# BAKALÁŘSKÁ PRÁCE

Kyberbezpečnost – rizika komunikace na síti

Cybersecurity – risks of communication on network

## STUDIJNÍ PROGRAM

Specializace v pedagogice

## STUDIJNÍ OBOR

Učitelství praktického vyučování a odborného výcviku

## VEDOUCÍ PRÁCE

doc. Ing. David Vaněček, Ph.D.

MICHALKOVÁ

KRISTÝNA

**2022**

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

## I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení: **Michalková** Jméno: **Kristýna** Osobní číslo: **492918**

Fakulta/ústav: **Masarykův ústav vyšších studií**

Zadávající katedra/ústav: **Institut pedagogických a psychologických studií**

Studijní program: **Specializace v pedagogice**

Studijní obor: **Učitelství praktického vyučování a odborného výcviku**

## II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

**Kyberbezpečnost – rizika komunikace na síti**

Název bakalářské práce anglicky:

**Cybersecurity – Risks of Communication on Network**

Pokyny pro vypracování:

Tématem bakalářská práce je kybernetická bezpečnost a rizika komunikace na síti. Práce je rozdělena na dvě části – teoretickou a empirickou. Teoretická část se zabývá hlavními zásadami zajištění ochrany informací a pravidly pro bezpečné používání prostředků výpočetní, informační a komunikační techniky. Empirická část prezentuje výsledky dotazníkového šetření. Cílem šetření bylo zjistit, s jakými bezpečnostními riziky se uživatelé setkali a zda mají negativní zkušenost.

Seznam doporučené literatury:

CLOUGH, Jonathan, 2015. Principles of cybercrime. Second edition. Cambridge, United Kingdom: Cambridge University Press. ISBN 9781107034570.
LUCAS, George R., 2017. Ethics and cyber warfare: the quest for responsible security in the age of digital warfare. New York, NY: Oxford University Press. ISBN 9780190276522.
ŠEVČÍKOVÁ, Anna. Děti a dospívající online: Vybraná rizika používání internetu. Praha: Grada Publishing, 2014. ISBN 978-80-247-5010-1.
STOWELL, Louie. Bezpečnost dětí na internetu. Praha: Svojtka & Co., 2017. ISBN 978- 80-256-2083-0.
KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně n@ internetu: průvodce chováním ve světě online. Computer Press, 2016. ISBN 978-80-247-5595-3.

Jméno a pracoviště vedoucí(ho) bakalářské práce:

**doc. Ing. David Vaněček, Ph.D. institut pedagogických a psychologických studií**

Jméno a pracoviště druhé(ho) vedoucí(ho) nebo konzultanta(ky) bakalářské práce:

Datum zadání bakalářské práce: **06.01.2022** Termín odevzdání bakalářské práce: **28.04.2022**

Platnost zadání bakalářské práce: _____

| doc. Ing. David Vaněček, Ph.D.<br>podpis vedoucí(ho) práce | doc. Ing. David Vaněček, Ph.D.<br>podpis vedoucí(ho) ústavu/katedry | prof. PhDr. Vladimíra Dvořáková, CSc.<br>podpis děkana(ky) |
|---|---|---|

## III. PŘEVZETÍ ZADÁNÍ

Studentka bere na vědomí, že je povinna vypracovat bakalářskou práci samostatně, bez cizí pomoci, s výjimkou poskytnutých konzultací. Seznam použité literatury, jiných pramenů a jmen konzultantů je třeba uvést v bakalářské práci.

Datum převzetí zadání _____ Podpis studentky _____

MICHALKOVÁ, Kristýna. *Kyberbezpečnost – rizika komunikace na síti*. Praha: ČVUT 2022. Bakalářská práce. České vysoké učení technické v Praze, Masarykův ústav vyšších studií.

MASARYKŮV ÚSTAV
VYŠŠÍCH STUDIÍ
ČVUT V PRAZE

# Prohlášení

Prohlašuji, že jsem svou bakalářskou práci vypracovala samostatně. Dále prohlašuji, že jsem všechny použité zdroje správně a úplně citovala a uvádím je v přiloženém seznamu použité literatury.

Nemám závažný důvod proti zpřístupňování této závěrečné práce v souladu se zákonem č.121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

V Praze dne: podpis: ……

# Poděkování

Chtěla bych touto cestou vyslovit poděkování všem, kteří se jakýmkoliv způsobem podíleli na zpracování této bakalářské práce. Zejména bych ráda vyjádřila poděkování svému vedoucímu bakalářské práce, panu doc. Ing. Davidu Vaněčkovi, Ph.D., za jeho odborného rady a připomínky. Zároveň bych ráda poděkovala i SOŠ podnikání a mediální tvorby v Kolíně, neboť mi tato škola umožnila u nich realizovat mé dotazníkové výzkumné šetření pro sběr dat do mé empirické části bakalářské práce.

# Anotace

Tématem bakalářská práce je kybernetická bezpečnost a rizika komunikace na síti. Práce je rozdělena na dvě části – teoretickou a empirickou. V teoretické části je vymezen pojem internet a sociální sítě, v této kapitole je zmíněna mládež a možná rizika, jež z užívání sociálních sítí plynou. V další kapitole jsou přiblíženy kybernetické hrozby a rizika spojená s tímto tématem. Dále je nastíněna i problematika zabezpečení přístupových údajů. Empirická část prezentuje výsledky dotazníkového šetření. Cílem šetření bylo zjistit, s jakými bezpečnostními riziky se uživatelé setkali a zda mají negativní zkušenost.

## Klíčová slova

Internet, osobní údaj, sociální sítě, rizika, kybernetické hrozby, útočník, oběť, prevence

# Annotation

The topic of the bachelor thesis is cybersecurity and risks of communication on the network. The thesis is divided into two main parts – theoretical and empirical. The theoretical part defines the concept of the internet and social networks, this chapter mentions social networks and youth and the possible risks that arise from the use of social networks. The next chapter describes the cyber threats and risks asssociated with this topic. The issue of access data security i salso outlined. The empirical part presents the results of the questionnaire survey. The aim of the survey was to find out, what security risks were users faced with and whether they had a negative experience.

## Key words

Internet, personal data, social network, risks, cybersecurity threat, aggressor, victim, prevention

# Obsah

# Seznam symbolů a zkratek

**ICT –** Infromation and communication technologies

**NBÚ –** Národní bezpečnostní úřad

**GDPR –** obecné nařízení o ochraně osobních údajů

**HITM –** man i the middle (člověk uprostřed)

**Quid pro quo –** něco za něco

**URL –** Uniform resource locator (jednotný lokátor zdroje)

**2FA –** Dvoufaktorová autentizace

**IRC –** Internet relay chat

**DNS server –** Domain Name Systém

**IANA** – internet Assigned Numbers Authority

**ICANN** – internet Corporation For Assigned Names and Numbers

**IRC** – Internet relay chat

# ÚVOD

Spojitost mezi internetem, sociální sítí a dětmi se stává poměrně diskutovanou záležitostí. Téměř neomezený přístup k informacím, přináší dětem a mladistvým možnost komunikace s kýmkoliv, kdekoliv a hlavně kdykoliv. Děti jsou v online prostředí velice důvěřivé a nemají problém se svěřit cizí osobě. Autor si myslí, že většina mládeže si ani neuvědomuje možná rizika komunikace na síti. V této bakalářské práci jsou zmíněna rizika jako flaming, hoax, kyberšikana, grooming, kyberstalking, krádež identity a sexting. Tato rizika jsou ta nejzávažnější a měla by se jim věnovat pozornost.

Cílem této bakalářské práce je seznámit čtenáře se zásadami zajištění ochrany informací a pravidly pro bezpečné používání prostředků výpočetní, informační a komunikační technologie. Dále také popsat možné nebezpečí, která prostředí internetu a sociálních sítí mohou přinést.

Bakalářská práce se skládá z teoretické a empirické části. Teoretická část je rozdělena na čtyři kapitoly. V první kapitole je vymezen pojem internet. Následuje druhá kapitola, kde autor popisuje, co jsou sociální sítě, jejich výhody a nevýhody, mládež a možná rizika komunikace na sociálních sítích. Rizika jsou v této kapitole přesněji popsána a čtenář se zde dozví, co na sociální síti hrozí za rizika a jak se takovému riziku bránit. Další kapitola se zabývá kybernetickými hrozbami a hlavními zásadami zajištění ochrany informací. Dále také pravidly pro bezpečné používání prostředků výpočetní, informační a komunikační techniky. V této podkapitole autor popisuje, jaká rizika mohou nastat, jak jim lze předcházet a jak se zachovat při vzniku bezpečnostního incidentu. Poslední kapitolou teoretické práce je zabezpečení přístupových údajů. Jsou zde popsána jednotlivá zabezpečení jako chování uživatele, význam a efektivnost hesla, dvoufaktorová ověření, záloha dat a mnoho dalších.

Praktická část je provedena pomocí dotazníkového šetření. Které je aplikováno na studenty střední odborné školy. Cílem tohoto šetření je zjistit, s jakými bezpečnostními riziky se respondenti setkali a zda mají negativní zkušenost. Zjistit, jak velký je rozsah znalostí studentů vybrané školy o rizicích vyplývajících z aktivního využívání sociálních sítí a také zda mají vhodně zabezpečená svá zařízení a vytvořené profily. Součástí dotazníkového šetření jsou také čtyři předpoklady, které budou pomocí tohoto testování přijaty, nebo v opačném případě zamítnuty.

# I. TEORETICKÁ ČÁST

# 1. Internet

Internet je rozsáhlá síť, která propojuje počítače po celém světě a stala se součástí dnešního moderního života. Prostřednictvím internetu lidé mohou sdílet informace a komunikovat odkudkoliv. Internet poskytuje schopnost tak výkonnou a obecnou, že ji lze použít téměř pro jakýkoliv účel, který závisí na informacích.

## 1.1 Vymezení pojmu internet

Internet představuje globální elektronickou síť propojující několik sta milionů uživatelů, kterým nabízí nejrůznější využití a služby. Internet pomáhá uživatelům vyhledávat jakékoliv informace, nakupovat přes internetové obchody, pracovat v online prostředí a možnosti komunikace přes několik tisíc kilometrů. Komunikace se díky internetu velmi rozvinula a nyní máme možnost komunikovat s kýmkoliv a kdekoli na světě, či už zvukovým, písemným anebo obrazovým způsobem. Internet je síť údajů, která nám nabízí celosvětové zpravodajství, sport, filmy, hry, muziku, služby a mnoho dalších jiných možností. V dnešním světě je internet součástí našich životů, to se týká hlavně mladé generace, která skoro celý svůj život řídí přes internet a počítačové technologie bere jako samozřejmost. Toto vše z nich ovšem dělá ty nejlehčí cíle a hrozí jim různá rizika. Toto téma je více rozebráno v podkapitole 2.2 rizika sociálních sítí.[1]

Ze statistiky zpracované Mezinárodní telekomunikační unií vyplývá, že k internetu bylo k roku 2021 na celém světě připojeno cca 4,9 miliardy lidí neboli 63% světové populace, to tedy představuje nárůst o 17 % od roku 2019.[2]

Internet jako celek nikdo nevlastní ani neřídí, jeho funkčnost je dána na touze lidí být propojeni. Je velmi důležité internet koordinovat a jelikož nemá žádného majitele, existuje několik nadnárodních organizací jako je například **IANA,** což je nezisková organizace odpovědná za koordinaci činností pro bezproblémové fungování internetu. Další takovou organizací je organizace **ICANN,** která je také nezisková společnost, jejímž hlavním úkolem je udržovat internet stabilní a bezpečný.[3]

---

[1] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9.

[2] ITU *Internet usage statistics* (online) (25.03.2022) Dostupné z: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[3] ICANNWIKI *Internet Assigned Numbers Authority* (online) (25.03.2022) Dostupné z: https://icannwiki.org/Internet_Assigned_Numbers_Authority

# 2. Sociální sítě

Na internetových stránkách můžeme zveřejňovat svůj soukromý (osobní), ale i profesní život sdílením nejrůznějších informací a obsahů. Nejčastěji, tak činíme na sociálních sítích, neboť ty jsou fenoménem dnešní doby. Internetové sociální sítě můžeme chápat jako prostředí, které virtuálně propojuje skupinu uživatelů a poskytuje jim vzájemnou komunikaci mezi sebou prostřednictvím nejrůznějších komunikačních prostředků. Prostřednictvím sociálních sítí si můžeme organizovat svůj soukromý společenský, ale i profesní život a navazovat a udržovat tak i vzdálené kontakty s ostatními lidmi. Sociální sítě nemůžeme chápat pouze jako zdroj pozitivních věcí, neboť mají i své stinné stránky. I sociální sítě přinášejí a souvisejí s určitými riziky a negativními dopady na uživatele. V níže uvedených podkapitolách bude tato problematika sociálních sítí a medií podrobněji rozebrána.

## 2.1 Vymezení pojmu sociální sítě

Sociální sítě můžeme chápat jako internetové služby, které umožňují svým uživatelům vytvářet soukromé, firemní či uzavřené profily, dále také nabízejí prostředí pro sdílení informací, videí, fotografií, obsahu, k provozování chatu a dalších aktivit. Mezi sociální sítě jsou zařazeny i diskuzní fóra, na kterých pomocí internetu dochází k výměně názorů a poznatků mezi uživateli k určitým tématům jako jsou například automobily, mateřství, mazlíčci atd.[4]

V současné době mezi nejvíce používané sociální sítě patří Facebook. Ten každý měsíc používá 2,9 miliardy uživatelů (2022), tím je Facebook první v žebříčku nejaktivnější sociální sítě. Tato čísla ukazují, že zhruba 36,8 procent všech lidí na zemi používá Facebook. Facebook je také velice dobře optimalizován pro mobilní telefony, až 94 procent uživatelů Facebooku, jej používá právě na mobilním zařízení.[5] Druhou nejvíce používanou sítí je YouTube. YouTube byla vždy platforma především pro sdílení videí, aktuálně však nabízí možnosti publikaci textového obsahu na profily uživatelů. Další v pořadí oblíbenosti je Instagram, díky kterému máte možnost sdílet na svém profilu fotografie a videa. Instagram nabízí možnost takzvaného obchodního profilu, který vám nabídne možnost analýzy návštěvnosti profilu a pomáhá s následným plánováním budoucích příspěvků. Jednou z nejvíce úspěšných sociálních sítí je

[4] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.
[5]DATAREPORTAL *Facebook stats and trends* (online) (03.04.2022) Dostupné z: https://datareportal.com/essential-facebook-stats

čínská sociální síť TikTok. TikTok oznámil, že na konci září 2021 překonal hranici 1 miliardy aktivních uživatelů měsíčně, čímž se stal teprve sedmou platformou s takovou aktivitou. TikTok dosáhl takového čísla, i když je stále blokován v Indii (zemi která je domovem více než 650 milionů uživatelů internetu, tedy zhruba 15 procent celosvětové internetové populace). Jedná se o aplikaci, která uživatelům umožňuje vytvářet a sdílet krátká hudební videa na jakékoliv téma. Právě TikTok je nejvíce oblíben mezi dospívající mládeží.[6] Mezi další oblíbené sociální sítě řadíme také Whattsapp, WeChat, Snapchat, Pinterest, Twitter, FB messenger, QQ, telegram a Reddit.[7]

## 2.2 Sociální sítě a jejich výhody a nevýhody

Sociální sítě umožňují uživatelům spojit se s ostatními a vytvářet tak komunity. Facebook, Instagram, Youtube, TikTok a mnoho dalších sociálních sítích jsou součástí každodenního života téměř každého ve 21. století. Ovšem tyto sociální sítě s sebou nesou řadu výhod a nevýhod.

Jednou z hlavních výhod sociálních sítí je především komunikace a sdílení informací. Lidé spolu mohou komunikovat a sdílet informace s kýmkoliv z celého světa, a to kdykoliv a odkudkoliv. Tato forma komunikace, která nás všechny spojuje, je snadno dostupná. Vzestup sociálních sítí a obecný zájem studentů, učitelů a mnoha dalších, přitáhl pozornost k využívání internetových nástrojů k rozvoji distančního vzdělávání. Pomocí internetu se uživatelé mohou plně vzdělávat a zdokonalovat se od specialistů v určitém oboru. Sociální sítě jsou také velmi výhodné pro všechny podnikatele či další lidi, kteří chtějí propagovat své služby, výrobky, nápady apod. Díky sociálním sítím mají podnikatelé mnoho možností, jak se dostat blíže k zákazníkovi a přesvědčit ho, o nákupu či využití jeho služeb. V dnešní moderní době se zrodilo mnoho influencerů, kteří mají své kanály, blogy, profily apod., na kterých dělají kontent pro své publikum. Tak vzniklo úplně nové prostředí pro reklamu a propagaci.[8]

Prostřednictvím sociálních sítí se můžeme průběžně informovat o všech událostech a novinkách ve světě, nebo v něčím životě. Sociální sítě jsou nejlepší platformou pro zveřejňování čehokoliv, na co máte chuť. Ať už je to hudba, umělecká tvorba, recept, video

[6] GROWTH QUARTERS *Analysis: TikTok soars and global social media users hit 4.5 bilion* (online) (2.4.2022) Dostupné z: https://thenextweb.com/news/analysis-global-digital-statshot-report-october-2021
[7] SMART INSIGHTS *Global social media statistics research summary 2022* (online) (2.4.2022) Dostupné z: https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/
[8] PIMPERNEL GAWKROGER *Advantages and disadvantages of social media* (online) (2.4.2022) Dostupné z: https://medium.com/@clinguen/advantages-and-disadvantages-of-social-media-47cd957b73d5

a mnoho dalšího. Sociální sítě zvyšují a předávají kreativitu jedince tak, aby oslovil miliony uživatelů. Sociální sítě fungují také jako skvělý prostředek na odbourávání stresu, například tím že se lidé z různých koutů světa spojují a budují si pozitivní vztahy. Existují různé skupiny a můžete narazit na mnoho lidí, kteří vám mohou pomoci v boji se stresem, depresí a izolací. Ke zlepšení situace v oblasti kriminality, využívají policisté a vláda sociální sítě k nalezení zločinců a k boji proti kriminalitě ve své zemi.[9]

Výhod sociálních sítí je mnoho, ovšem přináší i své značné nevýhody, jako je například problém se soukromím. Sociální sítě mohou velice snadno způsobit problémy, které nelze nikdy vyřešit. Sdílením svých osobních informací se vždy uživatelé vystavují riziku, ať už hovoříme o riziku z pohledu pracovního či osobního života. Můžeme zde mluvit o sdílení nevhodné fotografie, sdílení či tvoření nevhodného obsahu, sdílení polohy zařízení, sdílením hesel k účtům a mnoho dalších případů. Obsah, který na internet uživatel nahraje, už z internetu nezmizí, proto by se každý měl minimálně dvakrát zamyslet, před sdílení jakékoliv osobní informace na sociální sítě.

Velkým problémem dnešní doby je závislost, a to závislost na sociálních sítích. Tato závislost zasahuje zejména mladší generaci, která na mobilních zařízení tráví celé dny. Používat něco není špatné, ale získat na tom závislost může být katastrofální. Lidé na sociálních sítích plýtvají svým produktivním časem i energií. Sociální sítě se staly překážkou na cestě sociálního a emocionálního spojení. Ať už jde o vyjádření vlastních pocitů, či řešení životních problémů. Lidé si stále více a častěji zvykají na komunikaci prostřednictvím chatu a zpráv. Mnoho lidí takto ztrácí schopnosti vyjádřit svůj názor nebo řešit problémy. Emoce a pocity člověka nelze procítit pouhou textovou zprávou. Mezi lidmi tedy chybí vzájemné spojení a ztrácejí schopnost chápat a rozpoznat pocity a emoce toho druhého.[10] Kdykoli se probudíte nebo půjdete spát, máte impuls zkontrolovat, zda váš telefon neobsahuje oznámení a zprávy. Jednou z velkých nevýhod sociálních sítích v našem životě, je dlouhé sezení zaneprázdněné používáním moderních technologií, které vede k různým zdravotním problémům, jako je únava, krevní tlak, obezita, stres, deprese atd.[11]

[9] VINAY PRAJAPATI *Advantages and Disadvantages of cosial media* (online) (03.04.2022) Dostupné z: https://www.techprevue.com/advantages-and-disadvantages-of-social-media/
[10] BOYD, Danah. *Je to složitější: sociální život teenagerů na sociálních sítích*. Přeložil Lukáš NOVÁK. Praha: Akropolis, 2017. ISBN 978-80-7470-165-8.
[11] BILAL AHMAD *Advantages and Disadvantages of social media for society* (online) (8.4.2022) Dostupné z: https://www.techmaish.com/advantages-and-disadvantages-of-social-media-for-society/

## 2.3 Sociální sítě a mládež

Dětství je důležitou etapou člověka a tato etapa trvá od narození až po dospělost, tedy do osmnácti let. Podle Vágnerové (2012) období dětství můžeme dělit na období prenatální, novorozenecké, kojenecké, batolecí věk, předškolní období, věk školní, pubescence a adolescence. Dítě je jedinec, který se nachází v určitém věkovém období, označovaném jako dětství. Je velmi důležité se zajímat o to, co se v tomto období dítěte děje a co je jeho obsahem. V tomto období se osobnost a psychika dítěte vyvíjí. Dále se také vyvíjí sociální začlenění, vztah k druhým lidem, ale i k sobě samému. Vyvíjí se také vlastnosti a projevy, poznání, konání a emoční prožívání, nastává také vývoj tužeb, chtíče a morálního postoje.[12]

Mladší generace, především v období adolescence není výjimkou v používání sociálních sítí a internetu celkově. Bohužel, příliš mnoho lidí, si stále neuvědomuje, odmítá či podceňuje možná rizika sociálních sítí, většinou si ani nedokážou představit možné hrozby. Sociální sítě nabízejí mladistvým jednoduchý přístup ke komunikaci s jejich vrstevníky a přáteli, ale i s cizími lidmi na celém internetu. Dospívající mládež je skupina, která je sociálními sítěmi nejvíce ohrožena. Především proto, že sociální sítě jsou každodenní součástí života mnoha uživatelů, málo kdo si dnes představí život bez komunikace „online“. V oblasti sociálních sítí vládne nepoměr pozitivních i negativních stránek, celkový obsah sociálních sítí je velmi často nevhodný pro nižší věkovou kategorii, tedy děti, které by neměly v tak brzkém věku používat sociální sítě, bohužel je k tomu dnešní moderní doba nutí. Většina sociálních sítí má nastavenou věkovou hranici pro používání od 13 let, avšak děti si mohou uměle navýšit svůj pravý věk, díky takovému kroku se mohou dostat k nevhodnému obsahu, kontaktu s cizími uživateli a může jim také hrozit riziko ukradení osobních informací.[13]

Využívání sociálních sítí je rizikové také pro životní styl mládeže. Většinu svého volného času tráví za počítačem nebo u mobilního zařízení, kde společně komunikují přes internet, namísto osobní interakce venku. Tímto vzniká závislost, která by se dala přirovnat k závislosti na alkoholu a tabákových výrobcích. S touto závislostí souvisí úzce také tzv. hráčství. Internet slouží mládeži k nalezení zábavy a relaxace. Hlavním dodavatelem zábavy pro volný čas na internetu, je především videoherní průmysl. Hraní videoher je pro mladistvé cestou odreagování se, například při cestě hromadnou dopravou, či po náročné činnosti jako

[12] VÁGNEROVÁ, Marie. *Vývojová psychologie: dětství a dospívání*. Vydání druhé, doplněné a přepracované. Praha: Karolinum, 2012. ISBN 978-80-246-2153-1.
[13] ECKERTOVÁ, Lenka a Daniel DOČEKAL. *Bezpečnost dětí na internetu: rádce zodpovědného rodiče*. Brno: Computer Press, 2013. ISBN 978-80-251-3804-5.

oddychová aktivita, většina mladistvých hraní videoher považuje za únik z nudy. Hraní videoher pomáhá mladistvým k navozování konverzace, zapojení se do kolektivu a v hledání nových kamarádů. Ovšem i samotné hraní videoher má své pozitiva a negativa. Videohry jsou dobré pro to, aby pomohly dětem rozvíjet dovednosti při řešení problémů, zlepšení nálad, podpora relaxace a snížení úzkosti. Mladiství si také mohou vybudovat emocionální odolnost tím, že se naučí vyrovnat se s prohrou ve videohře. Jak zde autor již zmiňoval, obrovskou výhodou videoher je socializace, v digitálním světe se dospívající mohou spojit se svými přáteli a uvolnit stres. Samotné hraní videoher má i své negativa, jako je narušení spánku, závislost a násilné chování. Samotné videohry nejsou jediným důvodem, proč se stává dítě agresivním, jsou zde i jiné faktory jako komunikace mezi hráči samotnými. Dítě se může stát závislým na videohrách, v tomto případě zde mluvíme o hráčství. To může vyvolat podrážděnost, halucinace, fyzickou bolest a riziko nadváhy.[14]

Období adolescence s sebou nese tělesné ale i duševní rozvoje, které jsou u každého jedince naprosto jiné, tyto rozvoje vedou k velkým biologickým změnám a ty vedou k emočnímu napětí. Mládež umí na sociálních sítích a internetu celkově vyhledávat nejrůznější informace, hrát online hry, komunikovat s kýmkoliv na celém světě, získávat nepřeberné informace a dokážou se na internetu také vzdělávat. Velké množství adolescentů se na internetu zajímá o existenční otázky života, jako jsou například vztahy a výběr partnera, tvoření vlastních hodnot a také k vyjasnění vlastních postojů. V dnešní době jsou naprosto normální mobilní telefony a tablety, tudíž děti a mladiství sdílejí na sociálních sítích fotografie a videa, často se sexuálním podtextem, nahotou a další nevhodné obsahy podporující krutost a násilí. Tato mládež cítí na internetu svobodu, nejsou zde většinou žádné hranice či rodiče, kteří by je kontrolovali, je to tak hlavně proto, že dospělí se většinou plně neorientují v této oblasti. Tento pocit může přispívat ke konfliktům, ale i ke ztrátě zábran či zapletení se do určitých rizik tohoto internetového světa. Je potřeba mládež seznámit se základy bezpečnosti a možnými riziky na sociálních sítích. Je potřeba si dávat pozor, kam své osobní údaje zadáváte a jak je spravujete, bohužel někteří uživatelé dokážou tyto informace zneužít.[15]

[14] KVĚTON, Petr. *Hraní videoher v dětství a dospívání: dopady a souvislosti v sociálně-psychologické perspektivě*. Praha: Grada, 2020. Psyché (Grada). ISBN 978-80-271-2887-7.

[15] Lindeberg, Katajun.; Kindt, Sophie.; Szász-Janocha, C. *Internet Addiction in Adolescents*; SpringerLink: Germany, 2020. ISBN: 978-3-030-43784-8

## 2.4 Rizika sociálních sítí

Sociální sítě a diskuzní fóra jsou primárně určeny k prezentaci, komunikaci a získávání či udržování kontaktů, nicméně řadou uživatelů jsou úmyslně a cíleně zneužívány. Tito uživatele záměrně a většinou anonymně šíří nepravdivé informace, obtěžují, uráží, vydírají, vyhrožují, případně nutí své oběti k aktivitě proti jejich vůli, anebo i k osobnímu kontaktu s tímto uživatelem. Důsledkem takové komunikace či aktivitě útočníka pak může být těžká psychická, ale i fyzická újma oběti. Níže uvedené praktiky patří mezi nejzáludnější a nejčastěji používané. Lze se s nimi setkat jak na sociálních sítích a diskuzních fórech, ale řada z nich může být útočníkem praktikovaná i jinou formou, například komunikační platformou nebo e-mailem.

Při takové internetové komunikaci vzniká trestní činnost prostřednictvím informačních technologií. Informační technologie se poté stává cílem, místem anebo také nástrojem pro spáchání trestného činu. Prostřednictvím internetu vzniká široké spektrum nelegální aktivity, také zde může docházet k podvodům, krádeži, vydírání či sexuálnímu obtěžování.[16]

Pomocí internetu je velmi jednoduché tvořit a distribuovat nelegální obsah mezi uživateli. Mezi nejvíce ohroženou skupinu patří děti, které využívají sociální sítě velmi často, a tak se ne jednou s kriminalitou páchanou na internetu setkaly. Nejvíce rizikové oblasti týkající se dětí jsou například, získávání osobních informací, videí a fotografií oběti a vystavování oběti nevhodným materiálům jako je pornografie. Dále můžeme mluvit o nebezpečné komunikaci s obětí, kdy útočník usiluje o osobní schůzku s dítětem. Prostřednictvím internetu je výroba a distribuce materiálů zneužívaných dětí velice jednoduchá. K největším problémům dnešní doby patří také flaming, kyberšikana, kyberstalking, grooming a sexting. Podrobněji se těmto problémům budeme věnovat v jednotlivých kategoriích.[17]

Přemýšlejte nad obsahem, který sami zveřejňujete na sociální sítě, případně komu ho zpřístupňujete. Fotka celé rodiny z dovolené může potěšit nejen vaše přátele, ale i zloděje, kterému jste příspěvkem oznámili, že máte prázdný dům. Myslete na to, že každým svým příspěvkem či zveřejněnou fotografií publikujete veřejné informace, které s vysokou pravděpodobností uvidí i někdo, komu byste je nikdy v normálním životě nesdělili.

Možnosti, jak se bránit a předejít možnému riziku na sociální síti:

[16] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.
[17] HULANOVÁ, Lenka. *Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality*. Praha: Triton, 2012. ISBN 978-80-7387-545-9.

- Nezveřejňujte informace, které by mohl někdo zneužít.
- Chcete-li se na sociální síti pochlubit fotkami z dovolené, zveřejněte je až po návratu.
- Ověřujte si informace z více zdrojů, zejména ty negativní, nepříznivé, poplašné a těžko uvěřitelné.
- Vyhýbejte se komunikaci s neznámými lidmi, případně i komunikaci, která na vás působí negativně již od počátku.
- Nenechte se vyprovokovat a zatáhnout se do komunikace, která vás obtěžuje a způsobuje nepříjemné pocity, úzkost či jakoukoliv psychickou újmu.
- Překročila-li aktivita útočníka vámi stanovenou mez, kdy se už nedokážete sami bránit, přerušte komunikaci a pokud kontakt od útočníka pokračuje, nebojte se obrátit na policii české republiky.[18]

### 2.4.1 Flaming

Flaming je umisťování nepřátelských, urážlivých, diskriminačních nebo obtěžujících vzkazů s cílem někoho urazit, rozzlobit, zesměšnit nebo vyprovokovat. Flaming se obvykle vyskytuje na diskuzních fórech, chatu, IRC či v emailech. Útočník opakovaně umisťuje na sociální sítě vzkazy a následně stupňuje své útoky. Flamer utočí na jiného uživatele, s jehož názory nesouhlasí, ovšem nepoužívá podloženou a propracovanou argumentaci, pouze hrubě nadává, uráží a vyhrožuje. Velmi důležité je rozdělovat od sebe flamera a trolla. Troll je uživatel sociálních sítí, který chce svými činy vyvolat konflikt a během konverzace se nebojí použít vulgární komentáře, které často nesouvisí s tématem. Flamewar je označení internetové diskuze která překročila hranice konstruktivní výměny názorů a stala se emotivně vyhrocenou a nepřehlédnutelnou hádkou.[19]

### 2.4.2 Hoax

Hoax je úmyslné šíření poplašných zpráv, a to nejen formou sociálních sítí, ale i formou řetězových e-mailových zpráv. Takové zprávy mohou obsahovat například varování před počítačovými viry, údajná zdravotní rizika, hororové příběhy, konspirační teorie a mnoho

[18] CLOUGH, Jonathan. *Principles of cybercrime. Second edition. Cambridge, United Kingdom: Cambridge University Press,* 2015. ISBN 9781107034570
[19] E-BEZPEČÍ, *co je flaming* (online) (08.04.2022) Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/dalsi-temata/38-35

dalších. Příběhy v těchto zprávách jsou navrženy tak, aby vás zaujaly, ale nejsou založené na faktech. Příkladem takového hoaxu může být velkorysý zakladatel Facebooku který zněl „*Pokud to budete sdílet, Mark Zuckerberg Vám pošle 4,5 milionu dolarů*“[20]. Za cílem podvodných zpráv, může být také pokus o získání vašich údajů o kreditní kartě, uživatelském jméně a hesle. Cílem takové zprávy je šíření nepravdivé nebo zkreslené informace, která má šířit paniku, vystrašit příjemce a donutit ho k unáhleným nebo nebezpečným činům. Samostatná falešná zpráva je neškodná, pokud oběť nezačne jednat. Před kliknutím na tlačítko přeposlat, to se mi líbí nebo sdílet, zkontrolujte každou e-mailovou zprávu a příspěvek na sociálních sítích. Součástí hoaxu jsou také takzvané fake news, falešné zprávy úmyslně šířící dezinformace a poplašné zprávy za účelem zmanipulování příjemce. K šíření fake news se nevyužívají jen sociální sítě, ale především neseriózní internetová média.[21]

### 2.4.3 Kyberšikana

Kyberšikana je soustavné zasílání obtěžujících, urážlivých či útočných vzkazů s cílem někomu dlouhodobě psychicky, či následně fyzicky ubližovat. Kyberšikana je označení šikany páchané pomocí elektronických médií, jako je internet, email, sociální sítě, mobilní telefony, SMS, fotografie, videonahrávky a mnoho dalších, za účelem poškození daného uživatele. Extrémně nebezpečnou formou kyberšikany je nahrávání ponižujících scén na mobilní telefon a následné zveřejňování videa na internetu, často s rozesíláním odkazu známým oběti.

„*Kyberšikana je kolektivní označení forem šikany prostřednictvím elektronických médií, jako je internet a mobilní telefony, které slouží k agresivnímu a záměrnému poškození uživatele těchto médií. Stejně jako tradiční šikana i kyberšikana zahrnuje opakované jednání a nepoměr sil mezi agresorem a obětí“* [22]

V posledních letech se mnoho lidí, zejména dětí, stalo obětí kyberšikany, protože v dnešní době je velmi snadné vytvořit si falešné profily a vyhrožovat druhé osobě. Kyberšikana má za následek mnoho sebevražd, problémů s depresemi atd. Lidé začali využívat sociální sítě jako platformu pro šíření falešných zpráv a fám. Obrovský problém kyberšikany je, že se s touto formou šikany můžeme setkat prakticky kdykoliv a kdekoliv, stačí nám pouze

[20] G DATA *What is actually is a hoax?* (online) (08.04.2022) Dostupné z: https://www.gdatasoftware.com/guidebook/what-actually-is-a-hoax
[21] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.
[22] MEGAN Price, DALGLEISH John, *Cyberbullying experiences* (2010) (online) (12.04.2022) Dostupné z: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.469.2077&rep=rep1&type=pdf

připojení k internetu anebo mobilní síti. Oběťmi kyberšikany se většinou stávají děti, které jsou často z kolektivu odmítány a nejsou v tomto prostředí populární. Můžeme zde mluvit o dítěti plachém, nejistém, úzkostném či o výrazně vybočujícím jedinci, jako je například barva pleti a vlasů, rovnátka, brýle, styl oblékání atd.[23] U kyberšikany ve velké většině oběť ani netuší pravou totožnost útočníka, o to více je kyberšikana na rozdíl od klasické šikany závažnější. Do kyberšikany jedné oběti se může zapojit více útočníků a celkové ponížení oběti může sledovat i více lidí.

Vágnerová ve své knize uvádí „*Na rozdíl od šikany agresorem nemusí být fyzicky a sociálně zdatný jedinec, agresorem je jedinec silný v informačních technologiích, může to tedy být prakticky kdokoliv*“.[24]

Účinky kyberšikany mohou trvat dlouho a ovlivnit člověka mnoha způsoby, ať už psychicky, emocionálně nebo fyzicky. Pokud se uživatel setká s kyberšikanou, může se začít stydět, být nervózní, nejistý a úzkostný. To vše může vést k odloučení od rodiny a přátel, negativním myšlenkám a pocitu viny za činy které uživatel udělal anebo neudělal. Častý je také pocit osamělosti, přetížení, bolest hlavy, nevolnost a bolest žaludku. Může dojít i ke ztrátě motivace a pocitu izolace od lidí, které milujeme a kterým důvěřujeme. To vše může mít negativní vliv na duševní zdraví a pohodu. Mladí lidé se často obracejí, v důsledku těchto aspektů, k látkám, jako je alkohol a drogy, nebo násilné chování, aby se vypořádali s psychickou a fyzickou bolestí. V případě kyberšikany je prvním krokem k získání pomoci rozhovor s blízkou osobou či rodinou, nebo školním poradcem a nebojte se obrátit na národní centrum bezpečnějšího internetu, nebo policii české republiky.[25]

### 2.4.4 Grooming

Grooming je druh kyberšikany, jejímž cílem je pomocí psychické manipulace vybudovat emocionální spojení s obětí, vylákat z oběti osobní údaje a vyvolat falešnou důvěru. Rozhovory, fotografie nebo videa se sexuální tématikou jsou nedílnou součástí groomingu. Tento získaný obsah poté útočník může využít jako prostředek k vyhrožování nebo vydírání. Cílem útočníka je vylákat oběť na osobní schůzku, kde většinou dochází k fyzickému násilí,

[23] CLOUGH, Jonathan. *Principles of cybercrime. Second edition. Cambridge, United Kingdom: Cambridge University Press*, 2015. ISBN 9781107034570
[24] VÁGNEROVÁ, Kateřina. *Minimalizace šikany: praktické rady pro rodiče*. Vyd. 2. Praha: Portál, 2011. ISBN 978-80-7367-912-5.
[25] PAPEŽOVÁ, Zděnka. *Prevence – kyberšikana* (online) (08.04.2022) Dostupné z: https://www.policie.cz/clanek/prevence-kybersikana.aspx

sexuálnímu zneužití, zneužití oběti pro dětskou prostituci a k výrobě dětské pornografie. Nejvíce obtěžovanou skupinou jsou děti do 18 let, a to především mladé dívky.

Kožíšek a Písecký uvádí: „*Je to takové chování uživatelů na internetu, jehož cílem je pomocí internetových komunikačních prostředků a jiných technologií vyvolat v dospělém/ dítěti pocit důvěry a prostřednictvím falešné identity ho zneužít nebo vylákat na schůzku*“[26]

Útočníci si zakládají falešné profily na sociálních sítích jako je například Facebook. Zde si vytvoří profil s falešnou identitou mladistvého a poté jsou k oběti velice přátelští. Útočník využívá samozřejmě více profilů a vytváří si svému účtu i kamarády, to vše, aby tento účet vypadal pravdivěji a bylo lehčí si získat důvěru mladé osoby. Konverzace mezi útočníkem a obětí začínají většinou ohledem věku, rodiny, zájmů, školy, mazlíčcích a poté se konverzace stupňuje k sexuálním tématům. Útočník tímto způsobem může kontaktovat více dětí najednou. Útočník se poté snaží svou oběť nalákat na různé věci, které oběť zrovna potřebuje. Dítě, které bylo vystaveno groomingu má poté pocit zrady, zklamání, může to vést ke strachu dítěte a nízkému sebevědomí. Je důležité mladší generaci o tomto riziku informovat, a to samozřejmě i jejich rodiče a školství.[27]

V únoru roku 2020 vyšel do kin dokumentární film V Síti, který pojednává právě o groomingu. Ze statistik vyplývá že třetina českých dětí byla obětí groomingu a byly svědky masturbace prostřednictvím webkamery. Protagonistky v tomto dokumentárním filmu jsou tři dospělé ženy, které předstírají, že jsou dvanáctileté dívky. Během pouhých 10 dnů „dívky“ oslovilo 2458 osob. Herečky si tedy píšou a volají s těmito predátory a chovají se jako dvanáctileté dívky, většina predátorů se z dívek snaží vylákat obnažené fotografie, videa a další nevhodné materiály. Samozřejmě i samotní predátoři dívkám posílají spoustu nevhodného materiálu, mluvíme zde i o online hovorech s kamerou. Poté co predátor fotografii od herečky získá, začne okamžitě herečky vydírat, například tím, že obnažené fotografie nahraje na internet, pošle rodině anebo tento nevhodný obsah zveřejní po škole. Tento dokumentární film není pouze o online komunikaci mezi „dívkami“ a predátory, ale představí nám také osobní schůzky s některými predátory na veřejných místech, jako je například cukrárna. Vše je samozřejmě za doprovodu skrytých kamer a dohledem ochranky. Po odvysílání tohoto dokumentárního filmu si od režiséra Klusáka policie vyžádala natočený materiál 42 osob.[28]

[26] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.
[27] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.
[28] WIKIPEDIE *V síti* (online) (08.04.2022) Dostupné z: https://cs.wikipedia.org/wiki/V_s%C3%ADti

### 2.4.5 Kyberstalking

Kyberstalking je druh stalkingu, kdy útočník využívá internetu a dalších technologií k zastrašování, vydírání a obtěžování oběti. Kyberstalking je zpravidla provázen nevyžádanými zprávami, pomluvami, vydíráním, krádeží identity, shromažďováním citlivých informací, snahou o vylákání peněz apod. Kyberstalking může mít podobu e-mailu, textových zpráv, příspěvků na sociálních sítích a dalších. Do této kategorie spadají například neschválené proslulé e-mailové zprávy, které po oběti požadují výkupné za nezveřejnění její aktivity na internetu, a to včetně záznamu z webkamery oběti.[29] V dnešní době není problém si o určité osobě najít spoustu informací na sociálních sítích. Útočník se úmyslně snaží v oběti navodit pocit strachu o své soukromí, zdraví a v krajních případech i o vlastní život. Oběť poté může trpět úzkostmi, depresí a pocitem strachu. Existují dokonce zprávy, že důsledkem kyberstalkingu oběti mohou trpět posttraumatickou stresovou poruchou a sebevražednými myšlenkami.[30] Obětmi kyberstalkingu se často stávají celebrity, díky dostupnosti veškerých potřebných informací na internetu. Tento útočník se do oběti zamiluje a posílá různé dárky či dopisy, bylo mnoho případů, kdy útočníkova touha mít oběť jen pro sebe došla až k fyzickému napadení či pokusu o vraždu. Od roku 2010 je stalking trestným činem v české republice a je kvalifikován jako & 354 nebezpečné pronásledování. Můžeme tedy říct, že pronásledování je trestný čin[31] Nejlepší verzí obrany proti stalkerovi je projevit nezájem o jakýkoliv kontakt s útočníkem, myslíme tím zprávy, hovory, SMS a schůzky. Veškeré důkazy proti útočníkovi se doporučují ukládat a poté předat policii ČR k dalšímu šetření.[32]

### 2.4.6 Krádež identity

Krádež identity je trestný čin, páchaný za účelem získání osobních nebo finančních údajů jiné osoby. Tyto údaje jsou zneužity za účelem páchání podvodu, jako je provádění neoprávněných transakcí. Krádeže identity jsou páchány mnoha různými způsoby a jejich obětem je obvykle způsobeno poškození financí a pověsti. Krádež identity dříve byla zjednodušeně fyzické vydávání se za někoho jiného díky ukradeným dokumentům. Dnešní

[29] VERYWELL MIND *What is cyberstalking?* (online) (08.04.2022) https://www.verywellmind.com/what-is-cyberstalking-5181466
[30] PUBMED *The impact of cyberstalking: the lived experience a thematic analysis* (online) (08.04.2022) Dostupné z: https://pubmed.ncbi.nlm.nih.gov/24875706/
[31] PAPEŽOVÁ, Zděnka. Prevence – kyberšikana (online) (08.04.2022) Dostupné z:https://www.policie.cz/clanek/prevence-stalking.aspx
[32] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

podoba se změnila pouze v tom, že je vše prováděno online. Krádež identity může být spáchána mnoha způsoby, jako jsou prohledávání pevných disků, procházení sociálních sítí, používáním podvodných e-mailů, nabouráním se do počítačové sítě či samotného počítače, kde následně útočník získá přístup k počítačovým záznamům za použití např. malwaru, který poté shromažďuje informace. Toto téma autor dále nastiňuje v podkapitole 3.2 softwarová rizika.[33]

Příklady krádeží identity:

- **Krádež finanční identity** – je nejběžnější formou krádeže, která směřuje k získání úvěru, zboží, služeb anebo výhod.
- **Krádež sociální identity –** při získání čísla sociálního zabezpečení, útočník může zažádat o půjčku a poté neplatit dlužné částky.
- **Krádež lékařské identity –** útočník se vydává za jinou osobu, aby získal bezplatnou lékařskou péči.
- **Daňová krádež identity –** útočník použije získané osobní údaje k podání falešného daňového přiznání, k získání refundace.
- **Zločinecká krádež identity –** útočník se během zatčení vydává za jinou osobu, aby se vyhnul odsouzení.

Podle Kožíška a Píseckého (2016), počet případů krádeže identity stále roste. Někteří uživatelé internetu se snaží vystupovat jako někdo jiný a pomocí falešné identity své informace zkrášlují. Mnozí z těchto uživatelů se vydávají za celebrity, lékaře, producenty, investory a také za normální lidi. Někteří mají svou identitu tak promyšlenou, že i pro odborníky, je těžké falešnou identitu rozpoznat. Tito uživatelé se poté snaží přesvědčit člověka o jeho pravosti.[34]

Nejsilnější obranou proti krádeži identity jsou silná hesla, která jsou na každé službě jiná. Dalším krokem obrany je uvádět o sobě co nejméně informací na sociálních sítích a pravidelně si kontrolovat své zabezpečení. O tomto tématu autor dále hovoří v kapitole 4. zabezpečení přístupových údajů. Pokud přesto dojde ke krádeži, je na místě vše oznámit Policii ČR.

[33]INVESTOPEDIA *Identity Theft* (online) (22.04.2022) Dostupné z:https://www.investopedia.com/terms/i/identitytheft.asp

[34] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

### 2.4.7 Sexting

Sexting je rozesílání a zveřejňování textových zpráv, fotografií a videí se sexuálním obsahem, šířené na jakémkoliv zařízení. Tento materiál obsahuje nahotu anebo přímo samotný sexuální akt. Na internetu je dnes velice snadné a rychlé se dostat ke sexuálnímu obsahu, a to i náhodou či úmyslně. Úmyslné vyhledávání tohoto obsahu je zejména u mladistvých naprosto normální, je spojeno s potřebami dospívajících jedinců. Přestože tento obsah můžou uživatelé legálně shlédnout až od osmnácti let, je mnoho mladistvých, kteří si tento obsah přesto shlédnou, nejsou nijak poskytovateli kontrolováni a vše je v naprosté anonymitě. Samotný sexting je hrozbou pro mladistvé, u kterých je velké riziko že se stanou obětí přes sociální sítě, ať už jako odesílatelé či adresáti. Hlavním důvodem rozesílání intimního obsahu, je touha upoutat pozornost a flirt. K samotnému sextingu se hojně využívá sociálních sítí jako je například Facebook, Messenger, Instagram a Snapchat. Mladší uživatelé sociálních sítí si mohou naivně myslet, že si adresát veškerý tento materiál uchová pro sebe, ovšem ten následně tento materiál může velice snadno zneužít a zveřejnit jej na sociálních sítích nebo je rozesílat e-mailem. Samotný sexting probíhá nejčastěji mezi vrstevníky a partnery, u kterých hrozí riziko zneužití tohoto obsahu po ukončení vztahu. Následky tohoto zneužití bývají velice často šikana, vydírání, ponižování a zesměšňování, které poté vede k velmi vážným psychickým a sociálním problémům a toto všechno může skončit i sebevraždou. Některé státy pojmy sexting a dětská pornografie nerozlišují.[35]

Jako příklad, kdy tento obsah zaslaný v soukromí byl zneužit, je případ, kdy na sociální síti Facebook vznikla skupina nesoucí název „Pražské roztahovačky“, na které její uživatelé nahrávali fotografie a videa které jim v soukromí dívky zaslaly. Samozřejmě u tohoto obsahu zveřejnili také jméno dívky a popis o jakou dívku se jedná. K této skupině se poté přidala další města jako je Brno či Olomouc. Později se tímto případem začala zabývat i Policie ČR.[36]

Podle Kožíška a Píseckého je sexting považován: „*za jedno z nejrizikovějších chování, jehož důsledky mohou být fatální. V některých případech je na oběť činěn takový nátlak, který může končit dehonestací, sebepoškozením nebo sebevraždou*“ [37]

[35] ECKERTOVÁ, Lenka a Daniel DOČEKAL. *Bezpečnost dětí na internetu: rádce zodpovědného rodiče*. Brno: Computer Press, 2013. ISBN 978-80-251-3804-5.
[36] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.
[37] Tamtéž

**Obrázek 1: Důvody zaslání fotografie anebo video se sexuálním obsahem**


**Zdroj: Kožíšek, Martin a Václav, Písecký (2016).**

Hlavní prevencí mohou být rodiče, kteří informují své děti o těchto rizicích a kontrolují aktivitu svých dětí na sociálních sítích. Je velice důležité mluvit o tomto tématu otevřeně a informovat mladistvého o rizicích digitálního soukromí a jeho narušování. Pokud přeci jen tento problém nastane je třeba ho řešit okamžitě. Posíláním či vyžádáním sexuálního obsahu osobám mladším patnácti let, útočník porušuje zákon § 192 o výrobě a jiném nakládání s dětskou pornografií.[38]

[38] POLICIE ČESKÉ REPUBLIKY *Počítačová mravnostní kriminalita* (online) (09.04.2022) Dostupné z: https://www.policie.cz/clanek/pocitacova-mravnostni-kriminalita.aspx

# 3. Kybernetické hrozby

Rizika sociálních síti se stávají převážně běžným uživatelům, kdežto kybernetické hrozby a útoky, jsou spíše směřovány na firmy a státní složky. Samozřejmě mohou cíleně anebo plošně zasáhnout i jednotlivce. Informační a komunikační technologie ve spojitosti s internetem se v průběhu posledních deseti letí stali neoddělitelnou součástí našich životů. Tyto technologie slouží k široké škále aktivit a podílejí se na nejrůznějších činnostech. S nárůstem počtu těchto uživatelů se i zvýšila počítačová kriminalita. Ta probíhá prostřednictvím kybernetických hrozeb a útoků. Kybernetické hrozby jsou činy, které mohou provádět jednotlivci, ale i organizované skupiny se škodlivými úmysly, jejímž cílem je získat data, způsobit nejrůznější poškození (škody) anebo narušit výpočetní systémy. Kybernetické útoky mohou být cílené na konkrétní organizace (podniky) anebo na jednotlivce. V reakci na tyto hrozby a útoky se začala rozvíjet i oblast kybernetické bezpečnosti. Tato třetí kapitola se věnuje nastínění této problematiky. Zmíněny budou nejrůznější bezpečnostní události, incidenty a rizika. Je nutné si uvědomit fakt, že kybernetickému útoku můžeme být vystaven každý uživatel internetu.

Kybernetické hrozby mohou pocházet od různých aktérů, včetně firemních špionů, hacktivistů, teroristických skupin, nepřátelských národních států, zločineckých organizací, osamělých hackerů a nespokojených zaměstnanců. V posledních letech vedly četné, vysoce profilované kybernetické útoky k odhalení citlivých dat.[39]

## 3.1 Úvod do kybernetické bezpečnosti

Pod pojmem informační a kybernetická bezpečnost si lze představit soubor technických, organizačních, administrativních a režimových opatření k zajištění tří klíčových atributů informací a dat. Prvním atributem je **důvěrnost**, informace je v tomto případě přístupná pouze oprávněným uživatelům. Další v pořadí je **integrita**, informace je přesná a kompletní, nelze ji neoprávněné změnit. Třetí klíčový atribut je **dostupnost**, informace je oprávněným uživatelům k dispozici v požadované době. Všechna opatření nastavená v rámci zajišťování informací a kybernetické bezpečnosti mají za úkol zajistit, aby se kompletní informace bezpečně dostala pouze k těm osobám, pro které je určena. Můžeme tedy říct, že kybernetická bezpečnost je praxe ochrany systému, sítí a programů před digitálními útoky. Tyto útoky jsou obvykle

[39] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

zaměřeny na přístup k citlivým informacím, jejich změnu nebo zničení. Zavádění účinných opatření v oblasti kybernetické bezpečnosti je dnes obzvláštně náročné, protože existuje více zařízení než lidí a útočníci jsou stále inovativnější.

Pojem kybernetická bezpečnost bývá nejčastěji definován jako „*souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru*“.[40] Zde je zmínka o pojmu kybernetický prostor (kyberprostor).

Kyberprostor si můžeme představit jako nehmotný svět plný informací, který se za pomocí informačních a komunikačních systémů neustále rozšiřuje.

Jak zmínil Kolouch „*Kyberprostor je virtuální realitou, nemající konec ani začátek. Tato virtuální realita je však zcela závislá na materiální podstatě, tedy technologiích nacházejících se ve světě reálném“*.[41]

Podle Jiráska pojem kyberprostor bývá nejčastěji definován jako „*digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, službami a sítěmi elektronických komunikací*“[42].

Jde tedy o samostatný svět, který je vytvářen počítači. Tento svět umožňuje uchovávat, vytvářet, využívat a vyměňovat si informace mezi lidmi, stejně jako v reálném životě. Lidé si zde mohou sdílet informace, nakupovat zboží, pracovat, hrát či prozkoumávat obsah a zjišťovat nové informace.

## 3.2 Sociální inženýrství

Sociální inženýrství je cílený sběr citlivých informací, které mají být následně zneužity. Využívání psychologické manipulace k získání informací či donucení uživatele udělat chybu. Z pohledu bezpečnosti ICT jde zejména o sběr dat prostřednictvím internetu či telefonní komunikace. Tyto útoky zneužívají důvěřivosti uživatelů a slouží obvykle k získávání přístupových údajů do informačních systémů, bankovních aplikací atd. Sociální inženýrství je způsob manipulace lidmi za účelem získávání informací nebo provedení určité činnosti. K útokům sociálního inženýrství dochází v jednom nebo i více krocích. Techniky sociálního

[40] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. ISBN 978-80-7251-397-0.
[41] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.
[42] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. ISBN 978-80-7251-397-0.

inženýrství jsou obzvlášť nebezpečné, jelikož spoléhají na lidskou chamtivost, strach nebo závist, než na zranitelnost softwaru a operačních systémů.[43]

Techniky sociálního inženýrství:

- **Spear phising** je útok, který je předem naplánovaný a cílí na konkrétní firmu nebo fyzickou osobu. Své jednání poté útočník přizpůsobuje na základě charakteristik pracovních pozic a kontaktů patřícím oběti. Spear phising vyžaduje ze strany útočníka mnohem větší úsilí a jeho odstranění může trvat týdny anebo měsíce.
- **Pharming** je útok, kdy útočník nastrčí falešné stránky místo legitimních. Oběť tedy tyto stránky přesměrují na škodlivý web, kde v mnoha případech je cílem útočníka získat finanční údaje anebo ověřovací údaje oběti. Tato stránka se tedy může tvářit jako vaše internetová bankovní služba a po zadání vašich přihlašovacích údajů, tyto údaje útočník obdrží.[44]
- **Vishing** je útok, který je prováděn telefonicky, případně formou SMS či zpráv přes komunikační aplikace, za účelem krádeže osobních informací od oběti. Útočník využívá důvtipné taktiky sociálního inženýrství, aby přesvědčil oběť a získali si jejich důvěru. Snaží se takto získat soukromé informace a přístupy do bankovních účtů. Útočník spoléhá na to, že přesvědčí oběť, že dělá správnou věc tím, že odpovídá na otázky. Často se útočník vydává za někoho z vlády, daňového úřadu, policie anebo banky.[45]
- **Spoofing** je falšování identity či maskování komunikace z neznámého zdroje. Spoofing se může vztahovat na e-maily, telefonní hovory či webové stránky. Útoky mohou být více technické jako je falšování IP adresy nebo DNS serveru.
- **HITM** (man in the middle) je metoda útoku, při které útočník zasahuje nepozorovaně do komunikace mezi dvěma subjekty (např. bankou a klientem).
- **Pretexting** je útok, kde se útočník snaží pomocí předem vymyšlené záminky a dobře promyšlených lží, získat od oběti potřebné informace. Obvykle využívá kombinaci pravdivé informace a lži, snaží se vzbudit dojem legitimity. Často se

[43] LUCAS, George R., *Ethics and cyber warfare: the quest for responsible security in the age of digital warfare. New York, NY: Oxford University Press*. 2017. ISBN 9780190276522
[44] PROOF POINT *What is pharming?* (online) (10.04.2022) Dostupné z: https://www.proofpoint.com/us/threat-reference/pharming
[45] LUCAS, George R., *Ethics and cyber warfare: the quest for responsible security in the age of digital warfare. New York, NY: Oxford University Press*. 2017. ISBN 9780190276522

vydává za kolegu z práce, policejního vyšetřovatele, zaměstnance státní správy, agenta pojišťovny, bankovního poradce nebo jiné osoby, které mají právo vědět citlivé informace oběti. Pomocí tohoto útoku jsou zjištěna osobní informace oběti, jako jsou například čísla sociálního zabezpečení, osobní adresy, telefonní čísla, data ze zaměstnání, bankovní záznamy a mnoho dalších.[46]

- **Baiting** je útok provádění pomocí tzv. návnady. Používá se falešný slib, aby podnítil chamtivost nebo zvědavost oběti. Lákají uživatele do pasti, která poté ukradne jejich osobní údaje nebo zasáhne systémy malwarem. Velmi oblíbená je také metoda kdy útočník zanechá malwarem infikované médium (USB disk, CD) někde, kde je snadné jej najít. Médium bývá úmyslně označeno legitimně a zároveň tak, aby vzbuzovalo zvědavost oběti. Vložením do zařízení se instaluje škodlivý kód, obvykle umožňující útočníkovi přístup k zařízení.
- **Quid pro quo** je útok kdy útočník, vydávající se za pracovníka technické podpory, náhodně vytáčí telefonní čísla za účelem nalezení slabého článku (oběti) s vymyšlenou historkou o nutnosti vyřešení technického problému na zařízení oběti. Cílem útočníka je však přimět oběť k instalaci škodlivého kódu nebo k umožnění přístupu k firemnímu zařízení či síti.[47]
- **Phising** je útok který spočívá ve snaze útočníka nalákat svou oběť do prostředí, kde mu uživatel dobrovolně a v dobré víře předá své osobní údaje. Většinou přístupové údaje k bankovním účtům nebo čísla platebních karet. Útočník takzvaně nahodí udičku a uživatel se buď chytne, nebo nikoliv. K „nahození udičky“ jsou obvykle využívány matoucí e-mailové zprávy, SMS, případně zprávy rozesílané přes komunikační nástroje nebo sociální sítě. Nejčastěji jde o velice sofistikované útoky, které spočívají v nalákání uživatele na falešné webové stránky, kde je následně vyzván k zadání přihlašovacích údajů nebo čísla platební karty. Tyto údaje se pak útočník snaží zneužít, a to zpravidla bezprostředně po jejich získání.[48] Aktuálně jde o nejvíce rozšířenou

[46] CLOUGH, Jonathan. *Principles of cybercrime. Second edition. Cambridge, United Kingdom: Cambridge University Press*, 2015. ISBN 9781107034570

[47] IMPERVA – *Social engineering* (online) (10.04.2022) Dostupné z: https://www.imperva.com/learn/application-security/social-engineering-attack/

[48] ESET *Pojmy z oblasti internetové bezpečnosti a ochrany – Phishing* (online) (24.03.2022) Dostupné z: https://www.eset.com/cz/phishing/

kybernetickou hrozbu, jejíž způsob provedení útočníci neustále vylepšují a přizpůsobují moderním trendům a požadavkům doby.[49]

Příklady phisingu: uživatel je vyzván k aktivitě na svém bankovním účtu, například ke změně hesla či ověření údajů, oznámení o uzamčení platební karty s výzvou k jejímu odemčení atd. Prvním krokem v obraně proti phisingu je zamyslet se, zda zpráva, která vás nutí k nějaké akci jako je vstup na webovou stránku, vyplnění formuláře, provedení platby, odpověď na zprávu atd. dává smysl. Neklikejte bezhlavě na odkazy ve zprávách, používejte dvoufaktorovou autentizaci pro přihlášení do důležitých aplikací, jako je internetové bankovnictví. U méně známých internetových obchodů, speciálně u těch s podezřele nízkými cenami si ověřte uživatelské recenze, a to z více zdrojů, podezřelým e-shopům se rovnou vyhněte.

### 3.3 ICT

Zkratka ICT pochází z anglického výrazu information and communication technologies. Oblast ICT zahrnuje veškeré informační technologie používané pro komunikaci a práci s informacemi, a to, jak hardwarová zařízení jako jsou osobní počítače, servery, mobilní telefony atd., tak jejich softwarové vybavení jako operační systémy, aplikace, síťové protokoly atd. V moderním světě představují informační a komunikační technologie důležitou a nepostradatelnou součást veřejné, podnikatelské i soukromé sféry. Povinností každého, kdo přichází do styku s informacemi nebo využívá technické prostředky ICT, je mít povědomí o rizicích spojených se zpracováním informací a používáním technických prostředků ICT, bezpečně zacházet s informacemi, bezpečně užívat služby a technické prostředky a dodržovat stanovená bezpečnostní opatření. Z tohoto důvodu patří jejich ovládání mezi klíčové kompetence. Každý uživatel by měl dodržovat obecně platná bezpečnostní pravidla pro práci s technickými prostředky ICT, mezi které obvykle patří zamezení možnosti zneužití služeb, ochrana dat proti poškození, odcizení, ztrátě, zálohování lokálně uložených dat, zákaz instalace jiných než schválených aplikací atd.[50]

S utajovanými informacemi se může seznamovat pouze fyzická osoba, která je nezbytně nutně potřebuje k výkonu své funkce, pracovní nebo jiné činnosti, a která splňuje podmínky pro přístup k informacím určitého stupně utajení. Státní správu v oblasti ochrany utajovaných

[49] LUCAS, George R., *Ethics and cyber warfare: the quest for responsible security in the age of digital warfare. New York, NY: Oxford University Press*. 2017. ISBN 9780190276522
[50] HOFRICHTER, Kamil. *ICT strategie*. Vydání druhé. [Praha]: Vysoká škola ekonomie a managementu, 2015. ISBN 978-80-87839-61-4.

informací a bezpečnosti způsobilosti provádí Národní bezpečností úřad (NBÚ), který zajišťuje jednotné provádění ochrany utajovaných informací v ČR. NBÚ se řídí zákonem č. 412/2005 Sb.,[51] o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. NBÚ rozhoduje o vydání osvědčení fyzické osoby a vydání dokladu o zrušení platnosti tohoto osvědčení.[52]

## 3.4 Legislativní rámec

Problematika informační a kybernetické bezpečnosti je upravena řadou legislativních norem. Mezi nejdůležitější patří zákon č. 181/2014 SB.,[53] o kybernetické bezpečnosti, který upravuje práva, povinnosti osob, působnosti a pravomoci orgánů veřejné moci v oblasti elektronických komunikací a informačních systémů. Zákon dále vymezuje orgány a osoby, kterým jsou ukládány povinnosti v oblasti kybernetické bezpečnosti, stanovuje systém zajištění kybernetické bezpečnosti a vymezuje stav kybernetického nebezpečí. Vyhláška č. 82/2018 SB.,[54] o kybernetické bezpečnosti zpracovává příslušný předpis EU směrnice Evropského parlamentu a Rady EU č.2016/1148 pro vybrané informační systémy upravuje obsah a strukturu bezpečnostní dokumentace, obsah a rozsah bezpečnostních opatření. Typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů, náležitosti a způsob hlášení kybernetického a bezpečnostního incidentu. Způsob likvidace dat, provozních údajů, informací a jejich kopií.

## 3.5 Bezpečnostní událost a incident

Bezpečnostní událost je stav, při kterém došlo k ohrožení bezpečnosti informací nebo k porušení pravidel, které může způsobit narušení služeb, bezpečnosti a integrity sítí elektronických komunikací. Během této události mohou být odhalena firemní nebo soukromá data. K bezpečnostním událostem dochází často. Některé organizace, v závislosti na jejich velikosti a proslulosti, zažívají denně stovky útoků ve formě phisingových e-mailů, nedbalosti zaměstnanců a mnoho dalších útoků. Bezpečností incident vzniká v důsledku selhání či nedodržení bezpečnostních opatření. Bezpečností událost může být příčinou vzniku bezpečnostního incidentu. Bezpečnostní incident může být i pouhý neúspěšný pokus o zcizení

[51] Zákon č. 412/2005 Sb., (online) (09.04.2022) Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412
[52] NBU *národní bezpečností úřad* (online) (10.04.2022) Dostupné z: https://www.nbu.cz/cs/o-nas/
[53] Zákon č. 181/2014 SB., (online) (26.03.2022) Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181
[54] Vyhláška č. 82/2018 SB., (online) (26.03.2022) Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82

nebo jiné znehodnocení informací. S bezpečností událostí obvykle přichází do prvního kontaktu běžný uživatel. Rozpoznání události a rychlost reakce nezřídka rozhoduje o tom, zda přejde v incident a jaký bude mít další dopad. Pokud událost vyústí v narušení dat anebo soukromí, je tato událost považována za bezpečnostní incident.[55]

Bezpečnostní incident a jeho příklady:

- **Narušení důvěrnosti informací** – informace získal někdo, kdo k nim neměl mít přístup, zneužití přístupu k datům (krádež, odposlech, či jinak nelegálně získané přístupové údaje), zveřejnění chráněných dokumentů (osobní údaje, interní data společnosti, obchodní tajemství atd.), ztráta či krádež techniky které obsahovaly chráněné informace.
- **Narušení integrity informací** – data byla změněna neautorizovaným postupem anebo bez vědomí vlastníka.
- **Snížení dostupnosti informací** – výpadky aplikací, nefunkční zálohování dat a nefunkční obnova dat.

## 3.6 Softwarová rizika

Ve světě globálně propojených sítí jsou informační a komunikační systémy ohroženy sofistikovanými útoky jednotlivců i organizovaných skupin. „*Jinými slovy, rizikem se myslí, jakákoliv nežádoucí událost, jež může, ale také nemusí nastat*“. [56]V důsledku krádeže, ztráty dat nebo zneužití identity, hrozí nevyčíslitelné ztráty nejen společnostem, ale i fyzickým osobám. Je proto důležité, aby byl každý uživatel prostředků a systémů ICT průběžně seznamován se zásadami bezpečného chování při práci s informacemi a prostředky ICT.

### 3.6.1 Malware

Výrazem malware se označují škodlivé programy, které jsou zpravidla instalovány do zařízení jako je notebook, mobilní telefon, a to bez vědomí uživatele. Existuje celá řada typů škodlivého kódu, které se rozlišují hlavně způsobem „vstupu“ do zařízení a druhem aktivity, kterou v zařízení vyvíjí. Autoři malwaru jsou nesmírně kreativní, rychle reagují na vývoj

[55] CORSICA TECHNOLOGIES Whats the difference between a security incident and an event? (online) (10.04.2022) Dostupné z: https://www.corsicatech.com/blog/whats-the-difference-between-a-security-incident-and-an-event/

[56] ŠEVČÍKOVÁ, Anna. *Děti a dospívající online: vybraná rizika používání internetu*. Praha: Grada, 2014. Psyché (Grada). ISBN 978-80-210-7527-6.

v oblasti ICT a neustále vyvíjejí nové typy malwaru, které využívají chyb v nových technologiích (aplikacích, operačních systémech, webových prohlížečích atd.) či neznalosti nebo neopatrnosti uživatelů pro neautorizovaný, respektive skrytý průnik do zařízení. Pro běžného uživatele je často prakticky nemožné rozpoznat, že jeho zařízení bylo napadeno.

Snažte se tedy udržovat operační systém a aplikace aktualizované, útočník hledá slabá místa v zastaralém softwaru. Instalujte pouze aplikace, které potřebujete a budete je používat, také si dávejte pozor odkud tyto aplikace instalujete. Neklikejte na neznáme odkazy a dávejte si pozor na nežádoucí e-maily, snažte se používat pouze známé a důvěryhodné weby.[57]

### 3.6.2 Virus

Virus je obecné označení pro software, který může infikovat zařízení a samovolně se nainstalovat, spouštět a nadále se šířit bez vědomí nebo svolení uživatele. Nejvíce rozšířenou definicí pojmu virus je je z knihy Freda B. Cohena. *„A virus is a program that can „infect" other programs by modifying them to include a, possibly evolved, version of itself."*[58]. Řada virů vykonává pouze obtěžující, ale jinak neškodnou aktivitu, například zatěžují procesor a zpomalují chod zařízení. Většina je ovšem navržena tak, aby získávala kontrolu nad napadeným zařízením a prováděla destruktivní akce, jako například vymazání nebo šíření dat z napadeného zařízení. Virus k šíření nejčastěji využívá spustitelné soubory, aplikace, dokumenty, tzv. dávkové soubory a skripty, případně vyhrazené sektory datových nosičů. Obrana proti virusu začíná bezpečnostní bariérou, kterou je instalovaný a pravidelně aktualizovaný antivirový program, který dokáže zareagovat na vstup, přítomnost i spuštění viru, mnohem důležitější je ale chování uživatele.[59] Nejčastější druhy virů jsou:

- **trojský kůň** je škodlivý kód, obsažený ve zdánlivě neškodné aplikaci, kterou může být například hra, freeware (tedy bezplatná aplikace) atd. Trojský kůň se často šíří infikovanými e-mailovými přílohami.

[57] MCAFEE *Co je malware?* (online) (11.04.2022) Dostupné z: https://www.mcafee.com/cs-cz/antivirus/malware.html
[58] COHEN, Frederick B. *A Short Course on Computer Viruses. Pittsburgh: ASP Press, 1990. ISBN 1-878109-01-4*
[59] NORTON *what is a computer virus?* (online) (11.04.2022) Dostupné z: https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html

- **Červ** je samovolně se šířící škodlivý program, který se šíří například prostřednictvím e-mailu, v rámci počítačové sítě. Počítačový červ se šíří jako příloha e-mailu nebo odkazem na nebezpečné webové stránky.

- **Spyware** je software, zaznamenávající aktivitu uživatele na zařízení, například sledované webové stránky, zadávané přístupové údaje nebo čísla platebních karet. Mezi spyware patří i takzvané keyloggery, které dokážou zaznamenávat aktivitu uživatele na klávesnici. Zaznamenané údaje jsou skrytě odesílány útočníkovi. Spyware se často sám do počítače nainstaluje společně s jiným programem.

- **Adware** je software, který uživateli zobrazuje nevyžádaná reklamní sdělení jako jsou vyskakovací okna, bannery, oznámení atd. Ne vždy jde o nelegálně šířený program, adware obsahuje i řada aplikací, obvykle distribuovaných zdarma.

- **Rootkit** je program, který umožňuje útočníkovi získat administrátorská práva k vašemu zařízení. Rootkit se do vašeho zařízení dostane nainstalováním zdánlivě neškodné aplikace či programu.

- **Ransomware** je velice nebezpečný a sofistikovaný druh viru, který omezuje uživateli přístup k zařízení nebo datům, a to obvykle zašifrováním pevného disku. Uživatel je následně vyzván k úhradě výkupného s tím, že po provedení platby, mu bude zařízení opět zpřístupněno. [60]

[60] AVAST *Online hrozby* (online) (11.04.2022) Dostupné z: https://www.avast.com/cs-cz/c-online-threats

# 4. Zabezpečení přístupových údajů

Neoprávněné získávání a následné zneužívání přístupových údajů k zařízením ICT, bankovním účtům, aplikacím, e-mailovým schránkám nebo firemním informačním systémům je noční můrou nejednoho uživatele, ale i administrátora systému. Optimální způsob zabezpečení přístupových údajů k datům lze jednoduchým způsobem přirovnat k optimálnímu zabezpečení domu nebo bytu. Firewally jsou technologické bariéry zabudované do počítačové sítě pro řízení přístupu. Firewally mají zabránit neoprávněným uživatelům v přístupu k datům a programům.

## 4.1 Osobní údaje

„*Osobní údaje jsou jakékoli informace, které se týkají identifikované nebo identifikovatelné žijící osoby. K osobním údajům patří i různé jednotlivé informace, které společně jako celek mohou vést k identifikaci určité osoby*“[61]. Osobním údajem je každá informace o fyzické osobě, kterou lze přímo či nepřímo identifikovat. Zpracování osobních údajů se rozumí jakákoliv operace, která je s osobními údaji prováděna např. shromažďování, zaznamenávání, uspořádávání, strukturování, ukládání, vyhledávání, zpřístupnění atd.

Příklady osobních údajů:

- Jméno příjmení
- Domácí adresa
- Fotografie
- E-mailová adresa
- Číslo identifikační karty
- Lokační údaje
- IP adresa

Správce musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu a vůči subjektu údajů transparentně a korektně. Osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou

[61] EUROPA, *Co jsou osobní údaje?* (online) (28.03.2022) Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_cs

zpracovány a musí být technicky a organizačně zabezpečeny. Osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovány.

GDPR neboli obecné nařízení na ochranu osobních údajů je soubor pravidel na ochranu dat. GDPR se týká každého, kdo zpracovává, shromažďuje a pracuje s osobními údaji Evropanů.[62] Problematika ochrany osobních údajů je od roku 2018 upravena v obecném nařízení na ochranu osobních údajů, jehož cílem je umožnění občanům Evropské unie lépe kontrolovat své osobní údaje. Nařízení současně modernizuje a sjednocuje předpisy umožňující organizacím snížit administrativní zátěž a mít prospěch z větší důvěry spotřebitelů.

## 4.2 Zásady zajištění ochrany informací a dat

Nejdůležitější složkou zabezpečení přístupových údajů je samotné chování uživatele. Před každým zadáním přihlašovacích údajů zkontrolujte, že jste skutečně na webové stránce aplikace podle URL adresy a že jste připojeni přes zabezpečené připojení. Nepřihlašujte se do klíčových aplikací z veřejných zařízení jako je internetová kavárna, hotel atd. Nezapomeňte se odhlásit z aplikací nebo zařízení po ukončení práce. Pravidelně měňte hesla, minimálně tak jednou za rok a okamžitě po zveřejnění informace, že byla z nějakého vámi užívaného systému hesla odcizena.[63]

Nejběžnějším způsobem zabezpečení přístupu k datům je ochrana heslem. Většina používaných účtu ať už zde hovoříme o účtech na sociálních sítích, bankovního prostředí, aplikací atd., je chráněna přístupovými údaji. Heslo si můžeme nastavit už při vstupu na profil počítače, také na konkrétní softwarové programy, takže pokud útočník získá přístup na počítačový profil, nemůže poté spustit konkrétní programy. Přístupové údaje se obvykle skládají z uživatelského jména nebo e-mailové adresy a hesla.[64]

Zásady pro tvorbu bezpečného hesla jsou:

- Nepoužívejte jednoduchá a snadno uhodnutelná hesla. Snažte se vyvarovat v heslu použití vašeho jména, názvu aplikace, datumu narození, části adresy, jména mazlíčka, vaší přezdívky atd.

[62] GDPR co *je GDPR a jak bude aplikování v Česku* (online) (28.03.2022) https://www.gdpr.cz/gdpr/co-je-gdpr/
[63] E-BEZPEČÍ *Jak zabezpečit počítač* (online) (11.04.2022) Dostupné z: https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1653-jak-zabezpecit-pocitac
[64] ACE THE ELECTORAL KNOWLEDGE NETWORK *Data access security* (online) (11.04.2022) Dostupné z: https://aceproject.org/main/english/et/ete01b.htm

- Krátká hesla se snáze prolomí, proto používejte minimálně osm znaků dlouhá hesla.
- Nejbezpečnější hesla budou obsahovat kombinaci písmen, čísel, znaků a různé velikosti písma. Pamatujte si, že čím je heslo komplikovanější, tím je pro útočníka těžší vaše heslo odhalit.
- Hesla je výhodné pravidelně měnit.
- Hesla není dobré sdílet s jinou osobou, ať už je to kolega z práce, kamarád či partner.

Pro účty, které se nachází v online prostředí je velmi dobré používat tzv. dvoufaktorové ověření, které se využívá hlavně v bankovním sektoru. Jedná se o ověření heslem a poté mobilním telefonem. Po přihlášení heslem musí uživatel zadat také jedinečný kód, který je odeslán na mobilní zařízení prostřednictvím SMS. Tato metoda se může zdát zbytečná, ovšem zvyšuje bezpečnost online účtu.[65]

Zálohování je postup kopírování dat z primárního do sekundárního umístění, aby data byla chráněna v případě katastrofy, nehody nebo útoku jiného uživatele. Pod pojmem data si můžeme představit dokumenty, mediální soubory, konfigurační soubory, obrazy, operační systém atd. V podstatě všechna data, která si přejete zachovat, lze uložit jako záložní data. Vaše data se zkopírují na jedno nebo více úložných míst.[66]

Příklady zálohování dat:

- **Vyměnitelná média** – jsou jednoduchou možností, jak zálohovat svá data. Jedná se o vyměnitelná média jako jsou CD, DVD a USB flash disky. Tato možnost je praktická pouze při zálohování menšího objemu dat a také se musíte ujistit, že zálohu uložíte na bezpečné místo, jinak mohou být také ztraceny při katastrofě.
- **Externí pevný disk** – do sítě můžete nasadit velkoobjemový externí pevný disk a pomocí archivačního softwaru uložit změny na tento disk. S rostoucími objemy dat však jeden externí disk stačit nebude.
- **Cloudové zálohovací systémy** – vaše místí data se odesílají do veřejného nebo soukromého cloudu a v případě ztrátě originálních dat, lze tato data z cloudu obnovit. Data jsou uložena na vzdáleném místě.

[65] E-BEZPEČÍ *Jak zabezpečit počítač* (online) (11.04.2022) Dostupné z: https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1653-jak-zabezpecit-pocitac
[66] CLOUDIAN *Data backup in depth. Concepts, Techniques and Storage Sechnologies (*online) (18.04.2022) Dostupné z: https://cloudian.com/guides/data-backup/data-backup-in-depth/

Téměř každý, kdo je dnes online, má na svém počítači nebo mobilním zařízení přístup na webový prohlížeč. Webový prohlížeč může přehrávat multimediální soubory, hrát hry, pracovat s formuláři, textovými dokumenty atd. Na webovém prohlížeči si zakládáme různé účty, e-maily atd. Tyto informace často uživatelé do webového prohlížeče ukládají. Útočníci se zaměřují na webové prohlížeče, za účelem získání e-mailových účtů, uživatelských jmen, nejrůznějších hesel a osobních či firemních informací. Mohou jej také použít pro přístup k samotnému zařízení. Webové prohlížeče nabízejí velké množství funkcí. Pro prevenci ztráty informací se doporučuje využívat nejnovější verzi webového prohlížeče, využívat možnost blokování falešné stránky, tato funkce zabrání neplánovaným návštěvám škodlivých webových stránek. Dávejte si pozor, z jakých stránek stahujete své aplikace, vždy si ověřte zdroj. Dále si dávejte pozor na kameru a mikrofon, ty by se nikdy neměly spouštět automaticky, prohlížeč by se měl vždy dotázat, zda uživatel chce použít kameru nebo mikrofon. Soubory cookies, pluginy (doplňky) a vyskakovací okna zcela deaktivujte a povolujte tyto aktivity pouze v případě, že je potřebuje důvěryhodný web.[67]

Antivirový program je velice účinnou cestou v zajištění ochrany informací a dat, jedná se o software, který má pomoci detekovat, předcházet a odstraňovat škodlivé softwary ze zařízení. Antivirus se využívá k prevenci, pouští se na pozadí a poskytuje ochranu před virovými útoky v reálném čase. Antivirové programy jako jsou např. Bitdefender, Norton, Avast, ESET, AVG, Avira, Malwarebytes, McAfee atd., pomáhají chránit soubory a data před malwarem, jako jsou červi, trojské koně a mnoho dalších.[68]

Připojování se k veřejným sítím Wifi např. v kavárnách, ve vlaku, v obchodním centru a mnoha dalších místech, není bezpečné. Na těchto free sítích uživatelé pracují, přihlašují se do e-mailů, nakupují věci na webu, přihlašují se na internetové bankovnictví, přihlašují se do firemní databáze atd., a to je velice riskantní. Bez zabezpečení VPN nejsou vaše osobní informace v bezpečí. VPN služby fungují tak, že data z uživatelského zařízení jsou zašifrována a posílána na VPN server. Webová stránka, na kterou se přihlašujete tedy nezná vaší IP adresu, ale pouze VPN serveru. To znamená, že všechna vaše data uchovává pouze zmíněný VPN

[67] SOURCE DEFENSE *web browser security* (online) (23.04.2022) Dostupné z: https://sourcedefense.com/glossary/web-browser-security/
[68] ESET *antivirus* (online) (22.04.2022) Dostupné z: https://www.youtube.com/watch?v=MPD0_dziK1o&t=1s

server, je tedy nezbytně důležité, si vybírat takový server ve který máte důvěru. Doporučují se VPN servery antivirových programů anebo firemní VPN.[69]

Šifrování webových stránek je další možností zajištění ochrany dat. Některé webové stránky začínají http a jiné https. Pokud web, který používáte má v URL adrese http, web šifrovaný není a veškerá komunikace a vámi zadávané informace, které přes tento web probíhají, mohou být zachyceny a změněny. Útočník tedy může ukrást vaše osobní údaje a tato webová stránka se pro vás stává rizikem. Webové stránky začínající https znamenají to, že tento web je šifrovaný a vámi zadávané údaje nelze odposlouchávat a zcizit. Bohužel šifrování https nemusí být vždy 100 %.[70]

Další způsob ochrany můžeme nalézt v prohlížečovém režimu inkognito, který vám pomůže udržet vaše aktivity při prohlížení v soukromí před ostatními uživateli, kteří mohou mít přístup k vašemu počítači. Tato funkce je také známá jako režim soukromého prohlížení či jako anonymní režim. Může hovořit o tom, že se jedná o další ochranný prvek, který může přispět k vyšší anonymitě a bezpečnosti, neboť zabraňuje místnímu protokolování vaší aktivity. Je nutné si uvědomit, že tento režim je pouze funkcí vašeho prohlížeče a že zároveň anonymní režim nešifruje vaše data. Tato funkce v základu funguje tak, že si otevřete novou relaci (kartu) ve vašem prohlížeči, a ta následně zajistí, že deaktivuje historii vašeho prohlížeče spolu s webovou mezipamětí. Například prohlížeč Google Chrome v tomto režimu neukládá následující informace: vaší historii prohlížení, soubory cookies, data stránek a v neposlední řadě zadávané informace do přihlašovacích a registračních formulářů.[71]

Při zajištění ochrany informací a dat dbejte na stále aktualizovaný systém, programy v počítači a v mobilních zařízeních. Mějte své účty zabezpečené silným heslem, využívejte možnost dvoufaktorového ověření a zálohujte svá citlivá data. Udržujte aktualizované také antivirové programy a u stahování aplikací si vždy dávejte pozor, z jakého zdroje tyto aplikace stahujete.

---

[69] JOHANA NÁDVORNÍKOVÁ *bezpečnost na veřejném hotspotu WIFI* (online) (22.04.2022) Dostupné z: https://www.kvalitni-internet.cz/bezpecnost-na-verejnem-hotspotu-wifi-ktery-bezpecny-byt-nemuze-pokud-nemate-vpn

[70] JOHANA NÁDVORNÍKOVÁ *bezpečnost na veřejném hotspotu WIFI* (online) (22.04.2022) Dostupné z: https://www.kvalitni-internet.cz/bezpecnost-na-verejnem-hotspotu-wifi-ktery-bezpecny-byt-nemuze-pokud-nemate-vpn

[71] PCWORLD *Jak funguje anonymní režim* prohlížeče (online) (25.04.2022) Dostupné z: https://www.pcworld.cz/clanky/jak-funguje-anonymni-rezim-weboveho-prohlizece/

## 4.3 Pravidla pro bezpečné používání internetu

Mezi základy zajištění ochrany dat a informací patří tzv. desatero pravidel pro bezpečné používání internetu. Jedná se o souhrn doporučení pro zabezpečení vašich přístupových údajů. Autor všechna tato opatření již zmínil v teoretické části této bakalářské práce.

- **Ochrana osobních údajů –** Nedávejte na sociální sítě a internetové stránky své osobní údaje. Nezveřejňujte adresu, telefonní číslo, čísla karet atd. To vše platí i pro platební údaje, ty zadávejte pouze v ověřeném internetovém bankovnictví.
- **Nastavení soukromí –** Nastavte si své soukromí, zkontrolujte si své sociální sítě a ujistěte se, že citlivé údaje nejsou viditelné všem.
- **Surfování bezpečně –** Neklikejte na podezřelé webové stránky s např. možnou výhrou iPhonu. Tento obsah může být pro váš počítač či mobilní zařízení nebezpečný.
- **Bezpečné připojení –** Pokud se budete chtít připojit na veřejnou Wifi síť a nemáte VPN, vyhněte se jakémukoliv zadávání osobních údajů.
- **Bezpečná hesla –** Mějte vždy silné a bezpečné heslo k vašim účtům a pokud zaznamenáte neoprávněnou aktivitu na vašem účtu, heslo okamžitě změňte.
- **Bezpečné stahování –** Stahování je nejjednodušší způsob, jak můžete infikovat své zařízení. Stahujte tedy aplikace, hry, filmy atd. vždy ze spolehlivých zdrojů.
- **Bezpečná platba –** Při platbě na internetu si dávejte pozor, kam svá data karty zadáváte. Využívejte bezpečné placení přes internetové bankovnictví či bezpečné platební metody jako je například PayPal.
- **Hlídejte si posty –** Obsah, který na internet nahrajete s největší pravděpodobností už na internetu zůstane a půjde dohledat. Dávejte si tedy pozor a před zveřejněním obsahu na internet se zamyslete, zda můžete uškodit sobě, rodině, kariéře atd.
- **Dbejte opatrnosti při seznamování –** Nevěřte každému, s kým si na internetu píšete. Dokud se s člověkem osobně nesetkáte, tak nesdělujte své citlivé informace, neposílejte peníze, obnažené fotografie atd., nikdy netušíte, kdo je na druhé straně monitoru a zda těchto informací a prostředků později nevyužije proti vám.
- **Hlídejte antivirus –** Pravidelně aktualizujte antivirový program, to samé platí i pro aplikace které využíváte.

## 4.4 Digitální stopa

Digitální stopou nazýváme záznamy o činnosti, které po sobě zanechává každý uživatel při aktivitách ve virtuálním prostoru. Tento fakt by si mě každý uživatel uvědomit. Tyto informace jsou dále ukládány na lokální i síťová zařízení (počítače, notebooky, mobilní telefony, servery, televize atd.). Digitální stopou nazýváme i jakýkoliv obsah, který byl uživatelem publikován na sociálních sítích, webových stránkách, odeslaném e-mailu atd. Digitální stopu si můžeme rozdělit na dva druhy, a to digitální stopu aktivní a pasivní. Aktivní digitální stopou jsou myšleny záznamy vzniklé vědomou činností (příspěvky na sociálních sítích, publikace na weby, e-mailové komunikace atd.). Pasivní digitální stopou jsou myšleny záznamy spojené s vědomou činností (IP adresy, vyhledávané výrazy, navštívené webové stránky atd.). Mějte na paměti, že většina vašich aktivit v online prostředí není anonymní. Data získaná z vašeho chování na internetu, mohou být následně zneužita k marketingovým účelům či počítačové kriminalitě.[72]

[72] INTERNETEM BEZPEČNĚ *Co je digitální stopa?* (online) (11.04.2022) Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/

# II. PRAKTICKÁ ČÁST

# 5. Výzkumné šetření

V teoretické části této bakalářské práce, se autor zabýval vymezení pojmu internet, sociální sítě, mládeže a rizik která v dnešním moderním světě mohou hrozit. Především mládež si neuvědomuje možná rizika komunikace na síti. Dále autor nastínil téma kybernetické hrozby a hlavní zásady zajištění ochrany informací. V empirické části této bakalářské práce, bylo realizováno výzkumné dotazníkové šetření, za účelem zjištění, s jakými bezpečnostními riziky se respondenti setkali, zda mají negativní zkušenost, jestli se respondenti cítí závislí na sociálních sítí a otázkou, jakým způsobem mají svá data a účty zabezpečeny.

V následujících podkapitolách se nacházejí všechny podrobnosti výzkumného šetření. Jeho cíle, metodika, charakteristika sledované školy a studentů. Na konci empirické části této bakalářské práce se nachází celkové shrnutí výsledků z výzkumného šetření, které je obsaženo v závěru celé práce.

## 5.1 Výzkumné cíle

Předmětem empirické části bakalářské práce je zjištění, jak je velký rozsah znalostí mladistvých studentů vybrané střední školy o rizicích, vyplývajících z aktivního užívání sociálních sítí a kybernetické bezpečnosti. Dále zjištění, zda mají studenti negativní zkušenost spojenou se sociálními sítěmi a kybernetickou bezpečností. Součástí výzkumu je zjištění, zda studenti šetření mají povědomí o rizicích, či se již dokonce s některými riziky osobně setkali. Zjištění, možného pocitu závislosti samotných respondentů a zda studenti vhodně zabezpečují svá zařízení a vytvořené profily.

Autor následně stanovil čtyři předpoklady, které znějí následovně:

- **Předpoklad č.1** - Více jak 50 % respondentů tráví na internetu více jak 3 hodiny denně.
- **Předpoklad č.2** - Alespoň 50 % respondentů si přijde závislá na internetu.
- **Předpoklad č.3** -Lze předpokládat, že 60 % respondentů má obavy, že by se mohli stát obětí počítačové kriminality.
- **Předpoklad č.4** - Méně jak 10 % respondentů svá data zabezpečená vůbec nemá.

## 5.2 Metodika výzkumného šetření a popis výzkumného nástroje

Autor práce při volbě kvantitativního výzkumu vycházel z toho, co uvádí ve své publikaci Gavora (2000). Gavora hovoří o tom, že „*kvantitativní výzkum pracuje s číselnými údaji. Zjišťuje množství, rozsah nebo frekvenci výskytů jevů, resp. jejich míru (stupeň). Číselné údaje se dají matematicky zpracovat. Je možno je sčítat, vypočítat jejich průměr, vyjádřit je v procentech nebo použít další metody matematické statistiky*.“[73]

V této práci jsou výsledky vyjádřeny prostřednictvím absolutních a relativních četností. Ty jsou následně autorem práce zaznamenány a předkládány do přehledných grafů či tabulek. Za účelem získání informací si autor zvolil vzhledem ke kvantitativní povaze anonymní dotazníkové šetření vlastní tvorby. Tento typ anonymního dotazníku umožnil respondentům otevřeně a bez obav prezentovat své názory, zkušenosti a postoje. Celý dotazník byl zpracován v online podobě, a to prostřednictvím internetové služby Survio.com. Při tvorbě otázek autor vycházel z informací, které jsou vystiženy a přiblíženy v teoretické části bakalářské práce. Tento dotazník se skládá z 21 otázek, kdy převládá varianta uzavřených otázek. Některé otázky mají charakter prosté dichotomické odpovědi ano-ne, anebo výběrové a výčtové odpovědi.

Otázka č. 1 a 2 byly úvodními otázkami na pohlaví a věk. Následovala otázka č.3 která dotazovala na čas strávený denně na internetu. Otázka č.4 byla zaměřena na komunikační technologie a jejich využití u mladistvých. Následující otázka č.5 se respondentů ptala, na co nejvíce využívají internet. Otázky č.6, 9 a 10 byly zaměřeny na sociální sítě a zadávání citlivých údajů na své veřejné profily. U otázek č.7 a 8 respondenti odpovídali na pocitu závislosti sebe a jejich okolí na internetu. Osobními údaji a poskytnutí těchto údajů cizí osobě se zaobírají otázky č.11 a 12. Následující otázky č.13 a 14 jsou zaměřeny na povědomí rodičů o aktivitě svých dětí na internetu a úhlu pohledu respondentů na kontrolu aktivity od rodičů. Otázky č. 15, 16 a 17 byly zaměřeny na rizika sociálních sítí, zdali se respondenti, nebo někdo z jejich okolí s některými již v minulosti setkali, zdali mají respondenti obavy z možného napadení a jak by takové riziko řešili. U otázky č.18 se respondentů autor ptá na osobní zkušenost s vložením nevhodného obsahu na sociální sítě. Otázky č.19, 20 a 21 byly zaměřeny na zabezpečení citlivých údajů a zdali jsou tyto údaje zadávány při využívání veřejných sítí.

[73] GAVORA, Peter. *Úvod do pedagogického výzkumu*. Brno: Paido, 2000. Edice pedagogické literatury. s. 31. ISBN 80-85931-79-6.

## 5.3 Charakteristika sledované školy a popis výzkumného vzorku

Výzkum byl realizován na odborné Střední škole podnikání a mediální tvorby Kolín s.r.o... Tato škola působila dříve jako základní umělecké učiliště, a to od roku 1992. Od roku 1996 se škola nachází v areálu pana Procházky, se kterým se škola dohodla. V tomto roce se škola změnila a působila nadále jako Střední odborná škola. Na této škole je možné studovat ekonomiku a podnikání, obalovou techniku, informační technologie, fotografickou tvorbu, grafický design a požární ochranu. Všechny tyto obory, jsou zakončeny maturitní zkouškou.

Na této škole působí 46 pedagogických pracovníků společně s 6 asistenty pedagoga. Studuje zde cca 300 žáků kteří mají přístup do tří počítačových učeben, jazykové učebny, dvěma ateliérům, dvěma fotografickým koutkům, filmové střižny a momentálně se dokončuje i grafické studio. Tato škola je taktéž bezbariérová a nabízí studium vozíčkářům a mentálně postiženým dětem, které mají svůj doprovod, nebo může být poskytnut školou.

Na toto výzkumné šetření byli vybráni studenti OSSP z důvodu rozmanitosti oborů a četného zastoupení dívek i chlapců. Dalším důvodem bylo, že většina těchto oborů je spjata s informačními a komunikačními technologiemi. Z pohledu metodologie výzkumného šetření vykazuje soubor atributy záměrného výběru na základě dostupnosti. Z teorie této bakalářské práce víme, že dospívající jsou ohroženou skupinou vzhledem k nižší sebereflexi, zkušenostem a s ohledem na to, že využívají internet téměř pořád a jsou tak rizikům více vystaveni než dospělý člověk v produktivním věku.

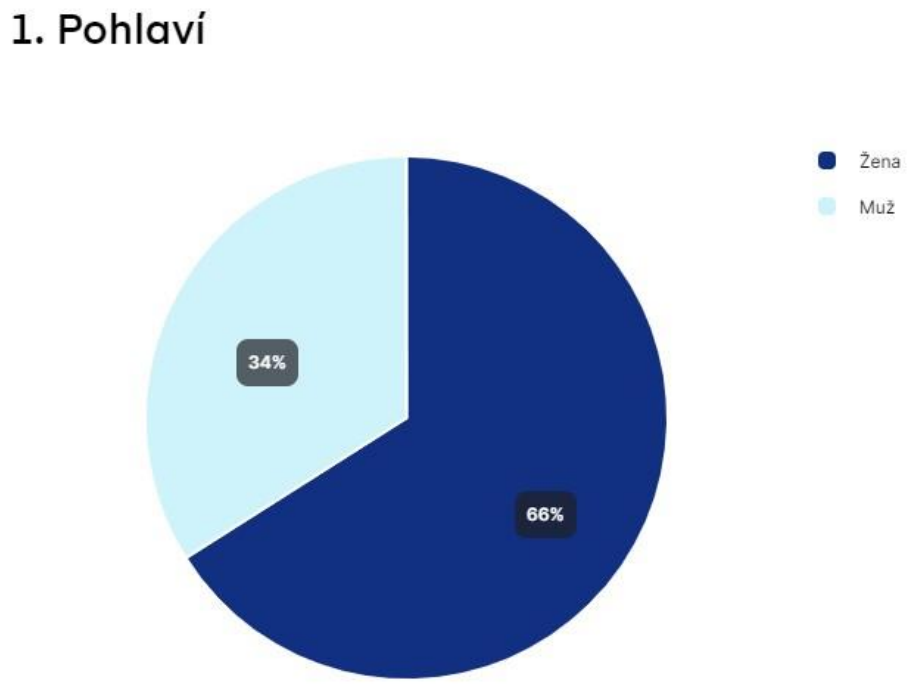
## 5.4 Výsledky výzkumného šetření

Výzkumné šetření proběhlo v polovině měsíce dubna 2022. Před tímto obdobím jsem kontaktovala ředitelku školy OSSP, zda by bylo možné realizovat výzkumné šetření pro účel mé bakalářské práce. Dotaz byl s informací, že je dotazník realizován zcela anonymně v online podobě. Dostalo se mi tedy svolení rozeslání dotazníku mezi všechny studenty této školy.

Výsledky výzkumného šetření jsou znázorněny zobrazením do grafů a tabulek se slovním popisem. Kapacita mého online dotazníku činila 100 respondentů. Z tohoto počtu jich bylo vyplněno 92. Konečný počet dotazníků s řádným vyplněným tedy činil 92 dotazníků, tj. 92 %.

**Otázka č.1: Pohlaví**

Tato otázka je úvodem tohoto dotazníku. Z 92 odpovědí studentů na otázku č.1 vyplývá, že dotazníkové šetření vyplnilo 61 respondentek a 31 respondentů střední odborné školy, procentuálně to je tedy 66 % dívek a 34 % chlapců.

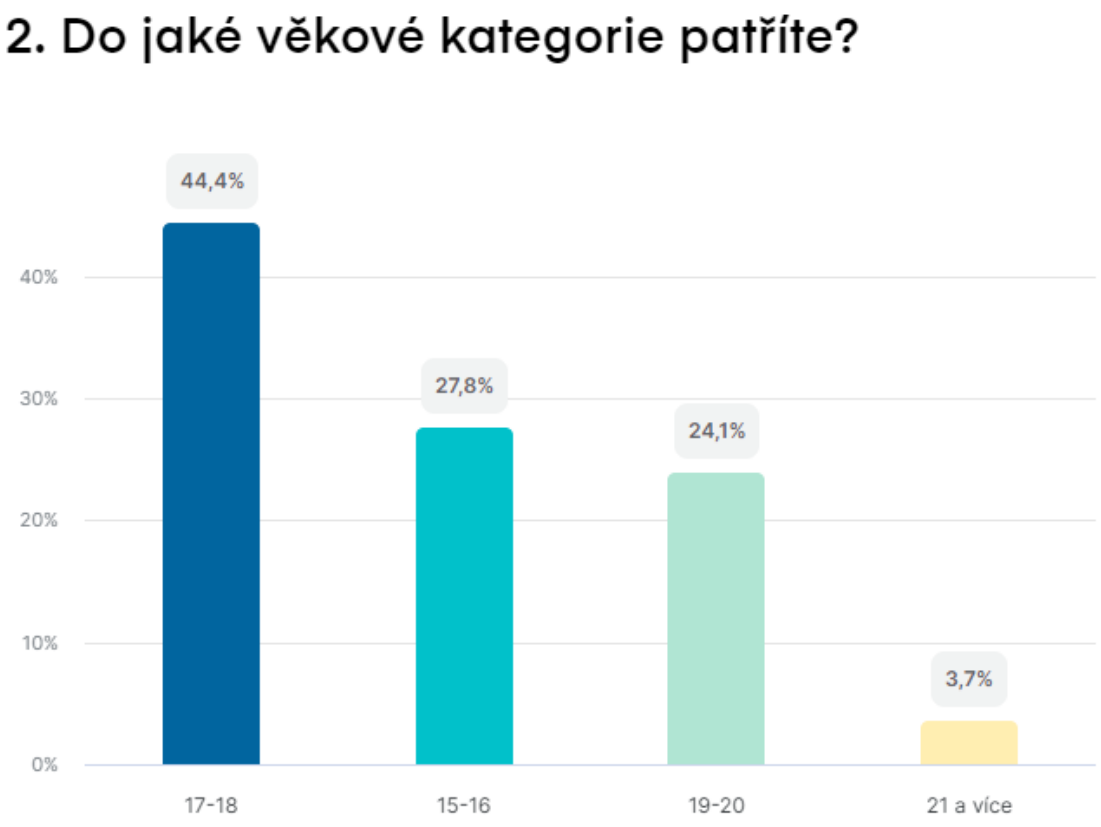



Obrázek 2: Graf 1: Pohlaví studentů
Zdroj: výsledek vlastního výzkumu 2022

**Otázka č.2: Do jaké věkové kategorie patříte?**

Dotazníkové šetření bylo provedeno na střední odborné škole, tudíž všichni respondenti spadali do věkové skupiny starší jak 15 let. Tato otázka měla pouze přiblížit, kolik respondentů již dosáhlo dospělosti.

Dle výsledků vidíme, že nejvíce zastoupenou věkovou skupinou jsou studenti ve věku 17-18 let, kteří tvoří 44,4 % z celkového počtu dotazovaných studentů. Poté je zde skupina 15-16 let která tvoří 27,8 % a skupinu 19-20 let respondentů s 24,1 % odpovědí. Zbylá 3,7 % jsou studenti starší 21 let.



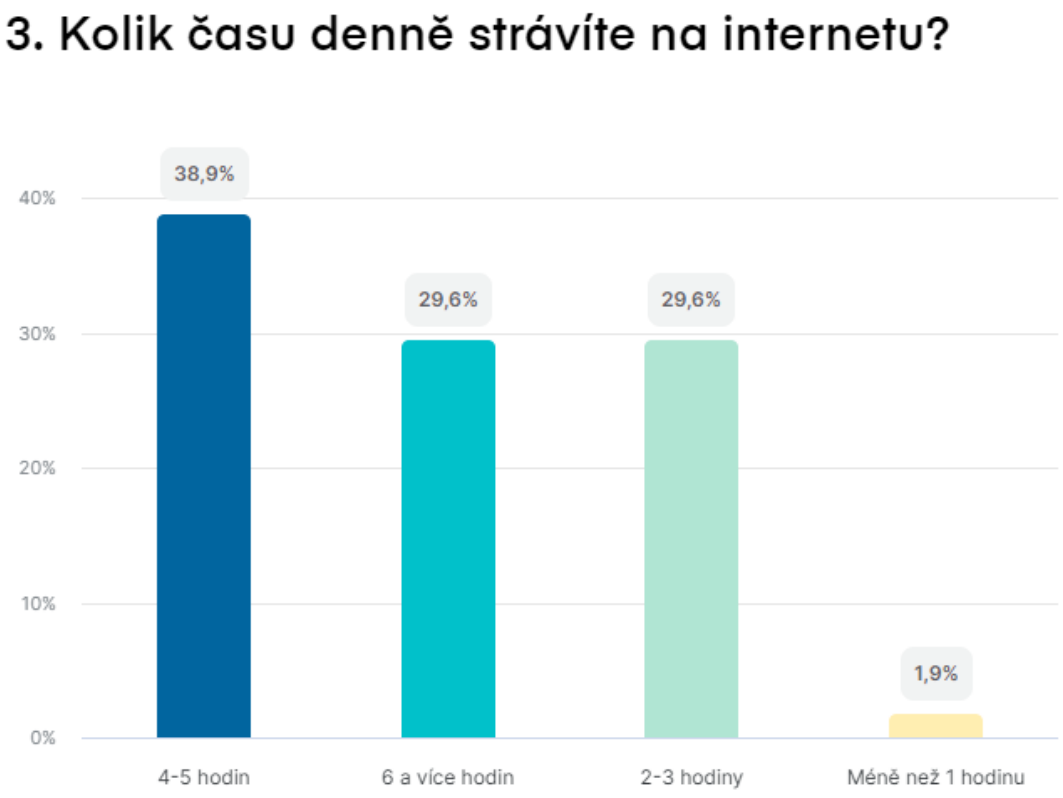

Obrázek 3: Graf 2: Věk studentů
Zdroj: výsledek vlastního výzkumu 2022

**Otázka č.3: Kolik času denně strávíte na internetu?**

Otázka č.3 vycházela z předpokladu č.1, který zněl: „Více jak 50 % *respondentů tráví na internetu více jak 3 hodiny denně*“.

Z grafu lze vyčíst že studenti tráví na internetu nejčastěji 4-5 hodin (celkem tedy 38,9 % z nich). 2–3 hodiny tráví každodenně na internetu 29,6 % dotázaných respondentů. Dokonce 29,6 % dotazovaných respondentů tráví na internetu 6 a více hodin denně. Nejméně častou odpovědí bylo méně než 1 hodinu, kterou zvolilo pouze 1,9 % respondentů.

Otázka č.7 a č.8 se dotazuje respondentů na závislost na sociálních sítích, internetu a jestli si sami přijdou závislí. Ovšem mnoho mladistvých nevyužívá internet pouze pro zábavu, ale i jako studijní prostředek a prostředek ke sběru informací a dalšímu vzdělání.




Obrázek 4: Graf 3: Čas strávený na internetu
Zdroj: výsledek vlastního výzkumu 2022

**Otázka č.4: Jaké komunikační technologie nejvíce používáte?**

Otázka č.4 se respondentů ptá, jaké komunikační technologie nejvíce využívají pro komunikaci a k práci na internetu. U této otázky měli respondenti možnost napsat svou odpověď. Z Word cloudu vyplývá, že nejčastěji využívanou komunikační technologie je mobilní zařízení, notebook a stolní počítač.

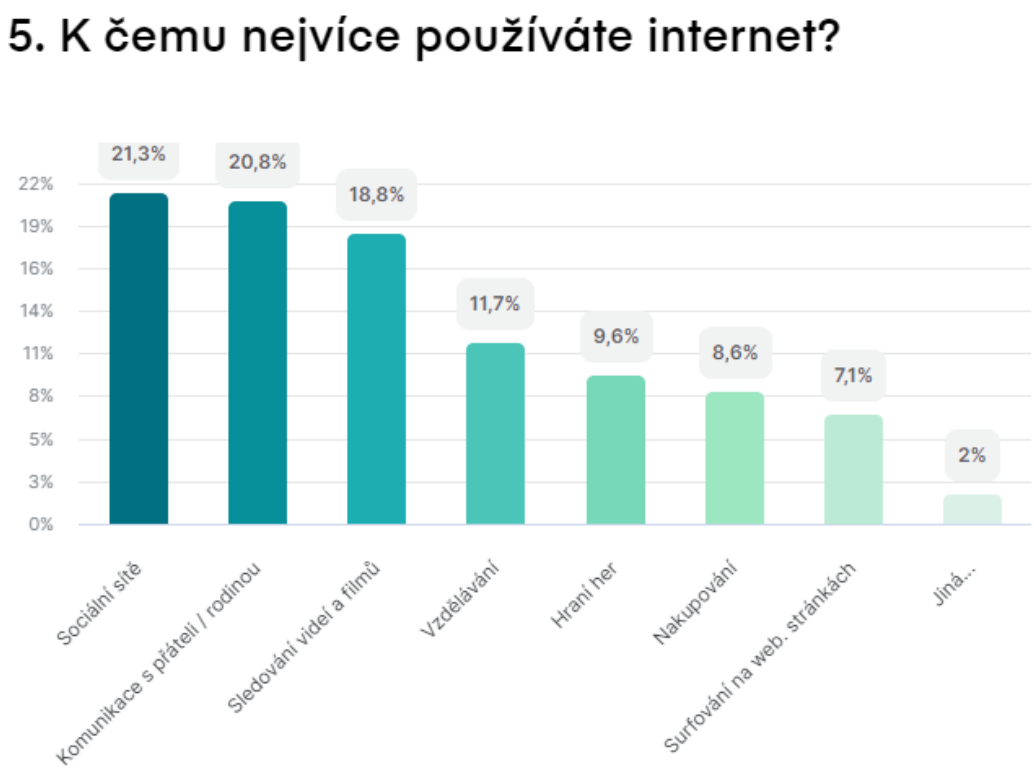
V dnešní moderní době je normální, že díky mobilním zařízením máme možnost být stále „online“ a máme tak přehled o veškerém dění kolem nás.


Obrázek 5: Word Cloud 1: Komunikační technologie
Zdroj: výsledek vlastního výzkumu 2022

**Otázka č.5: K čemu nejvíce používáte internet?**

Tato otázka se respondentů ptá, k čemu převážně využívají internet. U této otázky měli respondenti možnost vybrat více odpovědí. Z grafu č.4 vyplývá, že nejčastější aktivitou jsou sociální sítě s 21,3 %, komunikace s přáteli či rodinou s 20,8 % a 18,8 % odpovědí respondentů bylo pro sledování videí a filmů.

Vzdělávání označilo 17,7 %, hraní her 9,6 %, nakupování 8,6 %, surfování na web. Stránkách 7,1 % a 2 % dotazovaných respondentů označilo možnost jiná.



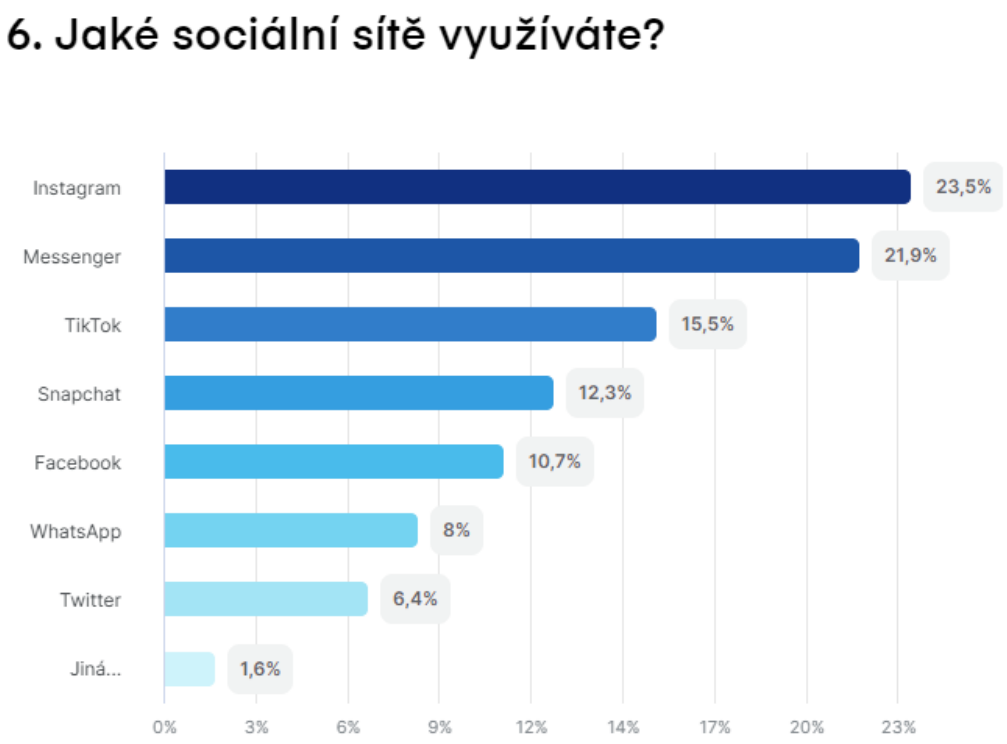

Obrázek 6: Graf 4: Využití internetu
Zdroj: výsledek vlastního výzkumu 2022

**Otázka č.6: Jaké sociální sítě využíváte?**

Na následujícím grafu č.5 lze vidět, které sociální sítě respondenti znají a využívají. U této otázky měli respondenti možnost vybrat více odpovědí.

Mezi nejvíce využívané sociální sítě se zařadil Instagram, Messenger, Tiktok a Snapchat. Při čemž Instagram využívá 23,5 %, Messenger 21,9 %, TikTok 15,5 % a Snapchat 12,3 % dotazovaných respondentů.

Naopak mezi nejméně používané se zařadil Twitter s 6,4 %, WhatsApp 8 % a Facebook 10,7 %. Možnost jiná využilo 1,6 % dotazovaných respondentů.

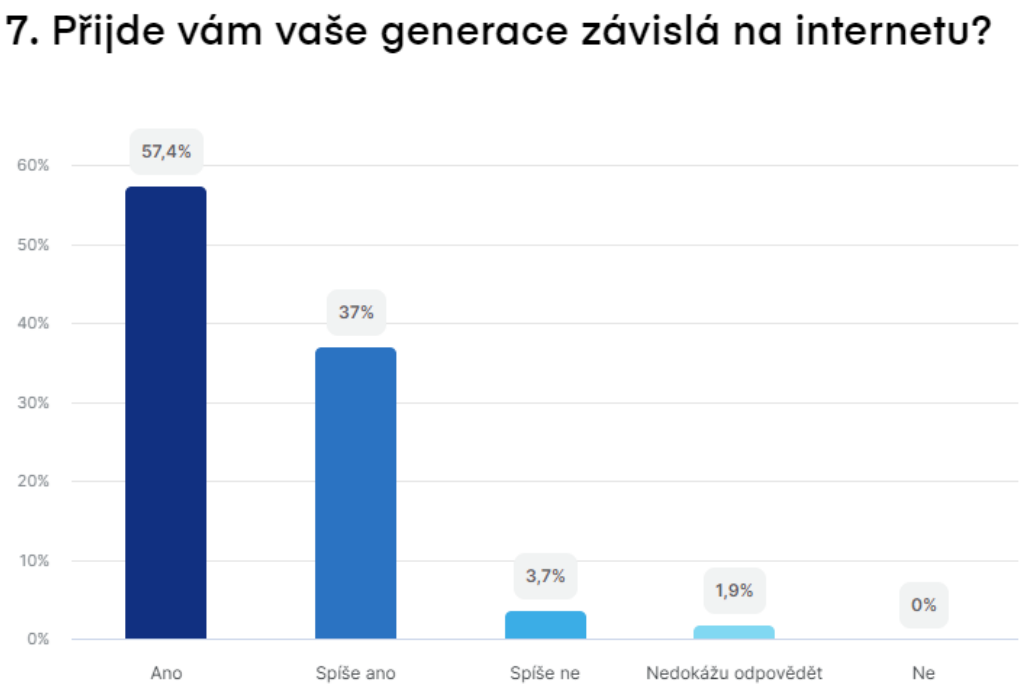



Obrázek 7: Graf 5: Sociální sítě
Zdroj: výsledek vlastního výzkumu 2022

**Otázka č.7: Přijde vám vaše generace závislá na internetu?**

Tato otázka měla zjistit, jak vnímají dotazovaní respondenti dnešní závislost na internetu u svých vrstevníků. V dnešním moderním světě, je téměř každý „online“ a to hlavně díky mobilním zařízením. Z využívání internetu ať už pro sociální sítě, hledání informací či hraní her, lze vybudovat závislost.

V této otázce jasně dominuje možnost ano, tuto možnost označilo 94,4 % dotazovaných respondentů a pouze 3,7 % odpovědělo možnost ne. Také je zde 1,9 % odpovědí pro možnost nedokážu odpovědět.

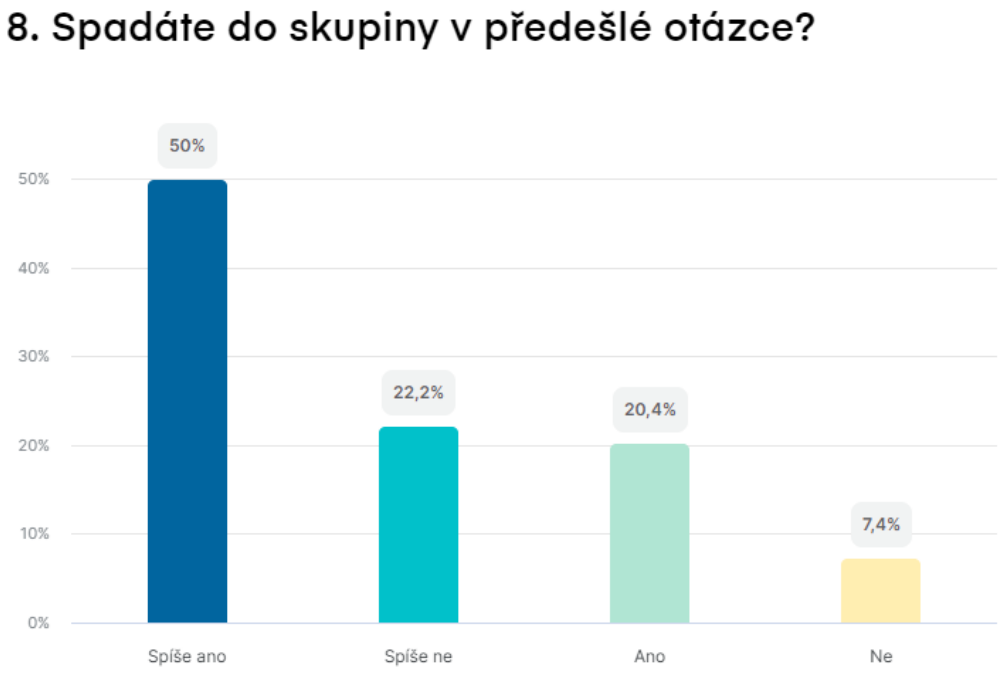



Obrázek 8: Graf 6: Přijde vám vaše generace závislá na internetu?
Zdroj: výsledek vlastního výzkumu 2022

**Otázka č.8: Spadáte do skupiny v předešlé otázce?**

Otázka č.8 vycházela z předpokladu č.2, který zněl: „*Alespoň 50 % respondentů si přijde závislá na internetu*“. A také navazuje na otázku č. 7.

V otázce č. 7 se respondenta autor ptá, zda si myslí, že je dnešní mladá generace závislá na internetu. V této otázce č.8 se tedy autor zaměřil na samotného respondenta, zdali se on sám cítí závislý na internetu. Odpověď ano zde označilo 70,4 % dotazovaných respondentů a 29,6 % označilo odpověď ne.

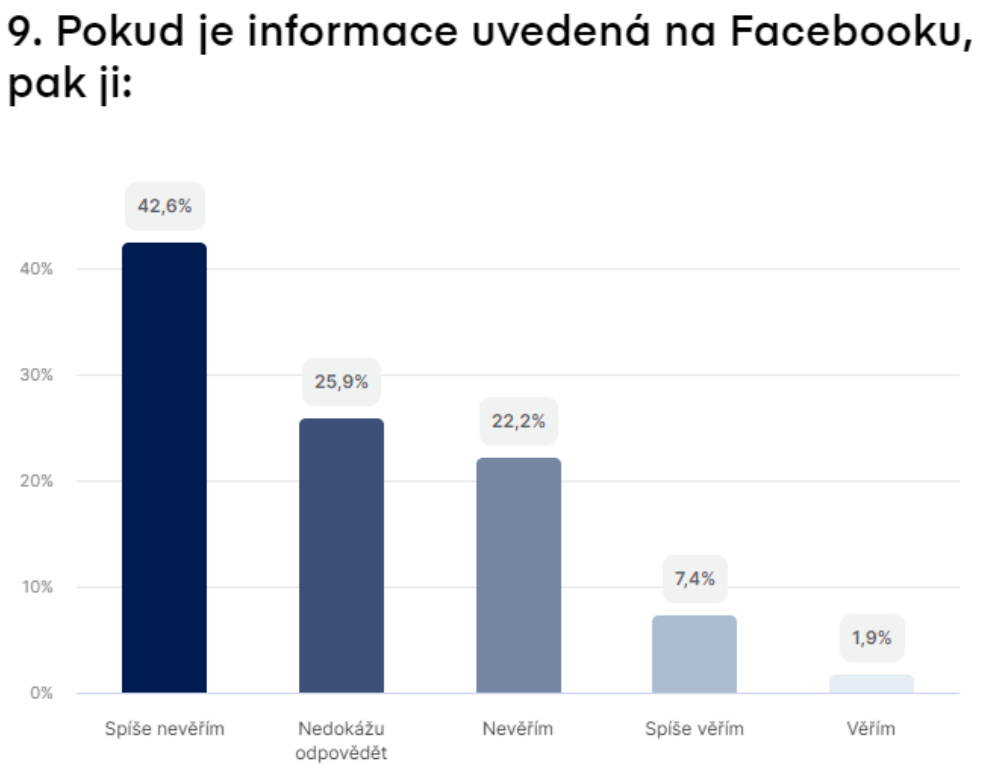



Obrázek 9: Graf 7: Spadáte do skupiny v předešlé otázce?
Zdroj: výsledek vlastního výzkumu 2022

**Otázka č.9: Pokud je informace uvedená na Facebooku, pak ji:**

Otázka č.9 je zaměřena na důvěru respondentů k informacím uvedeným na sociální síti Facebook. Veškeré informace uvedené na internetu by si každý uživatel měl ověřit minimálně ze dvou spolehlivých zdrojů.

Z výsledného grafu č.9 lze vyčíst, že informaci uvedené na Facebooku 64,8 % respondentů nevěří a pouze 9,3 % této informaci věří. 25,9 % dotazovaných respondentů zvolilo možnost nedokážu odpovědět.

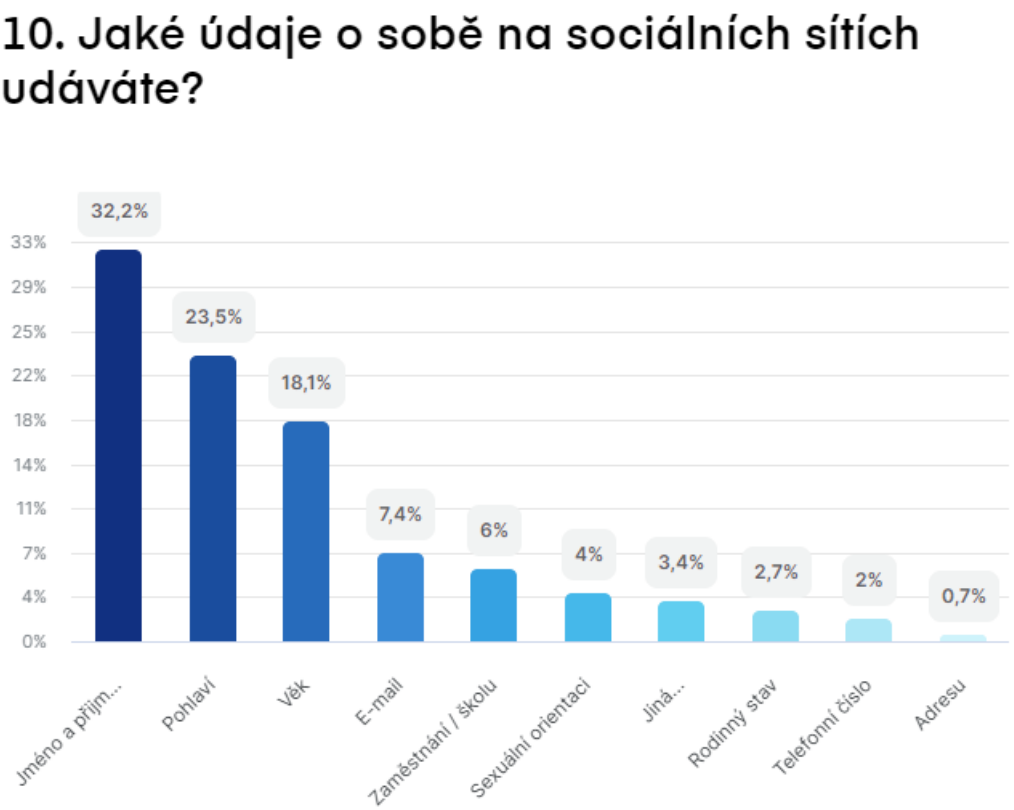



Obrázek 10: Graf 8: Informace na Facebooku
Zdroj: výsledek vlastního výzkumu 2022

**Otázka č.10: Jaké údaje o sobě na sociálních sítích udáváte?**

Otázka č.10 se zabývá osobními údaji, které si respondenti udávají veřejně na své sociální sítě. U této otázky měli respondenti možnost vybrat více odpovědí.

Mezi nejvíce udávané osobní údaje, které o sobě na sociálních sítích studenti uvádějí, patří především jméno a příjmení, které uvádí 32,2 % respondentů, dále je pohlaví 23,5 % a věk 18,1 %. Dále je zde e-mail, který uvádí 7,4 %, zaměstnání nebo školu uvádí 6 % a sexuální orientaci uvádí 4 % dotazovaných respondentů. Naopak údaje, které uvádí jen malé procento je rodinný stav 2,7 %, telefonní číslo 2 % a adresa, kterou uvádí jen 0,7 % respondentů. V této otázce byla možnost zvolit variantu jiná…, kterou nakonec zvolilo 3,4 % respondentů. Každý uživatel sociálních sítí, by si měl dávat pozor na to, jaké informace o sobě veřejně udává.




Obrázek 11: Graf 9: Osobní údaje na sociálních sítích

Zdroj: výsledek vlastního výzkumu 2022

**Otázka č.11: Vadí vám si na sociální síti psát s cizími lidmi?**

Následující tabulka č.1 ukazuje počet studentů, kterým vadí psát si na sociálních sítích s cizími lidmi. Komunikace s cizími lidmi na sociálních sítích s sebou nese jistá rizika a studenti by je měli mít v povědomí. Taková to komunikace může vést k nepříjemným situacím.

Výsledek tohoto šetření vyšel vskutku zajímavě, a to přesně poměrem 46 odpovědí pro ano a 46 odpovědí pro ne. Procentuální znázornění je tedy 50 % odpovědí pro ano a 50 % odpovědí pro ne.

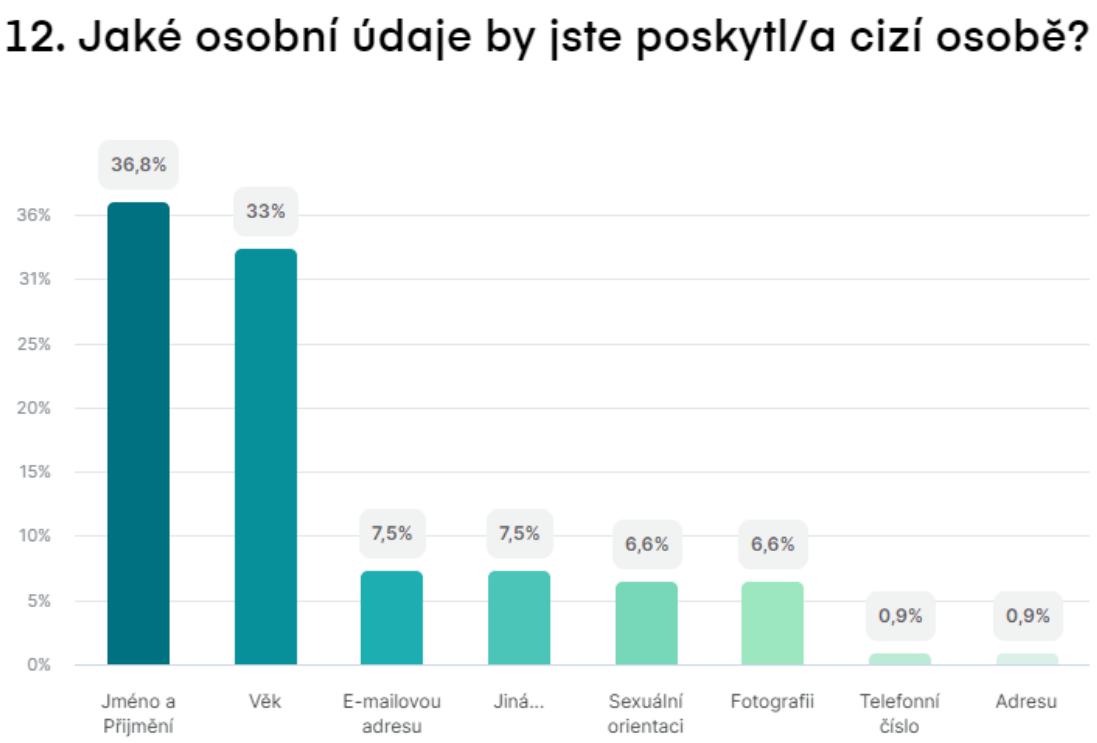

Tabulka 1: Psaní s cizími lidmi

Zdroj: výsledek vlastního výzkumu 2022

**Otázka č.12: Jaké osobní údaje byste poskytl/a cizí osobě?**

Tato otázka navazuje na otázku č.11, která pojednává o psaní si s cizími lidmi. V této otázce se studentů autor ptá, jaké osobní údaje jsou schopni poskytnou cizí osobě. U této otázky měli respondenti možnost vybrat více odpovědí.

Mezi nejvíce udávané osobní údaje, které jsou respondenti ochotni poskytnou cizí osobě patří jméno a příjmení 36,8 % a věk respondenta 33 %. Dále je zde e-mailová adresa 7,5 %, jiná… 7,5 %, sexuální orientace 6,6 % a fotografie 6,6 %. Mezi nejméně udávané osobní informace patří telefonní číslo 0,9 % a adresa 0,9 %.

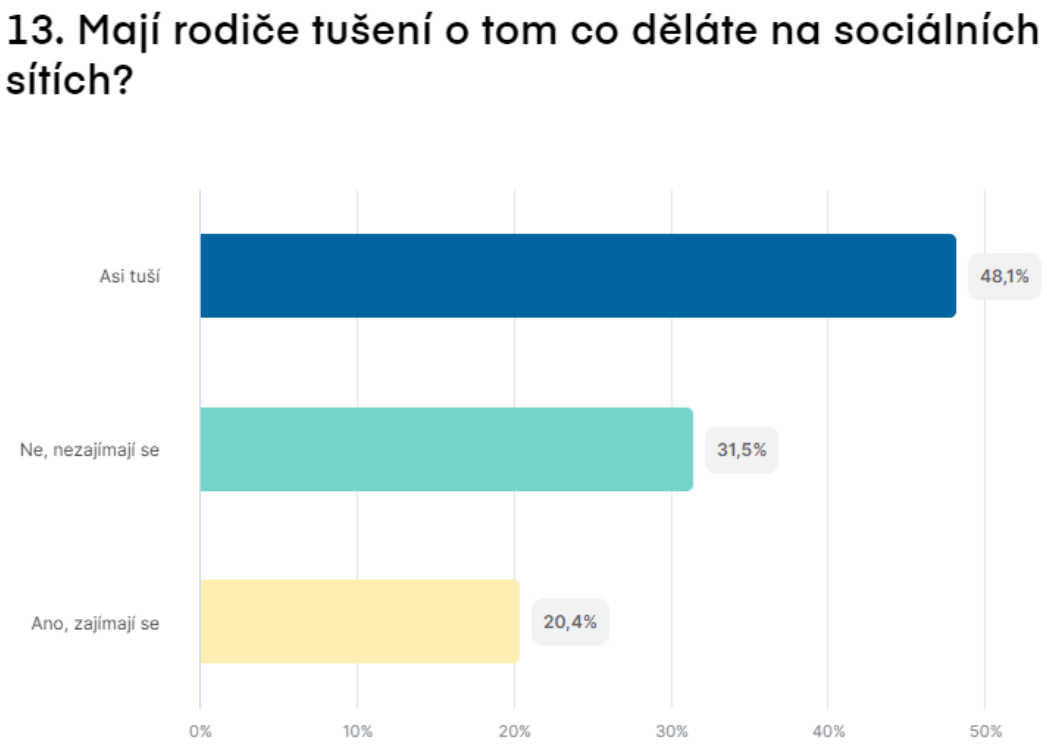



Obrázek 12: Graf 10: Osobní údaje poskytnuté cizí osobě
Zdroj: výsledek vlastního výzkumu 2022

**Otázka č.13: Mají rodiče tušení o tom, co děláte na sociálních sítích?**

Tato otázka byla zaměřena na to, zda rodiče mají povědomí o aktivitách svých dětí na sociálních sítích. O různých možnostech, jak rodiče řeší kontrolu svých dětí na sociálních sítích, se dá spekulovat. Můžeme zde mluvit o rodičovské kontrole a sledování historie činnosti dítěte na počítači.

Na tuto otázku odpovědělo 48,1 % respondentů že rodiče pravděpodobně tuší co na sociálních sítí dělají. 31,5 % respondentů uvedlo, že se jejich rodiče nezajímají o jejich aktivitu a pouhých 20,4 % dotazovaných respondentů zvolilo možnost ano, zajímají se.



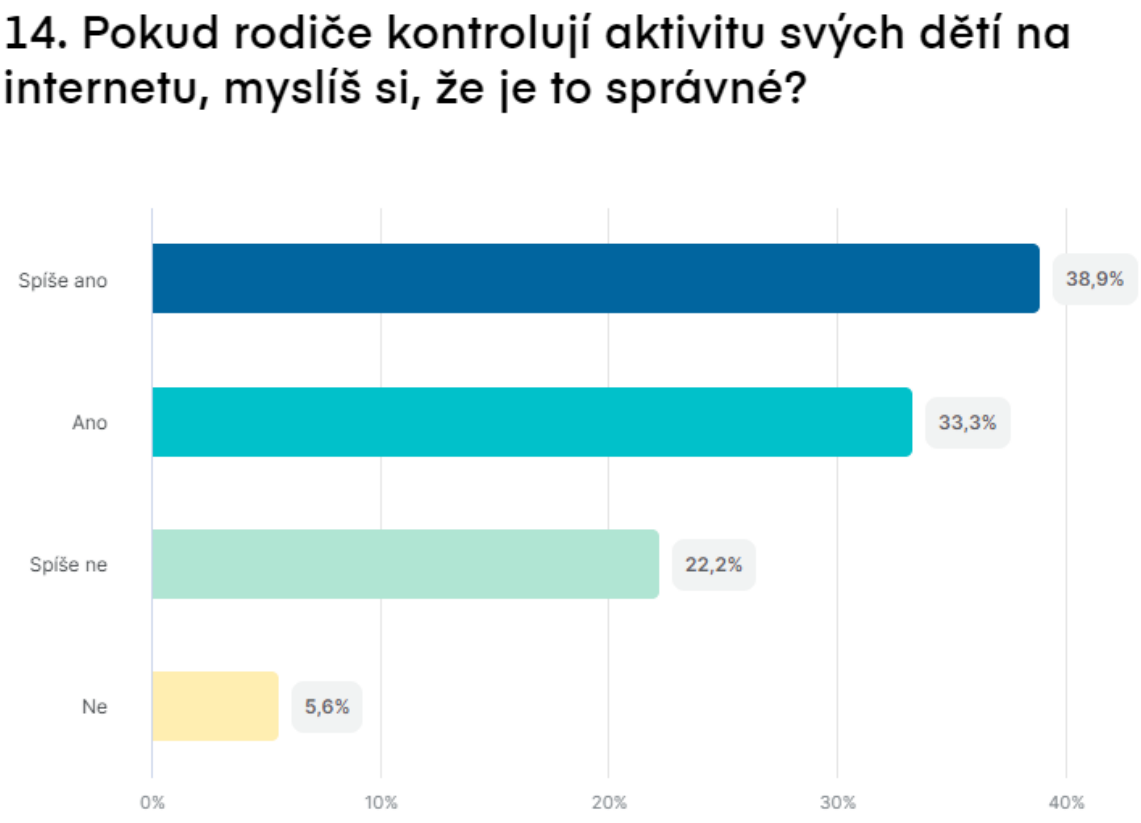

Obrázek 13: Graf 11: Mají rodiče tušení, co děláte na sociálních sítích?
Zdroj: výsledek vlastního výzkumu 2022

**Otázka č.14: Pokud rodiče kontrolují aktivitu svých dětí na internetu, myslíš si, že je to správné?**

Tato otázka navazuje na otázku č.13 a byla orientována na zjištění, zda respondenti souhlasí s rodičovskou kontrolou aktivity na sociálních sítích u svých dětí.

Z 92 dotazovaných respondentů hlasovalo 61,2 % pro odpověď spíše ano. Důvody této odpovědi mohou být různé, například ohledem dětské bezpečnosti, včasné prevenci a zabránění počátku kybernetického rizika.

27,8 % dotazovaných respondentů zvolilo možnost odpovědi ne a nemyslí si, že kontrola aktivity dětí na internetu od rodičů je správná. Důvody této odpovědi mohou být např. narušení jejich soukromí.



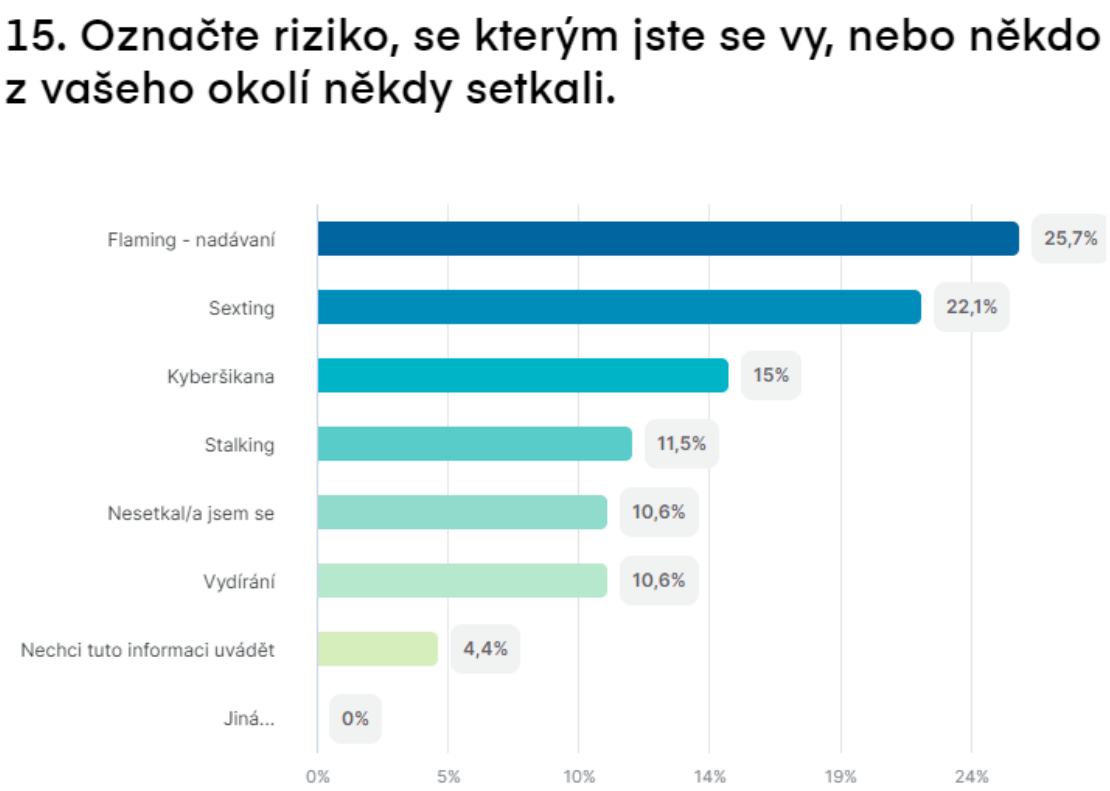

Obrázek 14: Graf 12: Kontrola rodičů dětí na internetu

Zdroj: výsledek vlastního výzkumu 2022

**Otázka č.15: Označte riziko, se kterým jste se vy, nebo někdo z vašeho okolí někdy setkali.**

U této otázky měli respondenti možnost vybrat více odpovědí. Mezi rizika, se kterými se dotazovaní respondenti, nebo někdo z jejich okolí někdy setkali, patří na prvním místě flaming s 25,7 %, dále sexting s 22,1 %, kyberšikana s 15 % a stalking s 11,5 % odpovědí. 10,6 % dotazovaných respondentů se s riziky nikdy nesetkala a 10,6 % respondentů byla vydírána. Znepokojující je fakt že 4,4 % dotazovaných respondentů nechce tuto informaci uvádět.

Rizika na sociálních sítích a internetu jsou znepokojivé téma a každý kdo se s jedním z těchto rizik někdy v životě setkal, si může nést psychické následky. Jak už autor uvádí v teoretické části této bakalářské práce, jakákoliv zkušenost s jedním z těchto rizik může mít velmi špatné následky, obzvlášť u mládeže.




Obrázek 15: Graf 13: Rizika, se kterými jste se setkali

Zdroj: výsledek vlastního výzkumu 2022

**Otázka č.16: Máte obavy, že byste se mohl/a stát obětí počítačové kriminality?**

Otázka č.16 byla zaměřena na obavy z možnosti se stát obětí počítačové kriminality. Tato otázka vycházela z předpokladu č.3, který zněl: „*Lze předpokládat, že 60 % respondentů má obavy, že by se mohlo stát obětí počítačové kriminality*“.

Z tabulky č.2 vyšel překvapující výsledek, a to že 37 % dotazovaných respondentů ani nepřemýšlelo o možnosti stát se obětí počítačové kriminality. Otázkou zůstává, zda o této možnosti nepřemýšleli z pocitu dostatečného zabezpečení, či proto, protože nejsou o možných rizicích dostatečně informováni. Obavy se stát obětí má 24,1 % respondentů, 20,4 % respondentů obavy nemá a zbylých 18,5 % nedokáže na tuto otázku odpovědět.

16. Máte obavy, že byste se mohl/a stát obětí počítačové kriminality?

| ODPOVĚĎ | RESPONZÍ | PODÍL |
|---|---|---|
| Nepřemýšlel/a jsem nad tím | 34 | 37% |
| Ano | 22 | 24.1% |
| Ne | 19 | 20.4% |
| Nedokážu odpovědˇ | 17 | 18.5% |

Tabulka 2: Obavy z počítačové kriminality

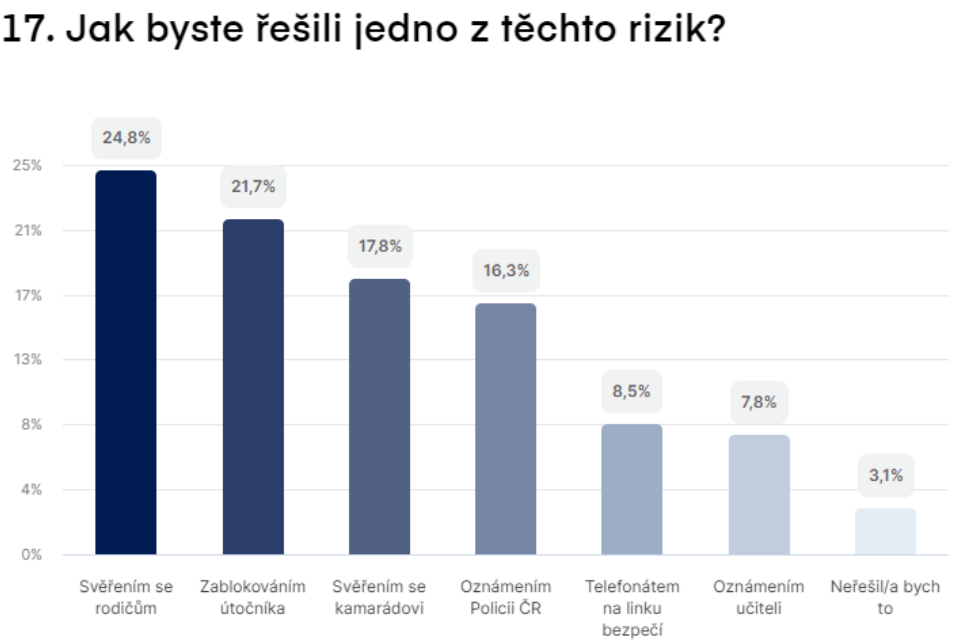
Zdroj: výsledek vlastního výzkumu 2022

**Otázka č.17: Jak byste řešili jedno z těchto rizik?**

Tato otázka vznikla na základě otázek č.15 a č.16. Cílem této otázky bylo zjistit, jak by respondenti řešili jedno z těchto rizik. U této otázky měli respondenti možnost vybrat více odpovědí.

Největší procento dotazovaných respondentů by se svěřilo rodičům, učinilo by tak 24,8 %. Druhou nejvíce využitou možností by bylo samotné zablokování útočníka, tak by učinilo 21,7 % dotazovaných respondentů. Ovšem u tohoto kroku si musíme dávat pozor, pokud bychom chtěli později toto riziko řešit a přijít s policií, kdo je útočníkem a zabránit mu v této aktivitě, nesmějí nám chybět data. Tím chce autor říct, že zablokováním útočníka, můžete přijít o důležité důkazy k možnému dopadení útočníka. 17,8 % respondentů by se svěřila svému kamarádovi, 16,3 % by tento incident nahlásila na policii, 8,5 % by zavolalo na linku bezpečí a 7,8 % dotazovaných respondentů by se svěřilo s tímto problémem svému učitelovi. Znepokojivé je 3,1 % respondentů kteří by toto riziko neřešili.

Samozřejmě u každého rizika záleží na intenzitě, jak už autor zmiňoval v teoretické části této bakalářské práce, každé z těchto rizik nelze brát na lehkou váhu. Je potřeba mládež informovat o možných rizicích a rozšířit povědomí o tomto problému, o tom, kam až tato problematika může zajít a jaké to může mít následky.




Obrázek 16: Graf 14: Jak byste řešili tato rizika?
Zdroj: výsledek vlastního výzkumu 2022

**Otázka č.18: Máte osobní zkušenost s vložením nevhodného obsahu na sociální sítě?**

Tato otázka byla zaměřena na osobní zkušenost dotazovaných respondentů s vložením nevhodného obsahu na sociální sítě. Nejvíce dotazovaných respondentů zvolilo možnost odpovědi ne a to 68,5 %. Odpověď ano zvolilo 20,4 % a 11,1 % respondentů zvolilo možnost nechci tuto informaci uvádět.

Studenti by měli být obeznámeni s fakty, že jakýkoliv obsah, který na sociální sítě vloží, tam zůstane zachován a může být i zneužit.

18. Máte osobní zkušenost s vložením nevhodného obsahu na sociální sítě?

| ODPOVĚĎ | RESPONZÍ | PODÍL |
|---|---|---|
| Ne | 63 | 68.5% |
| Ano | 19 | 20.4% |
| Nechci tuto informaci uvádět | 10 | 11.1% |

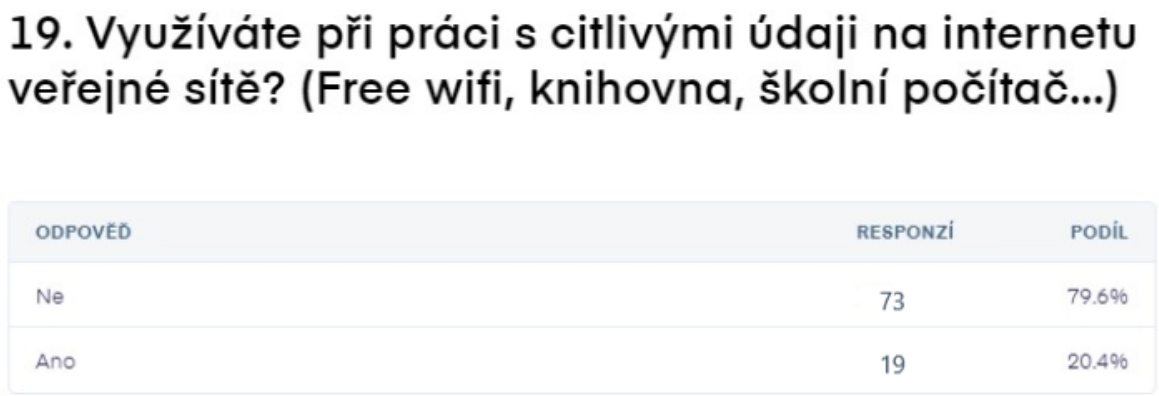
Tabulka 3: Osobní zkušenost s nevhodným obsahem

*Zdroj: výsledek vlastního výzkumu 2022*

**Otázka č.19: Využíváte při práci s citlivými údaji na internetu veřejné sítě?**

Tabulka č. 4 ukazuje, že pouze 20,4 % dotazovaných respondentů využívá při práci s citlivými údaji veřejné sítě, jako je například Free Wifi, knihovna, školní počítače atd. 79,6 % dotazovaných respondentů veřejné sítě při práci nevyužívá.

Tento výsledek ovlivňuje také fakt, že v dnešní době má většina lidí svá mobilní data a díky tomu veřejné sítě nepotřebují využívat. Některé mobilní telefony varují před napojením se k veřejné síti, o možných rizicích sdílení dat s jinými uživateli na stejné síti, což samo o sobě zvyšuje povědomí uživatelů ohledem tohoto rizika.



19. Využíváte při práci s citlivými údaji na internetu veřejné sítě? (Free wifi, knihovna, školní počítač...)

| ODPOVĚĎ | RESPONZÍ | PODÍL |
|---|---|---|
| Ne | 73 | 79.6% |
| Ano | 19 | 20.4% |

Tabulka 4: Využíváte při práci veřejné sítě?

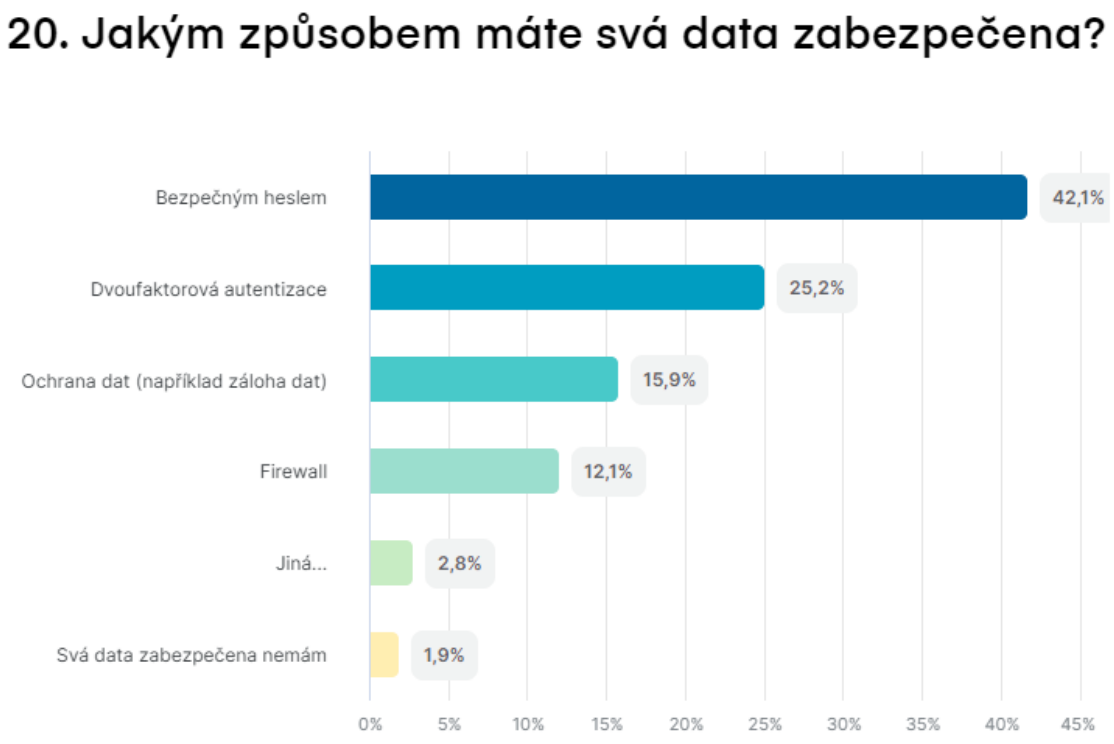
Zdroj: výsledek vlastního výzkumu 2022

**Otázka č.20: Jakým způsobem máte svá data zabezpečena?**

Otázka č.20 byla zaměřena na způsoby zabezpečení svých dat. Tato otázka vycházela z předpokladu č.4, který zněl: „*Méně jak 10 % respondentů svá data zabezpečena nemá*“.

U této otázky měli respondenti možnost vybrat více odpovědí. Graf č.15 znázorňuje, že 42,1 % dotazovaných respondentů využívá zabezpečení heslem, 25,2 % respondentů využívá dvoufaktorové autentizace, 15,9 % respondentů využívá možnosti zálohy dat, 12,1 % využívá softwarového programu firewall a pouze 2,8 % svá data zabezpečena nemá vůbec.

O zabezpečení dat by bylo dobré studenty informovat, a to také o možných rizicích. Nebylo by špatné se o zabezpečení dat informovat v hodinách Informatiky. Mnoho internetových stránek jako je například internetové bankovnictví, mají svá vlastní zabezpečení, jako je dvoufaktorová autentizace, která může data a uživatele zachránit.



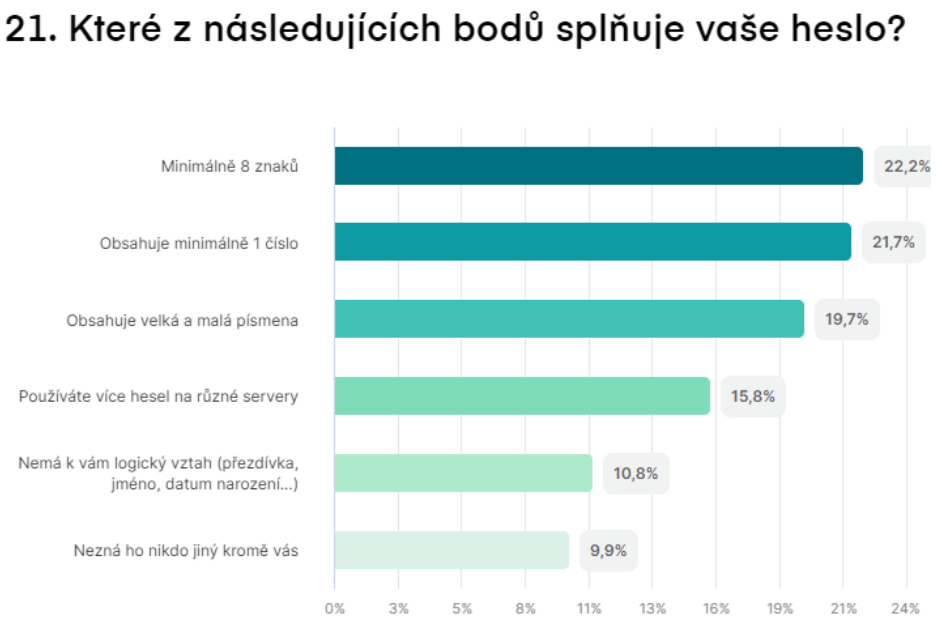

Obrázek 17: Graf 15: Zabezpečená data
Zdroj: výsledek vlastního výzkumu 2022

**Otázka č.21: Které z následujících bodů splňuje vaše heslo?**

Tato otázka měla zjistit, které z následujících bodů obsahuje respondentovo heslo. U této otázky měli respondenti možnost vybrat více odpovědí.

Z grafu č.16 lze vyčíst, že nejvíce využívaný bod splňující hesla respondentů je minimální délka 8 znaků, tuto skutečnost uvedlo 22,2 % uživatelů, bod obsahující minimálně 1 číslo v hesle označilo 21,7 % dotazovaných respondentů a obsažení velkého a malého písmenka v hesle označilo 19,7 % dotazovaných respondentů. Většina serverů a aplikací požaduje po uživateli, aby jeho heslo splňovalo určité podmínky. Většinou se jedná o kombinaci velkých a malých písmen, minimální délku hesla a minimálně jedno číslo v hesle. Zneklidňující fakt je, že pouze 15,8 % respondentů využívá různá hesla na různé servery a pouze 10,8 % dotazovaných respondentů využívá hesla, které k nim nemají žádný logický vztah. 9,9 % respondentů odpovědělo že nikdo jiný kromě nich tato hesla nezná.

Zabezpečení osobních údajů je nesmírně důležité a na tento fakt by měl být každý uživatel upozorněn a měl by věnovat dostatečnou pozornost k zabezpečení svých osobních údajů.




Obrázek 18: Graf 16: Heslo
Zdroj: výsledek vlastního výzkumu 2022

## 5.5 Výzkumné předpoklady

**Předpoklad č.1**

**Více jak 50 % respondentů tráví na internetu více jak 3 hodiny denně.**

Předpoklad se přijímá.

Tento předpoklad byl ověřen v otázce č. 3. Denně na internetu tráví více jak 3 hodiny 68,5 % dotazovaných respondentů.

**Předpoklad č. 2**

**Alespoň 50 % respondentů si přijde závislá na internetu.**

Předpoklad se přijímá.

Tento předpoklad byl ověřen v otázce č.7 a č.8. Na internetu si přijde závislá 70,4 % dotazovaných respondentů.

**Předpoklad č.3**

**Lze předpokládat, že 60 % respondentů má obavy, že by se mohli stát obětí počítačové kriminality.**

Předpoklad se zamítá.

Tento předpoklad byl ověřen v otázce č. 16. Ve které bylo zjištěno že pouze 24,1 % dotazovaných respondentů má obavy z možnosti stát se obětí počítačové kriminality. Je ovšem nutno zmínit, že 37 % respondentů o této problematice nikdy nepřemýšlelo.

**Předpoklad č.4**

**Méně jak 10 % respondentů svá data zabezpečená vůbec nemá.**

Předpoklad se přijímá.

Tento předpoklad byl ověřen v otázce č. 20. Svá data nemá nijak zabezpečeno pouze 1,9 % respondentů.

# ZÁVĚR

Cílem této bakalářské práce bylo seznámit čtenáře se zásadami zajištění ochrany informací a pravidly pro bezpečné používání prostředků výpočetní, informační a komunikační technologie. Dále rozebrat a popsat možné nebezpečí která prostředí internetu mohou přinést.

V teoretické části autor specifikoval a vymezil pojmy internet, sociální sítě a mládež, kde se zaměřil na možná rizika komunikace na sociálních sítích, jejich prevenci a doporučení. Dále je vymezen pojem kybernetické hrozby, kde se čtenář mohl dozvědět o možných softwarových rizicích a rozdílem mezi bezpečnostní událostí a incidentem. Poslední kapitola obsahuje zabezpečení přístupových údajů, zásady zajištění ochrany těchto údajů a desatero pravidel pro bezpečné používání internetu.

Praktická část bakalářské práce obsahuje 21 otázek s podrobným popisem a grafickým vyhodnocením dotazníkového šetření. Autor pomocí vhodných otázek zjistil, zdali se studenti na internetu a sociálních sítích cítí bezpečně, zdali jsou obeznámeni s riziky, na které na sociálních sítích mohou narazit a zda mají svá data vhodně zabezpečeny.

V praktické části byly při sestavování dotazníku vymezeny čtyři předpoklady. Z celkového počtu čtyř, se tři předpoklady přijaly. Předpoklad č.1 který zněl následovně: „*Více jak 50 % respondentů tráví na internetu více jak 3 hodiny denně“.* Na základě odpovědí v anonymním dotazníku bylo zjištěno, že předpoklad č.1 se přijal, a to až v 68,5 %. Tento výsledek dokazuje, že internet je nedílnou součástí života mladistvých. Předpoklad č.2 zněl následovně: „*Alespoň 50 % respondentů si přijde závislá na internetu.“*. Výsledek toho předpokladu ukázal, že se přijal, a to v 70,04 %. Autor se o možných rizicích závislosti na internetu a sociálních sítích zmiňuje v podkapitole sociální sítě a jejich výhody a nevýhody, dále také v podkapitole sociální sítě a mládež. Zamítnutým třetím předpokladem, který zněl následovně: „*Lze předpokládat, že 60 % respondentů má obavy, že by se mohli stát obětí počítačové kriminality“.* Zde byl výsledek pouhých 24,1 %, je ovšem důležité podoktnout, že 37 % dotazovaných respondentů o této problematice nikdy nepřemýšlelo. Tento fakt je varovným signálem, že je potřeba zvýšit povědomí studentů o bezpečnosti a možných rizicích, se kterými se v online světě mohou potkat. Poslední předpoklad č.4 byl přijat a zněl následovně: „*Méně jak 10 % respondentů svá data zabezpečená vůbec nemá“.* Výsledek můžeme označit za potěšující, neboť dosáhl hodnoty 1,9 %.

# SEZNAM PRAMENŮ A POUŽITÉ LITERATURY


1. ACE THE ELECTORAL KNOWLEDGE NETWORK Data access security (online) (11.04.2022) Dostupné z: https://aceproject.org/main/english/et/ete01b.htm

2. AVAST Online hrozby (online) (11.04.2022) Dostupné z: https://www.avast.com/cs-cz/c-online-threats

3. BILAL AHMAD Advantages and Disadvantages of social media for society (online) (8.4.2022) Dostupné z: https://www.techmaish.com/advantages-and-disadvantages-of-social-media-for-society/
4. BOYD, Danah. Je to složitější: sociální život teenagerů na sociálních sítích. Přeložil Lukáš NOVÁK. Praha: Akropolis, 2017. ISBN 978-80-7470-165-8.

5. CLOUDIAN Data backup in depth. Concepts, Techniques and Storage Sechnologies (online) (18.04.2022) Dostupné z: https://cloudian.com/guides/data-backup/data-backup-in-depth/

6. CLOUGH, Jonathan. Principles of cybercrime. Second edition. Cambridge, United Kingdom: Cambridge University Press, 2015. ISBN 9781107034570

7. CORSICA TECHNOLOGIES Whats the difference between a security incident and an event? (online) (10.04.2022) Dostupné z: https://www.corsicatech.com/blog/whats-the-difference-between-a-security-incident-and-an-event/

8. DATAREPORTAL Facebook stats and trends (online) (03.04.2022) Dostupné z: https://datareportal.com/essential-facebook-stats

9. E-BEZPEČÍ Jak zabezpečit počítač (online) (11.04.2022) Dostupné z: https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1653-jak-zabezpecit-pocitac

10. E-BEZPEČÍ, co je flaming (online) (08.04.2022) Dostupné z: https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/dalsi-temata/38-35

11. ECKERTOVÁ, Lenka a Daniel DOČEKAL. Bezpečnost dětí na internetu: rádce zodpovědného rodiče. Brno: Computer Press, 2013. ISBN 978-80-251-3804-5.

12. ESET Pojmy z oblasti internetové bezpečnosti a ochrany – Phishing (online) (24.03.2022) Dostupné z: https://www.eset.com/cz/phishing/

13. ESET antivirus (online) (22.04.2022) Dostupné z: https://www.youtube.com/watch?v=MPD0_dziK1o&t=1s

14. EUROPA, Co jsou osobní údaje? (online) (28.03.2022) Dostupné z: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_cs

15. GAVORA, Peter. Úvod do pedagogického výzkumu. Brno: Paido, 2000. Edice pedagogické literatury. ISBN 80-85931-79-6.

16. G DATA What is actually is a hoax? (online) (08.04.2022) Dostupné z: https://www.gdatasoftware.com/guidebook/what-actually-is-a-hoax

17. GDPR co je GDPR a jak bude aplikování v Česku (online) (28.03.2022) https://www.gdpr.cz/gdpr/co-je-gdpr/

18. GROWTH QUARTERS Analysis:TikTok soars and global social media users hit 4.5 bilion (online) (2.4.2022) Dostupné z: https://thenextweb.com/news/analysis-global-digital-statshot-report-october-2021

19. HOFRICHTER, Kamil. ICT strategie. Vydání druhé. [Praha]: Vysoká škola ekonomie a managementu, 2015. ISBN 978-80-87839-61-4.

20. HULANOVÁ, Lenka. Internetová kriminalita páchaná na dětech: psychologie internetové oběti, pachatele a kriminality. Praha: Triton, 2012. ISBN 978-80-7387-545-9.

21. ICANNWIKI Internet Assigned Numbers Authority (online) (25.03.2022) Dostupné z: https://icannwiki.org/Internet_Assigned_Numbers_Authority

22. IMPERVA – Social engineering (online) (10.04.2022) Dostupné z: https://www.imperva.com/learn/application-security/social-engineering-attack/

23. INTERNETEM BEZPEČNĚ Co je digitální stopa? (online) (11.04.2022) Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/dobre-vedet/digitalni-stopa/

24. INVESTOPEDIA Identity Theft (online) (22.04.2022) Dostupné z: https://www.investopedia.com/terms/i/identitytheft.asp

25. ITU Internet usage statistics (online) (25.03.2022) Dostupné z: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

26. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. ISBN 978-80-7251-397-0.

27. NÁDVORNÍKOVÁ, Johana bezpečnost na veřejném hotspotu WIFI (online) (22.04.2022) Dostupné z: https://www.kvalitni-internet.cz/bezpecnost-na-verejnem-hotspotu-wifi-ktery-bezpecny-byt-nemuze-pokud-nemate-vpn

28. KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

29. KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.

30. KVĚTON, Petr. Hraní videoher v dětství a dospívání: dopady a souvislosti v sociálně-psychologické perspektivě. Praha: Grada, 2020. Psyché (Grada). ISBN 978-80-271-2887-7.

31. Lindeberg, Katajun.; Kindt, Sophie.; Szász-Janocha, C. Internet Addiction in Adolescents; SpringerLink: Germany, 2020. ISBN: 978-3-030-43784-8

32. LUCAS, George R., Ethics and cyber warfare: the quest for responsible security in the age of digital warfare. New York, NY: Oxford University Press. 2017. ISBN 9780190276522

33. MCAFEE Co je malware? (online) (11.04.2022) Dostupné z: https://www.mcafee.com/cs-cz/antivirus/malware.html

34. MEGAN Price, DALGLEISH John, Cyberbullying experiences (2010) (online) (12.04.2022) Dostupné z: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.469.2077&rep=rep1&type=pdf

35. NBU národní bezpečností úřad (online) (10.04.2022) Dostupné z: https://www.nbu.cz/cs/o-nas/
36. NORTON what is a computer virus? (online) (11.04.2022) Dostupné z: https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html

37. PAPEŽOVÁ ZDEŇKA Policie České republiky prevence stalking (online) (08.04.2022) Dostupné z: https://www.policie.cz/clanek/prevence-stalking.aspx

38. PAPEŽOVÁ, Zděnka Prevence – kyberšikana (online) (08.04.2022) Dostupné z: https://www.policie.cz/clanek/prevence-kybersikana.aspx

39. PCWORLD Jak funguje anonymní režim prohlížeče (online) (25.04.2022) Dostupné z: https://www.pcworld.cz/clanky/jak-funguje-anonymni-rezim-weboveho-prohlizece/

40. PIMPERNEL GAWKROGER Advantages and disadvantages of social media (online) (2.4.2022) Dostupné z: https://medium.com/@clinguen/advantages-and-disadvantages-of-social-media-47cd957b73d5

41. POLICIE ČESKÉ REPUBLIKY Počítačová mravností kriminalita (online) (09.04.2022) Dostupné z: https://www.policie.cz/clanek/pocitacova-mravnostni-kriminalita.aspx

42. PROOF POINT What is pharming? (online) (10.04.2022) Dostupné z: https://www.proofpoint.com/us/threat-reference/pharming

43. PUBMED The impact of cyberstalking: the lived experience a thematic analysis (online) (08.04.2022) Dostupné z: https://pubmed.ncbi.nlm.nih.gov/24875706/

44. SMART INSIGHTS Global social media statistics research summary 2022 (online) (2.4.2022) Dostupné z: https://www.smartinsights.com/social-media-marketing/social-media-strategy/new-global-social-media-research/

45. SOURCE DEFENSE web browser security (online) (23.04.2022) Dostupné z: https://sourcedefense.com/glossary/web-browser-security/

46. ŠEVČÍKOVÁ, Anna. Děti a dospívající online: vybraná rizika používání internetu. Praha: Grada, 2014. Psyché (Grada). ISBN 978-80-210-7527-6.

47. VÁGNEROVÁ, Kateřina. Minimalizace šikany: praktické rady pro rodiče. Vyd. 2. Praha: Portál, 2011. ISBN 978-80-7367-912-5.

48. VÁGNEROVÁ, Marie. Vývojová psychologie: dětství a dospívání. Vydání druhé, doplněné a přepracované. Praha: Karolinum, 2012. ISBN 978-80-246-2153-1.

49. COHEN, Frederick B. *A Short Course on Computer Viruses. Pittsburgh: ASP Press, 1990. ISBN 1-878109-01-4*

50. VERYWELL MIND What is cyberstalking? (online) (08.04.2022) https://www.verywellmind.com/what-is-cyberstalking-5181466

51. VINAY PRAJAPATI Advantages and Disadvantages of cosial media (online) (03.04.2022) Dostupné z: https://www.techprevue.com/advantages-and-disadvantages-of-social-media/

52. Vyhláška č. 82/2018 SB., (online) (26.03.2022) Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82

53. WIKIPEDIE V síti (online) (08.04.2022) Dostupné z: https://cs.wikipedia.org/wiki/V_s%C3%ADti

54. Zákon č. 181/2014 SB., (online) (26.03.2022) Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

55. Zákon č. 412/2005 Sb., (online) (09.04.2022) Dostupné z: https://www.zakonyprolidi.cz/cs/2005-412

# Seznam obrázků



# Seznam tabulek

# Evidence výpůjček

Prohlášeni:

Dávám svolení k půjčování této bakalářské práce. Uživatel potvrzuje svým podpisem, že bude tuto práci řádně citovat v seznamu použité literatury.

Jméno a příjmení: Kristýna Michalková

V Praze dne: Podpis:

| Jméno | Oddělení/ Pracoviště | Datum | Podpis |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |