**Česká zemědělská univerzita v Praze**

**Provozně ekonomická fakulta**

**Katedra informačních technologií**


**Bakalářská práce**

# Ochrana soukromí na sociálních sítích

**František Šejhl**

# ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE


František Šejhl

Ekonomika a management
Provoz a ekonomika


Název práce

**Ochrana soukromí na sociálních sítích**

Název anglicky

**Privacy protection on social networks**

---

**Cíle práce**

Práce se zabývá problematikou sociálních sítí z pohledu bezpečnosti osobních údajů uživatelů
Cíle jsou:
- Analýza nebezpečí používání sociálních sítí, a to z hlediska ochrany osobních údajů
- Popis metod kyberšikany, či jiných způsobů poškození osoby v digitálním světě
- Návrh strategie ochrany soukromých údajů pro uživatele při zohlednění ekonomické náročnosti.

**Metodika**

Analytická část bakalářské práce se bude zakládat na analýze a rešerši odborných zdrojů. V praktické části práce budou na základě poznatků zjištěných v analytické části zhodnoceny data získané v dotazníkovém šetření od uživatelů sociálních sítí. Dále bude vytvořeno modelové řešení ochrany osobních údajů pro uživatele sociálních sítí s ohledem na ekonomickou náročnost. Na základě syntézy teoretických a praktických poznatků budou zpracovány závěry bakalářské práce.

**Doporučený rozsah práce**

35

**Klíčová slova**

sociální sítě, ochrana údajů, kyberšikana

---

**Doporučené zdroje informací**

MATES, Pavel. Ochrana soukromí ve správním právu. Praha: Linde, 2004. 307 s. ISBN 80-7201-458-7,
MATOUŠKOVÁ, M., HEJLÍK, L. Osobní údaje a jejich ochrana. 2. vydání. Praha: ASPI, Wolters Kluwer, 2008. 468 s. ISBN 978-80-7357-322-5, s. 1.

---

**Předběžný termín obhajoby**

2020/21 LS – PEF

**Vedoucí práce**

RNDr. Alexander Galba

**Garantující pracoviště**

Katedra informačních technologií

Elektronicky schváleno dne 29. 7. 2020

**Ing. Jiří Vaněk, Ph.D.**

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2020

**Ing. Martin Pelikán, Ph.D.**

Děkan

V Praze dne 14. 03. 2021

**Čestné prohlášení**

Prohlašuji, že svou bakalářskou práci " Ochrana soukromí na sociálních sítích " jsem vypracoval(a) samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 14.3.2021 _____

**Poděkování**

Rád bych touto cestou poděkoval panu RNDr. Alexandru Galbovi za jeho trpělivost, skvělé rady a vstřícnost vůči mé osobě. Za ochotu kdykoliv konzultovat možné nápady z mé strany. A autorům odborných článků a publikací, ze kterých jsem čerpal informace a dodávali mi inspiraci.

# Ochrana soukromí na sociálních sítích

**Abstrakt**

Bakalářská práce se zaměřuje na problematiku ochrany soukromí na sociálních sítích a zjišťuje míru povědomí uživatelů sociálních sítí ohledně jejich bezpečnosti.

V teoretické části analyzuje konkrétní formy nebezpečí, které na uživatele v online světě čekají. Dále poskytuje náhled na možné prostředky sloužící k ochraně dat a soukromí pro zařízení připojených k internetu.

V praktické části bylo provedeno dotazníkové šetření, jehož cílem bylo zjistit míru informovanosti dotazovaných ohledně dané problematiky a míru jejich zabezpečení. Na základě analýzy byla navržena strategie ochrany soukromí. Navržená strategie kombinuje hledisko efektivnosti a finanční náročnosti.

**Klíčová slova:** sociální sítě, ochrana soukromí, osobní data, kyberšikana, dotazníkové šetření, strategie, finanční nákladnost

# Privacy protection on social networks

**Abstract**

The bachelor's thesis focuses on the issue of privacy protection on social networks and determines the level of awareness of social network users about their security.

The theoretical part analyses the specific forms of danger that await users in the online world. It also provides insight into possible means of protecting data and privacy for devices connected to the Internet.

In the analytical part, a questionnaire survey was conducted with a goal to find out the level of knowledge of the respondents about this issue and the level of their security. Based on the analysis, a privacy protection strategy was proposed. The proposed strategy combines aspects of efficiency and cost.

**Keywords**: social media, privacy protection, personal data, cyberbullying, survey, strategy, financial cost

# Obsah

# Seznam obrázků



# Seznam tabulek

# 1 Úvod

Bakalářská práce se zabývá problematikou ochrany soukromí na sociálních sítích.

Teoretická část definuje pojem sociálních sítí a jejich rozdělení. Dále analyzuje nejčastější nebezpečí a případná rizika pro jejich uživatele. Popisuje následky kybernetických útoků v různých formách. Dále nabízí náhled na některé možnosti ochrany osobních dat ze strany možností nabízených sociálními sítěmi či softwarů určených k ochraně dat.

Praktická část má za úkol využít poznatků z teoretických východisek a aplikovat je v praxi. Bylo provedeno dotazníkové šetření, jehož výsledky byly podrobeny analýze pro navržení cílové strategie pro ochranu dat. Data jsou v práci analyzována a hledá se možná souvislost mezi odpověďmi na různé otázky. Dále jsou sestavena kritéria pro určení míry zanedbání ochrany osobních dat. Poté je provedeno porovnání vhodných softwarů s ohledem na cenu a efektivnost. Na základě dat dotazníkového šetření je navržena strategie pro ochranu dat, která má za úkol najít kompromis mezi efektivností ochranných prostředků a jejich ekonomické náročnosti.

# 2 Cíl práce a metodika

## 2.1 Cíl práce

Cílem práce je definovat pojem sociálních sítí a rozdělit je dle jejich charakteristik. Dále analyzovat nebezpečí hrozící uživatelům sociálních sítí, popsat možnosti ochrany soukromí.

Dílčími cíli práce jsou:

- Zhodnocení míry zanedbalosti ochrany osobních údajů dle stanovených kritérií.
- Na základě analýzy odpovědí respondentů dotazníkového šetření navrhnout strategii ochrany osobních dat kombinující hledisko efektivnosti a finanční náročnosti.

## 2.2 Metodika

Teoretická část se opírá o studium odborné literatury popisující téma sociálních sítí, jejich rozdělení dle charakteristik a rizik s nimi spojených.

Hlavními zdroji jsou odborné a vědecké články a elektronické publikace.

Praktická část analyzuje provedené dotazníkové šetření zkoumající míru informovanosti uživatelů ohledně problematiky práce. Cílem analýzy je navrhnout strategii ochrany osobních dat na základě odpovědí respondentů a porovnání dostupných prostředků sloužící k těmto účelům a zvolení kompromisního řešení. Toto řešení zohledňuje efektivnost použitých prostředků a jejich ekonomickou náročnost.

# 3 Teoretická východiska

## 3.1 Sociální sítě – účel a funkce

S technologickým pokrokem lidstvo a mezilidské vztahy změnily své základní principy jejich udržování. Internet s možnostmi, které přinesl vytvořením sociálních sítí svým způsobem ulehčil komunikaci mezi dvěma, nebo více jedinci, a to je možný důvod, proč tyto platformy momentálně zažívají raketový vzrůst.

Evropská agentura pro informační a síťovou bezpečnost ve své studii popisuje sociální sítě jako online komunitu, která umožnuje lidem skrze účty vytvořené na těchto stránkách, či aplikacích se potkávat, komunikovat, sdílet zážitky, nebo si vzájemně posílat obsah ve formě obrázků, videí atd. (ENISA, 2010)

V offline světě můžeme chápat sociální sítě jako sociální vazby, které nás spojují s ostatními lidmi jako jsou rodina, přátelé, známí, spolužáci, kolegové, sousedi a další. Představte si pavoučí síť. Všechna vlákna reprezentují naše vazby na okolní svět. Sociální sítě jsou digitální platformu, kde lidé, kteří se rozhodli být uživatelé této platformy, musí předem souhlasit s podmínkami užívání. Tyto platformy jsou prakticky virtuální verze našich každodenních sociálních interakcí.

Sociální sítě mají pro jejich uživatele široké možnosti užití. Lidé se zde mohou setkávat a komunikovat s ostatními a, sdílet své zážitky, diskutovat o různých tématech, hrát online hry. Mohou také tvořit různé komunity, a to se skupinami, které s jedincem sdílí některé vlastnosti jako například to mohou být lidé ze sousedství, kteří se v reálném světě neznají. Přesto v těchto skupinách komunikují a upozorňují na jednotlivé události odehrávající se dané části města. Dále to mohou být skupiny spjaté například pohlavím, zájmy, vírou a mnoho dalšími vlastnostmi charakteru uživatele.

Obchodní společnosti mohou sociální sítě využívat k přestavování a propagaci svých produktů, či dokonce k navázání spoluprací s ostatními společnostmi.

Různé typy sociálních sítí slouží k různým účelům. Některé dokonce dovolují autorům svou práci vystavit a tím získat cestu ke spolupráci, či živit se přímo propagací jiných produktů formou reklamy.

Ani vzdělávací instituty a organizace nezahálely a využívají těchto nynějších internetových trendů pro účely vzdělávání ať už adolescentů, či poskytováním kurzů lidem, kteří si chtějí osvojit znalosti v jistých oblastech vzdělání

Výhoda sociálních sítí tkví v tom, že mají prostředky a dokážou přimět uživatele k samostudiu**.** (Khan Academy, 2017)

Milos Papic ve své studii na téma možnosti užití určitých sociálních sítí pro účely vzdělávání uvádí, že internet a digitální sítě vytvářejí nový vzrušující svět plný informací a možností komunikace pro každého, kdo se k této síti připojí. Poskytují mladým lidem nespočet možností ke vzdělávání, komunikaci a utváření jejich vnímání světa kolem nich.

Dnešní technologie poskytují adolescentům mnohem komplexnější přístupnost informací, kultury a zábavy, který se zdál před dvaceti lety nemožný.

Dnešní forma sociálních sítí má obrovskou roli ve vzdělávací oblasti. Jsou to nástroje umožňující kooperaci, sdílení znalostí, interakce a komunikace uživatelů se stejnými zájmy, cíli, nebo potřebami z celého světa.

Proto mnoho studentů začalo zakládat skupiny na pomoc při vzdělávání. To přimělo učitele modernizovat své metody a začít využívat sociální sítě jako pomůcku při vyučování a tím zlepšit přístup studentů k látce a podpořit je v diskusi mezi sebou na dané téma.

Průzkum ukázal, že sociální sítě operují na mnoha úrovních společnosti, od rodiny až po celý stát. Hrají kritickou roli v determinaci našeho způsobu myšlení a řešení problémů, jak fungují organizace, nebo jak moc se jednotlivci podaří dosáhnout svých individuálních cílů. (Papic, Karadac 2016)

## 3.2 Sociální sítě a jejich rozdělení

Sociální sítě se rozlišují podle jejich zaměření. Různé sociální sítě se zaměřují na zcela jiné zájmy a poskytují jiné formy obsahu a aktivit, kterých se jejich uživatelé mohou účastnit.

### 3.2.1 Sociální sítě zaměřené na uživatele

Jsou zde sociální sítě, které se soustředí na uživatele a jejich profil jako takový. Tyto sociální sítě se zaměřují na jedince a jejich vzájemnou komunikaci. Mohou zde vytvářet skupiny, komunity zahrnující uživatele se stejnými zájmy, vírou

atd. Tyto platformy umožnují sdílení různého obsahu od obrázků či videí, přes hypertextové odkazy na různé dokumenty, videa na jiných platformách až po pozvánky do online her.

Celkově tyto stránky a aplikace shromažďují a sdružují různé druhy a způsoby komunikace a sdílení obsahu a tím pádem ulehčují komunikaci mezi uživateli.

Jedná se prakticky o virtuální osobnost určitého jedince, která projektuje svoje chování na této platformě.

Tento typ sociálních sítí patří mezi nejoblíbenější typy sociálních sítí a spadá pod ně například Facebook, LinkedIn nebo Twitter.

#### 3.2.1.1 Facebook

Facebook je stránka fungující jako sociální síť zprvu určena pro studenty Harvardské Univerzity pro účely diskuze o jejich známkách a aktivitách byla vytvořena Markem Zuckerbergem. (Hall, 2020)

Spuštěn byl v únoru 2004 a za pouhých 24 hodin už tato síť čítala 1200 studentů, kteří se k ní přihlásili. Později k ní byly přihlášeny všechny Bostonské univerzity.

V roce 2005 společně s nově přidanou funkcí označovat lidi na fotografiích, která zlepšila sdílení zážitků mezi uživateli se Facebook otevřel i pro Univerzity mimo USA.

Od roku 2006 byl Facebook spuštěn celosvětově pro všechny uživatele, kteří byli starší 13 let. (Phillips, 2007)

Nyní Facebook slouží jako nejpoužívanější sociální síť obsahující všechny výše zmíněné funkce a díky snadnému sdílení multimediálních souborů a dalším funkcím které obsahuje se stal průkopníkem v této sekci sociálních sítí. (TechTerms, 2008)

##### 3.2.1.1.1 Twitter

Twitter byl založen roku 2006 Evanem Williamsem a Biz Stonem. Oba pracovali v daném momentu pro firmu Google. William, který opustil Google založil firmu soustředící se na tvorbu podcastů Odeo. Vytvořil nástroj Blogger a viděl budoucnost v podprojektu SMS (short message service), který umožňoval zasílání krátkých zpráv, tak skoupil Odeo a založil firmu Obvious Corp. a tento projekt dále

rozšiřoval. Twitter byl oficiálně založen v dubnu roku 2007. (Encyclopedia Britanicca, 2020)

Nyní je Twitter je sociální síť umožňující jejím uživatelům zveřejňovat krátké příspěvky zvané tweety. Dále umožnuje reagovat na tweety ostatních formou komentářů a sledovat ostatní uživatele z různých zařízení. Tweety a odpovědi na ně se zasílají formou textových zpráv na mobilním zařízení a na stolním počítači sdílením příspěvku na stránce Twitter.com. (Cambridge Univesity Press, 2020)

Hlavní rozdíl Twitteru od Facebooku nebo LinkedIn je, že vše, co sdílíte je veřejné. K tomu, aby si někdo prohlédl vaše příspěvky nepotřebuje vaše svolení formou přijetí žádosti.

Tweety, které mohou obsahovat hypertextový odkaz mohou nést maximální délku 140 znaků a slouží z větší části ke sdílení názorů k určitému tématu a zavedení diskuze skrze funkce vlákna, která uchovává komentáře ostatních uživatelů na daný tweet.

Další funkcí je možnost retweetnutí (sdílení originálního příspěvku na svém profilu s informací o zdroji příspěvku), která slouží ke sdílení buď politických názorů, informací společností a jednotlivců o jejich produktech a projektech, nebo jen sdílení myšlenek autora tweetu.

Dále je zde možnost sdílení krátkých videí, gifů a dalších formátů obsahu. (Rouse, 2015)

#### 3.2.1.2 LinkedIn

LinkedIn je sociální síť zaměřena pro pracovní a business účely. Umožnuje sdílení informací týkajících se pracovních záležitostí a zobrazuje online seznam pracovních kontaktů uživatele.

Jako Facebook, nebo MySpace vám tato sociální síť umožňuje vytvořit svůj osobní profil, ale hlavní rozdíl je, že tento profil se vztahuje k pracovním informacím, které obsahuje namísto osobních údajů. LinkedIn například umožnuje vypsat a zvýraznit nejvýše dosažené vzdělání a minulé pracovní zkušenosti uživatele, tím pádem slouží prakticky podobně jako podrobný životopis.

Používáním LinkedIn může uživatel udržovat kontakt se současnými kolegy, nebo i s kolegy z minulosti. Může zde také hledat nové lidi a tím si, popřípadě najít nové business partnery. Lidé mimo váš užší okruh v síti si sice nemohou vidět celý

váš profil, ale zato mohou vidět vaše dosažené vzdělání a pracovní zkušenosti. Na základě těchto informací vám mohou zprávu pomocí „InMail“ služby, což může vést k novým pracovním nabídkám. (TechTerms, 2010)

### 3.2.2 Sociální sítě zaměřené na obsah

Tyto sociální sítě se zaměřují na obsah, který jejich uživatelé tvoří. Mohou zde sdílet jejich nápady, myšlenky, návody nebo další formu obsahu, která může lidi pobavit, nebo dokonce i vzdělávat.

Tyto sociální sítě umožnují sdílení fotografií, videí či hudby. Každá sociální síť je svým způsobem odlišná, tím pádem se liší její grafické zobrazení a chování od ostatních.

Podle statistik Pew Research Center se tyto sociální sítě za posledních 7 let pomalu stávají oblíbenější a používanější než sociální sítě zaměřené na uživatele. Sociální sítě jako je například Twitter nebo LinkedIn překonaly v počtu uživatelů sítě jako jsou YouTube, Instagram, nebo Tik Tok.

Jen Facebook se drží stále na prvním místě jako nejpoužívanější sociální síť dnešní doby. Tím, že skupuje ostatní sociální sítě jako Instagram, WhatsApp a mnoho dalších se zdá, že tento gigant ve svém oboru se prvního místa nechce vzdát. (Pew Research Center, 2019)

YouTube

YouTube je služba, která slouží ke sdílení příspěvku ve formě videí. Umožňuje uživatelům této platformy nahrát jejich videoobsah, nebo vyhledat a přehrát si videa vytvořené jinými uživateli této sociální sítě. (Technopedia.com, 2016)

Tato služba začala jako nezávislý projekt v roce 2005 a v roce 2006 byl zakoupen firmou Google.

Slogan této platformy „Broadcast Yourself“ (Vysílání sebe sama) indikuje hlavní záměry tohoto média. Je designována pro lidi, kteří chtějí tvořit a nahrávat videa na tuto platformu. YouTube používají i různé firmy a organizace na propagaci své kampaně, nebo produktů. Většinu uživatelů YouTube stále ale tvoří tvůrci amatéři.

YouTube umožňuje nahrát videa lidmi z celého světa, a to na jakékoli téma či styl. Proto poskytuje rozsáhlý sortiment obsahu, který se může skládat z amatérských

filmů, amatérské muziky nebo vtipných videí. Lidé také ale sdílí různé návody jako je například „Pomoc s počítačem krok za krokem“, domácí instruktážní videa na výrobu různých produktů a dalších podobných nápadů.

Od doby, co YouTube začal nabízet zisk za tzv „Kliky na reklamy“ vygenerované na stránce s videem se některým lidem podařilo vytvořit ze své YouTube produkce celkem profitující business.

Skrze svá videa získávají více a více sledujících a pomocí spoluprací s určitými firmami, které zobrazují své produkty na stránce nebo přímo ve videu, ať už reklamní přestávkou od videa nebo přímo promováním produktů, či služby samotným tvůrcem získávají peníze. Čím více lidí reklamu zhlédne, tím více zisku z toho tvůrce má.

Zatímco se YouTube dá využít pro business účely, slouží pro běžného uživatele jako prostředek zábavy a to je její hlavní účel. Problém s tím, že všichni uživatelé mohou nahrávat jakýkoliv obsah pořízený prakticky jakoukoli technikou znamená, že by lidé měli být pozorní, co nahrávají na servery, protože poté jejich obsah může vidět celý svět. (TechTerms, 2009)

#### 3.2.2.1 Instagram

V říjnu roku 2010 byl Instagram spuštěn pro zařízení IPhone a v prosinci téhož roku měl už 1 milion aktivních uživatelů. V roce 2011 se spustil celosvětově s novou možností přidat filtry k fotografiím a zažil raketový vzestup. V roce 2012 byl zpřístupněn pro zařízení Android, a ještě téhož roku byl skoupen firmou Facebook. (Newaudiencemedia.com.au, 2020)

Nyní je Instagram aplikace pro úpravu fotografií. Je to online služba pro sdílení fotografií. Umožnuje uživatelům pořídit, upravit, změnit filtry a sdílet fotografie během kliknutí. Jednoduchost této platformy ji přinesla takovou popularitu, jakou dnes má a masivní zájem o její služby.

Prakticky každý mobilní telefon má v sobě zabudovanou kameru a fotoaparát, ale ne vždy produkují kvalitní fotografie. Používáním Instagramu můžete oživit tyto fotografie různými nástroji jako jsou filtry pro zvýšení jasu a kontrastu fotografie, změnu teplosti barev, nebo dokonce přidání efektu rozmazání a upravit, aby vypadaly profesionálněji.

Primárně se tato služba využívá přes aplikaci na mobilních zařízeních nebo přes stránku Instagram.com a nabídne vám nahrávání, úpravu fotografií a sdílení s přáteli, které na nich můžete označit. Dále můžete využít dalších nástrojů jako přidání aktuální polohy, či malého segmentu hudby jako pozadí fotografie. (TechTerms, 2014)

#### 3.2.2.2 Twitch

Twitch je platforma, která umožnuje hráčům sdílet svůj obsah se svými diváky formou živého vysílání a tím s nimi vytvářet komunitu, kterou spojuje zájem o danou videohru, téma, které se řeší, nebo jen osobnost streamera (vysílajícího). Ti mohou buď vysílat přímo hraní videohry, sledovat vzdáleně esportové šampionáty, nebo podpořit svého kompetitivního hráče v dané sekci.

Twitch je spíše sociální komunita hráčů, nežli webová stránka sledovaná pro zábavu. Na rozdíl od jiných platforem, či profesionálních sportů, má divák na Twitchi možnost se spojit s vysílajícím v reálném čase (okamžitě) pomocí živého chatu, kde se mohou bavit mezi sebou, ptát se na otázky ohledně jistých témat, nebo přímo komunikovat s vysílajícím.

V roce 2019 je průměrný měsíční počet sledujících 1,274 milionu, kteří sledují 50 800 streamerů poskytujících živou formu obsahu.

Na rozdíl od Googlu nebo Youtube je Twitch platforma poskytující obsah zdarma a je poháněná hlavně formou odběrů, kterou mohou uživatelé podpořit svého oblíbeného streamera nebo formou reklam podobně jako na platformě YouTube.

Nicméně mateřská společnost vlastnící Amazon, která vlastní Twitch si od roku 2014 pohrává s business modelem, čímž hýbe s procenty a nutí kompetici podnikat jisté kroky jako odpověď na tyto jejich kroky.

Zisk z této platformy a všech akcí kolem se v roce 2021 odhaduje na 1,26 miliard amerických dolarů. (Fortney, 2019)

#### 3.2.2.3 TikTok

Tik Tok je v dnešní době masivně populární aplikace, která umožnuje uživateli sdílet videa kratší než 60 vteřin, kde uživatelé tzv „Lip syncují“ různé skladby. Tato videa se stala velice populárními a dala šanci na vzestup mnoha

mladým influencerům (uživatelům sociálních médií, kteří mají vliv na své obecenstvo/fanoušky). (Dictionary.com, 2020)

Tato aplikace pochází z aplikace Muscal.ly, která poskytovala sdílet patnácti vteřinové klipy, která měla přes 100 milionu uživatelů, kde mohli lidé pomocí lip syncu vytvářet zábavná videa pro ostatní uživatele.

V roce 2018 tuto aplikaci koupila čínská firma ByteDance a všechny tvůrce přemístila na aplikaci Tik Tok, kde se této formě podařilo získat ještě větší pozornost. (MarketingHub, 2020)

## 3.3 Analýza nebezpečí ohrožení osobních údajů při používání sociálních sítích

### 3.3.1 Viry, červi a další malwary

Nejběžnější způsob narušení zařízení a získání kontroly nad osobními daty jsou viry, červi a malwary. Tento způsob je pro laika užívající jakékoliv zařízení pro přístup k síti zcela cizí a nepochopený. Nejedná se zcela o lidskou chybu, ale přesto v ní chyba osoby užívající zařízení hraje značnou roli. Tím, že tato metoda není tak osobní, jako jiné metody, které se pro digitální útoky používají je obeznámení o prevenci vůči těmto útokům zcela podceňované a ignorované.

Jedná se o škodlivé programy a nástroje, které se do zařízení uživatele dostanou za pomocí stažení určitých dat ze sítě do konkrétního zařízení. (Nott, 2020)

### 3.3.2 Spyware a adwary

Spywary jsou předem navržené programy, které se se staženými daty dostanou do koncového zařízení a nainstalují se bez vědomí vlastníka zařízení. Tento program je spuštěn a operuje v pozadí. Bez příslušných programů, které jsou schopné tyto spywary detekovat a zneškodnit jsou pro nás prakticky neviditelné.

Spywary shromažďují informace o každém pohybu uživatele na síti a odesílá je strůjci tohoto programu. V praxi se jedná o program nejvíce využívaný pro sledování vašeho pohybu a vyhledávání informací, služeb nebo zboží na internetu a poskytování těchto informací jeho strůjci pro větší přehled o vašem pohybu a zájmech. Tento typ malwaru je jeden z nejnebezpečnějších malwarů existující v digitálním světě. Důvodem tohoto tvrzení je fakt, že spyware je nesmírně těžké

identifikovat, protože narozdíl od většiny ostatních malwarů jeho operace nejsou zcela viditelné uživateli. Nijak neupravuje, nemaže, nekopíruje data. Jen shromažďuje a odesílá osobě, která uživatele sleduje a má přehled o jeho soukromých zájmech.

Tento malware je občas užitý samotnými firmami nabízejícími své produkty na síti. Sleduje potenciální zákazníky a poskytuje informace o jejich vyhledávání a jako reakce na tyto operace následně zobrazuje pomocí adwarů reklamy a oznámení související s vyhledáváním uživatele.

Uživatel chce například koupit lyže na zimu a hledá ideální produkt, který chce koupit. Spyware zachytí jeho výsledky vyhledávání a odešle je osobě, která mu pomocí adwaru zobrazí reklamu na produkt na jejich e-shopu. (Nott, 2020)

### 3.3.3 Viry

Počítačový virus je program vytvořený a určený k operaci a páchaní škod a datech obsažených v zařízení. Vir je bez správného programu pro jeho zneškodnění těžké detekovat. Viry mají různé účely a tím pádem je můžeme rozdělit do různých kategorií.

Červ je vir určený pro napáchání škod na datech ve velkém měřítku. Tento vir může být například obsažený v emailu jako příloha a při jejím otevření se dostane do vašeho zařízení. Toto se vztahuje i k sociálním sítím, kde se tato příloha objeví v konverzaci dvou jedinců, a to i v podobě vtipného obrázku, nebo odkazu na externí stránku. Tyto viry jsou ale vytvořeny pro rychlé šíření, a proto je jejich přítomnost častější ve skupinových konverzacích, kde mohou infikovat více uživatelů, kteří ho mohou šířit do dalších skupinových konverzací.

Tato příloha může po otevření provést různé operace, ať už shromáždění osobních dat jako jméno, příjmení, datum narození a další, nebo získání přístupu k soukromým fotografiím, které mohou být dále využity pro další účely bez vědomosti osoby na nich zobrazené. Toto může vést k různým operacím jako například nezákonnému prodeji těchto dat jiné osobě, kyberšikaně a mnoha dalším účelům, které může osoba zodpovědná za vytvoření viru provést.

Virus se může šířit i v podobě audiovizuální nahrávky, videa, a dokonce i v podobě antivirových programů určených pro jejich detekci a eliminaci.

Dalším typem je například Trojský kůň. Název tohoto viru je mezi uživateli internetu poměrně známý a i laikovi v této oblasti něco řekne, ale bohužel si většina ze zmíněných neuvědomuje, co vlastně tento vir způsobuje. Na rozdíl od názorů, že uživateli „zpomalí a zaseká“ zařízení tento vir po instalaci umožnuje jeho tvůrci dálkově kontrolovat a ovládat zařízení, na kterém byl nainstalován. Může tím pádem odesílat data pro své účely. Získat přístup k chráněným prostředkům a používat je pro své účely.

Botnet je typem viru, který softwarovou část infikovaného zařízení vystaví v síti, kde nad ním má osoba zodpovědná za útok stejnou kontrolu jako v případě trojského koně čili plnou dálkovou kontrolu nad zařízením.

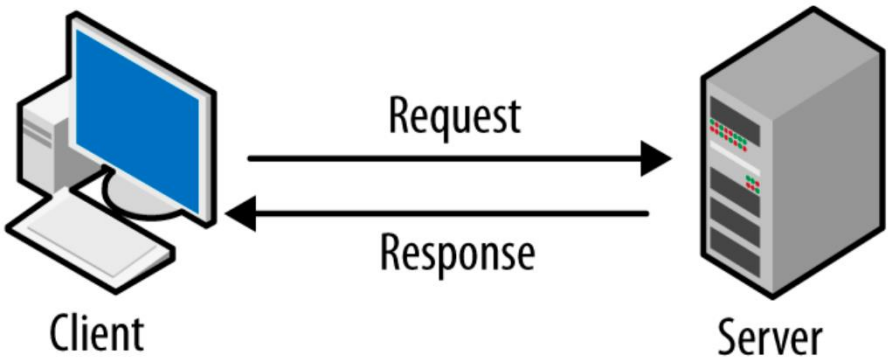
Je to speciální typ viru, který se maskuje, aby mohl infikovat zařízení. Může se maskovat i jako antivirový program. (Kaspersky Lab., 2020)

### 3.3.4 Phishing

Phishing je metoda získávání dat. Funguje na principu prostředníka. Osoba stojí mezi legitimní stránkou, které zasílá data ke zpracování a očekává odpověď od serveru.

Struktura klient-server, na které se tato metoda odcizení údajů vyskytuje, funguje na jednoduchém principu. Klient, pro nás uživatel pošle data na server obsahující jisté informace a požaduje po stránce jistou reakci formou odpovědi a zaslání potřebných údajů zpět na klientův konec. Tento princip například popisuje připojení na webovou stránku na určitém serveru. (Madooei, 2020)

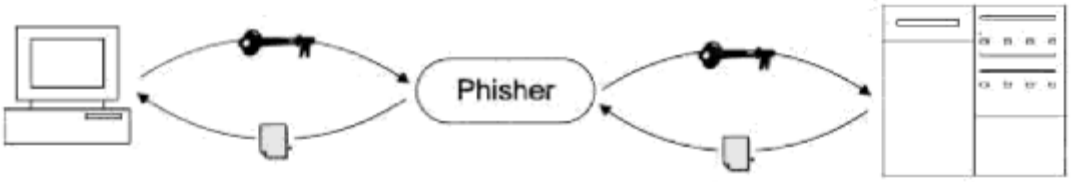
**Obrázek 1: Klient server schéma**




Zdroj: Moodie, 2020

Phishing je metoda, kde se do tohoto procesu přidá prostředník, který se nazývá „Phisher“. Jeho cílem není utnout, nebo měnit tok dat, která jedna strana zasílá druhé, ale krást a ukládat data obsažené v tomto přenosu. Tento styl krádeže je těžké detekovat, protože stránka se uživateli zdá legitimní a server nemá problém s klientem a data mu poskytne. Celá výměna dat tak proběhne naprosto v pořádku a uživatel nemá ponětí, že jeho soukromá data byla právě odcizena. (Wiley, 2006)

**Obrázek 2: Phishing and Countermeasures schéma**




Zdroj: Wiley, 2006

Phishing na sociálních sítích se stal velkým problémem v roce 2015, kdy mnoho jedinců založilo fiktivní účty již existujících firem a spoléhali se na víru zákazníků v dobré jméno firmy.

S tímto přístupem k mnoha uživatelům, kteří pravidelně komentovali a diskutovali o jejich potřebách, ale netušili, že se jedná o podvod začali zasílat emaily, ve kterých byly obsaženy malwary v mnoha formách.

Dále začali malwary šířit za pomocí příloh v komentářích, či soukromých konverzací v chatu s uživateli. S velkým přísunem uživatelů na sociální média a novým stylem marketingu se zvětšil počet případů pshishingu použitého tímto způsobem.

Phishing užitý tímto způsobem se nazývá „Angler phishing“. (Cunnane & Corcoran, 2018)

## 3.4 Generace Z a její soukromí

Generace Z je poslední známé zařazení generace. Jedná se o lidi narozené v devadesátých letech, kteří vyrůstali a dospívali po roce 2000 v přerodu a technologickém posunu společnosti.

Hlavní aspekty této generace, podle kterých je jasně odlišitelná od jiných generací se dají rozvrhnout do několika bodů.

Technologický posun za posledních 40 let byl markantní a měl velký vliv na personu člověka a s ní i vývoj jeho osobnosti. Je potřeba se adaptovat na chod světa, pokud chceme být jeho součástí. Generace Y byla u přelomu těchto změn a stále se adaptuje. Generace Z se narodila do této nové éry a nic jiného nepoznala, proto její jedinci preferují komunikaci skrze sociální média. Ať už se jedná o přímé konverzace, či podprahové konverzace za pomocí různých obrazových podnětů.

Pro tuto generaci je klíčové navazování sociálních interakcí, ale většinou se jedná o interakce s jednici spojené společným zájmem. Důsledkem pohybu v online světě mají přehled o globálním dění, ale nemají potřebu být aktivní, co se týče fyzického pohybu. (Tulgan, 2013)

Tyto aspekty vedou k samotné problematice této práce. S pohybem generace Z v digitálním světě by se mohlo zdát, že by jedinci této generace měli být obeznámení s nebezpečím, které se zde nachází, ale problém s postupem času a nástupem technologií na scénu se vyskytuje na internetu mnohem více uživatelů s věkem nevhodným k užívání této možnosti a privilegií s ní spjatými.

Ve většině případů se jedná o děti z rodin, kde rodiče značně zhýčkal technologický pokrok a využívají ho chybně při výchově dítěte.

Bc. Hana Havlíčková ve své diplomové práci formou otevřeného kódování zpovídá rodiče dětí předškolních let ohledně užívání technologií. Zpovídané maminky mají výhrady vůči technologiím, přesto jejich dětí vlastní a užívají jisté zařízení, které umožnují dětem přístup k internetu. Dítě dostalo tablet ke svým čtvrtým narozeninám. Dotazované maminky potvrzují, že vyhověli žádostem dětí o různá technologické zařízení, ale postupem času si začaly klást otázky, zda to pro jejich děti není škodlivé.

Mají dojem, že kombinace videoher a přístup k sociálním médiím jako je například YouTube, kde se dají nalézt videozáznamy různých aktivit a typu lidí, by je mohla poznamenat a přimět udělat věcí, kterých by pak litovali, ale vzhledem k jejich věku si to ještě neuvědomují. (Havlíčková, 2017)

Bohužel jsou zde i případy, kdy rodiče výchovu dětí přenechávají technologiím s přístupem k internetu bez obav, co dítě dělá, kde se v digitálním světě

pohybuje, nebo v extrémních případech jaké údaje svěřuje neznámým jedincům, se kterými na internetu interagují.

Tito jedinci mentálního stavu dítěte bez sebeuvědomění mohou být snadným tečem útočníků. Proto pro vstup a založení si svého profilu bylo stanoveno věkové omezení 13 let. Po dovršení třináctého roku života je předpokládáno, že má jedinec dostatečně vyvinutou osobnost a oplývá dostatkem zkušeností, aby mohl racionálně přemýšlet a „bezpečně“ používat tyto platformy.

## 3.5 Možnosti ochrany ze strany sociálních sítí

Pokud si chce uživatel vytvořit svůj účet a stát se členem komunity na sociální síti, musí odsouhlasit pravidla o Souhlasu pracování osobních údajů. Dle informací Evropské unie se proti tomuto souhlasu mohou odvolat a vznést námitku proti zpracování osobních údajů načež musí společnost neprodleně přestat užívat vaše data. Avšak záleží na situaci a na účelu zpracovávání vašich dat.

V některých oprávněných případech může být právo užívání vašich dat povoleno, a to, pokud společnost zpracovává data ve veřejném zájmu.

Zvláštní případ, který se týká dětí uvádí, že pro vstup na sociální sítě, stahování muziky, nebo her potřebují souhlas rodičů či zákonných zástupců, jelikož se v těchto případech jedná a zpracování osobních údajů dítěte. Potřeba souhlasu zákonných zástupců pomine v momentě, kdy jedinec dovrší 16 let. V některých zemích EU je tento limit nastaven dokonce na již zmiňovaných 13 let. Při tomto opatření jsou povinné zavedené kontroly pro ověření souhlasu rodičů, které mohou být zaslány například formou emailu. (Materiály poskytnuté Evropskou unií – Ochrana údajů a soukromí na internetu, 2020)

Je zde nutno také zahrnout faktor vstupu dětí na sociální sítě bez vědomí rodičů či rodiny, u kterých rodiče dítěte nedbají na základní prevence používání sociálních sítí ze strany mladistvých, nebo postrádají zájem své děti těmito kroky chránit.

Sociální sítě se postupem času snaží vylepšovat a rozšiřovat počet funkcí, které mají sloužit k ochraně osobních dat. Jednou z nejzásadnějších ochranou funkcí je tzv. Dvoufázové ověřování. Jedná se o dodatečnou funkci, která po zadání hesla vyžaduje potvrzení ze strany uživatele, který se na účet chce přihlásit formou kódu,

který mu je zaslán buď na emailovou adresu, nebo prostřednictvím SMS zprávy, nebo v nejvyšší formě ochrany požádá o zodpovězení bezpečnostních otázek. (Materiály poskytnuté Evropskou unií – Ochrana údajů a soukromí na internetu, 2020)

Jedná se jednoduché dodatečné ověření identity žadatele o přístup k profilu, které využívá jiný portál k poskytnutí potřebných dodatečných informací k úspěšnému přihlášení. Toto zabezpečení zamezí přístup útočníkovi k vašemu účtu i v případě, že prolomí vaši ochranu ve formě hesla. (Stanislav, 2015)

Sociální sítě dnes poskytují širokou škálu možností upravení sdílení vašeho obsahu a aktivit provedených na těchto platformách. Rozhodně není doporučeno provádět m-platby přímo na území sociálních sítí. Tyto platby je vždy doporučeno provádět přes externí bezpečné portály, které mají validní certifikát, nebo přes věrohodné portály, které poskytují ochranu při zadávání platebních údajů.

Dnešní opatření pro správu účtů poskytují i možnost zaslání emailu v případě pokusu o přihlášení, nebo pokusu o provedení změn některých aspektů účtu. (Materiály poskytnuté Evropskou unií – Ochrana údajů a soukromí na internetu, 2020)

## 3.6 Kyberšikana

S růstem uživatelů internetu a sociálních médií a snižováním věkové hranice uživatelů těchto platforem se objevuje nový problém.

Kyberšikana je forma poškozování jména, identity a zájmů osoby v digitálním prostředí, které se může přenést i do prostředí mimo online svět.

Kyberšikana má mnoho forem. Některé způsoby jsou legální a nedá se proti nim právně zasáhnout bez případných důkazů a ilegální formy kyberšikany.

Příklad může být nahrání obsahu vytvořeného jedincem bez jeho svolení. Například jednoduché „vtipné“ video, které jedinec natočí pro své přátele, kteří ho nahrají na server, kde ho může zhlédnout kdokoliv bez omezení v jednom konkrétním případě se takovéto video stalo hitem, překonalo 76 milionů zhlédnutí a i přesto, že přišlo lidem po celém světě vtipné, následky pro člověka na videu byly fatální. Musel změnit školu a potřeboval psychiatrickou pomoc.

Nebo se může jednat o vědomé písemné konverzace obsahující nadávky či hrozby vztahované k šikanované osobě. Další případ zaznamenal tuto formu šikany, kdy byli 2 studenti vyloučeni za zveřejňování příspěvků s mnoha dívkami

s komentáři, ve kterých zmiňují myšlenky na vraždu dívek utopením kvůli jejich vzhledu, což mělo na dotyčné značné následky. (Kowalski, Limber, Agatston 2009)

Forem kyberšikany je mnoho a je těžké pro dotyčného se bránit. To samé platí o zastavení útočníka, jelikož ne pokaždé se nachází fyzicky v okolí oběti. Jestliže se podaří zastavit tyto činy, útočník už na své oběti zanechal razantní škody.

Nebezpečí v digitálním světě na sebe bere mnoho podob. Jeden z nejvíce znepokojujících problémů dnešní doby jsou sexuální predátoři. Sexuální predátoři využívají ještě nevyvinuté osobnosti dítěte zkušenostmi interakce s cizími jednici. Na první pohled tito sexuální predátoři vypadají jako slušní, zdraví a spořádaní lidé a díky jejich vzhledu dokáží oklamat lidi, kteří jim věří.

Například Paul Bernardo a jeho žena Karla Homolka jsou pamatováni jako agresivní sexuální násilníci. Pro své okolí vypadali naprosto normálně. Rodina sdělila, že od svatby měli pocit, že je to dokonalý pár jako z pohádky. Přesto jejich činy jsou zaznamenané jako jedny z nejhorších v kanadské historii. (Ramsland, McGrain 2009)

Barbora Chalupová a Vít Klusák se letos rozhodli uskutečnit ambiciózní projekt. Provést průzkum na téma sexuálních predátorů s praktickými metodami a na základě výsledků tohoto průzkumu vytvořit film, který odhalí tuto problematiku veřejnosti.

Průzkum spočíval v najmutí 3 dospělých hereček, které měly v prostorách studia přestavěného do objektu 3 pokojů oddělených pouze stěnou, ve kterých mají nalíčené a přestrojené herečky hrát dospívající dívky ve věku 12 let za pomocí falešných předem vytvořených profilů a pokusit se zachytit v jakém prostředí se dítě může nacházet, s jakými jedinci se na těchto sociálních sítích mohou setkat, jaké situace mohou nastat a jaké požadavky mají tito sexuální predátoři na nezletilé dívky.

Tento radikální experiment za 10 dní jen za pomoci 3 hereček objevil 2458 potenciálních sexuálních predátorů, kteří v extrémních případech požadovali schůzku s dívkami na obrazovce či sex přes webkameru, zasílali fotografie choulostivých míst, odkazy na pornografické snímky. (Chalupová, Klusák 2020)

## 3.7 Softwary sloužící k zabezpečení dat

Pro zajištění bezpečí na internetu a všech jeho částech existují metody, nástroje a prostředky, které umožnují předcházet nedovoleným operacím s vašimi daty.

### 3.7.1 Antivirové programy

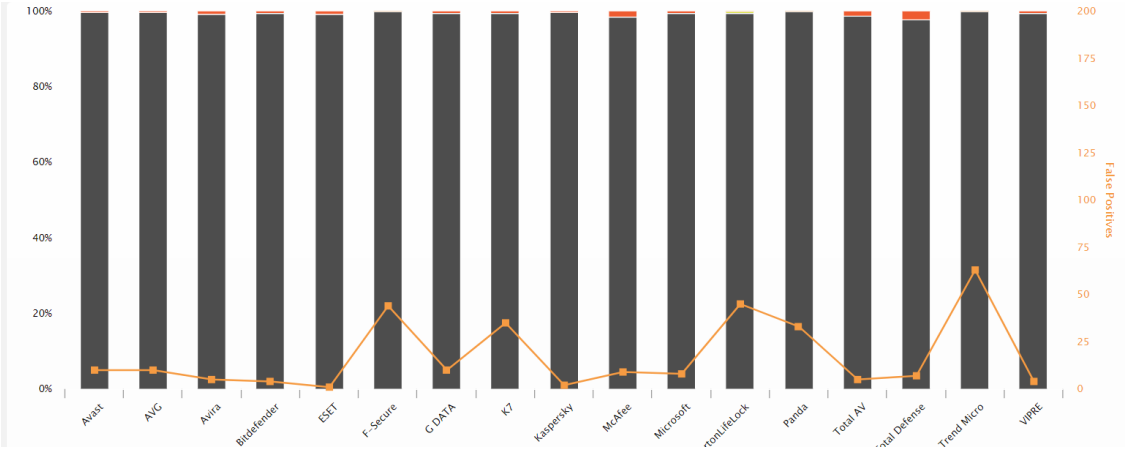
První z těchto nástrojů jsou tzv. antivirové programy. Programy, které chrání vaše zařízení proti útokům ze strany jedinců, kteří se snaží získat a využít data k dalším účelům pro tyto osoby profitující.

Tyto programy kontrolují data směřující z vnější sítě do vašeho zařízení pomocí stahování souborů různých formátů. Pomocí databáze škodlivých programů, mezi které patří viry, červi, malwary a mnoho dalších různých nástrojů pro vniknutí do zařízení a provádění nejrůznějších operací s obsaženými daty.

Funkce antivirového programu je ve zkratce kontrola příchozích dat a přítomnosti metadat, nebo vedlejších funkcí programu, které obsahují právě tyto malwary. (Johansen, 2019)

Webová stránka AV comparatives vytvořila graf nejspolehlivějších antivirových programů.

**Obrázek 3: Porovnání antivirových programů**




Zdroj: (AV-Comparatives, 2020)

Podle průzkumu jsou na tom nejlépe antivirové programy ESET, Kapersky, F-Secure a Bitdefenders. Toto pořadí se určuje pomocí osy znázorňující tzv. „False Positives“, které znázorňují soubory, které byly chybně označené jako škodlivé a

červený díl na jednotlivých sloupcích pro dané antiviry, který s černou částí sloupců znázorňuje procentuální poměr případů, kde byl malware detekován a eliminován černou částí. V červené části jde o případy, kde malware úspěšně pronikl do systému.

### 3.7.2 VPN nástroje

VPN nástroje pomáhají chránit uživatele při pohybu na internetu. Jednoduše řečeno vytvoří pomyslný tunel spojující uživatelovu lokální síť a koncový bod přenosu dat vzdálený s přehledem tisíc mil daleko. Tímto vytvoří iluzi toho, že se uživatel nachází na daném koncovém bodě.

Slouží též jako pomocný nástroj, který chrání zařízení připojené na veřejnou síť, kde hrozí, že přenos dat by mohl být kompromitován útočníkem nacházejícím se na stejné síti.

Může též sloužit pro skrytí informací jako je například historie vyhledávání, lokace zařízení, aktivitu uživatelé na internetu a přítomnost zařízení v sítí. (Symanovich, 2020)

# 4 Vlastní práce

## 4.1 Téma

Cílem vlastní práce je převést poznatky získané literární rešerší v teoretické části k vyhodnocení možných nástrah a nebezpečí, které čekají na uživatele nejen na sociálních sítích, ale na internetu jako takovém. Souhrn všech výše uvedených poznatků naznačuje, že v dnešní době hrozí uživateli při interakci s daty na internetu značná rizika, která mohou ovlivnit jeho činnost, kterou se snaží na internetu vykonávat, či dokonce ohrozit uživatele neautorizovanou úpravou, odcizením, či poškozením dat, se kterými uživatel pracuje, nebo zbytku dat, který není příslušně zabezpečen.

S technologickým pokrokem se ale nezdokonalují jen hrozby. Zdokonalují se také programy a techniky, které mají za úkol se těmto hrozbám kompletně vyhnout. Pokud se napadení zařízení koncového uživatele a poskytovatele dat pro stranu útočníka již nedá zabránit, mají tyto programy a techniky za úkol buď kompletně zabránit jakýmkoliv škodám, nebo v situacích, kdy je zařízení již kompromitováno, se pokusit zredukovat škody vzniklé kybernetickým útokem, a to co nejrychleji a nejefektivněji.

Dnešní technologie přináší široký sortiment a snaží se zabezpečit uživatele před mnoha způsoby napadení. Existuje velké množství společností, které poskytují ochranu svým klientům skrze software, jež se snaží udržet v aktuálním stavu a držet krok s neustálým pokrokem v oblasti technologie. Rozvíjí se nejen software pro ochranu ale také softwary užívané pachateli kybernetických útoků.

Sociální sítě využívá každý uživatel za jiným účelem, ale základní myšlenkou je spojování lidí na digitálních platformách a utváření komunit s podobným smýšlením a zájmy. Sociální sítě jako každé jiné služby poskytované na internetu, nespadají do plně zabezpečených oblastí. I když je v dnešní době antivirový program prakticky nutnost při každé zařízení pro řešení některých situacích kybernetického

útoku, lze nepříjemným zážitkům předejít za pomoci možností poskytnutých přímo ze strany sociálních sítí.

Sociální sítě se na technický pokrok snaží reagovat a neustále zajišťovat svým klientům bezpečné užívání jejich služeb. Ať už jasným stanovením pravidel a zásad, které předloží každému uživateli při zakládání účtu, tak neustálým informováním o jejich změnách pomocí zpráv při každé aktualizaci.

Jedním z nejzákladnějších faktorů, který může předejít nepříjemným zážitkům, nebo v horších případech napadení účtu, je selský rozum.

Pokud si je uživatel vědom hrozeb, jež na něho v online světě číhají a ví, že má odpovědnost za své činy, může svým jednáním předejít jakýmkoliv větším potížím.

## 4.2 Dotazníkové šetření ohledně uvědomělosti a schopnosti ochrany soukromí dotazovaných

K interpretaci výše zmíněných informací týkajících se hrozeb a pomůcek sloužících k ochraně v praxi a obeznámením čtenáře ohledně této problematiky, bylo provedeno dotazníkové šetření, jež mělo za úkol zaznamenat za pomoci položených otázek obecný přehled širší společnosti ohledně této problematiky. Dále zkušenosti, které zúčastněné potkaly a popřípadě přehled o tom jaké protiopatření používají. Na základě tohoto šetření byl v praktické části proveden kvantitativní výzkum a pomocí statistických metod zpracována data za účelem vytvoření ideální strategie pro běžného uživatele s přihlédnutím na finanční náročnost.

Použitý anonymní dotazník se skládal z 25 otázek. Otázky v dotazníku se soustředily na témata, která byla v teoretické části práce předložena. Šetření mělo i mimo jiné za úkol zjistit, jak se k této problematice staví různé věkové kategorie. Dotazník byl určen pro osoby starší 15 let (středoškoláci). Horní věková hranice stanovena nebyla. Omezení spodní věkové hranice bylo provedeno za účelem sběru dat od uživatelů sociálních sítí, kteří mají vyvinutou osobnost na takové úrovni, kdy plně chápou následky svých činů. Jsou si také vědomi nebezpečí, které používání sociálních sítí přináší. Dále je tato věková skupina první, jež má dle zákona možnost služeb sociálních sítí využívat bez rodičovské kontroly. Další rozdělení respondentů

si ukládalo za povinnost roztřídit pracující, studenty a jednice, kteří nespadají do těchto dvou kategorií. Toto rozdělení bylo provedeno z finančního hlediska.

Dalším smyslem šetření bylo zjistit za jakým účelem respondenti sociální sítě využívají a kolik času u nich denně stráví. Zda jsou si vědomi případných rizik spojených s jejich užíváním. Jestli využívají nějakých ochranných prostředků ve formě softwarů sloužících k těmto účelům a popřípadě jaké konkrétní softwary pro ochranu svého zařízení využívají.

Následně byly respondentům položeny otázky, které analyzovaly jejich přístup k podezřelým odkazům a účtům. Další otázky zkoumaly, jakým způsobem si dotazovaní chrání své soukromí. Zda si do kruhu přátel přidávají i jednice, jež osobně neznají, nebo zda nezveřejňují informace, které by mohly přinést komplikace ve formě útoku na jejich osobu data či majetek, a to jak digitální tak fyzický.

Šetření také zkoumalo míru zapojení rodičů v procesu ochrany svých dětí před potenciálními riziky, to nejen ve formě edukace svých ratolestí ohledně pravidel chování, ale také zabezpečení lokálního zařízení vhodným softwarem. Nemalou roli v zabezpečení účtu mladistvých také hraje rodičovská kontrola. Jedna z otázek šetření zkoumala, zda rodiče využívají této možnosti, která přidává další vrstvu ochrany a může předejít mnoha problémům.

## 4.3 Rozbor a analýza otázek dotazníkového šetření

Na dotazník celkem odpovědělo 204 osob.

Šetření se skládalo ze 2 otevřených otázek a 23 otázek uzavřených. Respondentům byly pokládány otázky s odpověďmi ve formě ano či ne nebo ve formě konkrétních odpovědí. Odpověď na jednu z (Tabulka 5: Dotazníkové šetření: Otázka č.20) byla sestavena formou Likertovy škály.

Níže jsou vybrány a analyzovány dvě rozdělovací otázky a čtyři důležité otázky úzce související s tématem.

Otázka č.2: Jaká je vaše věková skupina?

Druhá otázka měla za úkol zjistit, v jaké věkové kategorii se dotazovaní nacházejí. Z důvodů uvedených v úvodu praktické části jsou věkové skupiny rozvrženy do tříd. Cíl byl zaujmout všechny možné věkové kategorie. Nejmladší věkovou skupinu tvoří respondenti ve věku 15 až 19 let (středoškoláci). Právě

v tomto věku začínají jedinci dostávat kapesné a hledat brigády za účelem výdělku. Také je to první věková skupina, která dle norem Evropské unie může užívat služeb sociálních sítí bez rodičovské kontroly.

Z následující tabulky lze zřetelně vyčíst nadpoloviční většina dotazovaných je ve věkové skupině mezi 20 a 25 let (přesně 51,5%).

**Tabulka 1: Dotazníkové šetření: Otázka č.2**

| Možnosti | Odpovědi | Procentuální vyjádření |
|---|---|---|
| 20 - 25 | 105 | 51,5 % |
| 15 - 19 | 42 | 20,6 % |
| 26 - 40 | 33 | 16,2 % |
| 40 - 60 | 23 | 11,3 % |
| 60 + | 1 | 0,5 % |

Zdroj: Autor

Otázka č.3: Jste pracující, student, či jiné?

Účelem třetí otázky bylo roztřídit dotazované podle společenského statutu. Pracující člověk oplývá větším finančním obnosem než student či člověk, jež je nezaměstnaný. Tato otázka je potřebná pro určení finanční náročnosti cílové strategie.

Dle následující tabulky můžeme vidět, že nadpoloviční většina dotazovaných (61,8 %) jsou studenti. Je proto nutné přihlédnout k jejich finanční situaci.

**Tabulka 2: Dotazníkové šetření: Otázka č.3**

| Možnosti | Odpovědi | Procentuální vyjádření |
|---|---|---|
| Student | 126 | 61,8 % |
| Pracující | 65 | 31,9 % |
| Jiné | 13 | 6,4 % |

Zdroj: Autor

Otázka č.7: Máte, nebo měli jste špatné zkušenosti s využíváním služeb sociálních sítí?

Z následující tabulky je zřetelné, že necelá třetina dotazovaných (30,9 %) měla špatné zkušenosti při užívání služeb sociálních sítí. Přestože se většinou jedná o ne příliš závažné problémy, dokáží znepříjemnit život. Ať už na krátkodobé, či dlouhodobé bázi.

**Tabulka 3: Dotazníkové šetření: Otázka č.7**

| Možnosti | Odpovědi | Procentuální vyjádření |
|---|---|---|
| NE | 141 | 69,1 % |
| ANO | 63 | 30,9 % |

Zdroj: Autor

Otázka č.17: Čtete pozorně smluvní/licenční podmínky a updaty týkajících se ochrany, či pravidel?

Úkolem otázky bylo zjistit, zda dotazovaní čtou smluvní/licenční podmínky, které se týkají sociálních sítí, jejich pravidel a možných postupech ochrany uživatelů.

Překvapivě 76,5 % dotazovaných zvolilo odpověď „NE“. Existuje zde možná souvislost s otázkou číslo sedm, jelikož 49 z 59 dotazovaných, kteří v otázce sedm odpověděli, že za svůj pohyb na sociálních sítích nabyli špatných zkušeností různých forem, odpověděli, že právě tyto dokumenty pozorně nečtou.

**Tabulka 4: Dotazníkové šetření: Otázka č.17**

| Možnosti | Odpovědi | Procentuální vyjádření |
|---|---|---|
| NE | 156 | 76,5 % |
| ANO | 48 | 23,5 % |

Zdroj: Autor

Otázka č.20: Myslíte se, že je vaše momentální zabezpečení na internetu dostačující?

Tato otázka a její formulace měla za úkol přivodit možné sebeuvědomění na straně dotazovaných.

Z výsledků je zřejmé, že 25,4 % si nemyslí, že by byli dostatečně chráněni. Dalších 47,5 % si myslí, že jejich zabezpečení je dostačující a zbylých 22,5 % neví, jak na tom jejich zabezpečení na sociálních sítích je.

**Tabulka 5: Dotazníkové šetření: Otázka č.20**

| Možnosti | Odpovědi | Procentuální vyjádření |
|---|---|---|
| Spíše ano | 72 | 35,3 % |
| Spíše ne | 53 | 26 % |
| Nevím | 46 | 22,5 % |
| Určitě ano | 27 | 13,2 % |
| Určitě ne | 6 | 2,9 % |

Zdroj: Autor

Otázka č.24: Jaký je hlavní faktor, podle kterého vybíráte vhodný software pro ochranu dat a soukromí? (antivirový program, VPN atd....). Pokud jste pro své zařízení nevybírali takovéto softwary, odpovídat nemusíte.

Tato otázka sloužila jako jeden z hlavních základních kamenů pro sestavení cílové strategie pro ochranu uživatelů.

Pro dotazované je nejdůležitější faktor efektivnost (54,5 %). Cena se zdá být také znatelným faktorem pro rozhodování (32,5 %). Tyto 2 faktory budou hrát největší roli ve výsledném výběru zvoleného softwaru.

**Tabulka 6: Dotazníkové šetření: Otázka č.24**

| Možnosti | Odpovědi | Procentuální vyjádření |
|---|---|---|
| Efektivnost | 84 | 54,5 % |
| Cena | 50 | 32,5 % |
| Rychlost | 14 | 9,1 % |
| Jiné | 6 | 3,9 % |

Zdroj: Autor

Dotazníkové šetření vykazuje, že respondenti využívají sociální sítě za účely navázání kontaktu se známými a k zabavení se ve volném čase.

Dotazovaní, kteří zažili špatné zkušenosti (Tabulka 3: Dotazníkové šetření: Otázka č.7) odpověděli, že se jednalo o spam, zveřejňování obsahu zachycující postiženou osobu bez jejich svolení, napadení zařízení formou viru s vysokou variabilitou způsobů nebo ve formě sexuálního obtěžování.

Respondenti uvedli, že si do přátel nepřidávají lidi, které neznají a že o sobě zbytečně příliš nešíří informace, jež by mohly mít vliv na jejich zabezpečení. Dále se neúčastní podezřelých aktivit (například ve formě soutěží) a vyhýbají se podezřelým odkazům.

Nejpoužívanějšími operačními systémy mezi respondenty jsou Microsoft Windows od firmy Microsoft a MacOS od firmy Apple a nejrozšířenějším antivirovým programem je Avast.

Byly položeny také otázky rodičům ohledně ochrany jejich dětí v souvislosti s probíranou problematikou. Otázky zjišťovaly, zda zabezpečují zařízení svých dětí. Zda vzdělávají své děti ohledně rizik hrozících a možných způsobů omezení těchto rizik a zda uživatelské účty jejich dětí mají rodičovskou kontrolu pro jednodušší sledování podezřelých aktivit.

## 4.4 Míra zanedbání ochrany osobních dat

Pro tuto část byly stanovena kritéria pro hodnocení míry zanedbalosti ochrany osobních údajů dle určitých aspektů. Rozdělení do kategorií dle kritérií je prováděno na základě odpovědí respondentů dotazníkového šetření a relativní četnosti odpovědí naznačující jisté zanedbání ochrany vyplívajících z jejich aktivit.

Kritéria jsou následující:

- Pod 10 % - Nezanedbání
- Nad 10 % a pod 30 % - Mírné zanedbání
- Nad 30 % a pod 50 % - Znatelné zanedbání
- Nad 50 % a pod 80 % - Alarmující zanedbání
- Nad 80 % - Kritické zanedbání

První aspekt, který ovlivní užívání sociálních sítí a zabezpečení osobních dat je souhlas se smluvními podmínkami a zájem o zprávy týkajících se ochrany dat uživatelů. Přesně 76,5 % respondentů pozorně nečte licenční podmínky (Tabulka 4: Dotazníkové šetření: Otázka č.17), což je dle daných kritérií alarmující zanedbání ochrany osobních dat ze strany respondentů.

Dalším aspektem je využívání alespoň základního softwaru pro ochranu zařízení. Respondenti byli tázáni, zda a jakého antivirový program využívají. Přesně

24,5 % dotazovaných nevyužívá služby žádného antivirového programu, což je dle kritérií mírné zanedbání.

Dále je nutno uvést, že 37,7 % respondentů zveřejňuje na sociálních sítích informace, které mohou ovlivnit zabezpečení nejen jejich dat, ale také majetku. Dle stanovených kritérií tento aspekt spadá do kategorie znatelného zanedbání.

Kontrola totožnosti jedince, kterého si na sociálních sítích přidáváme do kruhu svých přátel, a ověřování, zda ho opravdu známe, je aspekt, jež se z počátku jeví jako nepatrný, ale v budoucnu s sebou může přinést velmi nepříjemné situace. Například napadení ve formě sexuálního obtěžování. Dle šetření 27,9 % dotazovaných si do tohoto kruhu přává lidi, které nezná osobně, což je mírné zanedbání ochrany osobních dat.

Menší skupinou respondentů (24 %) byli rodiče, kteří byli tázáni, zda se snaží zabezpečit zařízení, které používají jejich děti. Z této skupiny je 32,65 % rodičů, jejichž děti nemají zabezpečená zařízení vhodným softwarem, což spadá do kategorie znatelné zanedbání. Další otázka pro rodiče měla za úkol zjistit, kolik se jich se snaží vzdělávat své děti ohledně problematiky sociálních sítí, zabezpečení dat a případných rizik. Odpověď „Ne“ zvolila 21,28 % rodičů, což je dle kritérií mírné zanedbání. Poslední otázka pro rodiče se týkala rodičovské kontroly, která pomáhá sledovat aktivity dětí na sociálních sítích a zlepšit tak zabezpečení soukromí, osobních dat a využívání účtů svých dětí. Rodičů, kteří této možnosti nevyužívají bylo 58,18 %, což je dle kritérií alarmující zanedbání ochrany osobních dat.

## 4.5 Porovnání ekonomické náročnosti ochrany dat dostupné na trhu

Po analýze mnohých žebříčků a recenzí byla vytvořena tabulka nejvhodnějších antivirových programů.

Funkce těchto ochranných softwarů jsou například Ransomware štít, správce a trezor pro hesla, zabezpečení firewallu a nastavení routeru, šifrování dat a komunikace na internetu (ochrana před phisingem) či sken podezřelých souborů.

**Tabulka 7: Porovnání antivirových programů**

| Název | Typ | Cena za rok | Výhody | Nevýhody |
|---|---|---|---|---|
| Bitdefender Antivirus | Total Security | 1959 Kč | Velká ochrana pro finanční pohyby a transakce online. V ceně až 5 zařízení. | Problémy s čištěním ransomwaru (poddruh malwaru). |
| Norton Antivirus | Norton Antivirus Plus | 1 099 Kč | Velké množství funkcí. Užitečné balíčky pro obnovu dat. | Velké nároky na výkon. |
| Kapersky Anti-Virus | Kapersky Anti-Virus Internet security | 1488 Kč | Rychlost a možnost úpravy. Vysoce účinný proti malwarům. | Malé množství funkcí. |
| ESET | ESET Smart Security Premium | 1 890 Kč | Velký počet funkcí a jejich nastavení. Vysoká spolehlivost. | Cena. Uvedená cena je na rok pro 1 zařízení. Většina zde dostupných antivirů nabízí služby až pro 3 zařízení. |
| Avast | Avast Premium Security | 1524 Kč | Podpora mnoha operačních systémů. Velký počet funkcí. | Cena. Opět je uvedena cena jen pro jedno zařízení. |

Zdroj: Autor

Služba VPN může také přidat jistou vrstvu ochrany. Nevýhodou je ovšem finanční náročnost.

Příkladem mohou být VPN služby od firmy NordVPN. Jde o nejrozšířenější VPN služby na trhu s funkcemi jako šifrování dat, dostupnost dat poskytované jen

pro určité regiony, nebo skrytí IP adresy. Se zárukou udržení soukromí ze strany poskytovatele služby.

Tato forma je pro běžného uživatele formou zvýšení ochrany, jež by neměla být na prvním místě. Cenová dostupnost této služby za rok činí 3008 Kč s možností garance vrácení peněz do 30 dnů.

Alternativa, kterou dotazovaní také volili byla ExpressVPN. S podobnými funkcemi jako NordVPN s menším rozsahem regionů s cenovou dostupností služeb na rok za 2179 Kč.

# 5 Výsledky a diskuse

## 5.1 Cílová strategie

Dotazníkové šetření bylo navrženo pro co nejširší možný rozsah společnosti. Věkové kategorie byly rozděleny do této formy, aby se mohla zjistit možná souvislost s věkem a využíváním ochrany svých dat. Šetření poukázalo, že spíše dotazovaní mladší 25 let nevyužívají ochranného softwaru v podobě antivirových programů, které jsou v dnešní době nutností pro bezpečné používání zařízení připojených k internetu.

Nabízí se tu možnost, že mnoho lidí v tomto věku jsou studenti s omezeným rozpočtem a cena za služby těchto softwarů je vysoká. Proto je třeba při výběru softwaru zohlednit i cenovou dostupnost, jelikož jde o druhý nejčastější faktor, který ovlivňuje výběr softwarů u respondentů. První místo drží efektivnost (Tabulka 6: Dotazníkové šetření: Otázka č.24).

Strategie bude rozdělena do několika sekcí dle finanční náročnosti.

### 5.1.1 Možnosti ochrany dostupné zadarmo

Po analýze dat bylo zřejmé, že část z dotazovaných, kteří zažili špatné zkušenosti při užívání sociálních sítí se účastní různých soutěží, u kterých se naskýtá možnost kybernetického útoku v mnoha formách.

Dále 76,5 % dotazovaných odpovědělo, že nečte smluvní podmínky (Tabulka 4: Dotazníkové šetření: Otázka č.17) či zprávy o updatech ochrany dat ze strany sociálních sítí, což značně snižuje efektivnost funkčnosti této platformy pro uživatele.

Nejmladší věková kategorie dotazovaných se v některých zemích Evropské unie stále počítá mezi jedince (do 16 let), kteří by neměli vlastnit svůj účet na sociálních sítích bez kontroly rodičů. Tu je nutné ze strany sociálních sítí poskytnout všem, kteří o ní požádají. Souvisí s ní i informování o pohybu mladistvých na sociálních sítích formou emailu, nebo SMS zprávy.

Jedním ze základů dobrého zabezpečení účtu je silné heslo, které se nedá prolomit různými generátory základních hesel a kombinací. Proto by uživatel měl ke svému přístupu využívat silné heslo kombinující písmena a číslice. Heslo by nemělo souviset s dohledatelnými údaji o uživateli.

Dle analýzy výsledků odpovědí vyšlo najevo, že 90 % z dotazovaných, kteří měli zkušenost se sexuálním obtěžováním, byly studentky ve věku 15 až 25 let. Většina sociálních sítí má možnost blokování uživatele. Tato funkce může zastavit příchozí zprávy od konkrétního účtu, či dokonce zamezit, aby daný uživatel neměl přístup k žádnému odkazu, který je námi zveřejňován.

Selský rozum nic nestojí a je také dobré si rozmyslet, zda je vhodné nahrát daná data na sociální sítě předtím, než tak uživatel účinní. Uživatel by s měl zamyslet, zda data nemůže nikdo zneužít ve svůj prospěch, či dostat se k jiným citlivým údajům, které může odcizit. Je proto je doporučeno nesdílet obsah s nikým, komu kompletně nedůvěřujeme. Nejedná se jen o případy sexuálního obtěžování po sdílení citlivých fotografií. Tato situace se týká například příspěvků, který obsahuje vaši nynější adresu, či lokaci.

Tyto informace se dají lehce zneužít k dalšímu případnému útoku, a to jak kybernetickému tak i v reálném životě. Může to být například situace, kdy jedinec sdílí, že se chystá na dovolenou. Takové informace není vhodné sdílet se širšími kruhy v listu přátel na sociálních sítích. V některých situacích postižení sdíleli dobu trávenou mimo domov a dali tak útočníkům konkrétní čas, ve kterém vykrást dům.

Různé typy sociálních sítí nabízí různý typ tvorby obsahu, ale stále by uživatel neměl tvořit a sdílet obsah, kterého by v budoucnu litoval.

Dále má uživatel možnost zálohovat data na externí uložiště, pokud je dostupné, či využívat funkce operačního systému pro šifrování disku a možnost dvoufázového ověřování, kterou poskytují samy sociální sítě.

Tyto způsoby ochrany se mohou zdát jako triviální záležitost, ale jejich dodržování může značně omezit kybernetické útoky a zneužití dat jedince.

### 5.1.2 Doporučené možnosti ochrany s placenou licencí

Ochranný software je v dnešní době nutnost. Pokud je zařízení připojené k internetu, může se stát cílem útoků. Antivirový program je jednou součástí těchto ochranných softwarů. Je základem ochrany zařízení.

Dotazníkové šetření poukázalo, že hlavní faktor pro respondenty, který ovlivňuje výběr ochranného softwaru je efektivnost a druhým nejčastěji voleným faktorem je cena.

Nejpoužívanějším antivirovým programem u respondentů je Avast. Tento ochranný software je cenově dostupný většině dotazovaným. Dle tabulky srovnání (Tabulka 7: Porovnání antivirových programů) těchto programů je cenově přijatelnější jen antivirový program Norton Antivirus Plus, který ale má velké nároky na výkon zařízení, tím pádem by mohl být spíše zátěží pro uživatele se zařízením s nižší hardwarovou výbavou.

Doporučené antivirové programy na základě výsledků dotazníkového šetření jsou ESET Smart Security Premium, který je, co se týče efektivnosti nevhodnějším kandidátem pro ochranu zařízení. Cena za licenci na rok užívání tohoto softwaru činí 1890 Kč pro jedno zařízení. Co se týče finanční stránky, je tento software celkem náročný. Na druhou stranu, z technické části je velice spolehlivý a má implementovaných mnoho nástrojů, jež mohou automaticky zachytit a zneškodnit většinu hrozeb bez nutnosti pozornosti uživatele.

Alternativou je dle šetření nejpoužívanější antivirový program Avast. Ten nabízí mnoho možností a stupňů ochrany. Prvním stupněm je Avast Free Antivirus, který nabízí funkce blokování virů a malwarů a také ochranu proti ransomwaru. Tato forma je zcela zdarma, ale oplývá pouze limitovanými prostředky k ochraně dat.

Dalším stupněm je Avast Premium Security, který nabízí stejné funkce jako Avast Free Antivirus, ale přidává k nim ještě funkce jako ověřování bezpečnosti Wi-Fi připojení, varování před podezřelými a nebezpečnými webovými stránkami, ochrana před phishing stránkami a možnost vzdáleného zamezení útoku na zařízení. Tyto první dva stupně ochrany vyjdou uživatele na 1524 Kč na rok a je určen nejen pro operační systémy Microsoft Windows a MacOS, ale také pro Android IOS.

Poslední a nejvýše poskytovaný stupeň ochrany je Avast Ultimate. Ten mimo funkce předchozích dvou nabízí i funkce jako je premium čistění zařízení od nepotřebných souborů, registrů a dalšího zbytečného obsahu zabírající kapacitu uložiště, službu VPN a skrytí IP adresy při pohybu na internetu. Tento stupeň ochrany vyjde uživatele na ročních 2193 Kč.

Avast je nejen spolehlivý, ale i oblíbený v řadách respondentů, tím pádem jsou s ním už někteří lidé seznámeni a vědí, jak funguje. Proto je dle této strategie nejlepší volbou ze všech zde zmíněných. Je cenově dostupný i pro jedince s menšími příjmy, nevyžaduje lepší hardware a výkonu zařízení a nabízí mnoho funkcí, které pomohou s ochranou dat. Nejvhodnějším stupněm ochrany je Avast Premium

Security. Tento balíček obsahuje všechno potřebné k základnímu zabezpečení dat a v kombinaci s možnostmi zmíněnými v přechozí podkapitole je účinnou ochranou pro běžného uživatele sociálních sítí a internetu. Ovšem samotný software ochranu osobních dat nezajistí, a proto je doporučeno využívat možností zmíněných v první sekci (5.1.1 Možnosti ochrany dostupné zadarmo).

### 5.1.3 Dodatečné možnosti ochrany s větší finanční náročností

Tato metody ochrany zahrnuje především služby VPN. Službu poskytuje například Avast ve svém balíčku pro absolutní ochranu Avast Ultimate. Nebo se uživatel může odkázat na společnost, která se zaměřuje především na tyto služby. Nejlepšími kandidáty jsou NordVPN, jež pro jedno zařízení na rok poskytuje služby za 2174 Kč. ExpressVPN, který služby na rok poskytuje za 3008 Kč. Uživatel může využít služeb od těchto společností v kombinaci s doporučeným antivirovým programem (např. Avast Premium Security + NordVPN s licencí na rok vyjde uživatele na 3698). Kombinace ověřených metod s nejnižší finanční náročností.

Uživatel může využít právě těchto kombinací různých antivirových programů a služeb VPN u externí společnosti nebo balíčky ochranných softwarů, kde je služba VPN v ceně, ale není tak efektivní jako od společnosti, která se věnuje jen těmto službám. Je jen na uživateli, jakou variantu si zvolí.

Tyto metody jsou nadstandartními možnostmi pro ochranu dat a běžnému uživateli, který není s VPN službami obeznámen, neposkytuje ochranu dostačující její finanční náročnosti.

# 6 Závěr

Cíl práce byl pomocí syntézy poznatků z teoretických východisek a vlastní práce navrhnout strategii pro ochranu dat, která by měla být kompromisem efektivnosti a finanční náročnosti.

Teoretická část se zabývala tématem sociálních sítí. Popsala jejich rozdělení a uvedla příklady. Dále byla provedena analýza případných rizik a hrozeb pro uživatele sociálních sítí. Dále poskytla náhled na možné prostředky sloužící k ochraně dat před různými formami kybernetických útoků.

Praktická část využívala poznatků získaných z teoretických východisek a za pomoci dotazníkového šetření získala pohled od skutečných uživatelů sociálních sítí. Dotazníkové šetření bylo určeno všem uživatelům sociálních sítí nad 15 let (Tabulka 1: Dotazníkové šetření: Otázka č.2). Po analýze získaných dat za účelem najít možnou souvislost mezi odpověďmi byla stanovena kritéria a hodnocena míra zanedbalosti ochrany osobních údajů ze strany respondentů na základě jejich odpovědí a relativní četnosti daných odpovědí. Poté byla navržena cílová strategie formou modelového řešení, která má za použití efektivních ochranných softwarů a respektování finanční náročnosti pro běžného uživatele sociálních sítí zaručit kompromisní řešení ochrany osobních dat a soukromí. Kompromis byl tvořen mezi těmito dvěma faktory, jelikož respondenti dotazníkového šetření zvolili pravě tyto parametry jako nejdůležitější faktory pro výběr ochranného softwaru pro ochranu jejich osobních dat.

Autorem navržená strategie pro ochranu dat byla rozdělena do tří sekcí dle finančních nákladů potřebných pro jejich užívání, jelikož část respondentů byli studenti (61,8 %) (Tabulka 2: Dotazníkové šetření: Otázka č.3), kteří nemusí mít stabilní příjem na pokrytí nákladů spojených s pokročilejšími možnostmi ochrany. První sekce informuje o možnostech ochrany dostupných zdarma a popisuje poskytované možnosti.

Druhá sekce se zaobírá ochranou pomocí ochranných softwarů, a to konkrétně antivirových programů. V praktické části proběhla analýza žebříčků a recenzí, ze které byly vybrány zástupci vhodní pro cílovou strategii. V kombinaci s analýzou dat získaných z dotazníkového šetření byly vybrány dva programy pro cílovou strategii. Autorem zvolený nejvhodnější antivirový program je Avast

Premium Security. Tato sekce je dle strategie autora nejvhodnější s použitím se zmíněným ochranným softwarem a možnostmi ochrany, které nabízí za předpokladu, že se uživatel snaží komplikacím vyhnout využitím metod zmíněných v první sekci.

Poslední sekce je finančně nejnáročnější, avšak poskytuje nejvyšší možnou ochranu ze všech zde zmíněných kombinací. Jedná se o kombinaci antivirového programu a služeb VPN. Pro běžného uživatele, který se ale v těchto službách neorientuje a nevyužívá naplno nabízených služeb jde o nadbytečnou vrstvu ochrany, která nemusí vyjít vstříc uživatelům s menším příjmem.

# 7 Seznam použitých zdrojů

## 7.1 Elektronické zdroje:


KHAN ACADEMY. *What are social groups and social networks?* [online]. 2017 [cit. 2020-12-10]. Dostupné z: https://www.khanacademy.org/test-prep/mcat/society-and-culture/social-structures/a/what-are-social-groups-and-social-networks

ENISA. *Online as soon as it happens* [online]. 2010 [cit. 2020-12-10]. Dostupné z: https://www.enisa.europa.eu/publications/archive/onlineasithappens

PAPIC, Milos a Rada KANARAC. *POSSIBILITIES OF USING CERTAIN SOCIAL NETWORKS IN EDUCATION* [online]. 2016 [cit. 2020-12-10]. Dostupné z: https://www.researchgate.net/publication/324829083_POSSIBILITIES_OF_USING_CERTAIN_SOCIAL_NETWORKS_IN_EDUCATION

HALL, Mark. *Facebook: American company* [online]. 2020 [cit. 2020-12-10]. Dostupné z: https://www.britannica.com/topic/Facebook

PHILLIPS, Sarah. *A brief history of Facebook* [online]. 2007 [cit. 2020-12-10]. Dostupné z: https://www.theguardian.com/technology/2007/jul/25/media.newmedia

TECHTERMS. *Facebook: Definition* [online]. 2008 [cit. 2020-12-10]. Dostupné z: https://techterms.com/definition/facebook

ENCYCLOPEDIA BRITANNICA. *Twitter: Microblogging service* [online]. 2020 [cit. 2020-12-10]. Dostupné z: https://www.britannica.com/topic/Twitter

CAMBRIDGE UNIVESITY PRESS. *Twitter definition* [online]. 2020 [cit. 2020-12-10]. Dostupné z: https://www.pewresearch.org/internet/fact-sheet/social-media/

ROUSE, Margaret. *Twitter: Definition* [online]. 2015 [cit. 2020-12-10]. Dostupné z: https://whatis.techtarget.com/definition/Twitter

TechTerms. 2010. LinkedIn. TechTerms [online]. [cit. 2021-01-22]. Dostupné z: https://techterms.com/definition/linkedin#:~:text=LinkedIn%20is%20a%20social%20networking,to%20create%20a%20custom%20profile.

PEW RESEARCH CENTER. *Social Media Fact Sheet* [online]. 2019 [cit. 2020-12-10]. Dostupné z: https://www.pewresearch.org/internet/fact-sheet/social-media/

TECHNOPEDIA.COM. *What is YouTube? - Definition* [online]. 2016 [cit. 2020-12-10]. Dostupné z: https://www.techopedia.com/definition/5219/youtube

TECHTERMS. *YouTube Definition* [online]. 2009 [cit. 2020-12-10]. Dostupné z: https://techterms.com/definition/youtube#:~:text=YouTube%20is%20a%20video%20sharing,acquired%20by%20Google%20in%202006.&text=YouTube%20videos%20are%20posted%20by,from%20all%20types%20of%20backgrounds.

NEWAUDIENCEMEDIA.COM.AU. *Brief History of Instagram* [online]. 2020 [cit. 2020-12-10]. Dostupné z: https://www.newaudiencemedia.com.au/brief-history-of-instagram/

TECHTERMS. *Instagram* [online]. 2014 [cit. 2020-12-10]. Dostupné z: https://techterms.com/definition/instagram

FORTNEY, Lucas. How Amazon's Twitch Platform Makes Money. *Dictionary.com* [online]. 2019 [cit. 2020-12-10]. Dostupné z: https://www.investopedia.com/investing/how-does-twitch-amazons-video-game-streaming-platform-make-money/#:~:text=For%20the%20baby%20boomers%20and,on%20their%20favorite%20competitive%20players.

TikTok. *Dictionary.com* [online]. 2020 [cit. 2020-12-10]. Dostupné z: https://www.dictionary.com/e/tech-science/tiktok/

INFLUENCER, MarkrtingHub. *What is TikTok?: The Fastest Growing Social Media App Uncovered* [online]. 2020 [cit. 2020-12-10]. Dostupné z: https://influencermarketinghub.com/what-is-tiktok/

TULGAN, Bruce. Meet Generation Z: The second generation within the giant "Millennial" cohort. *Rain Maker Thinking* [online]. 2013, , 13 [cit. 2020-12-09]. Dostupné z: http://grupespsichoterapija.lt/wp-content/uploads/2017/09/Gen-Z-Whitepaper.pdf

*Ochrana údajů a soukromí na internetu* [online]. 2020 [cit. 2020-12-10]. Dostupné z: https://europa.eu/youreurope/citizens/consumers/internet-telecoms/data-protection-online-privacy/index_cs.htm#shortcut-4

CHALUPOVÁ, Barbora a Vít KLUSÁK. [online]. 2020 [cit. 2020-12-10]. Dostupné z: https://www.vsitifilm.cz/o-filmu.html

JOHANSEN, Alison Grace. *What is antivirus software? Antivirus definition* [online]. NortonLifeLock, 2019 [cit. 2020-12-10]. Dostupné z: https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html

SYMANOVICH, Steve. *What is a VPN?* [online]. NortonLifeLock, 2020 [cit. 2020-12-10]. Dostupné z: https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html

KASPERKY, Lab. *Malicious programs* [online]. NortonLifeLock, 2020 [cit. 2020-12-10]. Dostupné z: https://encyclopedia.kaspersky.com/knowledge/malicious-programs/

MADOOEI, Ali. *Client-Server Application* [online]. 2020 [cit. 2020-12-10]. Dostupné z: https://madooei.github.io/cs421_sp20_homepage/client-server-app/

NOTT, Christopher. *What is Spyware? - Definition & Types* [online]. 2020 [cit. 2020-12-10]. Dostupné z: https://study.com/academy/lesson/what-is-spyware-definition-types.html

, Mike. Tech Radar [online]. 2021 [cit. 2021-01-08]. Dostupné z: https://www.techradar.com/best/best-antivirus

## 7.2 Literární zdroje:

AYCOCK, John. Spyware and Adware: Advances in Information Security – Svazek 50 [online]. Springer Science & Business Media, 2010 [cit. 2020-12-08]. ISBN 0387777415. Dostupné z: https://books.google.cz/books?id=UKNgoM3nLe0C&printsec=frontcover&hl=cs&source=gbs_atb#v=onepage&q&f=false

WILEY, John. *Phishing and Countermeasures: Understanding the Increasing Problem of Electronic Identity Theft* [online]. John Wiley, 2006 [cit. 2020-12-08]. ISBN 0387777415. Dostupné z:

https://books.google.cz/books?id=UKNgoM3nLe0C&printsec=frontcover&hl=cs&source=gbs_atb#v=onepage&q&f=false

PROF. CUNNANE, Vincent a Niall DR. CORCORAN. *ECSM 2018 5th European Conference on Social Media* [online]. Academic Conferences and publishing limited, 2018 [cit. 2020-12-09]. ISBN 9781911218845. Dostupné z: https://books.google.cz/books?id=b09mDwAAQBAJ&pg=PA192&dq=phishing+on+social+media&hl=cs&sa=X&ved=2ahUKEwi1pdP3xMHtAhWnzIUKHfH-DzMQ6AEwAHoECAAQAg#v=onepage&q=phishing%20on%20social%20media&f=false

BC. HAVELKOVÁ, Hana. *Děti a technologie aneb je to o rodičích*. Brno, 2017. Diplomová práce. MASARYKOVA UNIVERZITA. Vedoucí práce Mgr. Lenka Gulová, Ph.D.

STANISLAV, Mark. *Two-Factor Authentication* [online]. IT Governance, 2015 [cit. 2020-12-10]. ISBN 9781849287340. Dostupné z: https://books.google.cz/books?id=3EU3DwAAQBAJ&pg=PA19&dq=two+step+verification&hl=en&sa=X&ved=2ahUKEwjUsNO2jsPtAhXRMewKHU-xCXIQ6AEwAHoECAEQAg#v=onepage&q=two%20step%20verification&f=false

KOWALSKI, Robin M., Susan P. LIMBER a Patricia W. AGATSTON. *Cyber Bullying: Bullying in the Digital Age* [online]. John Wiley, 2009 [cit. 2020-12-10]. ISBN 9781444321883. Dostupné z: https://books.google.cz/books?id=mAa5Z-HPWCcC&pg=PR13&dq=cyberbullying&hl=en&sa=X&ved=2ahUKEwjrxqaekcPtAhXEyYUKHYBJBvsQ6AEwAXoECAUQAg#v=onepage&q=cyberbullying&f=false

RAMSLAND, Katherine a Patrick N. MCGRAIN. *Inside the Minds of Sexual Predators* [online]. ABC-CLIO, 2009 [cit. 2020-12-10]. ISBN 9780313379611. Dostupné z: https://books.google.cz/books?id=gngG9zPmNKMC&pg=PA155&dq=sexual+predators&hl=en&sa=X&ved=2ahUKEwi7_LbMjMTtAhUrxYUKHeSmCqEQ6AEwAHoECAQQAg#v=onepage&q=sexual%20predators&f=false

# 8 Přílohy

## 8.1Příloha 1 – vzor dotazníku

Vážení čtenáři.

Prosím vás u vyplnění jednoduchého dotazníku určenému k průzkumu pro bakalářskou práci na téma Ochrana soukromí na sociálních sítích.

Dotazník je anonymní a nezabere déle než 5 minut.
Dotazník je určen pro všechny věkové skupiny od středoškoláků až po seniory.
Mnohokrát děkuji za váš čas a vaše odpovědi.

**Otázky**

1. **Pohlaví.**
   - Muž
   - Žena
2. **Věková skupina.**
   - 15 až 19
   - 20 až 25
   - 26 až 40
   - 40 až 60
   - 60 +
3. **Jste…?**
   - Pracující
   - Student
   - Jiné
4. **Využíváte služeb sociálních sítí? (Facebook, Instagram atd.)**
   - Ano
   - Ne
5. **Za jakým účelem sociální sítě využíváte?**
   - K navázaní kontaktu se svými známými.
   - K pracovním záměrům (propagace produktů služeb a další).
   - K hledání známostí.
   - Jako zábavu ve volném čase.
   - Sociální sítě nevyužívám.

- Jiné.

6. **Kolik času denně strávíte na sociálních sítích?**
    - Sociální sítě nevyužívám.
    - Méně než hodinu.
    - 1 až 2 hodiny.
    - 2 až 4 hodiny.
    - Více než 4 hodiny.
7. **Máte, nebo měli jste špatné zkušenosti s využíváním služeb sociálních sítí?**
    - Ano
    - Ne
8. **Pokud ano, tak jaké? (Není nutné odpovědět). [Otevřená otázka]**
9. **Přidáváte si do přátel i lidi, které neznáte osobně?**
    - Ano
    - Ne
    - Sociální služby nevyužívám.
10. **Zveřejňujete o sobě osobní informace na sociálních sítích? (fotografie, adresu, kam a na jak dlouho jedete na dovolenou atd.)**
    - Ano
    - Ne
    - Sociální služby nevyužívám.
11. **Jaký z následujících operačních systémů využíváte na svém zařízení? (mimo mobilní telefony).**
    - Microsoft Windows
    - Linux
    - MacOS
    - Operační systémy Unix
    - Jiné.
12. **Jaký z následujících prohlížečů pro své účely využíváte?**
    - Google Chrome
    - Firefox
    - Opera
    - Microsoft Edge
    - Safari

- Jiné.

13. **Účastníte se soutěží, které jsou zprostředkovány skrze sociální sítě?**
    - Vždy.
    - Někdy (u produktů, který mě zajímá).
    - Nikdy.
14. **Jaký na vás má vliv příspěvek "Vyhrajte IPhone....." a další podobné příspěvky.**
    - Rád/a se zasoutěžím.
    - Nevšímám si jich.
    - Vyhýbám se jim, protože těmto příspěvkům nevěřím.
    - Jiné.
15. **Jste si vědomi rizika výskytu malwarů (škodlivých programů, které se různým způsobem snaží poškodit, či odcizit soukromá data) v mnoha formách (přílohy ve zprávách, odkazy na obrázky, videa a další stránky) a podnikáte proti těmto útokům určité kroky?**
    - Ano
    - Ne
16. **Jste si vědomi rizika výskytu spywarů, adwarů a dalších způsobů monitorování vašich pohybů na internetu (tento způsob se nejvíce využívá při online nákupech, kdy pomocí různých nástrojů může jedinec sledovat vaše vyhledávání a na jeho základě vám nabízet podobné produkty na jeho e-shopu) a podnikáte proti těmto metodám nějaké kroky?**
    - Ano
    - Ne
17. **Čtete pozorně smluvní/licenční podmínky a updaty týkajících se ochrany, či pravidel?**
    - Ano
    - Ne
18. **Využíváte služeb nějakého antivirového programu? (zajišťuje co největší ochranu zařízení proti virům, malwarům a dalším formám útoků na osobní data).**
    - ESET
    - Avast
    - Bitdefender

- Kaspersky
- Norton
- Nevyužívám služeb žádného antivirového programu.
- Jiné.

19. **Využíváte služeb VPN? (chrání uživatele při práci na internetu a šifruje přenos dat pro zajištění jejich ochrany).**
    - ExpressVPN
    - NordVPN
    - CyberGhost
    - HMA
    - Nevyužívám služeb VPN.
    - Jiné.
20. **Myslíte se, že je vaše momentální zabezpečení na internetu dostačující?**
    - Určitě ano
    - Spíše ano
    - Nevím
    - Spíše ne
    - Určitě ne
21. **Otázka pro rodiče! Snažíte se zabezpečit zařízení, které vaše děti používají k přístupu na internet za pomocí různých softwarů, k tomuto účelu určených? (antivirový program atd.)**
    - Ano
    - Ne
    - Nejsem rodič.
22. **Otázka pro rodiče! Snažíte se vzdělat své děti ohledně bezpečného užívání sociálních sítí a internetu obecně? (nepsat si s cizími lidmi, nezveřejňovat o sobě osobní údaje, nezasílat finanční údaje atd.)**
    - Ano
    - Ne
    - Nejsem rodič.
23. **Otázka pro rodiče! Má účet vašich dětí (do 16 let/ v ČR méně) rodičovskou kontrolu, která informuje o pohybech dítěte na sociálních sítí, kterou dle směrnic EU musí tyto sociální služby poskytovat?**

- Ano
- Ne
- Nejsem rodič.

24. **Jaký je hlavní faktor, podle kterého vybíráte vhodný software pro ochranu dat a soukromý? (antivirový program, VPN atd....). Pokud jste pro své zařízení nevybírali takovéto softwary, odpovídat nemusíte.**
    - Cena
    - Efektivnost
    - Rychlost
    - Jiné.
25. **Používáte jiné metody zabezpečení dat, krom výše zmíněných a pokud ano, tak jaké? (pokud ne, neodpovídejte). [Otevřená otázka]**