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

BAKALÁŘSKÁ PRÁCE

PHISHINGOVÉ ÚTOKY: ANALÝZA METOD, PREVENCE A EFEKTIVNÍ OBRANA

Autor práce: Jiří Šrek, DiS.

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: Jiří Šrek, DiS.

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

Název bakalářské práce: Phishingové útoky: Analýza metod, prevence a efektivní obrana

Název bakalářské práce v anglickém jazyce: Phishing Attacks: Analysis of Methods, Prevention, and Effective Defense

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

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

Cíl bakalářské práce:
Cílem bakalářské práce je zhodnotit různé techniky phishingových útoků, identifikovat jejich dopady na uživatele a navrhnout preventivní opatření a strategie efektivní obrany pro minimalizaci rizika těchto útoků.

Student: Jiří Šrek, DiS.	27.11.2024 *datum*	 *podpis*
Vedoucí práce: RNDr. Růžena Ferebauerová	27.11.2024 *datum*	 *podpis*

Schvaluji zadání bakalářské práce:

Vedoucí katedry: doc. JUDr. Roman Svatoš, Ph.D.	12.12.2024 *datum*	 *podpis*
Prorektor pro studium a vnitřní záležitosti: doc. PhDr. Miroslav Sapík, Ph.D.	11.12.2024 *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

Šrek, J. Phishingové útoky: Analýza metod, prevence a efektivní obrana*: bakalářská práce.* České Budějovice: Vysoká škola evropských a regionálních studií, 2025. *79* s. Vedoucí bakalářské práce: RNDr. Růžena Ferebauerová.

Klíčová slova: phishing, kybernetické útoky, bezpečnost, internet, obrana

Bakalářské práce se zabývá problematikou podvodných aktivit, konkrétně s phishingem na internetu. Teoretická část se věnuje vysvětlení klíčových pojmů, rozlišení jednotlivých typů phishingových útoků a popisu jejich způsobů provedení. Dále se zaměřuje na možná preventivní opatření proti těmto útokům. Praktická část práce obsahuje kvantitativní průzkum realizovaný prostřednictvím dotazníku, přičemž zahrnuje formulaci hypotéz, které jsou následně ověřovány na základě získaných dat. Cílem této části je zjistit míru informovanosti veřejnosti, jejich osobní zkušenosti s phishingem a postoje k této problematice, dále jsou zde zakomponovány doporučení a návrhy obraných strategií vůči phishingu včetně jednoho modelového případu obrany proti phishingu.

ABSTRACT

Šrek, J. *Phishing Attacks: Analysis of Methods, Prevention, and Effective Defense: Bachelor Thesis.* České Budějovice: The College of European and Regional Studies, 2025. *79* pgs. Supervisor: RNDr. Růžena Ferebauerová.

Key words phishing, cyber attacks, security, internet, defense

The bachelor's thesis deals with the issue of fraudulent activities, specifically phishing on the internet. The theoretical part explains key concepts, distinguishes different types of phishing attacks, and describes their execution methods. It also focuses on possible preventive measures, against such attacks. The practical part of the thesis includes a quantitative survey conducted through a uestionnaire, involving the formulation of hypotheses that are subsequently tested based on the collected data. The aim of this section is to determine the level of public awareness, their personal experiences with phishing, and their attitudes toward this issue, additionally, recommendations and suggestions for defense strategies against phishing are included, along with a case study of defending against phishing.

Obsah

Úvod

Kybernetické útoky jsou jedním z největších bezpečnostních rizik současné digitální éry. Phishing, jako jedna z nejrozšířenějších forem kybernetických útoků, ohrožuje jednotlivce, firmy i organizace po celém světě. Tento typ útoku využívá sociálního inženýrství, tedy manipulace lidí, k získání citlivých údajů, jako jsou přihlašovací údaje, platební informace nebo osobní data.

Phishingové útoky se stávají stále sofistikovanějšími, což komplikuje jejich detekci a snižuje schopnost běžných uživatelů je rozeznat. V posledních letech je jejich aktuálnost umocněna rozvojem technologií, větší digitalizací a specifickými situacemi, jako byla pandemie COVID-19, kterou útočníci často zneužívali k cíleným útokům.

Důsledky phishingových útoků mohou být vážné – od ztráty finančních prostředků až po únik citlivých informací či narušení integrity systémů. Prevence a vzdělávání uživatelů představují klíčové nástroje, jak těmto útokům čelit. Přestože existují technologická řešení, jako jsou antivirové programy nebo spamové filtry, lidský faktor zůstává rozhodujícím prvkem při identifikaci a odhalení phishingových pokusů.

Problematika phishingu mě zaujala nejen svou aktuálností, ale také širokým dopadem na jednotlivce i organizace. Mým cílem je přispět k hlubšímu porozumění této problematiky a upozornit na klíčovou roli prevence. Phishingové útoky jsem osobně zaznamenal například ve formě podvodných e-mailů a sociálních sítí, což mě motivovalo k hlubšímu zkoumání tohoto fenoménu.

1 Cíl a metodika bakalářské práce

První kapitola této bakalářské práce se zaměřuje na stanovení cílů a použitou metodiku. Hlavním cílem bakalářské práce je zhodnotit různé techniky phishingových útoků, identifikovat jejich dopady na uživatele a navrhnout preventivní opatření a strategie efektivní obrany pro minimalizaci rizika těchto útoků.

Bakalářská práce se v teoretické části bude zabývat analýzou nejrozšířenějších typů phishingových útoků, včetně vymezení základních pojmů, a následně rozebere možnosti prevence a kybernetické bezpečnosti. V praktické části bude provedeno dotazníkové šetření mezi širokou veřejností prostřednictvím internetového prostředí na téma povědomí o phishingových útocích, bezpečnosti, znalostech a vnímání potenciálních hrozeb. Výsledky mohou poskytnout cenné informace o tom, jak nejlépe připravit jednotlivce na phishingový útok, který je směřován na jeho osobu, aby ho byl schopen včas odhalit a následně mu předejít. Poté dojde k vyhodnocení získaných dat za účelem doporučení do praxe.

Dotazník byl vytvořen s ohledem na tři stanovené hypotézy:

- **Hypotéza č.1:** Většina respondentů se v minulosti setkala s phishingovým útokem.
- **Hypotéza č.2**: V rámci phishingového útoku bude nejvyšší četnost provedení prostřednictvím e-mailové adresy.
- **Hypotéza č.**3: Mezi respondenty bude převaha těch, kteří si nekontrolují, od koho obdrželi emailovou zprávu.

Po ukončení dotazníkového šetření dojde ke grafickému zpracování pro lepší přehlednost a usnadnění interpretace výsledků a na základě nich dojde k vyhodnocení stanovených hypotéz.

Na závěr praktické části budou shrnuty doporučení a návrhy obranných strategií proti phishingu, na základě těchto doporučení bude vypracován modelový příklad jako praktická ukázka obrany.

2 Základní pojmy

2.1 Internet

Internet, což je zkratka pro „propojené sítě“ (interconnected networks), představuje globální systém, který propojuje uživatele různých zařízení do jednoho komplexního celku. Tento jedinečný projekt z minulého století zásadně změnil podobu elektronické komunikace. Internet si lze představit jako rozsáhlou pavučinu, kde jednotlivá vlákna tvoří spojení mezi uživateli, kteří jsou pomyslnými uzly této sítě.

Jedna z běžných definic internetu říká, že jde o propojenou síť počítačů, která umožňuje sdílení, komunikaci a přístup k informacím napříč celým kyberprostorem.[1]

Podle výkladového slovníku kybernetické bezpečnosti je internet definován jako "síť sítí, která se skládá z milionů soukromých, veřejných, akademických, obchodních a vládních sítí, s místním až globálním rozsahem, které jsou propojeny širokou škálou elektronických, bezdrátových a optických síťových technologií."[2]

Dle Lápáčka je internet: “Cosi, kam když připojíte svůj počítač, stanou se pro něj a tedy i pro Vás dostupnými úplně všechny počítače připojené jako ten váš. Můžete tedy například vést debatu s lidmi po celém světě – a vůbec není důležité, kde zrovna jsou, jaký mají počítač a jestli je u nich zrovna den nebo noc.“[3]

2.1.1 Historie Internetu

Devadesátá léta byla pro Českou republiku obdobím, kdy došlo k revolučnímu rozvoji internetu a počítačových sítí, které přinesly novou dynamiku. První významnou počítačovou sítí byla FidoNet, která vznikla kolem roku 1989. Tato síť byla čistě amatérská, nesloužila k obchodním účelům a nebyla podporována vládou.

Největší rozmach FidoNetu nastal mezi lety 1993 a 1996, kdy se lidé mohli připojit přes telefonní linku. Počítačové sítě přišly do Československa zároveň s přechodem k demokracii a začátkem zapojování země do globální infrastruktury. V roce 1990 byl v Praze díky podpoře nadace z USA spuštěn uzel pro síť EARN (European

[1] *Co je internet*. [online]. Správa sítě. 2022 [cit. 2025-01-12]. Dostupné z WWW: <https://www.sprava-site.eu/internet/.>
[2] JIRÁSEK, P., NOVÁK, L., a POŽÁR, J., *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Praha: Policejní akademie ČR v Praze, 2015, s. 49.
[3] LAPÁČEK, J. *Poznáváme Internet: rychle hotovo!.* Brno: Computer Press, 2007, s. 5.

Academic and Research Network), který byl evropskou částí sítě BITNET. O rok později došlo k posílení mezinárodního připojení, kdy byla přístupová trasa rozdělená na dvě nezávislé části – jedna zůstala pro síť EARN a druhá byla využita pro experimentování s internetem.[4]

2.2 Kybernetický prostor

Kyberprostor lze popsat jako virtuální prostředí vytvořené na základě lidské představivosti, kde se odehrávají různé propojené aktivity mezi počítačovými systémy.[5]

Nejlepší způsob, jak definovat kyberprostor, je jako virtuální a dynamický prostor vytvořený "klony" strojů.

Podle definice kyberprostoru jde o síť, která se skládá ze spotřebitelských počítačů, elektroniky a komunikačních sítí, prostřednictvím kterých je uživatel propojen se světem.

Kyberprostor se primárně vztahuje k počítačům, které tvoří virtuální síť a jsou elektronicky navrženy tak, aby umožňovaly online komunikaci. Tímto způsobem umožňují snadnou a dostupnou komunikaci po celém světě. Celý kyberprostor je tvořen velkými počítačovými sítěmi, které zahrnují mnoho podsítí.[6]

Co se týče právní definice kyberprostoru, lze vycházet například z § 2 písmena a) zákona číslo 181/2014 Sb. zákon o kybernetické bezpečnosti, kde je stanoveno, že „kybernetickým prostorem je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“[7]

[4] SATRAPA, P., *Deset let CESNETu*. [online]. Zpravodaj ÚVT MU. 2006. [cit. 2025-03-05]. Dostupné z WWW: <https://webserver.ics.muni.cz/zpravodaj/articles/517.html.>
[5] WALL, D. S. *Cybercrime. The Transformation of Crime in the Information Age*. Cambridge; Malden MA: Polity Press, 2007, s. 221.
[6] TIWARI, D., *Cyberspace and its Meaning*. [online]. Vendatu. 2025 [cit. 2025-01-15]. Dostupné z WWW: <https://www.vedantu.com/commerce/introduction-to-cyberspace.>
[7] *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů*. [online].. Zákony pro lidi. 2025 [cit. 2025-01-18]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2014-181?text=z%C3%A1kon+o+kybernetick%C3%A9+bezpe%C4%8Dnosti.>

2.3 Kybernetický útok

Kybernetický útok je jakýkoli záměrný pokus o krádež, zveřejnění, úpravu, deaktivaci nebo zničení dat, aplikací či jiných prostředků prostřednictvím neoprávněného přístupu k síti, počítačovému systému nebo digitálnímu zařízení.

Útočníci zahajují kybernetické útoky z různých důvodů, od drobných krádeží až po válečné operace. K dosažení svého cíle využívají různé metody, například útoky škodlivým softwarem, podvody založené na sociálním inženýrství nebo krádež hesel.[8]

Kybernetický útok lze také definovat jako jakoukoli nelegální aktivitu v kyberprostoru namířenou proti zájmům jiné osoby. Ne vždy se musí jednat o trestný čin, ale podstatné je, že takové jednání narušuje běžný chod života oběti. Tyto útoky využívají různé techniky a metody, jako je malware nebo phishing.[9]

Rostoucí závislost na informačních a komunikačních technologiích zvyšuje zranitelnost státu, společnosti i jednotlivců vůči kybernetickým útokům. Tyto útoky mohou sloužit jako nový nástroj vedení války, mít kriminální nebo teroristické motivy a být využity k destabilizaci společnosti. Únik strategicky důležitých informací, narušení informačních systémů státních institucí či klíčových podniků a organizací, které zajišťují základní funkce státu, může ohrozit strategické zájmy České republiky.[10]

2.4 Sociální sítě

Termín „sociální síť“ poprvé definoval sociolog J. A. Barnes v roce 1954. Původně šlo o čistě sociologický koncept popisující struktury propojené na základě přátelství, společných zájmů, náboženství, etnické příslušnosti nebo jiných faktorů. S rozvojem informačních technologií získaly sociální sítě nový, digitální rozměr. V kontextu webu 2.0 označuje tento pojem jakýkoli systém umožňující vytváření a správu propojených kontaktů. Internetové sociální sítě tak přenášejí mezilidské vztahy do online prostředí. Podle Pavlíčka do této kategorie spadají i platformy, kde navazování kontaktů není hlavní funkcí, ale pouze jednou z možností, které nabízejí.[11]

---

[8] IBM. *What is a cyberattack?* [online]. IBM. 2024 [cit. 2025-02-03]. Dostupné z WWW: <https://www.ibm.com/think/topics/cyber-attack.>

[9] KOLOUCH, J., BAŠTA, P. *Cybersecurity*. Praha:CZ.NIC, z.s.p.o., 2016. s. 78–79.

[10] SMEJKAL, V., a RAIS, K., *Řízení rizik ve firmách a jiných organizacích*. 4.vyd. Praha: Grada Publishing, 2013, s. 450 - 452

[11] PAVLÍČEK, A., *Nová média a sociální sítě.* Praha: Oeconomica, 2010, s. 126.

Jirásek a kolektiv říká, že sociální sítě jsou: „Propojená skupina lidí, kteří se navzájem ovlivňují. Tvoří se na základě zájmů, rodinných vazeb nebo z jiných důvodů. Tento pojem se dnes také často používá ve spojení s internetem a nástupem webů, které se na vytváření sociálních sítí přímo zaměřují (Facebook, Lidé.cz apod.), sociální sítě se mohou vytvářet také v zájmových komunitách kolem určitých webů, například na jejich fórech.“[12]

Dle Koloucha jsou sociální sítě "druh služby, která umožňuje uživatelům komunikovat, sdílet data a informace (více či méně trvalým způsobem) a provádět další aktivity.“[13]

Sociální sítě nejsou statické produkty, ale neustále se vyvíjející systémy, které se přizpůsobují nejen požadavkům uživatelů a záměrům jejich provozovatelů, ale také reakcím na konkurenční platformy.[14]

2.4.1 Facebook

Facebook je jedna z největších sociálních sítí na světě, která lidem umožňuje komunikovat, sdílet obsah a budovat online vztahy. Vznikl v roce 2004 díky Marku Zuckerbergovi a jeho spolužákům z Harvardu. Původně byl určen jen pro studenty této univerzity, ale brzy se otevřel veřejnosti a stal se globálním fenoménem.

Dnes má Facebook miliardy uživatelů po celém světě a podporuje desítky jazyků. Lidé na něm mohou vytvářet profily, přidávat si přátele, sdílet příspěvky, fotografie a videa, posílat zprávy a zapojovat se do skupin nebo událostí. Firmy a organizace ho využívají k propagaci svých produktů a služeb prostřednictvím speciálních stránek. [15]

2.4.2 Instagram

Instagram je populární sociální síť a mobilní aplikace, která slouží ke sdílení fotografií a videí. Uživatelé si zde mohou vytvářet profily, nahrávat svůj obsah, upravovat jej pomocí různých filtrů a efektů a následně sdílet s ostatními. Kromě klasických

[12] JIRÁSEK, P., NOVÁK, L., a POŽÁR, J., Výkladový slovník kybernetické bezpečnosti: Cyber security glossary, 2015, s. 177.
[13] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, z.s.p.o., 2016, s. 151.
[14] DIJCK, J., The culture of connectivity: a critical history of social media. New York: Oxford University Press, 2013, s. 7.
[15] Vše o Facebooku: Kompletní průvodce pro začátečníky i profíky. [online]. NeuroRestart. 2023. [cit. 2025-03-05]. Dostupné z WWW: <https://neurorestart.cz/socialni-site/vse-o-facebooku-kompletni-pruvodce-pro-zacatecniky-i-profiky/.>

příspěvků umožňuje Instagram i přidávání popisků, hashtagů a označování dalších uživatelů.

Aplikace byla spuštěna v roce 2010 a původně byla dostupná pouze pro iPhone, ale postupně se rozšířila i na zařízení s operačními systémy Android a Windows. Mezi hlavní funkce Instagramu patří krátkodobé „příběhy“ (Stories), které zmizí po 24 hodinách, krátká videa „Reels“ podobná obsahu na TikToku, platforma IGTV pro delší videa a také soukromé zprávy mezi uživateli.[16]

Instagram je dostupný nejen jako mobilní aplikace, ale i přes webový prohlížeč. Díky své popularitě je často využíván nejen jednotlivci, ale i firmami a influencery k propagaci produktů a služeb.[17]

2.4.3 Youtube

YouTube je největší internetová platforma pro sdílení videí, která byla spuštěna v únoru 2005. Původně sloužila jako platforma pro sdílení videí, ale rychle se vyvinula v mnohem více. Dnes má více než 2,5 miliardy aktivních uživatelů měsíčně a slouží jako mocný nástroj pro vzdělávání, zábavu i komerční aktivity.[18]

YouTube neustále rozšiřuje své služby a funkce. V posledních letech se stal dominantní platformou nejen pro tradiční videa, ale také pro podcasty, které měsíčně sleduje více než miliarda uživatelů. Díky své široké nabídce obsahu a funkcí, jako jsou živé přenosy, YouTube Shorts či YouTube Music, si platforma udržuje svou vedoucí pozici v oblasti online videí.[19]

V listopadu 2006 byl YouTube zakoupen společností Google za 1,65 miliardy dolarů a od té doby funguje jako její dceřiná společnost. Platforma se stala druhou nejnavštěvovanější webovou stránkou na světě, hned po samotném Googlu.[20]

---

[16] *Instagram: Vše, co potřebujete vědět o této populární aplikaci*. [online]. IGalerie. 2025. [cit. 2025-03-05]. Dostupné z WWW: <https://igalerie.cz/instagram-vse-co-potrebujete-vedet-o-teto-popularni-aplikaci/?.>

[17] *Co je Instagram?* [online]. Co je to? 2025. [cit. 2025-03-05]. Dostupné z WWW: <https://cojeto.superia.cz/software/instagram.php?.>

[18] *Kdy vznikl YouTube? Historie internetového giganta*. Safer internet. 2025. [cit. 2025-03-05]. Dostupné z WWW: <https://saferinternet.cz/kdy-vznikl-youtube-historie-internetoveho-giganta/.>

[19] Tamtéž

[20] *Za deset let se stal YouTube druhou nejnavštěvovanější stránkou*. [online]. ČT24. 2015. [cit. 2025-03-05]. Dostupné z WWW: <https://ct24.ceskatelevize.cz/clanek/media/za-deset-let-se-stal-youtube-druhou-nejnavstevovanejsi-strankou-132443.>

2.4.4 WhatsApp

WhatsApp je bezplatná aplikace pro zasílání zpráv a volání, která si získala popularitu po celém světě. Umožňuje uživatelům posílat textové zprávy, obrázky, videa a zvukové nahrávky zdarma pomocí mobilní sítě nebo Wi-Fi. Kromě toho nabízí možnost uskutečňovat hlasové a video hovory, a to jak mezi jednotlivci, tak ve skupinách. Aplikace je dostupná pro různé platformy, včetně Androidu, iOS a také ve verzi pro počítače.[21]

WhatsApp používá internetové připojení telefonu (Wi-Fi nebo mobilní data) k zajištění komunikace, což umožňuje uživatelům vyhnout se poplatkům za SMS či tradiční hovory. Díky své jednoduchosti a široké dostupnosti se stal jednou z nejpopulárnějších komunikačních aplikací na trhu.

2.5 Sociální inženýrství

Sociální inženýrství je v dnešní době vnímáno jako soubor technik a metod, které umožňují získat důvěrné nebo jinak užitečné informace. Klíčem k jeho úspěchu je neinformovanost oběti – pokud je některá z metod sociálního inženýrství použita, oběť si neuvědomuje, že dochází k manipulaci, a informace poskytne dobrovolně.

Jednou z nejrozšířenějších forem je takzvané „bezkontaktní sociální inženýrství“, kdy útočník s obětí nepřichází do přímého styku. Tento typ útoku se nejčastěji šíří prostřednictvím internetu, kde dominuje phishing – technika vyžadující základní znalosti programování.

Další variantou je „kontaktní sociální inženýrství“, které spoléhá na osobní interakci s obětí. Příkladem je pretexting, kdy útočník využívá vymyšlený scénář k získání požadovaných informací. V tomto případě je důležité ovládat neverbální komunikaci a umět ji využít ve svůj prospěch.[22]

Pachatelé se uchylují k sociálnímu inženýrství, protože je snazší oklamat člověka než prolomit bezpečnostní software, který byl navržen k ochraně citlivých informací, jako jsou hesla či osobní údaje. Pokud je některá z metod sociálního inženýrství úspěšně

[21] *Co je WhatsApp a jak jej používat na chytrém telefonu? Průvodce pro začátečníky*. [online]. MobilTown. 2025. [cit. 2025-03-05]. Dostupné z WWW: <https://www.mobiltown.cz/nastaveni/co-je-whatsapp-a-jak-jej-pouzivat-na-chytrem-telefonu-pruvodce-pro-zacatecniky/. >

[22] INFORMATION SECURITY OFFICE. *Social Engineering*. [online]. Carnegie Mellon University. 2025. [cit. 2025-02-03]. Dostupné z WWW: <https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html.>

použita, člověk, který s tímto softwarem pracuje, poskytne potřebné informace sám, aniž by si to uvědomoval.

Obětí přitom nemusí být přímo správce těchto údajů – cílem může být například i zaměstnanec ostrahy obchodu. Nevědomky může prozradit detaily, jako je jeho obchůzková trasa, časy přestávek nebo umístění bezpečnostních kamer, včetně tzv. „slepých míst“, která nejsou pod dohledem.[23]

2.6 Hardware a Software

Počítačový hardware je souhrnný termín používaný k označení fyzických součástí analogového nebo digitálního počítače. Tento pojem odlišuje hmatatelné části výpočetního zařízení od softwaru, který tvoří strojově čitelné instrukce nebo programy určující, co mají fyzické komponenty dělat a kdy mají vykonávat příkazy.

Hardware a software se navzájem doplňují. Počítač může efektivně fungovat a poskytovat užitečné výsledky pouze tehdy, pokud hardware a software správně spolupracují.

Počítačový hardware lze rozdělit na interní a externí komponenty. Interní hardware zahrnuje součásti nezbytné pro správný chod počítače, zatímco externí hardware se k počítači připojuje za účelem rozšíření nebo vylepšení jeho funkcí.[24]

Software je soubor instrukcí, dat nebo počítačových programů, které slouží k ovládání zařízení a provádění konkrétních úloh. Je opakem hardwaru, který označuje fyzické součásti počítače. V tomto kontextu se pod pojmem „software“ rozumí veškeré běžící programy, skripty a aplikace na daném zařízení.[25]

---

[23] *Social engineering techniques: 4 ways criminal outsiders get inside*. [online]. CSO. 2010 [cit. 2025-02-03]. Dostupné z WWW: <https://www.csoonline.com/article/2125205/social-engineering/social-engineering-techniques--4-ways-criminal-outsiders-get-inside.html.>

[24] AWATI, R., *Computer hardware*. [online]. TechTarget. 2021 [cit. 2025-02-03]. Dostupné z WWW: <https://www.techtarget.com/searchnetworking/definition/hardware.>

[25] *Computer hardware*. [online]. Geeks For geeks. 2023 [cit. 2025-02-03]. Dostupné z WWW: <https://www.geeksforgeeks.org/software-and-its-types/.>

3 Kybernetická kriminalita

Kuchta a Válková ve své práci o obecné fenomenologii majetkové kriminality uvádějí, že kybernetické podvody představují druhou nejrozšířenější formu majetkové kriminality, hned po krádežích.[26]

Rozvoj počítačových podvodů vznikl díky dvěma klíčovým technologickým změnám: rozvojem osobních počítačů a vzniku internetu. Tyto inovace umožnily pachatelům provádět podvody na dálku a zároveň se vydávat za jinou osobu.[27]

Podle Smejkala lze pod označení „počítačová kriminalita," které je synonymem pro kybernetickou kriminalitu, zařadit několik „…různých druhů trestné činnosti…", jejichž „…primárním nástrojem nebo cílem jsou počítače a informační systémy."[28] Z jeho definice vyplývá, že kybernetická kriminalita zahrnuje veškeré nezákonné jednání s prvky trestného činu, při kterém je digitální zařízení nebo informační systém využit jako nástroj, cíl, nebo obojí současně.

Trestné činy v oblasti kybernetické kriminality lze rozdělit podle tří hlavních kritérií:

1. Trestné činy zaměřené na ochranu počítačových systémů, jejich vybavení a komponent před útoky, které narušují jejich funkčnost a brání jejich správnému využití.

2. Trestné činy, při nichž je výpočetní technika a elektronické komunikační sítě využity způsobem přímo uvedeným v konkrétní skutkové podstatě.

3. Trestné činy, které nespadají do předchozích dvou kategorií, ale byly spáchány za použití výpočetní techniky a elektronických komunikačních sítí, přičemž jejich vyšetřování může využívat stejné postupy jako v kategoriích 1 a 2.[29]

[26] KUCHTA, J., a VÁLKOVÁ, H., *Základy kriminologie a trestní politiky*. Praha: C.H. Beck, 2005, s. 368.
[27] SMEJKAL, V., *Kybernetická kriminalita*, *3. vydání.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. s. 219.
[28] Tamtéž, s.33.
[29] NĚMEC, M., *Teorie a metodologie kriminalistiky pro magisterské studium*. Praha: Abook, 2018. s. 306-307.

4 Phishing

Abychom pochopili podstatu phishingu, je důležité nejprve tento pojem vymezit. Je třeba zdůraznit, že phishing je technika, která se neustále mění a vyvíjí, proto neexistuje univerzální definice. V odborných článcích, knihách a dalších materiálech o phishingu lze narazit na různé způsoby jeho definice.

Dle Smejkala je typickým phishingem podvodný e-mail, jehož cílem je "získání přihlašovacích údajů k internetovému bankovnictví, PINů platebních karet nebo dalších bezpečnostních údajů k různým finančním službám nebo serverům pro obchodování na internetu."[30] Tyto e-maily jsou obvykle zasílány z pečlivě upravených e-mailových adres, které vypadají důvěryhodně, a často obsahují odkaz na webové stránky, jež slouží k shromažďování osobních údajů. Phishingové zprávy bývají často rozesílány ve velkém množství, někdy i v tisících, aby se oslovilo co nejvíce lidí a zvýšila šance na úspěch útoku.[31]

Kolouch říká, že phishing nejčastěji "označuje podvodné či klamavé jednání, jehož cílem je získat informace o uživateli, jako jsou např. uživatelské jméno, heslo, číslo kreditní karty, PIN aj.“[32]

Internetový článek společnosti Cloudflare zase říká, že phishing označuje pokus o krádež citlivých informací, obvykle ve formě uživatelských jmen, hesel, čísel kreditních karet, bankovních informací nebo jiných důležitých údajů, které mají být využity nebo prodány. Útočník se vydává za důvěryhodný zdroj s lákavou žádostí, aby přilákal oběť a podvedl ji, podobně jako rybář používá návnadu k ulovení ryby.[33]

[30] SMEJKAL, V., *Kybernetická kriminalita*, *3. vydání.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. s. 224.
[31] HOLT, T., BOSSLER, A. a SEIGFRIED-SPELLAR K., *Cybercrime and digital forensic: An introduction.Third edition*. New York, NY: Routlege, 2022. s. 221.
[32] KOLOUCH, J*., CyberCrime*. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2016. s. 246.
[33] *What is a phishing attack?* [online]. Cloudflare. 2025. [cit. 2025-02-06]. Dostupné z WWW: <https://www.cloudflare.com/learning/access-management/phishing-attack/. >

5 Historie phishingu

Přesné určení prvního phishingového útoku může být složité. Phishingová technika byla poprvé popsána v roce 1987 v dokumentu mezinárodní skupiny uživatelů HP, Intertex. Phishing se dostal do širšího povědomí díky útoku, který šířil malware (škodlivý program) známý jako Love Bug. Tento útok se objevil 4. května 2000, kdy se v e-mailových schránkách po celém světě začala objevovat zpráva s předmětem „ILOVEYOU“. K e-mailu byl připojen zdánlivě neškodný soubor s názvem *LOVELETTER.txt*. Po jeho otevření se však spustil škodlivý červ, který přepsal obrazové soubory a následně rozeslal svou kopii všem kontaktům v adresáři Outlooku napadeného uživatele.

O několik let později, v červnu 2001, byl zaznamenán první známý phishingový útok na web elektronického obchodu, přičemž cílem se stala stránka E-Gold, útok však nebyl úspěšný.[34]

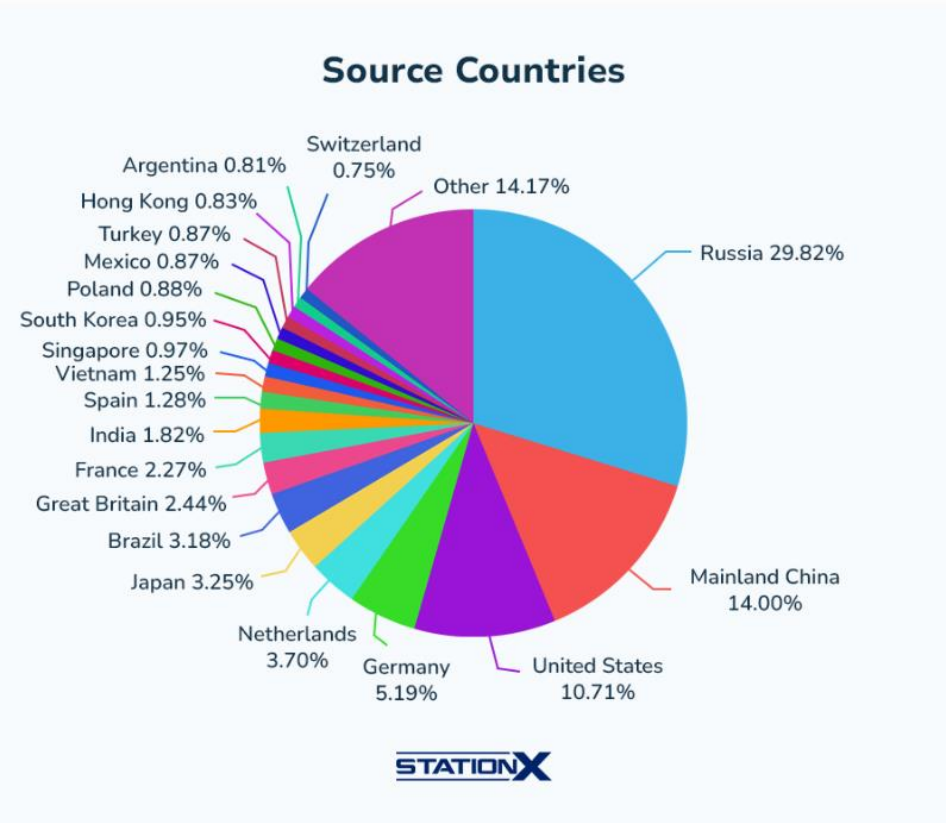
Od roku 2003 začali hackeři registrovat nové domény, které se podobaly názvům populárních webů, jako jsou eBay a PayPal. Následně pomocí škodlivého softwaru rozesílali podvodné e-maily zákazníkům těchto služeb. Ti, kteří se nechali nachytat, byli oklamáni a poskytli své údaje o platebních kartách a další osobní informace.

Na začátku roku 2004 se phishing vyvinul v lukrativní byznys a hackeři začali cílit na banky, podniky a jejich zákazníky. Jednou z hlavních metod používaných v té době bylo zobrazování vyskakovacích oken (pop-up), prostřednictvím kterých od nic netušících uživatelů získávali citlivé údaje. Postupem času začali hackeři vyvíjet další techniky, jako je spear phishing, vishing, nebo smishing.[35]

V roce 2022 bylo 29,82 % phishingových e-mailů odesláno z Ruska. Čína byla druhým nejčastějším zdrojem (14 %), následovaná Spojenými státy (10,71 %).[36]

[34] *The History of Phishing*. [online]. Graphus. 2023 [cit. 2025-02-06]. Dostupné z WWW: <https://www.graphus.ai/blog/history-of-phishing/.>
[35] *History of Phishing: How Phishing Attacks Evolved From Poorly Constructed Attempts To Highly Sophisticated Attacks*. [online]. Phishprotection. 2025. [cit. 2025-02-06]. Dostupné z WWW: <https://www.phishprotection.com/resources/history-of-phishing.>
[36] *Top Phishing Statistics for 2025: Latest Figures and Trends*. [online]. StationX. 2024 [cit. 2025-02-06]. Dostupné z WWW: <https://www.stationx.net/phishing-statistics/.>

Obrázek 1: Zdrojové země Phishingových útoků v roce 2022.[37]



V současné době je phishing nejběžnější formou kybernetické kriminality. Kyberzločinci každý den pošlou přibližně 3,4 miliardy e-mailů, které vypadají, jako by pocházely od důvěryhodných odesílatelů. To znamená více než bilion phishingových e-mailů ročně.[38]

[37] Zdroj: https://www.stationx.net/phishing-statistics/
[38] *Top Phishing Statistics for 2025: Latest Figures and Trends*. [online]. StationX. 2024 [cit. 2025-02-06]. Dostupné z WWW: <https://www.stationx.net/phishing-statistics/.>

6 Druhy phishingových útoků

6.1 E-mailový phishing

Pachatel používá e-mail k vylákání informací. Obvykle předstírá, že je Vaší bankou, vládou, doručovací společností nebo jakoukoli jinou organizací, které důvěřujete. Jejich cílem je, abyste otevřeli phishingový e-mail a stáhli přílohu, která skrývá malware, nebo abyste kliknuli na podezřelé odkazy. Chtějí vás přimět ke zveřejnění citlivých informací, jako jsou vaše přihlašovací údaje do internetového bankovnictví, nebo číslo vaší platební karty.[39]

Obrázek 2: Příklad E-mailového phishingu.[40]

6.2 Phishing skrze sociální sítě

Phishing na sociálních médiích je podvod, při kterém jsou uživatelé nalákáni na kliknutí na škodlivý odkaz nebo poskytnutí osobních informací. Zatímco tradiční phishing se primárně děje prostřednictvím e-mailu, phishing na sociálních médiích, jak název napovídá, se většinou vyskytuje na sociálních platformách. Útočník se často vydává za důvěryhodnou osobu, a přesvědčuje uživatele, aby poskytli své osobní údaje.[41]

[39] *What Is Phishing?* [online]. Proofpoint. 2025 [cit. 2025-02-06]. Dostupné z WWW: <https://www.proofpoint.com/us/threat-reference/phishing.>
[40] Zdroj: Vlastní zdroj
[41] *Social Media Phishing: A Primer*. [online]. InspiredeLearning. 2024 [cit. 2025-02-06]. Dostupné z WWW: <https://inspiredelearning.com/blog/social-media-phishing-prime.>

Obrázek 3: Příklad phishingu skrze sociální sítě.[42]

6.3 Smishing

Smishing je útok využívající sociální inženýrství, který používá falešné textové zprávy na mobilních telefonech k tomu, aby oklamal lidi a přiměl je stáhnout malware, sdílet citlivé informace nebo posílat peníze kyberzločincům. Termín „smishing“ je kombinací „SMS“ – neboli „short message service“, technologie stojící za textovými zprávami – a „phishingu“.

Smishing je stále populárnější formou kybernetického zločinu. Podle zprávy Proofpoint 2024 State of the Phish zažilo v roce 2023 75 % organizací útoky smishingu.[43]

Obrázek 4: Příklad smishingu.[44]

[42] Zdroj: Vlastní zdroj
[43] KOSINSKI, M., *What is smishing?* [online]. IBM. 2024 [cit. 2025-02-06]. Dostupné z WWW: <https://www.ibm.com/think/topics/smishing.>
[44] Zdroj: Vlastní zdroj

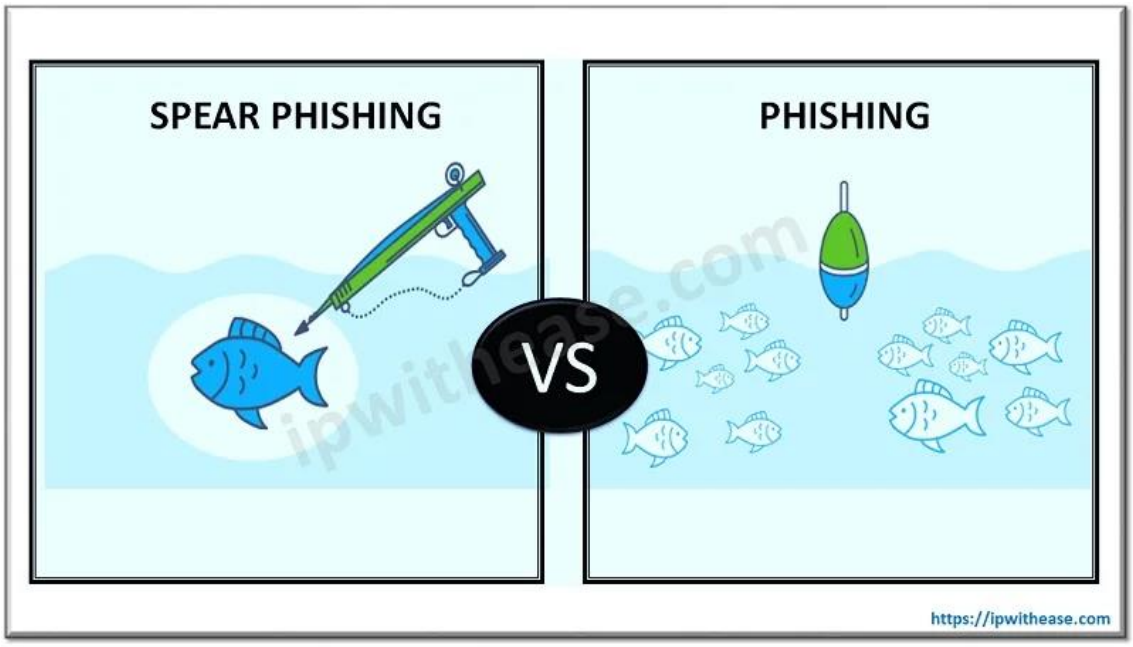
6.4 Vishing

Vishing, což je zkratka pro „voice phishing“, znamená podvodné jednání, při němž útočník zneužívá telefonního hovoru k tomu, aby přiměl oběť k poskytnutí citlivých informací. Cílem tohoto typu útoku je jako v předchozích případech získat osobní data oběti a následně je využít ve prospěch útočníka, přičemž obvykle jde o získání finanční výhody.[45]

6.5 Spear Phishing

Phishing je obecný pojem pro kybernetické útoky, ale útoky cílené se označují jako „spear phishing“. Jde o specifické a na míru šité kybernetické útoky, které míří na určité osoby nebo firmy. Útočníci často využívají spear phishingové e-maily, které vypadají důvěryhodně a přesvědčují příjemce, aby prozradil citlivé informace útočníkovi.[46]

Obrázek 5: Phishing vs Spear Phishing.[47]



6.6 Whaling

Whalingové útoky, často označované jako výkonný phishing, jsou sofistikované kybernetické hrozby zaměřené na vysoce postavené osoby v organizaci. Tyto útoky jsou

[45] *What Is Vishing And A Vishing Attack?* [online]. Fortinet. 2023 [cit. 2025-02-06]. Dostupné z WWW: <https://www.fortinet.com/resources/cyberglossary/vishing-attack.>
[46] *What is spear phishing? Definition and risks*. [online]. Kaspersky. 2025 [cit. 2025-02-16]. Dostupné z WWW: <https://www.kaspersky.com/resource-center/definitions/spear-phishing.>
[47] Zdroj: https://ipwithease.com/spear-phishing-attack-cyber-security/

pečlivě navrženy tak, aby oklamaly vrcholové manažery, jako jsou generální ředitelé a finanční ředitelé, a přiměly je k prozrazení citlivých informací. Termín „whaling“ odráží vysoké postavení těchto cílů, kteří mají významný přístup k důležitým datům a finančním aktivům. [48]

Obrázek 6: Spear phishing vs Whaling.[49]

Spear phishing i whaling silně využívají techniky sociálního inženýrství k oklamání svých cílů tím, že manipulují s lidmi, aby prozradili citlivé informace nebo provedli kroky, které ohrožují bezpečnost, tyto útoky využívají lidské psychologie místo technických slabin.[50]

[48] *Whaling*. [online]. Cisco. 2023 [cit. 2025-02-16]. Dostupné z WWW: <https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-whaling-attack.html#tabs-35d568e0ff-item-194f491212-tab.>
[49] Zdroj: https://phishgrid.com/blog/spear-phishing-vs-whaling/
[50] *Spear Phishing vs. Whaling: What Are the Differences?* [online]. LastPass. 2024 [cit. 2025-02-16]. Dostupné z WWW: <https://blog.lastpass.com/posts/spear-phishing-vs-whaling.>

7 Způsoby zakrytí identity útočníka

7.1 Spoofing

Spoofing je běžná taktika, kterou kybernetičtí útočníci používají k tomu, aby zamaskovali neznámý nebo neoprávněný zdroj komunikace, či přenos dat, aby se jevil jako známý a důvěryhodný. Tento podvod spočívá ve vydávání se za někoho nebo za něco jiného, aby oběti zmátli a získali jejich důvěru.[51]

7.1.1 Email spoofing

Falešná e-mailová adresa odesílatele, která vypadá, jako by pocházela od někoho, koho znáte a komu důvěřujete – možná od přítele, kolegy, člena rodiny nebo firmy, se kterou spolupracujete. V případě firmy nebo organizace může e-mail obsahovat známé brandingové prvky, jako je její logo, barva nebo písmo.[52]

7.1.2 Spoofing telefonního čísla

Spoofing telefonního čísla způsobí, že se na identifikátoru volajícího zobrazí telefonní číslo nebo jiné informace, které vypadají, jako by hovor pocházel od důvěryhodné osoby nebo firmy. I když mohou informace o volajícím vypadat autenticky, hovory jsou často uskutečňovány útočníky, kteří se nacházejí mimo stát nebo zemi. Spoofing je obvykle prováděn se škodlivými nebo neetickými motivy ze strany volajícího a vedl mnoho lidí k přesvědčení, že už není možné důvěřovat identifikátoru volajícího. Tento způsob se velmi často užívá ve spojitosti s Vishingem. [53]

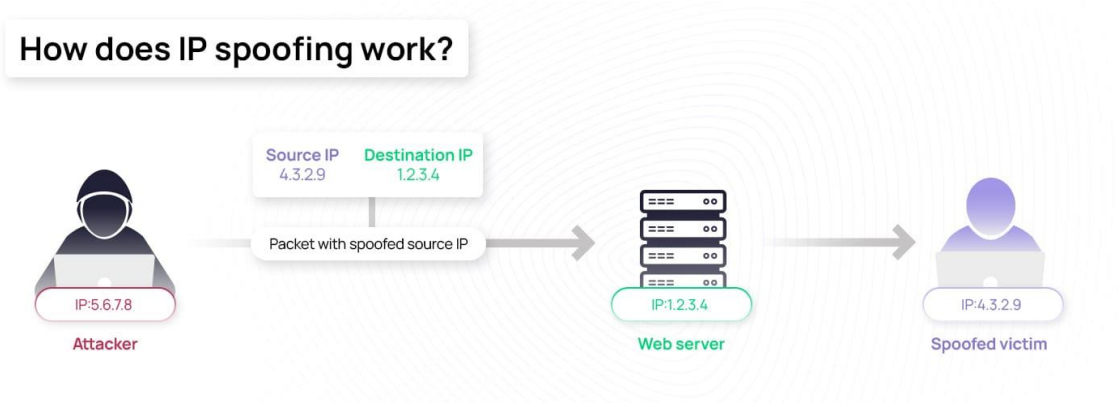
7.1.3 Spoofing IP adresy

Počítačové sítě komunikují prostřednictvím výměny síťových datových paketů, z nichž každý obsahuje několik hlaviček používaných pro směrování a zajištění kontinuity přenosu. Jednou z těchto hlaviček je „Source IP Address“ (IP adresa odesílatele), která označuje IP adresu odesílatele paketu.

[51] *What Is Spoofing?* [online]. Proofpoint. 2025 [cit. 2025-02-16]. Dostupné z WWW: <https://www.proofpoint.com/us/threat-reference/spoofing.>
[52] *Types of spoofing*. [online]. Malwarebytes. 2025 [cit. 2025-02-16]. Dostupné z WWW: <https://www.malwarebytes.com/spoofing.>
[53] *Everything to Know About Phone Number Spoofing*. [online]. Kaspersky. 2025 [online]. Dostupné z WWW: <https://www.kaspersky.com/resource-center/preemptive-safety/phone-number-spoofing.>

Spoofing IP adresy je falšování obsahu v hlavičce Source IP, obvykle s náhodně generovanými čísly, většinou za účelem zamaskování identity odesílatele.[54]

Obrázek 7: Příklad spoofingu IP adresy.[55]



Všechny tyto metody vyžadují použití speciálního softwaru nebo skriptů, které umožňují manipulovat s identifikátory a informacemi odesílatelů. Cílem je zmást oběť, aby udělala akce, které by normálně neudělala, nebo získat přístup k citlivým informacím.

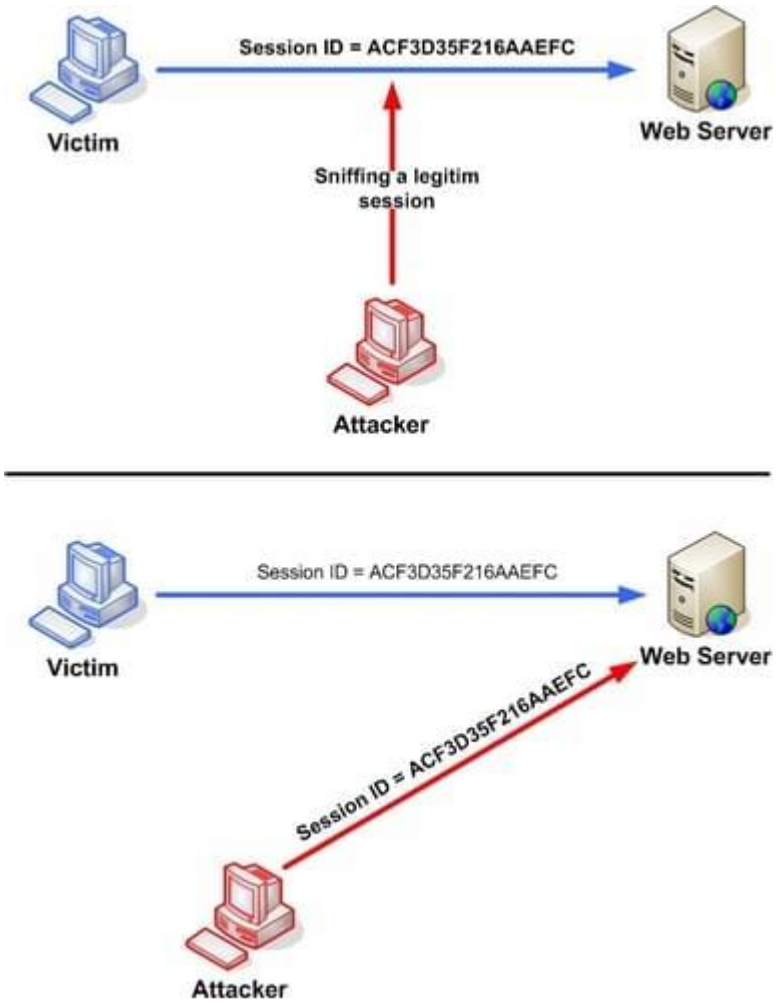
7.2 Page Hijacking

Page hijacking je podvodná technika, kterou kybernetičtí útočníci používají k manipulaci s webovým provozem. Vytvořením duplikátu legitimní webové stránky se útočníci snaží přesměrovat uživatele na škodlivý web. Toho mohou dosáhnout zneužitím algoritmů vyhledávačů, které mohou omylem upřednostnit škodlivou stránku před původní. K provedení útoku útočníci buď nainstalují malware na počítače uživatelů nebo převezmou kontrolu nad směrovači.

Hijacking může být využito k pharmingu (v tomto kontextu útočníci obvykle zobrazují nežádoucí reklamy za účelem generování příjmů) nebo k phishingu (zobrazením falešných verzí stránek, které uživatelé navštěvují, a krádeží jejich dat nebo přihlašovacích údajů).[56]

[54] *IP Spoofing*. [online]. Imperva. 2024 [cit. 2025-02-16]. Dostupné z WWW: <https://www.imperva.com/learn/ddos/ip-spoofing/.>
[55] Zdroj: https://sosafe-awareness.com/glossary/spoofing/
[56] *Domain name server (DNS) Hijacking*. [online]. Imperva. 2024 [cit. 2025-02-16]. Dostupné z WWW: <https://www.imperva.com/learn/application-security/dns-hijacking-redirection/.>

Obrázek 8: Přiklad page hijacking.[57]



7.3 Catfishing

Catfishing označuje situaci, kdy osoba bere informace a obrázky, obvykle od jiných lidí, a používá je k vytvoření nové identity pro sebe. V některých případech si catfisher ukradne kompletní identitu jiného jednotlivce – včetně jeho obrázku, data narození a geografické polohy – a předstírá, že je to jeho vlastní identita. Catfisher pak tuto identitu využívá k tomu, aby oklamal ostatní a přiměl je k navázání kontaktu nebo k online obchodování.

V některých případech je útok catfishing zaměřen na jednotlivce. V těchto případech si catfisher vytvoří identitu, která podle něj bude přitahovat jeho cílovou oběť. Catfishing je dlouhodobě běžný na online seznamovacích fórech a webech. Protože catfisher může skrýt jakoukoli část své skutečné identity bez toho, aby byl zpochybněn,

[57] Zdroj: https://developer.mozilla.org/en-US/docs/Glossary/Session_Hijacking

lidé často falšovali určité aspekty svého profilu, aby přitáhli svou cílovou oběť. To často zahrnuje použití profilové fotky, kterou ukradli někomu jinému, aby vypadali atraktivněji.[58]

[58] *What Is Catfishing?* [online]. Fortinet. 2025 [cit. 2025-02-16]. Dostupné z WWW: <https://www.fortinet.com/resources/cyberglossary/catfishing.>

8 Kazuistika

8.1 Emailový phishing

Lékařka Jana N. pracovala na soukromé klinice jako specialistka v oblasti stomatologie. Každý den komunikovala s pacienty, kolegy i dodavateli zdravotnického materiálu prostřednictvím e-mailu. Jednoho dne obdržela zprávu, která se tvářila jako oficiální oznámení od poskytovatele zdravotnického softwaru, který její klinika používala pro správu pacientských záznamů.

E-mail ji upozorňoval na nutnou bezpečnostní aktualizaci systému a obsahoval odkaz, na kterém mělo dojít ke stažení aktualizací. Podvodná e-mailová adresa se na první pohled tvářila jako oficiální, ale měla drobný rozdíl, kterého si Jana nevšimla. Oficiální podpora používala adresu support@medisoft.cz, zatímco podvodný e-mail přišel z adresy support@medls0ft.cz.

Jelikož Jana spěchala mezi ordinacemi, neověřila si pravost zprávy a na uvedený odkaz klikla. Ten ji přesměroval na přihlašovací stránku, která vypadala přesně jako ta, kterou běžně používala. Bez zaváhání zadala své přihlašovací údaje a pokračovala ve své práci.

Ve skutečnosti se ale jednalo o podvodnou stránku, která okamžitě odeslala její přihlašovací údaje útočníkům. Během několika hodin získali neoprávněný přístup do databáze pacientských záznamů a pokusili se stáhnout citlivé informace, včetně anamnéz a osobních údajů pacientů. Naštěstí si IT oddělení kliniky všimlo neobvyklé aktivity v systému a účet zablokovalo dříve, než došlo k závažnému úniku dat.

Jana si z této zkušenosti odnesla důležité ponaučení a od té doby si pečlivě kontroluje každou výzvu k přihlášení, aby se podobná situace už neopakovala.[59]

8.2 Phishing skrze sociální sítě

Lucie K. byla aktivní uživatelkou sociálních sítí, zejména Instagramu a Facebooku. Sdílela zde fotografie ze svého života, komunikovala s přáteli a sledovala oblíbené influencery. Jednoho dne obdržela soukromou zprávu na Instagramu, která se tvářila jako oficiální oznámení od podpory platformy. Zpráva ji varovala, že její účet byl

[59] Interní systém Policie České republiky

nahlášen kvůli porušení autorských práv a hrozí mu zablokování. Součástí zprávy byl také odkaz, kde měla „ověřit svůj účet“, aby předešla smazání profilu.

Lucie, vystrašená představou, že přijde o své fotky a vzpomínky, na odkaz klikla. Stránka, kam byla přesměrována, vypadala jako běžná přihlašovací stránka Instagramu, a tak bez váhání zadala své přihlašovací údaje. V tu chvíli se stránka načetla znovu, ale žádné potvrzení neproběhlo. Nevěnovala tomu pozornost a pokračovala ve svých činnostech.

O několik minut později však zjistila, že byla automaticky odhlášena ze svého účtu a nemůže se přihlásit zpět – její heslo bylo změněno. Hackeři, kteří získali její přihlašovací údaje, okamžitě převzali kontrolu nad profilem, změnili kontaktní e-mail a začali rozesílat podvodné zprávy jejím přátelům a sledujícím. Tvrdili, že se Lucie ocitla v nouzi a potřebuje urgentně peníze na opravu rozbitého telefonu. Někteří její známí v dobré víře na výzvu reagovali a poslali menší částky na uvedený bankovní účet.

Lucie si uvědomila, že se stala obětí kybernetického útoku, a pokusila se situaci vyřešit kontaktováním oficiální podpory Instagramu. Obnova účtu trvala několik dní, a i přesto se jí nepodařilo získat zpět část ztracených soukromých zpráv a příspěvků. Událost ji poučila o důležitosti kybernetické bezpečnosti – od té doby si vždy pečlivě ověřuje odkazy, které jí přijdou, a aktivovala si dvoufázové ověření pro přihlášení ke svým účtům.

Tento incident jí ukázal, jak snadné je stát se obětí podvodu na sociálních sítích a jak důležité je chránit nejen své údaje, ale i své kontakty, které by mohly být podobným způsobem zneužity. [60]

8.3 Whaling s Vhishingem a e-mailovým phishingem za užití spoofingu

Petr L. byl výkonný ředitel renomované české pojišťovny, která měla na starosti klíčové finanční operace a schvalování velkých transakcí. Díky své pozici měl přístup k citlivým informacím a pravidelně komunikoval s bankami a dalšími partnery společnosti.

Jednoho dne obdržel Petr telefonní hovor, který se na první pohled zdál být zcela legitimní. Hovor přišel z čísla, které mu bylo velmi dobře známo – číslo na generálního

[60] Interní systém Policie České republiky

ředitele pojišťovny, Martina D. Tento telefonní hovor měl však ve skutečnosti podvodnou povahu, což Petr nepoznal, protože telefonní číslo, které se na jeho obrazovce objevilo, vypadalo, jako by volal skutečný generální ředitel.

Osoba na druhé straně se představila jako Martin D. a okamžitě uvedla, že je nutné provést urgentní finanční transakci, aby byla zachována stabilita společnosti. Podle jeho slov byla identifikována podvodná platba na firemním účtu a bylo potřeba okamžitě přesměrovat prostředky na bezpečný bankovní účet, aby se zabránilo ztrátám. Hlas na druhé straně byl velmi přesvědčivý a Petr okamžitě věřil, že skutečně mluví se svým generálním ředitelem.

Vzhledem k urgentnosti situace a důvěře, kterou měl k vedení společnosti, se rozhodl bez váhání provést požadovanou platbu. Když se po telefonu ptal na podrobnosti transakce, osoba, která se vydávala za Martina, mu poskytla číslo účtu a varovala ho, že každé zpoždění by mohlo ohrozit stabilitu společnosti a ohrozit její mezinárodní kontrakty.

Petr obdržel následně e-mail, který se tvářil jako oficiální potvrzení od banky, s detaily transakce, a proto mu vše přišlo naprosto legitimní. E-mail také obsahoval instrukce pro platbu, které se shodovaly s informacemi poskytnutými telefonicky. Veškerá komunikace vypadala důvěryhodně, včetně podpisu a formálních náležitostí. Bez jakéhokoli ověření informací tedy Petr převedl částku ve výši 3 000 000 Kč na uvedený účet.

Po několika dnech se Petr rozhodl zkontrolovat provedenou transakci s kolegy a skutečným generálním ředitelem, a teprve tehdy zjistil, že uskutečněný hovor byl podvodný. Skutečný Martin nebyl v té době vůbec v kanceláři a neměl s transakcí nic společného.

Po podrobném vyšetření se ukázalo, že útočníci využili techniku spoofingu, tedy změnili identifikátor volajícího, aby telefonní číslo vypadalo jako oficiální číslo generálního ředitele. Tento trik, kdy se na displeji objevil důvěryhodný kontakt, vedl k tomu, že Petr neprověřoval, kdo skutečně volá, a okamžitě uskutečnil požadovanou platbu.

Po incidentu firma podala trestní oznámení, ale peníze již byly převedeny na zahraniční účet, a okamžitě vybrány.

Tento útok ukázal, jak nebezpečné může být využití spoofingu k obelstění vysokých manažerů a jak rychle mohou útočníci zneužít důvěryhodné kontakty a informační kanály k provedení whalingových a phishingových útoků. V tomto případě ztráta ve výši 3 000 000 Kč byla důsledkem nedostatečného ověření a technické manipulace s identifikátorem volajícího.[61]

[61] Interní systém Policie České republiky

9 Kybernetická bezpečnost a prevence

Mnoho lidí považuje kybernetickou bezpečnost za oblast, kterou řeší výhradně oddělení informačních a komunikačních technologií, a ostatní se jí nemusí příliš zabývat.[62] To je však mylná představa, protože k zajištění kybernetické bezpečnosti dnes přispívá každý jednotlivý uživatel. Právě proto je důležité tuto oblast nebrat na lehkou váhu.

Kyberprostor je úzce propojen s realitou prostřednictvím moderních technologií a výpočetní techniky, která slouží jako most mezi digitálním a fyzickým světem. Toto propojení probíhá současně na mnoha místech po celém světě a teoreticky může i jediné narušení způsobit škody nejen v kyberprostoru, ale i v reálném světě.[63]

Při zajišťování bezpečnosti je důležité zaměřit se na několik klíčových otázek:

- **Koho se bezpečnost týká?** (např. státu, jednotlivce)
- **Jaké hodnoty je potřeba chránit?** (např. data)
- **Před jakými hrozbami je třeba tyto hodnoty ochránit?** (např. kybernetickými útoky)
- **Jaké kroky je nutné podniknout k ochraně těchto hodnot?**[64]

Výraz „kybernetická bezpečnost“ nemá jen jednu přesnou definici. Nicméně definice, která mi připadá nejvýstižnější, je: „Souhrn právních, organizačních, technických a vzdělávacích prostředků směřující k zajištění ochrany kybernetického prostoru“[65]

9.1 Prevence phishingu

9.1.1 Identifikování útoku

Je důležité být ostražitý a nepodceňovat hrozbu phishingu. V minulosti bylo možné jednoduché phishingové zprávy rozpoznat díky špatné češtině, protože často pocházely ze zahraničí a byly překládány automaticky a nekvalitně. Dnes se však kvalita

[62] Kolouch, J., Bašta, P. *Cybersecurity*. Praha: CZ.NIC, 2019. s. 39.
[63] Sak, P. *Úvod do teorie bezpečnosti*. Havlíčkův Brod: Petrklíč, 2018, s 234–235.
[64] Kolouch, J., Bašta, P. *Cybersecurity*. Praha: CZ.NIC, 2019. s. 35.
[65] JIRÁSEK, P., NOVÁK, L., a POŽÁR, J., *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*, 2015, s. 57.

těchto překladů zlepšuje a zprávy mohou působit jazykově věrohodněji. Proto je potřeba všímat si i dalších varovných znaků.

Jedním z nich může být e-mailová adresa odesílatele – pokud vypadá podezřele nebo má neobvyklou doménu, jako například .ru místo .cz, je dobré být obezřetný. Nicméně sofistikované phishingové zprávy mohou přicházet i z důvěryhodně vypadajících adres. Z tohoto důvodu je obzvláště důležité být opatrný při klikání na jakékoliv odkazy přiložené v e-mailu. U propracovaného phishingu to často bývá jediný znak, podle kterého lze útok rozpoznat.

Útočníci také využívají grafickou podobu zpráv. Kvůli různorodosti vizuálních stylů používaných ve státní správě je pro uživatele někdy těžké odlišit oficiální vzhled od soukromého.[66]

9.1.2 Antivirové softwary

Antivirový software je sada programů, které dokážou zabránit šíření virů, detekovat je, odstranit a vyhledávat různé druhy škodlivého softwaru, jako jsou červi, trojské koně, adware a další. Tento software se nejčastěji používá na počítačových zařízeních, ale lze jej také využít na sítích a IT systémech. Nestačí však pouze nainstalovat antivirový program – je také nutné jej pravidelně aktualizovat, aby byla zajištěna ochrana před nejnovějšími hrozbami.[67]

Antivirový software běží na pozadí zařízení a neustále skenuje zařízení nebo servery na přítomnost hrozeb malwaru. Mezi jeho hlavní funkce patří:

- **Skenování souborů a složek:** Prohledává konkrétní soubory a adresáře na přítomnost vzorců malwaru, které by mohly naznačovat nebezpečí.
- **Plánované kontroly:** Umožňuje uživatelům naplánovat kontroly podle jejich potřeb a poté provádí skenování v určený čas.
- **Ruční skenování:** Uživatelé mohou kdykoliv spustit skenování systému podle potřeby.

[66] *Návod, jak poznat phishingové útoky*. [online]. GOV. 2025 [cit. 2025-02-16]. Dostupné z WWW: <https://portal.gov.cz/kam-dal/cesky-egovernment/navod-jak-poznat-phisingove-utoky.>
[67] VIGDERMAN, A., *How Does Antivirus Software Work?* [online]. Security.org. 2024 [cit. 2025-02-16]. Dostupné z WWW: <https://www.security.org/antivirus/how-does-antivirus-work/.>

- **Odstraňování malwaru:** Pokud software detekuje škodlivý program, odstraní ho ze systému. Některé programy to provádějí automaticky na pozadí, zatímco jiné požadují souhlas uživatele nebo ho informují před odstraněním.

Díky těmto funkcím antivirový software zajišťuje, že systém zůstane bezpečný a připravený k práci.[68]

9.1.3 Spam filtr

Spamové filtry mají stejný základní cíl: zabránit nevyžádaným e-mailům dostat se do uživatelských schránek. Existuje však několik různých typů spamových filtrů, které používají různé metody filtrování, aby účinně rozpoznaly spam.

Můžete použít filtr k nastavení specifických pravidel, která se aplikují na všechny e-maily přicházející do vašeho e-mailu. Pokud obsah nebo původ e-mailu odpovídá některému z pravidel, může být automaticky odeslán do složky spamu. Například můžete nastavit filtr tak, aby hledal konkrétní slova nebo fráze v textu e-mailu. Pokud se tato slova v e-mailu objeví, zpráva bude odeslána do složky spamu.

Spam totiž může obsahovat škodlivý obsah, který může infikovat počítače uživatelů viry nebo jiným malwarem. [69]

9.1.4 Heslo

Každý rok se miliony účtů stanou obětí krádeže hesel a phishingových podvodů, což vede k ničivým následkům, včetně krádeže identity, finančních ztrát a neoprávněného přístupu k citlivým informacím. V dnešním digitálním světě slouží vaše heslo jako brána k vašim osobním, akademickým a finančním údajům, což činí jeho ochranu naprosto klíčovou. Posílení vašich návyků v oblasti hesel a bdělost vůči phishingovým podvodům jsou nezbytnými kroky k ochraně vaší digitální identity.[70]

---

[68] *Antivirus Software*. [online]. Toppr. 2025 [cit. 2025-02-16]. Dostupné z WWW: <https://www.toppr.com/guides/computer-science/computer-fundamentals/utility-software/antivirus-software/.>

[69] *What Is Spam Filtering?* [online]. Fortinet. 2025 [cit. 2025-02-16]. Dostupné z WWW: <https://www.fortinet.com/resources/cyberglossary/spam-filters.>

[70] VENKAT, K., *Enhance Your Digital Security with Strong Passwords*. [online]. Seton Hall University. 2024 [cit. 2025-02-16]. Dostupné z WWW: <https://www.shu.edu/technology/news/strengthening-your-digital-security-password-and-phishing-tips.html.>

9.1.5 Firewall

Firewall je bezpečnostní zařízení pro síť. Vytváří bariéru mezi důvěryhodnou sítí a nedůvěryhodnou sítí. Například firewall může omezit internetový provoz, který se pokouší přistoupit k vaší soukromé síti. Funguje jako vrátný, který řídí příchozí a odchozí provoz podle předem stanoveného souboru bezpečnostních pravidel.[71]

9.1.6 Vzdělání

Zde se plně ztotožňuji s názorem Melada a kolektivu, kteří říkají, že školení lidí je jedním z nejefektivnějších způsobů, jak vybudovat ochranu proti phishingovým útokům. Aby bylo toto školení opravdu účinné, nestačí jen vybrat správnou formu, ale je důležité ho provádět pravidelně a systematicky.[72]

9.2 Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

Národní úřad pro kybernetickou a informační bezpečnost zkráceně NÚKIB „je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku veřejně regulované služby v rámci družicového systému Galileo.“[73]

NÚKIB vychází při své činnosti z pravidel stanovených v zákoně č. 181/2014 Sb. o kybernetické bezpečnosti a jeho novele č. 205/2017 Sb. Tento právní rámec je základem pro všechny jeho aktivity. Ačkoli NÚKIB nemá pravomoc přímo měnit tento zákon, může se podílet na jeho úpravách a navrhování změn ve spolupráci s jinými státními orgány a odborníky na kybernetickou bezpečnost. Fungování vládního CERT (GovCERT.CZ), který se specializuje na kybernetickou bezpečnost.

---

[71] *What Is a Firewall?* [online]. Coursera. 2023 [cit. 2025-02-16]. Dostupné z WWW: <https://www.coursera.org/articles/what-is-firewall?utm_medium=sem&utm_source=gg&utm_campaign=b2c_emea_x_multi_ftcof_career-academy_cx_dr_bau_gg_pmax_gc_s1_en_m_hyb_23-12_x&campaignid=20858198824&adgroupid=&device=c&keyword=&matchtype=&network=x&devicemodel=&creativeid=&assetgroupid=6484888893&targetid=&extensionid=&placement=&gad_source=1&gclid=CjwKCAiAtsa9BhAKEiwAUZAszUcvRBVsv-UAcAFJ7migf5z0VAonOrNy-Dy0B_xhTZJKPCoHX4zO6xoCNzAQAvD_BwE.>

[72] Al-Daeef, M., Basir, N. a Saudi, M., Security Awareness Training: A Review. In: *Proceedings of the World Congress on Engineering 2017 Vol I*. IAENG: London, U.K., 2017, s. 446–451. ISBN 978-988-14047-4-9.

[73] *O NÚKIB*. Národní úřad pro kybernetickou a informační bezpečnost: NÚKIB [online]. Česko: NÚKIB, [2017] [cit. 2022-03-05]. Dostupné z WWW: <https://www.nukib.cz/cs/o-nukib/>

Mezi hlavní činnosti NÚKIB patří:

- Prevence a ochranu před kybernetickými útoky zaměřenými na kritickou infrastrukturu, klíčové informační systémy a veřejnou správu.
- Řešení a koordinaci kybernetických incidentů v organizacích, které spravují kritickou infrastrukturu a poskytují základní služby.
- Realizaci vzdělávacích a osvětlovacích aktivit v oblasti kybernetické bezpečnosti.
- Spolupráci s národními a mezinárodními subjekty, které se podílejí na zabezpečení kybernetického prostoru.
- Organizaci a účast na kybernetických cvičeních, jak na národní, tak na mezinárodní úrovni.
- Podporu výzkumu a inovací v oblasti kybernetické bezpečnosti.
- Reprezentaci České republiky v mezinárodních organizacích zaměřených na kybernetickou bezpečnost.
- Hodnocení kybernetických rizik a přijímání opatření na jejich minimalizaci.
- Tvorbu bezpečnostní politiky a koordinaci mezinárodních závazků v rámci NATO, EU a dalších organizací.
- Vypracování komunikační strategie týkající se kybernetické bezpečnosti ve spolupráci s ostatními složkami úřadu.

Tyto činnosti přispívají k posílení bezpečnosti kybernetického prostředí v České republice.[74]

[74] *Kybernetická bezpečnost*. [online]. Národní úřad pro kybernetickou a informační bezpečnost: NÚKIB. 2025. [cit. 2025-03-05]. Dostupné z WWW: <https://nukib.gov.cz/cs/kyberneticka-bezpecnost/. >

10 Legislativa spojená s phishingem

S rozvojem technologií a rostoucí kreativitou útočníků se v oblasti kyberkriminality objevují případy, kdy určité jednání nelze jednoznačně zařadit pod žádný trestný čin, a to ani při širším výkladu právních předpisů.[75] Některé činy není nutné speciálně upravovat s ohledem na jejich kybernetický rozměr, protože stačí využít stávající právní normy, které již pokrývají dané skutkové podstaty. Příkladně to platí pro podvody jako je phishing. Na druhou stranu existuje mnoho činů spojených s kyberprostorem, které nemají přímý ekvivalent v reálném světě.[76]

Jak bylo již naznačeno v předchozím odstavci, ačkoli se v trestním zákoníku (zákon č. 40/2009 Sb.) pojem phishing explicitně nevyskytuje, neznamená to, že je jeho provádění považováno za legální a dovolené. Phishing, jako jednu z mnoha technik podvodného jednání, lze postihovat na základě § 209, který se zabývá trestným činem podvodu a spadá do páté hlavy trestního zákoníku. Tato část se věnuje trestným činům proti majetku.[77]

Každý trestný čin se liší svou objektivní stránkou. Objektivní stránkou trestného činu podvodu je situace, kdy pachatel podvodu „… sebe nebo jiného obohatí tím, že uvede někoho v omyl, využije něčího omylu nebo zamlčí podstatné skutečnosti, a způsobí tak na cizím majetku škodu nikoli nepatrnou…“[78]

Právní kvalifikace se liší podle konkrétních činů, které byly spáchány. Může se jednat o porušení § 230 trestního zákoníku, který se týká neoprávněného přístupu k počítačovému systému nebo zásahu do něj, dále o § 231, který se vztahuje na opatřování a uchovávání přístupových zařízení a hesel k počítačovým systémům a podobným datům, a nakonec o § 234, který se zaměřuje na neoprávněné získání, padělání nebo změnu platebních prostředků.[79]

[75] GŘIVNA, T., POLČÁK, R., Kyberkriminalita a právo. Praha: Auditorium, 2008, str. 82.
[76] JELÍNEK, J., Kriminologie. Praha: Leges, 2021, str. 499.
[77] *Zákon trestní zákoník* [online]. Zákony pro lidi. 2025. [cit. 2025-03-02]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40.>
[78] Tamtéž
[79] KRUPIČKA, J., *Kybernetická kriminalita*. [online]. Acta Universitatis Carolinae. 2012. ISSN 0323-0619. [cit. 2025-03-02]. Dostupné z WWW: <https://www.prf.cuni.cz/dokumenty-download/1404048928/.>

10.1 Zákon o kybernetické bezpečnosti

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, je klíčovým právním předpisem, který upravuje problematiku kybernetické bezpečnosti v České republice. Tento zákon, který vstoupil v platnost 1. ledna 2015, má za cíl zajistit ochranu před kybernetickými hrozbami, zajišťovat bezpečnost informačních systémů, sítí a služeb elektronických komunikací, a především vymezit rámec pro spolupráci mezi veřejnou správou, státními institucemi a soukromým sektorem při řešení kybernetických incidentů. Jak uvádí § 1 zákona, „cílem zákona je přispět k ochraně kybernetické bezpečnosti České republiky a ochrany důvěrnosti, integrity a dostupnosti dat v informačních a komunikačních systémech."[80]

Zákon o kybernetické bezpečnosti stanovuje povinnosti pro tzv. „kritickou infrastrukturu“, což jsou důležité systémy pro chod společnosti, jako jsou energetické sítě, vodovody, nemocnice nebo finanční instituce. Subjekty, které se podílejí na provozu těchto systémů, musí implementovat opatření k ochraně před kybernetickými útoky, pravidelně monitorovat bezpečnost a hlásit incidenty, které by mohly ohrozit bezpečnost nebo provoz těchto systémů. Jak specifikuje § 8, „subjekty provozující kritickou informační infrastrukturu jsou povinny přijímat opatření na ochranu před kybernetickými hrozbami.“ [81]

Jedním z hlavních cílů zákona je zlepšení spolupráce na národní i mezinárodní úrovni, a to jak v rámci veřejné správy, tak i ve spolupráci se soukromým sektorem. Zákon rovněž vymezuje pravomoci a povinnosti jednotlivých orgánů veřejné moci, jako je NÚKIB, který je klíčovým orgánem pro zajištění kybernetické bezpečnosti v ČR. Jak je uvedeno v § 5, „Národní úřad pro kybernetickou a informační bezpečnost je odpovědný za implementaci opatření a metodiky v oblasti kybernetické bezpečnosti v České republice.“ [82]

V roce 2017 byl tento zákon novelizován (zákon č. 205/2017 Sb.), aby se přizpůsobil novým evropským nařízením, konkrétně směrnici NIS (Network and Information Security Directive) Evropské unie, která vyžaduje zajištění vysoké úrovně kybernetické bezpečnosti v členských státech. Jak uvádí § 23, novelizovaný zákon

[80] *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. [online]. Zákony pro lidi. 2014. [cit. 2025-03-05] Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2014-181>
[81] Tamtéž
[82] Tamtéž

„v souladu s evropskou legislativou upravuje pravidla pro zajištění bezpečnosti sítí a informačních systémů.“[83]

10.2 Vyhláška o kybernetické bezpečnosti

Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti, je podzákonný předpis, který upřesňuje a konkretizuje požadavky stanovené zákonem č. 181/2014 Sb., o kybernetické bezpečnosti. Cílem této vyhlášky je zajistit praktickou implementaci pravidel a opatření na ochranu kybernetické bezpečnosti v České republice, a to jak v oblasti kritické infrastruktury, tak i v souvislosti s povinnostmi právnických a fyzických osob v souvislosti s kybernetickými hrozbami.

Vyhláška č. 82/2018 Sb. specifikuje bezpečnostní požadavky na informační systémy a komunikační infrastrukturu, které jsou klíčové pro národní bezpečnost a ekonomiku. Dále definuje postupy pro hodnocení, implementaci a kontrolu opatření k zajištění ochrany proti kybernetickým incidentům. Součástí vyhlášky je také určení požadavků na provádění auditu, školení pracovníků, testování a certifikace bezpečnostních opatření. Vyhláška vymezuje i konkrétní postupy pro oznamování kybernetických incidentů a spolupráci s příslušnými orgány, včetně NÚKIB.

Vyhláška stanovuje povinnost pro subjekty, které se podílejí na ochraně kritické infrastruktury, zavést opatření na ochranu proti útokům a ztrátám dat. Současně klade důraz na ochranu citlivých informací a dodržování technických a organizačních opatření. V souladu s touto vyhláškou mají všechny organizace povinnost provádět pravidelný monitoring a vyhodnocování bezpečnostních incidentů, stejně jako zajišťovat odpovídající vzdělávání pracovníků.

Podle vyhlášky jsou povinnosti v oblasti kybernetické bezpečnosti vázány na konkrétní kategorie subjektů a podle jejich významu pro stát jsou určena různá opatření a požadavky. Například pro subjekty, které spravují kritickou infrastrukturu, vyhláška stanoví přísnější pravidla a kontrolní mechanismy.[84]

[83] *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. [online]. Zákony pro lidi. 2014. [cit. 2025-03-05] Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2014-181>

[84] *Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat*. [online]. Zákony pro lidi. 2018. [cit. 2025-03-05]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2018-82.>

10.3 Budapešťská úmluva o kyberkriminalitě

Budapešťská úmluva o kyberkriminalitě, přijatá v roce 2001 pod záštitou Rady Evropy, je první mezinárodní smlouvou zaměřenou na boj proti trestné činnosti spáchané pomocí počítačových systémů a digitálních technologií. Jejím cílem je harmonizovat právní rámec mezi státy pro efektivní boj proti kyberkriminalitě a zajištění mezinárodní spolupráce. Úmluva definuje trestné činy, jako je nelegální přístup k počítačovým systémům, počítačové podvody, poškození dat a šíření nelegálního obsahu (např. dětská pornografie) a zavádí pravidla pro mezinárodní právní pomoc a výměnu informací mezi státy. Tyto kroky jsou nezbytné, protože kyberkriminalita často nezná státní hranice a vyžaduje rychlou spolupráci mezi zeměmi.

Česká republika je signatářem úmluvy a ratifikovala ji, což vedlo k přizpůsobení národní legislativy v oblasti kyberkriminality, zejména v oblasti kybernetické bezpečnosti. V souladu s úmluvou ČR přijala opatření pro rychlé vyhledávání digitálních důkazů a zajištění mezinárodní pomoci při vyšetřování kyberkriminality. Úmluva také zajišťuje, že státy mohou mezi sebou efektivně spolupracovat při řešení složitých kybernetických incidentů.[85]

[85] *Úmluva o počítačové kriminalitě*. [online]. EUR-Lex. 2023. [cit. 2025-03-05]. Dostupné z WWW: <https://eur-lex.europa.eu/CS/legal-content/summary/convention-on-cybercrime.html?fromSummary=28.>

11 Dopady phishingu

Phishingové útoky představují závažnou hrozbu v oblasti kybernetické bezpečnosti, jelikož mohou mít významné dopady na jednotlivce i organizace.

Jedním z nejčastějších důsledků je krádež citlivých informací. Útočníci se snaží získat důvěrná data, například přihlašovací údaje, čísla platebních karet nebo osobní identifikační údaje, které mohou následně zneužít k finančním podvodům či krádeži identity. Jakmile se útočník dostane k těmto údajům, oběť může čelit vážným problémům, jako jsou neoprávněné transakce nebo dokonce zneužití její identity k dalším podvodům.[86]

Dalším významným důsledkem phishingu jsou finanční ztráty. Oběti často přicházejí o peníze buď přímým převodem na účty podvodníků, nebo prostřednictvím neoprávněných transakcí provedených s odcizenými platebními údaji. Firmy mohou být rovněž cílem útoků, kdy útočníci podvodně získají přístup k firemním bankovním účtům nebo k jiným finančním zdrojům. Tyto ztráty mohou být obrovské a v některých případech vést až k finančnímu kolapsu společnosti.[87]

Phishingové útoky často vedou také k instalaci škodlivého softwaru na zařízení oběti. Stačí, aby uživatel klikl na odkaz v podvodném e-mailu nebo si stáhl infikovanou přílohu, a do jeho zařízení se může dostat malware. Tento škodlivý software může mít různé účinky – od špehování aktivit uživatele, přes ztrátu dat, až po využití napadeného zařízení k dalším útokům na jiné osoby nebo organizace.[88]

Kromě přímých finančních a technických dopadů mohou mít phishingové útoky i vážné následky pro pověst organizací. Pokud se firma stane obětí phishingu a uniknou jí citlivá data zákazníků nebo obchodních partnerů, může dojít ke ztrátě důvěry a poškození její reputace. To může mít dlouhodobé negativní dopady na vztahy se zákazníky a partnery, což v konečném důsledku ovlivní i její hospodářské výsledky.[89]

---

[86] *Co je phishing?* [online]. Avast. 2025. [cit. 2025-03-03]. Dostupné z WWW: <https://www.avast.com/cs-cz/c-phishing?>

[87] Tamtéž

[88] DOLNÍČEK, L., *Phishing a jak se proti němu bránit? 6 osvědčených technik*. [online]. GoodAccess. 2022. [cit. 2025-03-03]. Dostupné z WWW: <https://www.goodaccess.com/cs-blog/phishing-co-to-je-obrana?>

[89] KRÁLOVÁ, M., *Jak odhalit phishingový útok a nenaletět podvodníkům.* [online]. CDC DATA. 2024. [cit. 2025-03-03]. Dostupné z WWW: <https://www.cdc.cz/cs/jak-odhalit-phishingovy-utok-a-nenaletet-podvodnikum/.>

V některých případech mohou mít phishingové útoky i právní důsledky. Pokud například dojde k úniku citlivých informací kvůli nedostatečné ochraně dat, může být firma vystavena právním postihům a sankcím. Regulace na ochranu osobních údajů, jako je například GDPR v Evropské unii, ukládají organizacím povinnost zajistit odpovídající bezpečnostní opatření. Pokud tato opatření nejsou dodržována, hrozí vysoké pokuty a další právní důsledky.[90]

Vzhledem k těmto rizikům je důležité, aby jednotlivci i organizace věnovali dostatečnou pozornost ochraně před phishingovými útoky, neboť tím lze výrazně snížit pravděpodobnost úspěšného phishingového útoku a minimalizovat tak jeho dopady.

[90] KRÁLOVÁ, M., *Jak odhalit phishingový útok a nenaletět podvodníkům.* [online]. CDC DATA. 2024. [cit. 2025-03-03]. Dostupné z WWW: <https://www.cdc.cz/cs/jak-odhalit-phishingovy-utok-a-nenaletet-podvodnikum/.>

12 Praktická část

Praktická část bakalářské práce se týká široké veřejnosti a má za cíl prozkoumat povědomí osob o problematice phishingových útoků, tedy zjistit, jak často se lidé setkávají s touto formou kybernetických útoků a jaká je nejčastější užívaná forma těchto útoků. Dále se zde nachází několik doporučení a návrhů obranných strategií proti phishingu.

K získání dat bylo užito dotazníkového šetření prostřednictvím internetových stránek vyplnto.cz. Dotazník byl sestaven z patnácti otázek, přičemž u jedenácti otázek musel respondent vybrat jednu nejvhodnější odpověď určenou na základě osobního mínění a u zbylých čtyř otázek mu byla dána možnost zvolení více možností. Všechny otázky byly povinné, a tak dotazovaný musel vyplnit všechny otázky, aby se jeho odpovědi započetly do získaných dat.

Před vyplněním byl každý respondent seznámen s daným tématem dotazníku a upozorněn na to, že se jedná o anonymní dotazníkové šetření, které bude užito pouze k vypracování této bakalářské práce. Dotazník byl primárně distribuován prostřednictvím internetu na sociálních sítích a sekundární distribuce probíhala v okruhu známých, rodiny a kolegů sloužících v rámci útvarů Policie České Republiky.

Ke shromažďování dat docházelo v období od 26.11.2024 do 26.02.2025 a dotazník řádně vyplnilo 109 respondentů. Získaná data budou dále vyhodnocena a za užití statistické analýzy zpracována do grafů se zaokrouhlením na celá čísla a uvedením exaktních počtů respondentů v závorkách.

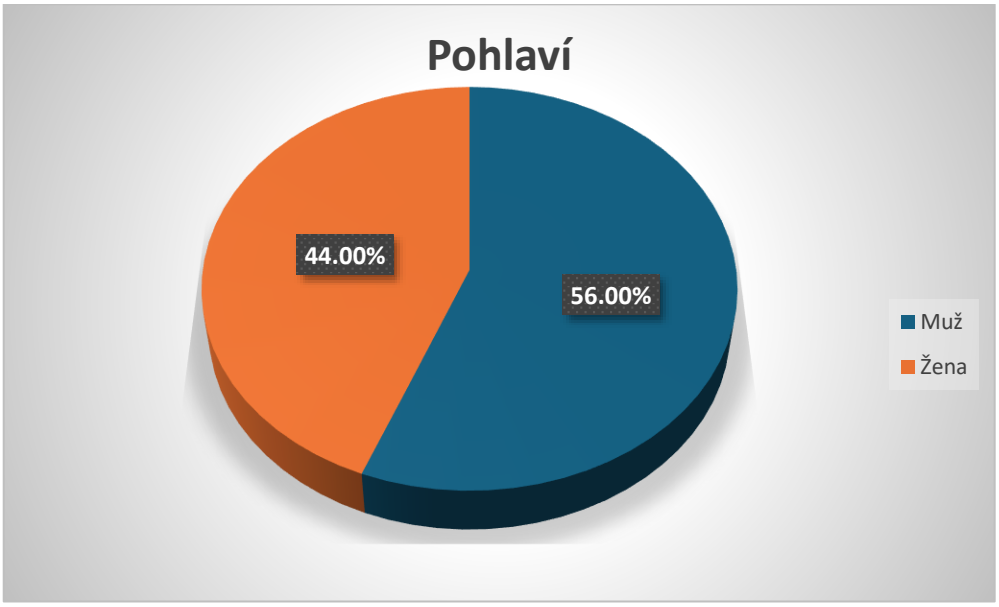
12.1 Hypotézy

Před distribucí dotazníku byly stanoveny tři hypotézy, které budou na základě získaných dat z dotazníkového šetření buďto ověřeny nebo vyvráceny.

- **Hypotéza č.1:** Většina respondentů se v minulosti setkala s phishingovým útokem.
- **Hypotéza č.2**: V rámci phishingového útoku bude nejvyšší četnost provedení prostřednictvím e-mailové adresy.
- **Hypotéza č.**3: Mezi respondenty bude převaha těch, kteří si nekontrolují, od koho obdrželi emailovou zprávu.

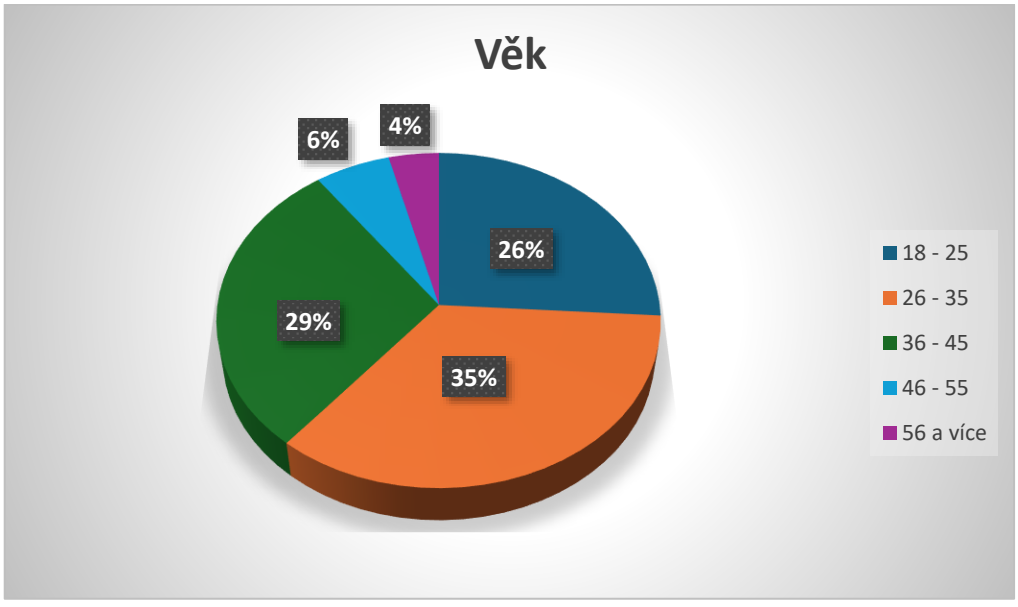
12.2 Vyhodnocení dat

Graf 1: Pohlaví.[91]



Dotazníkového šetření se zúčastnilo 109 respondentů z toho bylo 56 % (61) mužů a 44 % (48) žen.

Graf 2:Věk.[92]



V rámci dotazníku nás dále zajímá věk dotázaných, 26 % (28) z dotazovaných uvedlo, že je ve věku 18 – 25 let, dalších 35 % (38) bylo ve věku 26 – 35 let. 29 % (32)

[91] Zdroj: Vlastní zdroj
[92] Zdroj: Vlastní zdroj

osob zvolilo možnost, že jsou ve věku 36 – 45 let, 6 % (7) respondentů se nacházelo ve věkovém rozmezí od 46 – 55 let a nejméně, tedy 4 % (4) bylo osob ve věku 56 a více let.

Graf 3: Dosažené vzdělání.[93]

Jako nejvyšší dosažené vzdělání uvedlo 1 % (1) z dotázaných základní školu, střední odborné vzdělání s výučním listem dosáhlo 6 % (6) osob. Možnost střední odborné vzdělání s maturitou zvolilo 38 % (41) respondentů. 23 % (25) účastníků šetření uvedlo jako své nejvyšší dosažené vzdělání vyšší odborné. Bakalářské a magisterské vzdělání shodně uvedlo 17 % (18) z dotazovaných.

Graf 4: Slyšeli jste už o pojmu phishing?[94]

[93] Zdroj: Vlastní zdroj
[94] Zdroj: Vlastní zdroj

Respondenti se z velké většiny shodli na tom, že o pojmu phishing již v minulosti slyšeli, konkrétně tuto možnost zvolilo 87 % (95) z dotázaných a pouze 13 % (14) osob uvedlo, že o tomto pojmu neslyšeli.

Graf 5: Který z následujících popisů nejlépe odpovídá phishingu?[95]

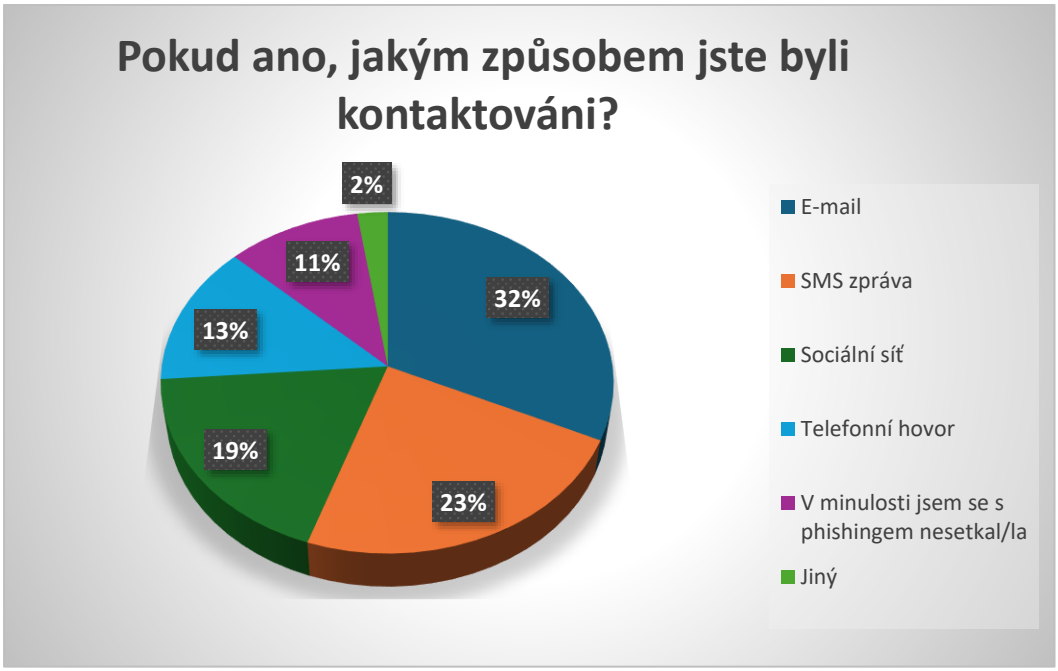
Většina respondentů zde zvolila odpověď, že pojem phishing nejlépe vystihuje možnost krádež osobních údajů pomocí podvodných e-mailů, tuto možnost zvolilo 87 % (95) z dotázaných. Možnost útok na počítačové systémy pomocí virů zvolilo 8 % (9) osob a poslední možnost, tedy zasílání masivních požadavků na server s cílem jeho přetížení jako správnou uvedlo 5 % (5) respondentů.

[95] Zdroj: Vlastní zdroj

Graf 6: Setkali jste se někdy s phishingovým útokem?[96]

71 % (77) z dotázaných uvedlo, že se již někdy s phishingovým útokem setkali, 20 % (22) respondentů uvedlo, že se s phishingovým útok nikdy nesetkali a 9 % (10) osob uvedlo, že si není jistý/á zda se s tímto v minulosti setkali, či nikoliv.

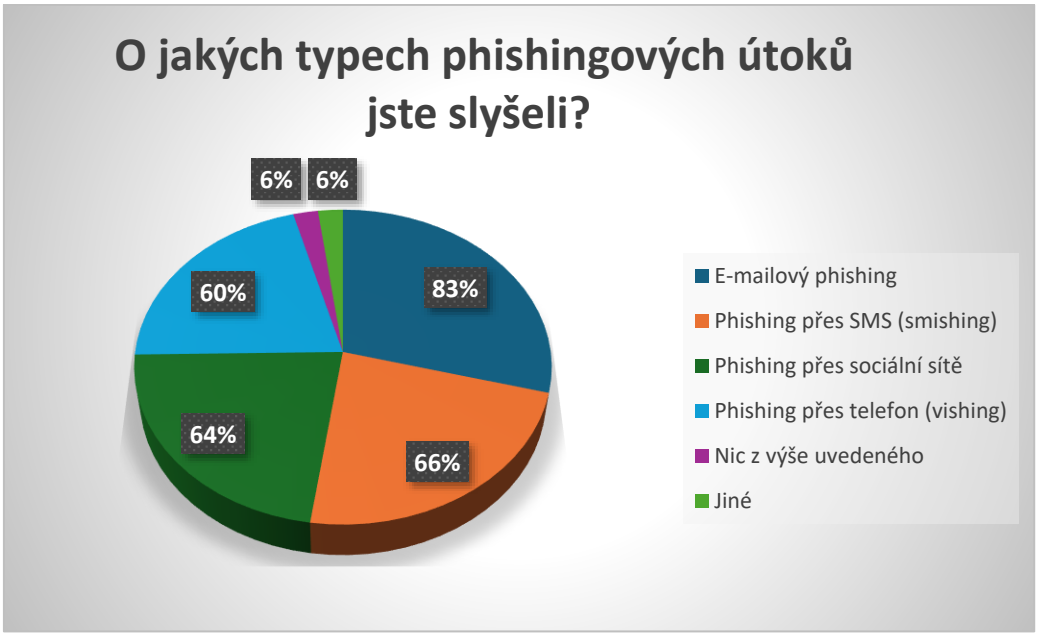
Graf 7: Pokud ano, jakým způsobem jste byli kontaktováni?[97]



[96] Zdroj: Vlastní zdroj
[97] Zdroj: Vlastní zdroj

67 % (73) respondentů uvedlo, že u nich došlo ke kontaktu s útočníky prostřednictvím e-mailu. Způsob kontaktování prostřednictvím SMS zprávy uvedlo 49 % (53) z dotázaných. 39 % (43) osob uvedlo, že byly zkontaktováni prostřednictvím sociálních sítí. Možnost telefonního hovoru uvedlo 28 % (30) účastníků dotazníkového šetření. 22 % (24) respondentů uvedlo, že se v minulosti nikdy s phishingem nesetkalo a 5 % (5) osob sdělilo, že bylo zkontaktování jiným způsobem, než bylo uvedeno v dotazu.

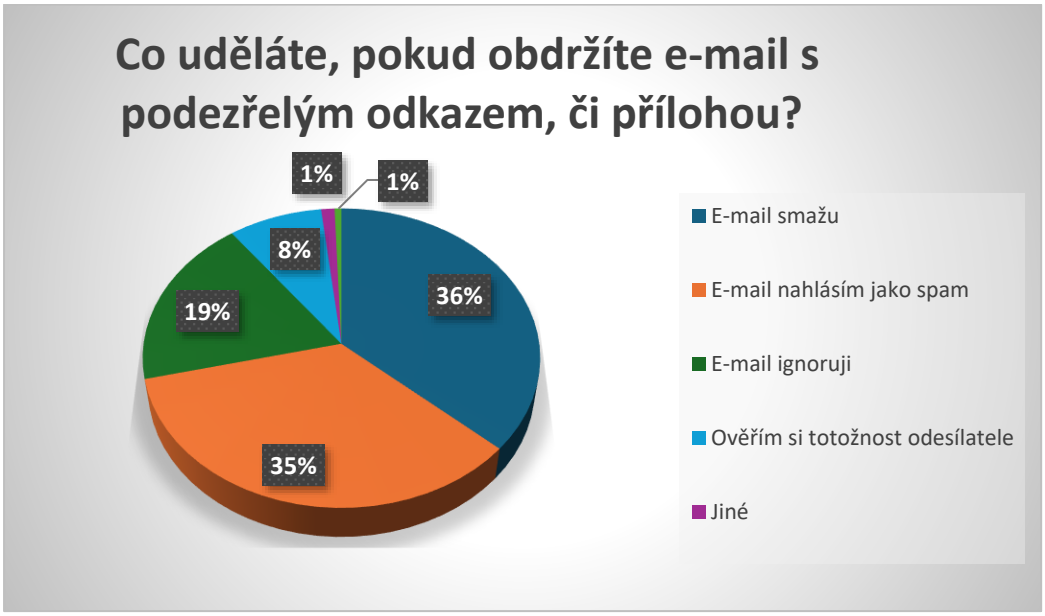
Graf 8: O jakých typech phishingových útoků jste slyšeli?[98]



Z grafu je patrné, že nejvíce respondentů zná e-mailový phishing, neboť tuto možnosti zvolilo 83 % (91) z dotázaných. 66 % (72) osob zná phishing přes SMS zprávu. 64 % (70) odpovědí byla možnost phishingu přes sociální sítě a 60 % (65) z dotazovaných je obeznámena s phishingem přes telefonní hovor. Dále 6 % (7) uvedlo, že neslyšelo o žádném z výše uvedených typů útoků a 6 % (6) zvolilo možnost jiné.

[98] Zdroj: Vlastní zdroj

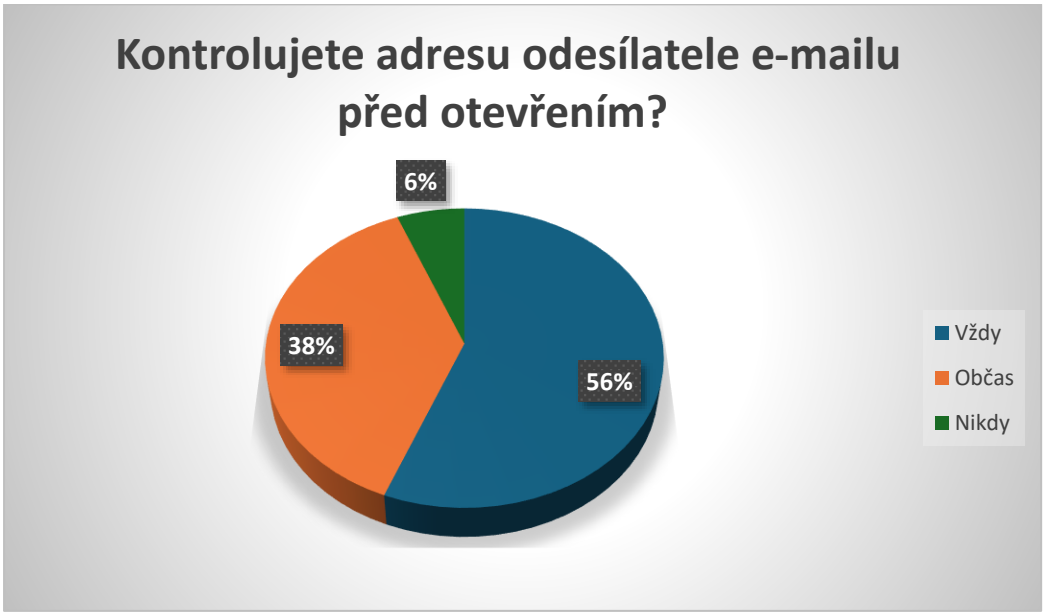
Graf 9: Co uděláte, pokud obdržíte e-mail s podezřelým odkazem, či přílohou?[99]



61 % (66) respondentů uvedlo, že e-mail smaže, 58 % (63) z dotázaných zase podezřelý e-mail nahlásí jako spam. Možnost, že e-mail jednoduše ignorují zvolilo 31 % (34) z dotázaných a 14 % (15) osob si zase ověřuje totožnost odesílatele. 2 % (2) z dotazovaných zvolilo možnost jiné a 1 % (1) respondentů otevře přílohu, nebo klikne na odkaz v e-mailu.

[99] Zdroj: Vlastní zdroj

Graf 10: Kontrolujete adresu odesílatele e-mailu před otevřením?[100]



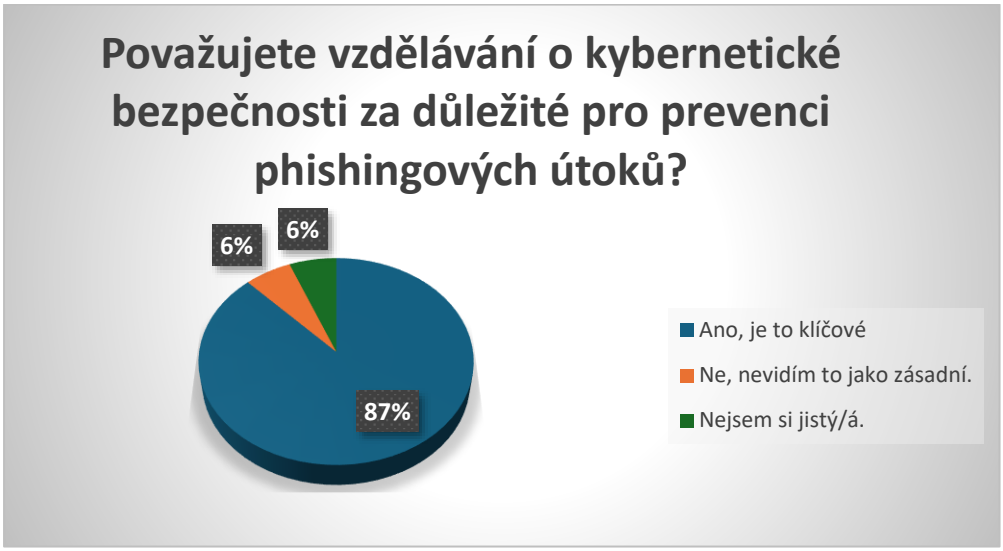
Většina respondentů, tedy 56 % (61) uvedla, že si vždy kontroluje adresu odesílatele e-mailu předtím, než ho otevře, avšak 38 % (41) osob si adresu odesílatele kontroluje jen občas a 6 % (7) z dotázaných toto nedělá nikdy.

Graf 11: Myslíte si, že je veřejnost dostatečně informována o phishingu? [101]

Většina z dotázaných, tedy 84 % (92), si myslí, že veřejnost není dostatečně informována o phishingu, avšak 16 % (17) osob si myslí, že ano.

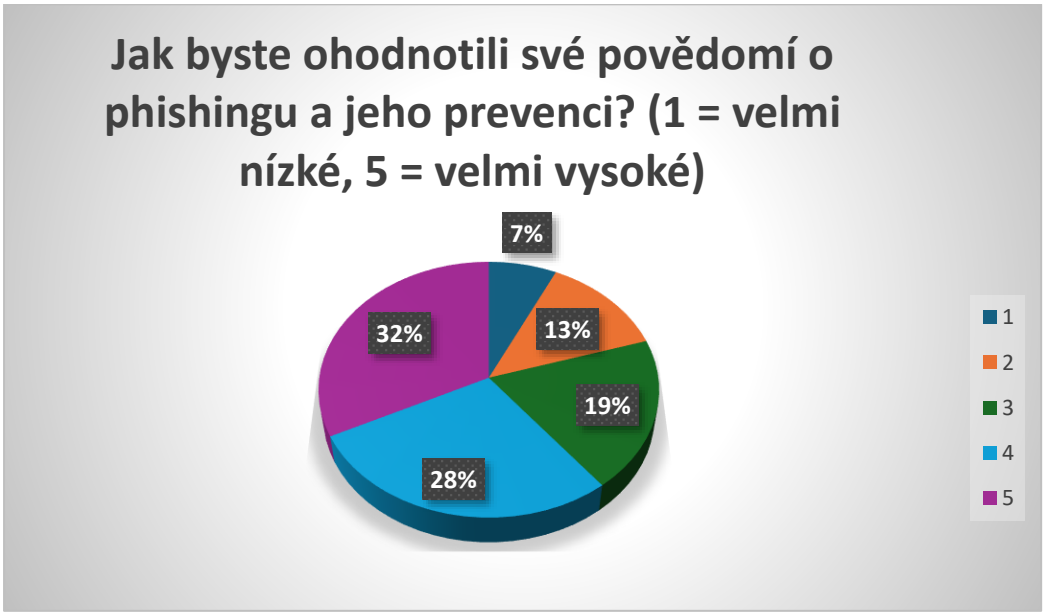
[100] Zdroj: Vlastní zdroj
[101] Zdroj: Vlastní zdroj

Graf 12: Považujete vzdělávání o kybernetické bezpečnosti za důležité pro prevenci phishingových útoků?[102]



87 % (95) respondentů si myslí, že vzdělávání o kybernetické bezpečnosti je klíčové pro prevenci phishingových útoků. Zbylý dotázaní, tedy 6 % (7) osob, shodně uvedlo, že vzdělání není klíčové jako prevence, nebo že si nejsou jistí.

Graf 13: Jak byste ohodnotili své povědomí o phishingu a jeho prevenci? (1 = velmi nízké, 5 = velmi vysoké)[103]



[102] Zdroj: Vlastní zdroj
[103] Zdroj: Vlastní zdroj

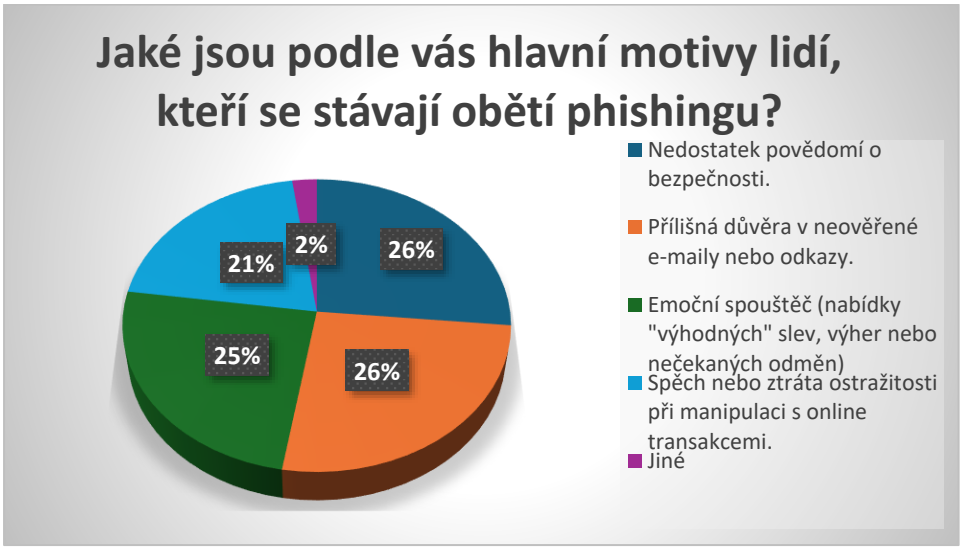
7 % (8) respondentů si myslí, že má velmi nízké povědomí o phishingu a tedy zvolilo možnost 1. Nízké povědomí uvedlo 13 % (14) z dotázaných a zvolilo tedy možnost 2. Průměrné znalosti o phishingu uvedlo nejvíce dotázaných 32 % (35) a zvolilo možnost 3. 28 % (31) osob uvedlo, že má vysoké vědomosti ohledně phishingu a tedy zvolilo možnost 4. Možnost 5, tedy velmi vysoké povědomí uvedlo 19 % (21) respondentů.

Graf 14: Kde jste se dozvěděli o phishingu?[104]

Nejvíce respondentů, tedy 47 % (51) , uvádělo, že se o phishingu dozvědělo prostřednictvím svého zaměstnání. Druhá nejčastěji volená odpověď se 17 % (19) byla Média. Volbu vlastní zkušenost zvolilo 14 % (15) osob. 11 % (12) z dotázaných uvedlo jako možnost školu. 6 % (7) respondentů uvedlo, že se o phishingu dozvědělo až díky tomuto dotazníku a možnost jiné zvolilo 5 % (5) osob.

[104] Zdroj: Vlastní zdroj

Graf 15: Jaké jsou podle vás hlavní motivy lidí, kteří se stávají obětí phishingu?[105]



Nejvíce respondentů si myslí, že hlavní motiv lidí, kteří se stávají obětí phishingu je nedostatek povědomí o bezpečnosti, tuto možnost zvolilo 71 % (77) osob. Druhá nejčastěji volená možnost s 70 % (76) byla přílišná důvěra v neověřené e-maily nebo odkazy. 66 % (72) z dotázaných si myslí, že je to nějaký emoční spouštěč. Možnost spěch nebo ztráta ostražitosti při manipulaci s online transakcemi zvolilo 55 % (60) respondentů a 6 % (7) z dotazovaných zvolilo možnost jiné.

12.3 Diskuze

Na začátek dotazníkového šetření byly nejprve zjišťovány informace o respondentech. Konkrétně se jednalo o pohlaví, věk a nejvyšší dosažené vzdělání. Na toto byly vypracovány dotazy jedna až tři.

Vyhodnocením dotazu číslo jedna „Jaké je Vaše pohlaví?“bylo zjištěno, že více účastníků průzkumu bylo mužského pohlaví, konkrétně se jednalo o 56 % (61) osob a zbytek, tedy 44 % (48) z respondentů bylo žen.

Na základě dat z dotazu číslo dva „Kolik je Vám let?“ bylo zjištěno, že nejvíce účastníků bylo ve věkovém rozmezí od 26 – 35 let. Jednalo se o 35 % (38) z dotázaných. Na druhém místě byl věk v rozmezí od 36 – 46 let, tuto možnost zvolilo 29 % (32) osob. Tímto bylo zjištěno, že dotazník byl vyplňován většinově z řad mladší generace, což může

[105] Zdroj: Vlastní zdroj

značně ovlivnit výsledky. Mladší generace má totiž ke kybernetické kriminalitě a obecně k technologiím často blíže než generace starší.

Data ze třetího dotazu „Jaké je Vaše nejvyšší dosažené vzdělání?“ poukazují na to, že se průzkumu účastnili lidé s průměrnou až vyšší úrovní vzdělání. Úplné střední vzdělání uvedlo jako své nejvyšší dosažené vzdělání 38 % (41) z dotázaných. Na druhém místě byla možnost vyššího odborného vzdělání, tuto možnost uvedlo 23 % (25) osob. Na třetím místě bylo shodně uváděno Bakalářské a Magisterské vzdělání s 17 % (18).

Na základě získaných dat z grafu číslo čtyři „Slyšeli jste už o pojmu phishing?“ můžeme říct, že většina respondentů, tedy 87 %, je obeznámena s pojmem phishing. Toto však může být způsobeno i tím, že ačkoliv primární distribuce dotazníku probíhala pomocí sociálních sítí a až sekundární distribuce byla v rámci jednotlivých složek policie, tak mohlo dojít k tomu, že dotazník nakonec vyplnilo více příslušníků policie než civilních občanů, a to na základě kolegiality příslušníků policie a nevůli široké veřejnosti k náhodným dotazníkům.

Na výše uvedené tvrzení poukazuje i fakt, že v rámci dotazu číslo čtrnáct “Kde jste se dozvěděli o phishingu?“ je nejvyšší četnost volené odpovědi 47 % (51) ze zaměstnání, což je skoro polovina respondentů. Avšak je pravdou, že se může jednat pouze o souhru náhod a respondenti se k našemu tématu skutečně dostali skrze jiné zaměstnání než je služba u policie. Díky tomu, že se jednalo o anonymní dotazník, tak v současné době není možnost, jak si toto tvrzení zpětně ověřit či ho vyvrátit.

Na dotaz číslo čtyři byl sestaven navazující dotaz číslo pět “Který z následujících popisů nejlépe odpovídá phishingu?“ ke zjištění, zda respondenti, kteří již o pojmu phishing slyšeli, jsou obeznámeni s tím, co tento pojem znamená. Ze získaných dat je zjištěno, že 87 % z dotázaných nejen že o pojmu slyšeli, ale ví, co tento pojem znamená. Na základě dotazu číslo čtyři a pět je tedy zřejmé, že pouze 13 % účastníků průzkumu nemá o projednávaném tématu žádné informace.

Dotaz číslo jedenáct, dvanáct a třináct byl věnován povědomí a vzdělání ohledně phishingu.

Ze získaných dat z dotazu číslo jedenáct „Myslíte si, že je veřejnost dostatečně informována o phishingu?“, je patrné, že veřejnost si nemyslí, že by toto téma bylo dostatečně známé, možnost ne zvolila drtivá většina z dotázaných, konktrétně 84 % (92).

Pouze 16 % (17) respondentů si myslí, že veřejnost je informována dostatečně. Z tohoto můžeme říct, že i přes veškeré informační kampaně a snahy státu o osvětu tohoto tématu si široká veřejnost nemyslí, že je informována dostatečně.

V rámci dotazu číslo dvanáct „Považujete vzdělávání o kybernetické bezpečnosti za důležité pro prevenci phishingových útoků?“, který navazuje na dotaz předchozí, bylo opět skoro jednoznačně ukázáno, že si respondenti myslí, že se jedná o klíčový prvek v boji proti phishingu a tuto odpověď zvolilo 87 % (95) z dotázaných. Toto jen opět poukazuje na to, jak je vzdělání v této oblasti klíčové a spolu s předchozím dotazem nám to tedy říká, že se jedná o důležitý aspekt v boji proti phishingu, avšak informací je poskytováno málo.

Co se týče dotazu číslo třináct „Jak byste ohodnotili své povědomí o phishingu a jeho prevenci? (1 = velmi nízké, 5 = velmi vysoké)“ tak zde bylo odpovídáno velmi nejednoznačně. Jedná se o subjektivní názor, který ne vždy reflektuje skutečnou úroveň znalostí respondenta. Nejčastěji volená odpověď byla číslo 3, a tedy respondent se domnívá, že má průměrné znalosti o řešené problematice. Tuto možnost zvolilo 32 % (35) osob. Druhá nejčastější volená odpověď je číslo 4, tedy vysoké povědomí o phishingu, zvolilo jí 28 % (31) respondentů. Následující nejčastěji volná odpověď byla číslo 5, což zastupuje velmi vysoké povědomí o phishingu, možnost zvolilo 19 % (21) dotázaných.

Závěr z dat získaných z dotazů jedenáct až třináct je poněkud paradoxní. Záleží však na tom, jak celou situaci vnímá čtenář. Paradox spočívá především v tom, že většina respondentů uvedla, že veřejnost je nedostatečně informována o phishingu, avšak když byli dotázáni na své vlastní znalosti, většinou uváděli, že jejich úroveň je vysoká až velmi vysoká, ačkoli právě oni v našem dotazníku zastupovali veřejnost.

V rámci otázky číslo patnáct „Jaké jsou podle vás hlavní motivy lidí, kteří se stávají obětí phishingu?“ mohli respondenti zvolit vícero možností. Zde všechny autorem uvedené možnosti, měli veliké procento volených odpovědí. Nejvyšší četnost volené odpovědi byla u možnosti „Nedostatek povědomí o bezpečnosti“ zvolilo jí 71 % (77) účastníků. Následující možnosti „Přílišná důvěra v neověřené e-maily nebo odkazy“, „Emoční spouštěč (nabídky "výhodných" slev, výher nebo nečekaných odměn)“ a „Spěch nebo ztráta ostražitosti při manipulaci s online transakcemi“ volilo vždy přes 55 % respondentů. A možnost „Jiné“ zvolilo pouze 6 % (7) respondentů. Toto poukazuje

hlavně na fakt, že mnoho respondentů volilo vícero možností. Díky tomu lze usuzovat, buď to, že se mnohdy jedná o kombinaci více faktorů, nebo že respondenti považují danou problematiku za složitější a multifaktorovou, než by naznačovaly jednotlivé, autorem volené, volby. Takové výsledky naznačují, že otázky nejsou vždy jednoduché a mohou mít více než jednu příčinu či důsledek, což odráží komplexitu situace, kterou se snažíme analyzovat.

12.4 Vyhodnocení hypotézy č. 1

První hypotéza předpokládá, že většina respondentů se v minulosti setkala s phishingovým útokem. Na ověření této hypotézy byl sestaven dotaz číslo šest „Setkali jste se někdy s phishingovým útokem?“ Na základě získaných dat bylo zjištěno, že ze 109 respondentů odpovědělo 71 %, tedy 77 osob, že se s tímto typem kybernetického útoku již v minulosti setkalo, což jednoznačně potvrzuje tuto hypotézu.

9 % z dotázaných, tedy 10 osob uvedlo, že si nejsou jistí, zda se s tímto útokem již v minulosti setkali. Což jen poukazuje na možnost, že zjištěné procento osob, které se s tímto fenoménem setkali, může být ještě o něco vyšší.

12.5 Vyhodnocení hypotézy č. 2

Druhá hypotéza předpokládá, že i přes technologický rozvoj společnosti a vynalézání stále nových způsobů útoků, bude nejčastější provedení phishingového útoku skrz e-mailové adresy, a to i z toho důvodu, že je tento způsob pro útočníka nejméně technologicky a časově náročný.

Na ověření tohoto tvrzení byla sestavena otázka číslo sedm „…jakým způsobem jste byli kontaktováni?“. Jednalo se o dotaz, ve kterém respondent musel zvolit minimálně jednu odpověď, tedy mohl jich zvolit vícero. Ze získaných dat vyplývá, že ze 109 dotázaných bylo útočníky, pomocí e-mailu zkontaktováno 73 osob, tedy 67 % z účastníků průzkumného šetření, což byla nejčastěji volená odpověď. Druhá nejčastěji volená odpověď byl útok prostřednictvím SMS zprávy, tuto volilo 53 respondentů, tedy 49 %.

K dotazu číslo sedm byl dále sestaven navazující dotaz číslo osm „O jakých typech phishingových útoků jste slyšeli?“ Opět se jednalo o dotaz, ve kterém respondent musel zvolit minimálně jednu odpověď, tedy mohl jich zvolit vícero. Ačkoliv se tento dotaz přímo netýkal stanovené hypotézy, bylo jím zjišťováno povědomí o jednotlivých typech útocích. Ze získaných dat je patrné, že ze 109 respondentů o e-mailovém phishingu

slyšelo 91 osob, což je 83 % z dotázaných a jedná se o nejčastěji volenou odpověď. Druhá nejčastěji volená odpověď byla phishing přes SMS zprávu tuto zvolilo 66 % (72) respondentů.

Na základě výše uvedeného nejen že se nám potvrdila druhá hypotéza, tedy že nejčastější provedení phishingového útoku bude skrz e-mailové adresy, ale zároveň jsme díky navazujícímu dotazu číslo osm zjistili, že se také jedná o nejznámější druh pshishingového útoku. Dále je z dat patrno, že druhý nejčastější a nejznámější phishingový útok je skrze SMS zprávy.

12.6 Vyhodnocení hypotézy č. 3

Třetí hypotéza je stanovena tak, že mezi respondenty bude převaha těch, kteří si nekontrolují, od koho obdrželi emailovou zprávu. Na ověření této hypotézy byl sestaven dotaz číslo deset „Kontrolujete adresu odesílatele e-mailu před otevřením?“ Vyhodnocením získaných dat bylo zjištěno, že ze 109 osob zvolilo 56 % (61) možnost vždy. Tedy že před každým otevřením e-mailu ověřují e-mailovou adresu odesílatele. 38 % (41) respondentů uvedlo, že adresu odesílatele kontrolují občas a zbylých 6 % (7) uvedlo, že adresu nekontrolují nikdy. Získanými daty byla tato hypotéza vyvrácena.

13 Doporučení a návrhy obranných strategií proti phishingu

S rostoucí digitalizací a propojeností online světa se phishing stává čím dál sofistikovanějším a obtížněji rozpoznatelným. Proto je klíčové nejen rozumět tomu, jak phishing funguje, ale především vědět, jak se mu efektivně bránit. Efektivní obrana proti phishingu spočívá v kombinaci technických opatření, osvěty uživatelů a správných bezpečnostních návyků.

13.1 Prevence a osvěta uživatelů

Jedním z nejúčinnějších způsobů obrany proti phishingu je vzdělávání uživatelů. I když existuje řada technických opatření, lidský faktor zůstává jedním z nejslabších článků v oblasti kybernetické bezpečnosti. Útočníci často využívají psychologické triky, jako je časový nátlak, vyvolání strachu nebo zvědavosti, aby přiměli uživatele ke kliknutí na škodlivý odkaz nebo otevření infikované přílohy.

Školení a simulované phishingové testy

- Organizace by měly pravidelně školit zaměstnance o hrozbách phishingu a ukazovat jim reálné příklady podvodných e-mailů.
- Simulované phishingové útoky pomáhají testovat, jak uživatelé reagují na podezřelé e-maily, a umožňují identifikovat slabá místa v bezpečnostním povědomí.
- Vzdělávací kampaně by měly být průběžné, nikoli jednorázové, a zahrnovat aktuální trendy v phishingových útocích.

Jak rozpoznat phishingový útok

Uživatelé by měli vědět, na jaké znaky si dát pozor:

- Podezřelé e-mailové adresy – phishingové e-maily často pocházejí z adres, které se snaží napodobit legitimní organizace, ale obsahují drobné odchylky.
- Gramatické chyby a špatný jazyk – mnoho phishingových zpráv má špatně přeložený nebo nesrozumitelný text.
- Neobvyklé požadavky – například žádosti o resetování hesla, zaslání osobních údajů nebo nečekané faktury.

- Naléhavost – útočníci často vytvářejí tlak na okamžité jednání (například „Váš účet bude deaktivován do 24 hodin!“).

13.2 Technická opatření

Kromě vzdělávání uživatelů je důležité zavést i technická opatření, která pomáhají phishingovým útokům předcházet nebo minimalizovat jejich dopad.

Antiphishingové filtry a antivirový software

- Použití bezpečnostního softwaru, který automaticky detekuje a blokuje podezřelé e-maily a webové stránky.
- Aktivace pokročilých filtrů pro e-mailové služby, které dokážou označit nevyžádanou nebo potenciálně nebezpečnou poštu.

Dvoufaktorová autentizace (2FA)

- I pokud útočník získá přihlašovací údaje oběti, 2FA přidává další bezpečnostní vrstvu tím, že vyžaduje dodatečné ověření (například kód zaslaný na mobilní telefon).
- Doporučuje se využívat bezpečné metody ověřování, například aplikace jako Google Authenticator.

Použití bezpečnostních protokolů

- **SPF, DKIM, DMARC** – ověřovací protokoly pro e-mailové servery, které pomáhají zabránit podvrženým e-mailům.
- **HTTPS a SSL/TLS šifrování** – zajistí bezpečnou komunikaci mezi uživatelem a serverem.

13.3 Bezpečné chování na internetu

Správné bezpečnostní návyky jsou klíčové pro prevenci phishingových útoků.

Opatrnost při otevírání e-mailů a příloh

- Nikdy neklikat na odkazy v e-mailech od neznámých odesílatelů.
- Ověřit si pravost e-mailu přímo na oficiálních stránkách organizace namísto klikání na odkazy.

Používání správců hesel

- Správci hesel umožňují generovat silná, unikátní hesla pro každou službu a ukládat je bezpečně.
- Používání jednoho hesla pro více služeb zvyšuje riziko úspěšného phishingového útoku.

13.4 Reakce na phishingový útok

Ani nejlepší prevence nezaručuje, že se phishingový útok nikdy neuskuteční. Proto je důležité mít připravený krizový plán.

Okamžitá reakce při podezření na phishing

- Pokud uživatel klikne na podezřelý odkaz nebo poskytne citlivé údaje, měl by okamžitě změnit heslo.
- Informovat IT oddělení nebo poskytovatele služby, aby mohli podniknout kroky k ochraně účtu.
- Provést antivirovou kontrolu zařízení.

Nahlášení phishingu

- Phishingové e-maily lze nahlásit přímo e-mailovým poskytovatelům (např. Gmail, Outlook).
- V České republice lze phishing hlásit na bezpečnostní týmy jako CSIRT.CZ nebo NÚKIB.

13.5 Modelový případ phishingové obrany

Jana pracuje jako účetní ve středně velké firmě a denně vyřizuje e-maily od dodavatelů i klientů. Jednoho dne obdrží zprávu, která se tváří jako oficiální e-mail od banky, se kterou její firma spolupracuje. E-mail obsahuje oficiálně vypadající logo a profesionálně napsaný text, který ji informuje, že její firemní bankovní účet byl z bezpečnostních důvodů dočasně zablokován. Pro jeho opětovné zpřístupnění je podle zprávy nutné, aby klikla na přiložený odkaz a přihlásila se do svého internetového bankovnictví.

Jana si nejprve chce být jistá, že se skutečně jedná o pravý e-mail, proto věnuje pozornost jeho detailům. Jako první se podívá na e-mailovou adresu odesílatele. Na první

pohled vypadá věrohodně, ale při bližším prozkoumání zjistí, že místo oficiální domény banky, která vždy končí na @bank.cz, je v adrese uvedena podezřelá doména @bank-security.com. To jí připadá zvláštní, protože ví, že banky obvykle nepoužívají odlišné domény pro komunikaci se zákazníky.

Dalším krokem, který Jana udělá, je zkontrolování odkazu, na který má podle pokynů v e-mailu kliknout. Místo toho, aby na něj rovnou klikla, na něj pouze najede kurzorem myši. V levém dolním rohu obrazovky se jí zobrazí skutečná URL adresa, kam by ji odkaz přesměroval. Vidí, že adresa neodpovídá oficiálním webovým stránkám banky, ale místo toho obsahuje podivnou kombinaci slov "bank-login-secure.com", což se jí zdá podezřelé. Jana si vzpomene na pravidla kybernetické bezpečnosti, která se naučila na školení ve firmě, a ví, že banka nikdy neposílá odkazy k přímému přihlášení přes e-mail.

Namísto toho, aby riskovala a na odkaz klikla, se rozhodne zavolat přímo na oficiální zákaznickou linku banky. Na infolince se spojí s pracovníkem podpory a vysvětlí mu situaci. Zaměstnanec banky ji ujišťuje, že s jejím účtem je vše v pořádku a že banka nikdy neposílá takovéto požadavky přes e-mail. Potvrzuje, že se jedná o phishingový útok, a doporučí jí, aby e-mail nahlásila jako nebezpečný.

Jana okamžitě informuje bezpečnostní oddělení své firmy a přepošle jim podezřelý e-mail k analýze. IT specialisté ve firmě následně rozešlou varování všem zaměstnancům, aby si dávali pozor na tento typ podvodných zpráv. Navíc vedení firmy rozhodne o dalším školení zaměstnanců v oblasti kybernetické bezpečnosti, aby si byli vědomi hrozeb a uměli je správně rozpoznat.

Díky své obezřetnosti a správnému rozhodnutí Jana phishingový útok úspěšně odvrátila. Kdyby na odkaz klikla a zadala své přihlašovací údaje, útočníci by mohli získat přístup k jejímu bankovnímu účtu a způsobit firmě značné finanční škody. Tento případ jasně ukazuje, jak důležité je věnovat pozornost detailům, neklikat bezmyšlenkovitě na odkazy v e-mailech a v případě pochybností si vždy informace ověřit přímo u instituce, která údajně e-mail odeslala.

Jana si uvědomuje, že i když phishingové e-maily mohou být stále sofistikovanější a vizuálně dokonalejší, existují způsoby, jak se jim bránit. Kontrola e-mailové adresy, ověření odkazu před kliknutím, telefonické potvrzení u dané instituce a obezřetné chování na internetu jsou klíčovými kroky k ochraně před kybernetickými hrozbami. Tento

incident pro ni byl cennou zkušeností a díky své opatrnosti nejen ochránila citlivé údaje, ale také pomohla informovat kolegy o aktuálních hrozbách a zvýšit celkovou bezpečnost ve firmě.

Závěr

Tato bakalářská práce se zaměřila na problematiku phishingových útoků, jejich metody, způsoby prevence a možnosti efektivní obrany. Cílem bylo nejen analyzovat, jak útočníci manipulují své oběti k získání citlivých údajů, ale také zjistit úroveň povědomí veřejnosti o tomto druhu kybernetického útoku. V rámci praktické části byl realizován průzkumný dotazník, jehož výsledky poskytly cenné informace o informovanosti a zkušenostech respondentů s phishingem.

Výsledky dotazníku ukázaly, že většina respondentů o phishingu již slyšela a dokázala určit, které konkrétní jednání tento pojem zahrnuje, což naznačuje rostoucí povědomí o kybernetických hrozbách. Značná část respondentů si uvědomuje riziko phishingu, což potvrzuje i fakt, že většina lidí uvedla, že by při obdržení podezřelého e-mailu s neznámým odkazem nebo přílohou jednala obezřetně.

Co se týče osobních zkušeností s phishingem, velmi malá část respondentů uvedla, že se s takovým útokem nesetkala, což opět poukazuje na rostoucí trend kybernetické kriminality obecně. Nejčastěji byli kontaktováni prostřednictvím e-mailu, ale objevily se i případy telefonických podvodů (vishingu) a podvodných zpráv na sociálních sítích (smishingu).

Jedním z důležitých zjištění bylo, že ne všichni respondenti pravidelně kontrolují adresu odesílatele před otevřením e-mailu, což je jedním ze základních způsobů, jak odhalit potenciálně nebezpečné zprávy. Přesto většina dotázaných vnímá vzdělávání v oblasti kybernetické bezpečnosti jako důležitý prvek prevence proti phishingu a považuje veřejnou informovanost za klíčový faktor v boji proti těmto útokům. Na škále hodnocení svého vlastního povědomí o phishingu a jeho prevenci se většina respondentů pohybovala ve středních hodnotách, což naznačuje, že lidé si jsou vědomi existence hrozby, avšak nemusí mít dostatek detailních znalostí o konkrétních metodách ochrany.

Získané poznatky potvrzují, že i přes rostoucí povědomí o phishingu je stále nutné zaměřit se na efektivnější vzdělávání a prevenci. Doporučením je nejen pravidelně informovat veřejnost o nových metodách útoků, ale také podporovat používání bezpečnostních opatření, jako je dvoufaktorové ověřování, důsledná kontrola e-mailových adres odesílatelů a kritické zhodnocení obsahu zpráv. Phishingové útoky se neustále vyvíjejí a je proto nezbytné, aby bezpečnostní opatření i úroveň znalostí uživatelů držely krok s novými hrozbami.

Tato práce tak přispěla k lepšímu pochopení phishingových útoků a ukázala, jak důležitou roli hraje informovanost a preventivní opatření v ochraně před touto formou kybernetické kriminality. Budoucí výzkumy by se mohly zaměřit na zlepšení metod osvěty a na vývoj nových strategií detekce phishingových útoků, které by pomohly snížit počet jejich úspěšných obětí.

Seznam použitých zdrojů

Literární zdroje

1. Al-Daeef, M., Basir, N. a Saudi, M., Security Awareness Training: A Review. In: *Proceedings of the World Congress on Engineering 2017 Vol I.* IAENG: London, U.K., 2017. 472 s. ISBN 978-988-14047-4-9.
2. DIJCK, J., *The culture of connectivity: a critical history of social media*. New York: Oxford University Press, 2013, 228 s. ISBN 978-0-19-997078-0.
3. GŘIVNA, T., a POLČÁK, R., *Kyberkriminalita a právo*. Praha: Auditorium, 2008. 220 s. ISBN 978-80-903786-7-4.
4. HOLT, T., BOSSLER, A. a SEIGFRIED-SPELLAR K., *Cybercrime and digital forensic: An introduction.Third edition*. New York, NY: Routlege, 2022. 790 s. ISBN 978-0-367-36007-8.
5. JELÍNEK, J., *Kriminologie.* Praha: Leges, 2021, 631 s. ISBN 978-80-7502-499-2.
6. JIRÁSEK, P., NOVÁK, L., a POŽÁR, J., *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 3. vyd. Praha: Policejní akademie ČR v Praze, 2015. 240 s. ISBN 978-80-7251-436-6.
7. KLIMEK, L., ZÁHORA, J., a HOLCR K., 2016. *Počítačová kriminalita v európskych súvislostiach*. Bratislava: Wolters Kluwer. 2016. 448 s. ISBN 978-80-8168-538-5.
8. KOLOUCH, J. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. 524 s. ISBN 978-80-88168-15-7.
9. Kolouch, J., Bašta, P. *Cybersecurity*. Praha: CZ.NIC, 2019. 560 s. ISBN 978-80-88168-31-7
10. KUCHTA, J., a VÁLKOVÁ, H., *Základy kriminologie a trestní politiky*. Praha: C.H. Beck, 2005, 544 s. ISBN 80-7179-813-4.
11. LAPÁČEK, J. *Poznáváme Internet: rychle hotovo!.* Brno: Computer Press, 2007. 212 s. ISBN 978- 80-251-1781-1.
12. NĚMEC, M., *Teorie a metodologie kriminalistiky pro magisterské studium*. Praha: Abook, 2018. 491 s. ISBN 978-80-906974-1-6.
13. PAVLÍČEK, A. *Nová média a sociální sítě*. Praha: Oeconomica, 2010, 181 s. ISBN 978-80-2451742-1.
14. Sak, P. *Úvod do teorie bezpečnosti*. Havlíčkův Brod: Petrklíč, 2018. 272 s. ISBN 978-80-7229-652-1

15. SMEJKAL, V., a RAIS, K., *Řízení rizik ve firmách a jiných organizacích*. 4.vyd. Praha: Grada Publishing, 2013, 488 s. ISBN 978-80-247-4644-9.
16. SMEJKAL, V., *Kybernetická kriminalita*, *3. vydání.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2022. 1158 s. ISBN 978-80-7380-849-5.
17. WALL, D. S. *Cybercrime. The Transformation of Crime in the Information Age.* Cambridge. Malden MA: Polity Press, 2007. 288 s. ISBN 978-0-7456-2735-9.

Elektronické zdroje

1. *Antivirus Software*. [online]. Toppr. 2025 [cit. 2025-02-16]. Dostupné z WWW: <https://www.toppr.com/guides/computer-science/computer-fundamentals/utility-software/antivirus-software/.>
2. AWATI, R., *Computer hardware*. [online]. TechTarget. 2021 [cit. 2025-02-03]. Dostupné z WWW: <https://www.techtarget.com/searchnetworking/definition/hardware.>
3. *Bezpečnost satelitních služeb*. [online]. Národní úřad pro kybernetickou a informační bezpečnost: NÚKIB. 2025. [cit. 2025-03-05]. Dostupné z WWW: <https://nukib.gov.cz/cs/galileo-prs/.>
4. *Co je Instagram?* [online]. Co je to? 2025. [cit. 2025-03-05]. Dostupné z WWW: <https://cojeto.superia.cz/software/instagram.php?.>
5. *Co je internet*. [online]. Správa sítě. 2022 [cit. 2025-01-12]. Dostupné z WWW: <https://www.sprava-site.eu/internet/.>
6. *Co je phishing?* [online]. Avast. 2025. [cit. 2025-03-03]. Dostupné z WWW: <https://www.avast.com/cs-cz/c-phishing?>
7. *Co je WhatsApp a jak jej používat na chytrém telefonu? Průvodce pro začátečníky*. [online]. MobilTown. 2025. [cit. 2025-03-05]. Dostupné z WWW: <https://www.mobiltown.cz/nastaveni/co-je-whatsapp-a-jak-jej-pouzivat-na-chytrem-telefonu-pruvodce-pro-zacatecniky/.>
8. *Computer hardware*. [online]. Geeks For geeks. 2023 [cit. 2025-02-03]. Dostupné z WWW: <https://www.geeksforgeeks.org/software-and-its-types/.>
9. DOLNÍČEK, L., *Phishing a jak se proti němu bránit? 6 osvědčených technik*. [online]. GoodAccess. 2022. [cit. 2025-03-03]. Dostupné z WWW: <https://www.goodaccess.com/cs-blog/phishing-co-to-je-obrana?>

10. *Domain name server (DNS) Hijacking*. [online]. Imperva. 2024 [cit. 2025-02-16]. Dostupné z WWW: <https://www.imperva.com/learn/application-security/dns-hijacking-redirection/.>
11. *Everything to Know About Phone Number Spoofing*. [online]. Kaspersky. 2025 [online]. Dostupné z WWW: <https://www.kaspersky.com/resource-center/preemptive-safety/phone-number-spoofing.>
12. *GALILEO, Příslušný orgán PRS (CPA)*. [online]. Národní úřad pro kybernetickou a informační bezpečnost: NÚKIB. 2025. [cit. 2025-03-05]. Dostupné z WWW: <https://nukib.gov.cz/cs/galileo-prs/program-galileo/.>
13. *History of Phishing: How Phishing Attacks Evolved From Poorly Constructed Attempts To Highly Sophisticated Attacks*. [online]. Phishprotection. 2025. [cit. 2025-02-06]. Dostupné z WWW: <https://www.phishprotection.com/resources/history-of-phishing.>
14. IBM. *What is a cyberattack?*. [online]. IBM. 2024 [cit. 2025-02-03]. Dostupné z WWW: <https://www.ibm.com/think/topics/cyber-attack.>
15. INFORMATION SECURITY OFFICE. *Social Engineering*. [online]. Carnegie Mellon University. 2025 [cit. 2025-02-03]. Dostupné z WWW: <https://www.cmu.edu/iso/aware/dont-take-the-bait/social-engineering.html.>
16. *Instagram: Vše, co potřebujete vědět o této populární aplikaci*. [online]. IGalerie. 2025. [cit. 2025-03-05]. Dostupné z WWW: <https://igalerie.cz/instagram-vse-co-potrebujete-vedet-o-teto-popularni-aplikaci/?.>
17. *IP Spoofing*. [online]. Imperva. 2024 [cit. 2025-02-16]. Dostupné z WWW: <https://www.imperva.com/learn/ddos/ip-spoofing/.>
18. *Kdy vznikl YouTube? Historie internetového giganta*. [online]. Safer internet. 2025. [cit. 2025-03-05]. Dostupné z WWW: <https://saferinternet.cz/kdy-vznikl-youtube-historie-internetoveho-giganta/.>
19. KOSINSKI, M., *What is smishing?* [online]. IBM. 2024 [cit. 2025-02-06]. Dostupné z WWW: <https://www.ibm.com/think/topics/smishing.>
20. KRÁLOVÁ, M., *Jak odhalit phishingový útok a nenaletět podvodníkům.* [online]. CDC DATA. 2024. [cit. 2025-03-03]. Dostupné z WWW: <https://www.cdc.cz/cs/jak-odhalit-phishingovy-utok-a-nenaletet-podvodnikum/.>

21. KRUPIČKA, J., *Kybernetická kriminalita*. [online]. Acta Universitatis Carolinae. 2012. ISSN 0323-0619. [cit. 2025-03-02]. Dostupné z WWW: <https://www.prf.cuni.cz/dokumenty-download/1404048928/.>
22. *Kybernetická bezpečnost*. [online]. Národní úřad pro kybernetickou a informační bezpečnost: NÚKIB. 2025. [cit. 2025-03-05]. Dostupné z WWW: <https://nukib.gov.cz/cs/kyberneticka-bezpecnost/. >
23. *Návod, jak poznat phishingové útoky*. [online]. GOV. 2025 [cit. 2025-02-16]. Dostupné z WWW: <https://portal.gov.cz/kam-dal/cesky-egovernment/navod-jak-poznat-phisingove-utoky.>
24. *O NÚKIB*. Národní úřad pro kybernetickou a informační bezpečnost: NÚKIB [online]. Česko: NÚKIB, [2017] [cit. 2022-03-05]. Dostupné z WWW: <https://www.nukib.cz/cs/o-nukib/>
25. *Ochrana utajovaných informací v ICT*. [online]. Národní úřad pro kybernetickou a informační bezpečnost: NÚKIB. 2025. [cit. 2025-03-05]. Dostupné z WWW: <https://nukib.gov.cz/cs/ochrana-ui-v-ict/.>
26. SATRAPA, P., *Deset let CESNETu*. [online]. Zpravodaj ÚVT MU. 2006. [cit. 2025-03-05]. Dostupné z WWW: <https://webserver.ics.muni.cz/zpravodaj/articles/517.html.>
27. *Social engineering techniques: 4 ways criminal outsiders get inside*. [online]. CSO. 2010 [cit. 2025-02-03]. Dostupné z WWW: <https://www.csoonline.com/article/2125205/social-engineering/social-engineering-techniques--4-ways-criminal-outsiders-get-inside.html>
28. *Social Media Phishing: A Primer*. [online]. InspiredeLearning. 2024 [cit. 2025-02-06]. Dostupné z WWW: <https://inspiredelearning.com/blog/social-media-phishing-prime.>
29. *Spear Phishing vs. Whaling: What Are the Differences?* [online]. LastPass. 2024 [cit. 2025-02-16]. Dostupné z WWW: <https://blog.lastpass.com/posts/spear-phishing-vs-whaling.>
30. *The History of Phishing*. [online]. Graphus. 2023 [cit. 2025-02-06]. Dostupné z WWW: <https://www.graphus.ai/blog/history-of-phishing/.>
31. TIWARI, D., *Cyberspace and its Meaning*. [online]. Vendatu. 2025 [cit. 2025-01-15]. Dostupné z WWW: <https://www.vedantu.com/commerce/introduction-to-cyberspace.>

32. *Top Phishing Statistics for 2025: Latest Figures and Trends*. [online]. StationX. 2024 [cit. 2025-02-06]. Dostupné z WWW: <https://www.stationx.net/phishing-statistics/.>
33. *Types of spoofing*. [online]. Malwarebytes. 2025 [cit. 2025-02-16]. Dostupné z WWW: <https://www.malwarebytes.com/spoofing.>
34. *Úmluva o počítačové kriminalitě*. [online]. EUR-Lex. 2023. [cit. 2025-03-05]. Dostupné z WWW: <https://eur-lex.europa.eu/CS/legal-content/summary/convention-on-cybercrime.html?fromSummary=28.>
35. VENKAT, K., *Enhance Your Digital Security with Strong Passwords*. [online]. Seton Hall University. 2024 [cit. 2025-02-16]. Dostupné z WWW: <https://www.shu.edu/technology/news/strengthening-your-digital-security-password-and-phishing-tips.html.>
36. VIGDERMAN, A., *How Does Antivirus Software Work?* [online]. Security.org. 2024 [cit. 2025-02-16]. Dostupné z WWW: <https://www.security.org/antivirus/how-does-antivirus-work/.>
37. *Vše o Facebooku: Kompletní průvodce pro začátečníky i profíky*. [online]. NeuroRestart. 2023. [cit. 2025-03-05]. Dostupné z WWW: <https://neurorestart.cz/socialni-site/vse-o-facebooku-kompletni-pruvodce-pro-zacatecniky-i-profiky/.>
38. *Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat*. [online]. Zákony pro lidi. 2018. [cit. 2025-03-05]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2018-82.>
39. *Whaling*. [online]. Cisco. 2023 [cit. 2025-02-16]. Dostupné z WWW: <https://www.cisco.com/site/us/en/learn/topics/security/what-is-a-whaling-attack.html#tabs-35d568e0ff-item-194f491212-tab.>
40. *What Is a Firewall?* [online]. Coursera. 2023 [cit. 2025-02-16]. Dostupné z WWW: <https://www.coursera.org/articles/what-is-firewall?utm_medium=sem&utm_source=gg&utm_campaign=b2c_emea_x_multi_ftcof_career-academy_cx_dr_bau_gg_pmax_gc_s1_en_m_hyb_23-12_x&campaignid=20858198824&adgroupid=&device=c&keyword=&matchtype=&network=x&devicemodel=&creativeid=&assetgroupid=6484888893&targetid=&extensionid=&placement=&gad_source=1&gclid=CjwKCAiAtsa9BhAKEiwAUZAszUcvRBVsv-UAcAFJ7migf5z0VAonOrNy-Dy0B_xhTZJKPCoHX4zO6xoCNzAQAvD_BwE.>

41. *What is a phishing attack?* [online]. Cloudflare. 2025. [cit. 2025-02-06]. Dostupné z WWW: <https://www.cloudflare.com/learning/access-management/phishing-attack/. >
42. *What Is Catfishing?* [online]. Fortinet. 2025 [cit. 2025-02-16]. Dostupné z WWW: <https://www.fortinet.com/resources/cyberglossary/catfishing.>
43. *What Is Phishing?* [online]. Proofpoint. 2025 [cit. 2025-02-06]. Dostupné z WWW: <https://www.proofpoint.com/us/threat-reference/phishing.>
44. *What Is Spam Filtering?* [online]. Fortinet. 2025 [cit. 2025-02-16]. Dostupné z WWW: <https://www.fortinet.com/resources/cyberglossary/spam-filters.>
45. *What is spear phishing? Definition and risks*. [online]. Kaspersky. 2025 [cit. 2025-02-16]. Dostupné z WWW: <https://www.kaspersky.com/resource-center/definitions/spear-phishing.>
46. *What Is Spoofing?* [online]. Proofpoint. 2025 [cit. 2025-02-16]. Dostupné z WWW: <https://www.proofpoint.com/us/threat-reference/spoofing.>
47. *What Is Vishing And A Vishing Attack?* [online]. Fortinet. 2023 [cit. 2025-02-06]. Dostupné z WWW: <https://www.fortinet.com/resources/cyberglossary/vishing-attack.>
48. *Za deset let se stal YouTube druhou nejnavštěvovanější stránkou*. [online]. ČT24. 2015. [cit. 2025-03-05]. Dostupné z WWW: <https://ct24.ceskatelevize.cz/clanek/media/za-deset-let-se-stal-youtube-druhou-nejnavstevovanejsi-strankou-132443.>
49. *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. [online]. Zákony pro lidi. 2014. [cit. 2025-03-05]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2014-181>
50. *Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů*. [online]. Zákony pro lidi. 2025 [cit. 2025-01-18]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2014-181?text=z%C3%A1kon+o+kybernetick%C3%A9+bezpe%C4%8Dnosti.>
51. *Zákon trestní zákoník.* [online]. Zákony pro lidi. 2025 [cit. 2025-03-02]. Dostupné z WWW: <https://www.zakonyprolidi.cz/cs/2009-40.>

Seznam obrázků a grafů

Seznam příloh

Přílohy

Příloha 1: Dotazník

Dobrý den,

tímto bych Vás chtěl požádat o vyplnění mého průzkumného dotazníku k bakalářské práci, která se zabývá velmi rozšířeným způsobem, jak připravit jedince o finanční prostředky. Konkrétně se jedná o phishingové podvody.

Za každé vyplnění Vám předem děkuji.

1. Jaké je Vaše pohlaví?

A) Muž

B) Žena

2. Kolik je Vám let?

A) 18 – 25

B) 26 – 35

C) 26 – 35

D) 46 – 55

E) 56 a více

3. Jaké je Vaše nejvyšší dosažené vzdělání?

A) Základní

B) Střední odborné vzdělání s výučním listem

C) Úplné střední odborné vzdělání s maturitou

D) Vyšší odborné vzdělání

E) Bakalářské vzdělání

F) Magisterské vzdělání

4. Slyšeli jste už o pojmu phishing?

A) Ano

B) Ne

5. Který z následujících popisů nejlépe odpovídá phishingu?

A) Zasílání masivních požadavků na server s cílem jeho přetížení.

B) Krádež osobních údajů pomocí podvodných e-mailů

C) Krádež osobních údajů pomocí podvodných e-mailů

6. Setkali jste se někdy s phishingovým útokem?

A) Ano

B) Ne

C) Nejsem si jistý/á.

7. Pokud ano, jakým způsobem jste byli kontaktováni?

A) E-mail

B) SMS zpráva

C) Sociální síť

D) Telefonní hovor

E) V minulosti jsem se s phishingem nesetkal/la

F) Jiný

8. O jakých typech phishingových útoků jste slyšeli?

A) E-mailový phishing

B) Phishing přes SMS (smishing)

C) Phishing přes sociální sítě

D) Phishing přes telefon (vishing)

E) Nic z výše uvedeného

F) Jiné

9. Co uděláte, pokud obdržíte e-mail s podezřelým odkazem, či přílohou?

A) E-mail smažu

B) E-mail nahlásím jako spam

C) E-mail ignoruji

D) Ověřím si totožnost odesílatele

E) Jiné

F) Otevřu přílohu, nebo kliknu na odkaz

10. Kontrolujete adresu odesílatele e-mailu před otevřením?

A) Vždy

B) Občas

C) Nikdy

11. Myslíte si, že je veřejnost dostatečně informována o phishingu?

A) Ne

B) Ano

12. Považujete vzdělávání o kybernetické bezpečnosti za důležité pro prevenci phishingových útoků?

A) Ano, je to klíčové.

B) Ne, nevidím to jako zásadní.

C) Nejsem si jistý/á.

13. Jak byste ohodnotili své povědomí o phishingu a jeho prevenci? (1 = velmi nízké, 5 = velmi vysoké)

A) 1

B) 2

C) 3

D) 4

E) 5

14. Kde jste se dozvěděli o phishingu?

A) Zaměstnání

B) Media

C) Vlastní zkušenost

D) Škola

E) Z tohoto dotazníku

F) Jiné

15. Jaké jsou podle vás hlavní motivy lidí, kteří se stávají obětí phishingu?

A) Nedostatek povědomí o bezpečnosti.

B) Přílišná důvěra v neověřené e-maily nebo odkazy.

C) Emoční spouštěč (nabídky "výhodných" slev, výher nebo nečekaných odměn)

D) Spěch nebo ztráta ostražitosti při manipulaci s online transakcemi.

E) Jiné