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

BAKALÁŘSKÁ PRÁCE

INZERTNÍ PODVODY V ČESKÉM KYBERPROSTORU: VYŠETŘOVÁNÍ A PREVENCE Z POHLEDU PŘÍSLUŠNÍKA POLICIE ČESKÉ REPUBLIKY

Autor práce: Tomáš Kubný, 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: Tomáš Kubný, DiS.
Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: Příbram

Název bakalářské práce: Inzertní podvody v českém kyberprostoru: vyšetřování a prevence z pohledu příslušníka Policie České republiky

Název bakalářské práce v anglickém jazyce: Classified Ad Fraud in the Czech Cyberspace: Investigation and Prevention from the Perspective of a Police Officer of the Czech Republic

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

Cíl bakalářské práce:
Hlavním cílem bakalářské práce je komplexně zhodnotit vývoj a aktuální trendy počítačové kriminality v České republice, se zaměřením na problematiku inzertních podvodů v souvislosti s technologickým pokrokem, a zároveň posoudit, jak moderní technologie, zejména umělá inteligence, ovlivňují způsoby jejich páchání z perspektivy příslušníka Policie České republiky.
Vedlejším cílem bakalářské práce je vyhodnotit úroveň povědomí uživatelů internetu o kybernetické bezpečnosti na základě dat získaných z dotazníkového šetření, určit nejčastější rizikové faktory, které uživatelé internetu často opomíjejí, a navrhnout opatření, jež mohou pomoci těmto hrozbám předcházet.

Student: Tomáš Kubný, DiS.	28.11.2025 *datum*	 *podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	28.11.2025 *datum*	 *podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	8.12.2025 *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*

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

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

.....

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

ABSTRAKT

Tato bakalářská práce se zabývá problematikou inzertních podvodů v českém kyberprostoru a jejich vyšetřováním z pohledu příslušníka Policie České republiky. Teoretická část vymezuje základní pojmy spojené s počítačovou kriminalitou, popisuje její historický vývoj a představuje právní rámec kybernetické bezpečnosti v České republice. Součástí je také přehled nejčastějších forem útoků a zásad bezpečného chování uživatelů internetu, včetně vlivu moderních technologií a umělé inteligence na způsoby páchání kybernetické trestné činnosti. Praktická část se zaměřuje na konkrétní případy podvodné inzerce z policejní praxe a na výsledky dotazníkového šetření, které hodnotí úroveň povědomí uživatelů o kybernetických hrozbách. Cílem práce je přiblížit současné trendy v oblasti inzertních podvodů, popsat jejich specifika a navrhnout opatření, která mohou přispět k prevenci tohoto typu trestné činnosti.

Klíčová slova: kyberkriminalita, inzertní podvody, Policie České republiky, kybernetická bezpečnost, umělá inteligence, phishing, prevence

ABSTRACT

This bachelor thesis focuses on classified advertisement fraud in the Czech cyberspace and its investigation from the perspective of a Police of the Czech Republic officer. The theoretical part defines key concepts related to computer crime, outlines its historical development, and presents the legal framework of cyber security in the Czech Republic. It also provides an overview of common cyber-attack techniques and principles of safe online behaviour, including the influence of modern technologies and artificial intelligence on the methods used to commit cybercrime. The practical part analyses specific cases of fraudulent online advertisements based on police practice and evaluates the results of a questionnaire survey examining users' awareness of cyber threats. The aim of the thesis is to describe current trends in online advertisement fraud, highlight their specific characteristics, and propose measures that may help prevent this type of criminal activity.

Key words: cybercrime, online advertisement fraud, Police of the Czech Republic, cyber security, artificial intelligence, phishing, prevention

Obsah

Úvod

V posledních dekádách se informační technologie a internet staly neodmyslitelnou součástí našich každodenních životů. Digitalizace pronikla téměř do všech oblastí, od osobních komunikací přes finanční transakce až po státní správu. Spolu s tímto vývojem se však objevila i nová hrozba – počítačová kriminalita. Tento fenomén zahrnuje široké spektrum nezákonných aktivit, od krádeží dat a útoků na informační systémy až po podvody a zneužívání osobních údajů. Počítačová kriminalita se stala globálním problémem, který zasahuje jednotlivce, firmy i státy, a její dopady jsou stále hmatatelnější.

První část práce se bude věnovat teoretickému vymezení pojmů tykajících se počítačové kriminality, jejich definicím a klasifikaci. Budou zde rozebrány různé formy počítačové kriminality od tradičních hackerů až po sofistikovanější formy útoků, jako jsou ransomware, phishing či sociální inženýrství. Následně bude zmíněna historie počítačové kriminality a blíže budou vymezeny základní principy chování, jakými se jednotlivci i organizace mohou proti útokům páchaných v kyberprostoru bránit.

Praktická část této práce bude věnována případovým studiím z policejní praxe a vyhodnocením dat, které budou získány na základě dotazníkového šetření. Cílem dotazníkového šetření je vyhodnotit úroveň povědomí uživatelů internetu o kybernetické bezpečnosti, určit nejčastější rizikové faktory, které uživatelé internetu často opomíjejí, a navrhnout opatření, jež mohou pomoci těmto hrozbám předcházet. Budou analyzovány názory veřejnosti na rizika spojená s touto problematikou a na to, jak jsou běžní uživatelé internetu připraveni těmto hrozbám čelit. Cílem šetření je nejen zjistit, do jaké míry jsou lidé informováni o kybernetické bezpečnosti, ale také posoudit jejich ochotu přijímat preventivní opatření, jako je používání silných hesel, dvoufázového ověřování nebo opatrnost při online transakcích.

Tato práce si tedy klade za cíl přispět k lepšímu porozumění dané problematiky a pomoci tak zvýšit povědomí o nutnosti ochrany v digitálním prostředí, které se stává stále zranitelnějším.

1 Cíl a metodika bakalářské práce

Teoretická část bakalářské práce se na základě rešerše literárních zdrojů a zákonů, zaměří na problematiku počítačové kriminality a kybernetické bezpečnosti v prostředí České republiky. Bude vymezen okruh základních pojmů, popsán historický vývoj a současné trendy v oblasti kybernetické trestné činnosti. Pozornost bude věnována jednotlivým formám útoků, jako jsou phishing, malware, ransomware, spoofing, darknet aj., včetně jejich dopadů na běžné uživatele. Součástí bude přehled legislativního rámce a preventivních opatření.

Praktická část se zaměří na internetové inzertní podvody, zejména v prostředí online tržišť a bazarových platforem. Její součástí budou konkrétní případové studie vycházející z praxe Policie ČR, které přiblíží typické scénáře těchto podvodů a postupy jejich řešení z pohledu policejního vyšetřovatele. Dále bude provedeno dotazníkové šetření mezi uživateli internetu, zaměřené na jejich zkušenosti, úroveň informovanosti o kybernetických hrozbách a zásady bezpečného chování na internetu. Výsledky budou statisticky vyhodnoceny a poslouží jako podklad pro návrh opatření, která mohou přispět ke snížení výskytu těchto trestných činů a k posílení informovanosti veřejnosti.

Hlavním cílem bakalářské práce je komplexně zhodnotit vývoj a aktuální trendy počítačové kriminality v České republice, se zaměřením na problematiku inzertních podvodů v souvislosti s technologickým pokrokem, a zároveň posoudit, jak moderní technologie, zejména umělá inteligence, ovlivňují způsoby jejich páchání z perspektivy příslušníka Policie České republiky.

Vedlejším cílem bakalářské práce je vyhodnotit úroveň povědomí uživatelů internetu o kybernetické bezpečnosti na základě dat získaných z dotazníkového šetření, určit nejčastější rizikové faktory, které uživatelé internetu často opomíjejí, a navrhnout opatření, jež mohou pomoci těmto hrozbám předcházet.

2 Vymezení základních pojmů

V souvislosti s počítačovou kriminalitou se lze často setkat s různými výrazy či pojmy, které jsou většinou převzaty z angličtiny anebo jsou odvozeny z cizích slov. V rámci bakalářské práce budou vybrány a popsány některé základní pojmy, se kterými se lze setkat právě v souvislosti s počítačovou kriminalitou. Pojmů by se dalo vyjmenovat nespočetné množství, ale budou vybrány pouze ty, které jsou v přímé souvislosti s tématem této práce, především s praktickou částí, která se bude blíže věnovat případovým studiím inzertních podvodů a následně dotazníkovému šetření týkajícího se povědomí o kyberkriminalitě.

2.1 Internet

Internet je celosvětový systém propojených počítačových sítí („síť sítí“), ve kterých mezi sebou počítače komunikují pomocí rodiny protokolů Transmission Control Protocol –„protokol pro řízení přenosu“/Internet Protocol – „protokol pro propojení sítí“ (TCP/IP). Společným cílem lidí využívajících internet je bezproblémová komunikace a výměna dat. Nejznámější službou poskytovanou v rámci internetu je služba World Wide Web – v doslovném překladu „světově rozsáhlá pavučina“ nebo „celosvětová síť“ (WWW), což je kombinace textu, grafiky a multimédií propojených hypertextovými odkazy a e-mail (elektronická pošta), avšak nalezneme v něm i desítky dalších.

Internet propojil životy osob a přinesl svět blíže ke každému uživateli, což nemusí být nutně velkou výhodou. Žijeme v době, ve které tvoříme a budujeme naše životy kolem drátových a bezdrátových sítí, a život bez internetu si již nelze tak jednoduše představit.[1]

2.2 Hacker, Cracker

Hacker je osoba s dokonalou znalostí informačního systému, s nímž dokáže pracovat a přizpůsobovat ho podle svých potřeb. Občas se s ním setkáváme pod pojmem geek – programátor a počítačový expert v jednom. [2]

[1] KOLOUCH, J. *Cybercrime*. Praha: CZ.NIC, 2016, s. 45–47. ISBN 978-80-88168-18-8.
[2] ESET. Kdo je hacker? [online]. Praha : ESET, 2024 [cit. 2026-03-11]. Dostupné z WWW: <https://www.eset.com/cz/hacker/>.

K termínu hacker se dost úzce váže i termín cracker neboli osoba, která se naprosto vědomě dopouští kyberkriminálních přečinů proti zákonu v kyberprostoru.

V podstatě se jedná o hackera, který tzv. hackuje či spíše crackuje, tedy proniká do systému za účelem krádeže osobních dat. U takových datových informací, u kterých není proveden backup (záloha), může dojít k absolutní ztrátě.

Dříve se oba pojmy slévaly (především kvůli médiím) do jednoho termínu, nicméně tzv. etický hacker hledá jen limity a chyby, na které pak upozorní, aby mohly být odstraněny. Cracker si nechává získané informace jen pro sebe, popř. je dále prodává na černém trhu např. pomocí tzv. Deepwebu popř. Darknetu.

2.3 Phishing

Phishing je forma kybernetického útoku, která spočívá v získávání citlivých informací, jako jsou hesla, bankovní údaje nebo osobní identifikační údaje, podvodným způsobem. Útočníci se obvykle pokoušejí získat tyto informace prostřednictvím e-mailů, textových zpráv nebo sociálních médií, při nichž se vydávají za důvěryhodnou osobu nebo organizaci.

Tyto zprávy často obsahují odkazy na falešné webové stránky, které vypadají jako legitimní, ale ve skutečnosti jsou vytvořeny útočníky k tomu, aby uživatele přiměly zadat své citlivé informace. Phishing je často spojen s cílem okrást jednotlivce nebo organizaci nebo získat přístup k jejich účtům či systémům.

Útočníci využívají umění tzv. **sociálního inženýrství**, což je strategie spočívající v **manipulaci a klamání**, jejímž prostřednictvím se jednotlivci nebo skupiny snaží lidi přimět, aby **odhalili citlivé informace** nebo aby podnikli kroky, kterými ohrozí vlastní bezpečnost. Jeho principem nejsou zvláštní dovednosti v oblasti moderních technologií, nýbrž znalosti psychologie a lidského chování. Jedná se o jakousi taktiku útočníka.[3]

2.4 Malware

Malware je zastřešující výraz pro jakýkoli typ škodlivého softwaru, jehož cílem je poškodit nebo zneužít libovolné programovatelné zařízení, službu nebo síť. Kyberzločinci jej obvykle používají k extrahování dat a tím k vyvinutí nátlaku na oběti

[3] JAMES, L. Phishing bez záhad. Praha: Grada Publishing, 2007, s. 18–22. ISBN 978-80-247-1766-1.

za účelem finančního zisku. K těmto datům mohou patřit finanční data, zdravotní záznamy, osobní e-maily a hesla – pokud jde o to, jaký druh informací může být ohrožen, možnosti jsou nekonečné.[4]

2.5 Deepfake

Deepfake je technologie založená na strojovém učení, která umožňuje vytvářet realisticky vypadající falešné audio-vizuální materiály. Tyto výstupy mohou být zneužity k podvodům, vydírání nebo k manipulaci veřejného mínění.[5] Mezi nejznámější případy patří např. zneužití vzhledu veřejně známé osobnosti (politika, herce), která v takto vytvořeném videu, které je zobrazováno přesně cílenému publiku, nabízí investice s výhodným úrokem, popř. jiný výhodný produkt či spoření. Za zmínku stojí i čím dál častější zneužití hlasového projevu osoby např. při zakládání smluv (nejčastěji úvěrových) pomocí prostředků dálkové komunikace.

2.6 Zranitelnost

Jedná se o chybu v zabezpečení sítě organizace nebo jednotlivce, díky které útočníci tuto ochranu relativně snadno prolomí. Může se jednat o určitou chybu systému, ať už hardwaru či softwaru, popř. i o chybu jednotlivce. Co se týká chyby jednotlivce, tak se může zejména jednat o nějaký druh phishingového útoku, kdy nějaký zaměstnanec vyplní své přihlašovací údaje do falešné stránky útočníka, popř. se může také jednat o nějaké fyzické pochybení např. vpuštění neoprávněné osoby do budovy jejím nedostatečným ověřením (útočník využije tzv. „neviditelnost modrých montérek“, kdy se vydává za údržbáře), popř. stačí pouhé nedostatečné dovření vstupních dveří.[6]

2.7 Umělá inteligence (AI)

Umělá inteligence představuje soubor metod a technologií umožňujících strojům vykonávat činnosti, které vyžadují určitou formu lidského rozhodování, učení nebo vyhodnocování dat. V oblasti kybernetické bezpečnosti je AI využívána jak k obraně, tak k útokům, zejména při automatizaci podvodných aktivit a generování falešného obsahu.[7]

[4] KOLOUCH, R.; KARČINÁK, R. *Bezpečnost v online prostředí*. Karlovy Vary: Biblio Kurzy Vary, 2016, s. 31–34. ISBN 978-80-260-9543-9.
[5] JIRÁSEK, P.; NOVÁK, L.; POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* Praha: Centrum kybernetické bezpečnosti, 2025, s. 68–69. ISBN 978-80-53054-00-3
[6] PAVINSKI, A. *Kyberkriminalita*. Praha: Wolters Kluwer, 2017, s. 41–43. ISBN 978-80-7552-758-5.
[7] JIRÁSEK, P.; NOVÁK, L.; POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti.* Praha: Centrum kybernetické bezpečnosti, 2025, s. 152–154. ISBN 978-80-53054-00-3.

2.8 Spoofing

Útočníci využívají funkce moderní telekomunikační sítě, která umožňuje to, že volanému zobrazuje jiné telefonní číslo, než ze kterého je ve skutečnosti hovor uskutečňován. Tato funkce byla prvotně vymyšlena proto, aby např. velké společnosti, které mají hodně zaměstnanců, a tedy i množství telefonních čísel, při volání svým klientům usnadnili identifikaci toho, kdo jim volá. Toto usnadnění spočívá v tom, že klientovi volá kterýkoliv zaměstnanec z jakéhokoliv telefonu společnosti a volanému se vždy zobrazí shodné telefonní číslo. Toto telefonní číslo může mít volaný uložené nebo v případě marketingu jej může znát např. z reklamy, webu společnosti reklamního letáku apod.

V rámci ČR je tento provoz regulován a operátor volaného vždy ví, z jakého telefonního čísla byl hovor doopravdy uskutečněn. Problém nastává v případě, kdy je počáteční hovor započat v zahraničí, kde tato regulace není sjednocena. Čeští operátoři zareagovali na vzrůstající případy takto zneužívané služby tím, že zablokovali příjem tzv. „spoofovaných“ hovorů započatých ze zahraničních pevných linek. Problém však nastává v případě, kdy počáteční hovor je započat z mobilního telefonu. Operátor nemůže jednoznačně rozeznat, zda se jedná o podvod nebo zda uživatel pouze nevyužívá služeb roamingu. Z tohoto důvodu je z technického hlediska zatím blokace takovýchto hovorů nemožná.

Nebezpečnost tohoto podvodného jednání spočívá hlavně v tom, že je takřka na první pohled nerozeznatelná i pro zkušenější uživatele, kteří jsou jinak v oblasti bezpečnosti obezřetní. Útočníci, kteří se např. vydávají za bankéře, volají tak, aby se volajícímu zobrazilo skutečné telefonní číslo předmětné banky a zároveň se může představit jako osoba, která v této bance doopravdy pracuje. Tyto údaje mohl útočník mimo jiné získat i na základě útoků uvedených výše, popř. je mohl zakoupit relativně bez problému na černém trhu. K tomuto se využívá např. Darknet, popř. Deepweb.

Takto spoofovat se dají nejen telefonní čísla, ale např. i e-mailové adresy, IP adresy apod. Odhalení původního uskutečnitele hovoru, popř. zprávy je dosti složité a nákladné, a to mimo jiné proto, protože útočník nezapočne hovor z jednoho čísla s tím,

že se volanému zobrazí jím zvolené telefonní číslo (spoofované), ale využívá řetězců volání v rámci více čísel napříč světem, které spoofuje mezi sebou navzájem.[8]

Data, na základě kterých lze dohledat předchozí číslo v řetězci, se u operátorů uchovávají omezenou dobu a v rámci světa není tato doba sjednocena, popř. se v některých zemích neuchovávají vůbec. Této slabiny právě útočníci využívají, a tím pádem jsou tyto útoky, při kterých je tato metoda využívána, obzvláště nebezpečné.

2.9 Darknet a Deepweb

Darknet (temný web) a Deepweb (hluboký web) jsou sítě a databáze, které nejsou běžnému uživateli dostupné a nelze je najít za pomoci běžných vyhledávačů či jiným zcela běžným způsobem. Velká část deepwebu je zcela legální, kdežto o darkwebu toto již říci nelze.

Deepweb je součástí klasického internetu, jak jej známe, ale jeho stránky nejsou tzv. indexovány, a tudíž nejsou nijak dohledatelné za pomocí klasických vyhledávačů jako je např. Google, Seznam apod. Pro přístup k jeho stránkám je třeba přímé zadání adresy tzv. Uniform Resource Locator (URL), popř. internetový protokol (IP adresa) a následné ověření. Zároveň se využívá tzv. doporučení uživatelů mezi sebou, kdy se již platný uživatel deepwebu zaručí za nového uživatele deepwebu. Udává se, že deepweb je až pětticíckrát větší než klasický web.[9]

Darknet již není součástí klasického internetu, jak jej známe, ale jedná se o jakousi součást deepwebu. K prohlížení jeho stránek je potřeba navíc využití speciálních prohlížečů a autorizací. Udává se, že nejméně 57 % obsahu darknetu je využíváno k obchodování se zbraněmi, pornografií, lidmi, drogami apod. Darknet se využívá i ke komunikaci mezi teroristy či jinými zločinci. Jako měna slouží vesměs virtuální měny, nejznámější z nich je Bitcoin.

Z tohoto důvodu končí většina prostředků, které byly nelegálně získány díky stále se rozšiřující kyberkriminalitě právě v tzv. „Bitcoinmatech“.

[8] POLICIE ČESKÉ REPUBLIKY. Vishing a spoofing [online]. Praha : Policie ČR, 2024 [cit. 2026-03-11]. Dostupné z WWW: <https://policie.gov.cz/clanek/vishing-a-spoofing.aspx>.
[9] KOLOUCH, J. *Cybercrime*. Praha: CZ.NIC, 2016, s. 201–205. ISBN 978-80-88168-18-8.

3 Historický vývoj počítačové kriminality

Podle autora publikace *Počítačová kriminalita* Michala Matějky lze považovat za první počítačový zločin případ, který se udál ve Francii v roce 1801, tedy 150 let před vznikem prvního počítače. Tkadlec Joseph-Marie Jacquard sestrojil zařízení umožňující automatizaci úkonů při tkaní speciálních látek. Zaměstnanci, obávající se ztráty práce, reagovali sabotáží tohoto zařízení. Tento případ je však nutné brát s nadsázkou, protože skutečné počítače vznikly až o mnoho let později.[10]

Kriminalita v této době kopírovala technické i uživatelské možnosti tehdejších systémů. Zpočátku docházelo k trestné činnosti zejména formou sabotáží motivovaných politicky nebo osobní mstou zaměstnanců. První doložený počítačový zločin na území dnešní České republiky pochází ze 70. let, kdy nespokojený pracovník Úřadu důchodového zabezpečení poškozoval magnetem záznamy na magnetických páskách. Tehdejší právní úprava neobsahovala specifické skutkové podstaty, a proto byl čin kvalifikován jako sabotáž.[11]

Dalšími trestnými činy byly tzv. dokladové delikty, kdy pachatelé měnili podklady určené ke zpracování počítačem. Jednalo se zejména o manipulace v mzdových účtárnách, zásobování či odbytu, kde měli zaměstnanci přístup k finančním prostředkům nebo zboží. V 80. letech bylo zaznamenáno 14 případů trestního stíhání tohoto typu. Právní kvalifikace se tehdy opírala zejména o § 132 trestního zákona („Rozkrádání majetku v socialistickém vlastnictví“). Dnes by byly tyto skutky posuzovány jako podvod podle § 209 trestního zákoníku, často v souběhu s § 230 („Neoprávněný přístup k počítačovému systému a nosiči informací“).[12]

Dalším způsobem páchání trestné činnosti bylo neoprávněné užívání počítačů, které byly majetkem zaměstnavatele. Počítače byly využívány například k tisku obrázků, výpočtům diplomových prací nebo k nelegálnímu podnikání. Vysoká míra neodhalitelnosti byla dána nehmotnou povahou počítačového času a tehdejším vztahem občanů ke společnému majetku.[13]

[10] MATĚJKA, M. *Počítačová kriminalita*. Praha: Computer Press, 2002, s. 21–22. ISBN 80-7226-419-2.
[11] MATĚJKA, M. *Počítačová kriminalita*. Praha: Computer Press, 2002, s. 106. ISBN 80-7226-419-2.
[12] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, s. 73–74. ISBN 978-80-7380-558-4.
[13] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, s. 75–76. ISBN 978-80-7380-558-4.

Masivní rozvoj výpočetní techniky po druhé světové válce vedl k nárůstu počítačové kriminality. Největší podíl na tomto rozvoji měly Spojené státy americké, Velká Británie, Japonsko a Německo. V USA byl první trestný čin tohoto druhu zaznamenán v roce 1958 a v roce 1977 byl přijat první zákon na ochranu proti počítačové kriminalitě – *Federal Computer Systems Protection Act*.[14]

Publikace *Kybernetická kriminalita* od Romana Raka rozděluje historický vývoj počítačové kriminality do tří časových úseků, které jsou popsány v následujících podkapitolách.[15]

3.1 Období technologického procitnutí

Období technologického procitnutí se datuje k první polovině devadesátých let 20. století. Jedná se o období po roce 1989, kdy se Československo otevřelo počítačovým technologiím západní provenience. Při porovnání úrovně a množství trestných činů v oblasti počítačů s obdobím před deseti lety lze konstatovat, že v 80. letech bylo spácháno a následně vyšetřováno minimum trestných činů tohoto druhu. Jednalo se zejména o zneužívání strojového času ve velkých podnicích, které vlastnily sálové počítače pro osobní potřeby zaměstnanců, a ojediněle o páchání sabotáže, například proti sovětské výpočetní technice.[16]

Nástup prvních osobních počítačů přinesl zásadní změny. Kupní síla obyvatelstva byla a stále je srovnatelně nižší než v západoevropských zemích a Spojených státech amerických. Rozmach rozšíření osobních počítačů byl provázen masivním nelegálním kopírováním softwaru. Odhaduje se, že více než 80–90 % veškerého programového vybavení bylo nelegálně kopírováno, distribuováno a následně používáno. Poškozenými byli především velcí zahraniční výrobci softwaru.[17]

Na počátku tohoto období nebyl stát připraven čelit novým formám trestné činnosti. Situace nebyla řešena ani z pohledu platné legislativy, ani na základě zkušeností orgánů činných v trestním řízení. Výrobci softwaru proto vyvíjeli výrazný tlak na státní

[14] HOLT, T. J.; BOSWORTH, A. M.; GRIMES, J. B. *Cybercrime and Digital Forensics*. London: Routledge, 2015, s. 44–46. ISBN 978-1-138-02130-3.
[15] RAK, R. a kol. *Kybernetická kriminalita*. Karlovy Vary: Vysoká škola Karlovy Vary, 2013, s. 20–26.
[16] RAK, R. a kol. *Kybernetická kriminalita*. Karlovy Vary: Vysoká škola Karlovy Vary, 2013, s. 20–21.
[17] JIROVSKÝ, V. *Kybernetická kriminalita*. Praha: Grada, 2007, s. 61–63. ISBN 978-80-247-1561-2.

orgány s cílem vytvoření nové právní úpravy chránící autorská práva, včetně práv výrobců softwaru.[18]

3.2 Období fascinace technologiemi

Období fascinace technologiemi se datuje do druhé poloviny devadesátých let 20. století. V tomto období došlo k intenzivnímu využívání počítačových technologií. Osobní počítače postupně nahradily klasické psací stroje a začaly se významně podílet na zpracování administrativních agend institucí. Současně se rozvíjely vnitropodnikové počítačové sítě a rostl význam podnikových informačních systémů s centrálním uložením dat.[19]

Internet, který byl pro běžné občany technologicky i cenově nedostupný, využívaly především státní instituce, univerzity a velké podniky. Nejrozšířenější operační systém Windows 95 však nebyl dostatečně připraven na práci v prostředí rozsáhlé celosvětové počítačové sítě, a to zejména z důvodu řady bezpečnostních nedostatků. Koncentrace citlivých osobních údajů v informačních systémech a jejich nedostatečné zabezpečení vyvolávaly obavy z jejich zneužití pro komerční či jiné účely.[20]

Ochrana základních lidských práv a svobod se v prostředí moderních technologií postupně proměnila v ochranu citlivých osobních údajů v informačních systémech. Poškozenými byli zejména občané, jejichž osobní údaje bylo možné zneužít bez jejich vědomí. V tomto období stát reagoval tvorbou nové legislativy zaměřené na ochranu osobních údajů a současně docházelo ke vzniku a rozvoji specializovaných státních institucí, jejichž úkolem bylo dohlížet na dodržování těchto pravidel.[21]

3.3 Počátek období 21. století

Toto období bylo poznamenáno prohlubující se globalizací a dalším rozvojem informačních a telekomunikačních technologií, které se staly dostupné široké veřejnosti. Internet se již nevyužíval pouze jako pracovní nástroj státních a nestátních institucí, ale stal se součástí každodenního života středně společensky situovaných rodin. Často

[18] VLČEK, M. *Počítače a kriminalita: trestněprávní a kriminologické aspekty*. Praha: Academia, 1989, s. 42–44. ISBN 80-200-0139-5.
[19] RAK, R. a kol. *Kybernetická kriminalita*. Karlovy Vary: Vysoká škola Karlovy Vary, 2013, s. 22–24.
[20] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, s. 78–80. ISBN 978-80-7380-558-4.
[21] HOLT, T. J.; BOSWORTH, A. M.; GRIMES, J. B. *Cybercrime and Digital Forensics*. London: Routledge, 2015, s. 51–53. ISBN 978-1-138-02130-3.

se hovoří o tzv. „všemasovém konzumenství“. Více než 50 % domácností využívalo osobní počítače.[22]

Docházelo k masovému používání mobilní komunikace, mobilních telefonů a bezdrátových přenosů dat pomocí technologie Wireless Fidelity (Wi-Fi). Technologie začala sloužit rovným dílem institucím i občanům. Následkem masového využití technologií stoupal objem zpracovávaných, přenášených a uchovávaných dat. Informační systémy obsahovaly data všech oblastí lidské aktivity i údaje o jejich původcích.[23]

V digitální podobě lze nalézt více informací o jednotlivci, než znají jeho blízcí či kolegové. Orientace na uživatelskou přívětivost technologií, poháněná komerčním tlakem a snahou o co největší rozšíření produktů, nesla s sebou i rizika. Počet uživatelů rostl, ale jejich počítačová gramotnost spíše klesala. Slabiny v zabezpečení telekomunikačních a datových přenosů se staly hlavním problémem výpočetních a technologických systémů.[24]

Reálnou hrozbou začal být kybernetický terorismus, který mohl s relativně jednoduchými a nenákladnými prostředky vést k ochromení státu. Počítačová kriminalita byla často spojována s termínem „teroristický útok“. Jako příklad lze uvést celosvětově známý čin z 11. září 2001 v New Yorku. Tyto události ovlivnily i svět informačních a komunikačních technologií.[25]

Po útocích se předpokládalo, že se kybernetický terorismus stane novou zbraní útočníků. Nebyly však zaznamenány žádné významné aktivity v této oblasti, a proto se o problematice přestalo hovořit. Ostražitost bezpečnostních specialistů však neklesla. Začaly se ozývat hlasy volající po zpřísnění předpisů, zejména v oblasti monitorování elektronické komunikace. Část odborníků zastávala názor, že by bylo vhodné vzdát se části soukromí výměnou za vyšší bezpečnost, jiní upozorňovali na riziko zásahů do základních práv občanů.[26]

---

[22] RAK, Roman a kol. *Kybernetická kriminalita.* Karlovy Vary: Vysoká škola Karlovy Vary, 2013, s. 24–27. ISBN 978-80-87182-72-3.
[23] SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015, s. 82–84. ISBN 978-80-7380-558-4.
[24] SMEJKAL, Vladimír. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015, s. 85–86. ISBN 978-80-7380-558-4.
[25] MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002, s. 112–113. ISBN 80-7226-676-0.
[26] HOLT, Thomas J.; BOSWORTH, Adam M.; GRIMES, Joshua B. *Cybercrime and Digital Forensics.* Routledge, 2015, s. 59–62. ISBN 978-1-138-02130-3.

Je také důležité zmínit vznik tří technologických zlomů, které umožnily masivní rozvoj počítačové kriminality:

- nástup osobních počítačů,
- vznik počítačových sítí a vzdáleného přístupu,
- exponenciální růst mobilní telefonie a dostupnost anonymních předplacených karet.[27]

Nové technologie otevřely pachatelům cestu k novým možnostem, jak využívat počítače pro klasickou trestnou činnost, která se stávala snáze proveditelnou. Významnou oblastí se staly činy podle ustanovení:

- § 209 – Podvod,
- § 230 – Neoprávněný přístup k počítačovému systému a nosiči informací,
- § 231 – Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému.

Masivními se staly také útoky na funkčnost počítačových systémů. Začalo nasazování různých typů malware a spyware, útoky organizované státy či teroristickými skupinami a snahy získat obsah nebo informace zpracovávané na počítačích či přenášené v datových sítích.[28]

Závěrečnou kategorií trestné činnosti spojené s počítači a elektronickými komunikacemi je porušování autorských práv, označované jako počítačové pirátství.

3.4 Současné trendy a nové formy kybernetické kriminality

Současné trendy kybernetické kriminality jsou úzce spjaty s dynamickým rozvojem digitálních technologií a jejich masovým využíváním v každodenním životě. Kybernetický prostor se stal prostředím, ve kterém dochází k páchání trestné činnosti

[27] RAK, Roman a kol. *Kybernetická kriminalita.* Karlovy Vary: Vysoká škola Karlovy Vary, 2013, s. 27–29. ISBN 978-80-87182-72-3.
[28] HOLT, Thomas J.; BOSWORTH, Adam M.; GRIMES, Joshua B. *Cybercrime and Digital Forensics.*, s. 71–75.

s minimálními náklady, vysokou mírou anonymity a obtížnou vymahatelností práva. Pachatelé již nejsou omezeni geografickými hranicemi a mohou své aktivity realizovat z jakéhokoli místa na světě.[29]

Významným trendem posledních let je profesionalizace kybernetické kriminality. Pachatelé často působí v organizovaných skupinách, které fungují na principu dělby práce. Vznikl fenomén označovaný jako *Crime-as-a-Service*, kdy jsou jednotlivé nástroje, služby nebo celé útoky nabízeny na specializovaných internetových fórech a tržištích. Tyto služby zahrnují například tvorbu škodlivého softwaru, provoz phishingových kampaní nebo zajištění anonymní infrastruktury.[30]

Dalším výrazným trendem je zneužívání umělé inteligence a automatizovaných nástrojů. Umělá inteligence umožňuje vytváření realistických falešných obrazových, zvukových a audiovizuálních záznamů, tzv. *deepfake*. Tyto technologie jsou zneužívány k podvodům, vydírání nebo k manipulaci s veřejným míněním. V kombinaci se sociálním inženýrstvím představují deepfake technologie významné bezpečnostní riziko, neboť výrazně zvyšují důvěryhodnost podvodných scénářů.[31]

Specifickým prostředím pro páchání kybernetické kriminality je darknet, který umožňuje anonymní komunikaci a obchodování. Na darknetových tržištích dochází k prodeji nelegálního zboží a služeb, včetně kradených osobních údajů, přístupových údajů k účtům, platebních karet nebo nástrojů určených k páchání trestné činnosti. Anonymita tohoto prostředí výrazně komplikuje činnost orgánů činných v trestním řízení.

Současná kybernetická kriminalita se stále častěji zaměřuje na běžné uživatele internetu, kteří se stávají oběťmi podvodů, vydírání nebo krádeží identity. Typickým příkladem jsou inzertní podvody, které využívají důvěry uživatelů v online prostředí a kombinují technické prostředky s psychologickým nátlakem. Tyto formy trestné činnosti představují významnou výzvu nejen pro bezpečnostní složky, ale i pro oblast prevence a vzdělávání veřejnosti.[32]

[29] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, s. 101–103. ISBN 978-80-7380-558-4.
[30] KOLOUCH, J. *Cybercrime*. Praha: CZ.NIC, 2016, s. 156–159. ISBN 978-80-88168-18-8.
[31] CASEY, E. *Digital Evidence and Computer Crime*. Burlington: Academic Press, 2011, s. 215–218. ISBN 978-0-12-374268-1.
[32] ALBRECHT, Ch. D. a kol. *Fraud Examination*. Boston: Cengage Learning, 2016, s. 312–315. ISBN 978-1-337-61867-7.

4 Právní rámec kybernetické kriminality v České republice

Kybernetická kriminalita představuje oblast trestné činnosti, která se neustále vyvíjí a reaguje na technologický pokrok. Právní úprava v České republice proto kombinuje trestněprávní předpisy, zákony v oblasti kybernetické bezpečnosti a evropské normy, které společně vytvářejí rámec pro postih pachatelů, ochranu poškozených a prevenci kybernetických hrozeb. Tento rámec je klíčový nejen pro orgány činné v trestním řízení, ale také pro provozovatele informačních systémů a běžné uživatele internetu.

4.1 Trestní zákoník

Základním předpisem upravujícím trestné činy spojené s kybernetickou kriminalitou je zákon č. 40/2009 Sb., trestní zákoník. Ten obsahuje několik skutkových podstat, které se přímo vztahují k neoprávněnému přístupu, manipulaci s daty nebo podvodnému jednání v online prostředí.

Mezi nejvýznamnější ustanovení patří:

- **§ 230 – Neoprávněný přístup k počítačovému systému a nosiči informací**
  Postihuje pachatele, kteří se neoprávněně dostanou do počítačového systému, obcházejí zabezpečení nebo manipulují s daty.[33]

- **§ 231 – Opatření a přechovávání přístupového zařízení a hesla**
  Týká se držení nebo šíření přístupových údajů, které mohou být zneužity k trestné činnosti.

- **§ 232 – Poškození záznamu v počítačovém systému a na nosiči informací**
  Postihuje úmyslné mazání, pozměňování nebo blokování dat.

- **§ 209 – Podvod**
  Nejčastěji využívané ustanovení u inzertních podvodů, kdy pachatel uvede oběť v omyl s cílem získat prospěch.[34]

[33] GŘIVNA, T.; POLČÁK, R. *Kyberkriminalita a právo.* Praha: Auditorium, 2008, s. 112–115.
[34] MATĚJKA, M. *Počítačová kriminalita.* Praha: Computer Press, 2002, s. 72–75.

- **§ 181 – Poškození cizích práv**
  Používá se v případech zneužití identity jiné osoby.

Odborný výklad těchto ustanovení je podrobně rozpracován v komentářích k trestnímu zákoníku, které zdůrazňují zejména význam úmyslu pachatele, způsob provedení a dopad na poškozeného.[35]

4.2 Zákon o kybernetické bezpečnosti

Základním předpisem upravujícím oblast kybernetické bezpečnosti v České republice je zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Tento zákon stanovuje povinnosti správcům a provozovatelům informačních systémů, definuje bezpečnostní opatření a upravuje hlášení kybernetických incidentů.[36]

Významnou změnu přinesla **novela zákona č. 264/2025 Sb.**, která nabyla účinnosti dne **1. listopadu 2025**. Tato novela implementuje směrnici Evropského parlamentu a Rady (EU) 2022/2555 (NIS2) do českého právního řádu a zásadně rozšiřuje okruh povinných subjektů, zpřísňuje požadavky na bezpečnostní opatření a zavádí vyšší sankce za jejich porušení.[37] Novela rovněž posiluje pravomoci Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), zejména v oblasti kontroly a řízení kybernetických incidentů.

Odborný výklad principů kybernetické bezpečnosti, povinností organizací a role státu v této oblasti je podrobně popsán v odborné literatuře, která zdůrazňuje zejména význam prevence, řízení rizik a včasné detekce incidentů.[38]

4.3 Mezinárodní a evropské předpisy

Kybernetická kriminalita je globální problém, a proto je nutná mezinárodní spolupráce. Česká republika je součástí několika klíčových mezinárodních rámců.

[35] ŠÁMAL, P. a kol. *Trestní zákoník. Komentář.* 2. vydání. Praha: C. H. Beck, 2023, s. 1450–1455.
[36] ČESKO. Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In Sbírka zákonů, Česká republika. 2014, částka 75, s. 2226-2249.
[37] ČESKO. Zákon č. 264/2025 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In Sbírka zákonů, Česká republika. 2025, částka 108, s. 3120-3125.
[38] SMEJKAL, V. *Kybernetická kriminalita.* Plzeň: Aleš Čeněk, 2015, s. 210–213.

4.3.1 Budapešťská úmluva o kyberkriminalitě (2001)

První mezinárodní smlouva zaměřená na harmonizaci trestního práva v oblasti kybernetické kriminality a zajištění spolupráce mezi státy.[39]

4.3.2 Směrnice NIS a NIS2

Stanovují povinnosti pro členské státy EU v oblasti kybernetické bezpečnosti, včetně ochrany kritické infrastruktury a hlášení incidentů. Směrnice NIS2 nahrazuje původní směrnici NIS a zavádí přísnější požadavky na řízení rizik, povinné bezpečnostní standardy a rozšíření okruhu povinných subjektů

4.3.3 Obecné nařízení o ochraně osobních údajů (GDPR)

GDPR představuje základní evropský předpis v oblasti ochrany osobních údajů. Ačkoli se primárně zaměřuje na zpracování osobních dat, má přímý dopad i na kybernetickou bezpečnost, protože ukládá povinnost chránit osobní údaje před neoprávněným přístupem, ztrátou nebo zneužitím.[40]

Nutnost jednotného postupu států a vzájemné sdílení informací za pomocí kterých lze efektivněji proti kyberkriminalitě, respektive osobám, které tuto kriminalitu páchají bojovat, je uváděn již ve starších odborných literaturách, kdy jedna z nich je kniha autora Martina Vlčka z roku 1989: Počítače a kriminalita: trestněprávní a kriminologické aspekty.[41] Je tedy zřejmé, že společný postup států napříč světa a tím nutnost tvorby mezinárodních smluv je plně odůvodněn.

[39] ČESKO. Sdělení Ministerstva zahraničních věcí č. 104/2013 Sb. m. s. o sjednání Úmluvy o kyberkriminalitě. In Sbírka mezinárodních smluv, Česká republika. 2013, částka 45, s. 1051-1087.
[40] ČESKO. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In Úřední věstník Evropské unie. 2016, L 119, s. 1-88.
[41] VLČEK, M. *Počítače a kriminalita: trestněprávní a kriminologické aspekty.* Praha: Academia, 1989, s. 41–43.

5 Bezpečnostní chování uživatelů internetu

Útočníci v kyberprostoru se stále více zdokonalují a využívají dokonalejší a vychytralejší postupy. Existují základní principy chování uživatele internetu, které – když je běžný uživatel dodržuje – sice nezamezí veškerým možným útokům a nástrahám, jež na něj v kyberprostoru číhají, ale výrazně sníží procento úspěšnosti útočníků, kteří by dosáhli svého cíle. Na nutnost dodržování těchto zásad dlouhodobě upozorňuje odborná literatura i Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).[42]

5.1 Používání originálního softwaru

Zde se nejedná přímo o zásadu chování na internetu, ale přímo souvisí s tímto problémem. Pokud si uživatel stáhne nebo nainstaluje do svého počítače, tabletu či mobilního telefonu software, který nepochází z ověřeného zdroje, či dokonce software tzv. „crackovaný“ – což je software, který je standardně přímo od výrobce placený, ale někdo jej upravil, aby ho bylo možné používat zdarma (počítačové hry, kancelářské programy, operační systém…) – riskuje, že ten, kdo program upravoval, do něj vložil nějaký druh škodlivého softwaru (malware). Odborné publikace uvádějí, že nelegální software patří mezi nejčastější zdroje infekce škodlivým kódem.[43]

5.2 Aktualizace softwaru

Pravidelná aktualizace softwaru, ať už operačního systému či jiných aplikací, je důležitá z toho důvodu, že výrobci softwaru neustále pracují na zabezpečení svých aplikací a optimalizují je tak, aby byly vůči útokům imunní. Výrobci mají vlastní týmy legálních „hackerů“, kteří napodobují útoky aktuálně známými způsoby a své aplikace vůči těmto útokům upravují.

U uživatele, jenž používá zastaralou a neaktualizovanou aplikaci, je vyšší pravděpodobnost, že jeho software bude útočníky překonán, protože využijí zranitelnost aplikace, která by byla aktualizací odstraněna. Útočník bude postupovat

[42] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Minimální bezpečnostní standard v1.2 [online]. Brno: NÚKIB, 2023 [cit. 2026-03-09]. Dostupné z WWW: <https://nukib.gov.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf>.

[43] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, s. 210–213. ISBN 978-80-7380-558-4.

„cestou menšího odporu“.[44] NÚKIB doporučuje mít automatické aktualizace zapnuté všude, kde je to možné.

5.3 Bezpečné připojení k internetu

Je důležité používat pouze bezpečné připojení k internetu. Zejména při používání bezdrátového připojení je nutné mít síť dostatečně šifrovanou, a to nejen samotným heslem pro připojení k Wi-Fi, ale také zabezpečením zařízení, díky kterému se k Wi-Fi síti bude možné připojovat (Wi-Fi router, Access Point (AP) apod.). Toto zařízení by mělo být dostatečně zabezpečeno silným heslem.

Většina uživatelů nevěnuje zabezpečení těchto zařízení větší pozornost, přitom z výroby bývá uživatelské jméno a heslo pro vstup do administrace tohoto zařízení v jednoduchém základním formátu „admin“ a „admin“. Pro případného útočníka potom není složité změnit si v administraci zařízení heslo k Wi-Fi, popř. si vytvořit další vlastní podsíť, díky které se pak může zcela anonymně v síti pohybovat.

Zároveň je nutné, aby se uživatelé internetu vyhýbali připojení k veřejným Wi-Fi sítím bez dostatečného zabezpečení. Jedná se například o internetové kavárny, různé druhy „free Wi-Fi“ v restauracích či obchodech apod. Jako vhodné zabezpečení je doporučeno využít běžným uživatelem např. virtuální soukromou síť VPN (Virtual Private Network) a až přes tuto síť dále se zařízením pracovat.

5.4 Používání silných hesel

Je důležité používat unikátní a silná hesla pro každý účet. Silná hesla by měla obsahovat kombinaci velkých a malých písmen, čísel a speciálních znaků. Je nutné vyhýbat se použití snadno uhodnutelných hesel, jako jsou datum narození, jméno apod.

Dále je více než vhodné využívat pro přihlašování tzv. dvoufázové ověřování (2FA)[45] – což je způsob přihlášení, jenž vyžaduje dva nezávislé způsoby ověření identity uživatele, jako je heslo a ověřovací kód poslaný např. na mobilní telefon. Tento kód s nikým nesdílet a nikam jej nepřeposílat. Odborné zdroje uvádějí, že 2FA dokáže zabránit většině útoků založených na odcizení hesla.

[44] JIRÁSEK, P. Kybernetická bezpečnost v praxi. Praha, 2020, s. 56–57. ISBN 978-80-271-2056-4.
[45] JIRÁSEK, P.; NOVÁK, L.; POŽÁR, J. Výkladový slovník kybernetické bezpečnosti. Praha: Centrum kybernetické bezpečnosti, 2023. ISBN 978-80-908243-1-6.

5.5 Ochrana svého soukromí

Je nutné dobře zvážit, jaké informace bude o sobě uživatel sdílet na různých sociálních sítích a webových stránkách, a zároveň je důležité, aby bylo použito nastavení soukromí umožňující omezení viditelnosti příspěvků pouze určitému okruhu uživatelů (přátel).

Nikomu prostřednictvím e-mailů, online chatů či jiným obdobným způsobem neodesílat své intimní fotografie ani jiný materiál, který by mohl být zneužit třetí osobou. V online prostoru si nemůže být nikdo jistý, zda např. účet či e-mail osoby, se kterou komunikace probíhá, není zneužit jinou osobou.

GDPR (General Data Protection Regulation) ukládá povinnost chránit osobní údaje před neoprávněným přístupem, což se vztahuje i na běžné uživatele, kteří by měli dbát na bezpečné nakládání s daty.[46]

5.6 Základní znaky „nebezpečné“ webové stránky

Zabezpečená adresa (URL) – adresa musí začínat „http**s**“, kdy písmeno „**s**“ na konci znamená „secure“ (Hypertext Transfer Protocol Secure) neboli zabezpečená. Toto značí, že komunikace je šifrovaná. Dále je před touto adresou vyobrazen symbol zámečku, kdy po kliknutí na tento znak se můžeme dozvědět více o použitém certifikátu.

Překlepy v doméně – často používají překlepy, které nejsou na první pohled zjistitelné, např. „m“ místo „n“, „i“ místo „j“ apod.

Údaje o provozovateli webu – pokud se jedná např. o e-shop, je vhodné zkontrolovat údaje o provozovateli, včetně názvu firmy a IČO, každý e-shop je musí mít umístěny na svých stránkách, dále je vhodné přečíst si obchodní podmínky. Často bývají zkopírovány z jiné stránky, tedy nesedí kontakty, firma apod.

Kontaktní údaje – je potřebná kontrola, zda se na stránce nachází odpovídající kontaktní údaje nebo zda je zde pouze jednostranný formulář. Použití bezplatných emailových služeb taktéž nepřidá na důvěryhodnosti.

[46] ČESKO. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In Úřední věstník Evropské unie. 2016, L 119, s. 1-88.

Nadměrná reklama – pokud se na stránce nachází až příliš reklamních bannerů, vyskakovacích oken a láká-li stránka na až nesmyslně vysoké slevy, tak je dobré minimálně zbystřit pozornost.

Jazyk a obsah – pokud stránka budí špatný dojem v rámci obsahu a jazyka použitého na webové stránce. Může se jednat o strojový překlad z cizího jazyka, který útočníci často využívají.

6 Internetové podvody – případové studie

Trestný čin podvodu patří mezi jeden z nejčastěji páchaných trestných činů nejen v České republice, ale i v rámci celého světa. V právním řádu České republiky je tento čin definován v trestním zákoníku, konkrétně v § 209, kde je uvedeno, že „kdo sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoliv nepatrnou, dopustí se trestného činu podvodu.[47]

Dlouhou dobu bylo podvodné jednání spojováno především s osobním kontaktem pachatele a oběti, kdy podvodník využíval důvěry nebo nepozornosti oběti, aby ji uvedl v omyl a získal tak finanční nebo jiný majetkový prospěch. Typickým příkladem může být uzavření falešných smluv, vydávání se za někoho jiného nebo manipulace s dokumenty.

Nicméně s rozvojem digitálních technologií a rozšiřováním internetu dochází k výraznému posunu v charakteru páchaných podvodů. V dnešní době se stále více podvodů přesouvá z reálného světa do online prostředí. Podvody páchané na internetu se stávají dominantní formou tohoto trestného činu a klasické podvody jsou již pomalu na ústupu.

V rámci praktické části práce budou popsány dvě případové studie zaměřené především na bazarové podvody a jejich následné šetření. Byly vybrány dva případy, v nichž se podařilo ztotožnit pachatele, což vzhledem k anonymitě online internetového prostředí nebývá příliš často.

V těchto studiích budou změněna jména, data a místa, aby nebyla možná identifikace s reálnými osobami a případy. Jedná se o starší případy, které byly šetřeny v rámci zařazení na obvodním oddělení policie.

[47] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník. In Sbírka zákonů, Česká republika. 2009, částka 11, s. 427.

6.1 Podvodná inzerce – značkové boty

Na obvodní oddělení policie přišla paní Eva nahlásit podvod. Uvedla, že svému synovi objednala k Vánocům nové značkové boty, ale místo objednaných bot jí prodejce zaslal staré obnošené kopačky.

Paní Eva popsala skutek tak, že si na internetu vyhlédla značkové boty, jejichž hodnota v kamenném obchodě přesahovala částku 10.000 Kč. Na jednom inzertním serveru, který se specializoval na prodej oblečení a doplňků, je našla za 4.500 Kč. Tento server fungoval jako tzv. „nástěnka“, na které mohl každý registrovaný uživatel nabízet a nakupovat bazarové zboží. Server zajišťoval korektnost prodeje tím, že sloužil jako prostředník plateb mezi prodávajícím a kupujícím. Kupující za vybrané zboží zaplatil prostřednictvím platební brány na účet serveru, který přeposlal peníze prodejci až v okamžiku, kdy kupující udělil pozitivní recenzi o doručení. Paní Eva tento server znala, často ho využívala i k prodeji svého, již nepoužívaného oblečení. Rozhodla se kontaktovat prodejce bot prostřednictvím chatu serveru, aby získala podrobnější informace o inzerovaných botách. Prodejce jí téměř ihned odpověděl a sdělil, že se jedná o zcela nové, nikdy nepoužívané boty, které dostal jako dárek, ale protože již stejné má, rozhodl se tyto prodat. Poslal také fotografie bot jako důkaz, že boty jsou opravdu nové. Paní Evě se boty líbily a zakoupila je standardním způsobem, tedy kliknutím na tlačítko „koupit“ a zaplacením pomocí své platební karty prostřednictvím platební brány serveru.

Dva dny po koupi přišel paní Evě e-mail ze serveru s informací, že objednávka byla stornována prodejcem a peníze jí budou do pěti dnů vráceny na bankovní účet. Kontaktovala proto opětovně prodejce, aby zjistila důvod storna. Prodejce jí sdělil, že s prodejem přes server nemá zkušenosti a omylem klikl na možnost „storno prodeje“ místo „zboží jsem již odeslal”. Dále uvedl, že boty má již zabalené, ale nemůže je odeslat, protože by mu z důvodu storna nebyly vyplaceny peníze. Navrhl tedy, že jí zboží zašle prostřednictvím kurýrní služby na dobírku.

Protože se blížily Vánoce a paní Eva se obávala, zda by dárek pro syna dorazil včas, souhlasila s tímto způsobem doručení, i když to bylo zcela mimo kontrolu inzertního serveru. Sdělila prodejci adresu výdejního místa kurýrní služby, které se nachází v prodejně tabáku, ve které zároveň pracuje.

Za dva dny obdržela notifikaci o nové zásilce, ale místo do prodejny tabáku mělo být zboží doručeno do výdejního boxu kurýrní společnosti v sousední vesnici. Ihned

kontaktovala prodejce, který jí vysvětlil, že jí zvolené výdejní místo je před Vánoci přetíženo a jedinou možností poblíž byl výdejní box. (Paní Eva mu v předchozí komunikaci sdělila, že pracuje přímo na výdejním místě.)

Paní Eva si navíc ještě musela stáhnout a nainstalovat do svého telefonu aplikaci pro platbu a otevření výdejního boxu. Po pracovní době se vydala k výdejnímu boxu, zaplatila dobírku ve výši 4.500 Kč v aplikaci telefonu a zásilku vyzvedla. Protože nic nenasvědčovalo tomu, že by se jednalo o něco jiného než o boty, balíček ihned nerozbalila a spěchala do divadla. Balíček rozbalila až s třídenním zpožděním. Po otevření zjistila, že místo objednaných bot obdržela staré obnošené pánské kopačky.

Snažila se prodejce kontaktovat, ale jeho profil na prodejním serveru již neexistoval. Obrátila se proto na zákaznickou linku kurýrní služby a pokusila se zablokovat platbu dobírky. Operátorka jí poradila, aby vše nahlásila Policii České republiky (PČR), která o blokaci dobírky požádá. Protože byl pátek, paní Eva požádala operátorku o zdržení vyplacení dobírky do pondělí, jelikož věděla, že z rodinných důvodů se dříve na oddělení PČR nestihne dostavit. Operátorka slíbila, že udělá, co bude v jejích silách, ale nic negarantovala.

V pondělí, téměř týden po vyzvednutí balíčku (vyzvedla ho v úterý předchozího týdne), se paní Eva dostavila na obvodní oddělení PČR, aby věc nahlásila. Vzhledem k aktuálním informacím nebyly v policejních systémech zjištěny žádné společné znaky s jinými případy. Z tohoto důvodu byla vzhledem k výši způsobené škody věc zaevidována jako přestupek proti majetku dle § 8 odst. 1 písm. a) bod 3 zákona č. 251/2016 Sb.[48]

S paní Evou byl sepsán úřední záznam o podaném vysvětlení dle § 61 zákona č. 273/2008 Sb.[49] a následně byla datovou schránkou odeslána žádost o zajištění a vydání důkazního prostředku dle § 34 odst. 1 zákona č. 273/2008 Sb.[50] s odkazem na § 74 odst. 1, 2 zákona č. 250/2016 Sb.[51] a to na adresu kurýrní společnosti.

[48] ČESKO. Zákon č. 251/2016 Sb., o některých přestupcích. In Sbírka zákonů, Česká republika. 2016, částka 82, s. 3362-3372.
[49] ČESKO. Zákon č. 273/2008 Sb. o Policii České republiky. In Sbírka zákonů, Česká republika. 2008, částka 88, s. 4674-4712.
[50] ČESKO. Zákon č. 273/2008 Sb. o Policii České republiky. In Sbírka zákonů, Česká republika. 2008, částka 88, s. 4674-4712.
[51] ČESKO. Zákon č. 250/2016 Sb. o odpovědnosti za přestupky a řízení o nich. In Sbírka zákonů, Česká republika. 2016, částka 81, s. 3290-3361.

6.1.1 Šetření ve výše uvedené věci

V rámci šetření byla požádána zásilková společnost a inzertní server o poskytnutí všech doposud známých informací. Vzhledem k dlouhému časovému odstupu mezi platbou a nahlášenou události na PČR se však peníze již nepodařilo zajistit.

Podle informací od kurýrní společnosti byl balíček odeslán prostřednictvím boxu umístěného v malé vesnici v Jihomoravském kraji, prostřednictvím aplikace registrované na telefonní číslo XXX a e-mailovou adresu YYY. Dále byl zjištěn bankovní účet, na který byla platba dobírky odeslána. Jméno a příjmení uvedené při registraci bylo na první pohled smyšlené.

Na základě informací získaných od inzertního serveru byly zřejmé registrační údaje, které zahrnovaly smyšlené jméno, adresu vlakového nádraží, ve kterém se nacházel box a ze kterého došlo k odeslání podvodného balíčku, bankovní účet jiného čísla, než který byl zjištěn od kurýrní společnosti. Dále telefonní číslo, které rovněž nebylo shodné s telefonním číslem, které bylo uvedeno při prodeji. Ve vztahu k údajům platební karty nebylo zjištěno kompletní číslo karty, ale pouze jeho část, dále jméno, příjmení a konec platnosti karty. Byla zjištěna uživatelská přezdívka (NICK), jejíž části se vyskytovaly i v jedné z e-mailových adres.

Jméno z údajů ke kartě bylo lustrováno pomocí Centrálního registru obyvatel (CRO), byla zjištěna pouze jedna shoda s osobou z Jihomoravského kraje a bylo patrné, že má trvalý pobyt ve stejném okrese jako vesnice, kde stojí box, ze kterého byl odeslán balíček. Tato osoba byla prověřena i na sociálních sítích. V rámci přátel této osoby byla rozpoznána osoba, která měla příjmení nápadně podobné přezdívce i jednomu z použitých e-mailů.

Podrobnou lustrací této osoby byl zjištěn trvalý pobyt ve stejné obci, jako box zásilkové služby, ze kterého byl podvodný balíček odeslán. V rámci dalších šetření bylo blíže nespecifikovanými policejními postupy zjištěno, že telefonní čísla, která byla součástí případu, byla dříve použita v mobilním telefonu, ve kterém bylo použito telefonní číslo, ke kterému existuje v policejních evidencích konkrétní osoba. Bylo potvrzeno, že tato osoba je matka osoby, která má pobyt v obci, kde stojí box. Tímto způsobem došlo ke ztotožnění obou osob.

Na základě těchto zjištění byly sepsány žádosti o výslech všech ztotožněných osob. Vyšlo najevo, že osoba ustanovená z platební karty je bývalým spolužákem osoby pachatele. Ztotožněný pachatel při výslechu uvedl, že svého spolužáka využil. Řekl mu, že potřebuje něco zaplatit, protože sám nemá bankovní kartu. Spolužák s tím souhlasil a přitom nevěděl, že tím způsobem pachateli autorizoval účet na inzertním serveru.

Ztotožněná matka pachatele při výslechu uvedla, že první zjištěný bankovní účet zakládala svému nezletilému synovi jako studentský účet. Druhý bankovní účet byl přímo její osobní účet, který v minulosti používala, ale nyní ho také přenechala svému synovi jako tzv. „spořící". Dále sdělila, že svému synovi přenechala i svůj původní mobilní telefon. Ohledně předmětných bot uvedla, že u svého syna nikdy žádné takové boty neviděla a ani si není vědoma, že vůbec něco prodával.

Ztotožněný pachatel se při výslechu přiznal ke všem skutečnostem i k samotnému skutku. Uvedl, že tento podvod nebyl jeho jediný pokus, ale že šlo o první podvod, u kterého si byl jistý, že mu vyšel. Proto pak následně podobné skutky zopakoval ještě třikrát, přičemž celková částka přesáhla výši 20.000 Kč. Dále uvedl, že věci nelituje, bere to jako rychlý a jednoduchý výdělek.

Vzhledem k tomu, že byla ve věci zjištěna účast mladistvého a také na základě zjištěných skutečností se již nejednalo o přestupek, ale přečin „Podvod podle § 209 – trestního zákoníku"[52], převzala případ místně příslušná Služba kriminální policie a vyšetřování (SKPV), podle trvalého pobytu pachatele.

6.2 Podvodná inzerce – prodej mobilních telefonů

Na obvodní oddělení policie přišel pan Adam nahlásit podvod. Uvedl, že si na inzertním serveru vybral starší mobilní telefon v hodnotě 5.000 Kč. S prodejcem se domluvil, že zboží bude odesláno kurýrní službou a platba proběhne formou dobírky. Po třech dnech mu dorazil balíček na domácí adresu, který u kurýra zaplatil. Když však balíček rozbalil, místo mobilního telefonu v něm našel tři citrony.

Pan Adam se okamžitě pokusil reklamovat zásilku u kurýra, ale byl odkázán na oddělení policie. Protože v té době na základě dostupných informací nebylo zjištěno, že by se ve věci již vedlo společné trestní řízení a škoda činila 5.000 Kč, byla věc

[52] ČESKO. Zákon č. 40/2009 Sb. trestní zákoník. In Sbírka zákonů, Česká republika. 2009, částka 11, s. 318-479.

evidována jako přestupek proti majetku podle § 8 odst. 1 písm. a) bod 3 zákona č. 251/2016 Sb. [53]

S panem Adamem byl sepsán úřední záznam o podaném vysvětlení podle § 61 zákona č. 273/2008 Sb. Současně byla prostřednictvím datové schránky odeslána žádost kurýrní službě o zajištění a vydání důkazního prostředku podle § 34 odst. 1 zákona č. 273/2008 Sb., s odkazem na § 74 odst. 1, 2 zákona č. 250/2016 Sb.

V rámci svého vysvětlení pan Adam uvedl, že s prodejcem komunikoval pouze přes chatovací aplikaci WhatsApp a že si pouze psali. Prodejce na něj podle jeho slov působil „normálně“ a „seriózně“, takže nepojal žádné podezření, že by mohlo jít o podvod. Když se však po doručení balíčku s citrony snažil prodejce kontaktovat, zjistil, že veškerá předchozí komunikace již není k dispozici a prodejce nereaguje ani na volání, ani na zprávy.

6.2.1 Šetření ve výše uvedené věci

Ve věci bylo provedeno šetření, při kterém byla zásilková společnost a inzertní server požádány o veškeré dostupné informace. Současně se podařilo zajistit částku, kterou poškozený zaplatil prostřednictvím dobírky.

Na základě informací od zásilkové služby vyšlo najevo, že z téhož profilu byly odeslány ještě další dvě zásilky. Byla zjištěna tři čísla bankovních účtů a dvě další telefonní čísla. Inzertní server poskytl informace o minimálně deseti inzerátech podobného charakteru, IP adresy, ze kterých byly inzeráty vkládány a autorizační telefonní číslo, které sloužilo k ověření inzerátů před zveřejněním. Jelikož v rámci šetření vyšlo najevo, že shodný pachatel spáchal v rámci České republiky více skutků za pomoci stejného módu operandi s využitím shodných prostředků a tento případ přesáhl výší škody částku 10.000 Kč, která tvoří hranici mezi přestupkem a trestným činem, byly dále ve věci zahájeny úkony trestního řízení a další postup již probíhal podle trestního řádu. Byly vyžádány bankovní informace podle § 8 odst. 2 trestního řádu[54] a byla odeslána žádost o poskytnutí informací poskytovateli e-mailové schránky.

[53] ČESKO. Zákon č. 251/2016 Sb., o některých přestupcích. In Sbírka zákonů, Česká republika. 2016, částka 82, s. 3362-3372.
[54] ČESKO. Zákon č. 141/1961 Sb. o trestním řízení soudním (trestní řád). In Sbírka zákonů, Česká republika. 1961, částka 66, s. 441-486.

Díky získaným informacím byly ztotožněny tři osoby, přičemž podezření směřovalo k jedné z nich. Toto podezření vyplynulo z lustrace IP adres, které se protínaly ve všech objevených přístupech (e-mail, zásilková služba, inzertní server). Zjistilo se také, že tyto IP adresy pocházejí od místního poskytovatele internetu, který své služby nabízí pouze v pěti obcích, z nichž v jedné měla bydliště ztotožněná osoba.

Lustrace telefonních čísel byla neúspěšná. Zjištěno bylo pouze to, že pachatel používal jeden mobilní telefon se dvěma sloty na subscriber identity module (SIM). V obou případech se jednalo o předplacené karty.

V průběhu šetření vyšla najevo série podvodů s mobilními telefony. Bylo také zjištěno, že společné řízení již probíhalo na oddělení hospodářské kriminality (OHK) v jiném kraji. Zpracovatelem tohoto případu bylo sděleno, že evidují již 80 poškozených s celkovou škodou přesahující částku 400.000 Kč a ve věci mají podezřelého. Podezřelým byla shodná osoba, která byla námi zjištěna na základě zjištění IP adres.

Byl domluven další postup spočívající v přeslechnutí poškozených podle trestního řádu, jejich poučení dle TŘ, vydání případné komunikace dle TŘ a následném postoupení spisového materiálu na OHK.

7 Dotazníkové šetření

Dotazníkové šetření je výzkumná metoda, která slouží k systematickému sběru informací od respondentů prostřednictvím předem připravených otázek. Dotazníky mohou být distribuovány v tištěné podobě nebo online a jejich cílem je získat data týkající se určené problematiky od určité skupiny lidí. Tento nástroj se často používá v sociálních vědách, marketingu nebo při průzkumech veřejného mínění, protože umožňuje rychlý sběr velkého množství dat, která lze následně analyzovat.

7.1 Návrh otázek

Po stanovení tématu, na které byl dotazník zaměřen, byly sestaveny okruhy otázek. Nejdříve byly vytvořeny demografické otázky týkající se pohlaví, vzdělání, zaměstnání a věku.

U věku bylo zvoleno rozdělení podle generací. Toto dělení se často využívá ve veřejných diskuzích, studiích nebo výzkumech. Rozmezí let, které dělí jednotlivé generace, se mohou nepatrně lišit podle autorů a jejich pohledu. V této práci bylo použito členění z knihy *Generations: The History of America's Future, 1584 to 2069*, autorů Neila Howea a Williama Strausse.[55] Toto členění se zaměřuje na generace z hlediska jejich historického vývoje, sociokulturních trendů a technologického vývoje, které formulovaly jednotlivé generace.

Prvními jsou podle členění těchto autorů generace Silent, kteří se narodili před rokem 1946. Tito jsou následováni generací Baby Boomers, což jsou lidé narození mezi lety 1946–1964. Jedná se o skupinu, která vychází z rozsáhlého nárůstu porodnosti po válce a bývá často nejméně zapojena do sociálních sítí. Další kategorií je generace X, tedy lidé narození mezi lety 1965–1980. I tato generace bývá označována jako konzervativní v oblasti sociálních sítí a sdílení dat. Následuje generace Y (Millennials), zahrnující osoby narozené mezi lety 1981–1996, která je velmi aktivní na sociálních sítích. Poslední kategorií je generace Z, tedy lidé narození po roce 1997. Jedná se o skupinu, pro kterou jsou sociální sítě běžnou součástí každodenního života. Dále se lze setkat s označením generace Alfa, která je vymezována přibližně od roku 2013 do současnosti. Tato generace nebyla vzhledem k nízkému věku a zaměření dotazníku

[55] STRAUSS, William; HOWE, Neil. *Generations: The History of America's Future, 1584 to 2069.* New York: Harper Perennial, 1992, s. 60–65. ISBN 0688119123.

do šetření zahrnuta. Dále byly sestaveny otázky týkající se zkušeností s počítačovou kriminalitou, otázky zaměřené na obecné povědomí o počítačové kriminalitě a otázky týkající se bezpečnosti. Závěr dotazníku byl věnován otázkám týkajícím se návyků uživatelů při používání internetu a otázkám zaměřeným na prevenci.

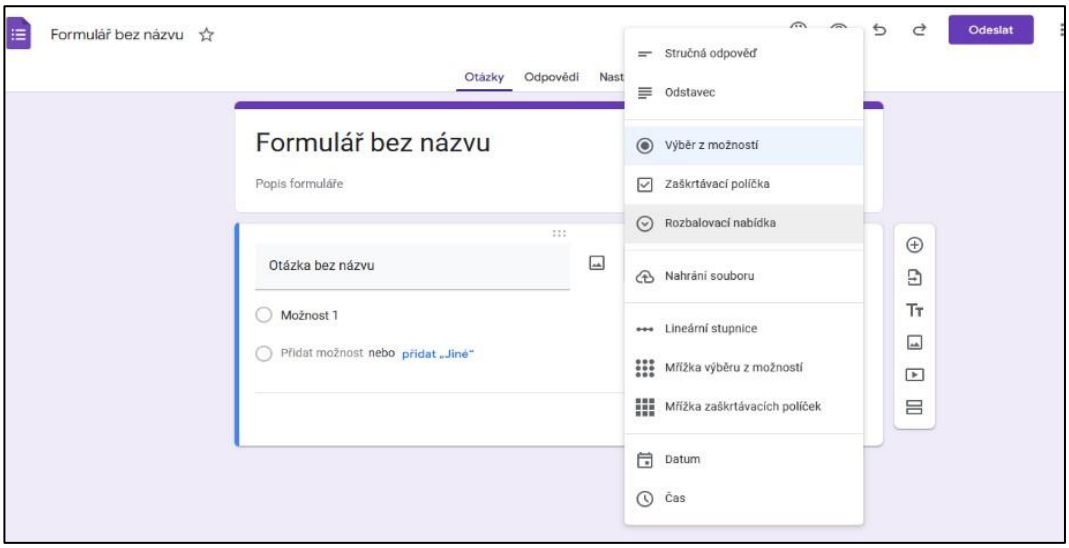
7.1.1 Tvorba dotazníku

Po sestavení otázek dotazníkového šetření bylo dalším krokem vytvoření dotazníku do podoby, která je snadno šiřitelná. K tomuto účelu byl využit nástroj společnosti Google – Google Forms. Tento nástroj je snadno dostupný, uživatelsky přívětivý a k jeho používání je zapotřebí pouze uživatelský účet společnosti Google.

Google Forms umožňuje rychlé a efektivní šíření dotazníků prostřednictvím internetu a zároveň jednoduchý sběr odpovědí. Odpovědi respondentů se automaticky ukládají do přehledných tabulek, které je možné dále exportovat v různých formátech a využít jako podklad pro další analýzu dat. Výhodou tohoto nástroje je rovněž možnost sledování odpovědí v reálném čase a jejich průběžná kontrola.

Právě z důvodu rychlosti, přehlednosti a efektivity byla pro účely tohoto dotazníkového šetření zvolena elektronická forma dotazníku prostřednictvím aplikace Google Forms.

Obrázek č. 1: Google Forms[56]



[56] Vlastní zpracování.

7.1.2 Rozeslání dotazníku respondentům

Elektronicky vytvořený dotazník byl nejprve prostřednictvím přímého odkazu rozeslán mezi menší okruh osob, aby bylo možné ověřit, zda jsou jednotlivé otázky pro respondenty srozumitelné a vhodně formulované.

Na základě zpětné vazby od tohoto zkušebního vzorku respondentů byly provedeny drobné úpravy formulace některých otázek. Následně byla rozeslána konečná verze dotazníku prostřednictvím sociálních sítí a komunikačních aplikací mezi známé, přátele a spolupracovníky, a to s prosbou o jeho další sdílení.

Aktuální stav vyplňování dotazníku a jednotlivé odpovědi respondentů byly průběžně sledovány v aplikaci Google Forms v reálném čase. Tento postup byl výhodný zejména z důvodu možnosti zaměřit se v případě potřeby na konkrétní skupiny respondentů, které byly v daném okamžiku zastoupeny v menší míře, a tím dosáhnout co nejvyrovnanějšího zastoupení jednotlivých skupin.

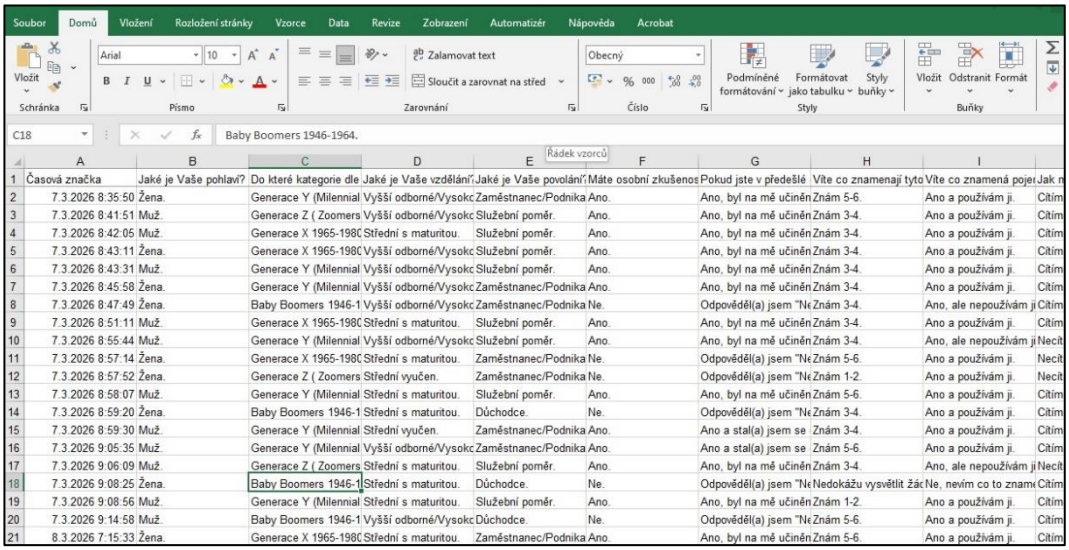
7.1.3 Zobrazení a ukládání dat

Odpovědi respondentů bylo možné sledovat přímo na hlavní stránce aplikace Google Forms, kde jsou jednotlivé otázky a odpovědi automaticky zobrazovány v přehledné grafické podobě. Tento způsob zobrazení umožňuje rychlou orientaci v průběžných výsledcích dotazníkového šetření.

Další možností bylo exportování získaných dat do tabulkového procesoru. Každá odpověď respondenta je v tomto případě zaznamenána do samostatného sloupce, ve kterém jsou shromažďovány jednotlivé odpovědi. Tento způsob práce s daty představuje významnou výhodu zejména pro jejich další zpracování a analýzu.

Jak již bylo uvedeno v úvodu kapitoly, elektronická forma sběru dat výrazně usnadňuje jejich následné zpracování v porovnání s klasickým, analogovým sběrem dat, kdy je nutné jednotlivé odpovědi ručně přepisovat a zpracovávat.

Obrázek č. 2: Export dat do aplikace Excel[57]



	A	B	C	D	E	F	G	H	I	
1	Časová značka	Jaké je Vaše pohlaví?	Do které kategorie dle	Jaké je Vaše vzdělání?	Jaké je Vaše povolání?	Máte osobní zkušenos	Pokud jste v předešlé	Víte co znamenají tyto	Víte co znamená pojer	Jak n
2	7.3.2026 8:35:50	Žena	Generace Y (Milennial	Vyšší odborné/Vysokc	Zaměstnanec/Podnika	Ano.	Ano, byl na mě učiněn	Znám 5-6.	Ano a používám ji.	Cítím
3	7.3.2026 8:41:51	Muž.	Generace Z (Zoomers	Vyšší odborné/Vysokc	Služební poměr.	Ano.	Ano, byl na mě učiněn	Znám 3-4.	Ano a používám ji.	Cítím
4	7.3.2026 8:42:05	Muž.	Generace X 1965-1980	Střední s maturitou.	Služební poměr.	Ano.	Ano, byl na mě učiněn	Znám 3-4.	Ano a používám ji.	Cítím
5	7.3.2026 8:43:11	Žena	Generace X 1965-1980	Vyšší odborné/Vysokc	Služební poměr.	Ano.	Ano, byl na mě učiněn	Znám 3-4.	Ano a používám ji.	Cítím
6	7.3.2026 8:43:31	Muž.	Generace Y (Milennial	Vyšší odborné/Vysokc	Služební poměr.	Ano.	Ano, byl na mě učiněn	Znám 3-4.	Ano a používám ji.	Cítím
7	7.3.2026 8:45:58	Žena	Generace Y (Milennial	Vyšší odborné/Vysokc	Zaměstnanec/Podnika	Ano.	Ano, byl na mě učiněn	Znám 3-4.	Ano a používám ji.	Cítím
8	7.3.2026 8:47:49	Žena	Baby Boomers 1946-1	Vyšší odborné/Vysokc	Zaměstnanec/Podnika	Ne.	Odpověděl(a) jsem "Ne	Znám 3-4.	Ano, ale nepoužívám ji	Cítím
9	7.3.2026 8:51:11	Muž.	Generace X 1965-1980	Střední s maturitou.	Služební poměr.	Ano.	Ano, byl na mě učiněn	Znám 3-4.	Ano a používám ji.	Cítím
10	7.3.2026 8:55:44	Muž.	Generace Y (Milennial	Vyšší odborné/Vysokc	Služební poměr.	Ano.	Ano, byl na mě učiněn	Znám 3-4.	Ano, ale nepoužívám ji	Necít
11	7.3.2026 8:57:14	Žena	Generace X 1965-1980	Střední s maturitou.	Zaměstnanec/Podnika	Ne.	Odpověděl(a) jsem "Ne	Znám 5-6.	Ano a používám ji.	Necít
12	7.3.2026 8:57:52	Žena	Generace Z (Zoomers	Střední vyučen.	Zaměstnanec/Podnika	Ne.	Odpověděl(a) jsem "Ne	Znám 1-2.	Ano a používám ji.	Necít
13	7.3.2026 8:58:07	Muž.	Generace Y (Milennial	Střední s maturitou.	Služební poměr.	Ano.	Ano, byl na mě učiněn	Znám 5-6.	Ano a používám ji.	Cítím
14	7.3.2026 8:59:20	Žena	Baby Boomers 1946-1	Střední s maturitou.	Důchodce.	Ne.	Odpověděl(a) jsem "Ne	Znám 3-4.	Ano a používám ji.	Cítím
15	7.3.2026 8:59:30	Muž.	Generace Y (Milennial	Střední vyučen.	Zaměstnanec/Podnika	Ano.	Ano a stal(a) jsem se	Znám 3-4.	Ano a používám ji.	Cítím
16	7.3.2026 9:05:35	Muž.	Generace Y (Milennial	Vyšší odborné/Vysokc	Zaměstnanec/Podnika	Ano.	Ano a stal(a) jsem se	Znám 5-6.	Ano a používám ji.	Cítím
17	7.3.2026 9:06:09	Muž.	Generace Z (Zoomers	Střední s maturitou.	Služební poměr.	Ano.	Ano, byl na mě učiněn	Znám 3-4.	Ano, ale nepoužívám ji	Necít
18	7.3.2026 9:08:25	Žena	Baby Boomers 1946-1	Střední s maturitou.	Důchodce.	Ne.	Odpověděl(a) jsem "Ne	Nedokážu vysvětlit žá	Ne, nevím co to znam	Cítím
19	7.3.2026 9:08:56	Muž.	Generace Y (Milennial	Střední s maturitou.	Služební poměr.	Ano.	Ano, byl na mě učiněn	Znám 1-2.	Ano a používám ji.	Cítím
20	7.3.2026 9:14:58	Muž.	Baby Boomers 1946-1	Vyšší odborné/Vysokc	Důchodce.	Ne.	Odpověděl(a) jsem "Ne	Znám 5-6.	Ano a používám ji.	Cítím
21	8.3.2026 7:15:33	Žena	Generace X 1965-1980	Střední s maturitou.	Zaměstnanec/Podnika	Ano.	Ano, byl na mě učiněn	Znám 5-6.	Ano a používám ji.	Cítím

7.2 Analýza dat

Po ukončení sběru dat byla získaná data exportována do tabulkového procesoru Microsoft Excel. Následně byla provedena kontrola úplnosti a správnosti jednotlivých odpovědí a poté samotná analýza dat. Program Microsoft Excel byl zvolen z důvodu dostupnosti a možnosti využití základních statistických funkcí, které byly pro zpracování dat dostačující.

Získaná data byla rozdělena do několika tematických oblastí, a to na oblast demografickou, oblast povědomí o hrozbách a ochranu a oblast pohybu respondentů v kyberprostoru. Toto rozdělení umožnilo přehlednější vyhodnocení jednotlivých okruhů otázek a jejich následnou interpretaci.

7.2.1 Popisná statistika

Celkem bylo získáno 126 vyplněných dotazníků. V prvních hodinách po rozeslání dotazníku počet odpovědí rychle narůstal, přibližně po 48 hodinách se však tempo přibývání odpovědí výrazně zpomalilo.

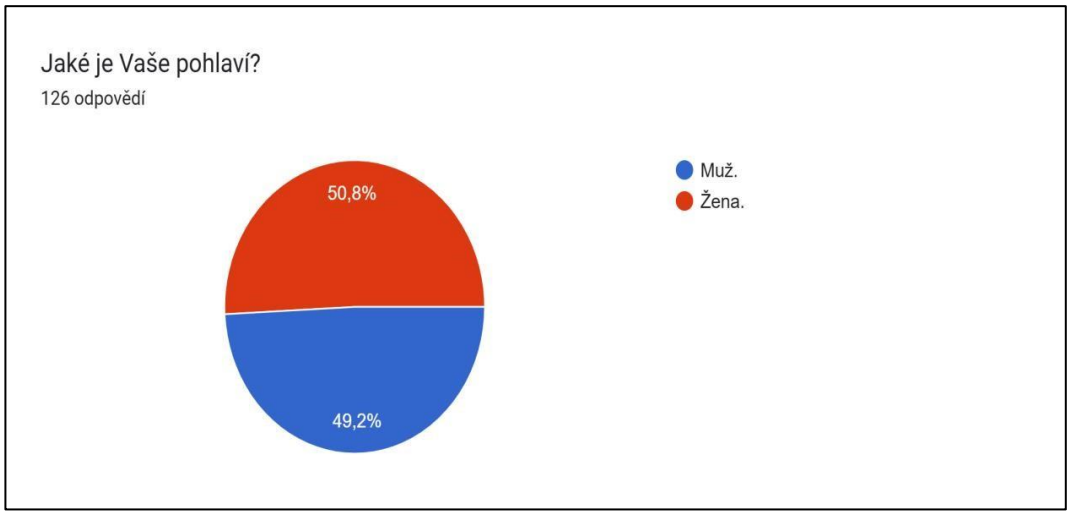
Odpovědi respondentů byly rozděleny do tří oblastí, a to na oblast demografickou, oblast povědomí o hrozbách a ochranu a oblast pohybu respondentů v kyberprostoru.

[57] Vlastní zpracování.

Demografické otázky:

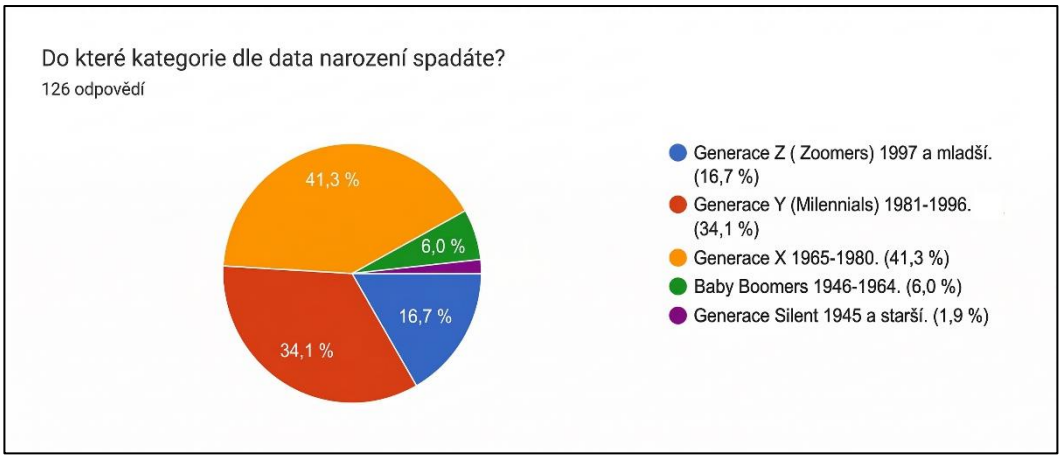
Dotazníkového šetření se zúčastnilo celkem 64 žen a 62 mužů, přičemž zastoupení pohlaví bylo poměrně vyrovnané.

Graf č. 1: Rozdělení podle pohlaví[58]



Věkové kategorie respondentů byly rozděleny podle generací, jejichž členění je zaměřeno na historický vývoj, sociokulturní trendy a technologický vývoj, které formovaly jednotlivé generace.

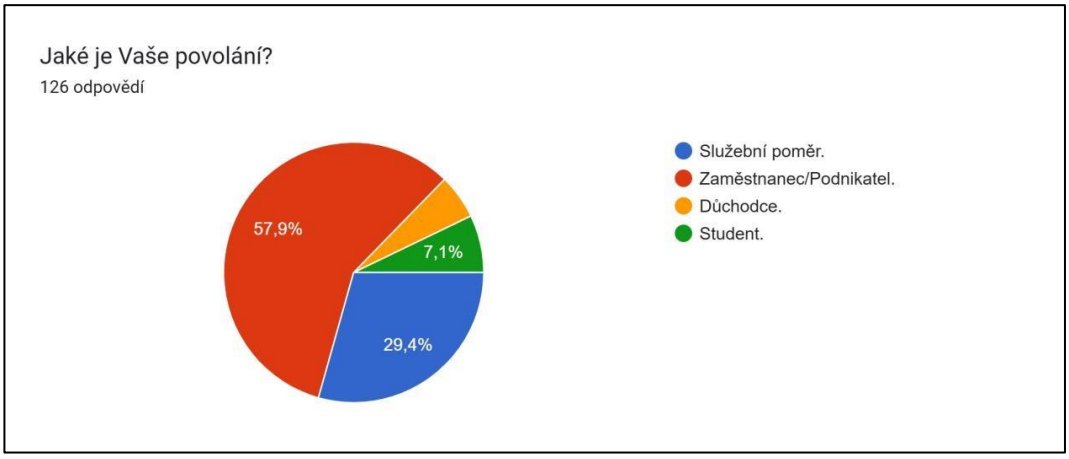
Graf č. 2: Rozdělení podle generací[59]



[58] Vlastní zpracování
[59] Vlastní zpracování

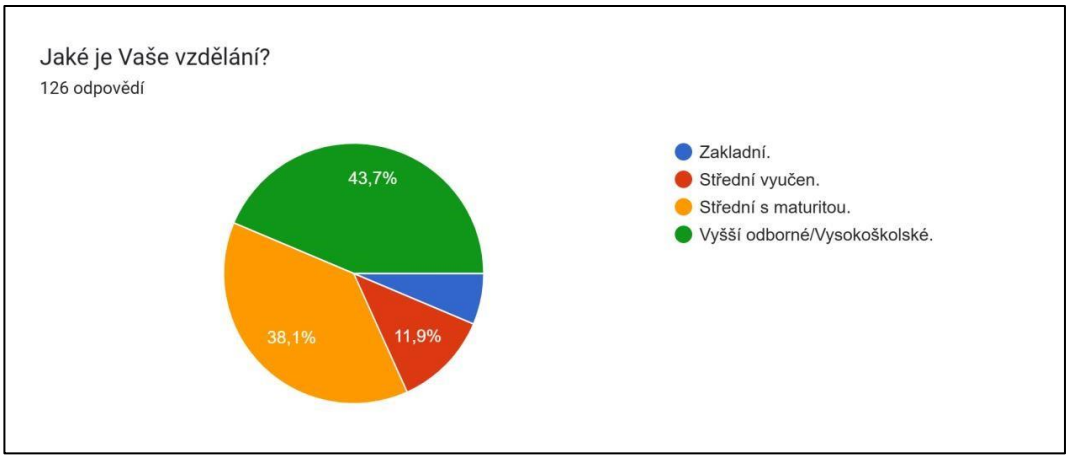
Na otázku týkající se povolání respondentů odpovědělo 57,9 % respondentů, že jsou zaměstnanci nebo podnikatelé, 29,4 % uvedlo služební poměr, 7,1 % respondentů byli důchodci a 5,6 % studenti.

Graf č. 3: Rozdělení podle povolání[60]



Dále bylo zjišťováno dosažené vzdělání respondentů. Vyšší odborné nebo vysokoškolské vzdělání uvedlo 43,7 % respondentů, střední vzdělání s maturitou 38,1 %, vyučení 11,9 % a základní vzdělání 6,3 % respondentů.

Graf č. 4: Rozdělení podle vzdělání[61]

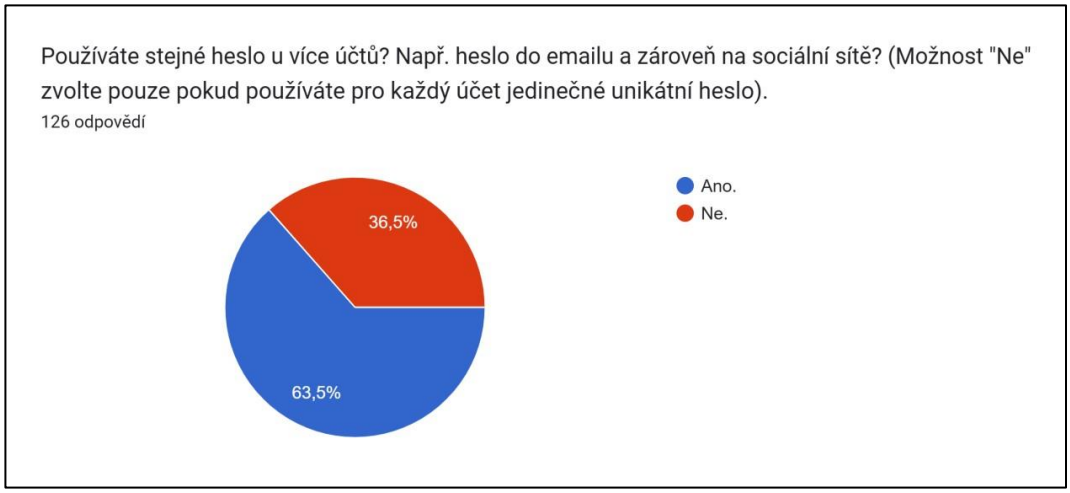


[60] Vlastní zpracování.
[61] Vlastní zpracování.

Oblast povědomí o hrozbách a ochrana:

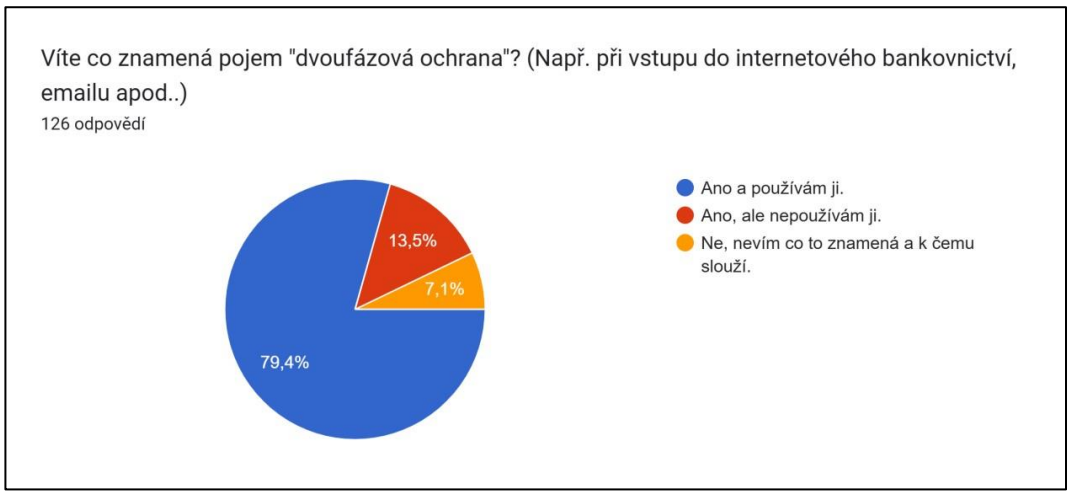
Na otázku, zda respondenti používají stejné heslo u více uživatelských účtů, odpovědělo 63,5 % respondentů kladně, zatímco 36,5 % uvedlo, že používá pro jednotlivé účty různá hesla.

Graf č. 5: Stejné heslo[62]



Na otázku týkající se povědomí o dvoufázové ochraně odpovědělo 79,4 % respondentů, že tuto formu zabezpečení zná a aktivně ji používá. Dalších 13,5 % respondentů uvedlo, že ví, co dvoufázová ochrana znamená, avšak ji nevyužívá. Pouze 7,5 % respondentů uvedlo, že neví, co dvoufázová ochrana je a k čemu slouží.

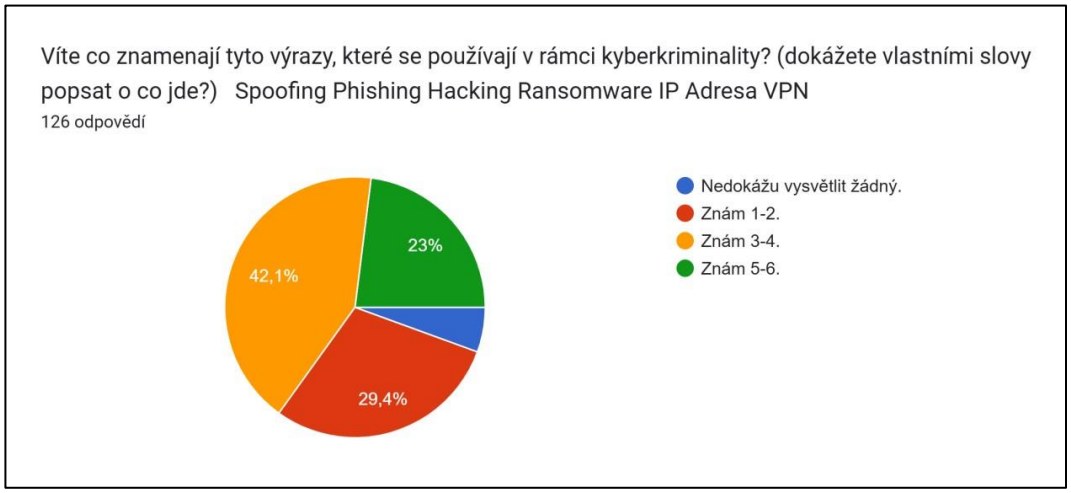
Graf č. 6: Dvoufázová ochrana[63]



[62] Vlastní zpracování.
[63] Vlastní zpracování.

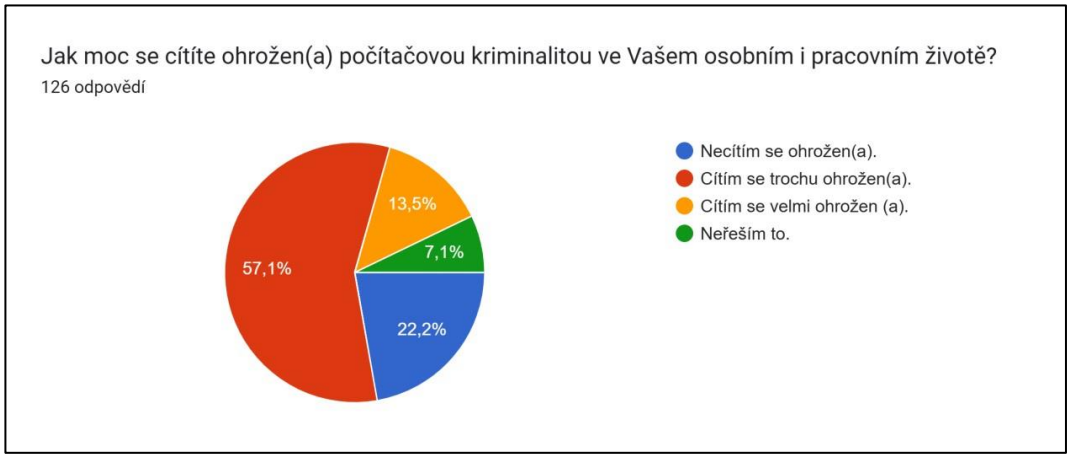
Další otázka byla zaměřena na znalost základních pojmů souvisejících s počítačovou kriminalitou, konkrétně pojmů spoofing, phishing, hacking, ransomware, IP adresa a VPN. Z výsledků vyplynulo, že 23 % respondentů dokáže vysvětlit pět až šest uvedených pojmů, 42,1 % respondentů zná tři až čtyři pojmy, 29,4 % respondentů zná jeden až dva pojmy a 5,6 % respondentů nedokáže vysvětlit žádný z uvedených.

Graf č. 7: Pojmy[64]



Na otázku, zda se respondenti cítí být ohroženi počítačovou kriminalitou, odpovědělo 57,1 % respondentů, že se cítí být ohroženi, 22,2 % uvedlo, že se ohroženi necítí, 13,5 % respondentů se cítí být velmi ohroženo a 7,1 % respondentů tuto problematiku vůbec neřeší.

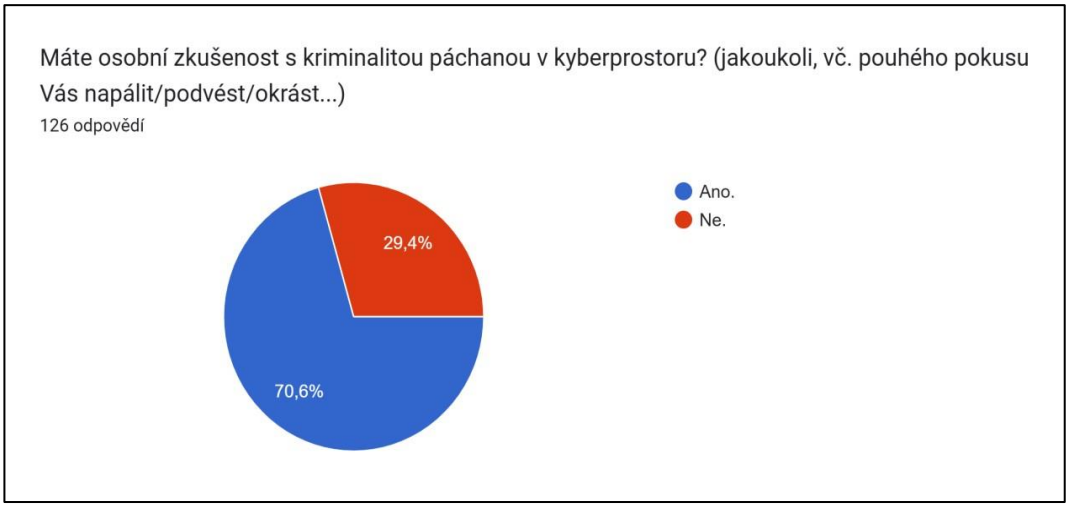
Graf č. 8: Pocit ohrožení[65]



[64] Vlastní zpracování.
[65] Vlastní zpracování.

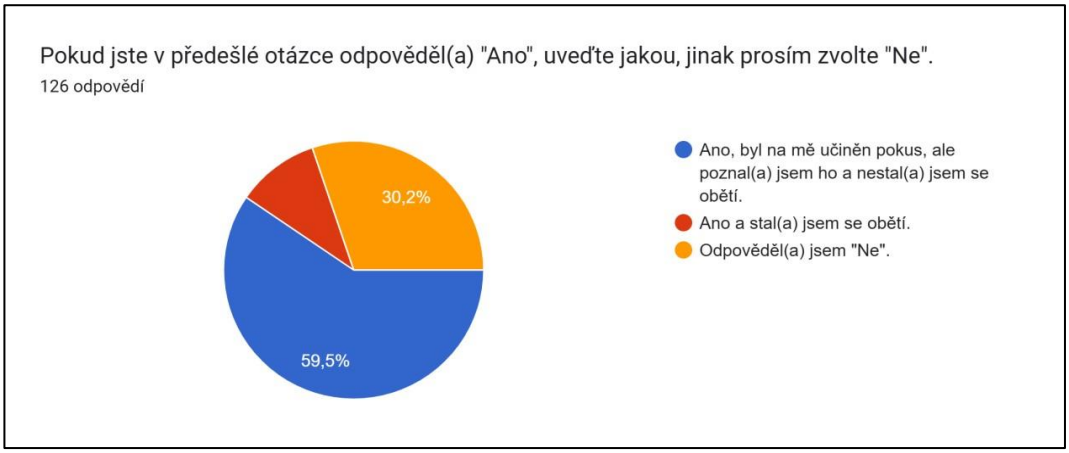
Na otázku týkající se osobní zkušenosti s kriminalitou páchanou v kyberprostoru odpovědělo 70,6 % respondentů kladně, zatímco 29,4 % uvedlo, že žádnou osobní zkušenost s kyberkriminalitou nemá.

Graf č. 9: Zkušenost s kyberkriminalitou[66]



V navazující otázce, která se týkala konkrétní zkušenosti a jejího dopadu, uvedlo 59,5 % respondentů, že se setkali s pokusem o podvod, avšak podařilo se jim jej rozpoznat a nestali se obětí. Dalších 10,3 % respondentů uvedlo, že se obětí kyberkriminality skutečně stali, a 30,2 % respondentů uvedlo, že žádnou zkušenost s kyberkriminalitou nemá.

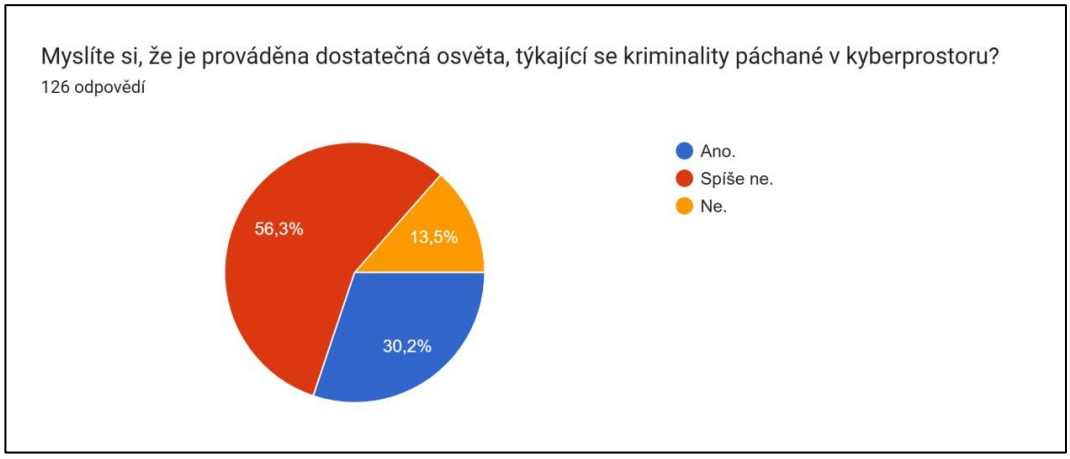
Graf č. 10: Zkušenost s kyberkriminalitou – dopad[67]



[66] Vlastní zpracování.
[67] Vlastní zpracování.

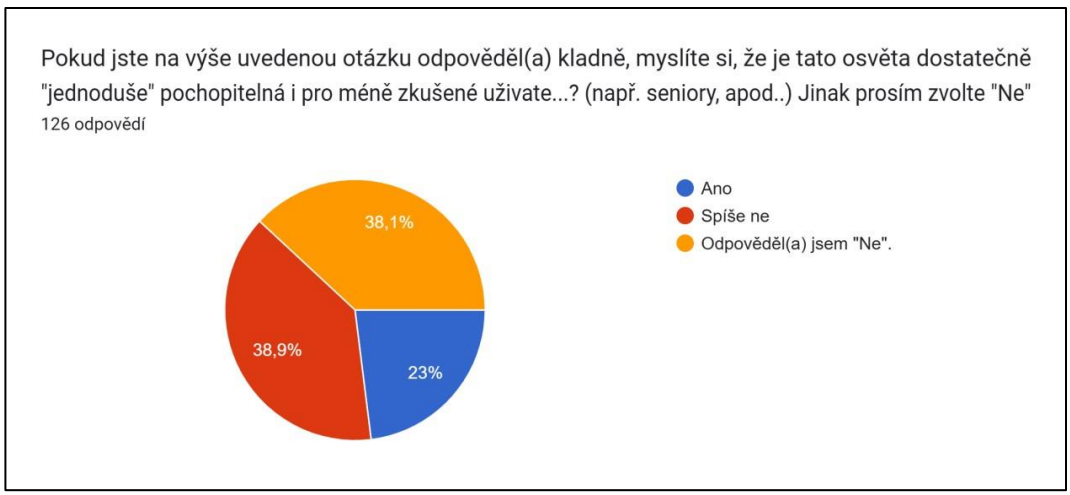
Na otázku, zda je podle respondentů prováděna dostatečná osvěta v oblasti kriminality páchané v kyberprostoru, odpovědělo 56,3 % respondentů, že spíše ne, 30,2 % respondentů uvedlo, že ano, a 13,5 % respondentů se domnívá, že osvěta není dostatečná.

Graf č. 11: Osvěta[68]



Z respondentů, kteří uvedli, že osvěta v oblasti kyberkriminality existuje, si 38,9 % myslí, že není dostatečně srozumitelná pro méně zkušené uživatele, například seniory. Naopak 23 % respondentů se domnívá, že je osvěta srozumitelná a dostačující.

Graf č. 12: Srozumitelnost osvěty[69]



[68] Vlastní zpracování.
[69] Vlastní zpracování.

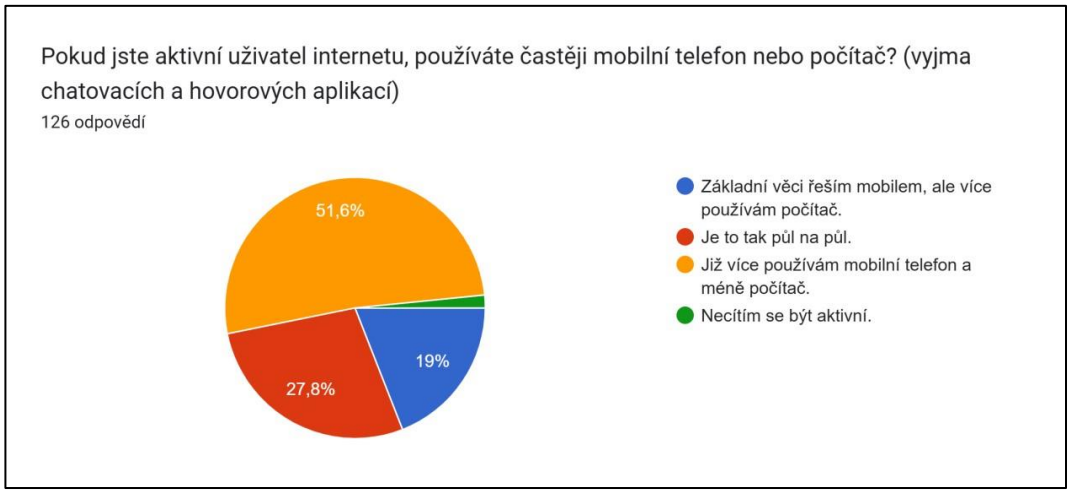
Na otázku, zda respondenti aktivně předcházejí kybernetickým útokům, odpovědělo 74,6 % respondentů, že se snaží navštěvovat pouze známé webové stránky, 6,3 % respondentů se aktivně zajímá o novinky v oblasti kybernetické bezpečnosti, 17,3 % respondentů spoléhá na automatickou ochranu internetových prohlížečů a operačních systémů a 1,6 % respondentů uvedlo, že se jich tato problematika netýká.

Graf č. 13: Předcházení kybernetickým útokům[70]

Oblast pohybování se v kyberprostoru:

Na otázku, zda respondenti při nákupech a pohybu v kyberprostoru preferují používání mobilního telefonu nebo počítače, odpovědělo 51,6 % respondentů, že využívá převážně mobilní telefon. Dalších 27,8 % respondentů uvedlo, že využívá obě zařízení přibližně stejnou měrou, 19 % respondentů používá více počítač a 1,6 % respondentů se nepovažuje za aktivního uživatele internetu.

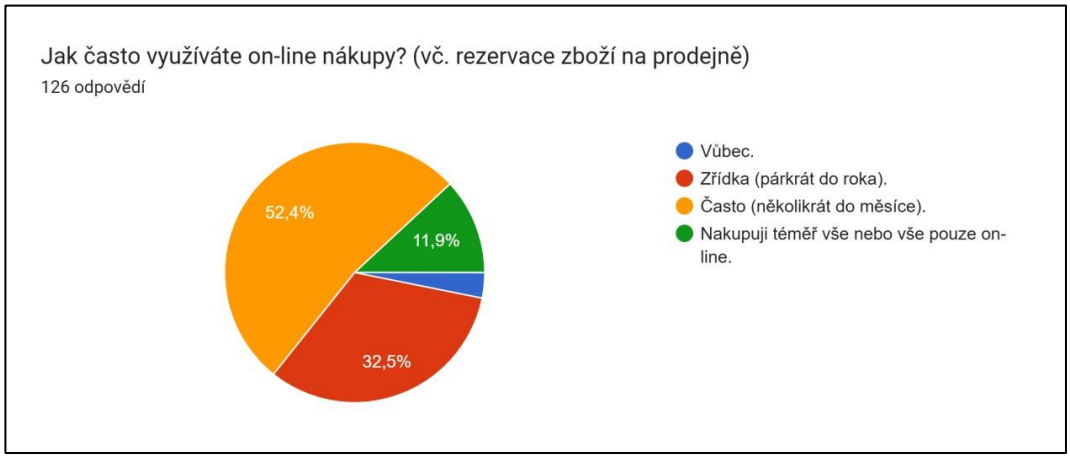
Graf č. 14: Poměr využití mobilního telefonu a počítače[71]



[70] Vlastní zpracování.
[71] Vlastní zpracování.

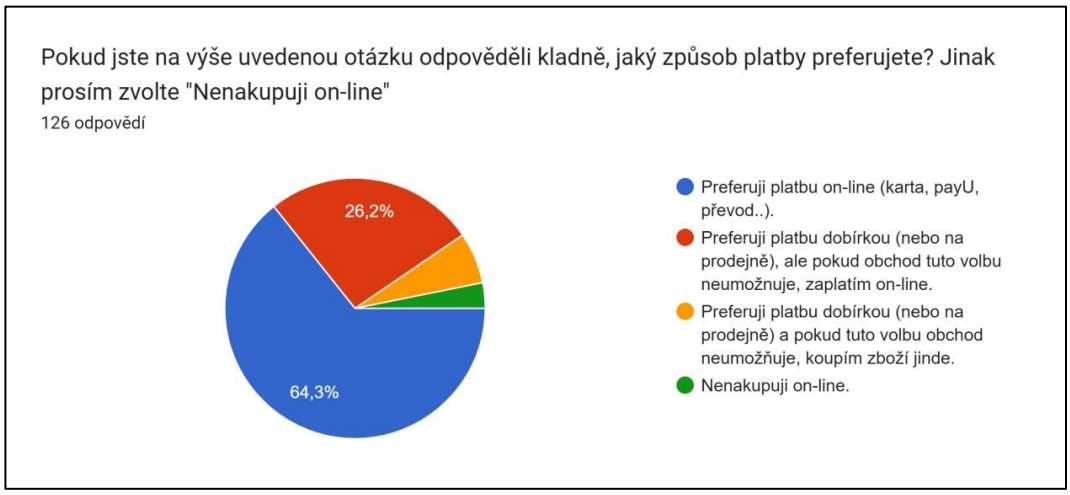
Na otázku týkající se četnosti využívání online nákupů odpovědělo 52,4 % respondentů, že nakupuje přes internet často, několikrát do měsíce. Dalších 11,9 % respondentů uvedlo, že téměř veškeré nákupy realizuje online. Zřídka nakupuje přes internet 32,5 % respondentů a 3,2 % respondentů uvedlo, že online nákupy vůbec nevyužívá.

Graf č. 15: Četnost využití nákupů on-line[72]



Způsob platby předem prostřednictvím online plateb preferuje 64,3 % respondentů. Platbu na dobírku nebo při osobním odběru na prodejně preferuje 26,2 % respondentů. Dalších 6,3 % respondentů uvedlo, že v případě nemožnosti platby na dobírku nebo při osobním odběru raději nakoupí u jiného prodejce. Zbylá část respondentů online nákupy nevyužívá.

Graf č. 16: Preference platby[73]



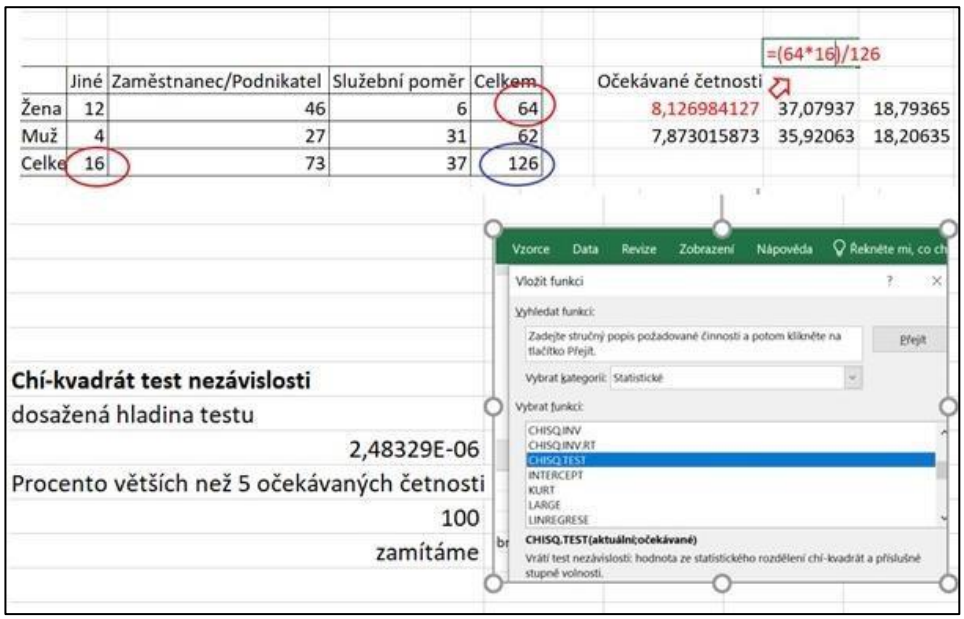
[72] Vlastní zpracování.
[73] Vlastní zpracování.

7.2.2 Sledování významnosti dat

Předchozí podkapitola měla za úkol popsat základní vlastnosti souboru získaných dat a jejich prezentaci. Tato podkapitola se věnuje testům statistické nezávislosti mezi daty. K testování byly použity statistické nástroje dostupné v aplikaci Microsoft Excel. V tomto programu byla z exportovaných dat vytvořena pro každou zajímavou dvojici proměnných (ty které bylo zajímavé mezi sebou porovnat), kontingenční tabulka četností jednotlivých kombinací hodnot. Následně byl pro každou z těchto tabulek aplikován postup, kdy pro přehlednost výsledků byla vytvořena kontingenční tabulka, která ukazuje, jak by hodnoty měly vypadat podle vzorců. Poté byl proveden test pomocí Chí-kvadrátu, konkrétně funkce **CHISQ.TEST** (aktuální, očekávané), který zjišťuje, zda mezi sledovanými hodnotami **existuje nějaká souvislost**, nebo zda je lze považovat **za nezávislé**. Často se při tomto testu používá hodnota 0,05, což je hranice, která nám ukazuje, zda jsou výsledky dostatečně spolehlivé.

Pokud vyjde hodnota nad touto hranicí, výsledky naznačují, že není možné potvrdit spojitost mezi daty. Aby byl test přesnější, je potřeba, aby většina očekávaných hodnot v tabulce byla vyšší než 5. Pokud tomu tak není, data se upraví spojením některých řádků nebo sloupců.[74]

Obrázek č. 3: Ukázka výpočtu v Microsoft Excel[75]



[74] [1] NEUBAUER, Jiří; SEDLAČÍK, Marek; KŘÍŽ, Oldřich. *Základy statistiky: aplikace v technických a ekonomických oborech.* Praha: Grada Publishing, 2012, s. 192–205. ISBN 978-80-247-4273-1.
[75] Vlastní zpracování

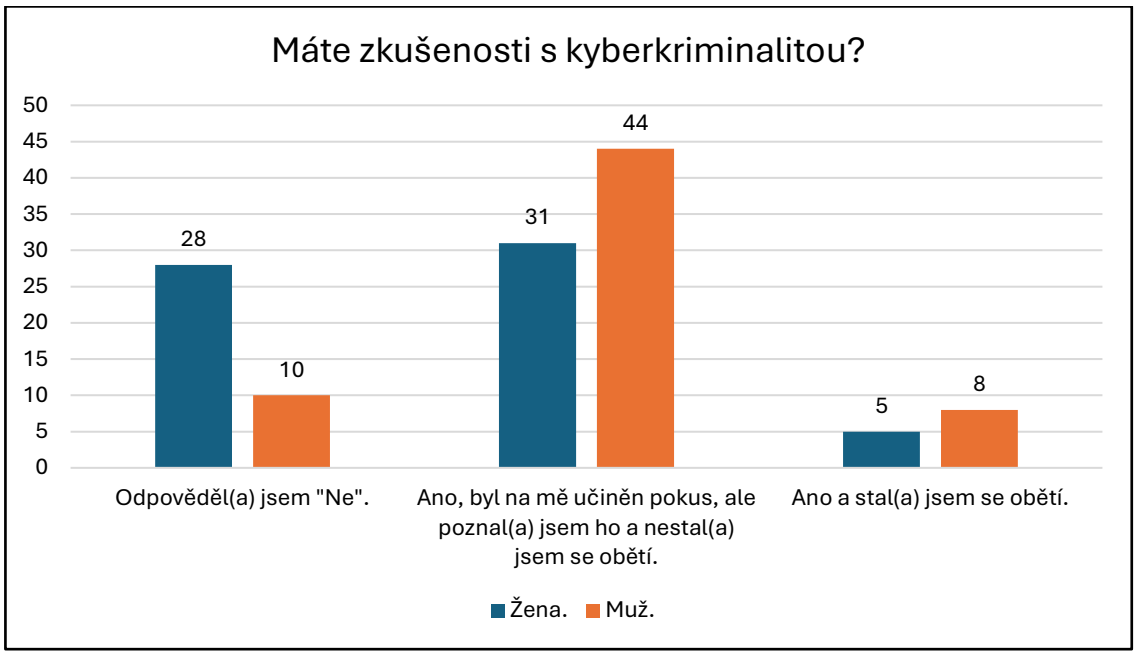
Takto bylo postupováno i u dalších vybraných kombinací. Pokud je u kombinací uvedeno zamítáme, znamená to, že na hladině významnosti 0,05 se tedy **připouští závislost mezi danými kombinacemi**. Z velkého množství kombinací byly vyhodnoceny pouze ty, ve kterých bylo splněno, že procento očekávaných četností je větší než 5, což bylo v 75 %.

Zamítnutá nezávislost:

Pokud byla zamítnuta nezávislost, tak to znamená, že na základě statistického testu (například Chí-kvadrát testu) existují dostatečné důkazy, které naznačují, že mezi zkoumanými proměnnými **existuje statisticky významná souvislost**. Jinými slovy, výsledek testu ukazuje, že pravděpodobnost, že jsou proměnné na sobě skutečně nezávislé (tj. že mezi nimi není žádný vztah), je velmi nízká.

Příklady graficky znázorněných odpovědí, u kterých byla zamítnuta nezávislost:

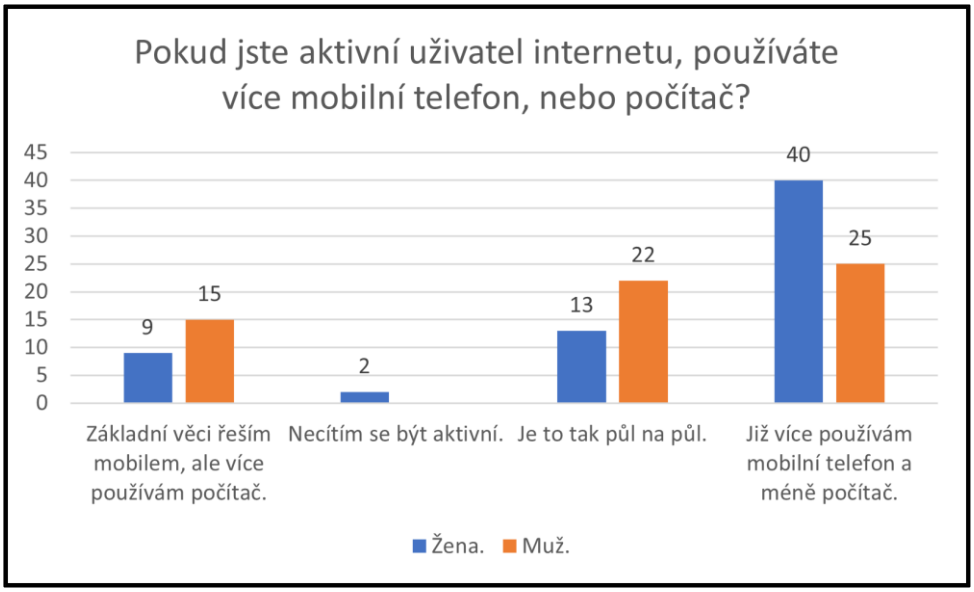
Graf č. 17: Vztah mezi pohlavím a zkušeností s kyberkriminalitou[76]



Dosažená hladina testu byla 0,024, což naznačuje, že mezi pohlavím a zkušeností s kyberkriminalitou může existovat statisticky významná závislost.

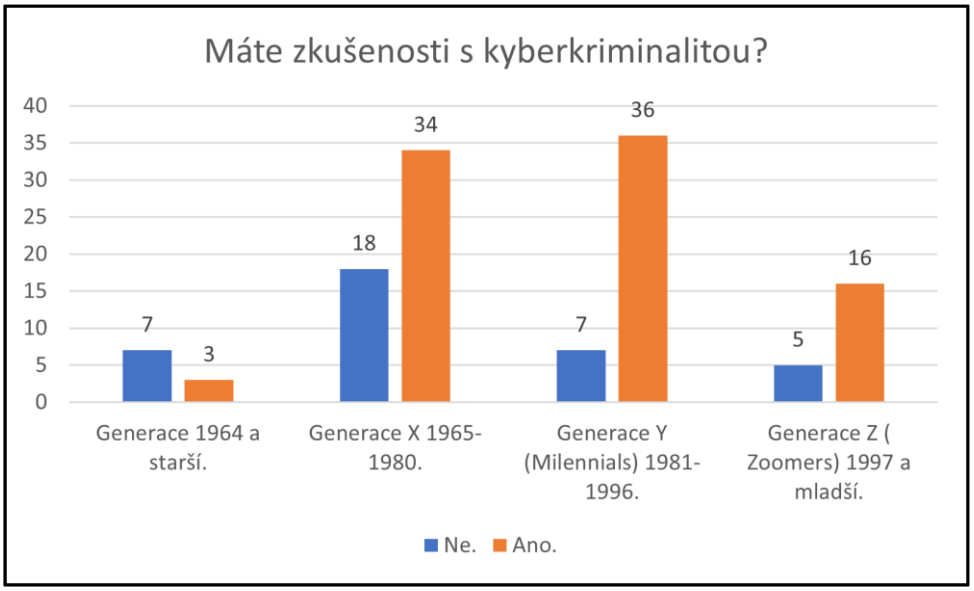
[76] Vlastní zpracování.

Graf č. 18: Vztah mezi zařízením a pohlavím[77]



Dosažená hladina testu 0,026. To znamená, že mezi pohlavím a používaným zařízením **<u>může existovat</u>** závislost.

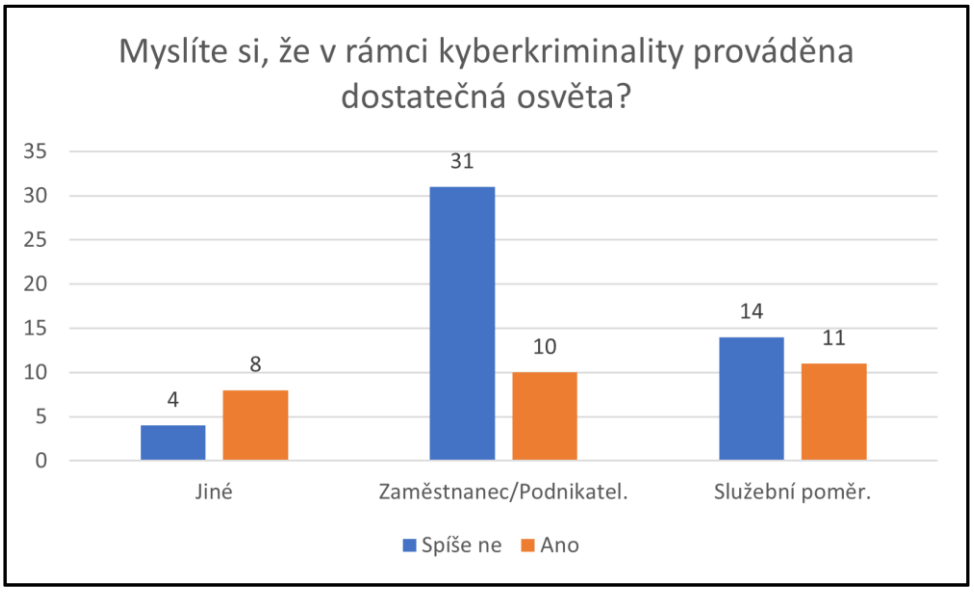
Graf č. 19: Vztah mezi datem narození a zkušeností s kyberkriminalitou[78]



Dosažená hladina testu 0,005. To znamená, že mezi datem narození a zkušeností s kyberkriminalitou **<u>může existovat</u>** závislost.

[77] Vlastní zpracování.
[78] Vlastní zpracování.

Graf č. 20: Vztah mezi povoláním a osvětou v rámci kyberkiminality[79]



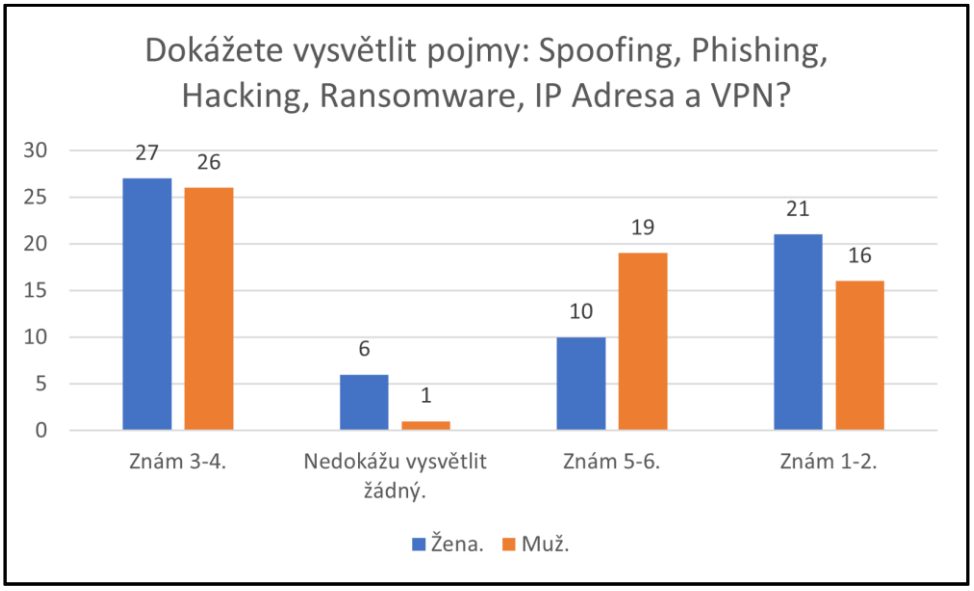
Dosažená hladina testu 0,024. To znamená, že mezi povoláním a osvětou v rámci kyberkriminality **<u>může existovat</u>** závislost.

[79] Vlastní zpracování.

Nezamítnutá nezávislost:

Pokud nebyla zamítnuta nezávislost, znamená to, že na základě výsledků statistického testu (například Chí-kvadrát testu) nebyly nalezeny dostatečné důkazy, které by naznačovaly závislost mezi zkoumanými proměnnými. Jinými slovy, test neprokázal, že by mezi proměnnými existovala statisticky významná souvislost, a proto se předpokládá, že jsou nezávislé. To však neznamená, že jsou určitě nezávislé, ale pouze to, že **dostupná data neposkytla důkazy pro zamítnutí nezávislosti**.

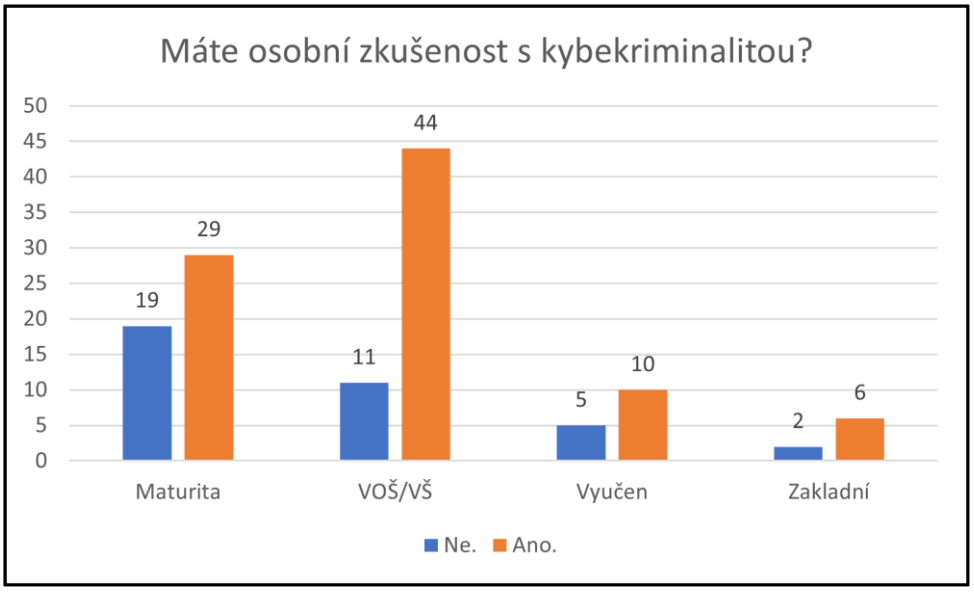
Graf č. 21: Vztah mezi pohlavím a znalostí pojmů[80]



Dosažená hladina testu 0,07. To znamená, že mezi pohlavím a znalosti pojmů týkajících se kyberkriminality, **nebyly nalezeny důkazy, že by mohla existovat závislost**. Jinými slovy, neexistuje statisticky významný důvod pro zamítnutí nezávislosti.

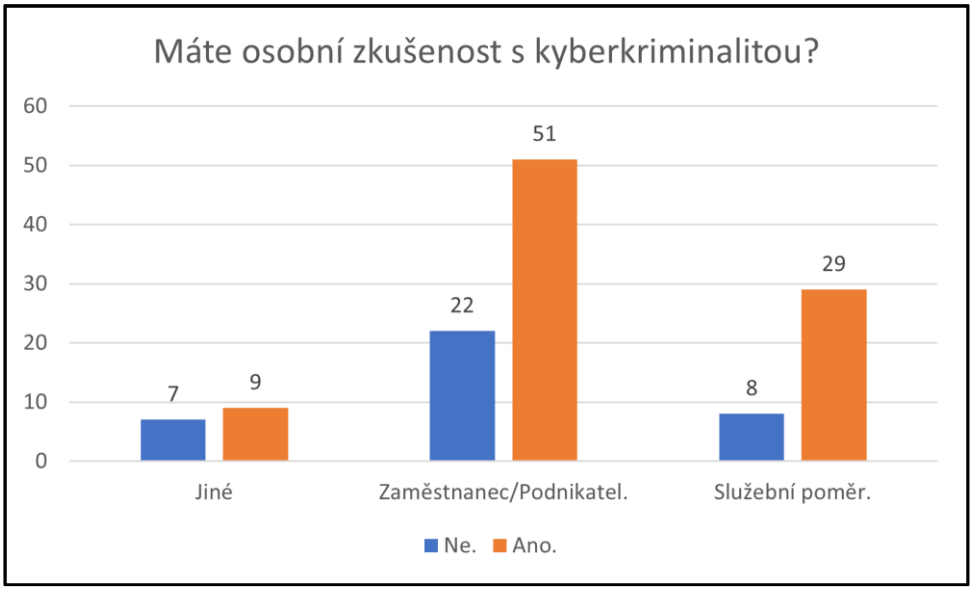
[80] Vlastní zpracování.

Graf č. 22: Vztah mezi vzděláním a zkušeností s kybekriminalitou[81]



Dosažená hladina testu 0,177. To znamená, že mezi vzděláním a zkušeností s kybekriminalitou **nebyly nalezeny důkazy, že by mohla existovat závislost**. Jinými slovy, neexistuje statisticky významný důvod pro zamítnutí nezávislosti.

Graf č. 23: Vztah mezi povoláním a zkušeností s kybekriminalitou[82]



Dosažená hladina testu 0,265. To znamená, že mezi povoláním a zkušeností s kybekriminalitou **nebyly nalezeny důkazy, že by mohla existovat závislost**. Jinými slovy, neexistuje statisticky významný důvod pro zamítnutí nezávislosti.

[81] Vlastní zpracování.
[82] Vlastní zpracování.

7.3 Vyhodnocení dotazníku

Cílem dotazníkového šetření bylo zjistit úroveň povědomí respondentů o kriminalitě páchané v kyberprostoru, jejich osobní zkušenosti s touto formou kriminality a způsoby, jakými se snaží předcházet možným kybernetickým hrozbám. Získaná data zároveň umožnila sledovat možné souvislosti mezi vybranými demografickými charakteristikami respondentů a jejich chováním či postoji v oblasti kybernetické bezpečnosti. Je však nutné zdůraznit, že veškeré závěry vycházejí výhradně z analyzovaného vzorku respondentů a nelze je bez dalšího považovat za obecně platné pro celou populaci.

Z demografických údajů vyplynulo, že vzorek respondentů byl z hlediska pohlaví poměrně vyrovnaný, což umožnilo sledovat případné rozdíly mezi muži a ženami bez výrazného zkreslení výsledků. Věkové rozložení respondentů podle generací ukázalo převahu generací Y a Z, což odpovídá způsobu šíření dotazníku prostřednictvím elektronických nástrojů a sociálních sítí. Tato skutečnost mohla ovlivnit některé výsledky, zejména v oblasti využívání digitálních technologií a online služeb, a je třeba ji zohlednit při jejich interpretaci.

Popisná statistika ukázala, že značná část respondentů používá stejné heslo pro více uživatelských účtů, což lze považovat za rizikové chování z hlediska kybernetické bezpečnosti. Na druhou stranu většina respondentů uvedla, že zná a využívá dvoufázové ověřování. Tento rozpor naznačuje, že samotná znalost bezpečnostních opatření nemusí automaticky vést k jejich důslednému uplatňování v praxi.

Významným přínosem dotazníkového šetření bylo sledování statistické významnosti vybraných vztahů mezi proměnnými pomocí Chí-kvadrát testu. Výsledky testování ukázaly, že v některých případech existuje statisticky významná závislost mezi demografickými charakteristikami respondentů a jejich zkušenostmi či chováním v kyberprostoru. Konkrétně byla potvrzena závislost mezi pohlavím a zkušeností s kyberkriminalitou, mezi pohlavím a používaným zařízením a mezi datem narození a zkušeností s kyberkriminalitou. Tyto výsledky naznačují, že určité skupiny respondentů mohou být vůči kybernetickým hrozbám vystaveny odlišným rizikům nebo se v kyberprostoru chovat rozdílným způsobem.

Naopak u některých sledovaných kombinací proměnných nebyla statisticky významná závislost prokázána. Jednalo se například o vztah mezi pohlavím a znalostí

pojmů souvisejících s kyberkriminalitou nebo mezi dosaženým vzděláním a zkušeností s kyberkriminalitou. Tyto výsledky ukazují, že samotná úroveň vzdělání nebo základní znalost odborných pojmů nemusí být rozhodujícím faktorem pro vznik osobní zkušenosti s kyberkriminalitou a že významnou roli mohou hrát i další okolnosti, například způsob využívání internetu nebo míra obezřetnosti uživatele.

V oblasti znalosti pojmů souvisejících s kyberkriminalitou se ukázalo, že většina respondentů má alespoň základní povědomí o nejčastějších typech kybernetických hrozeb. Přesto lze konstatovat, že hlubší znalost problematiky má pouze menší část respondentů. Při širším nebo jinak strukturovaném výzkumném vzorku by se úroveň znalostí i jejich vztah k dalším proměnným mohla lišit.

Významným zjištěním je rovněž skutečnost, že více než polovina respondentů se cítí být kyberkriminalitou ohrožena a zároveň velká část z nich uvedla osobní zkušenost s touto formou kriminality. Tyto výsledky potvrzují, že kriminalita páchaná v kyberprostoru představuje reálný problém. Zároveň však nelze vyloučit, že při zapojení většího počtu respondentů nebo při cíleném oslovení specifických skupin obyvatel by se četnosti jednotlivých odpovědí i výsledky testování významnosti mohly lišit.

Respondenti se ve většině případů domnívají, že osvěta v oblasti kyberkriminality není dostatečná, případně není dostatečně srozumitelná pro méně zkušené uživatele. Tento názor se objevoval napříč různými skupinami respondentů, přičemž statistické testování naznačilo možné souvislosti mezi profesním zařazením respondentů a jejich vnímáním dostatečnosti osvěty. Tyto výsledky poukazují na potřebu cílenější prevence, která by zohledňovala specifika jednotlivých skupin uživatelů.

Na základě vyhodnocení dotazníkového šetření lze konstatovat, že povědomí o kyberkriminalitě mezi respondenty existuje, avšak v některých oblastech je nejednotné a vykazuje prostor pro zlepšení. Výsledky dotazníku je možné považovat za orientační a vztahující se výhradně ke zkoumanému vzorku respondentů. Pro zobecnění závěrů a potvrzení zjištěných závislostí by bylo vhodné provést další výzkum na větším a demograficky rozmanitějším souboru respondentů.

Závěr

Cílem této bakalářské práce bylo komplexně zhodnotit vývoj a aktuální trendy počítačové kriminality v České republice se zaměřením na problematiku inzertních podvodů. Práce posuzovala vliv technologického pokroku na způsoby páchání této trestné činnosti z perspektivy příslušníka Policie České republiky. Vedlejším cílem bylo na základě dotazníkového šetření vyhodnotit úroveň povědomí uživatelů internetu o kybernetické bezpečnosti a navrhnout opatření, která mohou přispět k prevenci.

V teoretické části byly vymezeny základní pojmy a popsán historický vývoj kyberkriminality – od jednoduchých sabotáží až po moderní hrozby využívající umělou inteligenci. Pozornost byla věnována také pravidlům bezpečného chování, přičemž se potvrdilo, že lidský faktor zůstává jedním z nejvýznamnějších prvků ovlivňujících bezpečnost v kyberprostoru.

Praktická část práce prostřednictvím případových studií ilustrovala, že pachatelé často kombinují technické prostředky s psychologickým nátlakem. Využívání anonymity online prostředí výrazně ztěžuje odhalování těchto deliktů v policejní praxi. Z dotazníkového šetření dále vyplynulo, že i přes rostoucí informovanost uživatelů přetrvávají rizikové návyky, jako je například používání shodných hesel pro více uživatelských účtů.

Na základě provedené analýzy a poznatků z praxe jsou navržena následující preventivní opatření:

Zavádění bezpečných platebních mechanismů: Inzertní platformy by měly preferovat systémy, u kterých dochází k uvolnění platby prodejci až po potvrzení doručení nezávadného zboží kupujícím. Tímto způsobem lze eliminovat riziko podvodného zasílání bezcenných předmětů.

Cílená a srozumitelná osvěta: Je nezbytné transformovat preventivní rady do podoby, která bude srozumitelná i pro méně zkušené uživatele a seniory. Osvěta by měla být podávána srozumitelným jazykem bez nadbytečného technického žargonu.

Standardizace dvoufázového ověřování (2FA): U služeb spojených s finančními transakcemi nebo nakládáním s osobními údaji se doporučuje zavést

dvoufázové ověřování jako povinný bezpečnostní standard, nikoliv pouze jako volitelnou funkci.

Zvýšení informovanosti o včasném ohlášení: Důraz by měl být kladen na rychlost reakce poškozených. Včasné nahlášení podvodu Policii ČR zvyšuje šanci na efektivní zablokování finančních prostředků na účtech pachatelů a to se týká nejen inzertních podvodů, ale podvodů v kyberprostoru obecně.

Z výsledků práce vyplývá, že obětí kybernetické kriminality se může stát kdokoli bez ohledu na věk či vzdělání. Vzhledem k neustálému vývoji metod pachatelů je nezbytné klást důraz na neustálou prevenci a posilování bezpečnostních návyků. Bakalářská práce splnila stanovené cíle a poskytla ucelený pohled na problematiku inzertních podvodů v českém kyberprostoru.

Seznam použitých zdrojů

Literární zdroje

1. ALBRECHT, W. Steve; ALBRECHT, Chad O.; ALBRECHT, Conan C.; ZIMBELMAN, Mark F. Fraud Examination. Boston: Cengage Learning, 2016, 880 s. ISBN 978-1-305-07939-7.
2. CASEY, Eoghan. Digital Evidence and Computer Crime. Burlington: Academic Press, 2011, 840 s. ISBN 978-0-12-374268-1.
3. GŘIVNA, Tomáš; POLČÁK, Radim. Kyberkriminalita a právo. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4.
4. HOLT, Thomas J.; BOSWORTH, Adam M.; GRIMES, Joshua B. Cybercrime and Digital Forensics. London: Routledge, 2015, 394 s. ISBN 978-1-138-02130-3.
5. JAMES, Lance. Phishing bez záhad. Praha: Grada Publishing, 2007, 232 s. ISBN 978-80-247-1766-1.
6. JIROVSKÝ, Vladimír. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada Publishing, 2007, 200 s. ISBN 978-80-247-1561-2.
7. JIRÁSEK, Petr; NOVÁK, Lukáš; POŽÁR, Jan. Výkladový slovník kybernetické bezpečnosti. Praha: Centrum kybernetické bezpečnosti, 2025, 230 s. ISBN 978-80-530-5400-3.
8. KOLOUCH, Jan. Cybercrime. Praha: CZ.NIC, 2016, 216 s. ISBN 978-80-88168-18-8.
9. KOLOUCH, Jan; KARČINÁK, Roman. Bezpečnost v online prostředí. Karlovy Vary: Biblio Kurzy Vary, 2016, 120 s. ISBN 978-80-260-9543-9.
10. MATĚJKA, Michal. Počítačová kriminalita. Praha: Computer Press, 2002, 114 s. ISBN 80-7226-419-2.
11. NEUBAUER, Jiří; SEDLAČÍK, Marek; KŘÍŽ, Oldřich. Základy statistiky: aplikace v technických a ekonomických oborech. Praha: Grada Publishing, 2012, 280 s. ISBN 978-80-247-4273-1.
12. PAVINSKI, Adam. Kyberkriminalita. Praha: Wolters Kluwer, 2017, 184 s. ISBN 978-80-7552-758-5.
13. RAK, Roman a kol. Kybernetická kriminalita. Karlovy Vary: Vysoká škola Karlovy Vary, 2013, 221 s. ISBN 978-80-87182-72-3.

14. SMEJKAL, Vladimír. Kybernetická kriminalita. Plzeň: Aleš Čeněk, 2015, 431 s. ISBN 978-80-7380-558-4.
15. STRAUSS, William; HOWE, Neil. Generations: The History of America's Future, 1584 to 2069. New York: Harper Perennial, 1992, 538 s. ISBN 0-688-11912-3.
16. VLČEK, Martin. Počítače a kriminalita: trestněprávní a kriminologické aspekty. Praha: Academia, 1989, 156 s. ISBN 80-200-0139-5.

Elektronické zdroje

1. ESET. Kdo je hacker? [online]. Praha : ESET, 2024 [cit. 2026-03-11]. Dostupné z WWW: <https://www.eset.com/cz/hacker/>.
2. POLICIE ČESKÉ REPUBLIKY. Vishing a spoofing [online]. Praha : Policie ČR, 2024 [cit. 2026-03-11]. Dostupné z WWW: <https://policie.gov.cz/clanek/vishing-a-spoofing.aspx>.
3. NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. Minimální bezpečnostní standard v1.2 [online]. Brno: NÚKIB, 2023 [cit. 2026-03-09]. Dostupné z WWW: <https://nukib.gov.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf>.

Legislativní dokumenty

1. ČESKO. Zákon č. 141/1961 Sb. ze dne 29. listopadu 1961 o trestním řízení soudním (trestní řád). In: Sbírka zákonů Československé socialistické republiky. 1961, částka 66, s. 441-486. Dostupné z WWW: https://www.zakonyprolidi.cz/cs/1961-141/zneni-0. ISSN 1210-0005.
2. ČESKO. Zákon č. 273/2008 Sb. ze dne 17. července 2008 o Policii České republiky. In: Sbírka zákonů České republiky. 2008, částka 88, s. 4674-4712. Dostupné z WWW: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5345. ISSN 1210-0005.
3. ČESKO. Zákon č. 40/2009 Sb. ze dne 8. ledna 2009 trestní zákoník. In: Sbírka zákonů České republiky. 2009, částka 11, s. 318-479. Dostupné z WWW: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=5443. ISSN 1210-0005.

4. ČESKO. Sdělení Ministerstva zahraničních věcí č. 104/2013 Sb. m. s. ze dne 1. srpna 2013 o sjednání Úmluvy o kyberkriminalitě. In: Sbírka mezinárodních smluv, Česká republika. 2013, částka 45, s. 1051-1087. Dostupné z WWW: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=2559. ISSN 1210-0005.
5. ČESKO. Zákon č. 181/2014 Sb. ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Sbírka zákonů České republiky. 2014, částka 75, s. 2226-2249. Dostupné z WWW: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=6600. ISSN 1210-0005.
6. ČESKO. Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: Úřední věstník Evropské unie. 2016, L 119, s. 1-88. Dostupné z WWW: https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32016R0679. ISSN 1977-0677.
7. ČESKO. Zákon č. 251/2016 Sb. ze dne 12. července 2016 o některých přestupcích. In: Sbírka zákonů České republiky. 2016, částka 82, s. 3362-3372. Dostupné z WWW: https://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=30546. ISSN 1210-0005.
8. ČESKO. Zákon č. 264/2025 Sb. ze dne 18. července 2025, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Sbírka zákonů České republiky. 2025, částka 108, s. 3120-3125. Dostupné z WWW: https://www.e-sbirka.cz/sbirka-zakonu/vydani/2025/108. ISSN 1210-0005.

Seznam zkratek

AI – Umělá inteligence

AP – Access Point

CRO – Centrální registr obyvatel

GDPR – General Data Protection Regulation

IP – Internet Protocol

NIS – Network and Information Security

NIS2 – Směrnice Evropského parlamentu a Rady (EU) 2022/2555

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

OHK – Oddělení hospodářské kriminality

PČR – Policie České republiky

SIM – Subscriber Identity Module

SKPV – Služba kriminální policie a vyšetřování

TCP/IP – Transmission Control Protocol / Internet Protocol

VPN – Virtual Private Network

WWW – World Wide Web

Seznam obrázků a grafů

Seznam příloh

1. Jaké je Vaše pohlaví?

- Muž
- Žena

2. Do které kategorie dle data narození spadáte?

- Generace Z (Zoomers) 1997 a mladší.
- Generace Y (Milennials) 1981-1996.
- Generace X 1965-1980.
- Baby Boomers 1946-1964.
- Generace Silent 1945 a starší.

3. Jaké je Vaše vzdělání?

- Základní.
- Střední vyučen.
- Střední s maturitou.
- Vyšší odborné/Vysokoškolské.

4. Jaké je Vaše povolání?

- Služební poměr.
- Zaměstnanec/Podnikatel.
- Důchodce.
- Student.

5. Máte osobní zkušenost s kriminalitou páchanou v kyberprostoru? (jakoukoli, vč. pouhého pokusu Vás napálit/podvést/okrást...)

- Ano
- Ne

6. Pokud jste v předešlé otázce odpověděl(a) "Ano", uveďte jakou, jinak prosím zvolte "Ne".

- Ano, byl na mě učiněn pokus, ale poznal(a) jsem ho a nestal(a) jsem se obětí.
- Ano a stal(a) jsem se obětí.
- Odpověděl(a) jsem "Ne".

7. Víte, co znamenají tyto výrazy, které se používají v rámci kyberkriminality? (dokážete vlastními slovy popsat o co jde?) Spoofing, Phishing, Hacking, Ransomware, IP Adresa, VPN

- Nedokážu vysvětlit žádný.
- Znám 1-2.
- Znám 3-4.
- Znám 5-6.

8. Víte, co znamená pojem "dvoufázová ochrana"? (Např. při vstupu do internetového bankovnictví, emailu apod..)

- Ano a používám ji.
- Ano, ale nepoužívám ji.
- Ne nevím, co to znamená a k čemu slouží.

9. Jak moc se cítíte ohrožen(a) počítačovou kriminalitou ve Vašem osobním i pracovním životě?

- Necítím se ohrožen(a).
- Cítím se trochu ohrožen(a).
- Cítím se velmi ohrožen (a).
- Neřeším to.

10. Používáte stejné heslo u více účtů? Např. heslo do emailu a zároveň na sociální sítě? (Možnost "Ne" zvolte pouze pokud používáte pro každý účet jedinečné unikátní heslo).

- Ano
- Ne

11. Snažíte se aktivně předcházet možným útokům?

- Ne, spoléhám se na automatickou ochranu prohlížečů, operačního systému a emailových klientů, nijak aktivně možné riziko neřeším.
- Ne, mě se to nemůže stát, co by si na mě kdo vzal.
- Ano, snažím se navštěvovat pouze "známé" webové stránky, používám silná hesla a nereaguji na podezřelé emaily apod..
- Ano, zajímám se aktivně o novinky týkající se bezpečnosti a snažím se řídit veškerými mě známými pravidly týkající se bezpečného chování na internetu.

12. Jak často využíváte on-line nákupy? (vč. rezervace zboží na prodejně)

- Vůbec.
- Zřídka (párkrát do roka).
- Často (několikrát do měsíce).
- Nakupuji téměř vše nebo vše pouze on-line.

13. Pokud jste na výše uvedenou otázku odpověděli kladně, jaký způsob platby preferujete? Jinak prosím zvolte "Nenakupuji on-line"

- Preferuji platbu on-line (karta, payU, převod..).
- Preferuji platbu dobírkou (nebo na prodejně), ale pokud obchod tuto volbu neumožnuje, zaplatím on-line.
- Preferuji platbu dobírkou (nebo na prodejně) a pokud tuto volbu obchod neumožňuje, koupím zboží jinde.
- Nenakupuji on-line.

14. Pokud jste aktivní uživatel internetu, používáte častěji mobilní telefon nebo počítač? (vyjma chatovacích a hovorových aplikací)

- Základní věci řeším mobilem, ale více používám počítač.
- Je to tak půl na půl.
- Již více používám mobilní telefon a méně počítač.
- Necítím se být aktivní.

15. Myslíte si, že je prováděna dostatečná osvěta, týkající se kriminality páchané v kyberprostoru?

- Ano.
- Spíše ne.
- Ne.

16. Pokud jste na výše uvedenou otázku odpověděl(a) kladně, myslíte si, že je tato osvěta dostatečně "jednoduše" pochopitelná i pro méně zkušené uživatele internetu? (např. seniory, apod..) Jinak prosím zvolte "Ne"

- Ano.
- Spíše ne.
- Odpověděl(a) jsem "Ne