není ojedinělým jevem, ale běžnou realitou online prostoru.

7.2.7 Reakce na podezřelou zprávu

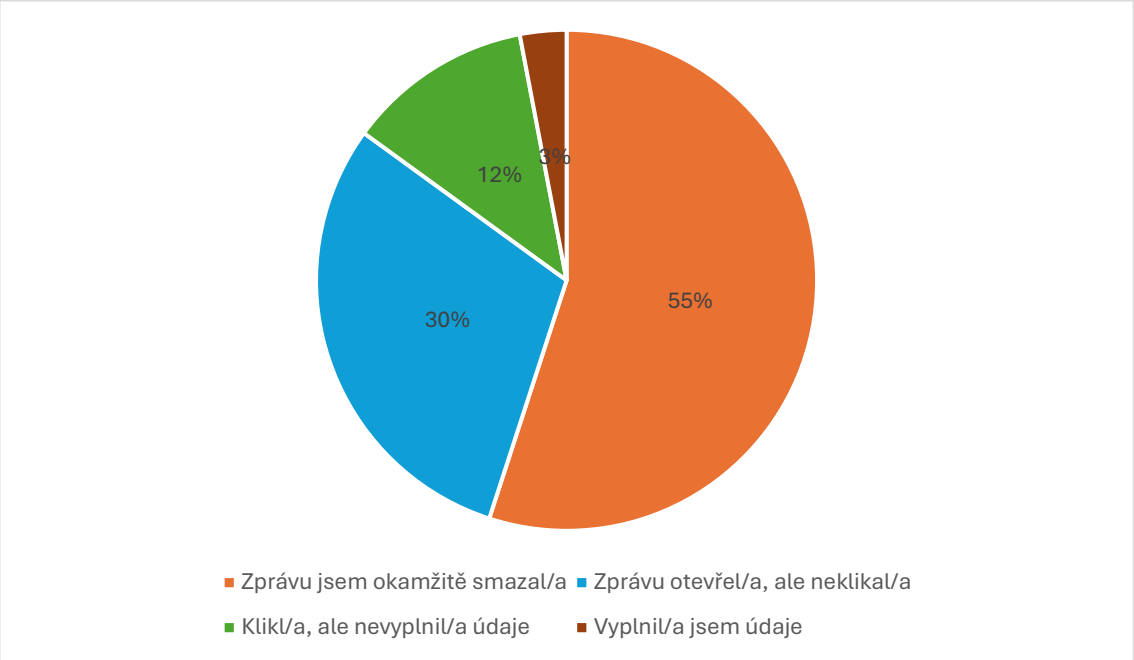
Respondenti, kteří v otázce č. 6 zvolili variantu „Ne, nikdy“ (celkem 38 osob), byli podle pokynů v dotazníku plynule přesměrováni k otázce č. 8, neboť se jich dotaz na konkrétní způsob reakce na podvodnou zprávu bez předchozí zkušenosti netýkal. Na otázku č. 7 tak odpovídalo pouze 76 respondentů, kteří v předchozí otázce uvedli zkušenost s phishingem.

[56] Vlastní zpracování.

Tabulka 7: Otázka dotazníku č. 7: Pokud ano, jak jste na takovou zprávu reagoval/a?[57]

Možnost	Počet odpovědí	Zastoupení respondentů v %
Zprávu jsem okamžitě smazal/a	42	55
Zprávu otevřel/a, ale neklikal/a	23	30
Klikl/a, ale nevyplnil/a údaje	9	12
Vyplnil/a jsem údaje	2	3

Graf č. 7: Otázka dotazníku č. 7: Pokud ano, jak jste na takovou zprávu reagoval/a?[58]



Analýza chování respondentů při přímé konfrontaci s hrozbou ukazuje, že nadpoloviční většina (55 %) postupuje správně a podezřelou zprávu bez interakce smaže. Na základě těchto dat lze však identifikovat také rizikovou skupinu seniorů v okrese Opava, která zprávu minimálně otevře (30 %) nebo na ni dokonce reaguje kliknutím na odkaz či vyplněním údajů (dohromady 15 %). Tento výsledek naznačuje, že i přes existující základní ostražitost je u části seniorské populace stále přítomna tendence k rizikové zvídavosti nebo důvěřivosti, což potvrzuje nutnost zaměřit vzdělávací aktivity na praktický nácvik bezpečné reakce a eliminaci strachu, který útočníci často zneužívají.

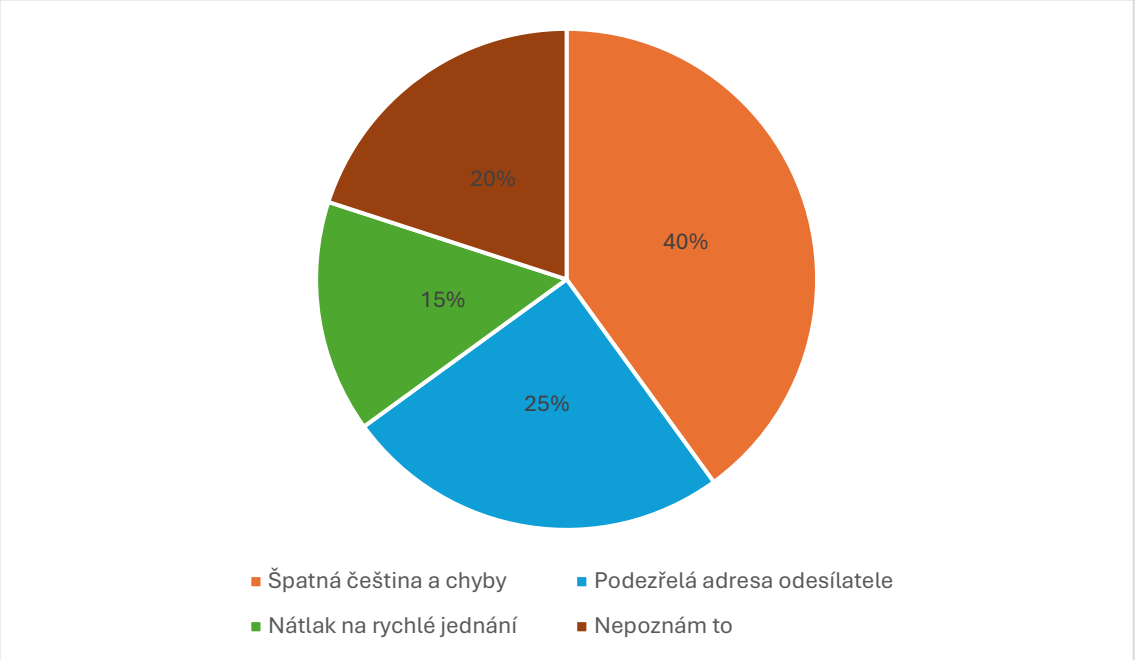
[57] Vlastní zpracování.
[58] Vlastní zpracování.

7.2.8 Rozpoznání podezřelé zprávy

Tabulka 8: Otázka dotazníku č. 8: Podle čeho poznáte, že je e-mail nebo SMS podezřelá?[59]

Možnost	Počet odpovědí	Zastoupení respondentů v %
Špatná čeština a chyby	46	40
Podezřelá adresa odesílatele	28	25
Nátlak na rychlé jednání	17	15
Nepoznám to	23	20

Graf č. 8: Otázka dotazníku č. 8: Podle čeho poznáte, že je e-mail nebo SMS podezřelá? [60]



Z hlediska identifikace podvodných znaků v online komunikaci se ukazuje, že senioři v okrese Opava nejčastěji spoléhají na jazykovou úroveň zprávy, konkrétně na špatnou češtinu a gramatické chyby (40 %). Na základě tohoto zjištění lze usuzovat, že vizuální a lingvistické nedostatky jsou pro tuto cílovou skupinu nejhmatatelnějším indikátorem nebezpečí, což však může být rizikové v kontextu moderních útoků využívajících umělou inteligenci k tvorbě bezchybných textů. Skutečnost, že pětina respondentů (20 %) přiznává neschopnost podvod identifikovat, podtrhuje naléhavost posílení technické ostražitosti a vzdělávání zaměřeného na rozpoznávání sofistikovanějších metod, jako je falšování adres odesílatele nebo zneužívání psychologického nátlaku.

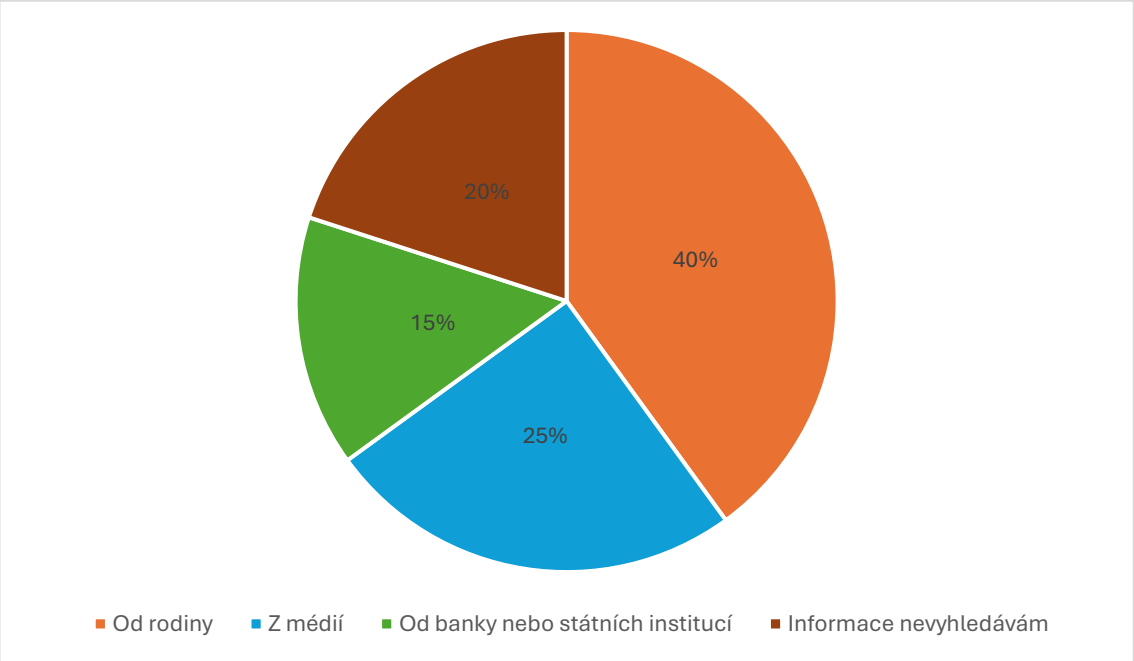
[59] Vlastní zpracování.
[60] Vlastní zpracování.

7.2.9 Zdroj informací o bezpečnosti na internetu

Tabulka 9: Otázka dotazníku č. 9: Kde čerpáte informace o tom, jak se na internetu chránit?[61]

Možnost	Počet odpovědí	Zastoupení respondentů v %
Od rodiny	46	40
Z médií	29	25
Od banky nebo státních institucí	17	15
Informace nevyhledávám	22	20

Graf č. 9: Otázka dotazníku č. 9: Kde čerpáte informace o tom, jak se na internetu chránit? [62]



Z hlediska informačních zdrojů, které senioři v okrese Opava využívají pro svou ochranu v online prostoru, dominuje rodinné zázemí (40 %). Tento výsledek poukazuje na vysokou míru důvěry v mezigenerační předávání zkušeností, avšak zároveň naznačuje potenciální riziko v případě, že mladší generace nedisponují aktuálními odbornými znalostmi. Skutečnost, že pětina respondentů (20 %) informace aktivně nevyhledává, pak definuje prostor pro cílenější preventivní kampaň v regionu, která by měla efektivněji oslovit i ty uživatele, kteří se o kybernetickou bezpečnost proaktivně nezajímají.

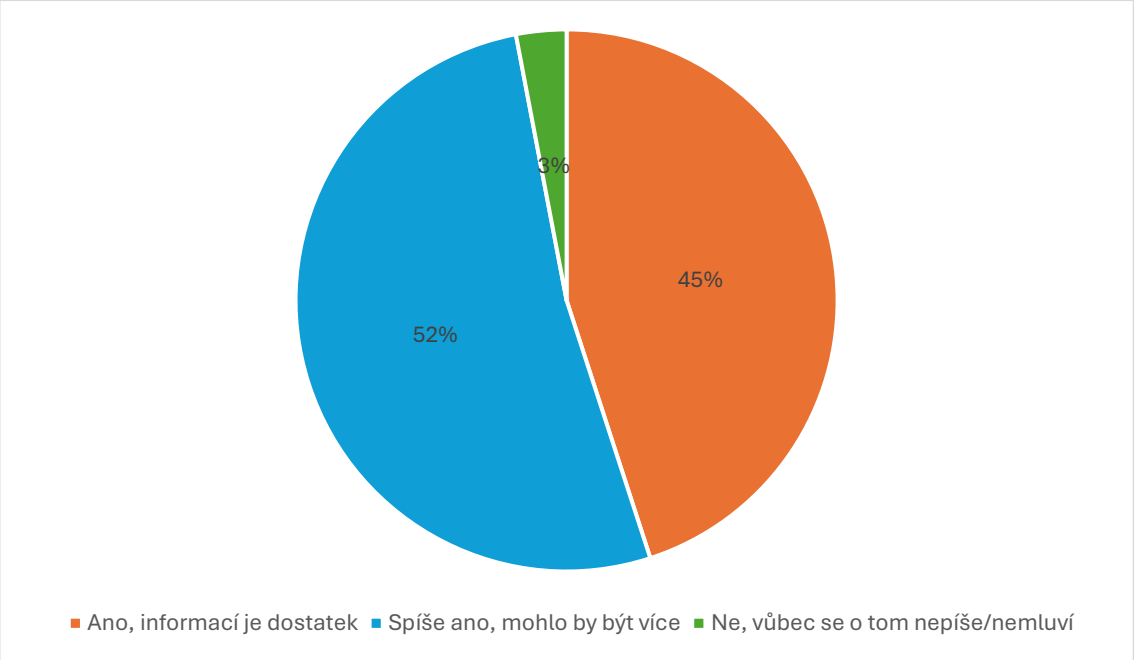
[61] Vlastní zpracování.
[62] Vlastní zpracování.

7.2.10 Dostatečnost informací v okrese Opava

Tabulka 10: Otázka dotazníku č. 10: Považujete informace o podvodech na internetu, které jsou dostupné v okrese Opava (např. v místním tisku, na vývěskách), za dostatečné?[63]

Možnost	Počet odpovědí	Zastoupení respondentů v %
Ano, informací je dostatek	51	45
Spíše ano, mohlo by být více	59	52
Ne, vůbec se o tom nepíše/nemluví	4	3

Graf č. 10: Otázka dotazníku č. 10: Považujete informace o podvodech na internetu, které jsou dostupné v okrese Opava (např. v místním tisku, na vývěskách), za dostatečné? [64]



Hodnocení dostupnosti preventivních informací přímo v regionu Opavska naznačuje, že informační kanály sice fungují, ale jejich intenzita je vnímána jako hraniční. Nadpoloviční většina respondentů (52 %) pociťuje potřebu posílení osvěty, což na základě těchto dat interpretujeme jako volání po konkrétnějších a častějších kampaních v lokálním prostředí. Skutečnost, že pouze zanedbatelná část seniorů (3 %) vnímá naprosté informační vakuum, je pozitivním signálem, nicméně převládající poptávka po rozšíření informovanosti poukazuje na nutnost hledat nové cesty distribuce bezpečnostních sdělení, které by lépe saturovaly potřeby seniorů přímo v místě jejich bydliště.

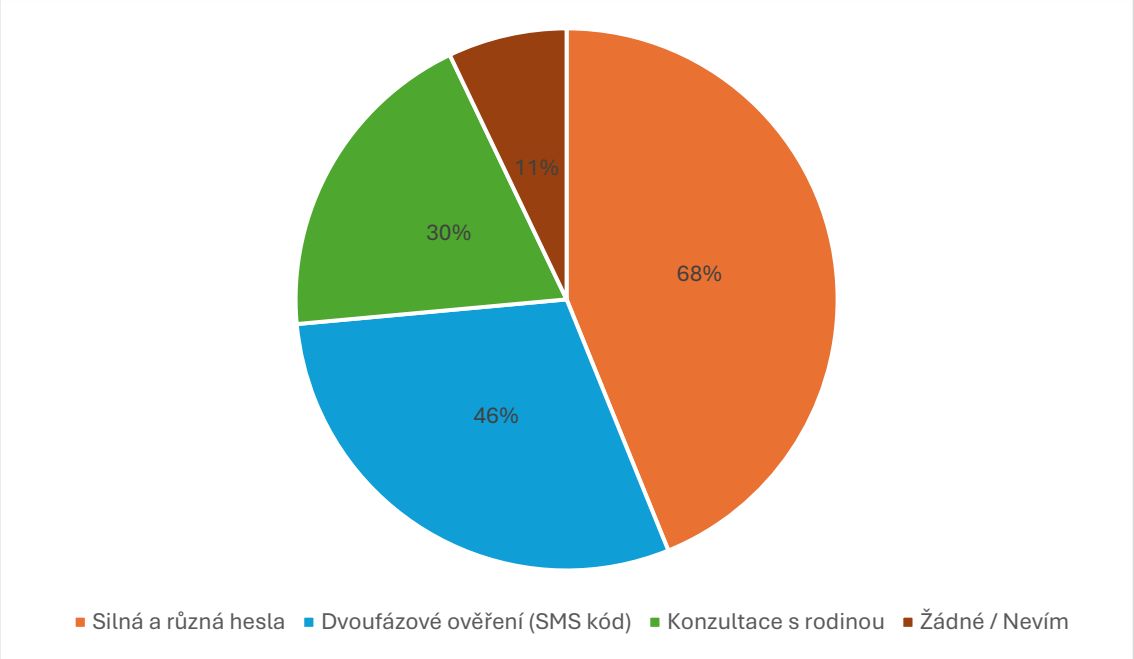
[63] Vlastní zpracování.
[64] Vlastní zpracování.

7.2.11 Používaná bezpečnostní opatření

Tabulka 11: Otázka dotazníku č. 11: Která z následujících bezpečnostních opatření aktivně používáte? (Možno zaškrtnout více)[65]

Možnost	Počet odpovědí	Zastoupení respondentů v %
Silná a různá hesla	78	68
Dvoufázové ověření (SMS kód)	52	46
Konzultace s rodinou	34	30
Žádné / Nevím	12	11

Graf č. 11: Otázka dotazníku č. 11: Která z následujících bezpečnostních opatření aktivně používáte? (Možno zaškrtnout více)[66]



Součet relativních četností je vyšší než 100 %, neboť respondenti mohli v této otázce zvolit více variant současně.

Z analýzy reálného chování seniorů v oblasti zabezpečení vyplývá, že nejrozšířenějším opatřením je konzultace s rodinnými příslušníky, kterou využívá 68 % respondentů. Na základě těchto dat lze usuzovat, že sociální kontrola a důvěra v blízké osoby hrají v kybernetické bezpečnosti seniorů na Opavsku zásadnější roli než samotné technické nástroje. Ačkoliv 46 % respondentů uvádí používání silných hesel a 30 % využívá dvoufázové ověření, stále existuje významná část populace, která se spoléhá

[65] Vlastní zpracování.
[66] Vlastní zpracování.

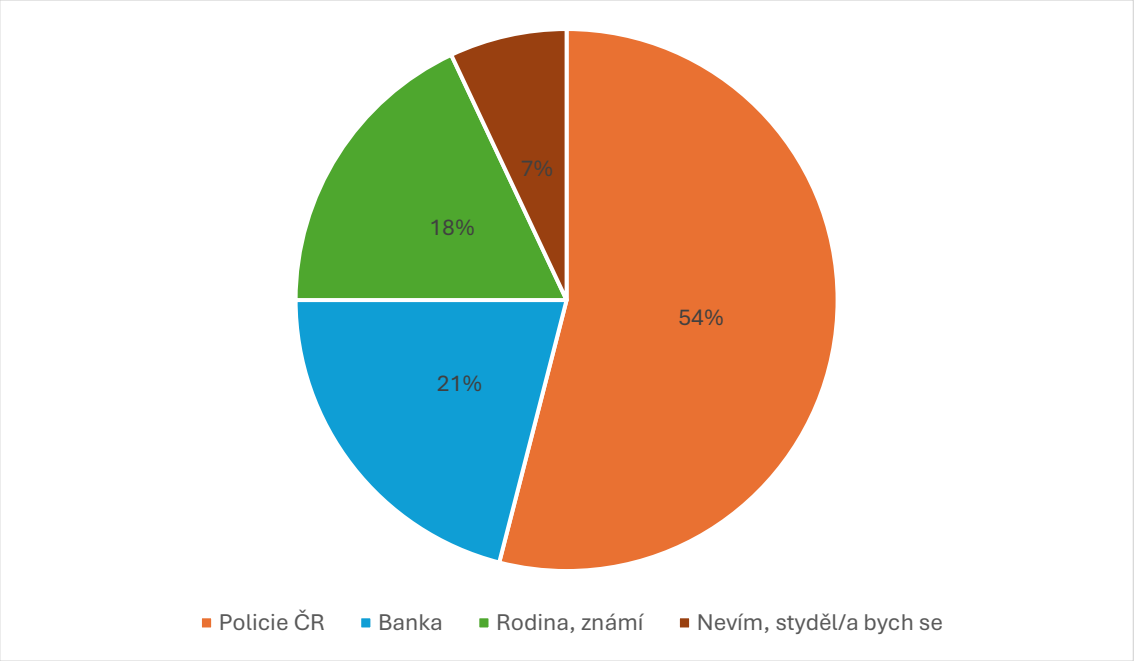
výhradně na subjektivní posouzení situace nebo nepoužívá žádné ochranné prvky. Tato diverzita v přístupech zdůrazňuje potřebu vzdělávání, které by propojilo technické dovednosti s rodinnou podporou.

7.2.12 První kontakt při oběti podvodu

Tabulka 12: Otázka dotazníku č. 12: Pokud byste se stal/a obětí podvodu (přišel/la o peníze nebo přístup k účtu), na koho byste se obrátil/a jako na prvního?[67]

Možnost	Počet odpovědí	Zastoupení respondentů v %
Policie ČR	62	54
Banka	24	21
Rodina, známí	20	18
Nevím, styděl/a bych se	8	7

Graf č. 12: Otázka dotazníku č. 12: Pokud byste se stal/a obětí podvodu (přišel/la o peníze nebo přístup k účtu), na koho byste se obrátil/a jako na prvního? [68]



Z analýzy krizového rozhodování vyplývá, že nadpoloviční většina seniorů v okrese Opava (54 %) vnímá jako primární instanci pro řešení kybernetického podvodu Policii ČR. Na základě tohoto zjištění lze usuzovat, že v této věkové skupině stále přetrvává vysoká důvěra v represivní složky státu, zatímco role banky jako prvního kontaktu je s 21 % vnímána jako sekundární. Tento výsledek naznačuje potřebu edukace

[67] Vlastní zpracování.
[68] Vlastní zpracování.

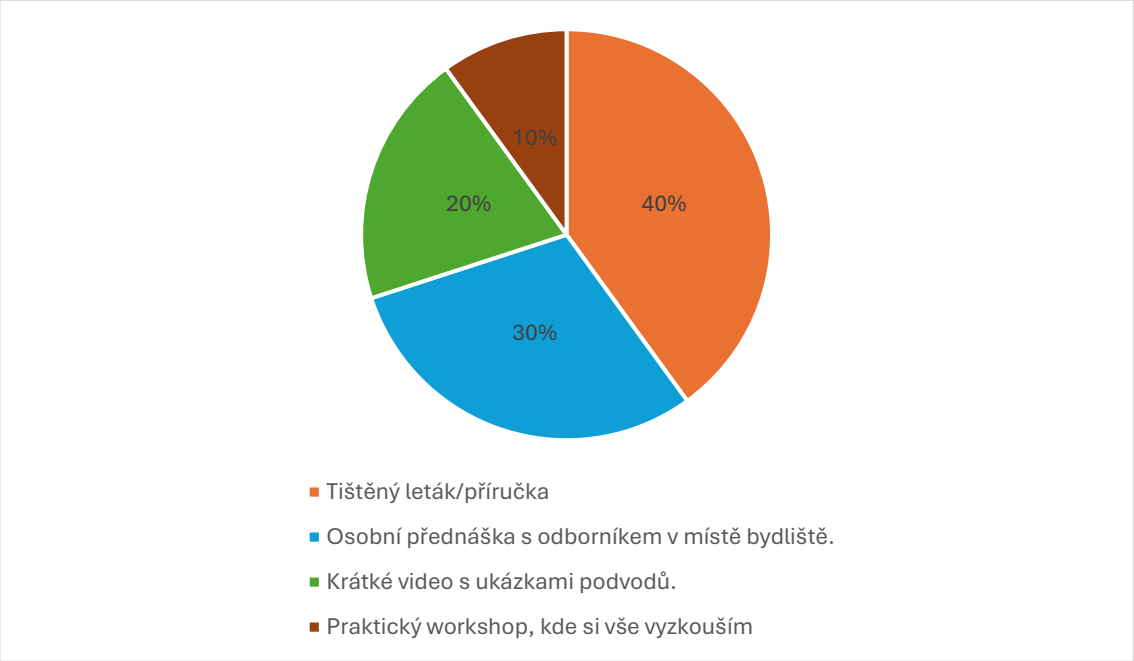
směrem k okamžité blokaci účtů, kde je banka rychlejším řešením než podání trestního oznámení. Pozitivním faktem zůstává, že pouze 7 % respondentů by se stydělo situaci nahlásit, což vyvrací obavy z masivní latentní kriminality způsobené pocitem osobního selhání u starší generace v regionu.

7.2.13 Preferovaná forma vzdělávání a prevence

Tabulka 13: Otázka dotazníku č. 13: Jakou formou byste se chtěl/a dozvědět více o bezpečnosti na internetu?[69]

Možnost	Počet odpovědí	Zastoupení respondentů v %
Tištěný leták/příručka	46	40
Osobní přednáška s odborníkem v místě bydliště.	34	30
Krátké video s ukázkami podvodů.	23	20
Praktický workshop, kde si vše vyzkouším	11	10

Graf č. 13: Otázka dotazníku č. 13: Jakou formou byste se chtěl/a dozvědět více o bezpečnosti na internetu?[70]



Analýza preferencí v oblasti dalšího vzdělávání ukazuje, že senioři v okrese Opava upřednostňují tradiční informační kanály, kdy 40 % respondentů zvolilo tištěný leták či příručku jako nejvhodnější formu osvěty. Na základě tohoto zjištění lze konstatovat, že fyzická dostupnost informací, které si uživatel může v klidu prostudovat,

[69] Vlastní zpracování.
[70] Vlastní zpracování.

hraje v této věkové kategorii stále klíčovou roli. Zájem o osobní přednášky (30 %) a videa (20 %) pak naznačuje potřebu kombinovat pasivní příjem informací s názornými ukázkami. Nízký zájem o praktické workshopy (10 %) může pramenit z určitého ostychu nebo obavy z vlastní technické neobratnosti, což by mělo být zohledněno při návrhu preventivních strategií, které by měly být především srozumitelné, neodrazující a snadno dostupné.

7.3 Vyhodnocení stanovených hypotéz

Na základě analýzy získaných dat a interpretace výsledků dotazníkového šetření lze konstatovat, že senioři v okrese Opava vykazují specifickou úroveň digitální gramotnosti, která je úzce spjata s jejich sociálním zázemím a dostupností technologií. Výsledky odhalují, že zkoumaný vzorek respondentů se aktivně zapojuje do online komunikace, avšak míra jejich reálného bezpečí je často podmíněna spíše intuitivním jednáním a důvěrou v blízké osoby než systematickými technickými znalostmi. Hodnocení dat naznačuje, že i přes rostoucí zkušenost s kybernetickými hrozbami zůstává tato věková skupina zranitelnou, což potvrzuje nezbytnost dalšího rozvoje preventivních strategií v regionu.

H1: Většina dotázaných seniorů v okrese Opava se v online prostoru již setkala s podezřelou zprávou (e-mail, SMS), která vykazovala znaky phishingu.

- Z výsledků otázky č. 6 vyplývá, že variantu „Ano, často“ zvolilo 16 % respondentů (18 osob) a variantu „Ano, občas“ 51 % respondentů (58 osob). Celkem 67 % respondentů potvrdilo přímou zkušenost s podezřelou komunikací vykazující znaky phishingu. Jelikož hodnota 67 % představuje nadpoloviční většinu zkoumaného vzorku, je splněna podmínka stanovená v hypotéze.
- Závěr: **Hypotéza H1 byla potvrzena.**

H2: Senioři jako primární zdroj informací o bezpečnosti na internetu využívají rodinné příslušníky (děti, vnoučata), nikoliv oficiální státní instituce nebo média.

- Podle výsledků otázky č. 9 uvádí 40 % respondentů (46 osob) jako hlavní zdroj informací rodinu. Média využívá 25 % a banky či státní instituce pouze 15 %. Tento trend potvrzují i data z otázky č. 11, kde konzultaci s rodinou jako aktivní bezpečnostní opatření využívá dokonce 68 %

respondentů. Rodina představuje pro seniory v okrese Opava nejsilnější a nejdůvěryhodnější informační kanál. Oficiální instituce (včetně Policie ČR) a média jsou využívána v podstatně menší míře.

- Závěr: **Hypotéza H2 byla potvrzena.**

7.4 Návrh pro zvýšení prevence ze strany Policie ČR

Vzhledem k potvrzení hypotézy H2, která identifikovala rodinu jako klíčový uzel v šíření informací, je nutné transformovat stávající model prevence. Pokud senioři nehledají informace u Policie ČR aktivně, musí Policie ČR **využít rodinu jako prostředníka** a přizpůsobit formy komunikace zjištěným preferencím.

Namísto cílení kampaní výhradně na seniory by měla Policie ČR cílit na ekonomicky aktivní generaci a studenty. Pokud děti a vnoučata dostanou od policie srozumitelný návod, předají ho seniorovi s mnohem vyšší úspěšností než cizí autorita.

Při realizaci mezigenerační prevence Policie ČR může:

- v rámci kampaní (např. na sociálních sítích cílených na mladší generaci) nabádat mladší rodinné příslušníky, aby při návštěvě u prarodičů provedli tzv. bezpečnostní audit jejich zařízení. Základem je pravidelná kontrola nastavení soukromí, aktualizace aplikací a zejména nastavení nízkých limitů pro platby kartou a v internetovém bankovnictví, které seniorovi zabrání přijít o vysoké částky při jednorázovém útoku.
- nabádat k nastavení tajného hesla či kontrolní otázky. Toto doporučení je velmi aktuální v souvislosti s rozvojem umělé inteligence a stále častějším výskytům tzv. deepfakes (podvržení hlasu, obrazových záznamů). Vyžadováním hesla je útočník zahnán do kouta a jeho podvodné jednání je odhaleno.
- informovat mladší generaci o možnostech digitální ochrany mobilního telefonu seniora prostřednictvím dostupných aplikací, nastavení daného smartphonu, biometrického ověřování, zabezpečení hesel aj.
- vytvářet edukativní obsah, který zaujme všechny generace. Společný prožitek a následná diskuse v rodině má mnohem vyšší účinnost než samostudium.
- poskytnout šablonu prevence, kterou mladší generace vyplní spolu se seniorem. Následně toto může být předmětem mezigenerační diskuze.

- využít prostoru v rámci preventivních programů na základních školách. Dítě funguje jako velmi silný a seniorovi emočně blízký nositel informace.

Na základě zjištěných preferencí respondentů, kteří projevili nejvyšší zájem o tištěné materiály (40 %) a osobní přednášky (30 %), lze pro zefektivnění preventivní činnosti formulovat následující doporučení v rámci stávající edukace:

- **Distribuce stručných informačních materiálů ve spolupráci s jednotlivými obcemi v okrese Opava.** Tyto materiály by měly být doručovány přímo do poštovních schránek, vyhotoveny ve zvětšeném písmu a obsahovat jasné instrukce k postupu při podezřelé komunikaci.
- **Realizace edukativních vstupů v rámci fungujících komunit, jako jsou kluby seniorů, univerzity třetího věku či tematické „seniorské dny" v okrese Opava.** Osobní interakce s příslušníkem Policie ČR přispívá k budování důvěry, což může v případě reálného napadení vést k eliminaci pocitu studu a zvýšení ochoty incident nahlásit.
- **Využití lokálních periodik a zřízení pravidelné preventivní rubriky v obecních a městských zpravodajích.** Policie ČR zde může pravidelně reflektovat aktuální podvodné trendy zachycené v rámci regionu, neboť senioři přikládají lokálním tiskovinám vyšší míru důvěry než médiím celostátním.

Vzhledem ke skutečnosti, že 60 % respondentů dotazníkového šetření využívá jako hlavní zařízení chytrý telefon, je žádoucí, aby se preventivní aktivity zaměřily také na **praktickou technickou pomoc**. V rámci osvětové činnosti lze doporučit pomoc s instalací a konfigurací ověřených aplikací pro blokování nevyžádaných či podvodných hovorů. Současně je nezbytné klást důraz na edukaci v oblasti rizikovosti přeposílání či potvrzování autorizačních SMS kódů třetím osobám, což představuje jeden z nejčastějších vektorů útoku na tuto cílovou skupinu.

Závěr

Bakalářská práce se podrobně zabývala problematikou phishingu jako specifické formy kyberkriminality, která v současnosti představuje jednu z nejvýznamnějších hrozeb pro cílovou skupinu seniorů. Hlavním cílem práce bylo komplexně vymezit fenomén phishingových útoků zaměřených na seniory v regionu okresu Opava a zhodnotit roli Policie ČR při jejich odhalování a prevenci.

Teoretická část se soustředila na detailní vymezení kyberkriminality, její historie a základního legislativního rámce v České republice. Zvláštní pozornost byla věnována mechanismům phishingu a jeho modifikacím, jako jsou smishing či vishing. V rámci této části byly rovněž prozkoumány postupy, které Policie ČR uplatňuje při prověřování a vyšetřování těchto skutků, včetně technických aspektů zjišťování IP adres a specifických výzev při dokazování v digitálním prostředí. Dílčím cílem bylo analyzovat faktory, jako je snížená digitální gramotnost či psychosociální aspekty stárnutí, které činí seniorskou populaci zvlášť zranitelnou.

Empirická část práce se zaměřila na zjištění míry povědomí a reálných zkušeností seniorů v okrese Opava s phishingovými hrozbami prostřednictvím dotazníkového šetření. Analyzovány byly reakce seniorů na podezřelou komunikaci a byly identifikovány klíčové zdroje, ze kterých tato skupina čerpá informace o online bezpečnosti. Na základě získaných dat byly potvrzeny obě stanovené hypotézy, což umožnilo formulovat konkrétní doporučení pro zlepšení preventivních opatření v regionu.

Ke splnění cílů práce byly využity adekvátní metodologické přístupy. Metoda studia odborné literatury a analýzy právních předpisů umožnila definovat teoretická východiska a procesní postupy bezpečnostních sborů. Kvantitativní výzkumná metoda ve formě dotazníkového šetření poskytla data od 114 respondentů, která byla následně statisticky analyzována. Metodou dedukce byly z výsledků šetření vyvozeny návrhy pro praxi, které zohledňují specifické preference seniorů na Opavsku.

Výsledky práce ukazují, že phishing představuje pro seniory v okrese Opava reálnou a častou hrozbu, neboť se s ním v online prostoru setkalo 67 % dotázaných. Přestože většina respondentů projevuje základní ostražitost, pouze 18 % zná přesný význam termínu phishing a pětina respondentů přiznává, že podvodnou zprávu nedokáže rozpoznat. Výzkum dále potvrdil, že klíčovou roli v informovanosti hraje rodinné zázemí,

které jako primární zdroj informací využívá 40 % seniorů, zatímco oficiální instituce jsou vnímány jako sekundární.

Na základě provedeného šetření bylo navrženo několik preventivních opatření cílených na okres Opava. Mezi hlavní doporučení patří transformace modelu prevence směrem k rodinným příslušníkům jakožto informačním prostředníkům, distribuce tištěných bezpečnostních materiálů ve zvětšeném písmu přímo do domácností a realizace osobních přednášek v místech přirozeného setkávání seniorů. Tato opatření by měla přispět k posílení digitální rezilience seniorů a snížení jejich viktimizace.

Práce přispěla k hlubšímu pochopení specifických rizik, kterým čelí starší generace v digitálním věku, a navrhla konkrétní kroky pro zefektivnění preventivní činnosti Policie ČR. Výsledky této bakalářské práce mohou sloužit jako praktické vodítko pro státní správu i neziskový sektor při tvorbě regionálních vzdělávacích programů, čímž byly naplněny hlavní i vedlejší cíle práce.

Seznam použitých zdrojů

Literární zdroje

1. ALBRECHT, CH. D. a kol. *Fraud Examination.* 6. vydání. Boston: Cengage Learning, 2019. s. 696. ISBN 978-1-337-61867-7.
2. GŘIVNA, T, POLČÁK R. *Kyberkriminalita a právo*. Praha: Auditorium, 2008. s. 220. ISBN 978-80-903786-7-4.
3. HORSKÁ, B.; LÁSKOVÁ, A. a PTÁČEK, L. *Internet jako cesta pomoci: internetové poradenství pro pomáhající profese.* Praha: Sociologické nakladatelství (SLON), 2010, s. 197. ISBN 978-80-7419-034-6.
4. CHALUPOVÁ K., ŠTEFUNKOVÁ M. a ŠEJVL J. *Základy prevence kriminality pro pedagogické pracovníky*. Praha: Klinika adiktologie, 1. lékařská fakulta Univerzity Karlovy v Praze a Všeobecná fakultní nemocnice v Praze ve vydavatelství Togga, 2012. s. 105. ISBN 978-80-87258-96-5.
5. JAMES, L. *Phishing bez záhad*. Praha: Grada Publishing, 2007. s. 281. ISBN 978-80-247-1766-1.
6. JELÍNEK, J. a kol. *Trestní právo hmotné.* 8. vydání. Praha: Nakladatelství Leges, 2022. s. 1040. ISBN 978-80-7502-576-0.
7. JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. *Výkladový slovník kybernetické bezpečnosti*. Praha: Centrum kybernetické bezpečnosti, z.ú., 2025. s. 396. ISBN 978-80-908388-9-5.
8. JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* Praha: Grada, 2007. s. 284. ISBN 978-80-247-1561-2.
9. KALNICKÝ, J. *Obecná gerontagogika*. Opava: Slezská univerzita v Opavě, Fakulta veřejných politik v Opavě, 2019. s. 129. Dostupné z: <https://is.slu.cz/publication/35020/Obecna_gerontagogika.pdf>
10. KOHOUT, R; KARCHŇÁK, R. *Bezpečnost v online prostředí*. Karlovy Vary: Biblio Karlovy Vary, 2016. s. 65. ISBN 978-80260-9543-9.
11. KOLOUCH, J. *Cybercrime*. Praha: CZ.NIC, z. s. p. o., 2016. s. 524. ISBN 978-80-88-168-18-8.
12. KOVALČÍK, M. *Nástrahy internetu, aneb, Informační (ne)bezpečnost*. I. vydání. Opava: Marek Kovalčík, 2024. s. 120. ISBN 978-80-11-05720-6.

13. MARTANOVÁ, V., B. JANÍKOVÁ, T. DANĚČKOVÁ, et al. *Učební texty ke specializačnímu studiu pro školní metodiky prevence.* Praha: Centrum adiktologie Psychiatrické kliniky 1. lékařské fakulty a VFN, Univerzita Karlova, 2007. s. 159. ISBN 978-80-254-0525-3.
14. SAK, P.; KOLESÁROVÁ, K. *Sociologie stáří a seniorů*. Praha: Grada, 2012. s. 226. ISBN 978-80-247-3850-5.
15. SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015. s. 640. ISBN 978-80-7380-501-2.
16. SMEJKAL, V.; SOKOL, T.; VLČEK, M. *Počítačové právo*. Praha: C. H. Beck, 1995. s. 264. ISBN 80-7179-009-5.
17. ZAVRŠNIK, A. *Kyberkriminalita.* Praha: Wolters Kluwer, 2017. Právní monografie. s. 148. ISBN 978-80-7552-758-5.

Elektronické zdroje

1. ČESKÉ DŮCHODY. *Podvody, nástrahy a zákeřnosti na internetu: Vyznejte se v hrozbách pro seniory.* [online]. [cit. 09. 02. 2026]. Dostupné z: <https://ceskeduchody.cz/navody/bezpecne-na-internetu-seniori-podvody-phishing-skodlive-programy>.
2. E-BEZPEČÍ. *Podvody - phishing, vishing, smishing*. [online]. [cit. 15. 01. 2026]. Dostupné z: <https://www.e-bezpeci.cz/index.php/z-jinych-webu/2684-podvody-phishing-vishing-smishing>.
3. INSMART. *Podvody na internetu v roce 2022? Varují banky i Policie*. [online]. [cit. 15. 01. 2026]. Dostupné z: <https://insmart.cz/internetove-podvody-varovani-pcr/>.
4. INTERNETEM BEZPEČNĚ. *Phishing.* [online]. [cit. 15. 01. 2026]. Dostupné z: <https://www.internetembezpecne.cz/internetem-bezpecne/podvodne-praktiky/phishing/>.
5. KYBERTEST. *Nejčastější typy podvodů na internetu.* [online]. [cit. 15. 01. 2026]. Dostupné z: <https://www.kybertest.cz/nejcastejsi-typy-podvodu>.
6. KYBERTEST. *Nejčastější typy podvodů: Phishing, podvodné emaily.* [online]. [cit. 15. 01. 2026]. Dostupné z: <https://www.kybertest.cz/nejcastejsi-typy-podvodu/phishing-podvodne-e-maily>.

7. KYBERTEST. *Nejčastější typy podvodů: Smishing, podvodné SMS zprávy*. [online]. [cit. 15. 01. 2026]. Dostupné z: <https://www.kybertest.cz/nejcastejsi-typy-podvodu/smsishing-podvodne-sms-zpravy>.
8. KYBERTEST. *Nejčastější typy podvodů: Vishing, podvodné telefonáty*. [online]. [cit. 15. 01. 2026]. Dostupné z: <https://www.kybertest.cz/nejcastejsi-typy-podvodu/vishing-podvodne-telefonaty>.
9. NÚKIB. *Kybernetická bezpečnost: Pomůcka pro seniory.* [online]. [cit. 09. 02. 2026]. Dostupné z: <https://nukib.gov.cz/download/vzdelavani/kurzy/Pomucka-SENIOR.pdf>
10. POLICIE ČR. *Policie ČR s ČSOB varují před zvýšenou aktivitou kybernetických zločinců.* [online]. [cit. 15. 01. 2026]. Dostupné z: <https://www.policie.cz/clanek/policie-cr-s-csob-varuji-pred-zvysenou-aktivitou-kybernetickych-zlocincu.aspx>.

Legislativní dokumenty

1. ČESKO. Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů. In *Sbírka zákonů, Česká republika.* 1961, částka 66. Dostupné z: <https://app.beck-online.cz>.
2. ČESKO. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In *Sbírka zákonů, Česká republika.* 2009, částka 11. Dostupné z: <https://app.beck-online.cz>.
3. ČESKO. Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, ve znění pozdějších předpisů. In *Sbírka zákonů, Česká republika.* 2011, částka 146. Dostupné z: <https://app.beck-online.cz>.
4. ČESKO. Zákon č. 45/2013 Sb., o obětech trestných činů a o změně některých zákonů (zákon o obětech trestných činů). In *Sbírka zákonů, Česká republika.* 2013, částka 20. Dostupné z: <https://app.beck-online.cz>.

Seznam zkratek

1. **ČR –** Česká republika
2. **GDPR –** General Data Protection Regulation
3. **ICT –** Information and Communication Technologies
4. **NÚKIB –** Národní úřad pro kybernetickou a informační bezpečnost
5. **TOPO –** Trestní odpovědnost právnických osob
6. **TOR –** The Onion Router
7. **TrŘ –** Trestní řád
8. **TrZ –** Trestní zákoník
9. **VPN –** Virtual Private Network
10. **VR –** Virtualní realita
11. **ZOOTČ –** Zákon o obětech trestných činů

Seznam tabulek a grafů

Seznam příloh

Přílohy

Příloha č. 1 - Dotazník

Dotazník: Bezpečnost a orientace seniorů v online prostoru (Okres Opava)

Dobrý den, jsem studentem Vysoké školy evropských a regionálních studií v Českých Budějovicích, pobočka v Příbrami a v rámci své bakalářské práce se věnuji bezpečnosti seniorů na internetu. Obracím se na Vás s žádostí o vyplnění krátkého dotazníku.

Cílem mého výzkumu je zjistit, jak se Vám v dnešním online světě orientuje, s jakými nástrahami se setkáváte a jak by se dala zlepšit ochrana seniorů přímo v okrese Opava.

Vaše zkušenosti jsou pro mě nesmírně cenné. Neexistují špatné odpovědi, zajímá mě Váš skutečný pohled na věc. Dotazník je zcela anonymní a získané údaje budou využity pouze pro zpracování mé práce.

Pokyny pro vyplnění:

- Časová náročnost: Vyplnění Vám zabere přibližně 5–10 minut.
- Jak odpovídat: Odpovídejte prosím podle své vlastní zkušenosti. U každé otázky zaškrtněte odpověď, která Vás nejlépe vystihuje (pokud není uvedeno jinak).
- Odevzdání: Po vyplnění prosím odevzdejte dotazník osobě, od které jste jej obdrželi, nebo jej ponechte na určeném místě.

Předem Vám velmi děkuji za ochotu, čas a pomoc.

S pozdravem

Martin Ligocki, DiS.

---

1) **Pohlaví:**
   a) žena
   b) muž
2) **Věk:**
   a) 60–65 let
   b) 66–75 let
   c) 76 let a více
3) **Jaké zařízení nejčastěji používáte k přístupu na internet?**

a) chytrý telefon

b) počítač/notebook

c) tablet

4) Které služby na internetu využíváte?

a) e-mail (Seznam, Gmail apod.)

b) sociální sítě (Facebook, WhatsApp)

c) internetové bankovnictví

5) Slyšel/a jste někdy termín "phishing" (podvodné zprávy lákající údaje)?

a) Ano, vím přesně, o co jde.

b) Slyšel/a jsem to slovo, ale nevím, co znamená.

c) Ne, nikdy jsem o tom neslyšel/a.

6) Obdržel/a jste někdy podezřelý e-mail nebo SMS (např. výzva k doplatku, zablokovaný účet v bance, výzva k zaslání peněz rodinnému příslušníku aj.)?

a) Ano, často (několikrát měsíčně).

b) Ano, občas.

c) Ne, nikdy (přejděte k otázce č. 8).

7) Pokud ano, jak jste na takovou zprávu reagoval/a?

a) Zprávu jsem okamžitě smazal/a.

b) Zprávu jsem otevřel/a, ale na nic neklikal/a.

c) Klikl/a jsem na odkaz, ale nevyplnil/a žádné údaje.

d) Vyplnil/a jsem požadované údaje.

8) Podle čeho poznáte, že je e-mail nebo SMS podezřelá?

a) Špatná čeština a chyby.

b) Podezřelá adresa odesílatele.

c) Nátlak na rychlé jednání (strach, hrozba pokutou).

d) Nepoznám to, všechny zprávy mi přijdou stejné.

9) Kde čerpáte informace o tom, jak se na internetu chránit?

a) Od rodiny (děti, vnoučata).

b) Z médií (televize, noviny).

c) Od banky nebo státních institucí (policie).

d) Informace nevyhledávám.

10) Považujete informace o podvodech na internetu, které jsou dostupné v okrese Opava (např. v místním tisku, na vývěskách), za dostatečné?

a) Ano, informací je v mém okolí dostatek.

b) Spíše ano, ale mohlo by jich být víc.

c) Ne, v mém okolí se o tom vůbec nepíše/nemluví.

11) Která z následujících bezpečnostních opatření aktivně používáte? (Možno zaškrtnout více)

a) Silná a různá hesla pro každý účet.

b) Dvoufázové ověření (např. potvrzení přihlášení v mobilu nebo SMS kódem).

c) Pravidelné konzultace s rodinou při podezřelých zprávách.

d) Žádné z uvedených / Nevím.

12) Pokud byste se stal/a obětí podvodu (přišel/la o peníze nebo přístup k účtu), na koho byste se obrátil/a jako na prvního?

a) Na Policii ČR.

b) Na svou banku.

c) Na rodinu nebo známé.

d) Nevím, styděl/a bych se to někomu říct.

13) Jakou formou byste se chtěl/a dozvědět více o bezpečnosti na internetu?

a) Tištěný leták/příručka (např. v čekárně u lékaře nebo v poštovní schránce).

b) Osobní přednáška s odborníkem v místě bydliště.

c) Krátké video s ukázkami podvodů.

d) Praktický workshop, kde si vše vyzkouším na svém telefonu/počítači.