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

BAKALÁŘSKÁ PRÁCE

KYBERNETICKÁ BEZPEČNOST A JEJÍ DOPADY NA OBYVATELSTVO

Autor práce: David Dráždil

Studijní program: Bezpečnostně právní činnost

Forma studia: Kombinovaná

Vedoucí práce: RNDr. Růžena Ferebauerová

Katedra: Katedra právních oborů a bezpečnostních studií

2025

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

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení studenta: David Dráždil

Studijní program: Bezpečnostně právní činnost
Forma studia: Kombinovaná
Místo studia: České Budějovice

Název bakalářské práce: Kybernetická bezpečnost a její dopady na obyvatelstvo
Název bakalářské práce v anglickém jazyce: Cyber Security and Its Impacts on the Population

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

Datum zadání bakalářské práce (měsíc, rok): prosinec 2024

Cílem bakalářské práce je posoudit problematiku kybernetické bezpečnosti z hlediska jejích dopadů na obyvatelstvo, zhodnotit hlavní hrozby a rizika v této oblasti, posoudit účinnost stávajících preventivních a ochranných opatření a navrhnout doporučení pro zlepšení informovanosti a ochrany občanů před kybernetickými útoky.

Student: David Dráždil	28.12.2024 *datum*	*podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	8.1.2025 *datum*	*podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	11.1.2025 *datum*	*podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	14.1.2025 *datum*	*podpis*
Rektor: doc. Ing. Jiří Dušek, Ph.D.	20.1.2025 *datum*	*podpis*

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

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

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

.....

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

ABSTRAKT

DRÁŽDIL, D. Kybernetická bezpečnost a její dopady na obyvatelstvo: bakalářská práce. České Budějovice: Vysoká škola evropských a regionálních studií, 2025. 58 s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová

Klíčová slova: Kybernetická bezpečnost, kybernetické útoky, kyberkriminalita, oběti podvodů, prevence, sociální dopady, Policie České republiky.

Bakalářská práce se zabývá analýzou problematiky kybernetických útoků a jejich dopadů na obyvatele České republiky. V teoretické části poskytuje přehled nejčastějších typů kybernetických útoků, popisuje jejich mechanismy a způsoby, jakými pachatelé manipulují své oběti. Praktická část prostřednictvím dotazníkového šetření na obvodních odděleních Policie České republiky v okrese České Budějovice zkoumá vliv kybernetických podvodů na finanční, psychologický a sociální život obětí. Práce rovněž navrhuje opatření, která mohou přispět k lepší ochraně proti těmto hrozbám. Cílem je poskytnout ucelený obraz současného stavu kybernetické bezpečnosti a zvýšit povědomí o rizicích spojených s kyberkriminalitou.

ABSTRACT

DRÁŽDIL, D. Cyber Security and Its Impacts on the Population: University of European and Regional Studies, 2025. 58 s. Bachelor thesis supervisor: RNDr. Růžena Ferebauerová

Key words: cybersecurity, cyberattacks, cybercrime, fraud victims, prevention, social impacts, Czech Police.

The bachelor's thesis focuses on the analysis of cybersecurity issues and their impacts on the population of the Czech Republic. The theoretical part provides an overview of the most common types of cyberattacks, describes their mechanisms, and explains how perpetrators manipulate their victims. The practical part, through a survey conducted at local police departments in the České Budějovice district, examines the effects of cyber fraud on the financial, psychological, and social lives of victims. The thesis also proposes measures that could contribute to better protection against these threats. The aim is to provide a comprehensive view of the current state of cybersecurity and raise awareness of the risks associated with cybercrime.

Obsah

Úvod

V současné době zažíváme prudký rozvoj digitálních technologií, který zásadním způsobem ovlivňuje každodenní život jednotlivců, firem i veřejných institucí. Internet a digitální služby jsou pevně zakořeněny v každé oblasti lidské činnosti – od práce a vzdělávání až po zábavu či mezilidskou komunikaci. Spolu s tímto vývojem však dochází i k nárůstu kybernetických hrozeb, jejichž rozsah, komplexita a důsledky překračují tradiční formy kriminality. Kyberprostor se stal nejen místem pro sdílení informací, ale rovněž prostředím pro páchání závažných trestných činů, které mohou mít destruktivní dopad na soukromí, finance i psychiku jednotlivců.

Kybernetická kriminalita se již dávno neomezuje pouze na úzce vymezený okruh technicky náročných útoků. Stále častěji se stává prostředkem k manipulaci důvěřivých uživatelů, kteří mnohdy netuší, že se stali terčem cíleného podvodu. Sociální inženýrství, phishing, malware či podvodné e-shopy jsou jen některé z forem, které se v posledních letech výrazně rozmohly a zasáhly širokou veřejnost napříč věkovými i sociálními skupinami. Závažnost tohoto fenoménu je umocněna tím, že oběti kybernetických podvodů mnohdy čelí nejen finančním ztrátám, ale i psychologickým následkům, jako je stres, pocity studu či ztráta důvěry v digitální svět.

Důležitost problematiky kybernetické bezpečnosti neustále narůstá, což reflektují nejen odborné publikace a vládní strategie, ale i každodenní praxe bezpečnostních složek a preventivních programů. Kybernetické útoky nejsou jen technickým problémem – mají reálné dopady na životy lidí, jejich vztahy, kariéry a někdy i zdraví. Tato skutečnost ukazuje, že ochrana v kyberprostoru by měla být vnímána jako základní kompetence moderního člověka.

Téma této bakalářské práce se proto soustředí na oblast kybernetické bezpečnosti v kontextu jejích konkrétních dopadů na obyvatele České republiky. Záměrem je nejen porozumět fungování kyberútoků a způsobům, jakými útočníci jednají, ale především poukázat na dopady těchto činů z pohledu běžných občanů. V tomto kontextu se práce snaží přispět k širší diskusi o tom, jak by měla vypadat účinná prevence, vzdělávání i legislativa v době, kdy hranice mezi reálným a digitálním světem již téměř neexistují.

Cíl a metodika bakalářské práce

Hlavním cílem bakalářské práce je analyzovat současnou situaci v oblasti kybernetické bezpečnosti a identifikovat nejčastější typy kybernetických útoků, které ovlivňují obyvatele České republiky. Práce se zaměřuje na popis mechanismů, které pachatelé používají k manipulaci svých obětí, a na zhodnocení finančních, psychologických a sociálních dopadů kyberkriminality na jednotlivce. Vedlejším cílem je navrhnout preventivní opatření, která mohou snížit riziko kybernetických útoků a zvýšit informovanost veřejnosti o této problematice.

Metodika bakalářské práce kombinuje teoretický a empirický přístup k dosažení stanovených cílů. Teoretická část se zaměřuje na rešerši odborné literatury a legislativních dokumentů týkajících se kybernetické bezpečnosti, přičemž popisuje nejčastější typy kybernetických útoků, jejich právní kvalifikaci a mechanismy, které pachatelé využívají při manipulaci obětí. Empirická část zahrnuje dotazníkové šetření realizované mezi oběťmi kybernetických podvodů, které se dostaví na obvodní oddělení Policie České republiky v okrese České Budějovice za účelem oznámení podvodu. Získaná data budou analyzována kvantitativní metodou s cílem identifikovat nejčastější typy kybernetických podvodů, jejich charakteristiky a konkrétní dopady na finanční, psychologický a sociální život obětí. Výsledky tohoto šetření budou interpretovány v kontextu stanovených hypotéz a cílů práce, aby poskytly ucelený pohled na problematiku a mohly přispět k návrhu účinných preventivních opatření.

Hypotézy bakalářské práce:

H1: Nejčastějším typem kybernetických podvodů v České republice jsou phishingové útoky zaměřené na získání finančních prostředků.

H2: Kybernetické podvody způsobují obětem nejen finanční ztráty, ale také závažné psychologické dopady, jako je stres a úzkost.

H3: Informovanost veřejnosti o rizicích kybernetických útoků a preventivních opatřeních je nedostatečná, což zvyšuje zranitelnost jednotlivců vůči těmto hrozbám.

1 Vymezení základní pojmů

Pro lepší porozumění problematice kybernetických útoků je nezbytné nejprve vysvětlit několik základních pojmů, které s touto tématikou úzce souvisejí. Mezi klíčové termíny patří počítačový systém, kybernetický prostor, internet a kybernetická kriminalita.

1.1 Internet

Počátky internetu sahají do 60. let 20. století, kdy Spojené státy usilovaly o vytvoření nové komunikační sítě, která by umožnila rychlou a spolehlivou výměnu dat i v extrémních podmínkách. Jedním z hlavních impulzů k jejímu vzniku byla obava z možného jaderného konfliktu, což vedlo k návrhu sítě schopné propojit země, města či velitelská stanoviště a zajistit efektivní sdílení taktických informací. Internet se však postupem času stal mnohem více než jen prostředkem vojenské komunikace. [1]

Dnes internet funguje jako univerzální platforma, kde může kdokoli sdílet jakýkoli obsah. Na internetu neexistuje žádné centrální řízení, což uživatelům umožňuje individuální přizpůsobení – od volby poskytovatele služeb až po obsah zobrazovaný na jejich zařízeních. Kromě své role v komunikaci a zprostředkování informací plní internet také významnou úlohu v oblasti obchodu, výzkumu, zábavy či her. Lze jej tedy chápat jako multifunkční nástroj, který zároveň slouží jako prostor pro svobodné publikování obsahu.

1.2 Kyberprostor

Kyberprostor představuje jeden z klíčových pojmů v oblasti kybernetické bezpečnosti, avšak jeho definice se v literatuře liší. Neexistuje jednotná a univerzální definice, která by zahrnovala všechny aspekty tohoto pojmu. Kyberprostor je často spojován s internetem, který hraje významnou roli v jeho fungování, a proto je v této práci uveden jako další základní pojem. Legální definici kyberprostoru lze najít v § 2 písm. a) zákona č. 181/2014 Sb., kde je definován jako „*digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací*“[2].

[1] SKLENÁK, V. *Data, informace, znalosti a Internet*. Praha, 2001, s. 10.
[2] 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

Podle Koloucha „*Kyberprostor představuje ono pomyslné pískoviště, na kterém se pohybujeme, ale zároveň se jedná o klíčový prvek v definici kybernetické kriminality. Aby bylo možné definovat kyberprostor, je nezbytně nutné vymezit pojem Internet, který právě s kyberprostorem bezprostředně souvisí.“*[3]

Jirovský zdůrazňuje, že kyberprostor “*se stal pátou dimenzí života společnosti, která zahrnuje všechny aspekty běžných společenských aktivit*”. Kyberprostor odráží politické, obchodní, kulturní i emocionální atributy reálného světa a zahrnuje širokou škálu aktérů – od profesionálů a sportovců až po zločince. [4]

1.3 Počítačový systém

Zákon č. 40/2009 Sb., trestní zákoník (dále jen „trestní zákoník“ nebo „TZ“), používá pojem „počítačový systém“ například v ustanoveních § 182, 230, 231 či 232. Přesto však tento pojem není v zákoně komplexně definován, což může v praxi vést k nejasnostem při jeho právní interpretaci. Podle komentáře k trestnímu zákoníku je „počítačovým systémem“ jakékoli zařízení nebo skupina vzájemně propojených či souvisejících zařízení, z nichž alespoň jedno je schopné na základě programu provádět automatické zpracování dat. Počítačový systém tedy zahrnuje jak technické vybavení (hardware), tak programové vybavení (software) a slouží k automatickému zpracování digitálních dat. [5]

Jako synonymum k pojmu počítačový systém je často používán pojem „počítač“, avšak tyto pojmy nejsou zcela totožné. Počítačový systém je širší pojem, který zahrnuje nejen samotné počítače, ale také síťově připojená zařízení, jež formálně nesplňují atributy počítače. Tento rozdíl spočívá zejména v tom, že počítačový systém zahrnuje celé prostředí propojených zařízení určených k automatickému zpracování dat. [6]

Počítačovým systémem může být buď samostatné zařízení, jako například notebook, smartphone nebo bankomat, nebo skupina vzájemně propojených zařízení tvořících například počítačovou síť. Mezi počítačové systémy lze rovněž zařadit televize či jiné domácí spotřebiče umožňující spouštění aplikací, včetně připojení na internet,

[3] KOLOUCH, J. *CyberCrime*. Praha2016, str. 42
[4] IROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. str. 16
[5] GŘIVNA, T. § 230 *Neoprávněný přístup k počítačovému systému a nosiči informa cí*. In: ŠÁMAL, Pavel a kol. Trestní zákoník II: komentář. § 140-421. 2. vyd. V Praze: C.H. Beck, 2012, s. 2306.
[6] JIRÁSEK, P., NOVÁK, L., POŽÁR J. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualiz. vyd. Praha: AFCEA, © 2015, s. 59. Dostupný z WWW: https://afcea.cz/cesky-slovnik-pojmu-kyberneticke-bezpecnosti/

nebo systémy v automobilech poskytující obdobné funkce. Specifickým typem počítačového systému je pak samotný internet, který zahrnuje rozsáhlou síť propojených zařízení a systémů.

1.4 Kybernetická kriminalita

Kybernetická kriminalita je stále častějším jevem v důsledku rostoucího využívání moderních technologií, zejména informačních a komunikačních. Tato trestná činnost bývá označována různými termíny, jako například počítačová, internetová nebo kybernetická kriminalita. Nejednotnost v pojmosloví často vede k nejasnostem v obsahovém vymezení těchto termínů. Odborné publikace a právní normy je často zaměňují a užívají jako synonyma, což komplikuje legislativní úpravu tohoto dynamicky se vyvíjejícího fenoménu. [7]

Mezinárodně se nejčastěji používá termín „*kybernetická kriminalita*“ nebo „*kyberkriminalita*“, který odkazuje na trestnou činnost, kde hrají klíčovou roli informační technologie. Jedním z významných právních aktů v této oblasti je Úmluva Rady Evropy č. 185 o kybernetické kriminalitě z roku 2001. Přestože oficiální překlad pracuje s termínem „*počítačová kriminalita*“, původní znění používá výraz „*cybercrime*“, což je dnes považováno za přesnější označení. Úmluva neposkytuje jednoznačnou definici kyberkriminality, ale rámcově vymezuje trestné činy, které do této kategorie spadají. Podle Policie ČR je kybernetická kriminalita definována jako trestná činnost páchaná v prostředí informačních a komunikačních technologií, které jsou buď cílem útoku, nebo prostředkem k jeho provedení. [8]

Podle ustanovení zákona č. 40/2009 Sb., trestního zákoníku, ve znění pozdějších právních předpisů, lze v oblasti kybernetické kriminality identifikovat tři hlavní skutkové podstaty majetkových trestných činů. Tyto skutkové podstaty zahrnují:

- neoprávněný přístup k počítačovému systému a nosiči informací (§ 230),
- opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231),
- poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232).

[7] JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007, s. 19.
[8] MATĚJKA, M. *Počítačová kriminalita*. Praha: Computer Press, 2002, s. 18-22

Kromě toho existují trestné činy, při nichž pachatel záměrně využívá kyberprostor jako prostředek k jejich páchání, což může mít závažné důsledky pro společnost. Mezi tyto trestné činy patří:

- šíření pornografie (§ 191),
- výroba a jiné nakládání s dětskou pornografií (§ 192),
- navazování nedovolených kontaktů s dítětem (§ 193b),
- porušení autorského práva, práv souvisejících s právem autorským a práv k databázi (§ 270),
- hanobení národa, rasy, etnické nebo jiné skupiny osob (§ 355),
- podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod (§ 356),
- šíření poplašné zprávy (§ 357),
- pomluva (§ 184),
- vydírání (§ 175). [9]

Tato trestná činnost často představuje specifické hrozby spojené s kyberprostorem, kde rozsah a dopad jednotlivých činů mohou být mnohonásobně větší než v tradičním prostředí.

1.5 Kybernetický útok

Kybernetický útok lze obecně charakterizovat jako "*jakékoliv protiprávní jednání v kyberprostoru, jehož cílem je narušení zájmů jiné osoby*"[10]. I když ne každý kybernetický útok musí nutně splňovat podmínky trestného činu, každý kybernetický trestný čin lze vždy považovat za kybernetický útok.

Navzdory existenci mnoha definic tohoto pojmu dosud neexistuje jednotné právní vymezení, které by bylo obecně přijímáno. Mnohé definice navíc omezují rozsah pojmu a nezohledňují všechny možné hrozby v kyberprostoru, jako například útoky vedoucí k odepření služeb počítačového systému bez narušení jeho dat nebo shromažďování citlivých informací bez přímého poškození samotného systému. [11]

[9] NGSS. *Zločiny v době moderních technologií: Jak řeší české právo kybernetickou kriminalitu a jak se proti ní bránit?* [online]. [cit.2025-01-11]. Dostupné z WWW: https://www.ngss.cz/clanek/zlociny-v-dobe-modernich-technologii-jak-resi-ceske-pravo-kybernetickou-kriminalitu-a-jak-se-proti-ni-branit-2023-05-16

[10] KOLOUCH, J., BAŠTA, P. *Cybersecurity*, Praha, 2019, s. 78-79.

[11] VÁCLAVÍK, L. *Většina internetu je skrytá. Co jsou to deep a dark web?* [online]. [cit.2025-01-11]. Dostupné z WWW: https://www.cnews.cz/clanky/co-je-to-deep-invisible-hluboky-dark-temny-web/

2 Typologie útoků a jejich trestněprávní kvalifikace

S neustálým rozvojem informačních a komunikačních technologií (dále jen IT) se otevírají nové možnosti i pro pachatele protiprávního jednání, kteří využívají stále sofistikovanější metody. Tato kapitola se zaměří na různé podvodné praktiky v IT prostředí, od nejčastěji používaných až po méně známé techniky. Jejím cílem je podrobně analyzovat jednotlivé druhy těchto podvodů, objasnit jejich rozdíly a ukázat možné vzájemné propojení. Dále se kapitola bude věnovat jejich dopadům na uživatele IT systémů a strategiím, jak se proti nim účinně bránit a přizpůsobit se novým variantám těchto hrozeb.

Pro lepší pochopení této problematiky budou uvedeny konkrétní příklady a případové studie, které ilustrují, jak podvody v IT prostředí probíhají v praxi. Znalost širokého spektra těchto podvodů i konkrétních ukázek přispívá k lepší ochraně uživatelů, pomáhá jim včas rozpoznat nebezpečí a zvolit vhodná preventivní opatření.

Kybernetická kriminalita je oproti tradičním formám trestné činnosti, jako je fyzická krádež nebo loupež, pro pachatele často výhodnější. Důvodem je nižší riziko osobního ohrožení, potenciálně vyšší finanční zisky, mírnější trestní postihy a obtížnější identifikace pachatele, což vede ke snížené pravděpodobnosti jeho dopadení a odsouzení.[12]

2.1 Phishing

Phishing představuje formu podvodu, při níž útočník klame oběť s cílem vylákat z ní citlivé informace, jako jsou přihlašovací údaje k bankovním účtům, přístup k sociálním sítím či údaje o platebních prostředcích. K dosažení tohoto cíle se využívají různé manipulativní techniky, včetně šíření nepravdivých či zavádějících informací.

Jedním z nejčastějších phishingových triků je použití falešných webových stránek, které svým vzhledem co nejvěrněji napodobují originální stránky, aby u uživatele nevyvolaly podezření. Tyto podvodné stránky bývají šířeny prostřednictvím e-mailových zpráv, obsahujících odkazy nebo škodlivé přílohy. Jakmile uživatel na takový odkaz klikne a zadá své údaje, jsou automaticky předány útočníkovi. K úspěchu phishingového útoku je zásadní využití metod sociálního inženýrství, které pomáhá útočníkovi lépe cílit na konkrétní skupinu obětí a zvýšit pravděpodobnost úspěchu.

[12] KOŽÍŠEK, M. *Počítačová kriminalita*. Praha: Computer Press, 2002. 60 s.

Podle publikace *CyberCrime* lze phishingový útok rozdělit do několika fází:

1. **Příprava útoku** – Útočník vybírá svou cílovou skupinu a rozhoduje se, jakou strategii použije. Zvažuje také úroveň zabezpečení cíle a analyzuje možná rizika odhalení.
2. **Technická realizace** – Dochází k technickému zajištění útoku, například sběru e-mailových adres obětí, vytvoření úložiště pro získaná data a přípravě podvodného sdělení, které bude rozesláno uživatelům.
3. **Provádění útoku** – Podvodné e-maily jsou rozesílány cílovým osobám. Úspěšnost této fáze závisí na kvalitě falešné zprávy a na tom, jak snadno se uživatel nechá oklamat.
4. **Shromažďování údajů** – Útočník získává data, která uživatelé neúmyslně zadali na podvodných stránkách.
5. **Zneužití získaných informací** – Pomocí odcizených údajů se útočník dostává k finančním prostředkům obětí, které následně převádí na další účty, často v zahraničí, aby minimalizoval riziko odhalení. [13]

Phishing má několik variant, například **pharming**, **spear phishing**, **vishing** (hlasový phishing) nebo **smishing** (phishing přes SMS).

V období pandemie COVID-19, kdy mnoho organizací přecházelo na práci na dálku, se kyberzločinci rychle přizpůsobili nové situaci. Zvýšený počet uživatelů pracujících z domova a častější využívání online služeb vytvořily ideální podmínky pro phishingové útoky. Mezi únorem a březnem 2020 došlo k dramatickému nárůstu phishingových aktivit – mezi prvním a druhým čtvrtletím téhož roku vzrostl počet útoků až o 389 %.[14]

Trestněprávní kvalifikace phishingových útoků v České republice lze určit na základě zákona č. 40/2009 Sb., trestní zákoník. Konkrétní skutkové podstaty trestných činů, které mohou být naplněny při phishingu a souvisejících kybernetických útocích, zahrnují:

- Podvod (§ 209 TZ)
- Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 TZ)

[13] KOLOUCH, J. *CyberCrime*. Praha2016, str. 247-248.
[14] Phishing Stats You Should Know In 2022. Expert Insights [online]. [cit.2025-02-05]. Dostupné z WWW: https://expertinsights.com/insights/50-phishing-stats-you-should-know/

- Legalizace výnosů z trestné činnosti (§ 216 TZ – praní špinavých peněz)[15]

2.2 Malware

Malware, neboli škodlivý software, zahrnuje jakýkoli program určený k narušení fungování počítačového systému, krádeži dat nebo neoprávněnému přístupu do systému. Kromě počítačů se v dnešní době stále častěji objevuje i mobilní malware, který představuje významnou bezpečnostní hrozbu. Názvy těchto škodlivých programů obvykle souvisejí s jejich funkcí, přičemž jeden program může být navržen tak, aby vykonával více škodlivých aktivit současně, v závislosti na způsobu jeho naprogramování. Malware lze rozdělit do různých kategorií na základě jeho specifických vlastností a způsobu šíření.

V současnosti se však častěji používá souhrnný pojem malware, s výjimkou některých specifických typů, jako je ransomware, který představuje aktuální hrozbu. Mezi běžné kategorie škodlivého softwaru patří například adware, spyware, počítačové viry, červi, trojské koně, backdoory, rootkity nebo keyloggery. Kromě těchto tradičních forem se v současnosti objevují i nové typy malwaru, které se neustále vyvíjejí a přizpůsobují moderním bezpečnostním opatřením. [16]

Trestněprávní kvalifikace malwarových útoků v České republice lze určit na základě zákona č. 40/2009 Sb., trestní zákoník. Konkrétní skutkové podstaty trestných činů, které mohou být naplněny při malwaru a souvisejících kybernetických útocích, zahrnují:

- Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 TZ)
- Poškození záznamu v počítačovém systému a zásah do vybavení (§ 231 TZ)
- Legalizace výnosů z trestné činnosti (§ 216 TZ – praní špinavých peněz) [17]

2.2.1 Ransomware

Pojem **ransomware** pochází z anglického slova „ransom“, což znamená výkupné, a označuje specifický druh škodlivého softwaru určeného k vydírání obětí. Tento typ

[15] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In Sbírka zákonů, Česká republika. 2009, částka 11
[16] KOŽÍŠEK, M., PÍSECKÝ, V. *Bezpečně na internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. 125 s
[17] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In Sbírka zákonů, Česká republika. 2009, částka 11

malwaru po spuštění buď kompletně zašifruje celý počítačový systém, nebo cílí pouze na určitou část dat, k nimž následně zablokuje přístup. Útočníci poté požadují zaplacení výkupného, které bývá nejčastěji hrazeno prostřednictvím bankovního převodu nebo kryptoměn, což jim umožňuje zůstat anonymní. [18] Jednou z nejznámějších variant ransomware je tzv. **policejní ransomware**, který po infikování systému zobrazí falešné varování, vydávající se za oficiální oznámení policejních složek. Uživatel je v něm obviněn z údajného spáchání trestné činnosti na internetu a k „zastavení" domnělého trestního řízení je vyžadována platba.

V posledních letech se ransomware stal významnou kybernetickou hrozbou. Obzvlášť masivní útoky byly zaznamenány v roce 2017, kdy škodlivý software napadl vládní instituce, nemocniční systémy a další organizace po celém světě. Tento incident ukázal, jak ničivý dopad může mít ransomware na klíčové infrastruktury a jak důležité je zavádět účinná bezpečnostní opatření proti tomuto typu hrozeb.

Šíření a použití ransomwaru může naplnit několik skutkových podstat trestných činů podle **zákona č. 40/2009 Sb., trestního zákoníku**:

- Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 TZ)
- Poškození a zneužití záznamu v počítačovém systému (§ 231 TZ)
- Vydírání (§ 175 TZ)
- Podvod (§ 209 TZ)
- Legalizace výnosů z trestné činnosti (§ 216 TZ – praní špinavých peněz) [19]

2.2.1 Keylogger

Keylogger je sofistikovaný typ softwaru určený k tajné registraci všech stisků kláves na cílovém zařízení. Jeho primární funkcí je shromažďování citlivých údajů, mezi které patří přihlašovací jména, hesla, bankovní informace, přístupové údaje k sociálním sítím a další důležité data. Tento škodlivý program pracuje nenápadně – po infikování počítače nebo jiného zařízení se skryje v systému, takže si uživatel jeho přítomnosti obvykle nevšimne. Díky tomu dokáže nepřetržitě sledovat veškeré interakce uživatele s klávesnicí, zaznamenávat vložené informace a předávat je útočníkovi.

[18] THOMAS, F. *Adware: The Only Book You'll Ever Need.* Lulu Press, Inc, 2015, s. 47-49.
[19] ČESKO. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In Sbírka zákonů, Česká republika. 2009, částka 11, s. 354

Hlavním cílem keyloggeru je získání citlivých údajů, které mohou být následně zneužity k odcizení finančních prostředků, narušení soukromí oběti nebo k dalším nelegálním aktivitám, včetně podvodů a krádeží identity. Keyloggery jsou často součástí širších kybernetických útoků a představují vážnou bezpečnostní hrozbu.[20]

2.2.2 Počítačoví červi

Počítačoví červi mají mnoho společných rysů s počítačovými viry, avšak zásadní rozdíl mezi nimi spočívá ve způsobu šíření. Zatímco viry potřebují ke své existenci hostitelský program, červi se mohou šířit zcela samostatně. Nejsou tedy závislí na jiném softwaru, což jim umožňuje mnohem rychlejší a efektivnější šíření v digitálním prostředí.

Díky své schopnosti rychlé replikace mohou červi snadno zahltit počítačové sítě nebo dokonce celou IT infrastrukturu. Na rozdíl od klasických virů navíc disponují schopností samostatně analyzovat slabiny v zabezpečení a zneužívat zranitelnosti v systémech. Právě tato vlastnost je činí nebezpečnými, ale zároveň užitečnými při testování bezpečnostních mezer v rámci kybernetické ochrany. [21]

2.2.3 Spyware

Pojem spyware pochází z anglického výrazu „spy software“, což v překladu znamená špionážní software. Tento škodlivý program je navržen tak, aby tajně monitoroval aktivitu uživatele a získaná data odesílal útočníkovi bez vědomí či souhlasu oběti. Mezi shromažďované informace mohou patřit osobní údaje, podnikatelské informace, historie prohlížení webových stránek a další citlivé údaje.

Spyware se může šířit samostatně jako nezávislý malware, ale často bývá skrytě integrován do jiných programů, které se na první pohled jeví jako bezpečné. Po instalaci zůstává spyware aktivní i v případě, že uživatel odstraní aplikaci, se kterou byl původně propojen – nadále pracuje na pozadí systému a nepřetržitě sbírá data o činnosti uživatele. V praxi se spyware často vyskytuje také v mobilních aplikacích, kde uživatel při instalaci nevědomky udělí souhlas se sledováním svých dat prostřednictvím podmínek použití. Tento typ softwaru může představovat vážné riziko pro ochranu soukromí i bezpečnost digitálních zařízení. [22]

[20] AYCOCK, J. *Spyware and Adware.* Springer US, 2010, s. 94.
[21] OSTERHOUDT, M. *Computer Health Made Easy V.2 - Beware of the "Wares" Adware, Malware and Spyware*. Lulu Press, Inc, 2013, s.40-42.
[22] AYCOCK, J. *Spyware and Adware.* Springer US, 2010, s. 74.

2.2.4 Adware

Adware je typ softwaru, který automaticky zobrazuje, přehrává nebo stahuje reklamní obsah na zařízení uživatele, obvykle po instalaci nebo během používání daného programu. V některých případech slouží reklamy k financování vývoje aplikace, což umožňuje její bezplatnou distribuci.

Adware bývá často zaměňován se spywarem, avšak mezi nimi existují rozdíly. Zatímco některé reklamní programy slouží výhradně k zobrazování reklam, jiné nepozorovaně sledují aktivitu uživatele a shromažďují jeho data. V takovém případě již nejde pouze o zobrazování reklam, ale o narušení soukromí, což jej posouvá do oblasti škodlivého softwaru. [23]

2.3 Elektronické obchodování

Podvodné praktiky v online prostředí jsou stále rozšířenější, zejména v oblasti internetového obchodování. Tyto podvody se objevují v různých formách – od falešných inzerátů na bazarových a aukčních portálech až po podvodné e-shopy či nevyžádané nabídky zasílané prostřednictvím e-mailů nebo jiných elektronických komunikačních kanálů.

Způsob provedení bývá často podobný – jde o klamavé nabídky týkající se zboží, služeb, pracovních příležitostí, půjček nebo dokonce zvířat. Typickým znakem je neobvykle výhodná nabídka, která působí lákavě díky výrazně nízké ceně nebo jiným výhodám. Výsledkem může být nejen nedodání objednaného zboží či služby, ale také doručení nekvalitního, poškozeného nebo padělaného produktu. V některých případech dochází i ke zneužití osobních údajů obětí. [24]

2.3.1 Podvodné e-shopy

E-shopy, neboli elektronické obchody, představují online alternativu ke klasickým kamenným prodejnám a umožňují nakupování přes internet. Hlavním rozdílem oproti tradičním obchodům je skutečnost, že veškeré transakce probíhají v digitálním prostředí, bez potřeby fyzické návštěvy prodejny. Na e-shopech si zákazník může prohlížet a vybírat produkty, které následně přidává do virtuálního košíku. Systém mu pak zobrazí souhrn objednávky, včetně celkové ceny a počtu položek. Většina online

[23] THOMAS, F. *Adware: The Only Book You'll Ever Need.* Lulu Press, Inc, 2015, s. 57-58.
[24] SMEJKAL, V, SOKOL, T., VLČEK, M. *Počítačové právo*. Praha: C.H. Beck, 1995, s. 44-47.

obchodů umožňuje filtrování produktů podle různých kritérií, jako jsou značka, cena či kategorie, a nabízí také hodnocení od ostatních zákazníků či porovnání s podobnými výrobky.

Pro dokončení nákupu musí uživatel zadat doručovací údaje, zvolit způsob platby a dopravy. Po odeslání objednávky obdrží potvrzení na svou e-mailovou adresu. Mezi nejznámější a ověřené internetové obchody v České republice patří například Alza.cz, Tsbohemia.cz nebo Allegro.cz. Ačkoli elektronické obchodování přináší mnoho výhod, existují i různá rizika spojená s podvodnými praktikami. Mezi nejčastější patří falešné e-shopy, phishingové útoky, zneužití platebních údajů či další formy internetových podvodů, které mohou zákazníky připravit o peníze nebo osobní údaje. [25]

2.3.1 Internetové inzerce a bazary

V České republice patří mezi nejznámější internetové bazary, kde dochází k častému zneužívání k podvodným aktivitám, Bazoš.cz. Kromě něj však existuje řada dalších platforem, jako například sBazar.cz, Hyperinzerce.cz nebo Facebook Marketplace, kde se rovněž mohou objevovat pochybné nabídky. Na těchto portálech se podvodníci často snaží zlákat kupující na atraktivní nabídky zboží a služeb, přičemž odhalení podvodného inzerátu může být na první pohled složité. Vytvoření falešného profilu a publikace podvodného inzerátu je poměrně snadná záležitost a nevyžaduje žádné pokročilé znalosti.

Jedním z hlavních důvodů, proč jsou tyto podvody tak rozšířené, je jejich jednoduché provedení. Stačí napsat text nabídky, připojit obrázek stažený z internetu, nastavit výrazně nízkou cenu a vyčkat na zájemce. Díky nízké vstupní bariéře se internetové bazary často stávají cílem podvodníků, kteří využívají důvěřivosti kupujících.[26]

2.4 Vishing, Smishing a Spear Phishing

Kybernetičtí útočníci se neomezují pouze na podvodné e-maily, ale často využívají také telefonní hovory (vishing) a SMS zprávy (SMiShing) k vylákání citlivých

[25] KOLOUCH, J. *CyberCrime*. Praha2016, str. 204-210.
[26] KOŽÍŠEK, M., PÍSECKÝ, V. *Bezpečně na internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. 109-113 s

informací. V rámci hlasového phishingu pachatel kontaktuje oběť telefonicky a snaží se ji přesvědčit, aby mu sdělila přihlašovací údaje nebo jiné důvěrné informace. [27]

Odhalení tohoto podvodu komplikuje fakt, že útočníci často zneužívají technologii VOIP (Voice over Internet Protocol) a speciální metodu caller ID spoofingu, která umožňuje falšovat identitu volajícího. Oběť tak může mít dojem, že hovor pochází z důvěryhodného zdroje, například z banky nebo jiné instituce. S rozvojem umělé inteligence se vishingové podvody stávají ještě sofistikovanějšími – stále častěji jsou využívány audio deepfakes, tedy technologie umožňující napodobit hlas konkrétní osoby. To ještě více ztěžuje možnost rozpoznání podvodu a zvyšuje riziko, že oběť na podvod naletí. Naopak SMiShing, tedy phishing realizovaný prostřednictvím podvodných SMS zpráv, není z hlediska četnosti tak výrazný, přesto může představovat riziko pro méně obezřetné uživatele. Mezi sofistikovanější formy phishingu patří spear phishing, který je mnohem cílenější než běžné phishingové útoky. Tento druh podvodu je zaměřen na konkrétní osobu a celý plán útoku je individuálně přizpůsoben na základě informací, které útočník získal předchozí interakcí v rámci sociálního inženýrství. Díky této personalizaci působí spear phishing velmi důvěryhodně a je pro oběť mnohem obtížnější ho odhalit.[28]

[27] JONES, C. *Phishing, Vishing, SMiShing, Whaling And Pharming: How To Stop Social Engineering Attacks* [online]. [cit.2025-02-05]. Dostupné z WWW: https://expertinsights.com/insights/phishing-vishing smishing-whaling-and-pharming-how-to-stop-social-engineering-attacks/

[28] DVOŘÁK, M. *Phishing, pharming a jejich trestněprávní postih.* Trestněprávní revue. 2018, č. 4, s. 84–89. [online]. [cit.2025-02-05]. Dostupné z WWW: https://portaro.mfcr.cz/#!/records/72f56d42-7604-4ea0-956a-5dd7c6e35917

3 Působení pachatele na oběti podvodu

Obětí kybernetického podvodu se může stát jakýkoliv subjekt – fyzická osoba, právnická osoba, ale i stát. Kybernetické podvody zasahují oběti v různých oblastech, zejména ekonomické, sociální a psychické. Zasažená osoba často nejen přichází o finanční prostředky, ale může čelit i vážným psychickým důsledkům, jako jsou stres, úzkost či ztráta důvěry v digitální prostředí. Statistiky o kybernetické kriminalitě často nezachycují skutečný rozsah problému, protože mnoho obětí si ani neuvědomuje, že se staly terčem podvodu. To je způsobeno například sofistikovaností některých útoků, kdy pachatel využívá pokročilé metody sociálního inženýrství k tomu, aby oběť jednala nevědomě v jeho prospěch. Dalším faktorem je neochota obětí podvod nahlásit – některé z nich se bojí ztráty důvěryhodnosti (např. firmy a bankovní instituce), jiné pociťují stud nebo obavu z komplikovaného právního procesu.[29]

Vztah mezi pachatelem a obětí kybernetického podvodu je specifický v tom, že mezi nimi zpravidla neexistuje osobní kontakt. Podvodník může působit odkudkoliv na světě a často využívá anonymizační technologie, aby skryl svou totožnost. To nejen ztěžuje odhalení pachatele, ale i následné právní kroky. Právní jurisdikce se totiž může lišit podle země, odkud pachatel operuje, což značně komplikuje mezinárodní vyšetřování a stíhání těchto trestných činů.

S rostoucím rozšířením internetu mezi stále větší počet uživatelů se zároveň zvyšuje i množství potenciálních pachatelů kybernetické kriminality. Tato skupina není homogenní – zahrnuje osoby různého věku, socioekonomického postavení, pohlaví, vzdělání či místa bydliště. Obecně lze pachatele kybernetické kriminality rozdělit do dvou kategorií:

- Amatéři – zaměřují se na jednodušší formy trestné činnosti, jako jsou podvody při prodeji zboží, kyberšikana či neoprávněné získávání přístupových údajů.
- Profesionálové – zkušení hackeři a organizované skupiny, které sledují aktuální trendy v oblasti kybernetické bezpečnosti, vyvíjejí vlastní škodlivý software (malware) a hledají způsoby, jak obejít ochranné mechanismy.

[29] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s. 487

Přestože je kyberkriminalita často spojována s pokročilými technologiemi, její páchání není výhradně podmíněno vysokým vzděláním. Klimek, Záhora a Holcr uvádějí, že pachatelé kybernetických trestných činů jsou obecně vysoce inteligentní[30] – s tímto tvrzením však nelze zcela souhlasit. Moderní technologie jsou stále uživatelsky přívětivější, což umožňuje i méně technicky zdatným jedincům využívat internet k nelegálním aktivitám.[31] Založení falešného internetového obchodu nevyžaduje pokročilé znalosti a podvody na online bazarech či sociálních sítích jsou ještě jednodušší. To dokazuje, že kyberkriminalita není výsadou pouze technologicky vzdělaných jedinců, ale může se jí dopustit prakticky kdokoli s přístupem k internetu a základními dovednostmi.[32]

Pachatelé kybernetických podvodů se nejčastěji nacházejí ve věkové skupině 17 až 30 let. Tento trend lze vysvětlit několika faktory – starší generace často nevykazují takovou ochotu či schopnost pracovat s moderními technologiemi, zatímco mladší lidé, kteří s digitálním prostředím vyrůstají, mají k těmto technologiím přirozeně bližší vztah a dokážou je efektivně využívat. Internet a výpočetní technika tvoří nedílnou součást jejich každodenního života, což jim poskytuje značnou výhodu při páchání kybernetických podvodů. Motivace pachatelů kybernetických podvodů je klíčovým faktorem při určování jejich jednání a charakteru trestné činnosti. Kuchta upozorňuje, že porozumění motivům pachatelů je důležité nejen pro pochopení jejich psychologického profilu, ale i pro správnou kvalifikaci trestného činu. Nejčastější motivací bývá snaha o finanční zisk, což je hlavní hnací síla většiny kybernetických podvodníků. Kromě toho se však objevují i další důvody, jako je touha po pomstě, politické či ideologické cíle, případně sexuální motivy. Motivy se často vzájemně kombinují a vytvářejí složitější vzorce chování pachatelů. [33]

Kybernetická kriminalita v posledních letech roste, zatímco tradiční kriminalita v mnoha oblastech klesá. Jedním z hlavních důvodů tohoto trendu je snadnost, s jakou lze kybernetické podvody páchat – internet umožňuje pachatelům oslovit velké množství potenciálních obětí během krátké doby, přičemž mnohé podvodné techniky jsou nenáročné na technické znalosti. Například šíření pomluv či manipulativních informací

[30] KLIMEK, L, ZÁHORA, J, a HOLCR, K, Počítačová *kriminalita v európskych súvislostiach*. Praha: Wolters Kluwer, 2016., s. 53.
[31] HOLCR, K, BUBELÍNI, J, FENYK, J. a kol. *Kriminológia*. Bratislava: Iura Edition, s. 361.
[32] VELIKOVSKÁ, M. *Psychologie obětí trestných činů. Praha*: Grada Publishing, 2016, s. 35-38.
[33] KUCHTA, J, *Základy kriminologie a trestní politiky*. 2. vyd. Praha: C. H. Beck, s. 606.

je díky sociálním sítím extrémně rychlé a může mít široký dosah, přičemž pachatelé často spoléhají na anonymitu digitálního prostředí.

Dalším faktorem, který přispívá k nárůstu kyberkriminality, je nižší riziko odhalení – pachatelé využívají anonymizační technologie, kryptoměny a další metody, které ztěžují jejich identifikaci. Smejkal k tomu dodává, že pro některé pachatele představuje kybernetická kriminalita také intelektuální výzvu – snahu dokázat svou technickou zdatnost, získat pocit převahy nad obětí nebo nad orgány činnými v trestním řízení. Tento aspekt je typický zejména pro hackery, kteří vnímají prolomení bezpečnostních systémů jako test svých schopností. [34]

3.1 Dopady trestného činu na oběť a její okolí

Dopady trestného činu na oběť mohou být ekonomické, psychologické, sociální i právní. Kromě primární újmy, která vzniká přímo v důsledku podvodu (např. finanční ztráta), se oběť často potýká i se sekundární viktimizací, tedy druhotným poškozením, jež může být stejně závažné nebo dokonce horší než samotný trestný čin. Sekundární viktimizace nastává zejména v důsledku nespolupráce oběti s Policií ČR a justicí nebo kvůli nevhodným reakcím okolí na skutečnost, že se oběť stala terčem podvodu. Jak uvádí Čírtková, sekundární rány mají především psychologický charakter a mohou vést k dlouhodobým negativním změnám v chování a prožívání oběti. [35]

Podle Čírtkové představuje samotný podvod jen začátek procesu viktimizace – následuje další zraňování a poškozování jedince, které často přichází ze strany institucí či okolí oběti. K těmto následkům patří trojice nejčastějších pocitů, které mohou výrazně ovlivnit psychický stav oběti:[36]

1. **Pocit nespravedlnosti** – vzniká kvůli **nedostatku informací o vyšetřování**, když je pachatel stále na svobodě, nebo při zdlouhavém a neefektivním soudním procesu. Včasné a jasné informace mohou tento pocit zmírnit.

[34] SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s. 472.
[35] ČÍRTKOVÁ, L. *Viktimologie pro forenzní praxi*. Praha: Portál, s. 71.
[36] ČÍRTKOVÁ, L., VITOUŠOVÁ, P. *Pomoc obětem (a svědkům) trestných činů: příručka pro pomáhající profese*. Praha: Grada, s. 53.

2. **Pocit nedůstojnosti** – oběť se může cítit **ponížená a zahanbená**, zejména při **necitlivých výsleších** či v případě negativního mediálního obrazu, který ji může dále stigmatizovat.
3. **Pocit izolace** – oběť podvodu se může setkat s **nepochopením a distancováním ze strany rodiny či přátel**, což vede k pocitům osamělosti a v některých případech i ke změně jejího chování.

V České republice je problematika sekundární viktimizace málo zmapovaná, neboť chybí podrobné výzkumy. Policie ČR sice eviduje oběti kybernetických podvodů, ale zaměřuje se především na materiální škody a zdravotní následky. Psychická újma sice bývá zahrnuta do statistik jako „jiný následek“, avšak většinou se jedná o primární důsledky podvodu, zatímco dopady sekundární viktimizace často zůstávají opomíjeny.

3.2 Rozšířené techniky sociálního inženýrství používané pachateli

Pachatelé kybernetických podvodů se nezaměřují pouze na technické prostředky, ale čím dál častěji využívají psychologické a manipulační techniky, které spadají do oblasti tzv. **sociálního inženýrství**. Tento pojem označuje soubor metod, jejichž cílem je zmanipulovat oběť k tomu, aby sama poskytla útočníkovi důvěrné informace, nainstalovala škodlivý software, případně provedla jinou akci ve prospěch pachatele. Vedle známých forem jako phishing či spear phishing, které jsou v této práci již popsány, existují i další způsoby působení na oběti, které bývají méně známé, avšak velmi efektivní:

- **Pretexting**: Útočník vytváří smyšlený scénář (např. že je zaměstnancem banky, policie či IT technikem), aby získal důvěru oběti a přiměl ji sdělit přístupové údaje nebo jiné citlivé informace. V těchto případech se oběť často domnívá, že jedná s autoritou nebo důvěryhodnou institucí, což zvyšuje pravděpodobnost úspěchu útoku.
- **Baiting**: Jde o techniku využívající „návnady“, například infikovaného USB zařízení zanechaného na veřejném místě (např. v čekárně nebo u vchodu do firmy). Oběť, vedená zvědavostí nebo dobrými úmysly, médium připojí k počítači, čímž dojde k automatickému spuštění škodlivého kódu.
- **Nigerijské dopisy (Nigerian scam)**: Oběť je kontaktována zprávou, často psanou emotivním a důvěřivým jazykem, která slibuje podíl na převodu velké částky peněz výměnou za předem zaplacené poplatky. Tento podvod spoléhá na chamtivost, soucit nebo důvěřivost oběti.

- **Quishing**: Novější forma útoku kombinující phishing a QR kódy. Útočník oběti předloží falešný QR kód, který ji přesměruje na podvodné webové stránky, často nerozeznatelné od legitimních. Oběť je pak vyzvána ke stažení aplikace, zadání přístupových údajů nebo potvrzení platební transakce. [37]

Podle Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) se v posledních letech výrazně zvýšila sofistikovanost těchto útoků. Útočníci stále častěji využívají tzv. **multikanálové scénáře** – kombinují např. podvodné e-maily, následné telefonáty a falešné webové stránky, čímž vytvářejí iluzi věrohodnosti a zvyšují tlak na oběť. Tyto metody potvrzují, že při kybernetických podvodech už často nejde pouze o technické prolomení ochrany, ale o psychologický boj, ve kterém pachatel cíleně využívá slabin lidského chování – důvěry, neznalosti, strachu či nátlaku. To činí z oběti nejen pasivního příjemce škody, ale i aktivního účastníka, který je k podvodu nevědomky manipulován.[38]

[37] *Národní úřad pro kybernetickou a informační bezpečnost - Sociální inženýrství* [online]. Brno, © 2016 [cit. 2025-03-29]. Dostupné z WWW: https://nukib.gov.cz/cs/infoservis/doporuceni/1497-socialni-inzenyrstvi/

[38] *Národní úřad pro kybernetickou a informační bezpečnost: Kybernetické incidenty pohledem NÚKIB - březen 2023* [online]. Brno, © 2023 [cit. 2025-03-29]. Dostupné z WWW: https://nukib.gov.cz/cs/infoservis/aktuality/1954-kyberneticke-incidenty-pohledem-nukib-brezen-2023/

4 Bezpečností opatření a postupy pro prevenci kybernetických hrozeb

V současné době se prevence stává nezbytným nástrojem ochrany před nejrůznějšími riziky a negativními jevy. Lze ji chápat jako souhrn opatření a strategií, které mají za cíl předcházet nebezpečným situacím a minimalizovat jejich dopady. Využívá se v mnoha oblastech lidské činnosti, přičemž jejím hlavním účelem je zamezit vzniku problémů dříve, než skutečně nastanou. S rozvojem technologií se digitální svět stal neoddělitelnou součástí života a už od raného věku mají děti přístup k mobilním telefonům, tabletům či počítačům. Moderní technologie umožňují komunikovat v reálném čase, nakupovat, objednávat služby nebo spravovat finance odkudkoliv na světě. Přestože tato konektivita přináší mnoho výhod, zároveň s sebou nese i významná rizika.[39]

Digitální prostředí se stále více stává prostorem, kde se pachatelé zaměřují na zranitelné skupiny, zejména děti a mladistvé. Mnoho rodičů si neuvědomuje potenciální hrozby spojené s online aktivitami jejich dětí, ať už kvůli nedostatku času, neznalosti moderních technologií, nebo pocitu falešného bezpečí. Dnešní mladá generace často ovládá digitální nástroje lépe než jejich rodiče, což může vést k nižší úrovni kontroly a vyšší zranitelnosti. [40]

Prevence v oblasti kybernetické kriminality je proto nezbytná pro ochranu všech věkových skupin, od dětí přes dospělé až po seniory. Kybernetické hrozby se neustále vyvíjejí a jejich pachatelé často předbíhají bezpečnostní opatření o několik kroků. Z tohoto důvodu je klíčové neustále inovovat preventivní strategie a hledat nové způsoby, jak eliminovat nebezpečí spojená s kybernetickou kriminalitou. Osvěta, vzdělávání a aktivní přístup k digitální bezpečnosti jsou hlavními pilíři, které mohou pomoci minimalizovat rizika a zvýšit celkovou ochranu uživatelů internetu. [41]

[39] PRŮCHA, J., WALTEROVÁ, E., MAREŠ, J. *Pedagogický slovník. 7.* aktualiz. a rozš. vyd. Praha: Portál, 2013, s.219.
[40] MARTANOVÁ, V., B. JANÍKOVÁ, T. DANĚČKOVÁ, et al. *Učební texty ke specializačnímu studiu pro školní metodiky prevence*. Praha: Centrum adiktologie
[41] CHALUPOVÁ, K., ŠTEFUNKOVÁ, M., ŠEJVL, J. *Základy prevence kriminality pro pedagogické pracovníky*. Praha: Klinika adiktologie, 1. lékařská fakulta Univerzity Karlovy v Praze a Všeobecná fakultní nemocnice v Praze. Togga, 2012, s.11.

4.1 Ochrana osobních údajů a bezpečné užívání internetu

Digitální technologie se staly nedílnou součástí každodenního života a nabízejí široké možnosti v oblasti vzdělávání, komunikace a zábavy. Spolu s těmito výhodami však vznikají i rizika, která se nejčastěji dotýkají dětí a mladistvých. Zajištění bezpečnosti na internetu je proto klíčové pro ochranu osobních údajů, prevenci kybernetických útoků a minimalizaci negativních dopadů na duševní zdraví. [42]

Vzdělávání a prevence kybernetických hrozeb

- Pravidelná diskuze o kybernetických rizicích, jako jsou podvody, kyberšikana nebo škodlivý obsah, pomáhá všem uživatelům lépe rozpoznat potenciální hrozby a chránit se před nimi. Vzdělávání v oblasti digitální bezpečnosti a schopnost přistupovat k online obsahu s kritickým pohledem jsou klíčové pro včasné rozpoznání podezřelých situací a manipulativních praktik. Zvyšování digitální gramotnosti napříč věkovými skupinami přispívá k bezpečnějšímu a odpovědnějšímu chování v kyberprostoru.

Technologická opatření a kontrola přístupu

- Nastavení rodičovské kontroly a věkových omezení. Používání bezpečnostních filtrů pomáhá omezit přístup k nevyhovujícímu obsahu, čímž se minimalizuje riziko, že děti narazí na nevhodné nebo škodlivé materiály.
- Vysvětlování rizik nevhodných webových stránek. Otevřený dialog o důvodech, proč jsou některé stránky nebezpečné, podporuje samostatné rozhodování a pomáhá dětem pochopit rizika spojená s neověřeným obsahem.

Bezpečné přihlašování a ochrana osobních údajů

- Kvalitní heslo je základním bezpečnostním prvkem, který pomáhá chránit účty před neoprávněným přístupem. Správně vytvořené heslo, které kombinuje písmena, číslice a speciální znaky, výrazně snižuje riziko zneužití osobních údajů.
- Dvoufázové ověření jako další vrstva zabezpečení. Pro zvýšení bezpečnosti účtů na sociálních sítích je vhodné využít dvoufázové ověření, které poskytuje další ochranu při přihlašování. Pokud se někdo pokusí přihlásit k účtu z neznámého zařízení, systém vyžaduje zadání ověřovacího kódu zaslaného na telefon nebo e-mail. Tento

[42] KOLOUCH, J. CyberCrime. Praha, 2016, s. 172.

bezpečnostní prvek výrazně snižuje riziko neoprávněného přístupu a může zabránit mnoha pokusům o odcizení účtu. [43]

Obezřetnost při sdílení informací

- Uživatelé, zejména mladí lidé, by měli pečlivě zvažovat, jaké informace zveřejňují online. Sdílení osobních údajů, fotografií nebo polohy může být zneužito a vést k nežádoucím situacím. Důležité je také, aby si děti a dospívající byli vědomi možných důsledků a v případě pochybností se nebáli obrátit na dospělé nebo odborníky. [44]

Ochrana před kyberšikanou

- Kyberšikana je jedním z nejčastějších negativních jevů v online prostředí. Rodiče a učitelé by měli být schopni rozpoznat její projevy, například výhrůžné zprávy, šíření pomluv nebo zesměšňování na sociálních sítích. Otevřená komunikace mezi dětmi a rodiči je zásadní – mladí uživatelé by měli vědět, že mohou své zkušenosti sdílet a že jejich obavy budou brány vážně. Rychlá reakce na kyberšikanu může zabránit jejímu dalšímu šíření a minimalizovat psychické dopady na oběť.

Monitoring online aktivit

- Rodiče mohou využívat různé nástroje pro sledování online aktivit svých dětí, například kontrolu navštěvovaných webových stránek nebo komunikace na sociálních sítích. Přesto je důležité zachovat rovnováhu mezi kontrolou a důvěrou – přílišná kontrola může vést ke ztrátě důvěry, zatímco vhodně nastavené hranice pomáhají dětem lépe pochopit, jak se bezpečně pohybovat v digitálním světě. [45]

Bezpečné chování na internetu je nezbytnou součástí digitální gramotnosti a klíčem k ochraně uživatelů před online hrozbami. Správné vzdělávání, technická opatření a otevřená komunikace mohou výrazně snížit riziko kybernetických útoků, kyberšikany

[43] KOŽÍŠEK, M., PÍSECKÝ,V. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. s. 36-37.
[44] KAMIL, K., SZOTKOWSKI, R., KUBALA. L. *Bezpečné chování na internetu pro kluky a pro holky – náměty na výukové aktivity* [online]. [cit. 2025-16-03]. Dostupné z WWW: https://www.e-bezpeci.cz/index.php/ke-stazeni/tiskoviny/159-bezpecne-chovani-na-internetu-pro-kluky-a-pro-holky-2022/file , s.23.
[45] KAMIL, K., SZOTKOWSKI, R., KUBALA. L. *Bezpečné chování na internetu pro kluky a pro holky – náměty na výukové aktivity* [online]. [cit. 2025-16-03]. Dostupné z WWW: https://www.e-bezpeci.cz/index.php/ke-stazeni/tiskoviny/159-bezpecne-chovani-na-internetu-pro-kluky-a-pro-holky-2022/file , s.35.

či zneužití osobních údajů. Každý uživatel by měl být informován o rizicích online světa a umět přijímat preventivní **opatření**, která zajistí jeho bezpečnost a ochranu soukromí.

4.2 Preventivní programy v ČR

Programy zaměřené na prevenci kybernetické kriminality se soustředí na vzdělávání široké veřejnosti o rizicích spojených s internetem a sociálními sítěmi. Jejich hlavním cílem je zvýšit povědomí o kybernetických hrozbách a motivovat uživatele všech věkových kategorií k bezpečnějšímu a odpovědnějšímu chování v online prostředí. Tyto iniciativy se zaměřují na rozvoj digitální gramotnosti a podporují osvojení zásad bezpečného pohybu v kyberprostoru.

Dále pokračují dlouhodobé iniciativy jako „Bezpečně online“, „Kybernetická bezpečnost a děti“, „Ochrana na internetu“ a „Digitální cesta bezpečí“.

Internetem bezpečně

Projekt se zaměřuje na zvyšování povědomí o rizicích spojených s online prostředím prostřednictvím různorodých vzdělávacích aktivit. Aktivně reaguje na nové kybernetické hrozby a sdílí důležité informace na svých webových stránkách, sociálních sítích a během vzdělávacích akcí. Jeho cílem je nejen předcházet možným negativním dopadům těchto hrozeb, ale také přispět ke snížení protiprávního jednání v digitálním prostoru.[46]

Kyberbezpečí a Děti v síti

Iniciativa zaměřená na kybernetickou bezpečnost poskytuje informace o správném a bezpečném chování v online prostředí, zejména na sociálních sítích, v chatech a dalších veřejných komunikačních platformách. Jejím cílem je zvýšit povědomí o rizicích spojených s virtuální komunikací a nabídnout účinné strategie ochrany před možným online či reálným nátlakem.

Program preventivního vzdělávání „Děti v síti“ je určen rodičům, pedagogům a široké veřejnosti. Jeho hlavním posláním je informovat o konkrétních hrozbách, kterým

[46] PREVENCE KRIMINALITY. *Internetem bezpečně* [online]. © 2018 [cit. 2025-03-19]. Dostupné z WWW: https://prevencekriminality.cz/internetem-bezpecne/

děti čelí při používání internetu a online komunikaci. Díky tomu přispívá k vytváření bezpečnějšího digitálního prostředí pro nejmladší uživatele. [47]

Bezpečně v kyberprostoru

Iniciativa zaměřená na bezpečnost v digitálním prostoru usiluje o omezení šíření kybernetických hrozeb v Jihomoravském kraji, přičemž se soustředí na uživatele osobních počítačů. V rámci tohoto programu probíhá široká škála vzdělávacích aktivit, včetně seminářů, tvorby metodických materiálů pro učitele IT, natáčení videospotů, organizace soutěží a výstav, vydávání brožur pro rodiče, letáků a interaktivních komiksů.

Součástí iniciativy je také správa webových stránek a sociálních sítí, přičemž se aktuálně pracuje na vývoji mobilní aplikace. V regionu, kde se nachází více než 650 základních a středních škol, se program zaměřuje na školení ředitelů, učitelů IT, metodiků prevence, žáků, rodičů i širší veřejnosti. Zapojeni jsou také příslušníci Policie ČR, úředníci místních i krajských samospráv, probační pracovníci a odborníci na sociálně-právní ochranu dětí. [48]

Tvoje cesta onlinem

V roce 2019 byl vytvořen inovativní model policejní prevence, který propojuje dosavadní iniciativy s novými přístupy. Struktura programu se skládá ze tří hlavních oblastí, přičemž se zaměřuje na klíčové priority policejního prezidenta: boj proti drogové kriminalitě, bezpečnost v online prostředí a dopravní prevenci. Velký důraz je kladen na odpovědnost jednotlivců za vlastní bezpečí, což se týká i rodičů, kteří nesou zodpovědnost za ochranu svých dětí.

Součástí programu je sekce „Tvoje cesta onlinem“, která se věnuje digitální bezpečnosti. Tento projekt, vyvinutý ve spolupráci s ČSOB, nabízí metodické materiály a praktické návody, zaměřené především na rodiče a děti, s cílem podpořit účinnou

[47] PREVENCE KRIMINALITY. *Programy primární prevence „Kyberbezpečí“ a „Děti v síti“* [online]. © 2018 [cit. 2025-03-19]. Dostupné z WWW: https://prevencekriminality.cz/programy-primarni-prevence-kyberbezpeci-a-deti-v-siti/

[48] PREVENCE KRIMINALITY. *Bezpečně v kyberprostoru* [online]. © 2018 [cit. 2025-03-19]. Dostupné z WWW: https://prevencekriminality.cz/bezpecne-v-kyberprostoru/.

prevenci kybernetických rizik. Celkově přináší moderní a komplexní přístup k policejní prevenci, reflektující aktuální výzvy digitálního světa. [49]

Bezpečně v kyber!

Online vzdělávací program „Bezpečně v kyber!“ je zaměřen na prevenci a osvětu v oblasti rizikového chování v kyberprostoru, zejména u dětí a mládeže. Jeho hlavním cílem je přehlednou a srozumitelnou formou informovat o aktuálních hrozbách spojených s online světem. Program se věnuje tématům, jako jsou kyberšikana, kybergrooming, sexting, závislost na digitálních technologiích (tzv. netolismus), kyberstalking nebo problematika nenávistného projevu na internetu (hate speech). Důraz je kladen také na bezpečné užívání sociálních sítí, uvědomění si digitální stopy a zodpovědné online chování. Součástí programu jsou doporučení pro prevenci, praktické úkoly a informační zdroje, které mohou využít nejen pedagogové, ale i rodiče a další pracovníci v oblasti prevence. Program si klade za cíl zvýšit digitální gramotnost a podpořit bezpečné prostředí v online prostoru.[50]

[49] HODÁČKOVÁ, V. *Tvoje cesta* [online]. © 2023 Policie ČR [cit. 2025-03-19]. Dostupné z WWW: https://www.policie.cz/clanek/tvoje-cesta.aspx

[50] *Národní úřad pro kybernetickou a informační bezpečnost: Kurz Bezpečně v kyber! se otevírá veřejnosti* [online]. Brno, © 2021 [cit. 2025-29-03]. Dostupné z WWW: https://nukib.gov.cz/cs/infoservis/aktuality/1691-kurz-bezpecne-v-kyber-se-otvira-verejnosti/

5 Praktická část

Praktická část bakalářské práce se zaměřuje na oběti kybernetických podvodů v České republice a snaží se prostřednictvím empirického výzkumu porozumět jejich zkušenostem, prožitkům a informovanosti v oblasti kybernetické bezpečnosti. Hlavním cílem je identifikovat nejčastější typy kybernetických útoků, se kterými se tito lidé setkali, zmapovat jejich dopady – jak finanční, tak i psychologické – a zjistit, nakolik byli jednotlivci na dané hrozby připraveni. K získání relevantních dat byl využit anonymní dotazník, který byl osobně distribuován obětem kybernetických podvodů. Sběr dat probíhal v okrese České Budějovice, konkrétně na obvodních odděleních Policie České republiky: OOP Čtyři Dvory, OOP Město, OOP Suché Vrbné, OOP Lišov, OOP Hluboká nad Vltavou, OOP Boršov nad Vltavou a OOP Týn nad Vltavou. Všichni účastníci byli před vyplněním dotazníku informováni, že jejich odpovědi jsou zcela anonymní a budou využity výhradně pro účely této studie.

Dotazníkové šetření probíhalo v období od 1. února 2025 do 1. května 2025 a podařilo se získat 58 řádně vyplněných dotazníků. Vyplněné dotazníky byly následně vyhodnoceny, zpracovány a pro přehlednost převedeny do grafické podoby. Získaná data jsou analyzována pomocí základních statistických metod a interpretována v kontextu stanovených výzkumných hypotéz. Na základě těchto zjištění budou formulována doporučení a návrhy na zlepšení prevence, informovanosti i reakčních mechanismů v oblasti kybernetické bezpečnosti. Praktická část se opírá o následující výzkumné hypotézy:

5.1 Stanovené hypotézy

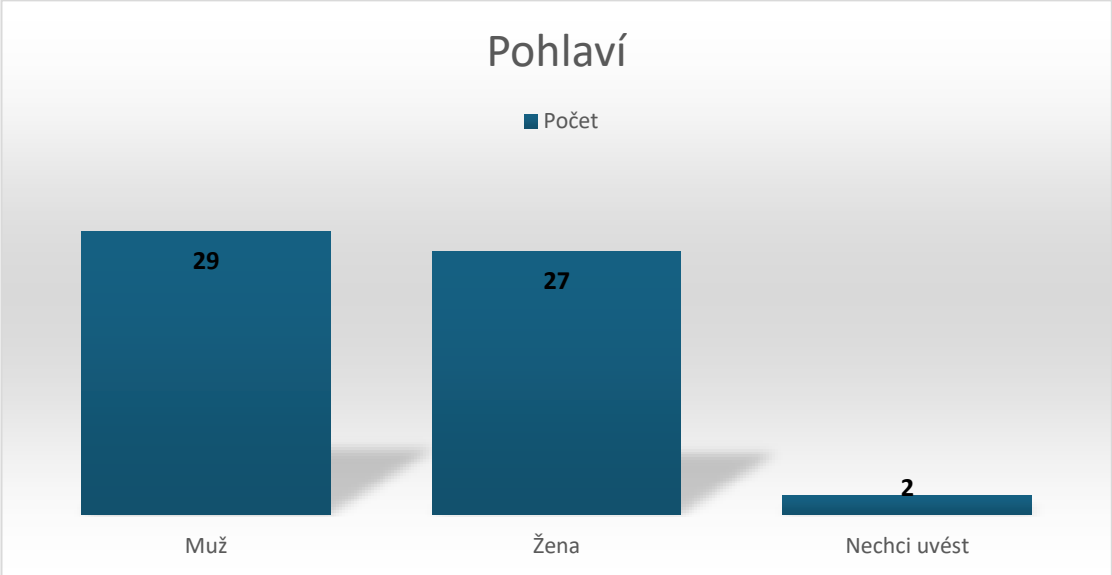
H1: Nejčastějším typem kybernetických podvodů v České republice jsou phishingové útoky zaměřené na získání finančních prostředků.

H2: Kybernetické podvody způsobují obětem nejen finanční ztráty, ale také závažné psychologické dopady, jako je stres a úzkost.

H3: Informovanost veřejnosti o rizicích kybernetických útoků a preventivních opatřeních je nedostatečná, což zvyšuje zranitelnost jednotlivců vůči těmto hrozbám.

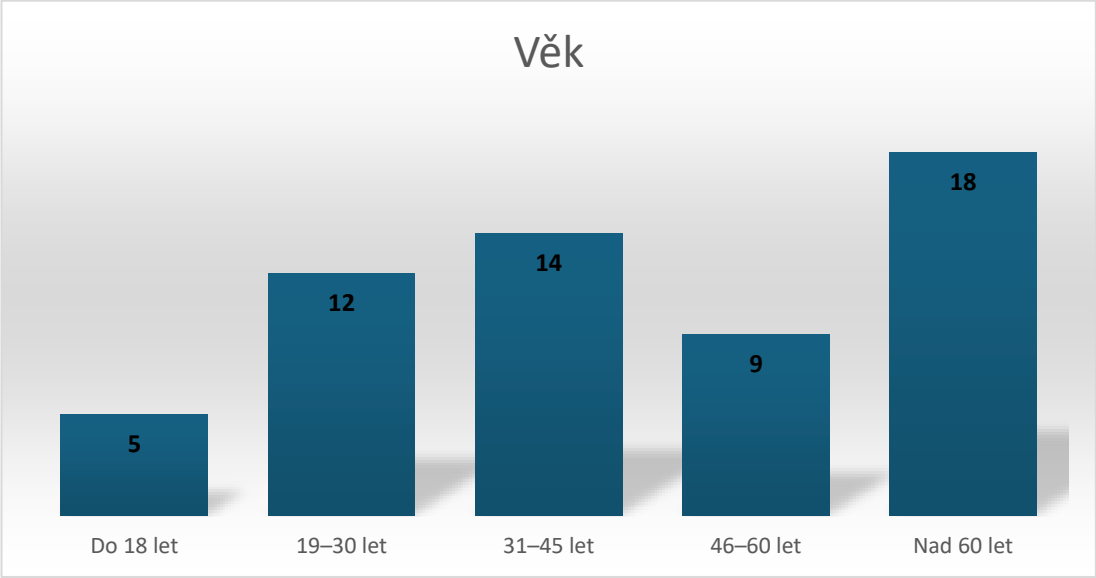
5.2 Vyhodnocení dotazníku

Graf č. 1: **Pohlaví** [51]



Nejvíce respondentů tvoří muži (29), což odpovídá 50 % celkového počtu. Žen odpovědělo 27 (46,6 %) a 2 respondenti (3,4 %) se rozhodli své pohlaví neuvést. Tato data ukazují, že výzkumu se zúčastnily téměř rovnoměrně obě pohlaví, přičemž podíl mužů mírně převyšuje.

Graf č. 2: **Věk** [52]



Nejpočetnější skupinu tvoří respondenti ve věku nad 60 let (18 osob; 31 %), následuje věková skupina 31–45 let (14 osob; 24,1 %) a 19–30 let (12 osob; 20,7 %). Méně

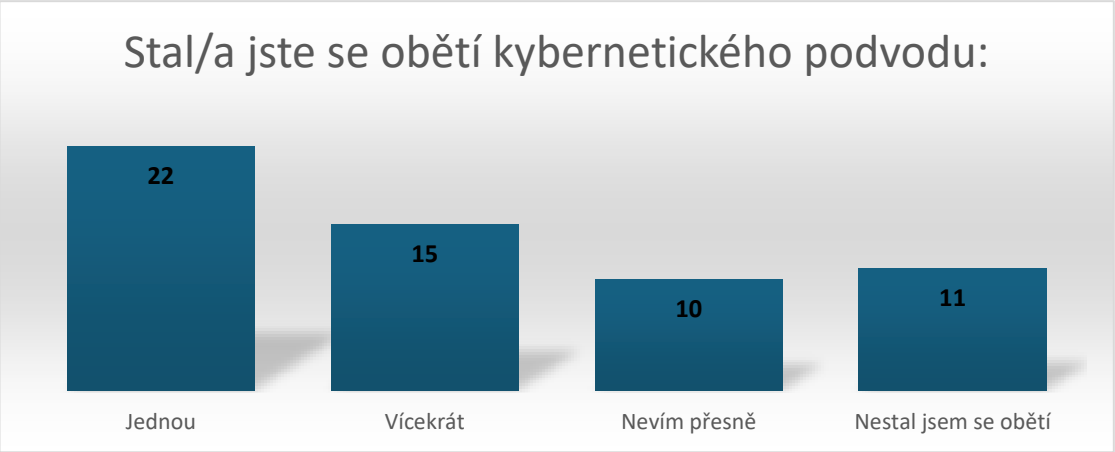
[51] Vlastní zpracování
[52] Vlastní zpracování

zastoupeni byli respondenti ve věku 46–60 let (9 osob; 15,5 %) a do 18 let (5 osob; 8,6 %). Výsledky ukazují, že se dotazníkového šetření zúčastnili lidé napříč věkovými kategoriemi, přičemž nejvýrazněji jsou zastoupeni starší dospělí.

Graf č. 3: **Nejvyšší dosažené vzdělání** [53]

Největší část respondentů uvedla středoškolské vzdělání s maturitou (20 osob; 34,5 %), následované vysokoškolským vzděláním (18 osob; 31 %). Dalších 9 respondentů (15,5 %) dosáhlo středoškolského vzdělání bez maturity. Základní vzdělání má 6 osob (10,3 %) a zbývajících 5 respondentů (8,6 %) zařadilo své vzdělání do kategorie „jiné“. Z výsledků je patrné, že většina dotázaných disponuje alespoň středoškolským vzděláním, přičemž značná část z nich má i vysokoškolský titul.

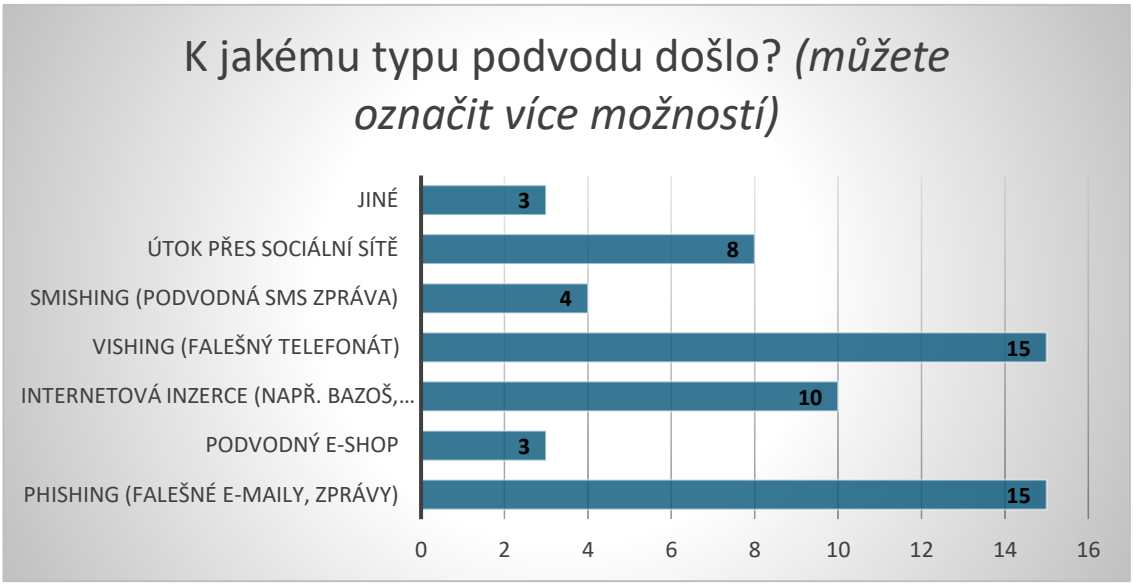
Graf č. 4: **Stal/a jste se obětí kybernetického podvodu**[54]



[53] Vlastní zpracování
[54] Vlastní zpracování

Nejvíce respondentů (22 osob; 37,9 %) uvedlo, že se stali obětí kybernetického podvodu jednou. Dalších 15 respondentů (25,9 %) se s touto zkušeností setkalo opakovaně. Deset osob (17,2 %) si není jistých, zda se obětí stali, a 11 respondentů (19 %) uvedlo, že se obětí kybernetického podvodu nestali. V těchto případech se však jednalo o situace, kdy šlo o pokus o podvod, který byl včas rozpoznán a následně nahlášen Policii ČR. Výsledky naznačují, že většina dotázaných má osobní zkušenost s kybernetickým podvodem, přičemž u části z nich šlo o opakovaný výskyt.

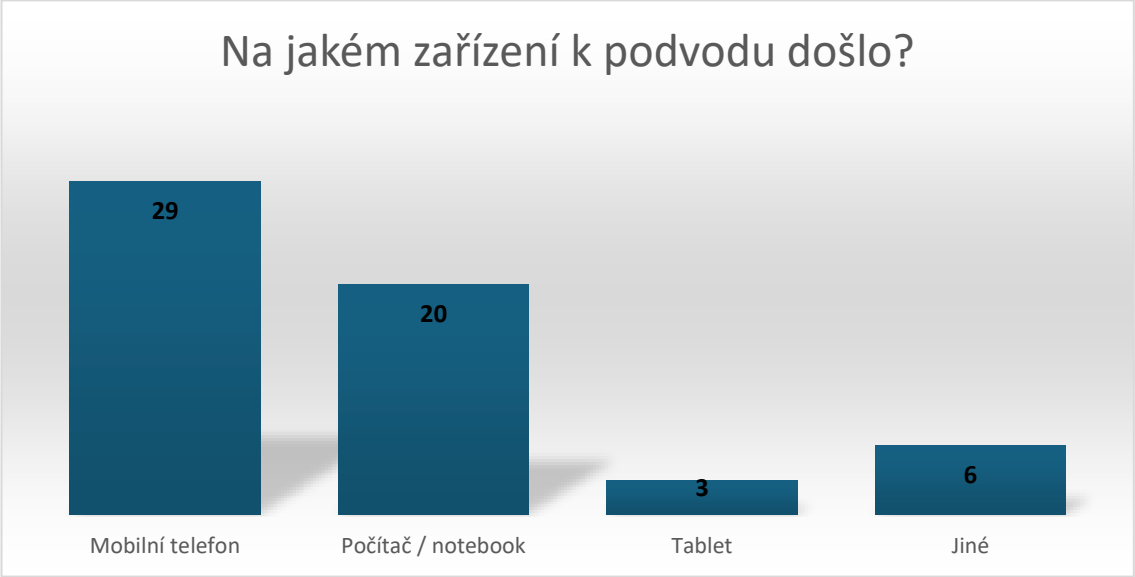
Graf č. 5: **K jakému typu podvodu došlo?** *(můžete označit více možností)* [55]



Nejčastějším typem kybernetického podvodu, který respondenti uvedli, byl phishing prostřednictvím falešných e-mailů a zpráv (15 respondentů; 25,9 %) a vishing, tedy podvodný telefonát, například od falešného pracovníka banky (15 respondentů; 25,9 %). Dále respondenti často zmiňovali podvod v rámci internetové inzerce (např. Bazoš, Facebook Marketplace), který se týkal 10 respondentů (17,2 %). Útoky vedené přes sociální sítě uvedlo 8 respondentů (13,8 %) a smishing – tedy podvodné SMS zprávy – označili 4 respondenti (6,9 %). Méně časté byly podvodné e-shopy (3 respondenti; 5,2 %) a kategorie „jiné“, kam spadaly méně typické útoky (3 respondenti; 5,2 %). Výsledky ukazují, že pachatelé využívají širokou škálu prostředků, přičemž e-mailová a telefonická komunikace jsou mezi respondenty nejčastěji uváděnými způsoby útoků.

[55] Vlastní zpracování

Graf č. 6: **Na jakém zařízení k podvodu došlo?** [56]



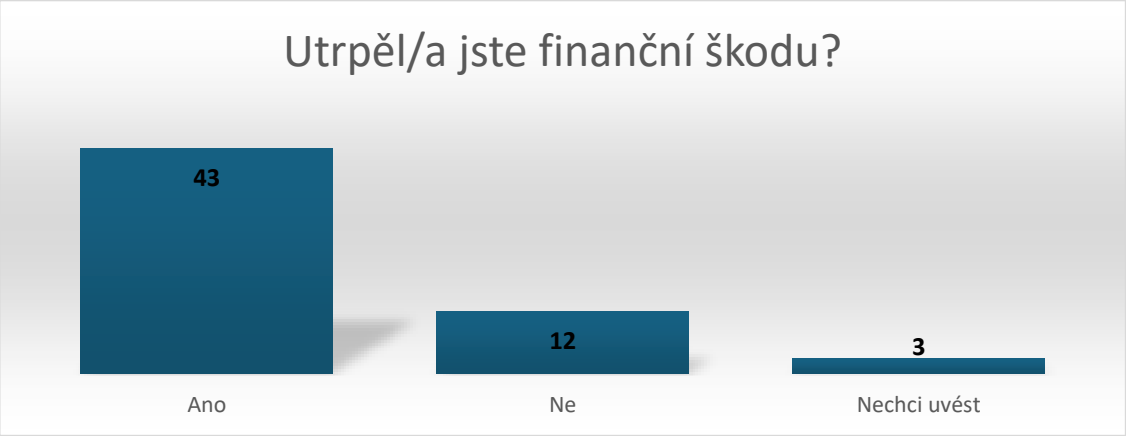
Nejčastěji respondenti uvedli, že k podvodu došlo prostřednictvím mobilního telefonu (29 respondentů; 44,8 %). Následovaly počítače nebo notebooky, které označilo 20 respondentů (25,9 %). Kategorie „jiné“ zahrnovala 6 respondentů (10,3 %), přičemž šlo například o chytré televize, herní zařízení nebo firemní systémy. Pouze 3 respondenti (5,2 %) uvedli tablet jako zařízení, přes které došlo k podvodnému jednání. Výsledky potvrzují, že mobilní telefon představuje nejrizikovější zařízení z hlediska kybernetických podvodů mezi dotázanými.

Graf č.7: **Jak jste se o podvodu dozvěděl/a?** [57]

[56] Vlastní zpracování
[57] Vlastní zpracování

Největší část respondentů (26 respondentů; 37,9 %) zjistila, že se stali obětí kybernetického podvodu, až zpětně – například při kontrole bankovního účtu nebo při vyúčtování. Okamžitě při samotném útoku si podvod uvědomilo 15 respondentů (32,8 %). Deset respondentů (17,2 %) bylo na podvod upozorněno ze strany banky nebo blízké osoby. Zbylých 7 respondentů (12,1 %) uvedlo jiný způsob, jak se o podvodu dozvěděli, např. při komunikaci s podvodníkem či během jiného technického zásahu. Výsledky ukazují, že značná část podvodů není odhalena v reálném čase, ale až s časovým odstupem.

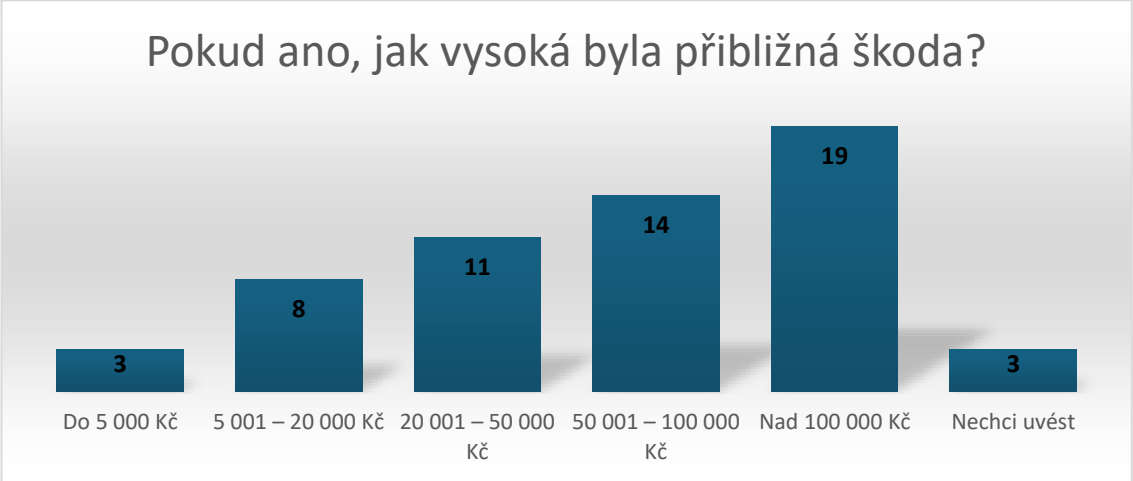
Graf č. 8: **Utrpěl/a jste finanční škodu?**[58]



Většina respondentů (43 respondentů; 53,4 %) uvedla, že v důsledku kybernetického podvodu skutečně utrpěla finanční škodu. Naopak 12 respondentů (29,3 %) ztrátu neutrpělo a 3 respondenti (17,2 %) nechtěli na tuto otázku odpovědět. Výsledky potvrzují, že více než polovina dotázaných měla s kybernetickými podvody přímou zkušenost s finančním dopadem, což podtrhuje závažnost tohoto fenoménu.

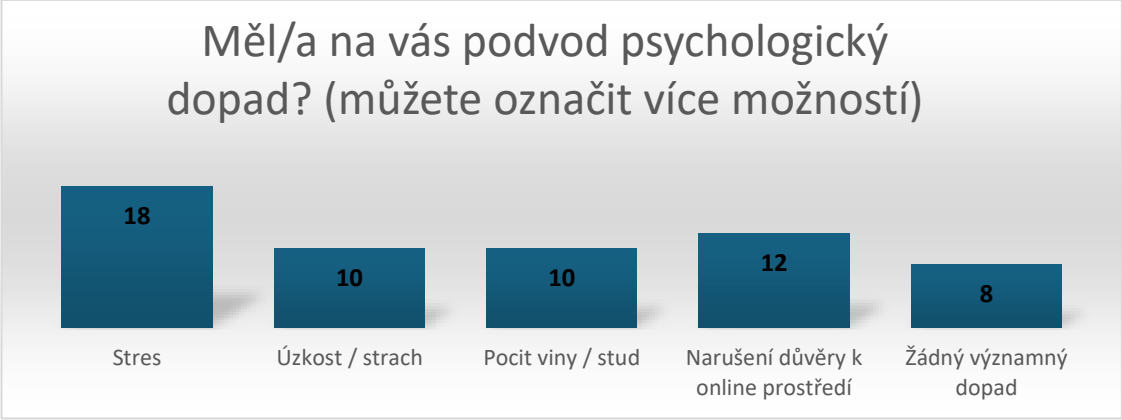
[58] Vlastní zpracování

Graf č. 9: **Pokud ano, jak vysoká byla přibližná škoda?** [59]



Nejčastěji respondenti uváděli škodu vyšší než 100 000 Kč (19 respondentů; 32,8 %), následovali ti, kteří odhadli škodu v rozmezí 50 001–100 000 Kč (14 respondentů; 24,1 %), a 20 001–50 000 Kč (11 respondentů; 18,6 %). Dále 8 respondentů (13,8 %) uvedlo škodu mezi 5 001–20 000 Kč, a pouze 3 osoby (5,2 %) zaznamenaly škodu do 5 000 Kč. Další 3 respondenti (5,2 %) výši škody neuvedli. Tyto výsledky ukazují, že v případech kybernetických podvodů často dochází k závažným finančním ztrátám.

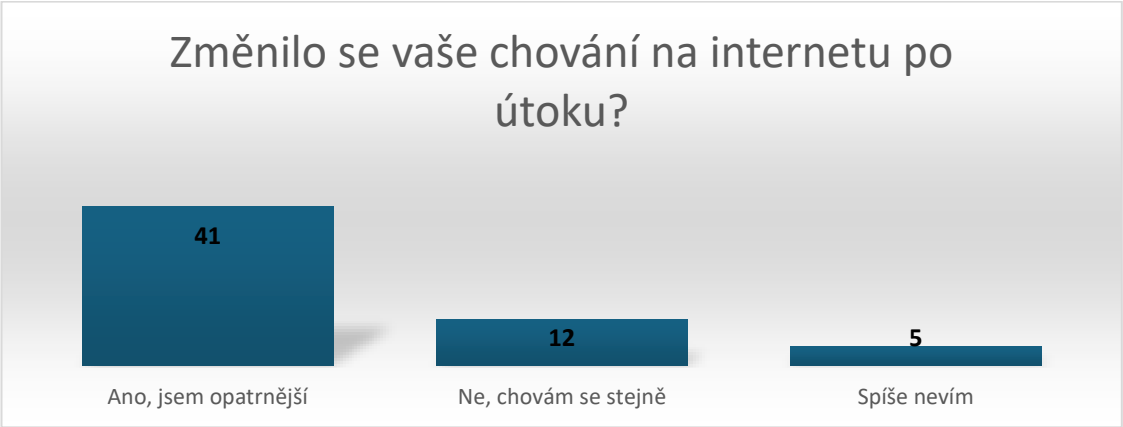
Graf č. 10: **Měl/a na vás podvod psychologický dopad?** *(můžete označit více možností)* [60]



Nejčastěji respondenti uváděli, že na ně měl podvod psychologický dopad ve formě stresu (18 respondentů; 31 %). Narušení důvěry k online prostředí zaznamenalo 12 respondentů (20,7 %). Shodně po 10 respondentech (17,2 %) uvedlo pocity úzkosti či strachu a také pocit viny nebo studu. Osm respondentů (13,8 %) označilo, že na ně podvod neměl žádný významný psychologický dopad. Výsledky potvrzují, že kromě finančních ztrát zanechávají kybernetické podvody u velké části obětí i výrazné psychologické následky.

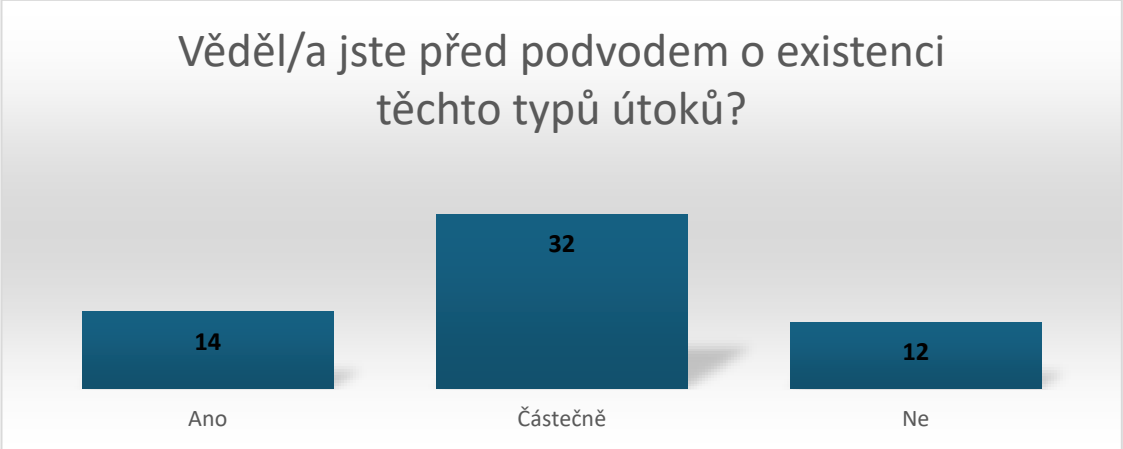
[59] Vlastní zpracování
[60] Vlastní zpracování

Graf č. 11: **Změnilo se vaše chování na internetu po útoku?** [61]



Většina respondentů (41 respondentů; 55,2 %) uvedla, že po kybernetickém útoku změnila své chování na internetu a stala se opatrnějšími. Dvanáct respondentů (31 %) uvedlo, že se jejich chování nezměnilo a nadále se online pohybují stejným způsobem jako dříve. Pět respondentů (13,8 %) odpovědělo, že si nejsou jisti, zda se jejich chování nějak změnilo. Výsledky naznačují, že většina dotázaných si je vědoma rizik a po negativní zkušenosti přistupuje k internetovému prostředí s větší obezřetností.

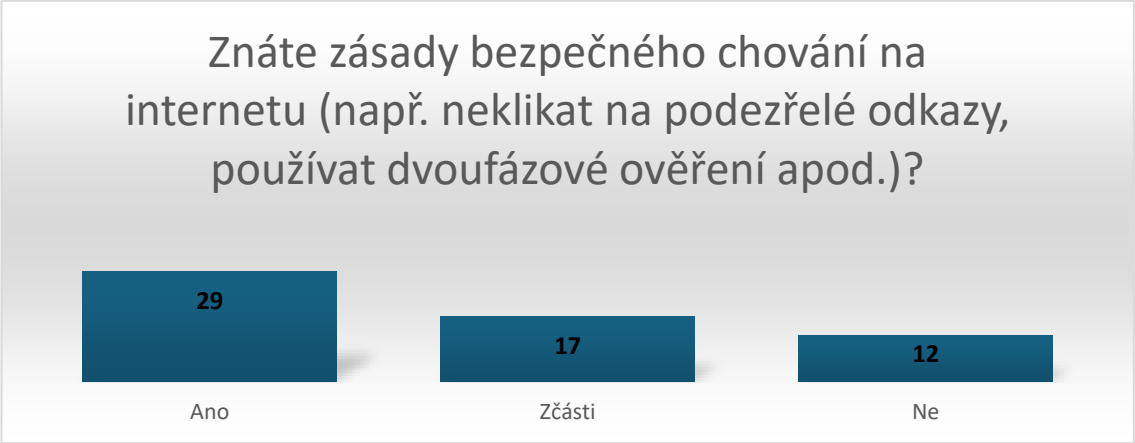
Graf č. 12: **Věděl/a jste před podvodem o existenci těchto typů útoků?** [62]



Více než polovina respondentů (32 respondentů; 55,2 %) uvedla, že o existenci daných typů kybernetických útoků měli pouze částečné povědomí. Čtrnáct respondentů (24,1 %) vědělo o těchto útocích již před tím, než se stali obětí. Naopak 12 respondentů (20,7 %) nemělo o existenci těchto forem podvodu žádné znalosti. Výsledky poukazují na to, že informovanost veřejnosti o konkrétních typech kybernetických hrozeb je často nedostatečná, což zvyšuje riziko úspěšnosti podvodných aktivit.

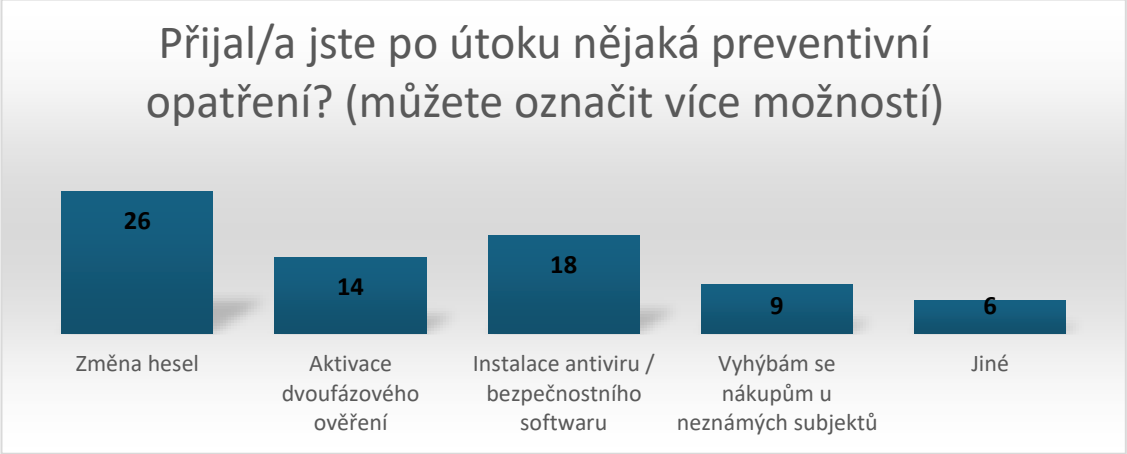
[61] Vlastní zpracování
[62] Vlastní zpracování

Graf č. 13: **Znáte zásady bezpečného chování na internetu (např. neklikat na podezřelé odkazy, používat dvoufázové ověření apod.)?** [63]



Polovina respondentů (29 respondentů; 50 %) uvedla, že znají zásady bezpečného chování na internetu, jako je například neklikat na podezřelé odkazy nebo využívání dvoufázového ověření. Dalších 17 respondentů (29,3 %) odpovědělo, že tyto zásady znají pouze částečně. Zbývajících 12 respondentů (20,7 %) přiznalo, že zásady bezpečného online chování vůbec neznají. Výsledky naznačují, že i přes rostoucí povědomí o kybernetické bezpečnosti je u části veřejnosti stále patrná informační mezera v oblasti preventivních opatření.

Graf: č. 14: **Přijal/a jste po útoku nějaká preventivní opatření?** *(můžete označit více možností)* [64]

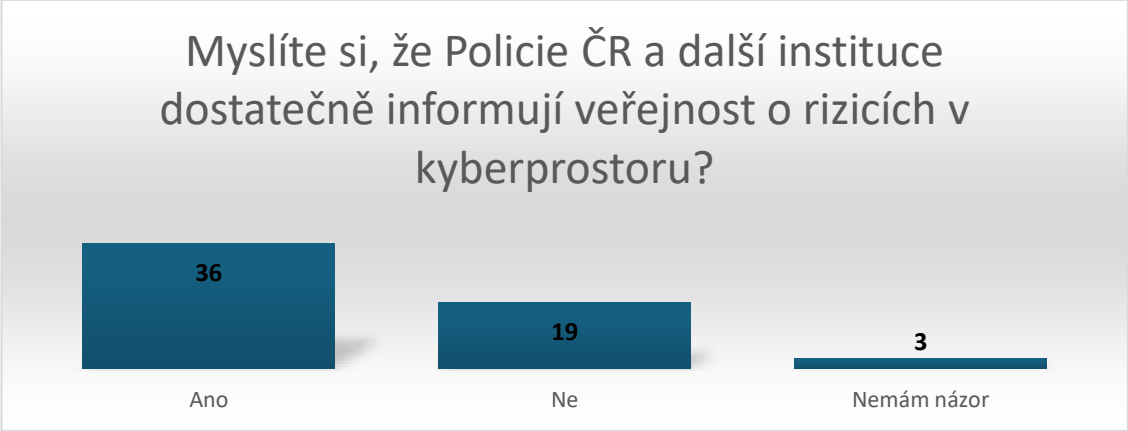


Nejčastěji respondenti po útoku provedli změnu hesel (26 respondentů; 35,6 %). Osmnáct respondentů (24,7 %) uvedlo, že si nainstalovali antivirový či bezpečnostní software, a 14 respondentů (19,2 %) aktivovalo dvoufázové ověření. Devět respondentů (12,3 %) se

[63] Vlastní zpracování
[64] Vlastní zpracování

začalo vyhýbat nákupům u neznámých subjektů a šest respondentů (8,2 %) zvolilo odpověď „jiné“, kde uváděli například zvýšenou obezřetnost při sdílení informací nebo omezení využívání online platebních metod. Výsledky ukazují, že značná část dotázaných se po negativní zkušenosti rozhodla pro aktivní změny ve svém online chování ve snaze předejít dalším incidentům.

Graf č. 15: **Myslíte si, že Policie ČR a další instituce dostatečně informují veřejnost o rizicích v kyberprostoru?** [65]



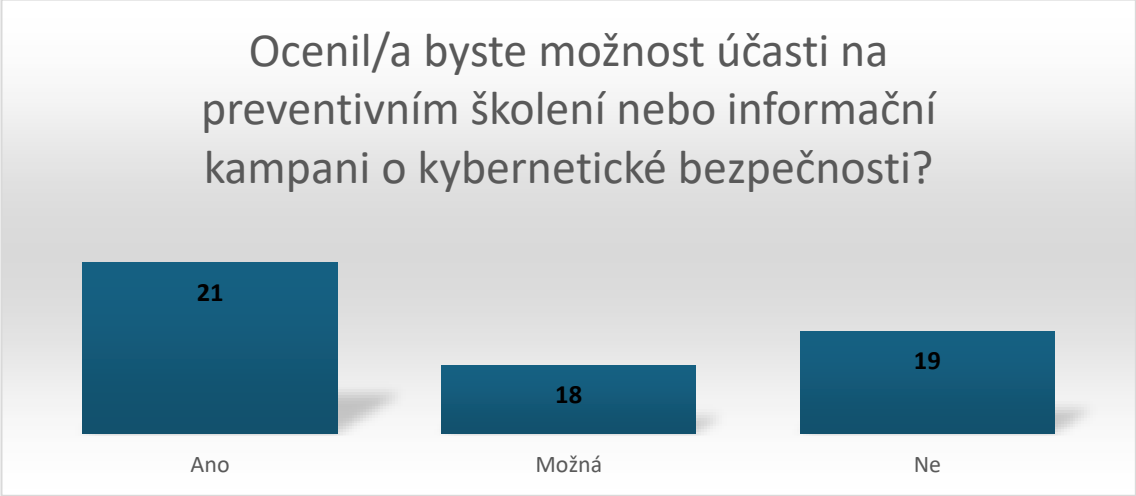
Mírná většina respondentů (36 osob; 55,4 %) se domnívá, že Policie ČR a další instituce dostatečně informují veřejnost o rizicích spojených s pohybem v kyberprostoru. Naopak 29,2 % respondentů (19 osob) považuje tuto informovanost za nedostatečnou a 4,6 % (3 osoby) uvedlo, že nemá na tuto otázku jasný názor. Výsledky ukazují, že přestože většina veřejnosti vnímá současnou informovanost jako dostačující, významná menšina ji stále považuje za nedostatečnou, což naznačuje prostor pro zlepšení v oblasti prevence a komunikace.

[65] Vlastní zpracování

Graf č. 16: **Kromě oznámení na Policii ČR – využil/a jste také jinou pomoc nebo podporu?** *(můžete označit více možností)* [66]

Více než polovina respondentů (29 respondentů; 50 %) uvedla, že po útoku již žádnou další pomoc nevyužila. Sedmnáct respondentů (29,3 %) kontaktovalo banku nebo jinou finanční instituci. Konzultaci s IT odborníkem vyhledali 4 respondenti (6,9 %), právní poradenství využili 3 respondenti (5,2 %) a pouze 2 respondenti (3,4 %) uvedli, že vyhledali psychologickou pomoc. Tři respondenti (5,2 %) označili možnost „jiné“, přičemž z odpovědí vyplývalo, že šlo například o pomoc od rodiny nebo blízkých známých. Data ukazují, že většina respondentů se spolehla především na vlastní řešení situace bez využití dalších odborných služeb.

Graf č. 17: **Ocenil/a byste možnost účasti na preventivním školení nebo informační kampani o kybernetické bezpečnosti?** [67]



[66] Vlastní zpracování
[67] Vlastní zpracování

Možnost účasti na preventivním školení nebo informační kampani o kybernetické bezpečnosti by ocenilo 21 respondentů (36,2 %). Osmnáct respondentů (31 %) uvedlo, že by takovou možnost zvažovali, a 19 respondentů (32,8 %) o školení zájem nemá. Výsledky ukazují, že téměř dvě třetiny respondentů by měly pozitivní nebo alespoň otevřený postoj k preventivnímu vzdělávání v oblasti kybernetické bezpečnosti, což svědčí o rostoucím zájmu o osvětu a zvýšení vlastního povědomí o hrozbách v online prostředí.

Graf č. 18: **Změnila se vaše důvěra v online prostředí po této zkušenosti?** [68]

U většiny respondentů došlo po negativní zkušenosti ke snížení důvěry v online prostředí. Nejčastěji respondenti uváděli, že se jejich důvěra spíše snížila (24 respondentů; 41,4 %) a dalších 13 respondentů (22,4 %) uvedlo, že se výrazně snížila. Naopak 21 respondentů (36,2 %) uvedlo, že jejich důvěra zůstala stejná. Z žádné z odpovědí nevyplývá, že by zkušenost vedla ke zvýšení důvěry. Výsledky naznačují, že kybernetické útoky významně ovlivňují vnímání bezpečnosti v digitálním prostoru, přičemž u většiny respondentů dochází k oslabení důvěry.

Graf č. 19: **Chcete k tématu něco dodat nebo sdílet svou zkušenost?** [69]

V rámci otevřené otázky se část respondentů rozhodla sdílet své zkušenosti nebo postřehy. Nejčastěji zmiňovali potřebu větší informovanosti ze strany institucí, ocenili by například školení nebo preventivní kampaň. Někteří respondenti popsali svou negativní zkušenost s útokem, která vedla ke ztrátě důvěry v online prostředí, nebo vyjádřili vděčnost za pomoc Policie ČR. Zároveň se ukázalo, že značná část respondentů otázku

[68] Vlastní zpracování
[69] Vlastní zpracování

ponechala bez odpovědi, což může odrážet buď neochotu sdílet osobní zážitek, nebo vyčerpání tématu během předchozích odpovědí.

5.3 Diskuze

Cílem praktické části bylo na základě dotazníkového šetření analyzovat zkušenosti obětí kybernetických podvodů a ověřit tři výzkumné hypotézy, které se týkaly jak samotné povahy útoků, tak jejich dopadu a informovanosti veřejnosti. Dotazník byl distribuován fyzicky na území okresu České Budějovice, konkrétně na několika obvodních odděleních Policie ČR. Výzkumný vzorek tvořilo 58 respondentů, kteří se stali oběťmi kybernetického podvodu, případně byli vystaveni pokusu o podvod. Získaná data umožnila podrobně vyhodnotit charakter útoků a reakce jednotlivců na tyto situace.

Hypotéza H1: *Nejčastějším typem kybernetických podvodů v České republice jsou phishingové útoky zaměřené na získání finančních prostředků.*

Hypotéza H1 byla na základě výsledků dotazníku potvrzena. Phishing, tedy útoky využívající falešné e-maily či zprávy s cílem vylákat přihlašovací údaje nebo osobní informace, byl označen jako nejčastější forma útoku. Tuto možnost zaškrtlo 15 respondentů, což představuje nejvyšší četnost napříč všemi kategoriemi útoků. Stejného počtu dosáhl také vishing, tedy telefonní útoky, přičemž tyto dva typy podvodů byly nejvíce zastoupené. Podstatné je, že oba způsoby útoků měly ve většině případů finanční motivaci. Respondenti uváděli ztráty v řádu desítek až stovek tisíc korun. Vysoká míra zastoupení těchto metod potvrzuje skutečnost, že phishing a vishing patří mezi hlavní hrozby v českém kyberprostoru.

Hypotéza H2: *Kybernetické podvody způsobují obětem nejen finanční ztráty, ale také závažné psychologické dopady, jako je stres a úzkost.*

Také druhá hypotéza byla potvrzena. Z výsledků vyplývá, že kybernetické podvody nezanechávají jen materiální škody, ale významně ovlivňují i psychickou stránku obětí. Nejčastěji respondenti uváděli stres (31 %) a narušení důvěry v online prostředí (21 %). Úzkost a pocity viny byly uváděny v dalších případech. Pouze 14 % respondentů označilo, že podvod na ně neměl žádný psychologický dopad. Někteří z postižených osob také uvedli, že byli nuceni vyhledat odbornou pomoc – například

kontaktovali IT specialistu nebo psychologa. Významná část dotázaných uvedla, že po útoku zcela změnila své chování na internetu, stali se opatrnějšími a více si ověřovali informace. To potvrzuje, že důsledky útoku mají dlouhodobý charakter, ať už z hlediska důvěry, bezpečnosti nebo celkového přístupu k technologiím.

Hypotéza H3: *Informovanost veřejnosti o rizicích kybernetických útoků a preventivních opatřeních je nedostatečná, což zvyšuje zranitelnost jednotlivců vůči těmto hrozbám.*

Tato hypotéza nebyla potvrzena. Výsledky dotazníkového šetření ukázaly, že 36 respondentů (55,4 %) vnímá informování ze strany Policie ČR a dalších institucí jako dostatečné. Naproti tomu 19 respondentů (32,8 %) považuje tuto informovanost za nedostatečnou a 3 osoby (5,2 %) nemají jasný názor. Přestože názorová převaha není výrazná, většina respondentů považuje úroveň informovanosti za uspokojivou. Navíc naprostá většina obětí po útoku uvedla, že sama přijala konkrétní preventivní opatření, jako je změna hesel či zavedení dvoufázového ověření.

Závěr

Bakalářská práce se zaměřila na problematiku kybernetických podvodů a jejich dopadů na občany. Hlavním cílem bylo analyzovat současnou situaci v této oblasti – zejména zmapovat nejčastější typy kybernetických útoků namířených proti uživatelům v České republice – a na základě zjištěných skutečností posoudit preventivní opatření ke snížení těchto rizik. K dosažení vytyčených cílů byla využita kombinace teoretické rešerše a empirického dotazníkového šetření, které dohromady poskytly komplexní pohled na fenomén kybernetických podvodů a jejich projevy v tuzemském prostředí.

Teoretická část práce se věnovala vymezení základních pojmů souvisejících s kybernetickou kriminalitou, přičemž důraz byl kladen na klasifikaci nejčastějších forem online podvodů, jako jsou phishing, vishing, malware nebo podvodné e-shopy. Popsán byl rovněž význam sociálního inženýrství a různé preventivní přístupy, které mají přispět ke zvýšení kybernetické gramotnosti. Teoretický rámec současně identifikoval řadu výzev v oblasti právního postihu pachatelů i ve sféře veřejné osvěty.

V praktické části byl realizován dotazníkový průzkum mezi 58 respondenty, kteří se stali obětí kybernetického podvodu nebo byli vystaveni jeho pokusu. Průzkum probíhal fyzicky v okrese České Budějovice prostřednictvím Policie ČR. Výsledky ukázaly, že nejčastějšími formami útoku byly phishing a vishing, tedy typické formy podvodů zaměřené na získání osobních nebo přístupových údajů. Tato zjištění potvrdila první hypotézu.

Z hlediska dopadů na oběti se potvrdilo, že většina respondentů utrpěla finanční škodu, často značného rozsahu. Psychologické následky byly rovněž přítomné – respondenti uváděli stres, narušení důvěry k online prostředí a změny v chování na internetu. Druhá hypotéza tak byla rovněž potvrzena. Pokud jde o informovanost veřejnosti, výsledky šetření ukázaly, že mírná většina respondentů (55,4 %) považuje komunikaci institucí – zejména Policie ČR – za dostatečnou. Třetí hypotéza, která předpokládala nízkou úroveň informovanosti veřejnosti, se tak nepotvrdila. Přesto však značná část respondentů uvedla opak, což poukazuje na existenci prostoru pro zlepšení v oblasti osvěty a prevence. Respondenti zároveň uváděli, že po útoku sami přistoupili k preventivním krokům, jako je změna hesel či zavedení dvoufázového ověřování.

Získaná data dále ukázala, že část respondentů by uvítala možnost účastnit se školení nebo informačních kampaní zaměřených na kybernetickou bezpečnost. Zároveň bylo zjištěno, že využívání dalších forem pomoci, například psychologického či právního poradenství, zůstává na nízké úrovni. To poukazuje na prostor pro rozvoj doprovodných služeb v oblasti podpory obětí.

Výsledky této práce tedy potvrzují význam praktického zkoumání kybernetických podvodů nejen z pohledu typologie útoků, ale i reálných důsledků pro jednotlivce. Přínos této práce spočívá zejména v propojení teoretického rámce s reálnými zkušenostmi obětí a v identifikaci konkrétních oblastí, které je třeba nadále rozvíjet – zejména v oblasti osvěty, prevence a institucionální podpory. Práce navíc aktualizuje poznatky o nejčastějších typech útoků a představuje výchozí bod pro navazující výzkumy.

Lze uzavřít, že práce naplnila stanovené výzkumné cíle, nabídla ověřený pohled na klíčové aspekty kybernetických podvodů a přinesla doporučení, která mohou přispět k účinnější ochraně veřejnosti. Vzhledem k neustálému technologickému vývoji a rostoucí míře digitalizace je nezbytné věnovat této problematice dlouhodobou odbornou pozornost a posilovat kompetence občanů i institucí v oblasti kybernetické bezpečnosti.

Seznam použitých zdrojů

Literární zdroje

1. AYCOCK, J. *Spyware and Adware. Springer*. Springer: 2011th edition, 2010, s. 160. ISBN 978-0387777405
2. ČÍRTKOVÁ, L. *Viktimologie pro forenzní praxi*. Praha: Portál, 2014. s. 160. ISBN 978-80-262-0582-1.
3. ČÍRTKOVÁ, L., VITOUŠOVÁ, P. *Pomoc obětem (a svědkům) trestných činů: příručka pro pomáhající profese*. Praha: Grada, 2007. s. 196. ISBN 978-80-247-2014-2.
4. GŘIVNA, T, POLČÁK R. *Kyberkriminalita a právo.* Praha: Auditorium, 2008, s. 220. ISBN 978-80-903786-7-4.
5. HOLCR, K, BUBELÍNI, J, FENYK, J. a kol. *Kriminológia*. Bratislava: Iura Edition, 2008. s. 403. ISBN 978-80-8078-206-1.
6. JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada, 2007. s. 284. ISBN 978-80-247-1561-2.
7. JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007. 284 s. ISBN 978-80-247-1561-2.
8. KLIMEK, L, ZÁHORA, J, a HOLCR, K, *Počítačová kriminalita v európskych súvislostiach*. Praha: Wolters Kluwer, 2016. s. 448. ISBN 978-80-8168-538-5.
9. KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC., s. 522. ISBN 978-80-88168-15-7.
10. KOŽÍŠEK, M. a PÍSECKÝ, V. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. s, 176. ISBN 978-80-247-5595-3.
11. KUCHTA, J, *Základy kriminologie a trestní politiky*. 3. vyd. Praha: C. H. Beck, 2019. s. 616. ISBN 978-80-7400-732-3.
12. MARTANOVÁ, V., B. JANÍKOVÁ, T. DANĚČKOVÁ, et al. *Učební texty ke specializačnímu studiu pro školní metodiky prevence*. Praha: Centrum adiktologie Psychiatrické kliniky 1. lékařské fakulty a VFN, Univerzita Karlova, 2007. s. 159. ISBN 978-80-254-0525-3.
13. MATĚJKA, M. *Počítačová kriminalita*. Praha: Computer Press, 2002. 120 s. ISBN 80-7226-419-2.

14. OSTERHOUDT, M. *Computer Health Made Easy V.2 - Beware of the "Wares" Adware, Malware and Spyware*. Lulu Press, Inc, 2013. s. 262. ISBN 978-1300054627.
15. PRŮCHA, J, WALTEROVÁ, E., MAREŠ, J. *Pedagogický slovník. 7.* aktualiz. vyd. Praha: Portál, 2008, 322 s. ISBN 978-80-7367-416-8.
16. PRŮCHA, J., WALTEROVÁ, E., MAREŠ, J. *Pedagogický slovník, 4. vydání*. Praha: Portál, 2021.s. 328. ISBN 80-7178-772-8.
17. SKLENÁK, V. *Data, informace, znalosti a Internet*. Praha, 2001, s. 507. ISBN 80-7179-409-0.
18. SMEJKAL, V. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015. s. 640. ISBN 978-80-7380-501-2.
19. SMEJKAL, V., SOKOL, T., VLČEK, M. *Počítačové právo*. Praha: C.H. Beck Beckova edice právo a hospodářství., 1995. s. 264. ISBN 80-7179-009-5.
20. THOMAS, F. *Adware: The Only Book You'll Ever Need.* Lulu Press, Inc, 2015. s. 49. ISBN 978-1329160330.
21. VELIKOVSKÁ, M. *Psychologie obětí trestných činů*. Praha: Grada Publishing, 2016. 168 s. ISBN 978-80-247-4849-8.

Elektronické zdroje

1. DVOŘÁK, M. *Phishing, pharming a jejich trestněprávní postih.* Trestněprávní revue. 2018, č. 4, s. 84–89. [online]. [cit.2025-02-05]. Dostupné z WWW: https://portaro.mfcr.cz/#!/records/72f56d42-7604-4ea0-956a-5dd7c6e35917
2. HODÁČKOVÁ, V. *Tvoje cesta* [online]. © 2023 Policie ČR [cit. 2025-03-19]. Dostupné z WWW: https://www.policie.cz/clanek/tvoje-cesta.aspx
3. JIRÁSEK, P., NOVÁK, L., POŽÁR J. *Výkladový slovník kybernetické bezpečnosti.* [online]. 2. aktualiz. vyd. Praha: AFCEA, © 2015, s. 59. Dostupný z WWW: https://afcea.cz/cesky-slovnik-pojmu-kyberneticke-bezpecnosti/
4. JONES, C. *Phishing, Vishing, SMiShing, Whaling And Pharming: How To Stop Social Engineering Attacks* [online]. [cit.2025-02-05]. Dostupné z WWW: https://expertinsights.com/insights/phishing-vishing smishing-whaling-and-pharming-how-to-stop-social-engineering-attacks/
5. KAMIL, K., SZOTKOWSKI, R., KUBALA. L. *Bezpečné chování na internetu pro kluky a pro holky – náměty na výukové aktivity* [online]. [cit. 2025-03-16].

Dostupné z WWW: https://www.e-bezpeci.cz/index.php/ke-stazeni/tiskoviny/159-bezpecne-chovani-na-internetu-pro-kluky-a-pro-holky-2022/file , s.35.

6. *Národní úřad pro kybernetickou a informační bezpečnost: Kurz Bezpečně v kyber! se otevírá veřejnosti* Vládní CERT [online]. Brno, © 2021 [cit. 2025-29-03]. Dostupné z WWW: https://nukib.gov.cz/cs/infoservis/aktuality/1691-kurz-bezpecne-v-kyber-se-otvira-verejnosti/
7. *Národní úřad pro kybernetickou a informační bezpečnost: Kybernetické incidenty pohledem NÚKIB - březen 2023* Vládní CERT [online]. Brno, © 2023 [cit. 2025-03-29]. Dostupné z WWW: https://nukib.gov.cz/cs/infoservis/aktuality/1954-kyberneticke-incidenty-pohledem-nukib-brezen-2023/
8. NGSS. *Zločiny v době moderních technologií: Jak řeší české právo kybernetickou kriminalitu a jak se proti ní bránit?* [online]. [cit.2025-01-11]. Dostupné z WWW: https://www.ngss.cz/clanek/zlociny-v-dobe-modernich-technologii-jak-resi-ceske-pravo-kybernetickou-kriminalitu-a-jak-se-proti-ni-branit-2023-05-16
9. Phishing Stats You Should Know In 2022. Expert Insights [online]. [cit.2025-02-05]. Dostupné z WWW: https://expertinsights.com/insights/50-phishing-stats-you-should-know/
10. PREVENCE KRIMINALITY. *Bezpečně v kyberprostoru* [online]. © 2018 [cit. 2025-03-19]. Dostupné z WWW: https://prevencekriminality.cz/bezpecne-v-kyberprostoru/.
11. PREVENCE KRIMINALITY. *Internetem bezpečně* [online]. © 2018 [cit. 2025-03-19]. Dostupné z WWW: https://prevencekriminality.cz/internetem-bezpecne/
12. PREVENCE KRIMINALITY. *Programy primární prevence „Kyberbezpečí“ a „Děti v síti“* [online]. © 2018 [cit. 2025-03-19]. Dostupné z WWW: https://prevencekriminality.cz/programy-primarni-prevence-kyberbezpeci-a-deti-v-siti/
13. VÁCLAVÍK, L. *Většina internetu je skrytá. Co jsou to deep a dark web?* [online]. [cit.2025-01-11]. Dostupné z WWW: https://www.cnews.cz/clanky/co-je-to-deep-invisible-hluboky-dark-temny-web/

Legislativní dokumenty

1. 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

2. ČESKO. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In *Sbírka zákonů, Česká republika.* 2009, částka 11, s. 354

Seznam zkratek

1. **IT** –Informační technologie
2. **ICT** –Informační a komunikační technologie
3. **IP** –Internet Protocol
4. **ISP** –Internet Service Provider (poskytovatel internetového připojení)
5. **DoS** – Denial of Service (útok odepřením služby)
6. **DdoS** – Distributed Denial of Service (distribuovaný útok odepřením služby)
7. **NÚKIB**– Národní úřad pro kybernetickou a informační bezpečnost
8. **NCKB** –Národní centrum kybernetické bezpečnosti
9. **CERT** –Computer Emergency Response Team
10. **Phishing** – Podvodná technika zaměřená na získání citlivých údajů prostřednictvím e-mailu
11. **Smishing** –Phishing prostřednictvím SMS zpráv
12. **Vishing** –Phishing prostřednictvím telefonních hovorů
13. **Malware** – Škodlivý software
14. **Spyware** –Špionážní software sledující aktivitu uživatele
15. **Adware** –Software zobrazující nevyžádanou reklamu
16. **Ransomware** – Malware, který šifruje data a požaduje výkupné
17. **Keylogger** – Software zaznamenávající stisky kláves
18. **DNS** – Domain Name System

Seznam tabulek a grafů

Seznam příloh

Přílohy

DOTAZNÍK PRO OBĚTI KYBERNETICKÝCH PODVODŮ
Vážená paní / Vážený pane,

tento anonymní dotazník je součástí bakalářské práce studenta Vysoké školy evropských a regionálních studií. Dotazník je určen obětem kybernetických podvodů a slouží ke zjištění typů útoků, jejich dopadů a informovanosti občanů o kybernetické bezpečnosti. Vyplnění dotazníku trvá přibližně 5–10 minut. Děkujeme za vaši spolupráci.

---

1. **Pohlaví:**
   ☐ Muž
   ☐ Žena
   ☐ Nechci uvést

2. **Věk:**
   ☐ do 18 let
   ☐ 19–30 let
   ☐ 31–45 let
   ☐ 46–60 let
   ☐ Nad 60 let

3. **Nejvyšší dosažené vzdělání:**
   ☐ Základní
   ☐ Středoškolské bez maturity
   ☐ Středoškolské s maturitou
   ☐ Vysokoškolské
   ☐ Jiné

4. **Stal/a jste se obětí kybernetického podvodu:**
   ☐ Jednou
   ☐ Vícekrát
   ☐ Nevím přesně

5. **K jakému typu podvodu došlo?** *(můžete označit více možností)*
   ☐ Phishing (falešné e-maily, zprávy)
   ☐ Podvodný e-shop
   ☐ Internetová inzerce (např. Bazoš, Facebook Marketplace)
   ☐ Vishing (telefonát od falešného pracovníka banky aj.)
   ☐ Smishing (podvodná SMS zpráva)
   ☐ Útok přes sociální sítě
   ☐ Jiné: _____

6. **Na jakém zařízení k podvodu došlo?**
   ☐ Mobilní telefon
   ☐ Počítač / notebook

☐ Tablet

☐ Jiné: _____

7. **Jak jste se o podvodu dozvěděl/a?**
   ☐ Okamžitě při útoku
   ☐ Až zpětně (např. kontrolou účtu)
   ☐ Upozorněním banky / blízké osoby
   ☐ Jinak: _____
8. **Utrpěl/a jste finanční škodu?**
   ☐ Ano
   ☐ Ne
   ☐ Nechci uvést
9. **Pokud ano, jak vysoká byla přibližná škoda?**
   ☐ Do 5 000 Kč
   ☐ 5 001 – 20 000 Kč
   ☐ 20 001 – 50 000 Kč
   ☐ 50 001 – 100 000 Kč
   ☐ Nad 100 000 Kč
   ☐ Nechci uvést
10. **Měl/a na vás podvod psychologický dopad?** *(můžete označit více možností)*
    ☐ Stres
    ☐ Úzkost / strach
    ☐ Pocit viny / stud
    ☐ Narušení důvěry k online prostředí
    ☐ Žádný významný dopad
    ☐ Jiné: _____
11. **Změnilo se vaše chování na internetu po útoku?**
    ☐ Ano, jsem opatrnější
    ☐ Ne, chovám se stejně
    ☐ Spíše nevím
12. **Věděl/a jste před podvodem o existenci těchto typů útoků?**
    ☐ Ano
    ☐ Částečně
    ☐ Ne
13. **Znáte zásady bezpečného chování na internetu (např. neklikat na podezřelé odkazy, používat dvoufázové ověření apod.)?**
    ☐ Ano
    ☐ Zčásti
    ☐ Ne

14. **Přijal/a jste po útoku nějaká preventivní opatření?** *(můžete označit více možností)*
    - ☐ Změna hesel
    - ☐ Aktivace dvoufázového ověření
    - ☐ Instalace antiviru / bezpečnostního softwaru
    - ☐ Vyhýbám se nákupům u neznámých subjektů
    - ☐ Jiné: _____

15. **Myslíte si, že Policie ČR a další instituce dostatečně informují veřejnost o rizicích v kyberprostoru?**
    - ☐ Ano
    - ☐ Ne
    - ☐ Nemám názor

16. **Kromě oznámení na Policii ČR – využil/a jste také jinou pomoc nebo podporu?** *(můžete označit více možností)*
    - ☐ Konzultace s IT odborníkem
    - ☐ Právní poradenství
    - ☐ Psychologická pomoc
    - ☐ Kontaktoval/a jsem banku nebo jinou finanční instituci
    - ☐ Nevyužil/a jsem žádnou další pomoc
    - ☐ Jiná možnost: _____

17. **Ocenil/a byste možnost účasti na preventivním školení nebo informační kampani o kybernetické bezpečnosti?**
    - ☐ Ano
    - ☐ Možná
    - ☐ Ne

18. **Změnila se vaše důvěra v online prostředí po této zkušenosti?**
    - ☐ Výrazně se snížila
    - ☐ Spíše se snížila
    - ☐ Zůstala stejná
    - ☐ Spíše se zvýšila
    - ☐ Výrazně se zvýšila

19. **Chcete k tématu něco dodat nebo sdílet svou zkušenost?**
    (volitelná otevřená otázka)