

Anonymita na internetu

Jiří Kuchaříč

Bakalářská práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně

Fakulta logistiky a krizového řízení

Ústav ochrany obyvatelstva

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Jiří Kuchařič
Osobní číslo:	L22287
Studijní program:	B1032A020002 Ochrana obyvatelstva
Forma studia:	Kombinovaná
Téma práce:	Anonymita na internetu

Zásady pro vypracování

- Objasněte základní pojmy předmětné problematiky.
- Popište související bezpečnostní rizika a opatření pro jejich mitigaci.
- Navrhněte doporučení pro bezpečnou komunikaci v prostředí internetu.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. ČESKO, 2014. *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů*. Online. In: *Zákony pro lidi*. AION CS, © 2010-2024. Dostupné z: <https://www.zakonyprolidi.cz/cs/2014-181/zneni-20220806>.
2. ČESKO, 2019. *Zákon č. 110/2019 Sb., o zpracování osobních údajů*. Online. In: *Zákony pro lidi*. AION CS, © 2010-2024. Dostupné z: <https://www.zakonyprolidi.cz/cs/2019-110>.
3. EVANS, Lester. *Cybersecurity: what you need to know about computer and cyber security, social engineering, the internet of things + an essential guide to ethical hacking for beginners*. USA, Lester Evans, 2019. ISBN 9781794647237.
4. JAN, Kolouch. *Cybersecurity*. Edice CZ.NIC, 2019, 1 online zdroj. ISBN 978-80-88168-32-4.
5. MITNICK, Kevin D. a VAMOSI Robert. *The art of invisibility: the world's most famous hacker teaches you how to be safe in the age of big brother and big data*. New York: Back Bay Books, Little, Brown and Company, 2019. ISBN 978-0-316-38052-2.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání bakalářské práce: **2. prosince 2024**
Termín odevzdání bakalářské práce: **2. května 2025**

L.S.

prof. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

V Uherském Hradišti, dne 29.04.2025

Jiří Kuchařič
podpis autora

ABSTRAKT

Tato bakalářská práce se zaměřuje na problematiku anonymity na internetu z pohledu běžného uživatele. V kontextu rostoucí digitalizace a zvyšující se míry sledování online aktivit se anonymita stává stále důležitějším aspektem ochrany osobního soukromí. Práce se věnuje tomu, jaká data uživatelé internetu předávají, ať už jde o běžná data, citlivá data nebo metadata a jaké jsou důsledky jejich sdílení.

Práce kombinuje teoretická východiska s praktickou částí založenou na kvantitativním výzkumu, který byl realizován formou dotazníkového šetření. Výsledky ukazují, jak je problematika anonymity vnímána mezi běžnými uživateli a do jaké míry aktivně přistupují k ochraně svého digitálního soukromí.

Klíčová slova: Internet, Anonymita, Data, Bezpečí, Tor, VPN

ABSTRACT

This bachelor thesis focuses on the issue of online anonymity from the perspective of the average internet user. In the context of increasing digitalization and the growing extent of online activity monitoring, anonymity is becoming an increasingly important aspect of personal privacy protection. The thesis examines what types of data internet users share whether common data, sensitive data, or metadata and what the consequences of such sharing may be.

The thesis combines theoretical background with a practical part based on quantitative research conducted through a questionnaire survey. The results reveal how the issue of anonymity is perceived by ordinary users and to what extent they actively seek to protect their digital privacy.

Keywords: Internet, Anonymity, Data, Safety, Tor, VPN

Tímto bych chtěl poděkovat panu ***Ing. Petrovi Svobodovi Ph.D.*** za přínosné rady a skvělé vedení při psaní této bakalářské práce. Dále bych chtěl poděkovat mé přítelkyni ***Bc. Jessice Márii Mikelové DiS.*** za neustálou podporu při psaní práce. Nakonec bych chtěl poděkovat ***Bohu*** za to, že jsem na to nikdy nebyl sám.

OBSAH

ÚVOD.....	11
I TEORETICKÁ ČÁST	13
1 INTERNET	14
1.1 DEFINICE INTERNETU	14
1.2 HISTORIE A VÝVOJ INTERNETU	15
1.2.1 Internet v České republice.....	16
1.2.2 Budoucnost internetu	16
1.3 KYBERPROSTOR	17
1.3.1 Umělá inteligence (AI).....	17
1.4 KYBERNETICKÁ BEZPEČNOST	18
1.4.1 Původ hackerství	20
1.4.2 Kybernetické útoky	20
1.5 DARKWEB	21
1.6 DATA	22
1.6.1 Běžná data	23
1.6.2 Citlivá data	23
1.6.3 Metadata	23
1.7 SOCIÁLNÍ SÍTĚ	23
1.7.1 Facebook	24
1.7.2 Instagram.....	24
1.7.3 Snapchat	25
2 ANONYMITA	26
2.1 DEFINICE ANONYMITY.....	27
2.1.1 Hnutí Cypherpunk.....	27
2.1.2 Triáda CIA	28
2.2 TOR.....	30
2.2.1 VPN over TOR.....	31
2.2.2 TOR over VPN.....	31
2.2.3 MAC adresa	32
2.3 HESLO	32
3 ŠIFROVÁNÍ.....	34
3.1.1 Biometrické šifrování.....	34
3.1.2 Kryptologie	34
3.1.3 Symetrické šifrování	35
3.1.4 Asymetrické šifrování	36
3.1.5 Hashování.....	37
3.1.6 Elektronický podpis	37
3.1.7 Postkvantová kryptografie	38

3.1.8	Instant messaging	39
3.1.9	Online identita	39
3.1.10	E-mail	40
4	LEGISLATIVA SOUVISEJÍCÍ S ANONYMITOU NA INTERNETU	42
5	DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI.....	44
II	PRAKTICKÁ ČÁST	45
6	IDENTIFIKACE SOUVISEJÍCÍCH RIZIK	46
6.1	SLEDOVÁNÍ UŽIVATELE	46
6.1.1	Cookies	47
6.1.2	Typy cookies	49
6.1.3	Browser Fingerprinting	50
6.1.4	Metadata	50
6.2	ÚNIKY INFORMACÍ.....	51
6.2.1	Největší úniky dat.....	52
6.2.2	Have I been pwned	53
7	DOTAZNÍKOVÉ ŠETŘENÍ	55
7.1	VÝZKUMNÁ OTÁZKA Č. 1.....	55
7.2	VÝZKUMNÁ OTÁZKA Č. 2.....	56
7.3	VÝZKUMNÁ OTÁZKA Č. 3.....	56
8	DOPORUČENÍ PRO MITIGACI BEZPEČNOSTNÍCH RIZIK	58
8.1.1	Internetová etika	58
8.1.2	Zásady bezpečného vystupování v online prostředí.....	59
8.1.3	Am I Unique	60
8.1.4	Cover Your Tracks	61
8.1.5	Privacy.net.....	62
8.1.6	Windscribe.....	63
8.2	BEZPEČNÁ KOMUNIKACE.....	64
8.2.1	Signal.....	64
8.2.2	Microsoft Teams.....	65
8.2.3	ZOOM	67
	ZÁVĚR.....	69
	SEZNAM OBRÁZKŮ	75
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	76
	SEZNAM PŘÍLOH.....	78

ÚVOD

V digitální době se používání internetu stalo každodenní samozřejmostí pro většinu lidí. Připojujeme se k síti kvůli práci, zábavě, studiu nebo komunikaci, často bez hlubšího zamyšlení nad tím, jaké informace o sobě při těchto aktivitách zanecháváme. Každá naše online činnost, od vyhledávání informací přes přihlášení do e-mailu až po sdílení příspěvku na sociální síti, generuje data, která lze zaznamenat, analyzovat a využít.

Tato data lze rozdělit do několika kategorií. Běžná data zahrnují například IP adresu, typ prohlížeče, jazyk systému nebo navštívené webové stránky. Citlivá data se týkají informací o naší identitě, zdravotním stavu, finanční situaci nebo osobních preferencích, tedy údajů, jejichž zneužití by mohlo mít vážné důsledky. Specifickou kategorií představují metadata, což jsou informace „o datech“, například kdy a odkud jsme se připojili k síti, jak často navštěvujeme určité stránky nebo s kým a jak často komunikujeme. I když metadata neobsahují konkrétní obsah komunikace, často postačí k vytvoření přesného obrazu o našich návycích a vztazích.

Data, která o sobě uživatelé internetu zanechávají, mohou být cenným artiklem pro firmy, reklamní společnosti, státní instituce, ale i kybernetické útočníky. Mohou sloužit k cílené reklamě, manipulaci, profilování, sledování nebo dokonce vydírání. Proto je stále důležitější klást si otázku: Jak si může běžný uživatel chránit své soukromí a zajišťovat si anonymitu v online prostředí?

Proto hlavním cílem této bakalářské práce je: Navrhnout doporučení pro zvýšení úrovně anonymity uživatelů v prostředí internetu.

Dílčí cíle jsou celkem čtyři a to:

- Seznámit se s problematikou digitálních stop
- Analyzovat dostupné nástroje a přístupy pro zajištění anonymity v prostředí internetu.
- Definovat výzkumné otázky ke zjištění aktuálního stavu vnímání problematiky anonymity v prostředí internetu.
- Zodpovědět výzkumné otázky s využitím dotazníkového šetření.

Práce se zaměřuje výhradně na jednotlivce, tedy na běžné uživatele internetu, nikoliv na firmy či organizace. Jejím cílem je nejen popsat možnosti ochrany soukromí, ale i zjistit, jak s nimi uživatelé v praxi nakládají. Výsledky mohou přispět k většímu povědomí o problematice digitální anonymity a zvýšení bezpečnosti jednotlivců v online světě.

Výstupem je mitigace bezpečnostních rizik a řešení v rámci bezpečné komunikace v podobě platforem a aplikací s dostačujícím zabezpečením pro zanechání minimální digitální stopy a vystavování svých dat třetím stranám.

I. TEORETICKÁ ČÁST

1 INTERNET

Pod pojmem internet si dnes každý vybaví něco trochu jiného, ale většina uživatelů ho spojuje s elektronickou poštou, sociálními sítěmi, zprávami a podobně. Tento pohled vychází z individuálních zkušeností a potřeb každého jednotlivce. V současnosti je připojení k internetu vnímáno jako běžná součást života. Lidé se připojují k síti, aniž by se zamýšleli nad tím, jak internet skutečně funguje, kam míří sdílené informace, nebo jaké důsledky má jejich online chování na soukromí a bezpečnost. (Stark, 2011)

Internet, označovaný také jako „sít' sítí“, může být užitečný nástroj, avšak problémy nastávají, pokud nad ním uživatelé ztrácejí kontrolu. Kritickým okamžikem je situace, kdy člověk kvůli přehnané důvěře v internet není schopen rozlišit pravdu od dezinformací. Stejně tak je rizikové, pokud ignoruje potřebu chránit své soukromí a nebere v potaz možné následky svého chování na internetu. (Stark, 2011)

Často se také řeší otázka, zda psát slovo Internet s velkým „I“ nebo malým „i“. Pokud mluvíme o globální komunikační síti, protokolech nebo připojení k ní, používá se velké písmeno. Naopak, v případě obecných počítačových sítí či datové konektivity je správné malé „i“. U intranetu nebo extranetu se rovněž píše malé písmeno, stejně jako ve výrazech „informace na internetu“, „seznámení s internetem“ nebo „nabízíme připojení k internetu“. (Chýlová, 2010)

1.1 Definice internetu

„Internet je decentralizovaná celosvětová síť spojující počítače různých vlastníků, která je odolná proti výpadku jedné nebo několika částí. Umožňuje sdílení dat, používání e-mailu a mnoho dalších služeb. Internet nekontroluje žádná autorita a celý systém je vybudován tak, aby se řídil sám“ (Blažková, 2005 str. 13)

Další definice popisuje internet jako globální počítačovou síť, která uchovává informace v elektronické podobě a zpřístupňuje je dalším zařízením. Jde o komplex technologií, jež umožňují přenos dat prostřednictvím standardizovaných komunikačních protokolů po celém světě. Internet je schopen zpracovávat i typy dat, které nebyly v době jeho vzniku předpokládány. (Bednář, 2007)

Internet se také ukázal jako efektivní nástroj pro propojení lidí, protože výrazně usnadňuje komunikaci mezi uživateli. Díky tomu umožnil vznik komunit, sociálních sítí a dalších platforem, které spojují lidi se společnými zájmy, a to i přesto, že by se v běžném životě pravděpodobně nikdy nesetkali. (Bednář, 2007)

Kromě toho poskytuje internet prostor pro rozvoj nových služeb, trhů a komerčních aktivit. Pro mnoho podniků představuje snadný způsob, jak expandovat na globální trh a zahájit podnikání s minimálními geografickými omezeními. (Bednář, 2007) (Blažková, 2005)

1.2 Historie a vývoj internetu

Základy internetu sahají do druhé poloviny 20. století, konkrétně do roku 1957, kdy vypuštění první umělé družice Sputnik 1 Sovětským svazem podnítilo Spojené státy k intenzivnímu zájmu o vesmírné a vojenské technologie. Během studené války USA reagovaly vytvořením agentury Advanced Research Project Agency (ARPA) v roce 1958 pod ministerstvem obrany. Cílem této agentury bylo podporovat výzkum inovativních technologií. (Svršek)

V roce 1962 byl zahájen projekt zaměřený na vytvoření počítačové sítě, která by zůstala funkční i při vyřazení některých jejích částí. Výsledkem byla unikátní decentralizovaná síť. Důležitým milníkem bylo 29. října 1969, kdy byla ve Spojených státech spuštěna experimentální síť ARPANET, která sloužila primárně pro vládní a vojenské účely. V roce 1973 došlo k rozšíření ARPANETu za hranice USA, konkrétně do Velké Británie a Norska. Ve stejném roce byly také položeny základy protokolu TCP/IP, jenž měl nahradit tehdejší Network Control Program (NCP). (Svršek)

V roce 1983 byla od ARPANETu oddělena vojenská síť MILNET a TCP/IP bylo poprvé implementováno v komerční sféře. Zároveň vznikly základy systému DNS. Do roku 1984 bylo k ARPANETu připojeno zhruba 1 000 zařízení. (Svršek)

V roce 1987 byl spuštěn projekt National Science Foundation NETwork (NSFNET) a poprvé se objevil termín „internet“. V roce 1989 Tim Berners-Lee a Robert Cailliau navrhli technologii World Wide Web (WWW) jako způsob práce s hypertextovými dokumenty. V roce 1991 byla technologie WWW poprvé použita v CERNu a 6. srpna téhož roku byla

spuštěna první webová stránka na adrese info.cern.ch, což byla domovská stránka CERNu. (Svršek)

1.2.1 Internet v České republice

Historii Internetu by člověk v České republice před rokem 1989 hledal zbytečně, protože tehdejší politická situace zemi bránila v zapojení se do celosvětové sítě. S ústupem komunismu byl pak 13. 2. 1992 na ČVUT poprvé spuštěn Internet v tehdeším Československu. (2014)

Současně byl zahájen i projekt Federal Educational and Scientific Network (FESNET), který se zabýval vývojem a výzkumem v oblasti pokročilých síťových technologií. Po rozdělení Československa byla zkratka změněna na CESNET. (2014)

Kolem roku 2000 podle statistik překročil počet českých uživatelů Internetu hranici jednoho milionu. V roce 2012 se pak už jednalo přibližně o 73 % z celkové populace České republiky. (2014) (2013)

1.3 Budoucnost internetu

Předpovídat budoucí vývoj je vždy obtížné, ale lze s jistotou říci, že internet bude nadále postupovat kupředu – jak z hlediska rozšiřování pokrytí a zvyšování rychlosti, tak i v oblasti jeho využití pro sociální a komerční účely. (Svršek)

Společnost CISCO, významný výrobce síťového hardwaru, provedla v roce 2010 analýzu budoucího vývoje internetu. Podle ní lze očekávat, že internet získá větší vliv v rozvojových zemích a že generace lidí narozených po roce 1990, často označovaná jako „internetová generace“, bude k internetu udržovat hlubší vazbu. Vývoj by se měl zaměřit také na nové způsoby ovládání – vedle tradiční klávesnice se budou stále více uplatňovat hlasové příkazy, gesta nebo biosenzory. Budoucnost internetu bude úzce spojena s rozvojem sítí, technologickým pokrokem a ochotou uživatelů přijímat nové služby a technologie. Společnost CISCO definovala čtyři možné scénáře budoucího vývoje. (Svršek)

První z těchto scénářů, který již můžeme pozorovat, předpokládá, že internet se stane neoddělitelnou součástí každodenního života. S tím souvisí rostoucí obliba videoobsahu a stále širší využívání cloudových služeb. (Svršek)

Další možností je, že internetové prostředí postupem času ztratí důvěryhodnost. Častější kybernetické útoky a rostoucí bezpečnostní hrozby by mohly způsobit, že ochrana soukromí a citlivých dat se stane příliš nákladnou. To by vedlo k úpadku komerčního využití internetu a k tomu, že sociální aspekty online světa budou hrát prim. (Svršek)

1.4 Kyberprostor

V anglickém jazyce se pro tento pojem používá termín Cyberspace, který lze definovat jako „prostor pro kybernetické aktivity“ nebo jako „prostor vytvořený informačními a komunikačními technologiemi“ (Kolouch, 2019)

Odborníci popisují kyberprostor prostřednictvím jeho charakteristických rysů, mezi které patří:

- globální povaha,
 - absence centralizace,
 - možnost interakce,
 - otevřenost,
 - vysoký objem dostupných informací,
 - schopnost ovlivňovat názory jednotlivců či prostřednictvím uživatelů další skupiny.
- (Kolouch, 2019)

Kyberprostor představuje prostředí, které může přispívat k rozvoji různých patologických forem chování a prožívání. (Blinka, 2015)

1.4.1 Umělá inteligence (AI)

Umělá inteligence (AI) je odvětvím informatiky, které se zaměřuje na vývoj systémů schopných imitovat či simulovat různé lidské kognitivní procesy, jako je schopnost učit se, rozhodovat, plánovat a reagovat na proměnlivé podmínky. AI zahrnuje různé algoritmy, modely a technologie, které umožňují strojům vykonávat činnosti obvykle vyžadující lidskou inteligenci. (Takeo, 2021)

AI pomáhá vylepšovat VPN služby, TOR síť a další anonymizační nástroje. Například může detekovat úniky dat a blokovat sledovací algoritmy. Dokáže také vytvářet realistické i

fiktivní identity, které chrání soukromí uživatelů (např. deepfake hlasy a obličeje pro anonymní komunikaci). Lze upotřebit také na identifikaci a blokování cookies, fingerpringing a další techniky používané pro sledování uživatelů na webu. (Takeo, 2021)

AI lze klasifikovat různými způsoby. Podle typu zpracovávaných dat ji lze rozdělit na úzce zaměřenou (specializovanou) AI, která je vytvořena pro konkrétní úkoly, obecnou AI, která představuje teoretický koncept univerzální inteligence schopné řešit různé problémy podobně jako člověk, a na superinteligenci, což je hypotetická forma inteligence překračující schopnosti lidské mysli. Z hlediska metodologie zahrnuje AI strojové učení, kde systémy samy získávají znalosti na základě dat, hluboké učení využívající vícevrstvé neuronové sítě, expertní systémy spoléhající na soubory pravidel a databáze znalostí, a zpracování přirozeného jazyka, umožňující komunikaci mezi stroji a lidmi. (Takeo, 2021)

Z aplikačního pohledu se AI dělí na reaktivní stroje, které pracují pouze s aktuálními informacemi, systémy s omezenou pamětí, jež využívají i historická data, na AI budoucnosti nazvanou teorie mysli, která by měla chápat emoce a sociální interakce, a hypotetickou sebevědomou AI, která by měla vlastní vědomí. (Takeo, 2021)

Využití umělé inteligence je velmi rozmanité. V průmyslové a výrobní sféře se uplatňuje při automatizaci procesů, predikci údržby a optimalizaci logistiky. Ve zdravotnictví slouží k diagnostice pomocí analýzy obrazových dat, při personalizaci léčby či ve vývoji léčiv. V dopravě přispívá k řízení autonomních vozidel, efektivnímu řízení dopravy a předpovědím dopravních zácp. Ve finančním sektoru je AI využívána k detekci podvodů, analýze trhů a v zákaznických službách, například prostřednictvím chatbotů. V oblasti e-commerce pomáhá analyzovat chování zákazníků a doporučovat produkty. Ve vzdělávání se aplikuje v personalizovaných výukových programech nebo při automatickém hodnocení testů. Nakonec, v zábavním průmyslu nachází uplatnění při tvorbě obsahu a ve streamovacích službách, které doporučují uživatelům vhodný obsah. (Takeo, 2021)

1.5 Kybernetická bezpečnost

Kybernetická bezpečnost označuje soubor metod, procesů a technologií, jejichž cílem je chránit počítačové systémy, sítě a data před neoprávněným přístupem, útoky, zneužitím a dalšími hrozbami. Tato oblast zahrnuje nejen ochranu fyzických zařízení a softwaru, ale také

zajištění důvěrnosti, integrity a dostupnosti dat. S rostoucí digitalizací a závislostí na informačních technologiích hraje kybernetická bezpečnost klíčovou roli ve všech odvětvích společnosti. (Dodge, 2020)

Pojem kybernetická bezpečnost vznikl v druhé polovině 20. století v souvislosti s rozvojem počítačových sítí, zejména internetu. Termín „kybernetika“ má svůj původ v řeckém slově „kybernetes“, což znamená kormidelník nebo řídicí činitel. Tento koncept poprvé zpopularizoval Norbert Wiener ve své knize *Cybernetics: Or Control and Communication in the Animal and the Machine* z roku 1948, která se zabývala teorií řízení a komunikace. Kybernetická bezpečnost jako samostatný obor se však začala formovat až v době, kdy se sítě staly kritickou součástí fungování organizací a jednotlivců, a to zejména s nárůstem počítačových hrozeb v 80. a 90. letech 20. století. (Dodge, 2020)

Počátky kybernetické bezpečnosti sahají do 70. let, kdy bylo poprvé nutné řešit bezpečnostní rizika v souvislosti s prvními počítačovými sítěmi, jako byl ARPANET, předchůdce dnešního internetu. Jedním z prvních známých incidentů byl v roce 1988 Morrisův červ, který infikoval tisíce počítačů připojených k síti a poukázal na potřebu ochrany před škodlivými programy. V 90. letech, s nástupem internetu pro veřejnost, se hrozby staly rozsáhlejšími a sofistikovanějšími, což vedlo k vývoji antivirových programů, firewallů a dalších bezpečnostních nástrojů. První zákony zaměřené na kyberkriminalitu, jako například americký zákon *Computer Fraud and Abuse Act* z roku 1986, byly rovněž důležitým milníkem v této oblasti. (Dodge, 2020)

S příchodem 21. století a masivní digitalizací se kybernetická bezpečnost stala strategickým tématem nejen pro firmy, ale také pro státy. Vznikly nové formy útoků, jako jsou ransomware, phishing a pokročilé perzistentní hrozby (APT), které cílí na kritickou infrastrukturu a citlivé informace. Reakce na tyto hrozby vedly k rozvoji pokročilých technologií, jako je šifrování, multifaktorová autentizace a behaviorální analýza. (Dodge, 2020)

Budoucnost kybernetické bezpečnosti bude ovlivněna pokračujícím vývojem technologií, jako jsou umělá inteligence, kvantové výpočty a internet věcí (IoT). Umělá inteligence se stává klíčovým nástrojem jak pro útočníky, tak pro obránce, protože umožňuje rychlou analýzu velkého množství dat a automatizované odhalování hrozeb. Kvantové výpočty

mohou v budoucnu narušit současné šifrovací metody, což si vyžádá vývoj kvantově odolných algoritmů. S rostoucím počtem zařízení připojených k internetu vzrůstají i bezpečnostní rizika spojená s IoT, což bude vyžadovat nové standardy a regulace. (Dodge, 2020)

Celkově lze říci, že kybernetická bezpečnost zůstane klíčovou oblastí jak pro ochranu jednotlivců a organizací, tak pro udržení stability a bezpečnosti digitální společnosti. Spolupráce na mezinárodní úrovni, vzdělávání a inovace budou nezbytné pro zvládnutí nových výzev v tomto neustále se vyvíjejícím oboru. (Dodge, 2020)

1.5.1 Původ hackerství

Kořeny hackerství sahají do poloviny 20. století, kdy se tento termín začal používat k označení lidí, kteří přistupovali k technologiím originálním a inovativním způsobem. První známé zmínky o hackerech pocházejí z 50. let z Massachusettského technologického institutu (MIT), kde studenti používali výraz „hack“ k označení chytrých a neobvyklých řešení technických problémů. Tito ranní hackeři se soustředili hlavně na zdokonalování výpočetních systémů a objevování jejich nevyužitých možností. V 60. letech nabralo hackerství na obrátkách díky rozvoji výzkumu počítačových sítí, kdy programátoři a technici s otevřeným přístupem k technologiím hledali nové způsoby jejich využití. S příchodem ARPANETu, předchůdce internetu, se tato činnost začala rozšiřovat z akademického prostředí do širší praxe. Hackerství tehdy nemělo negativní konotace a bylo spojováno spíše se zvědavostí, kreativitou a technologickými inovacemi. Situace se změnila v 80. a 90. letech, kdy počítače začaly být běžně dostupné a technologie si našly cestu do každodenního života. V této době se objevily skupiny, které využívaly své schopnosti k nelegálnímu pronikání do systémů a získávání citlivých dat. Tento vývoj zásadně ovlivnil obraz hackerů, kteří byli často vykreslováni jako zločinci, přestože původní podstata hackerství spočívala ve sdílení znalostí a technologickém pokroku. (Levy, 2010)

1.5.2 Kybernetické útoky

Kybernetické útoky jsou úmyslné akce zaměřené na narušení zabezpečení počítačových sítí, systémů nebo dat s cílem způsobit škody, získat neoprávněný přístup či zneužít důvěrné informace. Tyto útoky mají různé formy, počínaje základními phishingovými technikami, při nichž podvodné e-maily slouží k získávání citlivých údajů, až po komplexní ransomware útoky, které data zašifrují a požadují finanční výkupné za jejich dešifrování. Kybernetické

útoky provádějí nejen jednotlivci, ale také organizované skupiny či státní subjekty. Jejich cíle zahrnují finanční sektor, technologické firmy, zdravotnická zařízení, energetickou infrastrukturu nebo státní instituce. Dopady těchto útoků mohou být závažné, od ekonomických ztrát a oslabení důvěry veřejnosti až po narušení klíčových funkcí, jako jsou energetické dodávky či poskytování zdravotní péče. Vzhledem k rostoucí závislosti na digitálních technologiích a internetové infrastruktuře se riziko kybernetických útoků stále zvyšuje. Útočníci využívají moderní postupy, například sociální inženýrství nebo zneužití slabín v softwaru, což vyžaduje zlepšení obranných strategií, jako jsou sofistikované systémy pro detekci hrozeb, pravidelné aktualizace softwaru a důkladné vzdělávání uživatelů. (Singer, a další, 2014)

1.6 Darkweb

Temný web (Dark Web) je specifická část internetu, která není indexována běžnými vyhledávači a je přístupná pouze prostřednictvím speciálních prohlížečů, jako je Tor (The Onion Router). Tato skrytá část webu nabízí uživatelům vysokou míru anonymity, což přináší jak výhody, tak nevýhody. (Baker, 2025)

Počátky Dark webu sahají do poloviny 90. let 20. století, kdy americké námořnictvo vyvinulo technologii známou jako „onion routing“. Cílem bylo chránit online komunikaci vojenských a zpravodajských složek tím, že se data přenášela přes více šifrovaných uzlů, což zajišťovalo anonymitu uživatelů. Tato technologie se stala základem pro projekt Tor, který byl veřejně spuštěn v roce 2002. Původně sloužil k ochraně komunikace vládních agentur, ale postupem času se stal nástrojem pro širokou veřejnost hledající anonymitu online. (Haugabrook, 2025)

Temný web slouží k různým účelům, od legitimních po nelegální. Poskytuje platformu pro novináře, aktivisty a disidenty v zemích s omezenou svobodou slova, kteří potřebují sdílet informace bez obav z cenzury nebo represí. Na druhé straně je také místem pro nelegální aktivity, jako je obchod s drogami, zbraněmi, padělanými dokumenty či kradenými daty. Anonymita, kterou Temný web nabízí, láká různé skupiny uživatelů s odlišnými motivacemi. (Baker, 2025)

Pro přístup na Dark web je nejčastěji používán prohlížeč Tor. Jeho instalace je obdobná jako u jiných prohlížečů, avšak umožňuje přístup k webovým stránkám s doménou „onion“, které

nejsou dostupné prostřednictvím standardních prohlížečů. Je důležité poznamenat, že samotné používání Toru není nelegální; nelegální jsou až aktivity, které porušují zákony, bez ohledu na to, zda jsou prováděny na Temném webu či jinde. (Baker, 2025)

Mezi hlavní výhody Dark webu patří vysoká míra anonymity a svobody projevu. Uživatelé mohou sdílet informace a komunikovat bez obav z dohledu či cenzury. To je zvláště cenné v zemích s omezenou svobodou slova. Na druhou stranu anonymita Dark webu vytváří prostředí pro nelegální aktivity a podvody. Uživatelé mohou narazit na škodlivý obsah nebo se stát oběťmi podvodníků. Navíc, vzhledem k absenci regulace, neexistují záruky kvality či pravdivosti informací a služeb nabízených na Dark webu. (Haugabrook, 2025)

Anonymita je klíčovým prvkem Dark webu. Umožňuje uživatelům chránit svou identitu a soukromí, což je zásadní pro novináře, whistleblowery či obyvatele zemí s represivními režimy. Na druhé straně tato anonymita komplikuje práci bezpečnostních složek při potírání nelegálních aktivit. Je tedy důležité pečlivě zvážit, jak a k jakým účelům Dark web využívat, a být si vědom jak jeho potenciálních přínosů, tak rizik. (Baker, 2025)

1.7 Data

Data představují souhrn informací, které mohou být zaznamenány, uloženy a následně zpracovány. V digitálním světě se jedná o reprezentaci faktů, událostí nebo konceptů ve formě vhodné pro komunikaci, interpretaci či zpracování počítačovými systémy. (Jirásek, a další, 2022)

Historie dat je úzce spjata s vývojem lidské komunikace a technologií. Od prvotních záznamů na hliněných tabulkách přes vynález knihtisku až po digitalizaci v 20. století. S nástupem internetu a moderních technologií se objem generovaných a sdílených dat exponenciálně zvýšil. Tento růst dat přinesl nové výzvy v oblasti jejich správy, ochrany a soukromí. (Jirásek, a další, 2022)

S rostoucím množstvím citlivých dat na internetu se zvýšila potřeba chránit soukromí uživatelů. To vedlo k vývoji technologií a nástrojů zaměřených na anonymizaci a šifrování dat, aby byla zajištěna ochrana před neoprávněným přístupem a sledováním. (Jirásek, a další, 2022)

1.7.1 Běžná data

Jedná se o informace, které neobsahují citlivé či osobní údaje. Patří sem například veřejně dostupné statistiky, obecné informace o produktech nebo anonymizované souhrnné údaje. Tato data nepředstavují vysoké riziko zneužití a jejich ochrana není tak přísná jako u citlivých dat. (Jirásek, a další, 2022)

1.7.2 Citlivá data

Citlivá data zahrnují informace, jejichž neoprávněné zveřejnění nebo zneužití by mohlo vést k poškození jednotlivce či organizace. Patří sem osobní údaje (jako jsou jméno, adresa, rodné číslo), finanční informace, zdravotní záznamy nebo obchodní tajemství. Ochrana těchto dat je klíčová, aby se předešlo krádeži identity, finančním podvodům či jiným formám zneužití. (Jirásek, a další, 2022)

1.7.3 Metadata

Metadata jsou data o jiných datech. Poskytují kontext nebo popisují vlastnosti samotných dat, aniž by zasahovala do jejich obsahu. Příkladem může být informace o autorovi dokumentu, datum jeho vytvoření, velikost souboru nebo čas odeslání e-mailu. Metadata usnadňují organizaci, vyhledávání a správu dat. (Skleňák, 2001)

V souvislosti s anonymitou na internetu hrají metadata zásadní roli. I když je obsah komunikace šifrován nebo anonymizován, metadata mohou odhalit vzorce komunikace, časové údaje či vztahy mezi subjekty. Například čas a frekvence připojení mohou poskytnout informace o aktivitách uživatele. Proto je důležité chránit nejen samotná data, ale i jejich metadata, aby byla zajištěna skutečná anonymita online. (Skleňák, 2001)

1.8 Sociální síť

První sociální síť na internetu byla založena v roce 1995 pod názvem „Classmates.com“. Tento server fungoval jako platforma pro komunitní síť, která umožňovala uživatelům navázat spojení se svými kamarády. O dva roky později v roce 1997 byla spuštěna stránka SixDegrees.com. Tato platforma patřila k jedné z prvních, která umožňovala jejich uživatelům zakládat osobní profily a vytvářet seznamy přátel. Platformu SixDegrees.com využíval jeden milion uživatelů. Byla dostupná do roku 2002, kdy ale poté zanikla, protože v této době nebyl online svět tak populární a uživatelé na platformě nenacházeli blízký okruh svých známých, které znali z reálného života. (Pavlíček, 2010)

Po roce 2002 začaly být internetové stránky populárnější. Vznikla například stránka pojmenována jako „Friendster“, která získala tři miliony uživatelů za tři měsíce. Postupně začaly přibývat další platformy, pro dnešní uživatele již známější, jako je například LinkedIn, Facebook, Instagram, Snapchat a další. Mezi tři nejvíce využívané sítě v České republice patří Facebook, Instagram a Snapchat. (Pavlíček, 2010)

1.8.1 Facebook

Facebook vznikl v roce 2004. Nejdříve byla tato síť dostupná jenom studentům Harvardské univerzity, ke komunikaci v uzavřené skupině mezi sebou. Po měsíci fungování byl Facebook zpřístupněn i dalším univerzitám. V roce 2005 se tato platforma rozšířila do Evropy. (Hušková, 2025)

Facebook dnes využívá více než dvě miliardy uživatelů, to z této platformy dělá největší sociální síť na světě. V České republice Facebook využívá přibližně jedna polovina obyvatelstva. Z celkového počtu populace, která využívá Facebook, se 3,8 milionů uživatelů přihlašuje denně. (Hušková, 2025)

1.8.2 Instagram

Tato sociální síť je založená na sdílení fotografií, videí. Poprvé byla síť spuštěna v roce 2010 a její popularita rostla raketovou rychlostí. Dva měsíce po spuštění měl Instagram 200 milionů uživatelů. Sociální síť Instagram koupila v roce 2014 v dubnu společnost Facebook, za 1 miliardu dolarů. Po tomto kroku zaznamenal Instagram nejrychlejší růst popularity oproti všem ostatním sociálním sítím. (Karacher, 2017)

V květnu 2017 uskutečnila Britská královská společnost veřejného zdraví průzkum pod názvem „#StatusofMind“. Výsledky ukázaly, že Instagram je ze všech sociálních sítí nejvíce škodlivý pro duševní zdraví mladých lidí. Do průzkumu se zapojilo téměř 1 500 účastníků ve věku 14 až 24 let. Bylo zjištěno, že Instagram negativně ovlivňuje vnímání ideálního tělesného vzhledu, zejména u mladých dívek a žen, zhoršuje kvalitu spánku a přispívá k rozšíření fenoménu FOMO (fear of missing out), tedy obav z toho, že člověk něco zmešká v sociálním dění. Z průzkumu ale také vzešlo, že má pozitivní vliv na vytváření vlastní identity. (Karacher, 2017)

1.8.3 Snapchat

Snapchat byl založen v roce 2011. Tato sociální síť je určena primárně k jejímu využívání na mobilních telefonech. Oblíbená se stala hlavně u mladistvých, ve věku 13 až 24 let. Tato sociální síť slouží ke sdílení fotografií nebo krátkých videí. Odlišnost Snapchatu oproti ostatním sociálním sítím, je v délce zobrazení fotografií nebo videí. Snapchat neukládá sdílené fotky a videa na delší dobu. Po jejich zobrazení sdílený obsah hned zmizí a nebo je uložený maximálně na 24 hodin. Dříve byl v tomto Snapchat unikátní, dnes už mají tuto funkci i ostatní sociální sítě. V průběhu let tato síť získala největší množství kontroverze. Kritizována byla hlavně z důvodu, že je síť používána jako sextingový nástroj. Sexting znamená posílání zpráv, které jsou explicitně sexuální. (Malá, 2023)

2 ANONYMITA

V současném digitálním světě je anonymita vzácná a cenná. Každá online aktivita za sebou zanechává stopy, které lze analyzovat a sledovat. Lidé, kteří chtějí zachovat své soukromí a zůstat neodhalen, považují šifrování a ochranu dat za klíčové. Šifrování se dá přirovnat k digitálnímu trezoru, který zabezpečuje informace před neoprávněným přístupem. Bez ohledu na konkrétní metodu šifrování všechny spočívají na stejném principu: data jsou převedena do nečitelné podoby, kterou lze znovu číst pouze s odpovídajícím klíčem. (Nanosystem, 2023)

Základem online bezpečnosti jsou silná hesla, dvoufaktorová autentizace a pravidelně aktualizovaný software. Připojování k veřejným Wi-Fi sítím představuje určité riziko, a proto se doporučuje používat VPN, která šifruje komunikaci. K minimalizaci sledování online aktivit se osvědčily anonymní prohlížeče, například Tor Browser, a soukromé vyhledávače jako DuckDuckGo. I když však uživatelé využijí všechny dostupné technologie, absolutní anonymitu na internetu není možné zaručit. Moderní technologie sice znesnadňují sledování, ale nečiní jej nemožným. (Nanosystem, 2023)

Sociální sítě jsou dnes neodmyslitelnou součástí každodenního života, ale také otevírají otázky spojené s anonymitou na internetu. Vytvoření profilu bez použití skutečného jména může přinést výhody, ale také rizika. (Nanosystem, 2023)

Anonymita lidem poskytuje možnost svobodně vyjadřovat své názory bez obavy z následků nebo odsouzení. Tato svoboda je obzvláště důležitá v zemích, kde není svoboda slova samozřejmostí, nebo pro ty, kdo čelí pronásledování. Anonymní prostředí internetu také nabízí prostor k objevování různých identit a možnost hledat podporu ve skupinách bez strachu z odsouzení společností. Na druhou stranu anonymita může být zneužívána k šíření nenávisti, kyberšikaně a dezinformací. Lidé, kteří se skrývají za anonymními účty, často ztrácejí zábrany a mohou se chovat agresivně. Anonymita také komplikuje proces identifikace pachatelů online trestných činů a jejich postavení před spravedlností. (Nanosystem, 2023)

Je nutné si uvědomit, že anonymita na internetu nikdy nebude stoprocentní. I když se uživatelé rozhodnou neuvádět své skutečné jméno, jejich digitální aktivita zanechává stopy, které lze dohledat. (Nanosystem, 2023)

Celkově má anonymita na internetu své světlé i stinné stránky. Na jednu stranu umožňuje ochranu soukromí a svobodné vyjádření, na druhou stranu však může být nástrojem pro neetické a nezákonné chování. Každý uživatel by měl jednat zodpovědně a mít na paměti, že jeho chování v online prostoru může mít trvalé následky. (Nanosystem, 2023)

2.1 Definice anonymity

Anonymita na internetu znamená schopnost uživatele vykonávat různé online aktivity bez toho, aby byla jeho skutečná identita odhalena. To zahrnuje procházení webových stránek, komunikaci nebo účast v online diskuzích bez toho, aby jeho osobní údaje byly snadno přístupné. Přesto je důležité si uvědomit, že i když jsou některé informace chráněné, existují různé technologie, jako například sledování IP adres nebo cookies, které mohou umožnit identifikaci osoby. I když některé detaily zůstávají neznámé, mohou být v případě potřeby získány právními cestami nebo technickými prostředky. V důsledku toho je plná anonymita na internetu velmi těžko dosažitelná. (2023)

2.1.1 Hnutí Cypherpunk

Hnutí Cypherpunk vzniklo v 90. letech 20. století jako reakce na rostoucí obavy o soukromí a svobodu jednotlivců v digitálním věku. Jeho zakladatelé, mezi něž patří Timothy C. May, Eric Hughes a John Gilmore, se zaměřili na vývoj a propagaci silné kryptografie jako nástroje pro ochranu soukromí a svobody projevu na internetu. V roce 1993 Eric Hughes publikoval „A Cypherpunk's Manifesto“, ve kterém zdůrazňoval, že „soukromí je nezbytné pro otevřenou společnost“ v elektronickém věku a že „musíme bránit naše vlastní soukromí, pokud očekáváme, že nějaké budeme mít.“ (Americano, 2024)

Cypherpunkové věřili, že silná kryptografie a decentralizované technologie mohou přetvořit společenské, politické a ekonomické struktury směrem k větší svobodě a soukromí. Byli proti vládním regulacím, které omezovaly používání kryptografie, a usilovali o to, aby šifrování bylo dostupné všem bez omezení. Tento postoj vedl k intenzivnímu vývoji a šíření šifrovacích nástrojů, které umožnily bezpečnou komunikaci a transakce na internetu. (Americano, 2024)

Cypherpunkové se také zaměřili na otázky anonymity a pseudonymity. Věřili, že možnost anonymní komunikace je klíčová pro svobodu projevu a ochranu jednotlivců před neoprávněným sledováním. Diskutovali o metodách, jak skrýt samotné používání šifrování, aby se chránili před represivními režimy. Tato filozofie ovlivnila vznik a rozvoj různých anonymizačních nástrojů a sítí, jako je například Tor. (Americano, 2024)

Dnes je hnutí Cypherpunk považováno za předchůdce moderního hnutí za digitální svobody a soukromí. Jeho principy a filozofie ovlivnily vývoj mnoha technologií a iniciativ zaměřených na ochranu soukromí, jako jsou kryptoměny, šifrované komunikační platformy a decentralizované aplikace. Cypherpunkové ukázali, že technologie mohou být nástrojem pro posílení svobody jednotlivců a ochranu jejich práv v digitálním světě. (Americano, 2024)

2.1.2 Triáda CIA

Triáda CIA (důvěrnost, integrita, dostupnost) je v kybernetické bezpečnosti jedním z nejvíce uznávaných a běžně využívaných modelů. Nicméně samotné používání této triády bez přidání dalších důležitých principů již dnes není dostatečné pro zajištění adekvátní úrovně kybernetické bezpečnosti. V odborné literatuře se doporučuje rozšíření této triády o takzvaný Parkerian hexad, což je původní triáda CIA doplněná o tři další prvky: P/C (držení a kontrola), A (autentičnost) a U (užitečnost). (Kolouch, 2019)

Cílem kybernetické bezpečnosti je nejen chránit ICT, ale zejména data a informace, které jsou těmito systémy přenášeny, zpracovávány a uchovávány. Triáda CIA se přitom často zaměřuje především na ochranu informací. Tento úzký pohled je v souladu s definicí informační bezpečnosti, která se soustředí na ochranu samotných informací, bez ohledu na to, na jakém typu nosiče nebo v jakém systému jsou zpracovávány. Informační bezpečnost chrání informace v průběhu celého jejich životního cyklu. (Kolouch, 2019)

V současnosti se ale vynořuje otázka, zda je pojem informační bezpečnost adekvátní pro všechny aspekty kybernetické bezpečnosti. V souvislosti s ICT a aktivitami v kyberprostoru je lepší používat termín kybernetická bezpečnost, jelikož původní definice informační bezpečnosti ignoruje klíčové prvky kybernetické bezpečnosti. Za tyto prvky považujeme nejen samotné informace, ale i data a počítačové systémy, které jsou nezbytné pro přenos informací a dat. (Kolouch, 2019)

Data lze chápat jako jakékoli prvky s informační hodnotou, které jsou zpracovávány počítačovými systémy, a z nichž se následně vytvářejí informace. Informace jsou údaje, které byly zpracovány do formy užitečné pro příjemce. Podle Wienera jsou informace obsahem, který se vyměňuje s okolním světem, když na něj působíme svým přizpůsobením. Informace jsou tedy kvalitativně vyšší než data, která se stávají informacemi až tehdy, pokud jsou kontextualizována a získají význam pro člověka. (Kolouch, 2019)

V oblasti kybernetické bezpečnosti je klíčové spojení dat a vytvoření kontextu, který z nich vytváří informaci. Pokud bychom se drželi úzké definice informační bezpečnosti a chránili pouze informace, mohlo by dojít k vážným bezpečnostním problémům. (Kolouch, 2019)

V kyberprostoru jsou data a informace přenášeny prostřednictvím počítačových systémů, které jsou součástí širšího rámce kybernetické bezpečnosti. S ohledem na to je vhodné aplikovat triádu CIA nejen na informace, ale i na data a počítačové systémy. (Kolouch, 2019) Důvěrnost znamená, že k informacím, datům nebo ICT mají přístup pouze autorizované subjekty. Pro efektivní správu a ochranu informací je důležité zavést klasifikaci informací, kterou lze aplikovat i na další složky kybernetické bezpečnosti. (Kolouch, 2019)

Integrita se vztahuje na přesnost a úplnost dat a informací, přičemž porušení integrity znamená neautorizované změny, které mohou být dlouho neodhaleny. Je to záruka, že systémy a data zůstanou nepoškozené a nezměněné, pokud k tomu není oprávněná osoba. (Kolouch, 2019)

Dostupnost je zajištění přístupu k informacím, datům nebo počítačovým systémům, když je to potřeba. Bez dostupnosti není systém využitelný, i když splňuje ostatní požadavky na integritu a bezpečnost. (Kolouch, 2019)

Pokud bychom chtěli popsat prostor kybernetické bezpečnosti, můžeme tento prostor definovat jako průnik tří principů triády CIA, které zahrnují důvěrnost, integritu a dostupnost. (Kolouch, 2019)

2.2 TOR

Tor (The Onion Router) je anonymizační síť, která pomáhá uživatelům chránit jejich soukromí a bezpečnost na internetu. Namísto přímého připojení k webovým stránkám využívá síť dobrovolně provozovaných serverů, přes které přesměrovává internetový provoz pomocí vrstveného šifrování. Tento systém umožňuje uživatelům skrýt svou identitu a zároveň poskytuje nástroj k obcházení cenzury. Tor je užitečný pro běžné uživatele, novináře, aktivisty, právníky, firmy i vládní organizace, kteří potřebují bezpečně komunikovat či anonymně přistupovat k informacím. (2019)

Jednou z hlavních hrozeb, proti nimž Tor chrání, je tzv. analýza provozu, která umožňuje třetím stranám sledovat, kdo s kým komunikuje, odkud pochází internetový provoz a kam směřuje. I když je obsah komunikace šifrován, samotné metadaty mohou prozradit citlivé informace. Tor tento problém řeší tak, že data procházejí přes několik náhodně vybraných serverů (tzv. relé), přičemž žádný z nich nezná celou trasu přenosu. Každý server v řetězci zná pouze svého předchůdce a následovníka, což eliminuje možnost sledování kompletní komunikace. (2019)

Tor je nejen prostředkem pro anonymní prohlížení internetu, ale také umožňuje provoz tzv. onion služeb, což jsou webové stránky a služby, jejichž umístění není možné zjistit. To je výhodné například pro novináře komunikující s whistleblowery nebo pro organizace poskytující citlivé informace. Tor využívají i firmy ke skrytí svých obchodních strategií a ochraně před průmyslovou špionáží. Americká armáda jej používá k získávání otevřených zdrojových informací a orgány činné v trestním řízení ke sledování webových stránek bez odhalení své identity. (2019)

Přestože Tor poskytuje vysokou míru anonymity, není zcela imunní vůči útokům. Například pokud útočník monitoruje jak zdrojovou, tak cílovou adresu komunikace, může statistickou analýzou odhalit, že jsou propojené. Uživatelé by proto měli být opatrní a doplňovat Tor o další bezpečnostní opatření, jako je používání Tor Browseru a nevyplňování citlivých údajů na webových formulářích. (2019)

Tor je neustále vylepšován, aby byl bezpečnější a uživatelsky přívětivější. Čím více lidí jej používá a provozuje jeho relé, tím silnější se síť stává. V době rostoucího sledování a

omezení online svobody je Tor důležitým nástrojem pro ochranu soukromí a svobody slova. Uživatelé se mohou zapojit nejen jako běžní uživatelé, ale i jako dobrovolníci provozující relé nebo přispívající k vývoji softwaru. (2019)

2.2.1 VPN over TOR

VPN over Tor je metoda, při níž se uživatel nejprve připojí k síti Tor a následně naváže spojení s VPN serverem. Tento přístup nabízí specifické výhody, jako je další vrstva šifrování a možnost přístupu k webovým stránkám, které blokují výstupní uzly Toru. Za značnou výhodu lze považovat také to, že poskytovatel VPN nevidí skutečnou IP adresu uživatele. Nicméně, implementace této metody je technicky náročná a může vést k výraznému snížení rychlosti připojení. Zároveň pro uskutečnění tohoto připojení VPN poskytovatel musí podporovat připojení přes Tor (většina běžných VPN služeb tento typ připojení neumožňuje). Ideální případ pro použití této metody připojení je když potřebujete přístup k webovým stránkám, které blokují Tor. Obecně se doporučuje pouze pokročilým uživatelům, kteří rozumí konfiguraci obou technologií a jsou si vědomi potenciálních rizik spojených s kompromitací soukromí. (Proton, 2024)

2.2.2 TOR over VPN

Tor over VPN je metoda, při níž se uživatel nejprve připojí k virtuální privátní síti (VPN) a následně využívá síť Tor. Tento přístup poskytuje dodatečnou vrstvu ochrany soukromí a bezpečnosti. Při použití této metody je internetový provoz nejprve šifrován a směrován přes VPN server, čímž je skryta skutečná IP adresa uživatele. Následně je tento šifrovaný provoz přesměrován do sítě Tor, která dále anonymizuje uživatele tím, že jeho data prochází přes několik náhodně vybraných uzlů před dosažením cílové destinace. (Sidor, 2024)

Výhody tohoto přístupu zahrnují skrytí skutečné IP adresy uživatele před vstupními uzly sítě Tor, což zvyšuje úroveň anonymity. Poskytovatel internetových služeb (ISP) vidí pouze šifrované připojení k VPN, aniž by věděl o použití sítě Tor. To může být užitečné v zemích, kde je používání Toru omezeno nebo monitorováno. (Sidor, 2024)

Nevýhody zahrnují snížení rychlosti připojení, protože kombinace VPN a Tor přidává latenci. Také je důležité důvěřovat poskytovateli VPN, protože má přístup k reálné IP adrese uživatele. Nesprávná konfigurace nebo použití nedůvěryhodné VPN může vést ke snížení úrovně anonymity. (Sidor, 2024)

Fungování této metody spočívá v tom, že uživatel nejprve naváže šifrované spojení s VPN serverem. Poté, co je toto spojení navázáno, veškerý internetový provoz prochází přes VPN a následně je směrován do sítě Tor. Tím je zajištěno, že vstupní uzly Toru vidí jako zdrojovou IP adresu pouze IP adresu VPN serveru, nikoli skutečnou IP adresu uživatele. (Sidor, 2024)

Je důležité poznamenat, že použití Toru ve spojení s VPN není obecně doporučováno pro běžné uživatele, pokud nejsou dostatečně obeznámeni s konfigurací obou technologií a neznají potenciální rizika spojená s kompromitací soukromí. (Sidor, 2024)

2.2.3 MAC adresa

MAC adresa (Media Access Control) je jedinečný identifikátor přiřazený síťovému zařízení, který slouží k jeho jednoznačné identifikaci v síti. Tato adresa, známá také jako fyzická nebo hardwarová adresa, je obvykle přiřazena síťové kartě výrobcem a zůstává konstantní po celou dobu životnosti zařízení. MAC adresy se používají jako síťová adresa pro většinu síťových technologií IEEE 802, včetně Ethernetu a Wi-Fi. (Bryce, 2024)

Přestože je MAC adresa pevně zakódována v síťovém rozhraní, existují metody, jak ji softwarově změnit. Tato změna může být užitečná z různých důvodů, jako je ochrana soukromí, obcházení síťových omezení nebo řešení problémů s připojením. Například ve Windows lze MAC adresu změnit prostřednictvím Správce zařízení, kde v nastavení síťového adaptéru v sekci „Upřesnit“ lze upravit položku „Síťová adresa“. V Linuxu je možné použít příkazový řádek s příkazy jako 'ifconfig' nebo 'ip link', případně specializované nástroje jako 'macchanger'. (Merissa, 2025)

Je důležité poznamenat, že i když lze MAC adresu softwarově změnit, síťoví administrátoři mohou takové změny detekovat pomocí různých metod, jako je srovnávání MAC adres s databázemi výrobců nebo analýza síťového provozu. Proto by změna MAC adresy měla být prováděna s ohledem na platné zákony a pravidla sítě. (Bryce, 2024)

2.3 Heslo

Heslo je tajný údaj, obvykle ve formě slova, fráze nebo kombinace znaků, který slouží k ověření identity uživatele a k ochraně přístupu k systémům, účtům či informacím. Historicky se hesla používala v armádě jako předem domluvená slova pro rozlišení mezi vlastními a

nepřátelskými bojovníky, což pomáhalo zajistit bezpečnou komunikaci a identifikaci spojenců v bojových situacích. (NÚKIB, 2023)

Podle Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) je pravidelná změna hesel důležitá, protože snižuje riziko jejich kompromitace. Pokud útočník získá heslo, pravidelnou změnou lze omezit dobu, po kterou by jej mohl zneužívat. NÚKIB však zároveň doporučuje spíše používání silných a unikátních hesel než jejich častou změnu, která může vést k používání slabších hesel. (NÚKIB, 2023)

Existuje doporučený postup pro volbu hesla. Za prvé, silné přístupové fráze, ne hesla, by měly být dlouhé – alespoň dvacet až dvacet pět znaků. Náhodné znaky – například ck5iogh#skf&skd – fungují dobře. Bohužel lidská mysl má potíže s pamatováním si náhodných sekvencí. Proto používejte správce hesel. Použití správce hesel je mnohem lepší než si heslo vybírat sami. Preferuji open-source správce hesel, jako jsou Password Safe a KeePass, které ukládají data pouze lokálně na vašem počítači. (Vamosi, a další, 2019)

Dalším důležitým pravidlem pro dobrá hesla je nikdy nepoužívat stejné heslo pro dva různé účty. To je těžké, protože dnes máme hesla skoro ke všemu. Proto používejte správce hesel, které vám pomohou generovat a ukládat silná, jedinečná hesla. (Vamosi, a další, 2019)

I když máte silné heslo, technologie ho stále dokáže prolomit. Existují programy pro hádání hesel, jako například „John the Ripper“, což je bezplatný open-source program, který si kdokoli může stáhnout a který funguje na základě konfiguračních parametrů nastavených uživatelem. Například uživatel může určit, kolik znaků by měl program vyzkoušet, zda má použít speciální symboly, zda má zahrnout sady cizích jazyků a podobně. John the Ripper a další programy na prolomení hesel dokážou měnit písmena hesel podle sad pravidel, které jsou extrémně efektivní při jejich lámání. To znamená, že postupně zkouší každou možnou kombinaci čísel, písmen a symbolů v rámci daných parametrů, dokud se heslo nepodaří prolomit. (Vamosi, a další, 2019)

3 ŠIFROVÁNÍ

Od nepaměti existovala potřeba zajistit, aby důležité zprávy mohly číst pouze určené osoby, zejména v obchodní a vojenské komunikaci. K dosažení této ochrany se postupně vyvíjely metody, počínaje jednoduchými záměnami písmen za jiné znaky až po dnešní pokročilé šifrovací algoritmy. Šifrování představuje proces, při kterém se čitelný text (nebo data obecně) převádí na nečitelnou podobu pomocí určitého algoritmu. Opačný proces, tedy převod zpět do původní podoby, se nazývá dešifrování. Jak šifrování, tak dešifrování využívá tajný parametr známý jako (de)šifrovací klíč. Jen ten, kdo tento klíč vlastní, může zprávu zpětně převést na srozumitelný text. Aby byla šifra bezpečná, musí odolat pokusům o prolomení bez znalosti klíče. Kyberzločinci dnes využívají výkonné počítače a pokročilé metody k pokusům o dešifrování, ale kvalitní šifrovací algoritmus zajistí, že takový proces by trval extrémně dlouho, což útočníky odradí. (2025)

3.1.1 Biometrické šifrování

Biometrické šifrování je metoda zabezpečení dat, která kombinuje biometrické údaje s kryptografickými technikami. Využívá jedinečné fyziologické nebo behaviorální charakteristiky jednotlivce, jako jsou otisky prstů, rozpoznávání obličeje či skenování duhovky, k vytvoření nebo ochraně kryptografických klíčů. Tím se zvyšuje úroveň zabezpečení, protože biometrické údaje jsou pro každého člověka unikátní a obtížně padělatelné. Tato technologie nachází uplatnění v oblastech, kde je vyžadována vysoká úroveň ochrany informací, například v bankovníctví, zdravotnictví či vládních institucích. Integrace biometrických údajů do šifrovacích systémů zajišťuje, že k citlivým datům mají přístup pouze oprávněné osoby, což minimalizuje riziko neoprávněného přístupu. (Bitto, 2005)

3.1.2 Kryptologie

Kryptologie je vědní obor zabývající se studiem metod pro zabezpečení komunikace prostřednictvím šifrování a dešifrování informací. Její název pochází z řeckých slov „kryptós“ (skrytý) a „lógos“ (věda). Moderní kryptologie využívá pokročilé matematické metody, včetně teorie čísel a algebraických struktur, k vytváření komplexních šifrovacích algoritmů. Tyto algoritmy zajišťují důvěrnost, integritu, autentizaci a nepopíratelnost informací. Například asymetrické šifrovací metody, jako je RSA, využívají dvojici klíčů – veřejný a soukromý – k zabezpečení komunikace. (Cimino, 2018)

3.1.2.1 Kryptografie

Jedná se o součást kryptografie, která se zabývá návrhem a analýzou šifrovacích metod a algoritmů, které umožňují bezpečnou výměnu informací mezi stranami. Využívá matematické algoritmy k převodu čitelného textu na nečitelnou formu (šifrový text) a zpět.

Existují dva hlavní typy kryptografie:

- Symetrická kryptografie: Používá stejný klíč pro šifrování i dešifrování. Je rychlá a efektivní, ale vyžaduje bezpečné sdílení klíče mezi komunikujícími stranami.
- Asymetrická kryptografie: Využívá dvojici klíčů – veřejný klíč pro šifrování a soukromý klíč pro dešifrování. Tato metoda poskytuje vyšší úroveň bezpečnosti a je základem pro digitální podpisy a certifikáty. (Cimino, 2018)

3.1.2.2 Kryptoanalýza

Součástí kryptologie, kdy v tomto případě se jedná o disciplínu zaměřenou na studium metod prolomení šifrovacích systémů. Cílem je získat přístup k původnímu textu bez znalosti šifrovacího klíče. Kryptoanalytici využívají různé techniky, jako je analýza vzorců, statistická analýza nebo útoky hrubou silou, aby identifikovali slabiny v šifrovacích algoritmech a navrhli efektivní metody jejich prolomení. (Cimino, 2018)

3.1.3 Symetrické šifrování

Symetrické šifrování je základní technika v kryptografii, při které se pro šifrování i dešifrování dat používá stejný tajný klíč. Tento klíč musí být bezpečně sdílen mezi odesílatelem a příjemcem, protože jakákoli kompromitace klíče by znamenala ohrožení celého systému. Symetrické šifrování je efektivní, rychlé a vhodné pro šifrování velkých objemů dat, což je činí užitečné v oblastech, jako je šifrování disků, ochrana komunikace v reálném čase nebo šifrování souborů. (Poggi, 2021)

Při symetrickém šifrování je hlavním úkolem použít algoritmus, který zaručí, že při použití stejného klíče pro šifrování a dešifrování bude možné obnovit původní data pouze tím, kdo má správný klíč. K tomu slouží různé šifrovací algoritmy. Mezi nejznámější a nejčastěji používané patří DES (Data Encryption Standard), který byl široce používán, ale postupem času se ukázal jako zranitelný kvůli příliš malé délce klíče. Proto byl nahrazen pokročilejším algoritmem AES (Advanced Encryption Standard), který je považován za bezpečný a efektivní pro moderní aplikace. (Poggi, 2021)

AES podporuje různé délky klíče (128, 192 a 256 bitů) a je považován za velmi bezpečný i proti moderním metodám analýzy. Tento algoritmus je široce používán v různých aplikacích, od šifrování internetového přenosu až po šifrování dat na pevných discích. Symetrické šifrování je tedy klíčové pro zajištění důvěrnosti dat a je součástí téměř každého šifrovacího systému na světě. (Poggi, 2021)

3.1.4 Asymetrické šifrování

Asymetrické šifrování, také známé jako šifrování s veřejným a soukromým klíčem, je metoda kryptografie, která využívá dvojici klíčů: veřejný a soukromý. Tento systém umožňuje šifrování a dešifrování bez nutnosti sdílet stejný klíč mezi odesílatelem a příjemcem. Veřejný klíč je určen pro šifrování zpráv, zatímco soukromý klíč je používán pro jejich dešifrování. Tento princip poskytuje výrazně vyšší úroveň bezpečnosti ve srovnání se symetrickým šifrováním, protože soukromý klíč nikdy neopustí zařízení příjemce a nemusí být sdílen. (Poggi, 2021)

Asymetrické šifrování je základem pro různé aplikace, jako jsou digitální podpisy a certifikáty, které zajišťují autenticitu a integritu dat. Když odesílatel zašifruje zprávu veřejným klíčem, pouze příjemce, který má odpovídající soukromý klíč, může zprávu dešifrovat. Tento systém se často používá v kombinaci s dalšími technologiemi, například v protokolech SSL/TLS pro bezpečnou komunikaci na internetu. (Poggi, 2021)

Mezi nejběžnější asymetrické algoritmy patří RSA (Rivest-Shamir-Adleman), který využívá faktorizaci velkých čísel, a ElGamal, který je založen na problému diskretního logaritmu. Tyto algoritmy jsou široce používány v oblasti digitálních podpisů, šifrování e-mailů a při ověřování identity v moderních systémech. (Poggi, 2021)

Výhoda asymetrického šifrování spočívá v jeho flexibilitě a bezpečnosti, jelikož veřejný klíč může být distribuován veřejně, aniž by to ohrozilo soukromí komunikace. Na druhou stranu, je náročnější na výpočetní výkon než symetrické šifrování, což může ovlivnit jeho použití v některých aplikacích. (Poggi, 2021)

3.1.5 Hashování

Hashování je proces převodu libovolně dlouhých vstupních dat na výstup pevné délky, nazývaný hash nebo otisk. Tento výstup je unikátní pro každý vstupní soubor a jakákoliv změna ve vstupu vede k odlišné hashové hodnotě. Hashovací funkce jsou široce využívány v kryptografii, například při ověřování integrity dat, ukládání hesel nebo vytváření digitálních podpisů. Mezi nejznámější hashovací algoritmy patří MD5, SHA-1 a SHA-256. MD5 a SHA-1 jsou dnes považovány za zranitelné vůči kolizím, což znamená, že mohou existovat různé vstupy, které vedou ke stejné hashové hodnotě. SHA-256, součást rodiny SHA-2, je považován za bezpečnější a je široce používán v moderních aplikacích. Při hashování hesel je důležité použít bezpečné hashovací algoritmy a techniky, jako je přidání náhodného řetězce (salt) k heslu před jeho hashováním, aby se zvýšila bezpečnost uložených hesel. (Štráfelda, 2023)

3.1.6 Elektronický podpis

Elektronický podpis představuje data v digitální podobě, která jsou připojena k jiným elektronickým datům nebo s nimi logicky propojena a slouží k vyjádření souhlasu podepisující osoby. Jeho hlavním cílem je zajistit, aby elektronické dokumenty měly obdobnou právní platnost jako papírové dokumenty podepsané ručně. (Běhounková, 2024)

Elektronické podpisy se dělí na několik typů podle úrovně zabezpečení a právní síly. Základní variantou je prostý elektronický podpis, který může mít podobu naskenovaného ručního podpisu nebo textu napsaného na klávesnici. Pokročilejší variantou je zaručený elektronický podpis, který zajišťuje nejen identifikaci podepisující osoby, ale i odhalení případných úprav podepsaných dat. Nejvyšší úroveň zabezpečení pak představuje kvalifikovaný elektronický podpis, jenž je vytvořen prostřednictvím certifikovaného zařízení a odpovídá vlastnoručnímu podpisu z hlediska právní váhy. (Běhounková, 2024)

Díky elektronickým podpisům je možné efektivněji a rychleji podepisovat smlouvy, faktury a další důležité dokumenty bez nutnosti fyzické přítomnosti. Jejich zavedení významně přispělo ke zvýšení bezpečnosti a zjednodušení procesů při digitálních transakcích a komunikaci. (Běhounková, 2024)

3.1.7 Postkvantová kryptografie

Postkvantová kryptografie se v současnosti stává klíčovým tématem v oblasti informační bezpečnosti, neboť kvantové počítače představují vážnou hrozbu pro tradiční šifrovací metody. Kvantové počítače mají potenciál výrazně zrychlit řešení matematických problémů, na nichž stojí současné asymetrické šifrovací algoritmy jako RSA, Diffie-Hellman či ECC. Zatímco tyto algoritmy jsou pro běžné počítače extrémně náročné na prolomení, kvantové stroje vybavené Shorovým algoritmem dokáží tuto úlohu vyřešit v exponenciálně kratším čase, což zásadně oslabuje současné metody ochrany citlivých dat. I symetrická kryptografie, například algoritmy AES, je kvantovými technologiemi ohrožena, přestože Groverův algoritmus pouze zvyšuje efektivitu útoku na polovinu současné výpočetní složitosti, což lze vyvážit zvětšením délky klíče. (Houba, 2025)

Postkvantová kryptografie proto vyvíjí nové algoritmy, které budou odolné nejen vůči útokům tradičních počítačů, ale i těch kvantových. Mezi perspektivní přístupy patří metody založené na mřížových problémech, kódové kryptografii, mnohorozměrných polynomiálních rovnicích či hashovacích funkcích. Tyto algoritmy využívají matematické problémy, které zůstávají výpočetně složité i pro kvantové počítače. (Houba, 2025)

Vzhledem k rostoucí potřebě přechodu na bezpečnější kryptografické systémy zahájil americký Národní institut pro standardy a technologie (NIST) v roce 2016 proces standardizace postkvantových algoritmů. Po několika letech testování a výběrových kol byly v roce 2022 oznámeny první vybrané algoritmy, mezi nimiž figurují například Kyber, Dilithium nebo Falcon. Tyto algoritmy kombinují vysokou bezpečnost s efektivní výpočetní náročností a představují základ pro budoucí bezpečnostní standardy. (Houba, 2025)

Postkvantová kryptografie je klíčová pro ochranu citlivých dat v nadcházející éře kvantových počítačů. Přejít na tyto nové metody je nezbytný nejen pro státní instituce a finanční sektor, ale i pro běžné uživatele, jejichž data jsou stále více vystavena digitálním hrozbám. Vzhledem k rychlému pokroku v oblasti kvantových technologií je důležité, aby organizace i jednotlivci začali včas plánovat migraci na postkvantové šifrovací systémy a zajistili tak bezpečnost své digitální komunikace a datové infrastruktury. (Houba, 2025)

3.1.8 Instant messaging

Instant messaging (IM) se poprvé objevil již v 60. letech minulého století v rámci systémů jako CTSS a Multics, které umožňovaly komunikaci mezi více uživateli. Skutečný rozmach této technologie však nastal až v 90. letech, kdy se služby jako ICQ a AOL Instant Messenger dostaly do širšího povědomí veřejnosti. (Borth, 2025)

IM představuje formu online komunikace, která umožňuje uživatelům okamžitě si vyměňovat textové zprávy, multimediální soubory, a také provádět hlasové hovory a videohovory přes internet. Jeho hlavním přínosem je schopnost zajistit rychlou a efektivní komunikaci mezi jednotlivci či skupinami, ať už v osobním nebo pracovním kontextu. Vedle textových zpráv mohou uživatelé sdílet obrázky, videa, dokumenty a další soubory, čímž se zvyšuje interaktivita a usnadňuje spolupráce. (Borth, 2025)

Instant messaging přináší několik klíčových výhod. Mezi hlavní patří rychlost, kdy jsou zprávy doručovány prakticky ihned, což urychluje proces rozhodování. Další předností je možnost sledovat dostupnost kontaktů, díky čemuž lze komunikaci zahájit v optimálním čase. Moderní IM aplikace navíc nabízejí širokou škálu funkcí – vedle textové komunikace umožňují i hlasové hovory, videohovory a sdílení různorodých souborů. (Borth, 2025)

Díky těmto vlastnostem se instant messaging stal nepostradatelným nástrojem pro efektivní komunikaci, který se osvědčil jak v pracovním prostředí, tak i při běžné osobní komunikaci. (Borth, 2025)

3.1.9 Online identita

Online identita, často označovaná také jako digitální identita, představuje souhrn informací o jednotlivci dostupných v online prostředí. Tyto informace zahrnují osobní údaje, fotografie, příspěvky na sociálních sítích, e-mailové adresy, uživatelská jména a další digitální stopy, které uživatel zanechává na internetu. S rozvojem internetu a digitálních technologií vznikla potřeba reprezentace jednotlivců v online prostředí. Online identita umožňuje efektivní komunikaci, obchodní transakce a přístup k různým službám bez nutnosti fyzické přítomnosti. Postupem času se stala nezbytnou součástí digitálního světa, umožňující nejen identifikaci, ale i personalizaci a zabezpečení online interakcí. (McGowan, 2023)

Účel a využití online identity:

- Autentizace a ověřování totožnosti – Online identita slouží k přihlašování do služeb, jako jsou e-maily, sociální sítě, internetové bankovníctví nebo e-shopy.
- Personalizace služeb – Firmy a platformy využívají online identitu k přizpůsobení obsahu a nabídek podle preferencí uživatele.
- Sociální interakce – Pomáhá uživatelům komunikovat na sociálních sítích, v diskusních fórech nebo prostřednictvím chatovacích aplikací.
- Online nakupování a transakce – Umožňuje bezpečné platby, správu účtů a sledování objednávek.
- Zabezpečení a ochrana dat – Správná správa online identity pomáhá předcházet krádeži identity a podvodům. (McGowan, 2023)

Online identita je klíčová pro efektivní a bezpečný pohyb v digitálním prostoru. (McGowan, 2023)

3.1.10 E-mail

E-mail, zkráceně z anglického „electronic mail“ (elektronická pošta), je služba umožňující odesílání a přijímání textových zpráv přes elektronické komunikační systémy. Kromě textu lze k e-mailům připojovat i různé přílohy, jako jsou dokumenty, obrázky či jiné soubory. Funguje na principu přenosu dat mezi e-mailovými servery a klienty. První koncept e-mailu byl vyvinut v roce 1971 programátorem Rayem Tomlinsonem, který vytvořil systém pro odesílání zpráv mezi počítači pomocí symbolu @ k oddělení uživatelského jména a domény. Tento princip se stal standardem pro e-mailovou komunikaci. (Mikláš, 2010)

Díky své univerzálnosti se e-mail využívá v různých oblastech, od osobní komunikace po profesionální a marketingové účely. Umožňuje efektivní výměnu zpráv mezi jednotlivci i skupinami, a to bez ohledu na časovou nebo geografickou vzdálenost. V pracovním prostředí slouží jako klíčový nástroj pro komunikaci mezi zaměstnanci, partnery a zákazníky. Kromě textových zpráv lze prostřednictvím e-mailu připojovat různé typy souborů, včetně dokumentů, tabulek, obrázků či multimediálních souborů, což usnadňuje spolupráci na projektech. E-mail je často využíván v akademickém, firemním a státním sektoru pro zasílání oficiálních dokumentů, smluv či oznámení, díky čemuž nahrazuje tradiční

papírovou korespondenci. Firmy používají e-mail pro zasílání reklamních sdělení, newsletterů a zákaznické podpory. E-mailový marketing umožňuje cílené oslovování zákazníků a budování dlouhodobých vztahů s klienty. E-mailová adresa také slouží jako identifikátor uživatele při registraci do různých online služeb, jako jsou sociální sítě, internetové bankovníctví nebo e-shopy. (Mikláš, 2010)

4 LEGISLATIVA SOUVISEJÍCÍ S ANONYMITOU NA INTERNETU

Legislativa týkající se anonymity na internetu v České republice je upravena několika klíčovými právními předpisy, přičemž zásadní roli zde hrají Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a Zákon č. 110/2019 Sb., o zpracování osobních údajů. Tyto normy se zaměřují na ochranu uživatelů v digitálním prostředí, regulaci správců dat a poskytovatelů internetových služeb a zároveň stanovují povinnosti pro zajištění kybernetické bezpečnosti. (NÚKIB, 2024)

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, představuje klíčový právní rámec zaměřený na zajištění bezpečného provozu informačních systémů a sítí v České republice. Tento zákon klade důraz na ochranu kritické infrastruktury, veřejné správy i významných soukromých subjektů před kybernetickými hrozbami. Součástí zákona jsou požadavky na zavedení bezpečnostních opatření, monitoring sítí a povinnost ohlašovat bezpečnostní incidenty. Ačkoli zákon primárně neřeší anonymitu samotných uživatelů internetu, nepřímo ovlivňuje možnosti zachování soukromí online. Například poskytovatelé internetových služeb a správci systémů mohou být v rámci prevence kybernetických útoků povinni shromažďovat určité údaje o uživateli, což může anonymitu částečně omezit. (ČESKO, 2014)

Zákon č. 110/2019 Sb., o zpracování osobních údajů, který implementuje nařízení GDPR v českém právním řádu, významně posiluje ochranu osobních údajů uživatelů internetu. Tento zákon zajišťuje, že osobní údaje mohou být zpracovávány pouze na základě jasně definovaných právních důvodů a s přihlédnutím k zásadě minimalizace dat. Pro anonymitu na internetu je klíčové, že zákon zavádí přísné podmínky pro zpracování údajů umožňujících identifikaci jednotlivců. Pokud uživatelé využívají anonymizační nástroje, VPN nebo šifrovací technologie, poskytovatelé služeb mohou pouze v omezených případech vyžadovat informace o jejich identitě. Výjimku tvoří případy, kdy je zjištění identity nezbytné pro prevenci trestné činnosti, ochranu veřejné bezpečnosti nebo zajištění obrany státu. (ČESKO, 2019)

Prostřednictvím těchto zákonů se Česká republika snaží vyvážit ochranu kybernetické bezpečnosti s právem jednotlivců na soukromí a anonymitu při používání internetu. Přestože Zákon o kybernetické bezpečnosti může v určitých situacích vést k omezení anonymity v

zájmu veřejné bezpečnosti, Zákon o zpracování osobních údajů chrání uživatele před neoprávněným zneužitím jejich dat. V důsledku toho mají občané právo využívat nástroje pro zvýšení anonymity, avšak v mezích zákonných povinností stanovených pro ochranu kybernetické bezpečnosti a veřejného pořádku. (NÚKIB, 2024)

5 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

Teoretická část této bakalářské práce se zabývala klíčovými aspekty problematiky anonymity na internetu, která se v současné době stává stále více diskutovaným a důležitým tématem. Důvodem, proč jsem se tomuto tématu věnoval, je rostoucí význam ochrany osobních údajů a soukromí uživatelů v digitálním světě, kde se rizika jejich zneužití neustále zvyšují.

V úvodu teoretické části byla definována základní terminologie týkající se internetu, včetně jeho historie, významu kyberprostoru a základů kybernetické bezpečnosti. Uvedl jsem také problematiku dat, která uživatelé vytvářejí při své každodenní činnosti na internetu, s důrazem na rozdíly mezi běžnými, citlivými daty a metadaty. V kontextu zvyšujícího se množství generovaných dat bylo důležité poukázat na možné způsoby jejich zneužití a rizika pro uživatele.

Dále jsem se věnoval konkrétním aspektům anonymity, zejména definici anonymity a významu hnutí Cypherpunk, které hrálo významnou roli ve vývoji technologií umožňujících anonymní komunikaci na internetu. Významným prvkem teoretické části byl popis technologií a nástrojů, jako jsou Tor, VPN, šifrování a zabezpečení hesel, které uživatelé mohou využít k posílení svého soukromí a minimalizaci digitálních stop.

Teoretická část také zahrnovala kapitolu o legislativních opatřeních a zásadách kybernetické bezpečnosti, která určují právní rámec ochrany soukromí v digitálním prostředí. Analyzoval jsem význam jednotlivých technologií v souvislosti se současnými bezpečnostními hrozbami, jako jsou kybernetické útoky, hackerství či sledování uživatelů.

Důvodem pro detailní rozbor těchto oblastí bylo vytvoření uceleného přehledu o aktuálním stavu problematiky anonymity na internetu. Tento přehled slouží jako základ pro následující praktickou část práce, ve které jsou pomocí kvantitativního výzkumu zkoumány postoje uživatelů k anonymitě a jejich konkrétní chování ve vztahu k ochraně svého digitálního soukromí. Cílem tohoto závěru je shrnout získané poznatky a připravit půdu pro praktickou část práce, jejímž výstupem budou konkrétní doporučení pro zvýšení úrovně anonymity a bezpečnosti běžných uživatelů internetu.

II. PRAKTICKÁ ČÁST

6 IDENTIFIKACE SOUVISEJÍCÍCH RIZIK

Internet se stal nedílnou součástí našeho každodenního života, což vyplývá i z výsledků dotazníkového šetření, kde respondenti využívají internetové prostředí k práci, komunikaci, nákupům a sdílení osobních informací, přičemž během těchto aktivit na uživatele číhá celá řada nebezpečí, jako jsou např. škodlivé softwary, kyberšikana, krádeže osobních údajů, či finančních prostředků. Abychom se jim vyhnuli, je důležité chovat se na internetu zodpovědně a dodržovat základní pravidla bezpečného chování. Díky tomu můžeme předejít nepříjemnostem, které by mohly mít vážné následky. (Hvězda, 2024)

6.1 Sledování uživatele

I při zcela běžném používání internetu jsou uživatelé často vystaveni sledování, aniž by si to sami uvědomovali. Každá jejich činnost – ať už se jedná o odeslání e-mailu, přístup k online bankovníctví, přihlášení na sociální síť nebo přehrávání videa – zanechává digitální stopy. Tyto stopy je možné analyzovat a následně využít k monitorování aktivit uživatele nebo ke tvorbě jeho podrobného profilu. Například při zasílání e-mailu se kromě samotné zprávy přenášejí i tzv. metadata, která zahrnují IP adresu odesílatele, čas doručení, typ e-mailového klienta a informace o trasování zprávy přes e-mailové servery. Díky těmto údajům lze přesně určit, odkud byla zpráva odeslána a jaký byl její technický průběh. Pokud uživatel využívá služby jako je Gmail, jeho aktivita je navíc sledována i s cílem přizpůsobit mu reklamy a personalizovat prostředí služeb. (Špaček, 2021)

Dle dotazníkového šetření respondenti tráví čas na internetu také při online studiu prostřednictvím univerzitních systémů nebo vzdělávacích portálů, kde bývá zaznamenáváno, jaké studijní materiály student prohlíží, jak dlouho se na stránkách zdržuje, kdy se přihlašuje nebo co odevzdává. U služeb zaměřených na streamování videa a hudby, jako je YouTube, Spotify nebo Netflix, jsou kromě samotného obsahu sledovány i reakce uživatele, čas sledování, typ zařízení či oblíbené žánry. Algoritmy těchto platforem sbírají údaje o chování a zájmech uživatelů, což jim umožňuje doporučovat relevantní obsah, ale zároveň tím vytvářejí velmi detailní osobní profily, které mohou být využity i za komerčními účely. (Špaček, 2021)

Při přihlašování do internetového bankovníctví dochází ke zpracování vysoce citlivých informací – zaznamenává se nejen IP adresa, ale i poloha zařízení, typ připojení nebo způsob

ověření identity. Ačkoliv jsou tyto údaje určeny především ke zvýšení bezpečnosti, v případě úniku mohou být snadno zneužity. Sociální sítě pak sledují uživatele na zcela systematické úrovni. Zaznamenávají se nejen zveřejněné příspěvky a interakce, ale i aktivita v čase, geolokace či spojení s jinými účty. Platformy jako Facebook nebo Instagram využívají kromě interního sledování i nástroje, které fungují mimo samotnou síť – například sledovací pixely nebo soubory cookies vložené do externích webových stránek. Veškeré tyto informace přispívají k vytváření rozsáhlého digitálního obrazu každého uživatele, který může být následně využit nejen k personalizaci obsahu, ale také k ovlivňování chování, cílené reklamě, nebo dokonce k diskriminaci a porušování soukromí. (Špaček, 2021)

6.1.1 Cookies

Internetová reklama je dnes obrovský byznys a její úspěšnost stojí na sledování uživatelů. Základním nástrojem, který tuto činnost umožňuje, jsou cookies – malé textové soubory uložené v prohlížeči. Původně sloužily k usnadnění práce uživatelům, například k zapamatování přihlašovacích údajů nebo nastavení webových stránek. Velmi rychle se však staly nástrojem pro reklamní společnosti, které je využívají k podrobnému sledování aktivit uživatelů napříč různými weby. Reklamní společnosti jako Google nebo Facebook využívají tzv. cookies třetích stran. Když například uživatel navštíví web CNN, neukládají se do jeho prohlížeče pouze cookies od CNN, ale i od různých reklamních partnerů. Pokud tento uživatel poté přejde na jiný web, který spolupracuje s těmito reklamními partnery, systém ho ihned rozpozná a nabídne mu reklamy odpovídající jeho předchozímu chování. Takto se postupně vytváří detailní uživatelský profil, který pomáhá firemním algoritmům přesně zacílit reklamu podle věku, zájmů nebo nákupního chování. (Evans, 2019)

Problémem tohoto systému je, že uživatelé ztrácejí kontrolu nad svými osobními daty. Většina webových stránek sice v zásadách ochrany soukromí uvádí, že shromažďují informace o návštěvnicích, ale většina lidí tyto dokumenty nečte. To umožňuje firmám sbírat a analyzovat ohromné množství údajů, často bez jasného souhlasu uživatele. Typickým příkladem sledování je situace, kdy uživatel navštíví zpravodajský web a obdrží několik sledovacích cookies. Poté se přesune na YouTube, kde dostane další, tentokrát od jiných reklamních sítí. YouTube zároveň analyzuje jeho chování – například zda dokoukal reklamu do konce nebo zda na ni klikl. Všechny tyto údaje jsou následně propojeny a reklamní algoritmy dokážou určit, že jde například o 32letého muže se zájmem o turistiku. Na základě toho mu začnou být zobrazovány reklamy na outdoorové vybavení, sportovní oblečení nebo

dovolené v horách. Tento proces se opakuje každý den a vytváří složitou síť sledování, která pokrývá prakticky celý internet. Aby se omezilo nekontrolované sledování uživatelů, Evropská unie v roce 2018 zavedla nařízení GDPR, které mělo posílit ochranu soukromí. Webové stránky jsou nyní povinny informovat uživatele o používání cookies a získat jejich výslovný souhlas. V praxi však mnoho firem tento požadavek obchází – například tím, že zobrazují vyskakovací okna s výrazným tlačítkem „Souhlasím“, zatímco možnost odmítnutí cookies je složitě skrytá nebo vyžaduje ruční nastavení. (Evans, 2019)

Jedním z největších hráčů v oblasti sledování je Google, který na rozdíl od jiných společností tolik nevyužívá cookies třetích stran, protože on sám je třetí stranou. Google Ads se objevují na obrovském množství webů, což mu umožňuje shromažďovat data z různých zdrojů. I když uživatelé mohou v nastavení Googlu personalizaci reklam omezit, sledování se tím zcela nevyhne. Google navíc nevyužívá cookies jen k reklamám – pokud je na webu vloženo YouTube video, Google si automaticky nastaví cookie a sleduje chování uživatele i tam. Podobně fungují i Facebook, LinkedIn nebo další sociální sítě, které prostřednictvím tlačítek „To se mi líbí“ a „Sdílet“ získávají další data o uživateli. Uživatelé, kteří se chtějí bránit sledování, mohou využít několik možností. Prvním krokem je používání anonymního režimu v prohlížeči, který po zavření automaticky maže cookies. Další možností je blokování cookies třetích stran, což některé moderní prohlížeče, například Firefox, dělají automaticky. Dále lze instalovat rozšíření pro blokování reklam, jako je Adblock Plus nebo uBlock Origin, která zabráňují načítání sledovacích skriptů. Někteří uživatelé volí i alternativní vyhledávače, například DuckDuckGo, které neukládají žádná uživatelská data. (Evans, 2019)

Cookies jsou sice užitečné pro základní funkce webových stránek, ale zároveň se staly hlavním nástrojem pro masivní sledování uživatelů. Reklamní společnosti používají sofistikované metody k analýze chování uživatelů a přesně cílené reklamě. Přestože regulace, jako je GDPR, určité aspekty sledování omezují, stále zůstává mnoho prostoru pro zneužití. Pokud si chce uživatel uchovat své soukromí, měl by se naučit využívat nástroje pro blokování sledování a být obezřetný při poskytování souhlasu s ukládáním cookies. (Evans, 2019)

6.1.2 Typy cookies

Nezbytné cookies jsou klíčové pro základní funkčnost webových stránek, umožňují například navigaci nebo přístup k zabezpečeným sekcím webu. Bez těchto cookies by webové stránky nemohly správně fungovat. (NYP Holdings, 2025)

Funkční cookies umožňují webovým stránkám zapamatovat si volby a nastavení uživatele, jako je preferovaný jazyk nebo region, čímž poskytují vylepšené a personalizované funkce. (NYP Holdings, 2025)

Analytické cookies shromažďují informace o tom, jak návštěvníci používají webové stránky, například které stránky jsou nejčastěji navštěvovány nebo zda uživatelé dostávají chybové hlásky. Tyto cookies pomáhají provozovatelům webů porozumět interakci uživatelů s jejich stránkami a zlepšovat jejich funkčnost. (NYP Holdings, 2025)

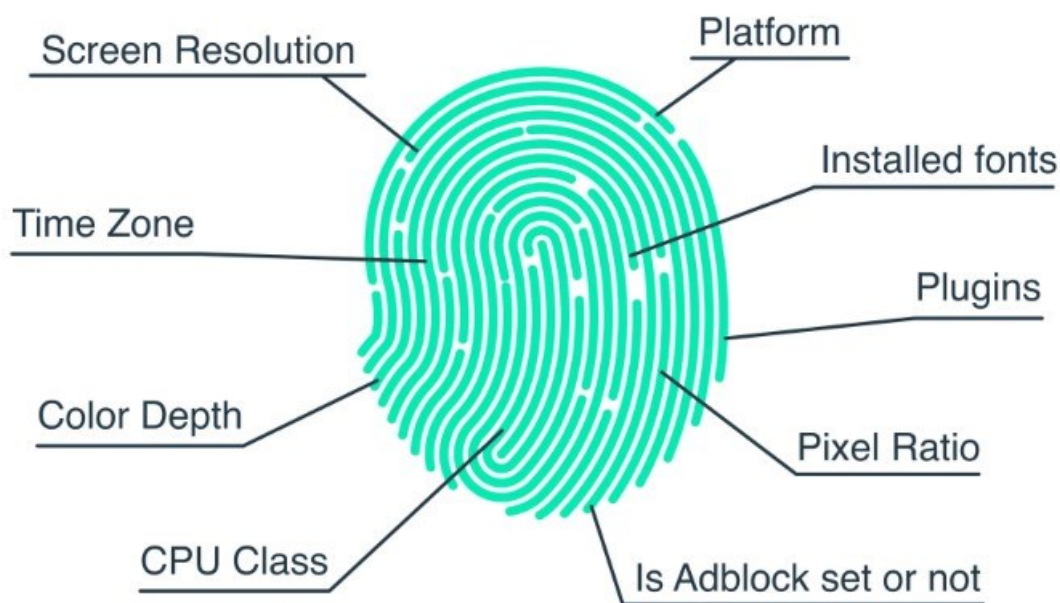
Reklamní cookies se používají k poskytování reklam, které jsou relevantní pro konkrétního uživatele. Mohou být také využity k omezení počtu zobrazení jedné reklamy a k měření efektivity reklamních kampaní. (NYP Holdings, 2025)

Cookies sociálních médií jsou nastaveny službami sociálních médií, které jsme přidali na web, aby uživatelé mohli sdílet obsah s přáteli a sítěmi. Tyto cookies jsou schopny sledovat prohlížeč uživatele napříč jinými weby a vytvářet profil jeho zájmů, což může ovlivnit obsah a zprávy zobrazované na jiných navštěvovaných webových stránkách. (NYP Holdings, 2025)

Je důležité poznamenat, že uživatelé mají možnost spravovat nebo mazat cookies prostřednictvím nastavení svého prohlížeče, což jim umožňuje mít kontrolu nad svým soukromím a daty. Respondenti v dotazníkovém šetření častokrát povolili všechny soubory cookies, nebo nezbytné soubory cookies, čímž se také mohou vystavovat odhalení svých digitálních stop. Kromě data prohlázeče ukládají data i do dalších uložišť, která jsou větší a nejsou tak často mazána, jako např. „Local Storage, IndexedDB“. Takové technologie se dají zneužít ke sledování uživatelů i po smazání cookies, protože data v nich často přetrvávají. Jsou součástí tzv. persistentního sledování. (NYP Holdings, 2025)

6.1.3 Browser Fingerprinting

Browser Fingerprinting umožňuje webovým stránkám sbírat rozličné údaje o uživateli, prohlížeči a zařízení s cílem vytvořit unikátní profil, který lze využít k jeho identifikaci a sledování online aktivit. Tento proces zahrnuje sběr informací, jako je používaný prohlížeč a jeho verze, operační systém, nainstalované doplňky, nastavené časové pásmo, preferovaný jazyk, rozlišení obrazovky či seznam dostupných písem. Kombinací těchto parametrů mohou webové stránky sestavit specifický „otisk“ prohlížeče, jenž umožňuje sledování uživatele napříč různými stránkami, aniž by bylo zapotřebí využívat běžné metody sledování, jako jsou cookies. Tento způsob monitorování představuje zásadní problém z hlediska ochrany soukromí, jelikož se mu uživatelé jen obtížně brání a často si nejsou vědomi toho, že jejich aktivita na internetu je tímto způsobem sledována. (Chea, 2024)



Obrázek 1 Grafické zobrazení fingerprintu

6.1.4 Metadata

Metadata jsou strukturované informace, které popisují, vysvětlují, lokalizují nebo jinak usnadňují vyhledávání, využívání a správu jiných dat. V digitálním prostředí se vyskytují prakticky u každého souboru a dokumentu – například u fotografií zahrnují informace o datu a čase pořízení, použitém zařízení, nastavení fotoaparátu a často i geografické souřadnice. U e-mailů metadata obsahují údaje o odesílateli, příjemci, čase odeslání, předmětu zprávy, IP adrese a trasování přenosu přes jednotlivé servery. Účelem metadat je tedy nejen popsat

základní charakteristiky dat, ale především umožnit jejich snazší třídění, dohledávání, archivaci a správu. (BASTL, 2021)

Metadata mohou uživatele ohrozit především tím, že i bez přístupu k samotnému obsahu dokumentu, fotografie nebo zprávy umožňují zjistit řadu citlivých informací, které mohou vést k odhalení identity, pohybu nebo zvyklostí dané osoby. Například fotografie pořízená mobilním telefonem často obsahuje údaje o přesném čase a místě pořízení, typu zařízení i softwarové verzi. Pokud uživatel takový soubor zveřejní na internetu nebo jej pošle jiným osobám bez odstranění metadat, může tím neúmyslně prozradit svou polohu, rutinu (např. opakující se pohyb), nebo dokonce domácí adresu. Stejně tak e-mailová metadata mohou odhalit reálné jméno odesílatele, jeho IP adresu, tedy přibližné místo připojení, a informace o použitém zařízení a softwaru, což útočníkovi umožňuje snadněji zacílit kyberútok. Dalším rizikem je možnost sledování tzv. komunikačních vzorců – i když není znám obsah zpráv, metadata prozradí, kdo, kdy, komu a jak často píše. Z těchto dat lze odvodit strukturu vztahů, pracovní nebo osobní vazby, nebo identifikovat klíčové osoby v síti. Toho mohou využít nejen komerční subjekty, ale také útočníci, státní orgány nebo špehovací software. V případě zneužití nebo úniku těchto informací může dojít k ohrožení soukromí, vydírání, sledování nebo manipulaci. Metadata jsou tak často přehlíženým, ale velmi silným nástrojem, který může zásadně narušit anonymitu i bezpečí běžného uživatele internetu. (BASTL, 2021)

6.2 Úniky informací

Jedním z nejzávažnějších bezpečnostních rizik souvisejících s anonymitou na internetu je únik citlivých informací. Únikem dat rozumíme jakoukoliv neautorizovanou ztrátu nebo zveřejnění údajů, které měly být chráněné před neoprávněným přístupem. Takový únik může nastat mnoha způsoby, přičemž mezi nejčastější patří kybernetické útoky, neopatrné chování uživatelů, nedostatečné zabezpečení systémů nebo selhání lidského faktoru uvnitř organizace. (Kosinski, 2024)

K úniku dat často dochází prostřednictvím kybernetických útoků, kdy se hackeři nebo jiní kyberzločinci snaží získat přístup do databází či jiných úložišť informací. Mezi nejznámější techniky patří phishing, malware, ransomware nebo využívání bezpečnostních zranitelností aplikací a systémů. Phishing, kdy útočník pomocí falešných e-mailů nebo webových stránek získává přístupové údaje uživatelů, představuje velmi častou metodu zneužití anonymity útočníka, který může nepozorovaně shromažďovat citlivá data. (Kosinski, 2024)

Informace však mohou uniknout i z důvodu nedbalosti samotných uživatelů. Často se stává, že lidé podceňují důležitost bezpečnosti, používají slabá hesla, která se dají snadno prolomit, sdílejí citlivé informace prostřednictvím nezabezpečených komunikačních kanálů nebo neúmyslně publikují osobní údaje veřejně na sociálních sítích. Dalším rizikovým faktorem jsou nedostatečně zabezpečené cloudové služby či mobilní aplikace, které mohou uchovávat data bez patřičné ochrany nebo je poskytovat třetím stranám bez vědomí uživatelů. (Kosinski, 2024)

Únik informací může mít vážné důsledky pro osoby, jichž se týká, včetně finančních ztrát, zneužití identity, vydírání nebo poškození osobní a profesní reputace. Data uniklá na internet mohou být zneužita jak individuálními kybernetickými zločinci, tak i různými organizovanými skupinami, které mohou informace využívat pro podvody, krádeže identity nebo další formy kriminality. Citlivé údaje mohou být navíc prodávány na černém trhu, kde se jejich hodnota odvíjí od jejich typu a množství. (Kosinski, 2024)

Aby bylo možné minimalizovat riziko úniku dat, je nutné věnovat zvýšenou pozornost kybernetické bezpečnosti, používat silná a unikátní hesla, pravidelně aktualizovat software a aplikace, dodržovat zásady bezpečného sdílení informací a vzdělávat uživatele o potenciálních rizicích a prevenci proti nim. (Kosinski, 2024)

6.2.1 Největší úniky dat

Historicky největší únik dat byl odhalen v lednu 2024 a je označován jako „Mother of All Breaches“ (MOAB). Tento incident zahrnoval více než 26 miliard záznamů, což z něj činí dosud nejrozsáhlejší známý únik informací. (Petkauskas, 2024)

Data byla objevena bezpečnostními výzkumníky na nezabezpečeném serveru. Jednalo se o kompilaci informací z předchozích úniků z různých platforem, jako jsou LinkedIn, Twitter, Weibo a Tencent. Přestože velká část těchto dat pocházela z dřívějších incidentů, MOAB pravděpodobně obsahoval i nově uniklé informace. (Petkauskas, 2024)

Mezi kompromitovanými údaji byly e-mailové adresy, uživatelská jména, hesla a v některých případech i další osobní informace. Rozsah a povaha těchto dat zvyšují riziko jejich zneužití pro účely phishingu, krádeže identity a dalších forem kybernetické kriminality. (Petkauskas, 2024)

Takto rozsáhlý únik dat má významné dopady na soukromí a bezpečnost uživatelů po celém světě. Umožňuje útočníkům provádět cílené phishingové útoky, získávat neoprávněný přístup k dalším účtům a páchat podvody. Organizace a jednotlivci byli vyzváni k okamžité změně hesel a posílení bezpečnostních opatření, jako je dvoufaktorová autentizace, aby minimalizovali riziko zneužití. (Petkauskas, 2024)

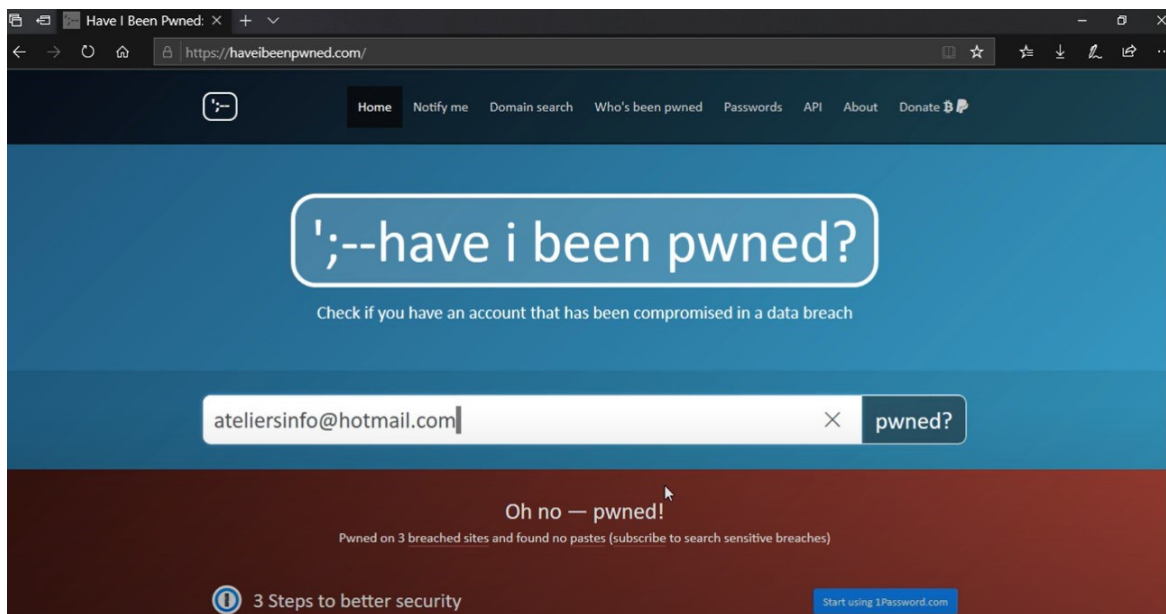
Tyto události zdůrazňují důležitost řádných bezpečnostních opatření a potřebu neustálé ostráživosti při ochraně osobních údajů v digitálním prostředí. (Petkauskas, 2024)

6.2.2 Have I been pwned

Skvělý způsob pro zjištění, zda byl některý z účtů uživatele zkompromitován během některého z datových úniků, je nástroj „have i been pwned“. Tento je dostupný online a aktuálně obsahuje údaje o únicích celkem z 879 napadených stránek, což představuje přibližně 15 miliard poškozených účtů. (Grauer, 2022)

Tento způsob je skvělou volbou pro jeho jednoduchost. Stačí si v internetovém prohlížeči vyhledat stránku „haveibeenpwned.com“, poté zadat do vyhledávacího pole hned na úvodní stránce svůj e-mail, který uživatel používá na různých internetových stránkách nebo aplikacích. Dalším krokem je kliknutí na tlačítko „pwned“. Služba následně prohledá databázi, ve které jsou shromažďovány uniklé údaje ze známých kybernetických incidentů. Pokud se zadaný e-mail nachází v databázi uniklých údajů, služba okamžitě zobrazí seznam bezpečnostních incidentů, ve kterých byly údaje kompromitovány. U každého úniku jsou viditelné podrobnosti, například datum úniku, jaké údaje byly zveřejněny (hesla, e-maily, telefonní čísla) a které služby byly ovlivněny. (Grauer, 2022)

Pokud služba nalezne údaje ze zadaného e-mailu v databázi uniklých informací, měli by uživatel neprodleně změnit své heslo na příslušných webových stránkách či službách. Doporučuje se také aktivace dvoufázového ověření tam, kde je to možné, aby se zvýšila bezpečnost vašeho účtu. (Grauer, 2022)



Obrázek 2 Výsledek nástroje „Have I been pwned“

7 DOTAZNÍKOVÉ ŠETŘENÍ

Cílem praktické části této bakalářské práce bylo provést kvantitativní výzkum zaměřený na vnímání anonymity na internetu a způsoby, jakými ji uživatelé chrání. Výzkum byl realizován formou anonymního dotazníku vytvořeného přes platformu Google Forms. Dotazník byl sdílen prostřednictvím stories na sociálních sítích Instagram a Facebook, kde byl zveřejněn odkaz vedoucí přímo na dotazník. Tento způsob distribuce oslovil zejména mladší generaci aktivních uživatelů internetu.

Dotazník obsahoval celkem 16 otázek, z nichž některé byly uzavřené, jiné umožňovaly více odpovědí nebo vyžadovaly vlastní vyjádření. Otázky byly rozděleny tak, aby odpovídaly třem výzkumným otázkám, které tvoří základ analýzy:

1. Jaké metody a nástroje využívají uživatelé internetu pro zajištění anonymity?
2. V jaké míře uživatelé internetu využívají tyto metody a nástroje pro zajištění anonymity?
3. Jaké digitální stopy zanechávají uživatelé v internetovém prostředí?

7.1 Výzkumná otázka č. 1

„Jaké metody a nástroje využívají uživatelé internetu pro zajištění anonymity?“

K zodpovězení této otázky byly využity především následující otázky z dotazníku:

- Otázka č. 9: Jaký je váš důvod pro anonymizaci na internetu?
- Otázka č. 10: Jak se chráníte před sledováním reklamních společností?
- Otázka č. 11: Které z následujících prostředků využíváte k zachování anonymity na internetu?

Z odpovědí vyplynulo, že nejčastěji využívaným nástrojem pro anonymizaci je anonymní režim v prohlížeči a blokování cookies a reklamních skriptů pomocí nástrojů jako je Adblock. Mnoho respondentů také uvedlo používání VPN služeb, které umožňují skrýt IP adresu a tím částečně maskovat svou digitální identitu. Naopak méně rozšířené je využívání prohlížeče Tor, který slouží k vyšší úrovni anonymizace, což může být způsobeno jeho složitějším používáním nebo nižším povědomím o jeho existenci.

Z hlediska motivace k anonymizaci nejčastěji zaznívaly důvody jako ochrana osobních údajů, omezení cílené reklamy a vyhnutí se sledování třetími stranami.

7.2 Výzkumná otázka č. 2

„V jaké míře uživatelé internetu využívají tyto metody a nástroje pro zajištění anonymity?“

S touto výzkumnou otázkou souvisí zejména tyto dotazníkové otázky:

- Otázka č. 3: Jak moc se zabýváte svou anonymitou na internetu?
- Otázka č. 5: Seznámili jste se s možnostmi nastavení soukromí v rámci sociálních sítí a nastavili jste si je?
- Otázka č. 8: Jak často si dobrovolně aktualizujete svá hesla k online účtům?

Z výsledků lze vyvodit, že většina respondentů se otázkou anonymizace příležitostně zabývá, ale aktivní a systematické chování, které by vedlo ke skutečnému snížení digitální stopy, je méně běžné. Například nastavení soukromí na sociálních sítích si upravila přibližně polovina respondentů, což značí určitou míru uvědomění, ale i rezervy v informovanosti nebo motivaci.

Pouze menší část dotazovaných si pravidelně mění hesla, což je jeden z klíčových preventivních nástrojů ochrany soukromí. Významná část respondentů uvedla, že se o anonymitu aktivně zajímá pouze tehdy, pokud narazí na problém nebo pokud mají podezření, že by mohli být sledováni.

7.3 Výzkumná otázka č. 3

„Jaké digitální stopy zanechávají uživatelé v internetovém prostředí?“

Odpovědi na tuto otázku se opírají zejména o:

- Otázka č. 1: Na škále od 1 do 10, jak moc se považujete za znalého v oblasti počítačové bezpečnosti?
- Otázka č. 2: Jaký je váš nejčastější způsob používání internetu?
- Otázka č. 4: Jaké informace na internetu považujete za nejcitlivější?
- Otázka č. 6: Co považujete za největší hrozbu pro anonymitu na internetu?

- Otázka č. 7: Omezili byste svou úroveň soukromí na internetu za cenu potenciálního snížení kybernetické kriminality?
- Otázka č. 12: Do jaké míry vnímáte kybernetickou bezpečnost jako aktuální problém na škále 1-10?
- Otázka č. 13: Která možná rizika vnímáte jako relevantní?
- Otázka č. 14: Čtete podmínky používání při registraci účtu, návštěvě webu?
- Otázka č. 15: Jak se zachováte, když navštívíte webovou stránku a objeví se vyskakovací okno, kde web žádá o povolení souborů cookies?

Výsledky ukazují, že i přesto, že značná část respondentů považuje svou úroveň znalostí počítačové bezpečnosti za průměrnou (hodnota mezi 4–6 na škále 1–10), často nejsou plně obeznámeni s tím, jaké digitální stopy po sobě zanechávají.

Za nejcitlivější informace považovali respondenti osobní údaje (např. jméno, adresa, číslo účtu), přihlašovací údaje a historii vyhledávání. Mezi nejčastěji vnímané hrozby pak patřilo sledování třetími stranami, ztráta soukromí a zneužití dat.

Na otázku ohledně čtení podmínek používání odpověděla většina respondentů negativně – většinou je nečtou nebo jen velmi zběžně, a u cookies většinou vybírají, které konkrétní cookies povolí, ale poměrně velká část uživatelů odklikne „Souhlasím“ bez hlubšího zkoumání. To naznačuje, že uživatelé sice chápou rizika zanechávání digitálních stop, ale aktivně jim čelí jen zřídka.

8 DOPORUČENÍ PRO MITIGACI BEZPEČNOSTNÍCH RIZIK

Mitigace bezpečnostních rizik v prostředí internetu je klíčovou oblastí, která si vyžaduje systematický přístup a komplexní opatření. Z odpovědí respondentů dotazníkového šetření anonymity na internetu je zřejmé, že spousta lidí má nedostatky v oblasti zabezpečení vlastní anonymity na internetu, nevyužívá anonymizační programy a jsou častokrát neznalí v oblasti počítačové bezpečnosti. Pro takové uživatele se objevuje mnohem více specifických hrozeb a rizik, než pro lidi, kteří si na svoje data a na jejich únik dávají velký pozor a dodržují určitá zabezpečení a pravidla pohybu na internetu. Mitigace takových rizik zahrnuje různé strategie a techniky zaměřené na minimalizaci pravděpodobnosti jejich vzniku, případně na snížení dopadů, pokud již dojde k incidentu. Mezi základní opatření patří edukace uživatelů, zavedení technických bezpečnostních kontrol, pravidelná aktualizace softwaru, silná autentizace uživatelů, využívání bezpečných komunikačních kanálů a implementace politiky řízení přístupu k informacím. Důležité je rovněž sledovat aktuální trendy v oblasti kybernetické bezpečnosti, vyhodnocovat rizika pomocí analýz a na jejich základě přijímat vhodná preventivní opatření. Celkovým cílem mitigace je vytvořit prostředí, které minimalizuje prostor pro zneužití anonymity k páčání kybernetické kriminality a chrání uživatele i organizace před potenciálními následky bezpečnostních incidentů. (Janko, 2023)

8.1.1 Internetová etika

Jedná se o soubor morálních zásad a pravidel chování, která upravují, jak by se jednotlivci i organizace měli chovat v online prostředí. Jedná se o relativně nový obor v rámci aplikované etiky, který se rozvíjí ruku v ruce s technologickým pokrokem a rozšiřujícím se využíváním internetu. Cílem internetové etiky je podporovat odpovědné, bezpečné a ohleduplné používání internetu s ohledem na práva, soukromí a důstojnost všech uživatelů. (Spinello, 2017)

Internetová etika zahrnuje široké spektrum témat. Mezi nejdůležitější oblasti patří ochrana osobních údajů, respektování autorských práv, pravdivost a ověřování informací, vyvarování se kyberšikany, nenávistných projevů nebo šíření dezinformací. Dále sem spadá také etické chování při online komunikaci, dodržování pravidel netikety (tj. etiky internetové komunikace), ochrana před zneužíváním anonymity a zodpovědný přístup k digitálním stopám, které uživatelé na internetu zanechávají. (Spinello, 2017)

S rozvojem digitálních technologií se stírá hranice mezi tím, co je veřejné a co soukromé, a právě internetová etika pomáhá definovat rámec chování, který je v souladu s demokratickými hodnotami, lidskými právy a respektováním ostatních účastníků digitálního prostoru. I když zákony mohou upravovat některé aspekty chování na internetu, etické zásady jdou často nad rámec právních předpisů a apelují na osobní odpovědnost a svědomí jednotlivce. (Spinello, 2017)

V kontextu anonymního online prostředí nabývá internetová etika na důležitosti, protože anonymita může vést k odosobnění, ztrátě zábrán a zvýšené míře nevhodného nebo škodlivého chování. Etické zásady tedy tvoří důležitý základ pro kultivované a udržitelné online soužití. (Spinello, 2017)

8.1.2 Zásady bezpečného vystupování v online prostředí

Vzhledem k výsledkům dotazníkového šetření, kde se projevilo, že většina respondentů nečte podmínky používání při registraci účtu (viz. otázka z dotazníkového šetření č. 14) a také si většina z nich pravidelně nemění hesla (viz. otázka z dotazníkového šetření č. 8), rostoucím hrozbám a stále sofistikovanějším formám podvodů je naprosté bezpečí na internetu v dnešní době obtížně dosažitelné. I krátká nepozornost může vést k vážným následkům. Proto je důležité dodržovat základní pravidla, která přispívají k ochraně osobních údajů a digitální identity. (Pavelková, 2023)

Před nákupy na internetu je nezbytné ověřit důvěryhodnost e-shopu, pročíst si obchodní podmínky a recenze ostatních zákazníků. Dále je třeba vyhýbat se podezřelým odkazům a stahování neznámých souborů, které mohou obsahovat škodlivý software. Osobní údaje, přihlašovací údaje a bezpečnostní otázky by měly zůstat důvěrné a sdílené pouze s ověřenými službami. (Pavelková, 2023)

Silná a unikátní hesla v kombinaci s dvoufázovým ověřením výrazně zvyšují ochranu uživatelských účtů. Při připojení k veřejným Wi-Fi sítím je vhodné používat VPN, která zabezpečí přenos dat a skryje digitální stopu. Nezbytné je také pravidelné aktualizování systému a aplikací, čímž se minimalizuje riziko zneužití zranitelností. Zálohování dat zajišťuje ochranu před jejich ztrátou v důsledku kybernetického útoku nebo technické závady. (Pavelková, 2023)

Dále se doporučuje používat blokátory reklam, které chrání před škodlivým obsahem, a antivirový software, který detekuje hrozby v reálném čase. Kritické myšlení a obezřetnost vůči nevyžádaným zprávám, podvodným výzvám a neověřeným nabídkám jsou základem prevence. Bezpečné online chování tak spočívá v kombinaci technických opatření a osobní odpovědnosti uživatele. (Pavelková, 2023)

8.1.3 Am I Unique

Webová stránka „amiunique.org“ analyzuje otisk prohlížeče s cílem zjistit, jak jedinečný je váš prohlížeč na internetu. Tato analýza napomáhá k pochopení, do jaké míry lze váš počítač identifikovat a sledovat na základě jeho konfigurace a nastavení. (Laperdrix, a další, 2016) Když uživatel vstoupí na tuto stránku, automaticky se z jeho prohlížeče získají různé atributy, jako je typ a verze prohlížeče, operační systém, rozlišení obrazovky, nainstalované pluginy, fonty, jazyková nastavení, časové pásmo, vlastnosti renderování grafiky přes WebGL nebo canvas, a další technické detaily, které se běžně odesílají při načtení webové stránky. (Laperdrix, a další, 2016)

Z těchto údajů se složí komplexní kombinace, která je pro většinu zařízení jedinečná. Tento otisk je pak porovnán s databází již nasbíraných otisků od ostatních uživatelů. Výstupem je informace o tom, jak moc je váš otisk jedinečný - tedy zda ho sdílí více uživatelů, nebo jste podle něj snadno identifikovatelní. Pokud je otisk unikátní nebo velmi vzácný, znamená to, že je možné vás na základě těchto technických údajů poměrně snadno sledovat napříč různými webovými stránkami, i bez použití cookies. (Laperdrix, a další, 2016)

Z výstupu tedy vyplývá, že i bez klasických sledovacích technik může být uživatel sledován prostřednictvím otisku svého prohlížeče, což má významné důsledky pro online soukromí. Jedinečný fingerprint lze využít ke sledování aktivity na internetu, a to často bez vědomí uživatele. Z tohoto důvodu stránka „Am I Unique“ nejen demonstruje tuto technologii, ale i upozorňuje na rizika, která s sebou přináší. (Laperdrix, a další, 2016)

Pro minimalizaci sledování prostřednictvím otisku lze využít například prohlížeče jako je Tor nebo Brave, které se snaží fingerprinting omezit, nebo si nainstalovat rozšíření jako Privacy Badger či CanvasBlocker. Žádné opatření sice nezaručí úplnou anonymitu, ale kombinace více metod může výrazně snížit pravděpodobnost sledování. (Laperdrix, a další, 2016)

8.1.4 Cover Your Tracks

Cover Your Tracks je nástupce online aplikace „Panopticlick“ a analyzuje několik faktorů tvého prohlížeče, aby zjistil, jak moc je tvůj prohlížeč jedinečný a tedy sledovatelný, například:

- typ a verzi prohlížeče
- používané doplňky a jejich nastavení (např. pluginy a rozšíření)
- nastavení cookies
- časové pásmo
- rozlišení obrazovky a barevnou hloubku
- fonty nainstalované v prohlížeči
- podporu JavaScriptu, HTML5 canvas fingerprintingu apod. (Toner, a další, 2017)

Kombinace těchto údajů je často unikátní, což umožňuje třetím stranám identifikovat tvůj prohlížeč i bez použití klasických metod sledování, jako jsou cookies. (Toner, a další, 2017) Postupem pro použití této funkce tvoří několik kroků. Nejprve je nutné si otevřít webovou stránku „coveryourtracks.eff.org“, zde kliknout na tlačítko „Test Your Browser“, po vyčkání několika vteřin se zobrazí výstup analýzy prohlížeče a jeho nastavení. (Toner, a další, 2017)

Výstupem je míra jedinečnosti prohlížeče (např. „Tvůj prohlížeč je unikátní mezi 150 000 dalšími prohlížeči.“). Dále informace o tom, zda jsou blokovány reklamy, cookies, fingerprinting apod., ale také podrobné výsledky jednotlivých testů (použité technologie, které tvoří váš fingerprint, např. použitá písma, rozlišení obrazovky, atd.). (Toner, a další, 2017)

Dle otázky č. 1. z dotazníkového šetření téměř nikdo se nepovažuje za velmi znalého v oblasti počítačové bezpečnosti. Ke zjištění míry anonymity na internetu, která je v již zmiňované oblasti počítačové bezpečnosti jedna z nejdůležitějších faktorů pro ochranu před hrozbami, slouží funkce „Cover Your Tracks“. Ten pomáhá identifikovat slabá místa v zabezpečení a anonymitě a zvyšuje povědomí o sledovacích technologiích. (Toner, a další, 2017)



Obrázek 3 Výsledek nástroje „Cover Your Tracks“

8.1.5 Privacy.net

Privacy.net je online nástroj, který analyzuje několik aspektů tvého prohlížeče a zařízení, aby zjistil, jak snadno může být tvůj prohlížeč sledován a identifikován pomocně metod fingerprintingu. Analyzuje například typ a verzi prohlížeče a operačního systému, IP adresu a související údaje (geolokace, poskytovatel připojení), rozlišení obrazovky a specifikaci hardwaru (CPU, GPU), nainstalované fonty v zařízení (font fingerprinting), podporu JavaScriptu, WebRTC, Canvas a WebGL fingerprintingu, ale také přítomnost pluginů a rozšíření v prohlížeči (Hariss, a další, 2017)

Kombinace těchto údajů vytváří unikátní fingerprint, který umožňuje sledovat prohlížeč a uživatele bez nutnosti použití klasických metod, jako jsou cookies. (Hariss, a další, 2017)

Postup použití privacy.net se skládá z několika kroků. Uživatel otevře webovou stránku „privacy.net/analyzer“, kde se spustí test po stisknutí tlačítka s nápisem „START TEST“. Po několika vteřinách jsou zobrazeny výsledky analýzy zařízení a nastavení prohlížeče. (Hariss, a další, 2017)

Výstupem analýzy je informace o míře jedinečnosti fingerprintu (např. „Tvůj fingerprint je unikátní mezi 200 000 dalšími uživateli.“), údaje o potenciálních hrozbách pro anonymitu (například únik IP adresy přes WebRTC), a detailní přehled použitých technologií, které fingerprint tvoří (použitá písma, WebGL nastavení, rozlišení obrazovky apod.). (Hariss, a další, 2017)

Privacy.net slouží k ověření skutečné míry anonymity a ochrany soukromí, identifikaci slabých míst zabezpečení prohlížeče a zvyšuje povědomí uživatele o možnostech a metodách sledování na internetu. (Hariss, a další, 2017)

8.1.6 Windscribe

Windscribe je VPN (Virtual Private Network) služba, která umožňuje uživatelům zvýšit soukromí a bezpečnost při používání internetu. Funguje tak, že šifruje internetovou komunikaci a maskuje skutečnou IP adresu uživatele. Windscribe analyzuje a poskytuje zabezpečení připojení pomocí několika funkcí:

- šifrování internetového provozu (AES-256)
- změna IP adresy uživatele (maskování skutečné lokace)
- blokování reklam a trackerů pomocí integrovaného nástroje „R.O.B.E.R.T.“
- ochrana před únikem dat přes WebRTC
- funkce Kill Switch (automatické odpojení internetu při selhání VPN) (Williams, 2023)

Postup použití služby Windscribe je jednoduchý. Uživatel nejprve stáhne a nainstaluje aplikaci ze stránky „windscribe.com“, poté aplikaci spustí a vybere si server, ke kterému se připojí. Po připojení je internetový provoz zašifrovaný a IP adresa maskovaná. (Williams, 2023)

Výstupem používání Windscribe je anonymizace uživatele, skrytí skutečné IP adresy (např. „Vaše IP adresa nyní ukazuje umístění v Německu.“), zvýšená bezpečnost při prohlížení webových stránek a snížení rizika sledování reklamami a jinými online trackery. (Williams, 2023)

Windscribe slouží ke zvýšení anonymity, ochraně soukromí na internetu, zabezpečení připojení na veřejných sítích (např. Wi-Fi) a omezení možností sledování uživatele ze strany třetích stran. (Williams, 2023)

8.2 Bezpečná komunikace

Dle otázky z dotazníkového šetření č. 2 „Jaký je váš nejčastější způsob používání internetu?“ jsou nejčastěji volenou otevřenou odpovědí sociální sítě. Proto je nezbytné pro anonymní pohybování se po sociálních sítích volit takové aplikace sloužící ke komunikaci, které jsou bezpečné vůči uživatelům a jejich citlivým datům, např. osobní údaje, hesla nebo firemní informace, které jsou ohrožena sledováním či jejich únikem. Bezpečná komunikace je důležitá, protože chrání uživatele před zneužitím jejich informací třetími stranami, před kybernetickými útoky, phishingem a dalšími hrozbami, které by mohly vést ke ztrátě dat nebo identitě. (Hackett, 2020)

Existuje několik nástrojů a platforem, které poskytují různé úrovně zabezpečení komunikace. Mezi nejznámější patří například komunikační platforma Signal, která vyniká především díky silnému end-to-end šifrování, čímž zaručuje, že obsah zpráv mohou číst pouze jejich skuteční účastníci. (Hackett, 2020)

Dalšími často využívanými platformami jsou aplikace Teams a Zoom. Obě platformy nabízejí různé bezpečnostní funkce a opatření, nicméně každá má svá specifika a slabá místa, která budou podrobně rozebrána v samostatných pododstavcích. (Hackett, 2020)

Základem bezpečné komunikace je volba vhodné platformy s ověřenými bezpečnostními funkcemi, jako jsou end-to-end šifrování, ochrana dat proti únikům a pravidelné aktualizace zabezpečení. (Hackett, 2020)

8.2.1 Signal

Signal je populární multiplatformní aplikace určená pro zabezpečenou a šifrovanou komunikaci. Přestože patří mezi relativně bezpečné nástroje, vyžaduje, aby každý uživatel správně nastavil aplikaci a dodržoval základní bezpečnostní opatření. Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) proto uživatelům doporučuje řídit se následujícími zásadami.

Při stahování aplikace je potřeba používat pouze oficiální webové stránky Signalu nebo ověřené obchody, jako jsou Google Play pro zařízení Android či App Store pro zařízení od společnosti Apple. Dále je důležité zabránit zneužití vašeho účtu, který je vázán na telefonní

číslo. K tomu slouží aktivace funkce „Zámek registrace“ v nastavení účtu, kam zadáte bezpečný alfanumerický PIN o délce minimálně šesti číslic. (NÚKIB, 2022)

Pro minimalizaci rizika neoprávněného přístupu k samotné aplikaci Signal aktivujte funkci „Zámek displeje“, která je dostupná v nastavení aplikace. Doporučuje se rovněž citlivou komunikaci zabezpečit aktivací funkce „Mizející zprávy“, která zajistí automatické odstranění zpráv po určité době. Nastavení notifikací je vhodné upravit tak, aby na uzamčené obrazovce bylo vidět pouze jméno odesílatele bez obsahu samotné zprávy. (NÚKIB, 2022)

Zároveň pravidelně kontrolujte v sekci „Připojená zařízení“, zda je váš účet používán výhradně na zařízeních, která rozpoznáváte a kterým důvěřujete. Pokud by došlo ke kompromitaci jednoho zařízení, útočník by získal přístup ke všem zprávám synchronizovaným v rámci účtu. (NÚKIB, 2022)

Důležité je také ověřovat identitu kontaktů kontrolou bezpečnostního čísla a nepřijímat žádosti od neznámých kontaktů bez ověření jinou cestou. Pro maximální ochranu udržujte aplikaci Signal vždy aktualizovanou, ideálně za pomoci automatických aktualizací. Dále doporučujeme pravidelně restartovat mobilní zařízení alespoň jednou denně, což pomůže odstranit případný malware bez perzistence. (NÚKIB, 2022)

Navzdory pokročilé ochraně a šifrování je však nutné používat Signal obezřetně, protože ani tato aplikace není zcela neprolomitelná. Za určitých okolností nelze zcela vyloučit možnost, že útočník dokáže při vynaložení vyššího úsilí získat přístup k vašemu účtu či obsahu komunikace. (NÚKIB, 2022)

8.2.2 Microsoft Teams

Microsoft Teams je komunikační platforma vyvinutá společností Microsoft, která je zaměřena na spolupráci v rámci týmů a organizací. Tato aplikace umožňuje efektivní komunikaci prostřednictvím chatu, videohovorů, sdílení souborů a dalších nástrojů pro spolupráci. (Houssier, 2023)

Instalace a používání Microsoft Teams je velmi intuitivní. Nejprve je nutné navštívit webovou stránku „teams.microsoft.com“ a stáhnout aplikaci odpovídající operačnímu systému uživatele (Windows, macOS, Android nebo iOS). Po stažení aplikace uživatel

spustí instalační soubor a řídí se pokyny na obrazovce. Po úspěšné instalaci se do aplikace přihlásí pomocí svého účtu Microsoft nebo účtu své organizace. Ihned po přihlášení může začít využívat všechny dostupné funkce, jako jsou chat, připojení k týmům, organizace schůzek, videokonference a sdílení dokumentů. (Houssier, 2023)

Mezi hlavní výhody Microsoft Teams patří zejména jeho integrace s ostatními produkty Microsoft Office, jako jsou Word, Excel a PowerPoint, možnost pořádat videokonference s velkým počtem účastníků, centralizované prostředí pro snadnou komunikaci a sdílení souborů a pravidelné aktualizace zabezpečení ze strany společnosti Microsoft. Přesto má aplikace i některé nevýhody, například náročnější provoz na systémové zdroje, zejména při videohovorech, možné problémy s kompatibilitou s jinými platformami mimo ekosystém Microsoftu a skutečnost, že některé pokročilé funkce jsou dostupné pouze v placené verzi. (Houssier, 2023)

Z pohledu anonymity a bezpečnosti Microsoft Teams zabezpečuje komunikaci pomocí šifrování. Na rozdíl od aplikací s kompletním end-to-end šifrováním (např. aplikace Signal) je však obsah komunikace přístupný poskytovateli služby, tedy společnosti Microsoft. Teams využívá šifrovací protokoly TLS (Transport Layer Security) a SRTP (Secure Real-time Transport Protocol), které chrání přenos dat mezi uživateli a servery. (Houssier, 2023)

Z hlediska anonymity na internetu Teams neposkytuje úplnou anonymitu, protože uživatelé jsou nuceni se přihlásit pomocí ověřitelného účtu. Data uživatelů jsou uložena na serverech Microsoftu, což může znamenat určité riziko z pohledu ochrany soukromí. Platforma rovněž umožňuje administrátorům monitorovat aktivity uživatelů, jako jsou přístupy k chatům nebo účasti na schůzkách. Existuje možnost anonymního přístupu ke schůzkám, avšak i v tomto režimu dochází k zaznamenávání určitých informací, například IP adresy a metadata komunikace. (Houssier, 2023)

Pro dosažení maximální bezpečnosti a ochrany soukromí je doporučeno, aby uživatelé dbali zvýšené opatrnosti při sdílení citlivých informací, pravidelně aktualizovali svá hesla a důkladně kontrolovali oprávnění udělená aplikaci. (Houssier, 2023)

8.2.3 ZOOM

Zoom je oblíbená komunikační platforma, která je široce využívána pro pořádání online schůzek, webinářů a videokonferencí. Uživatelům nabízí možnosti videohovorů, hlasových hovorů, chatu a sdílení obrazovky. Zoom se stal populární zejména díky své jednoduchosti, stabilnímu připojení a široké škále dostupných funkcí. (Rabasová, 2020)

Instalace a používání aplikace Zoom je snadná a rychlá. Nejprve je třeba navštívit oficiální webové stránky „zoom.com“ a stáhnout si aplikaci pro požadovaný operační systém (Windows, macOS, Android nebo iOS). Po dokončení instalace se uživatel přihlásí pomocí e-mailové adresy, účtu Google, Facebooku nebo účtu organizace. Poté může okamžitě začít vytvářet nové schůzky, připojovat se ke stávajícím pomocí odkazu nebo ID schůzky a používat funkce, jako je sdílení obrazovky, chat nebo nahrávání hovorů. (Rabasová, 2020)

Zoom má několik výhod, které přispívají k jeho popularitě. Patří mezi ně uživatelsky přívětivé rozhraní, spolehlivé připojení i při slabším internetu, možnost připojení velkého počtu účastníků a široké možnosti přizpůsobení schůzek. Umožňuje také integraci s kalendáři a dalšími nástroji, což usnadňuje plánování a organizaci komunikace. Mezi nevýhody lze zařadit určité bezpečnostní problémy, které byly medializovány zejména v období pandemie, například tzv. „Zoom-bombing“ (neoprávněné vniknutí do schůzek), omezené možnosti bezplatné verze a závislost na připojení k internetu. (Rabasová, 2020)

Z hlediska bezpečnosti Zoom implementoval end-to-end šifrování, avšak pouze pro určité typy schůzek a pouze tehdy, pokud je tato funkce aktivována. Standardní šifrování využívá protokol TLS pro přenos dat a AES-256 pro šifrování samotného obsahu. Přesto je třeba poznamenat, že ne všechny typy dat jsou šifrovány end-to-end a že některá metadata zůstávají dostupná poskytovateli. (Rabasová, 2020)

Pokud jde o anonymitu, Zoom neposkytuje úplné anonymní používání. I když je možné připojit se ke schůzce bez vytvoření účtu, aplikace stále zaznamenává určité informace, jako je IP adresa, název zařízení a metadata o spojení. Navíc schůzky často vyžadují zadání jména, které se zobrazuje ostatním účastníkům. Zoom také umožňuje správcům organizací sledovat některé aktivity účastníků, včetně připojení, doby trvání schůzky a sdíleného obsahu. (Rabasová, 2020)

Pro zvýšení bezpečnosti a ochrany soukromí při používání Zoomu se doporučuje používat silná hesla pro schůzky, aktivovat funkci čekárny (waiting room), nastavit přístupová práva, pravidelně aktualizovat aplikaci a v případě potřeby využívat režim end-to-end šifrování. Uživatelé by si měli být vědomi, že i přes výše zmíněná opatření nelze při používání Zoomu dosáhnout úplné anonymity. (Rabasová, 2020)

ZÁVĚR

Závěrem této bakalářské práce lze konstatovat, že anonymita na internetu zůstává velmi aktuálním a důležitým tématem, zejména v kontextu rostoucí digitalizace každodenního života a nárůstu kybernetických hrozeb. Teoretická část práce objasnila základní pojmy spojené s internetem, anonymitou, šifrováním a legislativním rámcem. Práce představila čtenáři pohled na široké spektrum využití internetu, jeho historii, ale také možný náhled do budoucna. Z teoretické části je zjevné, jaký vliv má rozhodování jednotlivců při pohybu v internetovém prostředí. Praktická část, založená na dotazníkovém šetření, poskytla přehled o povědomí a postojích uživatelů k anonymitě online. Výsledky ukázaly, že většina respondentů si je vědoma rizik spojených se sdílením osobních údajů na internetu, avšak jen malá část aktivně využívá dostupné anonymizační nástroje a technologie.

Zásadním přínosem pro čtenáře bylo objasnění bezpečnostních rizik a jejich mitigace. V této části byly představeny nástroje jako AmIUnique, Cover Your Tracks, Privacy.net a další, které uživatelům umožňují otestovat úroveň sledovatelnosti jejich prohlížeče a celkovou míru odhalitelnosti na internetu. Tyto nástroje poskytují přehled o tom, jak unikátní je otisk jejich prohlížeče (browser fingerprint), a tím napomáhají uvědomění si rizik spojených s běžným používáním internetu bez odpovídající ochrany. Zároveň nabízejí doporučení, jakými způsoby lze tyto otisky minimalizovat a zvýšit tak úroveň anonymity – například používáním VPN, blokováním skriptů třetích stran nebo nasazením prohlížečů zaměřených na soukromí.

Z pohledu komunikačních nástrojů byly v práci analyzovány aplikace Microsoft Teams a Zoom, přičemž hlavním kritériem srovnání byla míra zachování anonymity. Z analýzy vyplývá, že pro běžné uživatele, kteří kladou důraz na anonymitu při komunikaci na internetu, je aplikace Zoom výhodnější volbou než Microsoft Teams. Její flexibilnější možnosti připojení bez registrace, částečná podpora end-to-end šifrování a menší důraz na identifikaci uživatele poskytují vyšší úroveň soukromí. Microsoft Teams naopak klade důraz na integraci v rámci organizací a korporací, což s sebou nese potřebu přihlašování a sledování uživatelské aktivity, a tím i nižší míru anonymity. Přesto však ani Zoom nezaručuje úplnou anonymitu, a uživatelé by měli být i při jeho používání obezřetní a chránit své osobní údaje vhodnými nástroji a návyky.

Celkově lze říci, že dosažení úplné anonymity na internetu je velmi obtížné. Uživatelé by proto měli dbát na informovanost o moderních nástrojích, dodržovat zásady digitální hygieny a být si vědomi toho, že každý krok v online prostředí zanechává digitální stopu. Vědomé a odpovědné chování na internetu, podpořené technickými prostředky, je v současnosti tím nejúčinnějším způsobem, jak minimalizovat rizika spojená se ztrátou anonymity

SEZNAM POUŽITÉ LITERATURY

- Americano, Tall. 2024.** Cypherpunk Culture: Unravelling the Origins (1/2). *cypherpunktimes.com*. [Online] 2024. https://www.cypherpunktimes.com/cypherpunk-culture-unraveling-the-origins/?utm_source=chatgpt.com.
- Baker, Kurt. 2025.** Crowdstrike. *The Dark Web Explained*. [Online] 11. February 2025. <https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/dark-web/>.
- BASTL, Martin. 2021.** *Kybernetická bezpečnost: průvodce digitálním světem*. Brno : CPress, 2021. ISBN 978-80-264-3663-3.
- Bednář, Vojtěch. 2007.** Co je to Internet? *Lupa.cz*. [Online] 2007. <https://www.lupa.cz/clanky/co-je-to-internet/>.
- Běhounková, Tereza. 2024.** Jak je to tedy s tím prostým elektronickým podpisem? *Roklen24*. [Online] 2024. https://roklen24.cz/jak-je-to-tedy-s-tim-prostym-elektronickym-podpisem/?utm_source=chatgpt.com.
- 2023.** Bezpečnost a anonymita na internetu. *utb.cz*. [Online] 2023. <https://www.utb.cz/cvt/bezpecnost-anonymita-na-internetu/>.
- Bitto, Ondřej. 2005.** *Šifrování a biometrika*. 2005. ISBN 978-80-86686-48-6.
- Blažková, Martina. 2005.** *Jak využít internet v marketingu: krok za krokem k vyšší konkurenceschopnosti*. Praha : Grada, 2005. ISBN 80-247-1095- 1.
- Blinka, Lukáš. 2015.** *Online závislosti: jednání jako droga: online hry, sex a sociální sítě: diagnostika závislosti na internetu: prevence a léčba*. Praha : Grada, 2015. ISBN 978-80-210-7975-5.
- Borth, David E. 2025.** mobile telephone. *britannica.com*. [Online] 26. January 2025. <https://www.britannica.com/technology/mobile-telephone>.
- Bryce, Leo. 2024.** Co je MAC adresa? Plný formulář, jak ho najít Windows. *guru99.com*. [Online] 27. Červen 2024. <https://www.guru99.com/cs/what-is-mac-address.html>.
- Cimino, Al. 2018.** *Příběh Kryptologie - Od starověkých kódů po kvantovou kryptografii*. místo neznámé : Edice Knihy Omega, 2018. ISBN 978-80-7390-887-4.
- 2025.** Cover Your Tracks. *Cover Your Tracks.eff.org*. [Online] 2025. https://coveryourtracks.eff.org/results?&aat=1&t=1111&a=1111&dnt=1111&fp_i_whorls=%7B%22v%22%3A%7B%22plugins%22%3A%22Plugin+0%3A+Chrome+PDF+Viewer%3B+Portable+Document+Format%3B+internal-pdf-viewer%3B+%28Portable+Document+Format%3B+application%2Fpdf%3B+pd.
- ČESKO. 2019.** Zákon č. 110/2019 Sb., o zpracování osobních údajů. *Zákony pro lidi*. [Online] AION CS, © 2010-2024, 2019. <https://www.zakonyprolidi.cz/cs/2019-110>.
- . 2014.** Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. *Zákony pro lidi*. [Online] AION CS, © 2010-2024, 2014. <https://www.zakonyprolidi.cz/cs/2014-181>.
- Dodge, Ronald C. 2020.** *Introduction to Cybersecurity*. Boca Raton : CRC Press, 2020. ISBN 978-1-138-07337-3.
- Evans, Lester. 2019.** *Cybersecurity: What You Need to Know About Computer and Cyber Security, Social Engineering, The Internet of Things + An Essential Guide to Ethical Hacking for Beginners*. 2019. ISBN 9781794647237.
- Grauer, Yael. 2022.** How to Use 'Have I Been Pwned' to See If Your Data Was Compromised. *consumerreports.org*. [Online] 24. October 2022. <https://www.consumerreports.org/electronics/data-theft/how-to-use-have-i-been-pwned-data-breach-a6598286668/>.
- Hackett, Robert. 2020.** Which video chat app is best for security? *fortune.com*. [Online] 29. April 2020. <https://fortune.com/2020/04/29/video-chat-meetings-app-safe-to-use-security-whatsapp-signal-wickr-zoom-microsoft-teams-nsa/>.

- Hariss, Khalil, Noura, Hassan a Samhat, Abed Ellatif. 2017.** Journal of Information Security and Applications. *ScienceDirect*. [Online] June 2017. <https://www.sciencedirect.com/science/article/abs/pii/S2214212616303052?via%3Dihub>.
- Haugabrook, Lynelle. 2025.** Peraton. *Five Things To Know About The Dark Web*. [Online] 2025. <https://www.peraton.com/news/five-things-to-know-about-the-dark-web/>.
- Houba, Zdeněk. 2025.** Jak nás postkvantová kryptografie chrání před hrozbami kvantových počítačů? *cdr.cz*. [Online] 3. January 2025. <https://cdr.cz/clanek/jak-nas-postkvantova-kryptografie-chrani-pred-hrozbami-kvantovych-pocitacu#author1>.
- Houssier, Emily. 2023.** Microsoft Teams Security: Is Your Data Secure? *Powell-software.com*. [Online] 28. February 2023. <https://powell-software.com/resources/blog/microsoft-teams-security/>.
- Hušková, Lucie. 2025.** V Česku vyrostl počet denních uživatelů Facebooku na 3,8 milionů. *newsfeed.cz*. [Online] 2025. <https://newsfeed.cz/v-cesku-vyrostl-pocet-dennich-uzivatelu-facebooku-na-38-milionu/>.
- Hvězda, Ondřej. 2024.** Tipy na bezpečný pohyb na internetu. *kybez.cz*. [Online] 5. June 2024. <https://kybez.cz/tipy-na-bezpecny-pohyb-na-internetu/>.
- Chea, Evelyn. 2024.** <https://fingerprint.com/blog/browser-fingerprinting-techniques/>. *fingerprint.com*. [Online] 2024. <https://fingerprint.com/blog/browser-fingerprinting-techniques/>.
- Chýlová, Helena. 2010.** Problémové velké písmeno - Internet nebo internet. <https://plzen.rozhlas.cz/problemove-velke-pismeno-internet-nebo-internet-6800090#:~:text=Podle%20%C5%A1koln%C3%ADho%20vyd%C3%A1n%C3%AD%20Pavidel%20%C4%8Desk%C3%A9ho,Celosv%C4%Btov%C3%A1%20informa%C4%8Dn%C3%AD%20a%20komunika%C4%8Dn%C3%AD%20s%C3%AD%C5%A5>. [Online] 2010.
- Ijs.8u.cz. Budoucnost Internetu.* [Online] http://ijs2.8u.cz/index.php?option=com_content&view=article&id=33&Itemid=135.
- 2013.** *is.mendelu.cz. Internet.* [Online] 2013. https://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=40844.
- 2014.** Jak na Internet. *cz.nic*. [Online] 2014. <https://www.jaknainternet.cz/page/1205/historie-internetu/>.
- Janko, David. 2023.** Lekce 19 - Bezpečnost kyberprostoru a anonymita na internetu. *www.itnetwork.cz*. [Online] 2023. <https://www.itnetwork.cz/bezpecnost/bezpecnost-kyberprostoru-a-anonymita-na-internetu>.
- Jirásek, Petr, Novák, Luděk a Požár, Josef. 2022.** Výkladový slovník kybernetické bezpečnosti. *nukib.gov.cz*. [Online] 2022. https://nukib.gov.cz/download/publikace/podpurne_materialy/Vkladov%20slovnk_5.ver.pdf.
- Karacher, Matt. 2017.** #StatusOfMindSocial media and young people's mental health and wellbeing. Royal Society for Public Health. *rsph.org.uk*. [Online] 2017. <https://www.rsph.org.uk/static/uploaded/d125b27c-0b62-41c5-a2c0155a8887cd01.pdf>.
- Kazarez, Maria. 2024.** Browser Fingerprinting: How Does It Work? *Soax.com*. [Online] 7. October 2024. <https://soax.com/blog/browser-fingerprinting-what-is-it-and-how-does-it-work>.
- Kolouch, Jan. 2019.** Cybersecurity. [Online] 2019. ISBN 978-80-88168-32-4.
- Kosinski, Matthew. 2024.** What is data breach? *ibm.com*. [Online] 24. May 2024. https://www.ibm.com/think/topics/data-breach?utm_source=chatgpt.com.
- Laperdrix, Pierre, a další. 2016.** Beauty and the Beast: Diverting modern web browsers. *inria.hal.science*. [Online] 2016. <https://hal.inria.fr/hal-01285470/document>.

- Levy, Steven. 2010.** *Heroes of the Computer Revolution*. Sebastopol : O'Reilly Media, 2010. 978-1-4493-8509-2.
- Malá, Petra. 2023.** Historie a vývoj sociálních sítí: 8 „socek“, které dotvářejí naši realitu. *blog.aira.cz*. [Online] 2023. <https://blog.aira.cz/historie-vyvoj-socialnich-siti-8-socek-ktere-dotvareji-nasi-realitu>.
- McGowan, Emma. 2023.** Co je to vlastně digitální identita? *Avast.com*. [Online] 8. December 2023. <https://blog.avast.com/cs/co-je-to-vlastn%C4%9B-digit%C3%A1ln%C3%AD-identita>.
- Merissa. 2025.** Jak změnit adresu MAC. A Comprehensive Guide. *tech-lib.eu*. [Online] 2025. <https://tech-lib.eu/tech/jak-zmenit-adresu-mac-a-comprehensive-guide/>.
- Mikláš, Michal. 2010.** E-mail (Elektronická pošta). *gjszlin.cz*. [Online] 2010. <https://www.gjszlin.cz/ivt/esf/ostatni-sin/e-mail.php>.
- Nanosystem. 2023.** Internet bez jména: Kdo se skrývá za anonymitou online? *nanosystem.cz*. [Online] 2023. <https://nanosystem.cz/internet-bez-jmena-kdo-se-skriva-za-anonymitou-online/>.
- NÚKIB. 2022.** Doporučení pro používání aplikace Signal. *nukib.gov.cz*. [Online] 28. February 2022. <https://nukib.gov.cz/cs/infoservis/doporuceni/1816-doporuceni-pro-pouzivani-aplikace-signal/>.
- . 2023. Minimální bezpečnostní standard. <https://nukib.gov.cz/>. [Online] 2023. https://nukib.gov.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf?utm_source=chatgpt.com.
- . 2024. Nový zákon o kybernetické bezpečnosti. *portal.nukib.gov.cz*. [Online] 21. November 2024. <https://portal.nukib.gov.cz/informace/legislativa/zakon-o-kyberneticke-bezpecnosti>.
- NYP Holdings, Inc. 2025.** *nypost.com*. <https://nypost.com/cookie-notice/>. [Online] 8. 1 2025. <https://nypost.com/cookie-notice/>.
- Pavelková, Veronika. 2023.** Desatero bezpečného internetu. *blog.avast.com*. [Online] 5. March 2023. https://blog.avast.com/cs/desatero-bezpecneho-internetu?utm_source=chatgpt.com.
- Pavlíček, Antonín. 2010.** *Nová média a sociální sítě*. Praha : Oeconomica, 2010. ISBN 978-80-245-1742-1.
- Petkauskas, Vilius. 2024.** Mother of all breaches reveals 26 billion records: what we know so far. *cybernews.com*. [Online] 29. January 2024. https://cybernews.com/security/billions-passwords-credentials-leaked-mother-of-all-breaches/?utm_source=chatgpt.com.
- Poggi, Nicolas. 2021.** Encryption choices: rsa vs. aes explained. *Preyproject.com*. [Online] 2021. <https://preyproject.com/blog/types-of-encryption-symmetric-or-asymmetric-rsa-or-aes#:~:text=Asymmetric%20and%20symmetric%20encryption%20are,a%20private%20key%20for%20decryption..>
- Proton, Team. 2024.** Tor over VPN explained. *Protonvpn.com*. [Online] 3. Červenec 2024. http://protonvpn.com/blog/tor-vpn?srsId=AfmBOooY1zDpRBlsTERT6T2D9-M3UQ3dx_pQB3TvF5DrcutuyefdyhK.
- Rabasová, Michaela. 2020.** Videokonference přes Zoom jako bezpečnostní riziko. Na co si dát pozor? *master.cz*. [Online] 15. April 2020. <https://www.master.cz/blog/videokonference-pres-zoom-ochrana-soukromi/>.
- Sidor, Jon. 2024.** Using Onion over VPN - all you need to know. *Surfshark.com*. [Online] 4. Listopad 2024. <https://surfshark.com/blog/tor-over-vpn>.
- Singer, P. W. a Friedman, Allan. 2014.** *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford : Oxford University Press, 2014. 978-0-19-991809-6.
- Skleňák, Vilém. 2001.** *Data, informace, znalosti a Internet*. Praha : C.H.Beck, 2001. ISBN 80-717-9409-0.

Spinello, Richard A. 2017. *Cyberethics: Morality and Law in Cyberspace*. 2017. ISBN 978-1-284-10500-2.

Stark, Ivo. 2011. CO JE INTERNET? *imip.cz*. [Online] 29. Prosinec 2011. <https://www.imip.cz/internet-nebo-internet/>.

Svršek, Jiří. Historie sítě ARPANET/Internet. *Natura.baf.cz*. [Online] <http://natura.baf.cz/natura/2002/3/20020303.html>.

Špaček, Tomáš. 2021. *Kybernetická bezpečnost pro každého: jak se chránit v digitálním světě*. Praha : Grada, 2021. ISBN 978-80-271-2914-5.

Štráfelda, Jan. 2023. Hash. *strafelda.cz*. [Online] 2023. <https://www.strafelda.cz/hash>.

Takeo, Kanade. 2021. *Introduction to AI: Systems and Practices*. Tokyo : Springer, 2021. ISBN 978-4-431-55672-9.

Toner, Alan, Eckersley, Peter a Budington, Bill. 2017. Panoptick 3.0. *eff.org*. [Online] 28. November 2017. <https://www.eff.org/deeplinks/2017/11/panoptick-30>.

2019. Tor: Overview. *torproject*. [Online] 2019. <https://2019.www.torproject.org/about/overview.html.en>.

2025. Univerzita Tomáše Batí ve Zlíně, Kapitola 6 – Šifrování a elektronický podpis. *utb.cz*. [Online] 2025. <https://www.utb.cz/cvt/bezpecnost-sifrovani-elektronicky-podpis/>.

Vamosi, Robert a Mitnick, Kevin. 2019. *The art of invisibility: the world's most famous hacker teaches you how to be safe in the age of big brother and big data*. New York : Back Bay Books, Little, Brown and Company, 2019. ISBN 978-0-316-38052-2.

Williams, Mike. 2023. Windscribe VPN review. *techradar.com*. [Online] 2023. <https://www.techradar.com/reviews/windscribe>.

Windows, computers and Technology. 2019. Youtube.com - Have I been Pwned and What to do if you have been in a data breach. *Youtube.com*. [Online] 17. 1 2019. https://www.youtube.com/watch?v=4Ais1-ELL8g&ab_channel=Windows%2CcomputersandTechnology.

SEZNAM OBRÁZKŮ

Obrázek 1 Grafické zobrazení fingerprintu	50
Obrázek 2 Výsledek nástroje „Have I been pwned“	54
Obrázek 3 Výsledek nástroje „Cover Your Tracks“	62
Obrázek 4 Graf znalosti v oblasti počítačové bezpečnosti, dotazníkové šetření, 2025	79
Obrázek 5 Graf nejčastějšího způsobu používání internetu, dotazníkové šetření, 2025	80
Obrázek 6 Graf zabývání se anonymitou na internetu, dotazníkové šetření, 2025	81
Obrázek 7 Graf nejcitlivějších informací na internetu, dotazníkové šetření, 2025	82
Obrázek 8 Graf nastavení soukromí v rámci sociálních sítí, dotazníkové šetření, 2025	83
Obrázek 9 Graf největší hrozby pro anonymitu na internetu, dotazníkové šetření, 2025 ...	84
Obrázek 10 Graf snížení soukromí v internetovém prostředí za cenu snížení kybernetické kriminality, dotazníkové šetření, 2025	85
Obrázek 11 Graf aktualizace hesel k online účtům, dotazníkové šetření, 2025	86
Obrázek 12 Graf důvodů pro anonymizaci na internetu, dotazníkové šetření, 2025.....	87
Obrázek 13 Graf ochrany před sledováním reklamních společností, dotazníkové šetření, 2025	88
Obrázek 14 Graf prostředků využívaných k zachování anonymity na internetu, dotazníkové šetření, 2025	89
Obrázek 15 Graf kybernetické bezpečnosti jako aktuálního problému, dotazníkové šetření, 2025	90
Obrázek 16 Graf relevantních rizik, dotazníkové šetření, 2025	91
Obrázek 17 Graf čtení podmínek používání při registraci účtu, návštěvě webu, dotazníkové šetření, 2025	92
Obrázek 18 Graf povolení cookies souborů na webu, dotazníkové šetření, 2025	93
Obrázek 19 Graf osvěty stran digitální gramotnosti, dotazníkové šetření, 2025	94

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AES	Advanced Encryption Standard
AI	Artificial Intelligence
ARPA	Advanced Research Project Agency
CIA	Central Intelligence Agency
CNN	Cable News Network
CPU	Central Processing Unit
CTSS	Compatible Time-Sharing System
DES	Data Encryption Standard
DNS	Domain Name System
ECC	Elliptic-curve cryptography
FESNET	Federal Education and Scientific NETwork
GDPR	General Data Protection Regulation
GPU	Graphics Processing Unit
GL	Graphics Library
HTML	Hyper Text Markup Language
ICT	Information and Communication Technology
IEEE	Institute of Electrical and Electronics Engineers
IM	Instant Messaging
IoT	Internet of Things
IP	Internet Protocol
iOS	iPhone Operating System
MAC	Media Access Control
MD	Message Digest Algorithm
MILNET	Military Network
NET	Network

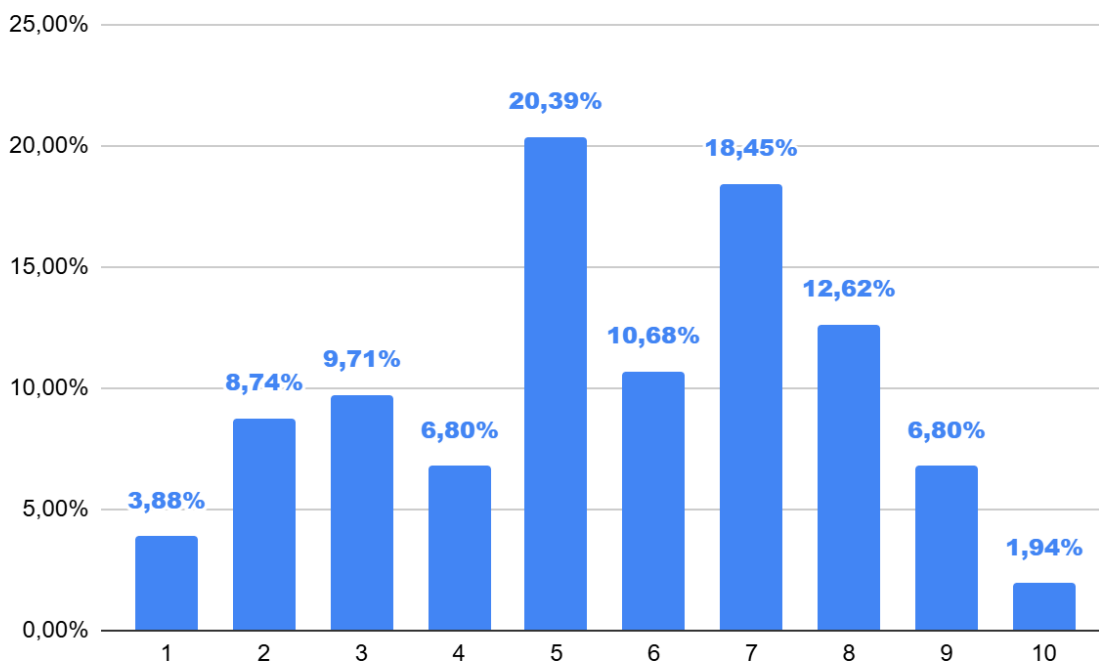
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TOR	The Onion Router
VPN	Virtual Private Network
WebRTC	Web Real-Time Communication
Wi-Fi	Wireless Fidelity
WWW	World Wide Web

SEZNAM PŘÍLOH

Příloha P I: Analýza dotazníkového šetření

PŘÍLOHA P I: ANALÝZA DOTAZNÍKOVÉHO ŠETŘENÍ

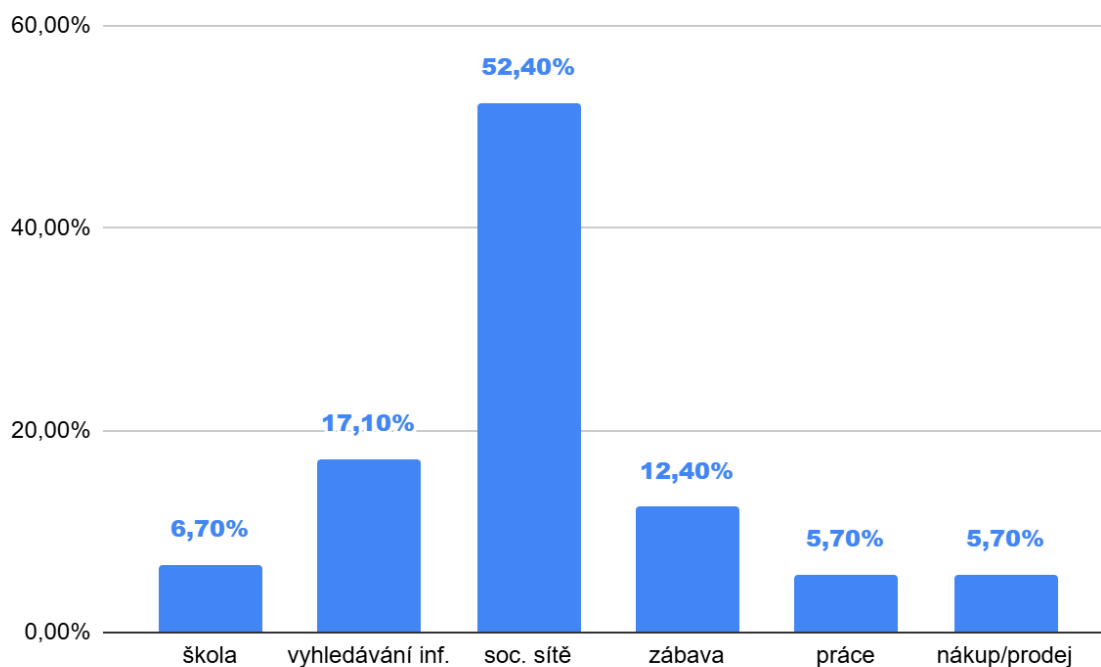
Vyhodnocení 1. otázky: Ta se zabývá znalostí respondentů v oblasti počítačové bezpečnosti na škále 1-10. Nejvíce volená možnost na stupnici byla „5“ v počtu 21 výběrů, druhou nejvíce volenou odpověď byla „7“ v počtu 19 výběrů. Z odpovědí tohoto grafu lze konstatovat, že většina uživatelů má průměrné znalosti v rámci počítačové bezpečnosti.



Obrázek 4 Graf znalosti v oblasti počítačové bezpečnosti, dotazníkové šetření, 2025

Vyhodnocení 2. otázky: Jedná se o otevřenou otázku zaměřenou na nejčastější způsob používání internetu respondentů. U této otázky byla volná odpověď, takže častokrát respondenti napsali více možností za sebe. Ze všech odpovědí bylo vyfiltrováno celkem 6 kategorií nejčastějších odpovědí, které jsou zobrazeny v grafu (Obrázek 2), zbylé odpovědi se vyskytovaly v zanedbatelném množství (1-2 odpovědi), a proto je neúčinné brát je v potaz v rámci tvorby opatření na danou problematiku. Nejčastější reakce na uvedenou otázku byla „sociální síť“ v počtu 55 odpovědí. Druhou nejvíce volenou odpovědí byla „vyhledávání informací“ v počtu 18 reakcí. Třetí volbou s počtem 13 hlasů byla „zábava“, čtvrtou pak „škola“ s počtem 7 hlasů. Pátou a šestou odpovědí byla se shodným počtem hlasů kategorie „práce“ a „prodej“ s 6 hlasy.

Výsledek hodnocení naznačuje, že vnímání internetu je pro většinu uživatelů primárně spojeno se zábavou a neformálním obsahem.



Obrázek 5 Graf nejčastějšího způsobu používání internetu, dotazníkové šetření, 2025

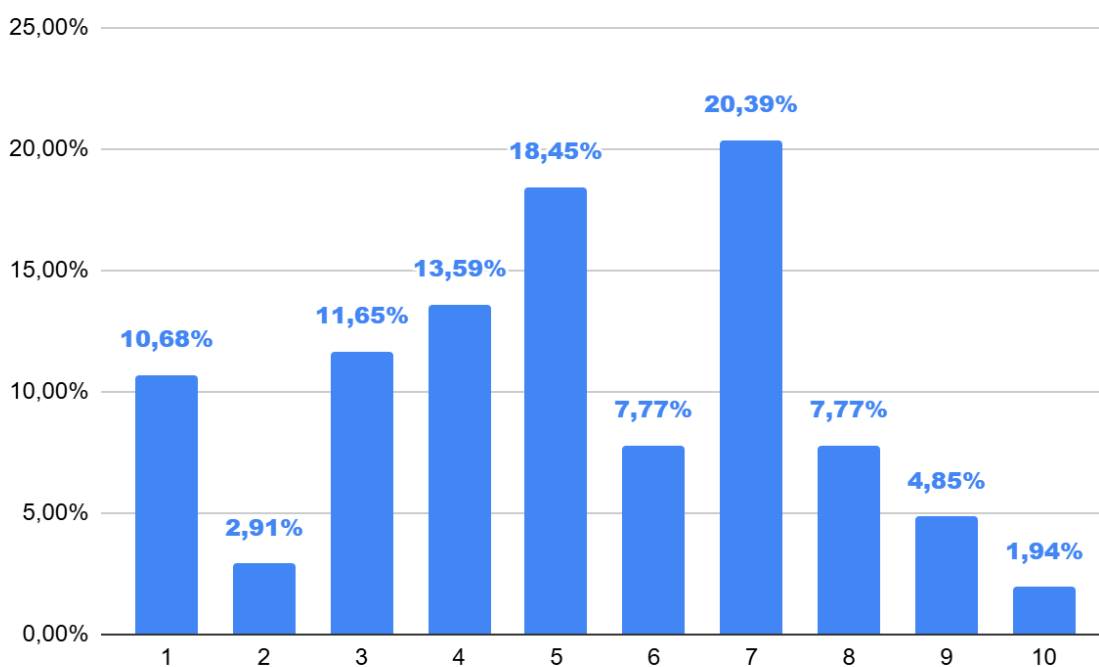
Vyhodnocení 3. otázky: Tato otázka je zaměřena na to, jak moc se zabývají respondenti svou anonymitou na internetu na škále 1-10, kdy 1 znamená „Neznalý“ a 10 „Velmi znalý“.

Respondenti volili následovně:

- 1 – 11x
- 2 – 3x
- 3 – 12x
- 4 – 14x
- 5 – 19x
- 6 – 8x
- 7 – 21x
- 8 – 8x
- 9 – 5x
- 10 – 2x

Na základě výsledku lze říci, že většina lidí odpovídající na tento dotazník se zabývá o svou anonymitu na internetu průměrně, a to v případě uvažování, že na škále jsou čísla 4-7 průměrné hodnoty. Tyto hodnoty totiž zvolilo 62 respondentů, což odpovídá přibližně 60% ze všech zvolených výsledků.

Tímto respondenti ukazují, že mají určité povědomí, ale je zde také prostor pro zlepšení v oblasti zájmu o anonymitu na internetu.

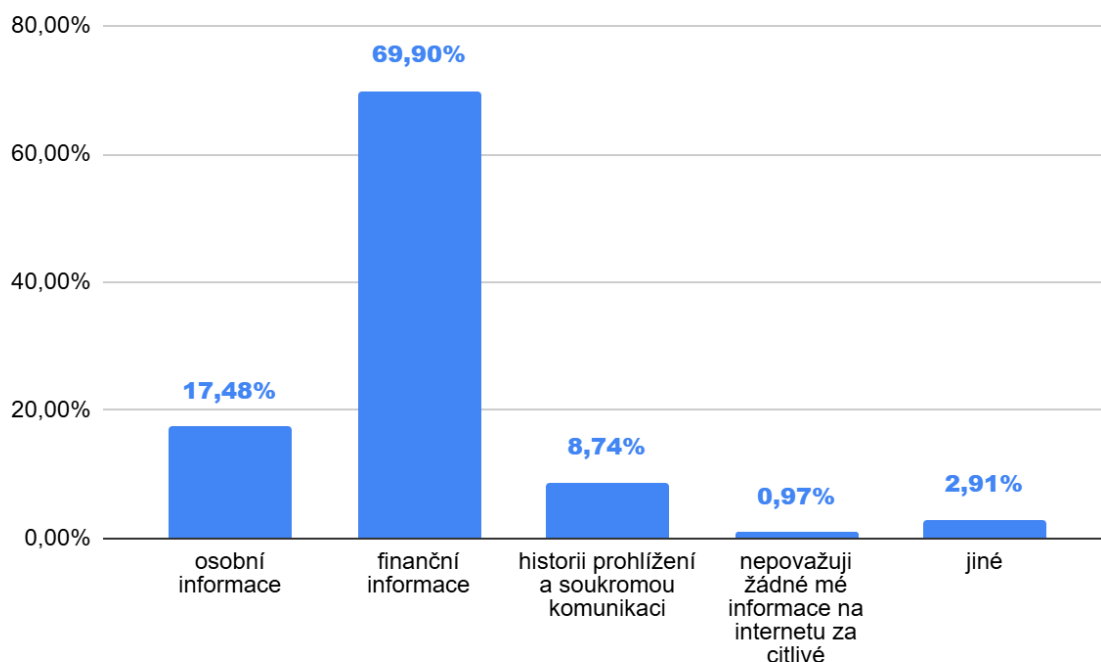


Obrázek 6 Graf zabývání se anonymitou na internetu, dotazníkové šetření, 2025

Vyhodnocení 4. otázky: Zde byli respondenti tázáni, jaké informace na internetu považují za nejcitlivější. Nejvíce volenou odpovědí byly „Finanční údaje“ a to celkem 72x. Druhou nejvíce volenou odpovědí byly „Osobní informace“ s počtem 18 hlasů, třetí pak „Historie prohlížení“ celkem s 9 hlasy, nejméně volenou odpovědí byla „Nepovažuji žádné mé údaje na internetu na citlivé“ zvolena pouze 1x, dále do otevřené odpovědi „jiné“ se vyjádřili 3 respondenti (1x „Fin. Údaje – nešlo zaškrtnout“, 1x „Finanční info i osobní údaje“, 1x „Finanční informace, historii prohlížení, soukromou konverzaci, telefonní číslo, adresa trvalého pobytu apod.“).

Z průzkumu je patrné, že respondenti vnímají jako nejcitlivější údaje především finanční informace. Ostatní typy údajů jako historie prohlížení nebo jiné osobní data jsou vnímány

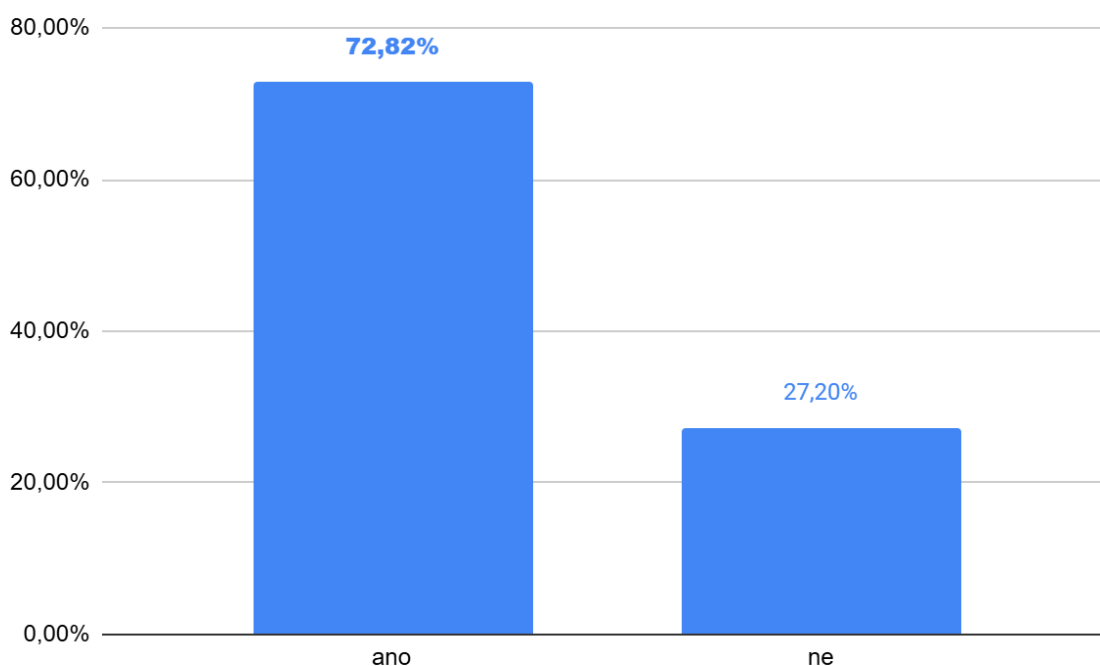
jako méně závažné. Tento výsledek potvrzuje, že rizika spojená s finančními podvody rezonují mezi veřejností nejvíce.



Obrázek 7 Graf nejcitlivějších informací na internetu, dotazníkové šetření, 2025

Vyhodnocení 5. otázky: Otázka dotazující se na to, zda se respondenti seznámili s možnostmi nastavení soukromí v rámci sociálních sítí a nastavili si je. Celkem odpovědělo 103 respondentů, kdy 75 odpovědělo „Ano“ a 28 odpovědělo „Ne“.

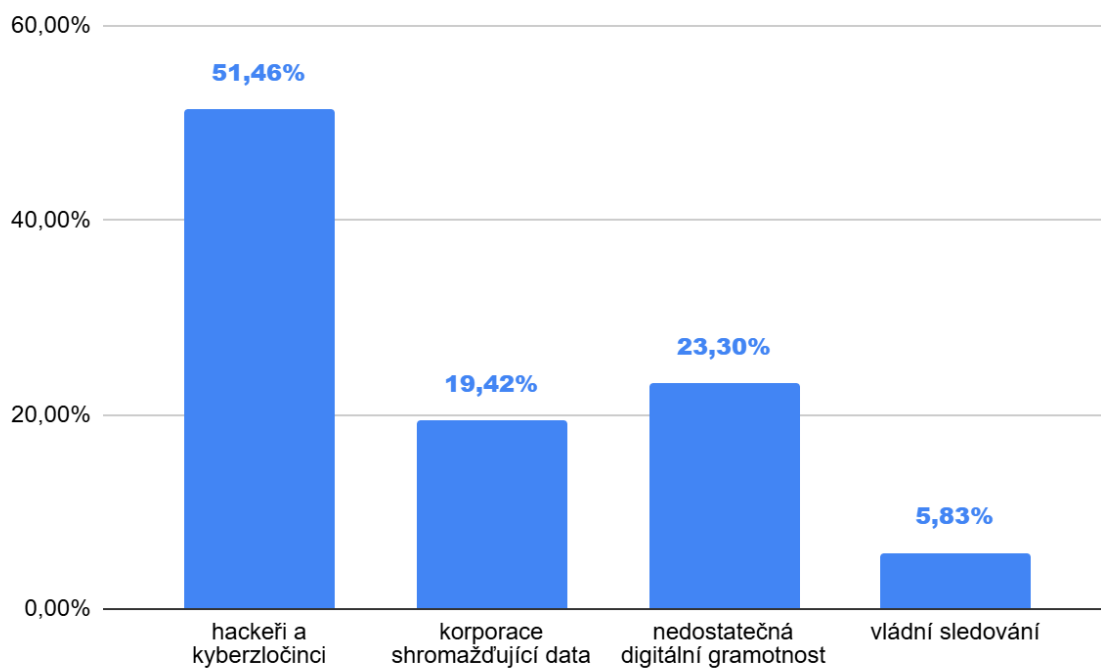
Většina dotázaných aktivně využívá možnosti nastavení soukromí, což signalizuje určité povědomí o rizicích spojených se sdílením osobních údajů na sociálních platformách. Přesto ale čtvrtina respondentů tyto nástroje nevyužívá, což představuje potenciální riziko z hlediska úniku informací.



Obrázek 8 Graf nastavení soukromí v rámci sociálních sítí, dotazníkové šetření, 2025

Vyhodnocení 6. otázky: „Co považujete za největší hrozbu pro anonymitu na internetu?“ Výsledky jsou zobrazeny na grafu 6. Ale je třeba zmínit, že nejvíce respondentů vybralo možnost „Hackeri a kyberzločinci“ a to celkem 53x. Druhou nejvíce volenou odpovědí byla „Nedostatečná digitální gramotnost“, tato byla vybrána 24x. Třetí nejvíce vybíranou variantou byla „Korporace shromažďující data“ 20x, a nejméně vybíranou možností bylo „Vládní sledování“, které bylo zvoleno 6x.

Výsledky jasně ukazují, že za hlavní hrozbu pro anonymitu jsou považováni hackeři a kyberzločinci. Respondenti ale rovněž vnímají významný podíl odpovědnosti na uživateli samotném – v podobě nedostatečné digitální gramotnosti. Vládní dohled je vnímán jako méně nebezpečný.

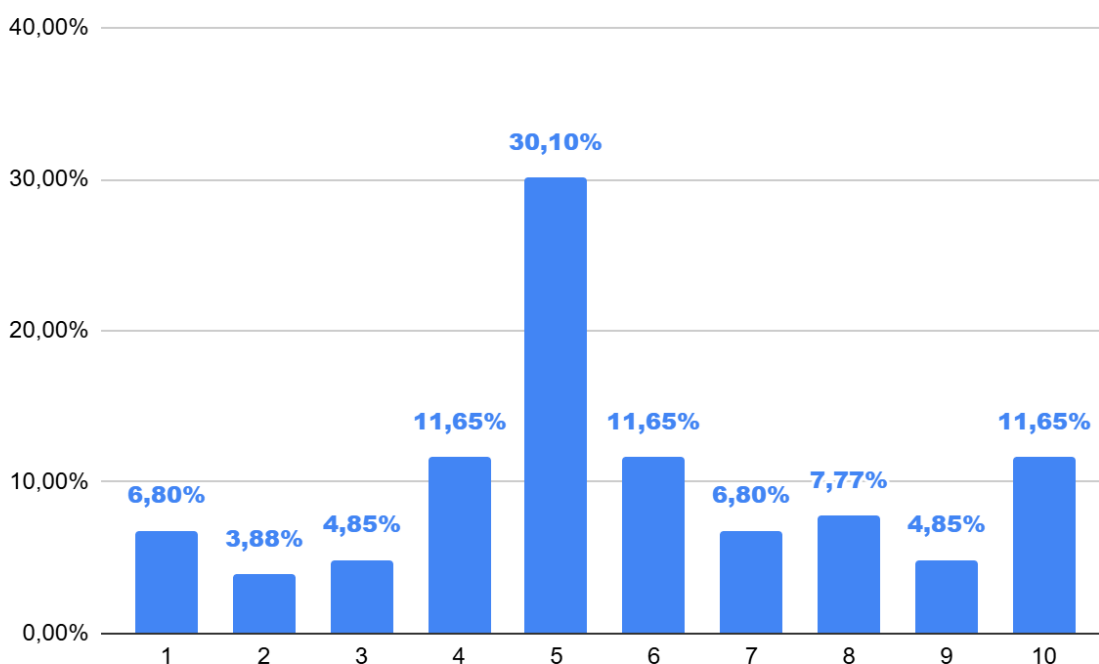


Obrázek 9 Graf největší hrozby pro anonymitu na internetu, dotazníkové šetření, 2025

Vyhodnocení 7. otázky: Zde jsou respondenti tázáni, zda by omezili svou úroveň soukromí za cenu snížení kybernetické kriminality. Odpověď je tvořena formou stupnice 1-10, kdy 1 znamená „Absolutně ne“ a 10 „Absolutně ano“. Respondenti volili následovně:

- 1 – 7x
- 2 – 4x
- 3 – 5x
- 4 – 12x
- 5 – 31x
- 6 – 12x
- 7 – 7x
- 8 – 8x
- 9 – 5x
- 10 – 12x

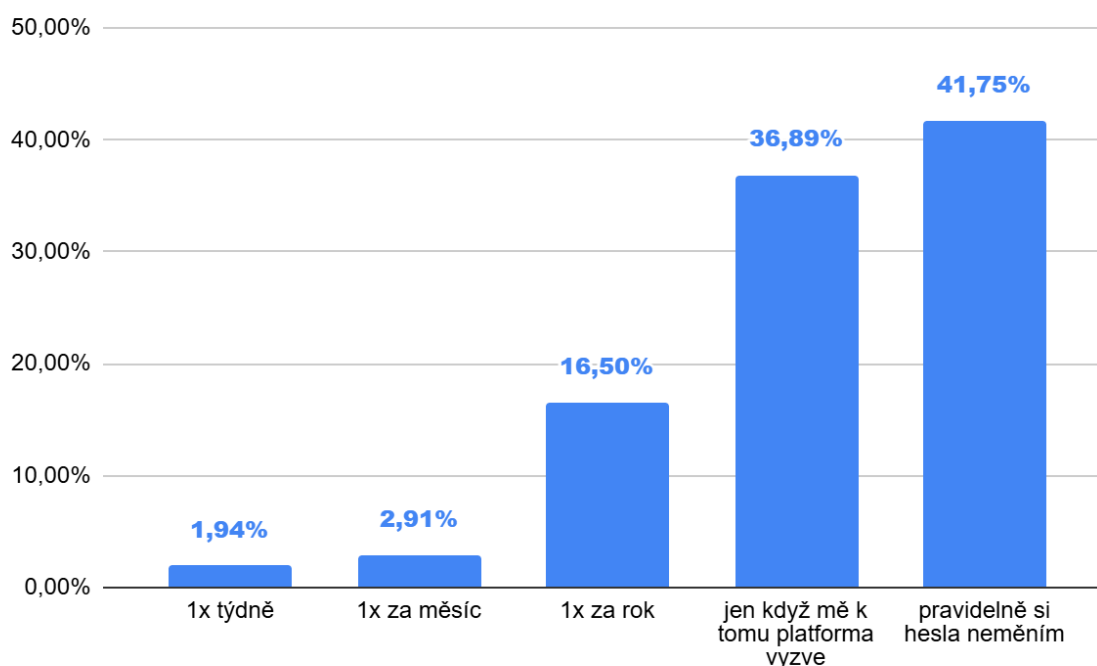
Na základě výsledku lze říci, že většina lidí odpovídající na tento dotazník by omezila své soukromí v internetovém prostředí za cenu potenciálního snížení kybernetické kriminality jen do určité míry a to v případě uvážení, že na škále jsou čísla 4-7 průměrné hodnoty. Tyto hodnoty totiž zvolilo 62 respondentů, což odpovídá přibližně 60% ze všech zvolených výsledků.



Obrázek 10 Graf snížení soukromí v internetovém prostředí za cenu snížení kybernetické kriminality, dotazníkové šetření, 2025

Vyhodnocení 8. otázky: U této otázky jsou respondenti dotazováni, jak často si dobrovolně aktualizují svá hesla k online účtům. Nejvíce zvolenou odpovědí je „Pravidelně si hesla neměním“ a to 43x. Druhou nejčastěji zvolenou odpovědí je „Jen když mě k tomu platforma vyzve“ 38x. Odpověď „1x za rok“ byla vybrána 17x, „1x za měsíc“ 3x a nejméně vybranou variantou byla „1x týdně“ a to pouze 2x.

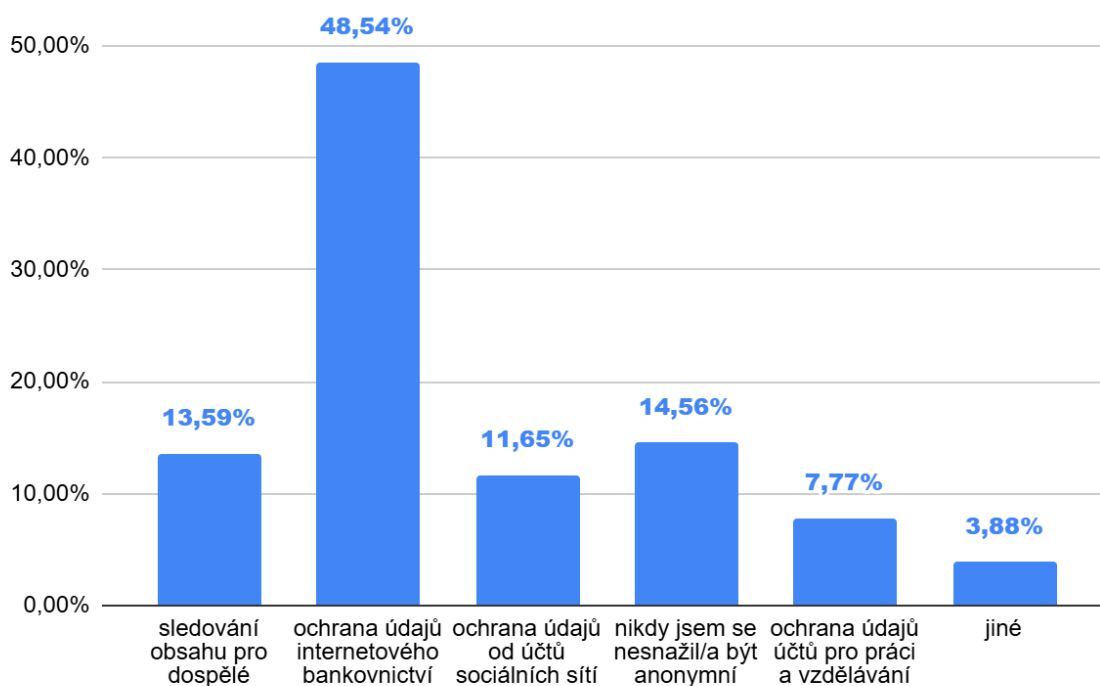
Většina respondentů hesla mění jen minimálně nebo až na základě výzvy systému. Pouze menšina aktivně přistupuje k jejich pravidelné změně. To ukazuje na nízkou prevenci proti potenciálním bezpečnostním rizikům spojeným s prolomením hesel.



Obrázek 11 Graf aktualizace hesel k online účtům, dotazníkové šetření, 2025

Vyhodnocení 9. otázky: U této otázky jsou respondenti dotazováni, jaký je jejich důvod pro anonymizaci na internetu. Ze 103 odpovědí je nejčastěji volenou „Ochrana údajů internetového bankovníctví“ a to celkem 50x. Druhou nejčastější volbou byla „Nikdy jsem se nesnažil/a být anonymní“ 15x, „Sledování obsahu pro dospělé“ 14x, „Ochrana údajů od účtů sociálních sítí“ 12x, „Ochrana údajů účtů pro práci a vzdělávání“ 8x a „Jiné“ vybráno celkem 4x (u této volby byla požadována vlastní odpověď, kdy se jednalo o 1x „Soukromí“, 1x „Vyhledávání věcí s dost pravděpodobným obsahem reklam“, 1x „Všechny zmíněné“, 1x „Aby mi nechodily reklamy, nebo hledám ceny letenek a podobně“).

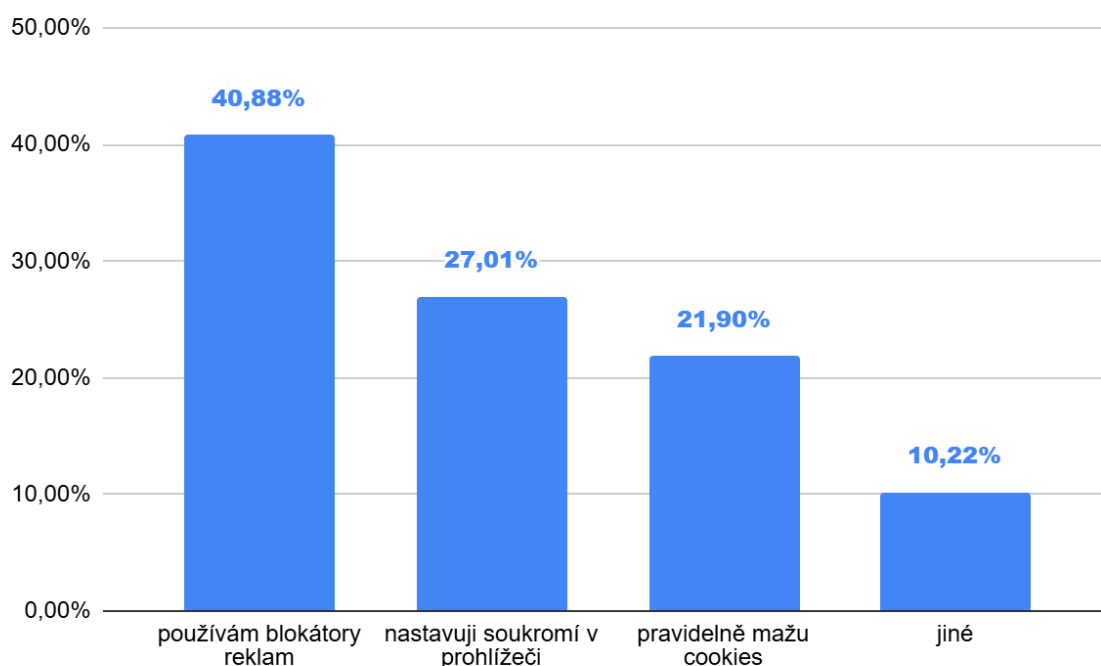
Výsledky naznačují, že potřeba anonymizace je vnímána především v kontextu finanční bezpečnosti, zatímco jiné oblasti, jako je ochrana na sociálních sítích nebo při práci, jsou často přehlíženy.



Obrázek 12 Graf důvodů pro anonymizaci na internetu, dotazníkové šetření, 2025

Vyhodnocení 10. otázky: Zde byli respondenti dotazováni, jak se chrání před sledováním reklamních společností, kdy u této otázky byla možnost vybrat více odpovědí. Nejvíce volenou variantou byla používání blokátorů reklam, kdy respondenti zvolili tuto variantu celkem 56x, dále volili nastavování si soukromí v prohlížeči a to celkem 37x, třetí odpovědí byla pravidelné mazání cookies v počtu 30 reakcí, poslední volbou bylo „jiné“, kde respondenti tvořili vlastní odpověď, kdy tuto variantu vybralo celkem 14 účastníků (u těchto se celkem 10x vyskytla odpověď, že se nijak proti sledováním reklamních společnostem nechrání, 2x se cíleně nechrání, z důvodu návrhu reklam podle hledaného obsahu, 1x vypnutí počítače a 1x „VPN, Location Spoofing, Malware, Ad a Tracker blocking“.

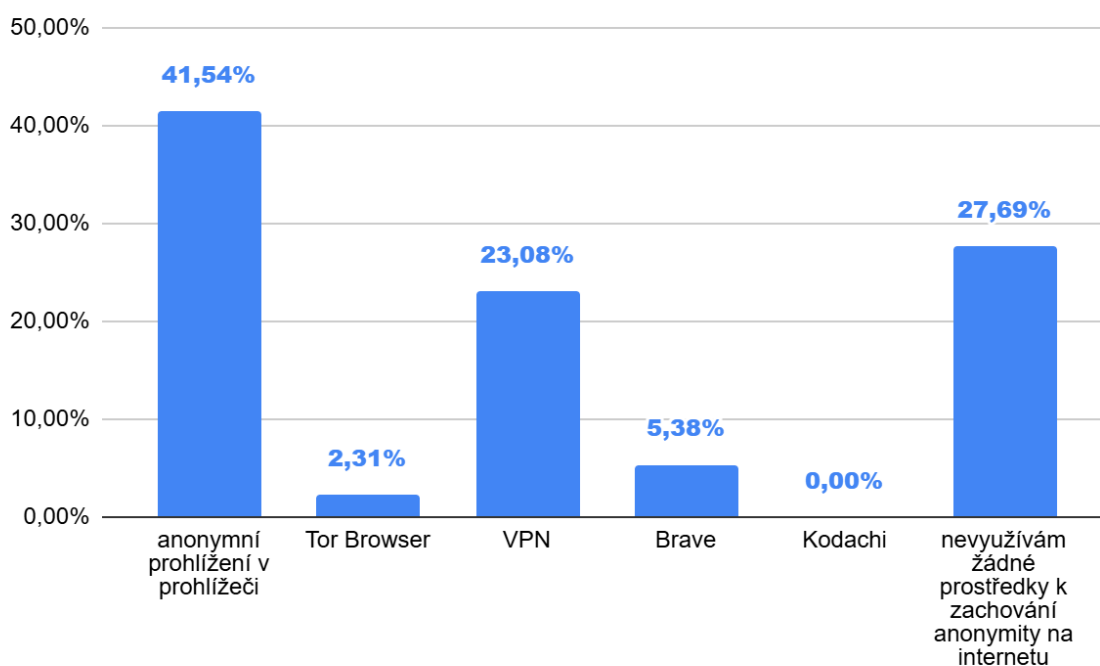
Z výsledků vyplývá, že uživatelé jsou si vědomi možnosti sledování a aktivně využívají alespoň základní nástroje pro jeho omezení. Přestože techniky jako fingerprinting nebo sledování přes třetí strany nejsou tímto zcela eliminovány, alespoň částečná obrana vůči personalizované reklamě je mezi uživateli běžná.



Obrázek 13 Graf ochrany před sledováním reklamních společností, dotazníkové šetření, 2025

Vyhodnocení 11. otázky: V této otázce respondenti uváděli, jaké prostředky využívají pro zachování anonymity na internetu. I zde bylo možné zvolit více odpovědí. Nejčastěji byla zvolena možnost anonymního prohlížení v prohlížeči, kdy se jedná o běžnou a snadno dostupnou funkci většiny moderních prohlížečů. Pro tuto variantu se rozhodlo celkem 54 respondentů. Druhou nejčastější volbou bylo „nevyužívám žádné prostředky k zachování anonymity na internetu“, kterou uvedlo 36 účastníků. Tato volba poukazuje na skutečnost, že značná část respondentů se o svou online anonymitu aktivně nestará, případně jí nepřikládá takovou důležitost. Následovala varianta VPN se 30 hlasy. Prohlížeč Brave byl zvolen 7 respondenty. Možnost „Tor Browser“ zvolili 3 účastníci. Jako poslední se umístil operační systém Kodachi, který nezískal žádný hlas.

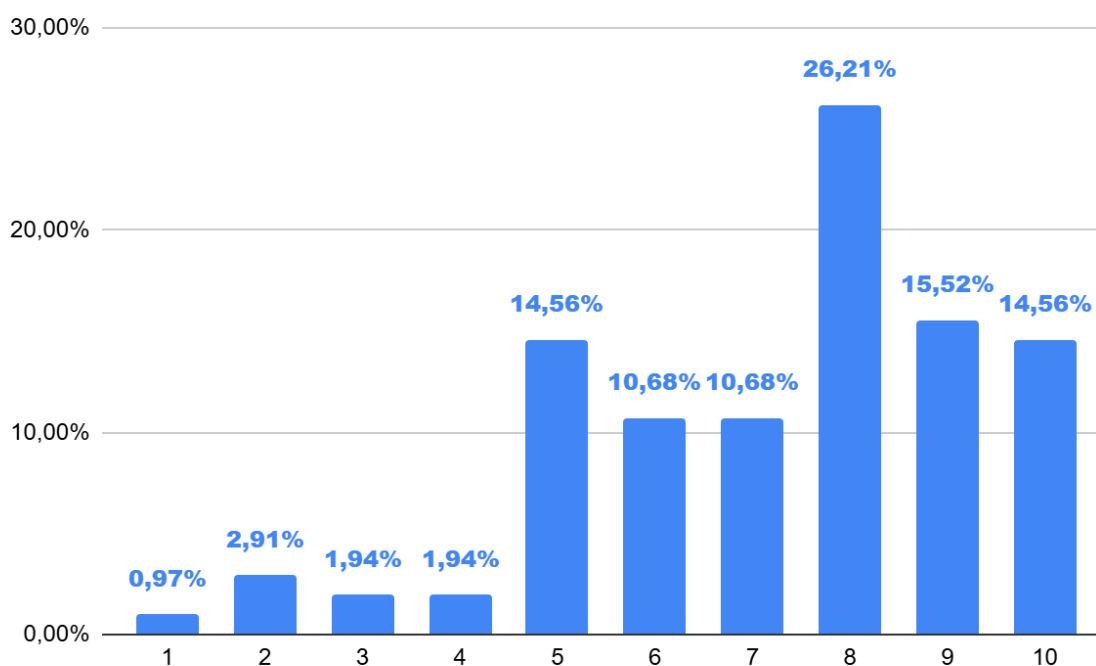
Pokročilé nástroje jako VPN nebo prohlížeč Tor využívá jen malá část uživatelů, což naznačuje, že hlubší technická řešení nejsou mezi běžnými uživateli rozšířená.



Obrázek 14 Graf prostředků využívaných k zachování anonymity na internetu, dotazníkové šetření, 2025

Vyhodnocení 12. otázky: Respondenti byli v této otázce vyzváni, aby na škále od 1 do 10 ohodnotili, do jaké míry vnímají kybernetickou bezpečnost jako aktuální problém. Hodnota 1 znamenala, že ji nepovažují za aktuální vůbec, zatímco hodnota 10 vyjadřovala, že ji považují za velmi aktuální a důležitý problém. Nejčastější hodnocení bylo číslo 8, které zvolilo 27 respondentů, což představuje 26,21 % ze všech odpovědí. Poměrně vysoké zastoupení měly také hodnoty 9 a 10 – konkrétně číslo 9 zvolilo 16 respondentů (15,52 %) a číslo 10 označilo 15 respondentů (14,56 %). Střední hodnota na škále – číslo 5 – byla vybrána 15 respondenty (14,56 %), což může poukazovat na skupinu, která vnímá kybernetickou bezpečnost jako částečně aktuální téma, ale neklade na něj zásadní důraz. Hodnoty 6 a 7 pak zaznamenaly shodný počet hlasů – každá byla označena 11 respondenty (10,68 %). Výrazně méně časté byly nízké hodnoty: číslo 1 zvolil pouze 1 respondent (0,97 %), číslo 2 tři respondenti (2,91 %) a hodnoty 3 a 4 zvolili po dvou respondentech (1,94 %).

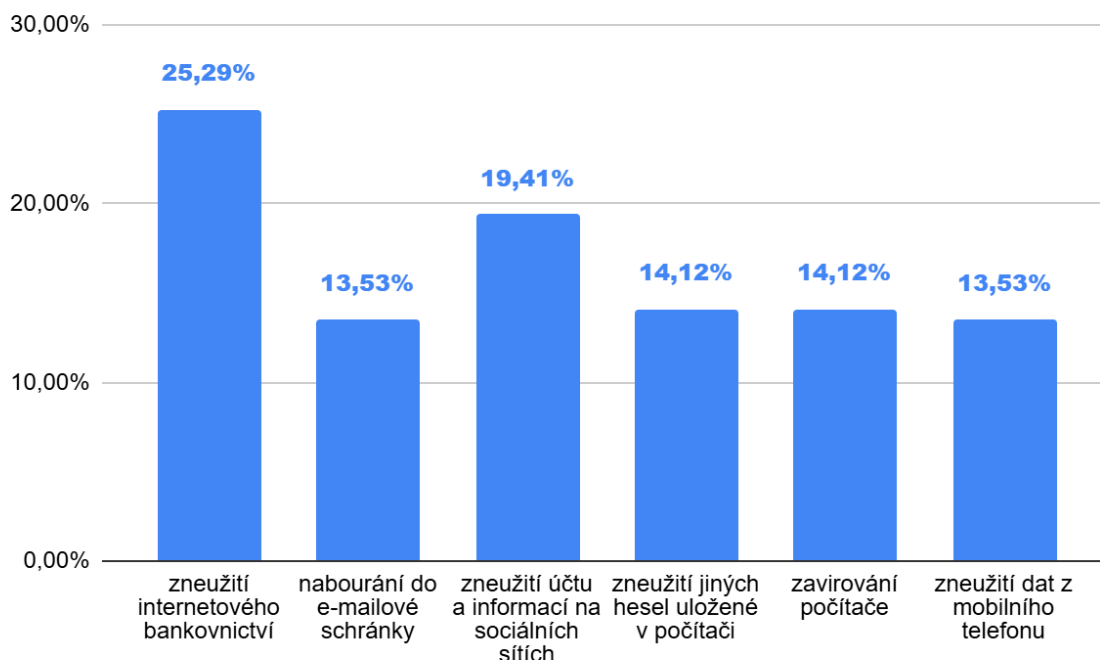
Celkově lze tedy konstatovat, že většina účastníků průzkumu vnímá kybernetickou bezpečnost jako aktuální a důležité téma, přičemž jen malé procento se k problematice staví laxe nebo s menší mírou obav.



Obrázek 15 Graf kybernetické bezpečnosti jako aktuálního problému, dotazníkové šetření, 2025

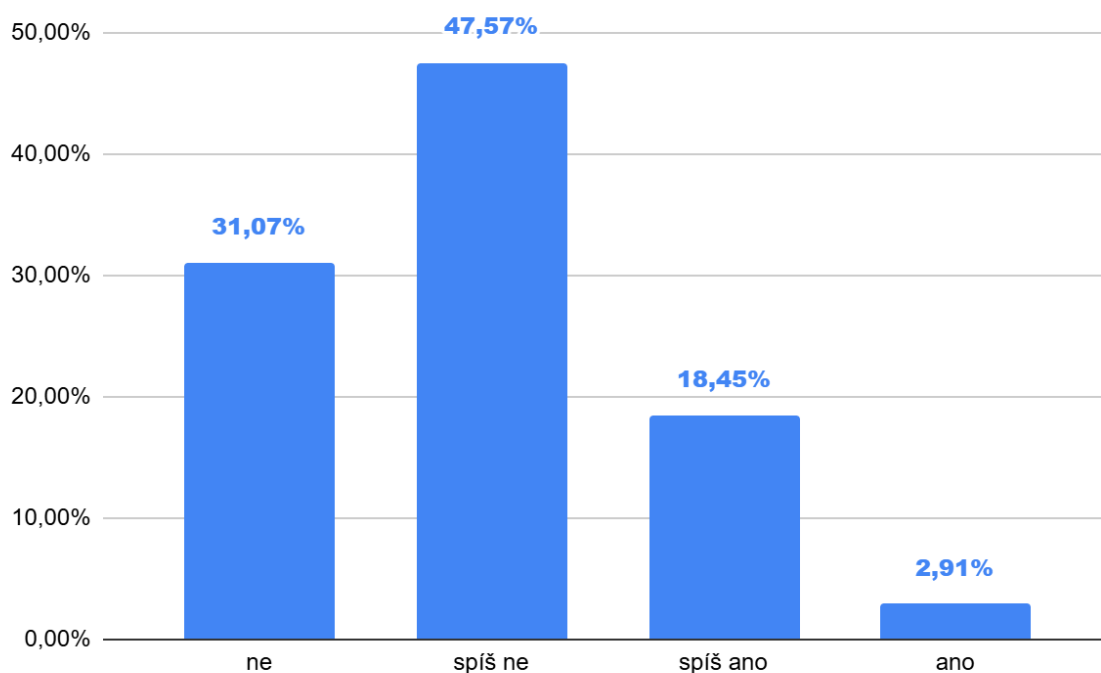
Vyhodnocení 13. otázky: V této otázce měli respondenti za úkol označit, která z uvedených rizik v oblasti kybernetické bezpečnosti považují za relevantní. Respondenti mohli vybrat více odpovědí současně, a tedy vyjádřit obavy z více hrozeb, které považují za aktuální nebo pravděpodobné. Nejčastěji zmiňovaným rizikem bylo zneužití internetového bankovníctví, které označilo 86 respondentů. Tento výsledek naznačuje, že finanční bezpečnost patří mezi nejzásadnější obavy uživatelů a že důvěra v online bankovní systémy je výrazně závislá na jejich zabezpečení. Druhé nejčastější obavy se týkaly zneužití účtu a informací na sociálních sítích, které jako relevantní riziko označilo 66 účastníků. To odráží vysokou míru vnímání rizik spojených s ochranou soukromí a identity v digitálním prostoru. Na třetím místě se umístila dvě rizika se shodným počtem hlasů a to 48 – konkrétně „zneužití jiných hesel uložených v počítači“ a „zavirování počítače“. Obě hrozby souvisejí s narušením bezpečnosti zařízení a nedostatečnou ochranou dat uložených lokálně. Dalšími vnímanými riziky bylo zneužití dat z mobilního telefonu, které označilo celkem 46 respondentů a nabourání do e-mailové schránky označilo 46 respondentů. Jako variantu „jiné“ vybrali 2 respondenti (1x „ukradení identity“, 1x „Zdaaaar“). Tyto výsledky ukazují, že si respondenti uvědomují potenciální zranitelnost jak osobních zařízení, tak komunikačních kanálů.

Celkově lze konstatovat, že respondenti vnímají největší riziko v oblastech, kde hrozí přímá finanční nebo osobní ztráta, a zároveň reflektují široké spektrum hrozeb, které s sebou přináší dnešní digitálně propojený svět.



Obrázek 16 Graf relevantních rizik, dotazníkové šetření, 2025

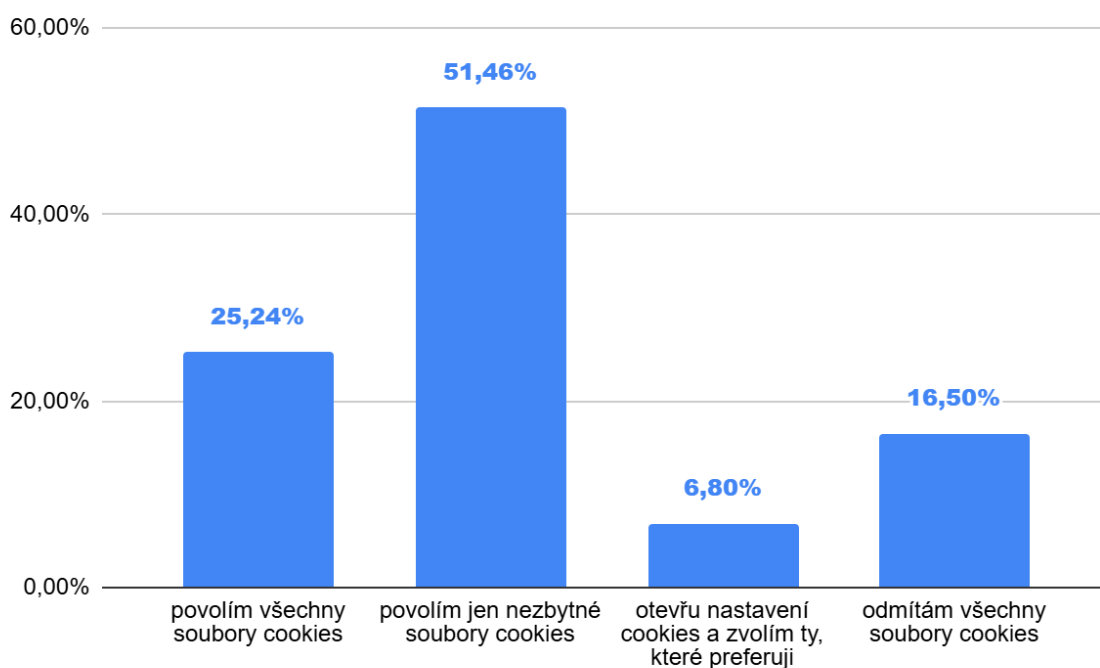
Vyhodnocení 14. otázky: Respondenti byli v této otázce dotázáni, zda čtou podmínky používání při registraci účtu či při návštěvě webových stránek. Nejčastější odpovědí bylo „Spíš ne“, kterou zvolilo 49 respondentů. To naznačuje, že ačkoliv si jsou vědomi existence podmínek používání, zřejmě je z časových důvodů, složitosti textu či nedůvěry v jejich smysluplnost důkladně nečtou. Druhou nejčastější odpovědí bylo „Ne“, kterou uvedlo 32 účastníků průzkumu. Tito respondenti přiznávají, že podmínky nečtou vůbec, a přijímají je automaticky, aniž by se seznámili s jejich obsahem. Opačný přístup tedy určitý zájem o obsah podmínek – deklarovalo menší procento respondentů. Variantu „Spíš ano“ označilo 19 účastníků, kteří si podmínky alespoň částečně pročítají. Plné čtení podmínek pak uvedli pouze 3 respondenti, kteří odpověděli „Ano“. Tento výsledek potvrzuje, že jen velmi malá část uživatelů přistupuje k těmto právním dokumentům s maximální pozorností.



Obrázek 17 Graf čtení podmínek používání při registraci účtu, návštěvě webu, dotazníkové šetření, 2025

Vyhodnocení 15. otázky: Respondenti byli dotázáni, jak reagují na výzvu k povolení cookies při návštěvě webu. Nejčastěji volili možnost „povolím jen nezbytné soubory cookies“, kdy tuto variantu vybralo celkem 53 respondentů, což ukazuje na snahu o ochranu soukromí. Dále 26 uživatelů povolí všechny cookies, zatímco 17 je odmítá zcela. Jen 7 uživatelů si ručně vybírá konkrétní typy cookies, což svědčí o nízké ochotě věnovat čas detailnímu nastavení.

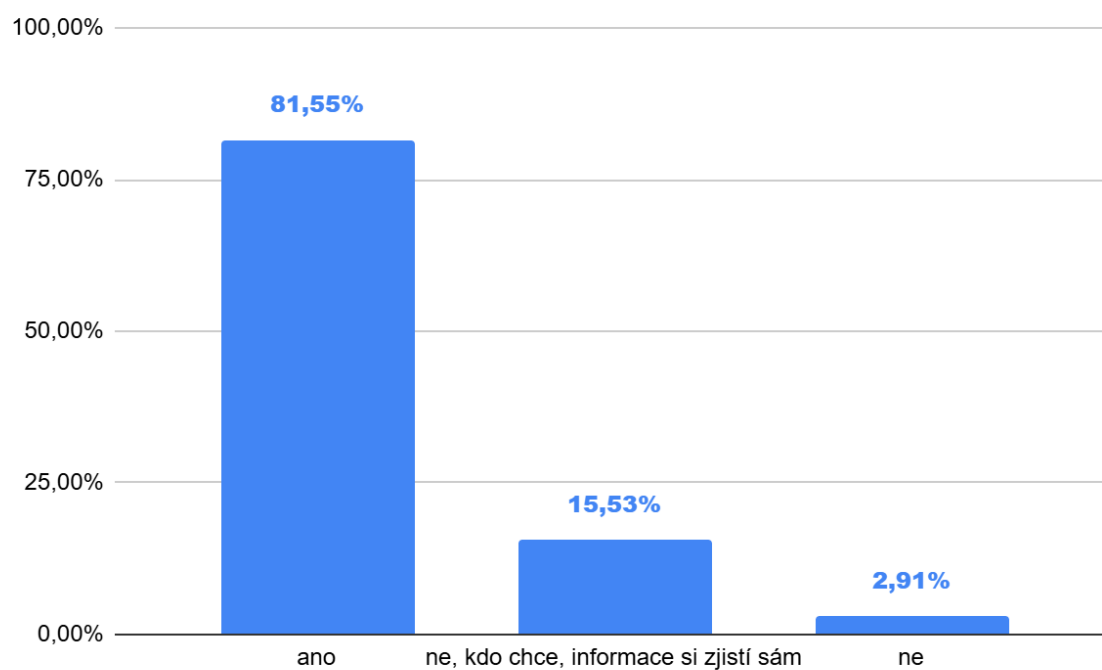
Celkově výsledky ukazují, že většina uživatelů si rizika spojená s cookies uvědomuje, ale aktivní správa zůstává okrajová.



Obrázek 18 Graf povolení cookies souborů na webu, dotazníkové šetření, 2025

Vyhodnocení 16. otázky: Na otázku, zda by respondenti uvítali větší osvětu v oblasti digitální gramotnosti, ze 103 respondentů odpověděla drtivá většina kladně – 84 z nich uvedlo „Ano“. Dalších 16 se domnívá, že informace si má každý zjistit sám, a pouze 3 účastníci průzkumu odpověděli „ne“.

Výsledky jasně ukazují, že je o vzdělávání v oblasti digitální bezpečnosti a gramotnosti výrazný zájem.



Obrázek 19 Graf osvěty stran diginální gramotnosti, dotazníkové šetření, 2025