

**UNIVERZITA KARLOVA**  
**HUSITSKÁ TEOLOGICKÁ FAKULTA**

**Rizikové chování na internetu se zaměřením na sociální sítě**  
**Risky behavior on the internet with a focus on social networks**

*Bakalářská práce*

Vedoucí práce:

PhDr. Jana Mottlová, Ph.D.

Autor:

Michaela Šestáková

Praha 2023

### **Poděkování**

Ráda bych skrze tuto práci poděkovala paní PhDr. Janě Mottlové, Ph.D, za vedení práce a poskytnuté rady spojené s bakalářskou prací. Dále bych chtěla poděkovat všem respondentům ve výzkumné části za jejich věnovaný čas a ochotu. Rovněž děkuji všem blízkým za trpělivost a velkou podporu.

### **Prohlášení**

Prohlašuji, že jsem předkládanou bakalářskou práci Rizikové chování na internetu se zaměřením na sociální sítě vypracovala samostatně. Dále prohlašuji, že všechny použité prameny a literatura byly řádně citovány a že tato práce nebyla využita k získání jiného nebo stejného titulu.

V Praze dne 3. 8. 2023

Michaela Šestáková

## **Anotace**

Bakalářská práce se zabývá tématem rizikového chování na internetu se zaměřením na sociální síť. Cílem práce je přiblížit rizika, kterým jsou děti a dospívající v dnešní době vystaveny. Bakalářská práce je rozdělena do dvou částí, teoretickou a praktickou část. Teoretická část práce popisuje sociální síť, vymezuje základní rizika online světa a zaměřuje se na prevenci v této oblasti. V praktické části je proveden kvantitativní výzkum formou dotazníkového šetření s cílem zjistit, zda má edukace, primárně od rodičů nebo školy, pozitivní dopad na prevenci problematického chování na internetu a sociálních sítích.

**Klíčová slova:** internet, rizikové chování, sociální síť, kyberprostor, prevence, edukace, děti a dospívající

## **Annotation**

Bachelor's thesis deals with the topic of risky behavior on the internet with a focus on social networks. The aim of the thesis is to present the risks that children and adolescents are exposed to in today's time. The bachelor thesis is divided into two parts, a theoretical and a practical part. The theoretical part of the thesis describes social networks, explains the basic risks of the online world and focuses on prevention in this area. In the practical part, a quantitative research in the form of a questionnaire survey is conducted with a goal of finding out if education, primarily from parents or school, has a positive impact on the prevention of problematic online behavior.

**Keywords:** internet, risky behavior, social networks, cyberspace, prevention, education, children and adolescents

# Obsah

Úvod.....	8
1 Sociální sítě .....	10
1.1 Dělení sociálních sítí: .....	10
1.2 Vznik a příklady sociálních sítí .....	11
2 Rizika online světa .....	15
2.1 Kyberkriminalita .....	16
2.1.1 Kyberšikana.....	17
2.1.2 Kybergrooming .....	19
2.1.3 Sexting.....	20
2.1.4 Kyberstalking .....	22
2.1.5 Podvody na internetu.....	23
2.2 Další patologické chování v kyberprostoru.....	24
2.2.1 Závislost na internetu .....	25
2.2.2 Nadměrné užívání internetu .....	27
3 Prevence .....	30
3.1 Netiketa .....	31
3.2 Preventivní chování a jednání .....	33
3.3 Jak reagovat při vzniku rizikového chování.....	36
3.4 Organizace, které se zabývají prevencí – příklady.....	37
4 Metodologie výzkumné části.....	39
4.1 Charakteristika výzkumných metod.....	39
4.2 Způsob výběru respondentů .....	39
4.3 Cíle výzkumu .....	40
4.4 Hypotézy .....	40
4.5 Záznam a zpracování dat výzkumu.....	41

4.6	Výsledky dotazníku.....	41
4.7	Analýza výsledků výzkumné části.....	49
4.7.1	Hypotézy k hlavnímu cíli .....	49
4.7.2	Hypotézy k vedlejšímu cíli.....	58
4.8	Shrnutí výzkumné části .....	60
	Diskuse.....	62
	Závěr .....	64
	Seznam použité literatury a dalších informačních zdrojů.....	65

**Seznam zkratk:**

FOMO – fear of missing out, strach ze zmeškání nebo že o něco přijdeme

MKN – Mezinárodní klasifikace nemocí

MŠMT – Ministerstvo školství, mládeže a tělovýchovy

# Úvod

Ve své bakalářské práci se budu zabývat tématem rizikového chování na internetu, zaměřím se převážně na sociální sítě. Sociální sítě jsou jedno z prostředí, ve kterém online rizika vznikají. V práci se zaměřím především na děti a dospívající, kteří využívají sociální sítě nejvíce ze všech skupin, tudíž mají vyšší riziko se setkat s nevhodným nebo nezákonným chováním na internetu.

Hlavním cílem mé práce je přiblížit rizika, kterým jsou děti a dospívající v dnešní době vystaveny. Pokusím se shrnout nejčastější nástrahy v kyberprostoru. Práce popíše nejen rizika, ale také se zaměří na prevenci od rodiny a školy. Účelem závěrečné práce je také poukázat na rizikové chování dětí a dospívajících na sociálních sítích či internetu.

Téma rizikové chování na internetu jsem si vybrala z toho důvodu, že je téma v dnešní době velice aktuální a může se ním setkat kdokoli, nejen děti. Motivem pro výběr tématu práce je nespočet článků, zpráv a rozhovorů, ve kterých se mluví o podvodech, vydírání nebo vyhrožování skrz sociálních sítí a internetu. Proto se chci více ponořit do problematiky a následně ji promítnout do závěrečné práce.

Na začátku teoretické části se budu zaměřovat na sociální sítě, jakou mají funkci a jejich smysl pro uživatele. Zmíním i na jaké druhy se sociální sítě dělí. Dále popíšu nejvíce využívané sociální sítě a jak vznikly. Následně se zaměřím na online rizika a jejich dělení. Podrobněji se ponořím do kyberkriminality a jednotlivých oblastí, které do ní spadají. Popíšu jednotlivé rizikové chování jako je kyberšikana, sexting nebo podvody na internetu. Budu se také zabývat dalším patologickým chováním v kyberprostoru jako je závislost nebo nadměrné užívání internetu.

Značnou pozornost budu věnovat prevenci rizikového chování. Zaměřím se na prevenci od rodiny i školy. Zmíním různá desatera, které dopomáhají k vyhnutí se rizik. Popíšu jaké by mělo být bezpečné chování na internetu a sociálních sítích. V závěru první části zmíním, jak by oběti rizikového chování měli reagovat a na jaké organizace se mohou obrátit a které se tématem zabývají.



Druhou část bakalářské práce budu věnovat kvantitativnímu výzkumu. Ten uskutečním formou dotazníku cíleným na děti a dospívající ve věku od 12-17 let. Odpovědi znázorním pomocí grafů a tabulek, které nám odpoví na stanovené hypotézy. Cílem mé výzkumné části bude zjistit, zda má edukace, primárně od rodičů nebo školy, pozitivní dopad na prevenci problematického chování na internetu. Dále mě v dotazníkovém šetření budu chtít ověřit chování studentů na sociálních sítích z hlediska potenciálního nebezpečí.

# 1 Sociální sítě

Sociální sítě a jejich vývoj je trend současného internetu. Klasický web je určen k získávání informací, ale sociální sítě slouží převážně k vyhledávání lidí. Digitální svět obsahuje určitý společenský účel. Vznik Facebooku ukázal, jaký vliv a dosah mají sociální sítě na utváření lidských vztahů. (Chatfield, 2013, s. 104)

Sociální sítě jsou internetové stránky, na kterých se vytváří soukromé, firemní nebo uzavřené profily. Přes tyto profily je možné sdílet fotografie, odkazy na jiné stránky, videa, psané příspěvky a jiné. Mohou se zde utvářet i tematické skupiny, jejichž členy spojuje například hudba, politické strany, koníčky a sport.

Dnešní digitální technologie využívají lidé naplno. Umožňuje jim komunikaci mezi sociálními skupinami i mezi kontinenty. Komunikace skrz nová média neslouží jen pro známé, ale spojuje i lidi se společným zájmem. Utvářejí se zde stránky fanoušků skupin, týmů nebo politických stran. Patricia Greenfield se tímto tématem zabývá. Uživatelé internetu a sociálních sítí přijímají a vytvářejí svá prostředí. Ve skupinách vznikají normy, pravidla a členové sdílí své názory, zážitky a pocity. Pro děti je jejich virtuální svět součástí každodenního života. Vytváří prostor ke sdílení radostí, problémů, zábavě i poznání. Výzkumy poukazují na to, že sociální, fyzický i virtuální svět se u mladých lidí propojují. Spojují se vztahy v online i off-line prostoru. (Ševčíková, 2014, s. 30-32)

Čas strávených na sociálních sítích se prodlužuje. V roce 2022 byl průměrný čas strávený na sítích dvě a půl hodiny denně. Toto je celkový průměr z populace, který se významně liší s ohledem na věk. (Georgiev, 2023)

## 1.1 Dělení sociálních sítí:

### 1. Profilově založené sítě

Jedná se o sociální sítě, které slouží k sebeprezentaci uživatelů. K prezentaci využívají osobní profily, na které je možné umístit osobní údaje, zájmy, fotografie, zaměstnání, studium atd. Takový profil si utváří uživatel sám při registraci. Sítě umožňují kontakt s ostatními uživateli. Příkladem takové sociální sítě je Facebook a LinkedIn.

## **2. Komunikační sociální síť**

Tuto službu využívají lidé po celém světě. Komunikace probíhá přes kamery a mikrofony počítačů nebo chytrých telefonů. Síť využívají uživatelé k pracovním i soukromým potřebám. Takové služby se v dnešní době používají každodenně. Příkladem je WhatsApp, Facebook Messenger a Skype.

## **3. Obsahové sociální síť**

Tyto sociální síť jsou zaměřené na zábavu. Je zde velké množství obsahu k sledování. Uživatel se může zapojit pasivně jen sledováním nebo aktivním tvořením obsahu. Obsahové síť se můžou lišit formou jako jsou například dlouhá nebo krátká videa, fotografie či hudba. Mezi takové síť spadá Instagram, YouTube nebo TikTok.

## **4. Virtuální světy – online hry**

V dnešní době je nepřeberné množství online her. Dělí se do mnoha skupin a druhů. Příkladem jsou logické, sportovní, strategické, simulátory nebo akční hry. Speciální kategorií jsou hry typu MMORPG. To jsou online hry s hrdiny ve virtuálním světě, kam se mohou připojit lidé z celého světa a interagovat mezi sebou. Typicky se zde může najednou nacházet tisíce až desetitisíce hráčů najednou. Příkladem takové online hry je EVE Online, World of Warcraft nebo World of Tanks.

## **5. Mikroblogy**

Jsou stránky, kde uživatelé píšou své poznatky, příběhy nebo informace ze světa. Forma sdělení jsou krátké příspěvky psaného textu. Je zde také výrazný způsob sebe prezentace uživatele ať už se jedná o politické preference, subkultury nebo zájmy. Příkladem rozsáhlé blogovací sítě je v Twitter. (Ševčíková, 2014, s. 23-29)

## **1.2 Vznik a příklady sociálních sítí**

V devadesátých letech se objevují první stránky specializované na utváření mezilidských vztahů. Jednalo se o zdokonalování chatovacích místností. Roku 1994 byla vytvořena první webová stránka theGlobe.com, která nabízela pokročilejší prostor na zveřejňování a sdílení informací okolí. Významnější se poté stala stránka SixDegrees.com. Ta se objevila v roce 1997 a jednalo se o skutečnou sociální síť, která umožnila vytvářet si skupiny přátel, osobní profily i pokročilou konverzaci mezi uživateli. Bohužel tato sociální

sít' předběhla dobu, protože v Devadesátých letech nebyl ještě internet zcela běžnou součástí domácností, jak je tomu dnes. Z důvodu finančních problémů služba ukončila činnost.

Velká změna nastala roku 2002, kdy byla spuštěna sociální síť Friendster. Tato stránka dokázala propojit lidi se společnými zájmy, procházet si různé profily uživatelů, navazovat kontakt vzdáleně v reálném čase, sdílet media a zprávy. Stránka měla více jak milion uživatelů. V roce 2003 byl jejich úspěch překažen a převzala ho stránka MySpace. Tento projekt rozběhla parta lidí, kteří se odtrhli od Friendsteru. Stránka se stala místem pro komunikaci mezi přáteli, ale zapojila se i kulturní scéna – například hudební skupiny a audio/video záznamy. MySpace měla i svou chatovací službu mezi uživateli a dala možnost si upravovat svůj profil. Služba dosáhla nevídaného úspěchu 100 milionů uživatelů. Bohužel jejich rozvoj zastavil vznik konkurenční sociální sítě Facebook.

## **Facebook**

Facebook byl založen roku 2004. Tato sociální síť byla vytvořena na Harvardské univerzitě studentem Markem Zuckerbergem. Služba byla po jeden rok vyhrazena pouze místním studentům. Posléze ji začali využívat další univerzity v USA. V roce 2006 nastal zlom, kdy si zde profil mohl založit kdokoli starší třinácti let. Po necelých šesti letech existence Facebooku zde mělo svůj profil přes půl miliardy uživatelů. V letech 2012 využívalo tuto sociální síť přes miliardu lidí. V dnešní době má Facebook skoro každý, proto se jedná o nejrozsáhlejší sociální síť. Osobní profil si může uživatel nastavit jako soukromý nebo veřejný. Stránky se vyvíjí a poskytují uživatelům mnoho výhod jako je vlastní chat s přáteli, sdílení fotografií, u příspěvku je možné označení místa i dalších osob, videa, souborů, subkulturní skupiny i fanouškovské, informování o událostech a konaných akcí, vytváření vlastních událostí a pozvánek pro přátele, hraní her s přáteli, spoustu možností tvoření vlastního profilu a mnoho dalšího. Komunikace mezi uživateli probíhá v aplikaci Messenger, která má prostor soukromé i skupinové konverzace. Služba kromě jiného poskytuje i videohovory a hlasové zprávy. (Chatfield, 2013, s. 104-107)

## **Instagram**

Další společností, kterou dnes řídí Mark Zuckerberg je Instagram. Stránka vznikla roku 2010 a o dva roky později ji odkoupil Facebook. Primárně se Instagram používá v aplikaci mobilního telefonu. Má jednoduchou funkci, umožňuje uživatelům sdílet fotografie. Profil se tedy především prezentuje fotografickou sbírkou, dalo by se říct online fotoalbum. Uživatelé své příspěvky mohou sdílet v mnoha podobách a využívat různé funkce

jako jsou například fotografie s použitím obrovským množstvím filtrů, označení reklam či jiných uživatelů, krátká videa, živé vysílání a mnoho dalších. Aplikace také umožňuje veřejné komentáře a rychlou reakci tzv. like pod sdíleným příspěvkem. Služba také poskytuje i možnost soukromých zpráv mezi uživateli. Profil lze nastavit jako soukromý nebo veřejný. Instagram využívá i mnoho známých osob z celého světa. V této službě se našli i celebrity, kteří fotkami propagují nejrůznější produkty a společnosti. Takovým osobám se říká influenceři. Instagram používá krátká videa zvaná Reels. Video se používají převážně pro zábavu, reklama na akce či produkty. Tyto krátká videa jsou dostupné od roku 2020 a umožňuje je i Facebook. (Klement, 2022)

### **LinkedIn**

Další využívanou sítí je LinkedIn. Byl založen roku 2002. Tato stránka slouží jako internetový pracovní profil. Uživatelé zde debatují o pracovních zájmech a možnostech. Stránka není určena k zábavě, ale poskytuje uživatelům pracovní nabídky a uživatelé se profesně zviditelní. Jedná se online propojení pracovního trhu. Usnadňuje navazovat vztahy a možnosti pracovní spolupráce. Funguje jako takový online životopis. Na profilu se většinou uvádí pracovní místa, vzdělání, zkušenosti a dovednosti. Web umožňuje vyhledávání osob v určitém odvětví, s různými zkušenostmi, navazování spojení a usnadňuje změnu i nábor firmám.

### **Twitter**

Twitter vznikl roku 2006. Jedná se o blogovací síť, kdy jednotliví uživatelé píšou krátké sdělení tzv. tweety. Zprávy se zobrazují na profilové stránce uživatele a ukáže se i sledujícím tohoto profilu. Jeho největší předností je rychlé sdělení informací a myšlenek v reálném čase. Sdělení bývá krátké a výstižné informace. Dalo by se říct, že se jedná o nejrychlejší zpravodajství, a to i díky tomu, že Twitter využívají vládní instituce, odborníci v různých odvětvích, známé osobnosti a novináři. (Chatfield, 2013, s. 104-107)

### **TikTok**

Sociální síť zvaná TikTok je jedna z nejmladších a vznikla v roce 2017 v Číně. Během krátkého období se stala velmi oblíbenou a nejrychleji rostoucí sítí na světě. Na této stránce se sdílí typicky krátká, několika sekundová videa. Tvůrci videí se na TikToku označují museři. Na této sociální síti nemusíte mít účet nebo profil pro sledování obsahu, je potřebný jen pro tvorbu videí. Obsah je velmi rychlý – jedná se především o videa doplněna hudbou, filtry, prostřihy nebo efekty. Z některých trefných se stávají trendy, které přebírají další

uživatelé. Využívají se také ke krátkým sdělení nebo reklamám. Obsah je zaměřen na vyvolání emocí ať už pozitivních tak negativních. Hlavním cílem sítě je zaujmout co nejvíce uživatele sledovat tyto videa. Ve srovnání s jinými sociálními sítěmi je velmi rychlá a dynamická, proto ji nejčastěji využívá mladší generace v rozmezí mezi 15-25 let. Je zde nepřetržitý proud videí, který udržuje uživatele na síti, protože nemá konce. (Internetem bezpečně, 2019)

### **Snapchat**

Snapchat je sociální síť sloužící především k zasílání fotografií. Vznik aplikace se datuje od roku 2011, kdy jí tři studenti Stanfordské univerzity založili. Tato platforma se liší tím, že fotografie se neukládají, jen se na dobu deseti sekund odhalí odesílateli. Momentky si můžete zasílat s přáteli, kteří využívají také tuto aplikaci. Další z funkcí, kterou Snapchat nabízí je stories, kde si video nebo fotografii může okruh přátel zobrazit po dobu 24. hodin. Další z funkcí je zasílání krátkého videa, které je dlouhé pouze 10 sekund. Snapchat nabízí i nově soukromý chat s uživateli. Sdílené fotografie lze upravovat pomocí filtrů, textů i hudby. Jedna z novinek je také sdílení vaší polohy s uživateli. Funkce se nazývá snap map. Funkce vám dává informace o pohybu svých přátel a sledujících. (O'Connell, 2020)

### **YouTube**

Tato služba slouží především ke sledování videí. Vznikla roku 2005 a o rok později YouTube odkoupila společnost Google. Svoji popularitu si získal po celém světě. V dnešní době má po celém světě miliardy přihlášených účtů, jen v české republice je to přes 5 milionu měsíčně. Video, která se zde objevují, jsou rozdílná. Obsah sdílený na YouTube je pestrý, například zábavná, hudební, umělecká, naučná, cestovatelská a sportovní videa. Na stránku můžete jít za zábavou, pro radu i se vzdělat. Krom sledování umožňuje i videa tvořit, sdílet, komentovat, hodnotit a lze se připojit i do živého vysílání. Tvůrci videí se označují jako youtubeři, kteří sdílí svůj obsah a mají fanoušky. Takových tvůrců je po světě mnoho a někteří dosahují neskutečné popularity přes miliony sledujících. Youtubeři mají velký vliv na své fanoušky a vytváří tak často vzory pro mladistvé a děti. YouTube má i mnoho přidávaných funkcí jako je prémiový účet nebo dětský kanál. Nejnovější rozšíření platformy o funkci je YouTube shorts. Jedná se o krátká videa, která mají formát několika sekund až jednu minutu. (Vaníčková, 2019)

## 2 Rizika online světa

Internet a sociální sítě jsou součástí života každého z nás. Dnešní společnost je také označována jako informační společnost. Většina mladých je ve virtuálním světě a sítích prakticky každodenně. Dnešní posun digitálních technologií dovoluje se připojit v podstatě kdekoliv a kdykoliv. Možnost činností a využití internetu je různorodá. Uživatelé ji využívají ke komunikaci s okolím, vyhledávání informací, plnění zadaných úkolů či zábavě. U dospívajících je digitální komunikace jedním z nástrojů, jak zůstat neustále v kontaktu s vrstevníky. Umožňuje jim to v reálném čase sdílet radosti i starosti. U dětí a mladistvých je off-line i online svět velmi propojený. Vzniká zde prostor pro formování sebe sama, tvoří se zde hodnoty, normy a životní styl. Online prostředí má pozitiva i negativa. Internet se stal prostředím, které dětem prospívá, ale přináší i mnoho rizik. Čím více jsme aktivní online, tím pravděpodobnější je, že se vystavíme nebo setkáme s některým rizikem. (Ševčíková, 2014, s. 34-35)

Nástrahy a rizika v online světě popíší v následující části. Jedna z klasifikací podle Livingstone a Haddon, dělí online rizika do čtyř skupin – komerčního, agresivního, sexuálního a hodnotového rázu. Ve virtuálním světě může dospívající a dítě vystupovat jako příjemce, účastník nebo pachatel.

### 1. Komerční rizika

Z pozice příjemce – nechtěná reklama, nabádání k posílání peněz nebo spam

Z pozice účastníka – ukládání a získávání citlivých informací a údajů

Z pozice pachatele – nelegální stahování materiálu, nabourávání účtů,

### 2. Agresivní rizika

Z pozice příjemce – násilný a agresivní obsah

Z pozice účastníka – oběť online obtěžování, kyberšikany a stalkování

Z pozice pachatele – vykonávání kyberšikany, stalkování a obtěžování v online

### 3. Sexuální rizika

Z pozice příjemce – sexuální či pornografický obsah

Z pozice účastníka – zasílání sexuálního materiálu, setkávání s neznámými lidmi

Z pozice pachatele – nahrávání a vytvoření pornografického materiálu

#### 4. Hodnotová rizika

Z pozice příjemce – rasistické a falešné informace

Z pozice účastníka – manipulace a přesvědčování od druhých lidí

Z pozice pachatele – poskytování ohrožujících rad a vytváření falešných informací.  
(Livingstone, Haddon, 2009)

Děti a dospívající se s rizikovým chováním setkávají přes online komunikaci a možnosti internetu. Jak je patrné z předchozího dělení, riziko může přijít v různých formách. Dospívající a děti se na rizikovém chování mohou i aktivně podílet. Pro širší rámec rizik spojených s internetem byl přepracován model od Bronfenbrennera. Tento model byl upraven a přizpůsoben v projektu EU Kids Online II.

Tento model je dělen do tří vrstev. První vrstvou je Individuální úroveň. V té mají vliv psychosociální charakteristiky jedince, které způsobují odolnost vůči rizikům a negativním dopadům. Další vrstvou je blízké sociální prostředí, do kterého spadá rodina, vrstevníci, spolužáci či kolegové. Poslední vrstvou, která ovlivňuje možná rizika je národní kontext, do něhož spadá kulturní postoje a hodnoty, právní rámec, vzdělávací systém nebo media. (Ševčíková, 2014, s.11)

### 2.1 Kyberkriminalita

Rychlý vývoj informačních technologií přináší s sebou i nová rizika a škodlivé jednání. Kybernetické kriminalitě je věnován stále intenzivnější zájem. Policií ČR je kyberkriminalita vnímaná jako trestní činnost, která je páchaná v prostředí komunikačních a informačních technologií zahrnující i sociální sítě. Kyberprostor slouží jako prostředek nebo předmět k páčání trestného činu. (pcr.cz, 2019).

Poslední statistika Policie ČR ohledně registrované spáchané kriminality z roku 2022 dokazuje přesun kriminality do kyberprostoru. Tato oblast kriminality má značný a pravidelný růst. Za minulý rok (2022) bylo registrováno 18 554 páchaných trestných činů v kybernetické kriminalitě. (Moravčík, 2023)

Kybernetická kriminalita má i své místo v trestním zákoníku. Trestné činy jsou upravené zákonem č. 40/2009 Sb. Zde jsou uvedené příklady činů, kterých se pachatel může dopustit.



- § 230- Neoprávněný přístup k počítačovému systému a nosiči informací
- § 231- Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
- § 232- Neoprávněný zásah do počítačového systému nebo nosiče informací z nedbalosti
- § 191- Šíření pornografie
- § 192- Výroba a jiné nakládání s dětskou pornografií
- §193- Zneužití dítěte k výrobě pornografie
- § 193b- Navazování nedovolených kontaktů s dítětem
- § 270- Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi
- §354- Nebezpečné pronásledování
- § 355- Hanobení národa, rasy, etnické nebo jiné skupiny osob
- § 356- Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod
- §357- Šíření poplašné zprávy
- § 184- Pomluva
- § 175- Vydírání (Zákon č.40/2009 Sb.)

V této části představím několik rizik a trestných činů, které se na sociálních sítích mohou stát. Budu se věnovat jednotlivě tématům jako je kyberšikana, kybergrooming, sexting a kyberstalking. Popíšu základní fakta, fáze rizikového chování a procesy zpracování oběti.

### **2.1.1 Kyberšikana**

Je takové jednání a chování na internetu, které záměrně a agresivním způsobem poškozují dalšího uživatele v kyberprostoru. Chování považované za kyberšikanu splňuje shodující prvky, kterými jsou úmysl nebo záměr, jednání se opakuje, nerovnováha účastníků a poškození oběti. U veřejně dostupných příspěvků poškozující oběť stačí jen jediný, nemusí se opakovat a je považován za kyberšikanu. (Zormanová, 2019)

V projektu EU Kids Online z roku 2020, kterého bylo Česko součástí uvádí, že zde je vystaveno online agresi 15% dětí ve věku od devíti až sedmnácti let. (Smahel, Machackova a kol., 2020)

U kyberšikany se využívá mnoho prostředků, kde a jakým způsobem oběti ublížit. Často se jedná o soukromé zprávy a volání s verbálním napadáním nebo výhružným obsahem. To stejné platí pro e-maily, přes který se zasílá obtěžující obsah. Skrz webové stránky, sociální sítě a jejich chaty, mohou vznikat skupiny uživatelů, ve kterých se objevují fotografie, videa a mnoho zesměšňujících komentářů o oběti. (Rogers, 2011, s. 33-35)

Kyberšikana zahrnuje mnoho druhů útoku. Oběť se může stát terčem verbálního napadení, pomlouvání, vyloučení, urážení a hanobení přes zprávy a sociální sítě. Útočník může využít k urážení sdíleného videa nebo fotografie. V kyberšikaně často dochází i k vyhrožování a vydírání. Nebo si útočník přivlastní identitu oběti a vydává se za ní pod falešným profilem na sociálních sítích nebo seznamkách. Kyberšikana není uvedena v trestním zákoníku. Projevy vystihující kyberšikanu do nich částečně spadají, např. vyhrožování, vydírání a mnoho dalších. (Burýšek, 2020)

Účastníků kyberšikany může být více. Nejedná se tedy jen o útočníka a oběť, ale i sekundární útočníky. Popíšu zde jednotlivé aktéry. U kyberšikany je útočník většinou neznámý. Využívá k anonymitě přezdívky a různých účtů, proto se jím může stát kdokoliv. Sekundární útočníci jsou považováni všichni, kdo útoky šíří nebo jen sledují. Pokud se kyberšikana odehrává skrze veřejné sítě sledovanost může být obrovská. Po přičtení sdílení se takový útok může dostat i za hranice naší země. (Kopecký, Krejčí, 2010, s. 5-6)

Motivy pro páčání kyberšikany jsou od útočníků různé. Jedním z nich může být upoutání pozornosti ostatních sledujících. Dále také z důvodu nudy a vyhledávání zábavy spojené s pokusem co oběť snese a vydrží. Dalším motivem může být i tendence patřit a zařadit se do skupiny. Posledním motivem je vytvoření něčeho velkého a významného. (Kopecký a kol., 2015, s. 23)

Oběti se může stát kdokoliv bez ohledu na věk, postavení či národnost, kyberprostor na takové pohledy nebere zřetel. Účastníci kyberšikany se nemusí znát ani osobně. Bohužel se šíří a trvá daleko déle a opakovaně, protože materiály umístěné na internet nelze stoprocentně odstranit. (Kopecký, Krejčí, 2010, s. 5-6)

Dopady kyberšikany na oběť mohou být závažné a psychicky škodlivé. Oběti mohou změnit názor sami na sebe. Ztrácí sebevědomí, sebedůvěru a mají špatné sebehodnocení.

Objevují se zde i neurotické a depresivní poruchy. Časté jsou i poruchy spánku s ohledem na ztrátu pohody. Závažným dopadem kyberšikany je i posttraumatická stresová porucha a trauma z události. U obětí se vyskytují i suicidální myšlenky z důvodu pocitu neřešitelné situace. (Kopecký a kol., 2015, s. 25)

### **2.1.2 Kybergrooming**

Je to takové chování uživatelů, jehož cílem je pomocí internetových komunikačních prostředků a jejich technologií vyvolat v dospívajícím/dítěti pocit důvěry a prostřednictvím falešné identity vylákat na schůzku. Na takové schůzce může dojít k sexuálnímu obtěžování, zneužití, fyzickému napadení nebo k výrobě pornografického obsahu. Kybergroomer si hledá své oběti převážně na sociálních sítích, seznamkách nebo zájmových stránkách. Postupně s nimi skrz různé manipulační techniky udržuje kontakt v soukromém chatu.

Manipulace s obětí prochází několika fázemi. Proces je velice propracovaný a plíživý. Po přečtení fází si můžete říct, že je to přeci jasné a nikdy byste se do toho nedostali, ale uvědomte si délku takového zpracovávání oběti. Komunikace útočníka může probíhat několik měsíců i roky, kdy dochází k utužování vztahů. (Kopecký, 2015, s. 331-333)

#### **1. Fáze navázání kontaktu**

V počátcích se útočník snaží kamarádským způsobem oslovit dítě nebo dospívajícího uživatele. Zpravidla to bývá reakce na nějakou fotku nebo zálibu. Útočník vystupuje většinou pod falešnou identitou mladšího člověka nebo jiného pohlaví. Cílem této fáze je získání co nejvíce osobních informací.

#### **2. Fáze izolace**

Díky získaným informacím kybergroomer ví, co dítě nebo dospívajícího trápí nebo ve svém životě prožívá. Ze svého postavení útočník vystupuje jako jediný, kdo jeho problémy chápe a často to doplní o nějakou situaci z jeho fiktivního života. Útočník se pokouší potlačit vztahy s vrstevníky a rodinou. Používá k tomu manipulaci a zastrašování například neříkej to, oni to nechápou nebo můžeme mít tajemství.

#### **3. Fáze podplácení**

K vytvoření závislosti a důvěry využívá kybergroomer manipulaci pomocí nabídek, odměn a slibů. Může se jednat například o zakoupení různých dárků, vstupenek, oblečení nebo zaslání peněz. Díky těmto nabídkám vzniká blízký vztah a v oběti vzbuzuje pocit

zájmu. Jako poděkování si může útočník poprosit třeba o fotky. Oběť má pocit závaznosti a za obměnu něco pošle.

#### **4. Fáze emoční závislost**

Po vzbuzení důvěry vzniká vztah a emoční závislost. Může se jednat o milostný či kamarádský vztah, ve kterém se svěřuje s problémy a intimnostmi. Útočník je v tuto chvíli jediný, komu může věřit a o vztahu nikomu jinému neříká. Toto jednání dává útočníkovi možnost toho následně zneužít.

#### **5. Fáze osobní setkání**

Kybergroomer usiluje o shledání se s obětí. S ohledem na to, že útočník má plnou důvěru a vybudovaný vztah, nepůsobí to nijak nebezpečně. Dítě se mnohdy na svého kamaráda z internetu naopak nemůže dočkat. Často navrhuje málo navštěvovaná místa nebo rozsáhlé prostranství kde uniknou pozornosti okolí. V této fázi má útočník mnoho informací a materiálu, kterými oběť může ke schůzce vydírat.

#### **6. Fáze zneužití, napadení či obtěžování**

Toto je fáze, kvůli které kybergroomer celou dobu udržoval blízký kontakt. Záměrem útočníka může být cokoli například osahávání, pornografický materiál, znásilnění nebo fyzické napadení. Takové osobní setkání se může opakovat a následně může kybergroomer vydírat oběť. Mnoho případů si tento nechtěný zážitek nechává pro sebe z důvodu studu před okolím. (O2 Chytrá škola-kybergrooming)

### **2.1.3 Sexting**

Sexting znamená zasílání sexuálního obsahu. Může se jednat o fotografie, video nahrávky či textové zprávy. Nejčastěji se takový obsah posílá přes sociální sítě Instagram a Snapchat. Zasílání takového obsahu může být ve dvou formách, a to konsensuální a nekonsensuální sexting. Konsensuální sexting znamená souhlas obou stran, tzn. jak příjemce, tak odesílatele. Nekonsensuální je pravý opak, kdy obsah chodí neohlášeně a nemístně. Výměna obsahu se sexuálním zaměřením probíhá mezi partnery nebo cizími lidmi se záměrem zaujmout.

Důsledky zasílání citlivého obsahu mohou být velmi rizikové. Příjemce může obsah použít jako zbraň pro vydírání a nátlak. Zasláním zprávy ztrácí odesílatel kontrolu s dalším použitím jako je například přeposlání nebo zveřejnění. U nezletilých se toto dá považovat za trestný čin. Sexting je především nebezpečný z důvodu následného vydírání. Hlavním cílem

vydíráním může být finanční odměna, pomsta, poškození a pošpinění osoby. Zveřejnění intimních fotografií může přijít i ze strany bývalého partnera. Při takovém jednání se dopouští trestné činnosti. (ESET, 2022)

Snapchat je jedna ze sociálních sítí, která představuje velké riziko v oblasti sextingu. Velkou oblibu si tato aplikace našla u mladistvých, kteří si zde posílají fotografie. Dobrovolně si zde zasílají intimní fotografie či videa. Společnost se brání svojí bezpečností, protože se pořízené fotografie po uplynutí doby smažou. Jak už tomu bývá i toto jde obejít a odeslané soubory nejsou v bezpečí. Opatření je že se uživatel zobrazí upozornění na pořízení snímku fotografie. Jsou různé způsoby, jak to obejít, aniž by se o tom uživatel dozvěděl. Proto tu soukromé fotografie nemají zaručené bezpečí. (Doležalová, 2018)

Při provozování sextingu mezi dospělými partnery není nic špatného. Zasílání lechtivých zpráv do vztahu dnešní doby nepochybně patří. Vypsání se ze sexuálních fantazií si zpestřuje život mnoho párů. Nejedná se o nic rizikového a nebezpečného. V pořizování a zasílání fotografií je důležité být obezřetní. Když už takové fotografie či videa zasíláte je nejlepší se vyhnout záznamu obličeje. Pro útočníka je jednodušší použít pro vydírání fotografii kde jste jasně identifikovatelní. Při spojení fotky s vámi stačí i výrazné znaménko, tetování, šperky nebo prostor ve kterém je fotka pořízená. (Kožíšek, Písecký, 2016, s. 91)

Pro vydírání skrze sexuální obsah u dětí existuje pojmenování sextortion. Vydírání probíhá skrze sociální sítě. Při vydírání pachatelé využívají jistý model chování pro ovlivnění obětí. Dají se rozdělit do pěti fází.

### **1. Navázání kontaktu**

Pachatel ve většině případů využívá cizí identitu s odlišným věkem nebo pohlavím. Konverzace probíhá ze začátku nezávazně, třeba jako reakce na fotku nebo událost, které se dítě zúčastnilo. Postupně konverzace mnohdy zachází k zasílání fotografií zatím bez sexuálního podtextu.

### **2. Manipulace pomocí lichotek**

Touto fází si pachatel získává oblibu a zájem dítěte. Na zasláný materiál píše samou chválu a pozitivní reakce. Dítě touží být chtěné, obdivované a uznávané, proto si je pomalu získává na svou stranu.

### **3. Ověření identity**

Oběť v této fázi ukáže svou pravou identitu. Pachatel vyžaduje potvrzující fotografii, například s časem, nápisem nebo datem, tak ověřuje skutečnou identitu. Taková metoda se běžně využívá k ověření osob na internetu, ale v tomto ohledu se identita potvrdí pro vydírání.

### **4. Stupňování intimity**

Stupňování tématu fotografií se postupně začíná proměňovat. Zpravidla tuto oblast zahajuje pachatel. Obsah si sdílejí navzájem jen je rozdíl je v pravdivosti fotografií, protože útočník využívá falešné fotografie z internetu. Postupně se z nevinných fotografií stává fotogalerie se sexuálním podtextem. Dostávají se až do fáze dětské pornografie.

### **5. Vydírání**

Pokud se oběť rozhodne přestat v této konverzaci, pachatel obvykle přejde k fázi vydírání skrze přátele nebo rodinu oběti. Vyhrožuje sdílením citlivého materiálu sledujícím nebo přátelům na sociálních sítích. Dalším stupněm je vyhrožování sdělením rodině, kdy se dítě bojí a většinou dále posílá materiály. Většina dětí se při takové situaci neobrací ani na rodinu, vrstevníky nebo školu. V pokročilém stádiu se jich mnoho obrací na anonymní poradnu nebo linku bezpečí. (Kopecký, 2014)

Podle článku z poradny E-Bezpečí se tímto tématem v poslední době značně zabývá. Na poradnu se obrací hodně lidí, kteří jsou vydírání skrz intimní materiál. Kvůli strachu se někteří neobrátili na pomoc včas a zaplatili značné částky pachatelům. Bohužel nevýhodou internetu je ta, že co se jednou na něj dá, může být použito i po smazání. Pachatel si data může uložit a použít je později nebo šířit dál. (E-bezpečí, 2023)

#### **2.1.4 Kyberstalking**

Jedná se o dlouhodobé nepříjemné obtěžování a pronásledování prostřednictvím kyberprostoru. Sledování se provádí skrz sociální sítě, e-maily, zprávy, webové stránky nebo určování polohy, což je dokonalý zdroj informací.

Kyberstalker využívá různé metody, jak oběť obtěžuje. Jedním z nich je právě již zmiňovaná aktuální poloha oběti bez svolení. Pro toto sledování musela být funkce povolena v telefonu, proto se v takovém případě musel telefon dostat do rukou útočníka. Další metodou je vytváření více falešných účtů, pomocí kterých sleduje aktivitu a kontaktuje oběť.

Stalker se může i nabourat do webkamery zařízení nebo nainstalovat sledování pro webové prohlížení a komunikaci. (Burdova, 2022)

Nebezpečné pronásledování je v České republice trestným činem. Kyberstalking je za něj považován při opakovaném jednání a jasném odmítnutí oběti. Motivace pro pronásledování je různá. Někdy se jedná o cizí osobu, která si oběť našla na internetu a mnohdy je cílem vydírání. Stalker může být osoba blízká například bývalý partner. Motivací je návrat partnera, hněv, pomsta a žárlivost. Cíl u blízké osoby může být zesměšnění, poškození a manipulace. Stalker si své oběti můžeme vyhledat v zaměstnání, škole i ve volném čase. Může se objevit i stalker, který uctívá slavné osobnosti. (O2 Chytrá škola – kyberstalking)

### **2.1.5 Podvody na internetu**

Velkým rizikem se v poslední době staly podvody v kyberprostoru. Cílem podvodníků jsou především peníze nebo osobní údaje. K takovému jednání využívají manipulaci a zastrašování uživatelů. Nepoužívají k tomu žádné nabourávání účtů, pod nátlakem jim mnoho lidí podlehnou a sami jim údaje i peníze dají. Podvodníci využívají různé metody a techniky. Příkladem mohou být phishing (podvodné e-maily) nebo vishing (podvodné hovory). Základem většiny metod je vzbudit v oběti silnou emoci, jako je například strach nebo obavy, které způsobí nerozmyšlené a impulzivní jednání. V takové situaci pak člověk vyplní citlivé informace k platební kartě nebo přístupová hesla do internetového bankovníctví. Podvodníci se neustále zdokonalují a posouvají své útoky. (ESET, 2022)

Kybernetická kriminalita se stává významnou složkou trestných činů páchaných v České republice. Policie potvrdila, že online podvody jsou významnou složkou v kyberkriminalitě. Česká bankovní asociace uvádí průměrnou škodu 161 500 korun, což je částka o kterou klienti přišli při internetových podvodech. V součtu pak škoda činí téměř dvě miliardy korun. (ČT 24, 2023)

Mezi nejčastěji využívanými podvody v kyberprostoru jsou podvodné nákupy a falešné stránky. Postupně popíšu dva způsoby podvodů a jejich průběh.

#### **Podvodné nákupy a inzeráty**

Nakupování pomocí internetu se stalo běžnou možností obchodu. Většina lidí má zkušenosti s e-shopy, které nabízí velké spektrum produktů a mnohdy za lepší ceny. Bohužel

si díky zvýšenému zájmu o nakupování online dali tuto možnost do hledáčku i podvodníci. Oběti podvodu se uživatel může stát jak z pozice kupujícího, tak prodávajícího.

Podvodné nákupy se mezi uživatele rozšiřují pomocí reklamy nebo rozesílaných odkazů na falešné e-shopy. Podvodníci je naplní zbožím, které je atraktivní a levné. Následně po zakoupení přes bankovní převod nebo platební bránu, nemusí zboží vůbec dorazit nebo bude velmi špatné kvality. Tímto způsobem podvodníci získávají od uživatelů finanční obnos a citlivé osobní informace. Takový web se pozná z recenzí na zboží, většinou nemají osobní odběr, nemají zákaznickou podporu a uvedený kontakt.

Z pozice prodávajícího se podvody konají přes veřejné inzeráty. Podvodník osloví uživatele skrz kontakt uvedený v inzerátu. Existuje spousta inzertních míst například Aukro, Ebay, Sbazar, Vinted nebo takovou službu nabízí i Facebook pod názvem Marketplace. Podvodník využívá roli zájemce prodáváného předmětu. Během domlouvání informací o předmětu, falešný zájemce může poslat formulář na vyplnění informací obsahující třeba i údaje k platební kartě nebo přihlašovací údaje do internetového bankovníctví. (Česká bankovní asociace, 2022)

### **Falešné stránky**

Pachatelé se přes takové stránky chtějí dostat k osobním údajům. Jednat se může o přístupové kódy, především k internetovému bankovníctví. Takové jednání začíná komunikací přes e-mail, telefonní hovor, SMS zprávy nebo sociální sítě. Podvodníci chtějí oběť vystrašit a poměrně často k tomu využívají lež s napadením účtu a předstírají banku. Pomocí strachu dokážou uživatele zmanipulovat k poskytnutí chtěných přístupových informací.

K tomu používají právě falešné stránky, které vypadají skoro stejně jako oficiální stránky úřadů nebo bank. Přístup na takovou stránku je zaslán přes odkaz. Na stránce jsou kolonky, do kterých uživatel vyplní informace, které pachatel požaduje. Oběť nemá vůbec tušení, že se jedná o podvod je přesvědčená o komunikaci s oprávněnou osobou. Pachatel na druhé straně vidí zadané informace jako je uživatelské jméno a heslo. Tím má přístup k internetové bance a vykrade ho. (Kožíšek, Písecký, 2016, s. 123-130)

## **2.2 Další patologické chování v kyberprostoru**

Mezi další rizikové chování ve spojitosti s internetem je závislost a nadměrné užívání. Jsou to dva rozdílné pojmy a mají různý vliv na jedince. Nadměrné užívání se



zaměřuje spíše na čas, který naplňuje jejich denní aktivitu. Čas trávený na internetu a aktivity s tím spojené jsou považované za koníčky a životní styl. Zatím co u závislosti vznikají patologické jevy. V takové fázi nemá už uživatel kontrolu a objevují se konflikty s okolím. (Ševčíková, 2014, s. 37-38)

### **2.2.1 Závislost na internetu**

Závislost na internetu není zatím uznána jako porucha v mezinárodní klasifikaci nemocí. Bohužel v některých případech se užívání internetu stalo neovladatelným nutkáním. Netolismus, tedy závislost na internetu, má mnoho společných prvků s jinými závislostmi. Takové chování spadá do skupiny nelátkových závislostí nebo jinak behaviorálních závislostí. Jedinec své chování nemá pod kontrolou a nemůže ho potlačit. Závislostní chování sebou přináší negativní dopady v oblasti sociálních vztahů, výkonu ve škole nebo práci, zdraví i problémy po finanční stránce. Nutkavé jednání se snadno může proměnit v patologické. Netolismus má různé formy a podoby. Jedná se od nakupování až po hraní her. Zaměření na určitý druh je dán věkem, pohlavím, sociálním prostředím, osobní vyrovnaností a sebevědomím i vlivem společnosti. (Státní zdravotní ústav)

Mark Griffiths sestavil šest kritérií, podle kterých se určí zda je jedinec závislý. Pokud není splněn pátý bod vzorce, konflikt, jedná se pouze o nadměrné užívání, které nemá tak závažné dopady na jedince jako závislost.

#### **1. Význačnost**

Činnost se stane nejdůležitější aktivitou v jeho životě. Zanedbává jiné základní životní potřeby jako je strava, spánek či hygiena. Díky tomu se mění i jeho myšlení, prožívání i cítění.

#### **2. Změny nálad**

Aktivita ovlivňuje náladu a jeho prožívání. Přináší mu určitý druh uvolnění, úlevy a uklidnění. Nebo mu naopak dodává vzrušení, které se mu jinak nedostane.

#### **3. Tolerance**

Fáze, ve které se zvyšuje čas na aktivitu. Prodlužuje se doba, kdy nastává uspokojení z dané činnosti.

#### **4. Abstinenční příznaky**

Příznaky se objevují v psychické formě. Objevují se, když danou aktivitu nelze uskutečnit nebo je nutné ji omezit. Příznaky se projevují depresí, nervozitou, agresivitou či prudkou změnou nálady.

#### **5. Konflikt**

Toto je moment kdy se objevuje konflikt sám se sebou i s okolím. Dané aktivitě věnuje člověk více energie a času. Interpersonální konflikt vede k obtížím ve vztazích s rodinou i přáteli. V intrapersonálním konfliktu si pak uvědomuje, že vše ostatní posouvá na druhou stranu, ale nemůže si pomoci a ztrácí kontrolu.

#### **6. Relaps**

Návrat k rizikovému chování po období kontroly a abstinence. (Viewegová, 2019)

#### **Druhy závislosti**

Závislost na internetu je velmi rozsáhlý a široký pojem. Druhy patologického užívání internetu se dělí do různých oblastí. Zde jsou vyjmenovány druhy jednotlivých závislostí spojené s internetem.

- Závislost na online hrách
- Přetížení informacemi – nadměrné vyhledávání informací
- Závislost na kybersexu-využívání webových stránek s pornografickým obsahem
- závislost na virtuálních vztazích – nadměrná komunikace v online prostoru
- Internetová kompulze – internetové nakupování nebo sázení (Kopecký a kol., 2015, s. 100)

Dále se jednotlivě zaměřím na dva ze zmiňovaných forem závislostí. Podrobně popíšu závislost na sociálních sítích a hraní her.

#### **Závislost na sociálních sítích**

Takový jedinci mají neustálou tendenci kontrolovat co se děje na sociálních sítích. Pravidelně navštěvují profily uživatelů, přidávají příspěvky, reagují nepřetržitě komentáři a zúčastňují se diskuzí na různých stránkách. Takové jednání se označuje jako syndrom FOMO, které vzniklo z anglického fear of missing out. Tento stav vyvolává pocit že o něco přicházíme a nebudeme v obraze. Syndrom spadá do behaviorálních závislostí a hlavním

projevem je nepřetržitá aktivita v online světě. U jedinců se projevuje neovladatelný pocit mít přehled co se děje na dané sociální síti.

U této závislosti hraje velký význam vnímání času a konflikt mezi reálným prožíváním a skutečností. Díky chytrým telefonům a aplikacím jsou sociální sítě dostupné v podstatě kdekoliv.

Na sociálních sítích se vše ukazuje moc růžové a dokonalé. Uživatelé se chlubí svými zážitky, dovolenými, životním stylem, oblečením, majetkem i předměty. Za všech okolností chtějí vypadat v tom nejlepším světle a být uznávaní. V případě, když se nedostavuje úspěch, se u závislého může dostavit úzkostné stavy a smutek. Takový uživatelé jsou v neustálé tenzi protože se snaží vyrovnat ostatním a být nejlepší. (Kopecký, 2017)

### **Závislost na hraní her**

Hraní her v kyberprostoru zabírá velkou část volného času a zábavy dospívajících. Hry mají obrovskou popularitu oproti jiným aktivitám. Velmi úspěšné a využívané jsou herní světy, ve kterých hraje několik hráčů souběžně. Někteří uživatelé v každodenním hraní, nacházejí v online světě lepší uspokojení a úspěchu než v realitě. Hráči zde mají komunity, které mohou nahradit opravdové vztahy. Hraní her poskytuje pestrý, pohlcující a nekonečný zážitek. Vývojáři her posouvají požitky dále pomocí technologií a neotřelých nápadů na další rozšíření a nové úkoly ve hře. Vnoření se do online světa hry může u mladších lidí omezit vnímání času. V takovém případě se může stát hra časově náročná a postupně neovladatelná.

Neovladatelným nutkáním k hraní vzniká prostor pro závislost na hrách. Nové vydání mezinárodní klasifikace nemocí (MKN- 11), by měla obsahovat zařazení patologického hráčství a hraní her jako poruchu. Za závislost na hrách se považuje takové jednání, u kterých je aktivita často opakující a stálá. Uživatel musí vykazovat nejméně po dobu jednoho roku vzorce závislostního chování uvedené v úvodu. Jedná se především o nezvládnutí kontroly, dáváním přednosti hraní před jinými aktivitami nebo konflikty s okolím. Online hraní může mít závažné dopady na fungování jedince. (Essau, Delfabbro, 2020, s. 185-186)

### **2.2.2 Nadměrné užívání internetu**

U nadměrného užívání je významným faktorem čas strávený při online aktivitách. U některých je srovnatelný s časem stráveným ve škole. Online svět hojně nahradil či omezil jiné aktivity u dětí jako je příprava ke studiu, navazování sociálních kontaktů nebo sportovní

aktivity. Jedná se o celkovou problematiku organizování volného času a životního stylu mladistvých. Mezi generacemi vzniklo rozdílné vnímání internetu. Pravidelné používání internetu zvyšuje analytické schopnosti, bystrost kognitivních funkcí či digitální gramotnost. Velké rozdíly jsou převážně mezi důvody používání internetu. Starší generace většinou používá internet jako další zdroj informací. Zatímco mladí na internetu vyhledávají pobavení.

Současné studie pracují s dvěma předpoklady, při kterých dochází k nadužívání internetu. Prvním důvodem mohou být psychosociální obtíže a druhou příčinou je snížené soustředění a vnímání.

První model předpokládá, že v souvislosti se závislostí či nadměrným užíváním internetu mohou vzniknout psychické obtíže. Především se jedná o nízkou sebedůvěru, mylné sebehodnocení, úzkosti nebo deprese. Týká se to převážně osob, které unikají od potíží v rámci zátěže. Při stresových situacích má internet úlohu bezpečného útočiště. Online svět jim poskytuje oporu, pochopení a uklidňující prostředí. Internet jim může dopřát i sociální vazby, které postrádají v realitě. Vztahy vzniklé v internetovém prostředí nejsou tak hluboké a silné. Úspěch a obdiv ve virtuálním světě se nemusí setkat s pochopením v reálném prostředí s vrstevníky. Z tohoto hlediska se užívání internetu jeví jako nevhodná strategie pro zvládnání zátěže.

Druhým významným faktorem vedoucím ke zvýšené aktivitě na internetu je tendence se nudit a tím vyhledávat vzrušení a impulzivní podněty. Internet poskytuje velkou škálu možností a zajímavých aktivit. Děti s poruchami pozornosti si rychleji zvyknou na pozitivní odměnu, která je ve virtuálním světě znatelnější. Útržkovitě probíhá i komunikace v internetovém prostředí. Nevedou se zde rozsáhlé komunikace, nevyžaduje tedy takovou potřebu pozornosti a soustředění. Toto může vést k problémům s udržováním vztahů a navazováním kontaktů v reálu. (Ševčíková, 2014, s. 38-41)

Rizikové dopady na nadměrné užívání internetu jsou různorodé. Může se objevit obtížné a komplikované navazování kontaktů v reálném světě s vrstevníky nebo partnery. U dětí a dospívajících vzniká mnohdy konflikt mezi rodiči ve spojitosti s aktivitami a časem tráveným na internetu a sociálních sítí.

Zdravotním rizikem je zhoršení spánku a nespavost. Při nadměrném užívání nemusí docházet k dostatečnému naplnění fyziologických potřeb jako je pohyb, strava nebo spánek. Bohatý a ničím nerušený spánek je potřeba pro správný vývoj jedince. Používání digitálních technologií není vhodné před spánkem. Internet a sociální sítě zvyšují pozornost a jas displeje prodlužuje čas usínání a tím i celkovou délku spánku. (Sadílková, 2020)

### 3 Prevence

Prevence slouží k bezpečnému užívání a vyhnutí se případnému riziku spojeným s užíváním internetu. Zaměřuje se také na minimalizaci dopadů. Prevence není jen informování o nástrahách a problémech v kyberprostoru. Prevence zahrnuje hlubší pohled. Její dopad na uživatele je příprava na situace, které mohou nastat. Výsledek prevence je obohacení o nové dovednosti a znalosti ochrany. Prevence by neměla být založená na vyvolání strachu a nepřiměřená k věku. Prevence musí být vedená zodpovědnou osobou, například učitelem, preventivním pracovníkem nebo rodičem. Probíhat by měla v bezpečném a nerušeném prostředí, ve kterém se dítě nebude bát zeptat a projevit se. Ideálním prostředím jsou malé skupiny, kde se účastníci prevence znají. Vytváří to důvěrnější prostředí pro sdělování zážitků, dotazu a diskuse na dané téma. (Kopecký, 2017)

#### **Prevence ve škole**

Škola by měla být informována a vzdělávána v rozvoji digitálních technologií a sociálních sítí. Vzdělanost učitelů je základ pro předávání informací dětem. Prevence v oblasti internetu se zařazuje do preventivních programů škol nebo do vzdělávacího programu jako mediální výchova.

Škola k výchově bezpečného chování na internetu může využít mnoho seminářů, kurzů, workshopů, které jsou akreditované MŠMT. Jednou z možností je návštěva nějakého preventivního specialisty v této oblasti nebo odborníky na téma. Škola také může využít různých materiálů, které různé organizace nabízejí bezplatně k dispozici. V některých materiálech se nachází i typy na interaktivní metody výuky. Dalším způsobem je využití audiovizuálních materiálů a filmů, které jsou následně převedeny do diskuse o tématu. (JSNS, 2023)

#### **Prevence v rodině**

Rodiče mají velkou roli ve vzdělávání v oblasti internetu. Jejich úkolem je vést a podporovat děti, aby se v kyberprostoru pohybovaly zodpovědně a obezřetně, proto by i oni měli být dostatečně informovaní. Rodiče by měli svým dětem dát pochopení, pomoc a být vzorem. Pochopení by se mělo dávat najevo otevřenou komunikací a zájmem o provozovaných aktivitách na internetu. Takové chování zvyšuje pravděpodobnost, že se děti na ně obrátí o pomoc.

Rodiče by se měli zajímat a informovat o nových trendech v informačních a komunikačních službách. S dětmi je důležité o dění komunikovat a respektovat je. Rodič

by měl mít přehled o tom co dítě sdílí nebo s kým komunikuje, proto je dobrým krokem stát se jedním ze sledujících. Nebo mohou rodiče u dítěte využít kontrolní programy na aktivitu ve virtuálním světě.

Vzdělávání v rodině by mělo proběhnout na téma ochrany soukromí, co je vhodné dávat a co ne, jak si sestavit bezpečné heslo nebo čemu věřit. Vhodné je se zaměřit i na netiketu. Vysvětlit dětem jaká jsou pravidla slušného chování na internetu a bavit se o možných nástrahách. (Internetem bezpečně – desatero dobrého kybernetického rodiče)

### **3.1 Netiketa**

Jedná se o soubor pravidel slušného chování v online prostředí. Vzniklo spojením dvou slov net (internet) a etiquette (etiketa). Prvně se termín netiketa objevil ve společnosti Intel roku 1995. Nejednalo se o pravidla jako taková, spíše doporučení, jak se chovat. Současná netiketa má definovaná pravidla chování uživatelů na sociálních sítích i celém internetu. Jsou to v podstatě sepsaná běžná pravidla slušného vystupování, která se bohužel v online prostředí nedodržují. (Kopecký, 2021)

Digitální svět často vytváří takové prostředí, že zapomínáme na reálné osoby sedící na druhé straně. Lidé se schovávají pod falešnými profily, pod kterými píší neslušné komentáře, zprávy a vydávají se za jiné osoby. Chování na internetu by se nemělo nijak lišit od skutečného. Vystupování v kyberprostoru by mělo být slušné, s respektem a uvážením. Sociální sítě lidi spojují, ale i oddalují. Není zde možné skrz psaný text přenést pravé emoce a umožňují psát věci co by se ve skutečnosti osoba bála říci. Běžná komunikace sebou nese i neverbální složku jako je mimika nebo gestikulace, která pomáhá ve vyjádření emocí. V internetové komunikaci si přijdeme anonymní, bezpeční, ničím neohrožení a to v zásadě ovlivňuje jednání na sociálních sítích nebo internetu.

U internetové komunikace se mnohdy stává, že zapomenete na reálného člověka, se kterým si píšete. Nespojíte si to s jeho osobou, a proto se můžete chovat moc kriticky, urážlivě, neslušně až agresivně. Často se může jednat i o zesměšňování situace, osoby nebo zprávy. (PortálDigi, 2018)

Netiketa a její doporučení není nic složitého. Obecně jsou to pravidla pro uživatele sociálních sítí a internetu. V zásadě jsou důležitá hlavně dvě pravidla komunikace: komunikace probíhá mezi reálnými lidmi a má obsahovat společný respekt. Důležité je si uvědomit, že nekomunikujeme s obrazovkou, fotkou nebo obrázkem, ale s živým člověkem. Neosobnost a anonymita právě vede k nevhodnému až agresivnímu chování, které někteří

uživatelé využívají. Proto pokud píšete něco, co byste do očí dané osobě neřekli, chováte se nepatřičně. Netiketa velmi závisí i na daném prostředí ve kterém se pohybujeme. Soukromé chaty nebo konverzace jsou více neformální a uživatelé se více otevrou. Ve veřejné komunikaci nebo komentářích by pak měl být uživatel více slušný a dbát na pravidla netikety. (Strapa, 2005)

Základní pravidla v chování na internetu vytvořila Virginia Shea, která popsala ve své knize Netiquette.

1. Pamatuj na člověka – při online komunikaci nesmíme opomenout reálného člověka na druhé straně. Obsah by neměl být nijak urážející, ponižující a agresivní, proto píšeme jen tehdy pokud si slova promyslíme a řekli bychom to osobě z očí do očí.

2. Dodržuj stejná pravidla chování jako v reálném životě – v online světě dodržujeme pravidla, normy a zákony, abychom svým jednáním nikoho neohrozili a neuškodili.

3. Uvědom si, kde se v kyberprostoru nacházíš – důležité je rozlišovat prostředí a komunikaci na různých stránkách. Do veřejných konverzací se nehodí urážlivé a nenávistné komentáře, ale argumentace fakty.

4. Respektuj čas ostatních lidí – sdělení by měla být jasná a stručná, aby nezdržovala jiného člověka.

5. Vybuduj si dobrou pověst v online světě – hlídejte si pravdivost různého obsahu co sdílíte. Záleží i na stylu a kvalitě komunikace. Psaný text by měl být slušný a neurážející.

6. Sdílej odborné znalosti – internet slouží jako odpověď na otázky. V dnešní době si musíme dát pozor na obsah sdílení. S informacemi je potřeba pracovat kriticky a opatrně, protože internet je plný dezinformací.

7. Pomáhej držet pod kontrolou flame wars – internetová diskuze by neměla překročit hranice výměny názorů a stát se hádkou s urážením a napadáním účastníků. Takové situace by se neměly dále šířit a mít dlouhého trvání.

8. Respektuj soukromí ostatních – v online komunikaci platí pravidlo nečíst soukromé zprávy a vstupovat do účtů bez souhlasu uživatele.



9. Nezneužívej své síly – pravidlo se týká lidí, kteří mají velký vliv na jiné osoby. Především se jedná o tvůrce stránek, kteří mají jiná uživatelská práva, ale dostupných informací i možností by neměli zneužívat.

10. Odpouštěj chyby jiným – převážně se jedná o gramatické chyby uživatelů. Měli bychom být tolerantní a neupozorňovat na chyby veřejně. (Recmanová, 2017)

### **3.2 Preventivní chování a jednání**

Několik společností, které se zabývají bezpečností uvádí soubor pravidel pro bezpečné fungování na internetu. Za mě nejvíce výstižné bylo pojetí od sdružení Bezpečně online, které zde uvedu.

#### **Desatero bezpečného chování**

##### **1. Uvažovat o tom co sdílíme**

Kvůli zneužití na internet nepatří osobní údaje a data. Je důležité mít stále na paměti, že to, co se jednou objeví na internetu, zde již zůstane. Obzvláště to platí o sdílení a označování fotografií druhých, od kterých není udělené schválení.

##### **2. Chránit své heslo a soukromí**

Přístupové hesla nesdělovat nikomu jinému, jsou určena pouze pro daného uživatele. Heslo se v nesprávných rukou může snadno zneužít k protizákonným činům nebo poškození uživatele.

##### **3. Používat zabezpečení**

Využívat ochranu zabezpečení skrz antivirové programy na všech digitálních zařízeních. Důležité je používat všude, kde se přihlašuje do uživatelských účtů jako jsou sociální sítě. Velké nebezpečí hrozí u stahování souborů.

##### **4. Nevěřit všemu na internetu**

Při konverzacích může docházet k ukradení nebo zfalšování identity uživatelů a následné oslovení dalších uživatelů s cílem jim uškodit. Neznámým osobám není vhodné svěřovat důvěrnosti. Proto je potřeba jednat opatrně a s rozmyslem.

## 5. Neotevírat podezřelé přílohy

Zasílání podezřelých zpráv s přílohami je mnoho a většina spadá do technik sociálního inženýrství s cílem získat přístupová hesla a obohacení. Příloha může obsahovat vir nebo malware, díky jemuž se umožní přístup do zařízení.

## 6. Ověřovat si pravdivost informací

Ne vše je na internetu pravdivé. Falešné zprávy dokážou ovlivnit mnoho lidí. Je nutné si podstatné informace ověřit u více zdrojů, než je možné je považovat za pravdivé.

## 7. Nákupy a prodej přes ověřené stránky

Zásadní je sledovat důvěryhodnost stránek, jejich recenze a kontaktní údaje. Podvod se koná jak z pozice prodávajícího, tak kupujícího. Vhodné jsou ověřené e-shopy a inzertní stránky.

## 8. Opatrnost při konverzacích a zaslaných materiálech

Intimní fotografie nejsou vhodné do konverzací na sociálních sítích. Vztah s druhou osobou, pro kterou je fotografie určena nemusí vydržet. Zneužití takové fotografie může mít velké dopady.

## 9. Hlídat si digitální stopu

Jednou za čas je vhodné vyhledat své účty na internetu. Zde se pozná, zda informace někdo nezneužil nebo neukradl identitu.

## 10. Ilegální stahování

Neporušovat autorský zákon. Kopírování a následné šíření je bráno za nelegální. (Bezpečně online, 2016)

Vyhnutí se napadení v kyberprostoru lze podpořit pár body ohledně zabezpečení služeb, účtu a digitálního zařízení. Především se jedná o správné nastavení soukromí na sociálních sítích a uživatelských účtech. Velmi zásadní je stavba přístupových hesel a zacházení s nimi.

### **Nastavení hesla**

Nastavení hesla může být poněkud složité. Musí splňovat různá kritéria jako je například neprolomitelnost ale i zapamatování pro uživatele. Hesla slouží k zabezpečení vašich osobních údajů a dat. K získávání hesel využívají pachatelé sociálního inženýrství, kdy

se pomocí např. falešných stránek nebo hovorů snaží obět' přimět ke sdílení hesla. Takové jednání bylo podrobně popsáno v předchozí kapitole podvody na internetu.

Neproniknutelné a silné heslo by mělo být dlouhé a komplikované. Nemělo by obsahovat osobní údaje, například věk, datum narození nebo jméno. S heslem by si uživatel měl dát záležet a ne volit banální číselné řady nebo slova. Uvádí se více jak patnáct znaků. Skládat by se mělo ze symbolů, čísel a malých a velkých písmen. Metoda k vytvoření hesla je i seskupení náhodných slov jdoucí za sebou nebo vytvoření věty. Aby heslo nebylo moc obsáhlé a zbytečně dlouhé lze použít i jen počáteční písmena.

Většina zásadních webových stránek s velmi citlivými daty využívá dvoufázové přihlašování. S tímto bezpečnostním přihlašováním se můžeme setkat u internetového bankovníctví nebo pro internetový vstup pojišťoven a úřadů. V první fázi je vaše klasické uživatelské jméno a heslo. Dalším krokem je zasláný kód na email nebo zprávou pro ověření uživatele. Některé organizace, například banky využívají pro ochranu biometrické přihlášení, kterým je otisk prstu nebo sken obličeje.

V neposlední řadě se v poslední době osvědčila funkce správce hesel. Služba umožňuje si zapamatovat jednotlivá přihlášení do všech účtů. Základem je si nastavit kvalitní a silné heslo k přihlášení do správce hesel. Tuto službu nabízí různé aplikace, antivirové společnosti nebo je i součástí účtu na Googlu. (Empey, 2019)

### **Nastavení soukromí**

Sociální sítě a jejich profily slouží k přiblížení se k ostatním uživatelům a k utužování vztahů mezi nimi. Sdělování informací je do značné míry pozitivní ale může být i negativní. Mezi negativní dopady může patřit zneužití osobních informací prostřednictvím informací uvedených na profilu. Tyto informace mohou být také zneužity pro páchaní trestné činnosti. Je nutné se proto preventivně zaměřit na údaje uvedené na profilu a nastavení soukromí profilu.

Při zveřejňování obsahu na sociálních sítích je nutné zvažovat několik aspektů. Prvním krokem je zvážit obsah informací které publikujeme i při dobrém nastavení soukromí. Musíme brát ohled i na možnost, že se informace dostane k někomu jinému, než pro koho je určena a počítat i s možností jejího zneužití. Pro dospívající tato představa může být komplikovaná. Dalším krokem je si uvědomit, že informace na internetu zůstává. Teď pro nás nemusí být nijak ubližující, ale postupem času by se mohla stát. V budoucnu by si

tyto informace mohl přečíst zaměstnavatel nebo partner. Uvědomění si této fáze s ohledem na budoucnost je obtížné i pro dospělé uživatele natož pro dospívající.

Soukromí lze regulovat nejen naším uvažováním co sdílet, tak i také funkcí konkrétních sociálních sítí. Na základě možností lze nastavit přístup k informacím. V nastavení se upravuje i pro koho je uvedený obsah otevřený a kdo informace může dostávat. Uživatelé často nemají takový přehled o lidech, co je sledují, do jakých patří skupin nebo koho mají v kontaktech.

Posledním krokem je také brát zřetel na provozovatele sociálních sítích. Má neustálý přístup k údajům zveřejněných na sociálních sítích. Osobní údaje uživatelů jsou velice cenné a obchoduje se s nimi. V běžné praxi se s používají k marketingovým účelům. Uživatel tedy nikdy nebude mít stoprocentní soukromí. Proto by se každý uživatel měl seznámit s provozovatelem a jeho politikou s manipulací informací od uživatelů. Je nutné i zohlednit proud času, změny v podmínkách a nastavení společnosti. (Ševčíková, 2014, s. 70-72)

### **Další bezpečnostní rady**

Mezi tyto body patří ochrana počítače nebo telefonu pomocí antiviru a firewallu. Programy brání a blokuje vstup na škodlivé stránky. Antivirové programy dokáží uchránit soubory a data v zařízeních.

Opatrnosti je třeba dbát i na veřejných sítích. Připojení je v dnešní době možné v podstatě kdekoliv. V některých případech nemusí být Wi-Fi zabezpečená. Na veřejných sítích se nepřihlašujte do banky nebo účtů s citlivými údaji. Při využívání cizího zařízení je bezpečnější vstup přes anonymní prohlížení. (NGSS, 2020)

### **3.3 Jak reagovat při vzniku rizikového chování**

V knize Bezpečně na internetu se objevují postupy, jak reagovat při vzniku různého rizikového chování. Ta dává oběti návod k postupu a řešení situace do které se dostal. Tyto postupy by se daly shrnout do jednotlivého návodu, který zde popíšu.

Jednání by se mělo zahájit okamžitě bez prodlužování. Hrozí zhoršení stávajícího stavu a prohloubení problému. Nevhodnou a nevyžádanou konverzaci v žádném případě nepřijímat a nereagovat na ní. Daného uživatele ignorovat, blokovat nebo nahlásit. Při probíhající konverzaci si dělat průběžnou zálohu pro sestavení důkazů o rizikovém chování. Při sdílení citlivých informací nebo fotografie, je vhodné kontaktovat správce stránek, který může obsah smazat nebo s ním manipulovat.

S problémem se svěřit důvěrné osobě, například rodičům, sourozencům, kamarádům nebo učitelům. Zásadní je se obrátit na ně a říct si o pomoc. U některých rizikových chování může vzniknout stud, že jste se nechali podvést nebo vmanipulovat k nějaké činnosti. Strach a hanba může bránit ve svěřeni se blízké osobě. V takovém případě je možné se obrátit na anonymní poradny a poprosit o pomoc tam.

Vzniklý problém lze řešit přes různé organizace, které poskytnou odbornou pomoc. V některých případech je nutné se obrátit i na policii. (Kožíšek, Písecký, 2016, s. 94-95)

### **3.4 Organizace, které se zabývají prevencí – příklady**

#### **E-bezpečí**

Je projekt, který se věnuje prevencí, vzdělávání, osvětě a výzkumu zaměřujícím se na rizikové chování na internetu. Hlavní složkou projektu je práce v terénu, tzn. přednášky, besedy, vzdělávací akce atd. Cílovou skupinou jsou primárně žáci, ale také učitelé, metodici prevence, rodiče i široká veřejnost. Na jejich webové stránce je k dispozici poradna, do které lze anonymně napsat se žádostí o radu nebo pomoc. (E-bezpečí- informace o projektu)

#### **Linka bezpečí**

Organizace cílí na pomoc dětem a mladistvým v tíživé životní situaci nebo s problémy. Linka je dostupná 24h denně na telefonním čísle 116 111, nicméně je možné se obrátit se žádostí o pomoc i přes chat na webových stránkách a také přes email. V rámci svých aktivit online poskytují také videa, podcasty a vedou svůj blog. Zaměstnanci nejsou dostupní pouze na telefonu, ale věnují se také prevenci a vzdělávání ve školách, sportovních klubech atp. (Linka bezpečí-o nás)

#### **Dětské krizové centrum**

Je nestátní nezisková organizace specializující se na odbornou, zejména psychosociální, pomoc dětem s fokusem na krizové a náročné životní situace. Na organizaci se mohou obracet obdobně jako na ostatní přímo děti a řešit své problémy. Dětské krizové centrum má svou vlastní linku důvěry, která se zabývá také riziky v kyberprostoru a má na tuto problematiku vyhrazené vlastní telefonní číslo. Z hlediska prevence se organizace věnuje i tvorbě různých materiálů, které jsou komiksové charakteru a mají díky tomu blíže k dětem. Tyto publikace se věnují nebezpečí internetu, ale i problémy se sociální integrací, kompetencemi a další. Veškeré publikace lze i objednat v tištěné podobě. (Dětské krizové centrum-jaké služby poskytujeme)

## **O2 Chytrá škola**

O2 Chytrá škola je projekt v rámci Nadace O2, který cílí na vzdělávání dětí, jejich rodičů a učitelů v tématu bezpečného chování na internetu. Na jejich webu lze nalézt informační materiály a tipy, jak se vyhnout rizikům na internetu, jak ho bezpečně využívat ale i pomoci někomu jinému v případě, že se dostane obtíží. Nově O2 chytrá škola spustila portál [bezpecnevsiti.cz](http://bezpecnevsiti.cz) který obsahuje články zaměřené primárně na vzdělávání rodičů, učitelů a široké veřejnosti. Web obsahuje spoustu novinek a sleduje trendy rizik na internetu v různých oblastech, nejen v rámci sociálních sítí, ale např. i podvody na internetu, online hry, jak hlídat děti na internetu aj. (O2 Chytrá škola- o nás)

### **Bud' safe online**

Bud safe online je nevýdělečný projekt v rámci MŠMT od společnosti AVAST, jehož cílem je vzdělávání dětí na základních školách v tématu bezpečného chování na internetu. Webové stránky obsahují množství tipů na bezpečné chování na internetu, sekci pro učitele s metodickou příručkou, jak správně vzdělávat děti a také sekci pro rodiče. Na webu lze nalézt i online kurz, který lze poskytnout dětem. Kurz je provádí různými rizikovými situacemi a učí je se v nich správně chovat – např. jak reagovat na vydírání, jaké věci dávat online, jak vyhodnotit podezřelé zprávy a mnoho dalšího. (Bud safe online- pro média)

### **JSNS.CZ**

JSNS – jeden svět na školách – je vzdělávací program od organizace Člověk v tísni, který se od roku 2001 zaměřuje na výchovu mladých lidí a dětí. Na webu lze nalézt množství výukových materiálů v tomto tématu, které se zaměřují nejen na vzdělávání, ale i prevenci, a to nejen ohledně bezpečného chování na internetu. Mezi materiály lze nalézt přes 380 dostupných filmů k promítání na škole a přes 1700 výukových materiálů. Web vedle toho řeší např. i problematiku boje s dezinformacemi a jak vyhodnotit že se o dezinformaci jedná. Vedle toho lze nalézt na webu i informace k současným a velmi aktuálním tématům jako je např. válka na Ukrajině. JSNS klade hlavní důraz na využitelnost materiálů, které vznikají ve spolupráci s učiteli. Záběr JSNS je opravdu široký a s jeho materiály se tak setkali žáci na více než 4000 školách. (JSNS.CZ- o nás)

## **4 Metodologie výzkumné části**

Výzkumná část se věnuje oblasti prevence a rizikovému chování na internetu se zaměřením na sociální sítě. Pro získání informací k výzkumným cílům jsem zvolila kvantitativní výzkum formou dotazníku. Tuto metodu jsem si vybrala z důvodu poměrně velkého množství získaných dat v krátkém čase. Výhodou také je to, že dotazník zachovává respondentům anonymitu, tudíž jsou jejich odpovědi více pravdivé a neovlivněné zadavatelem. Některé z otázek byly zaměřené na citlivé informace, kdy pro respondenta je zachování bezpečného soukromí základem. Což u takového citlivého tématu je zajisté výhodou. Jsou zde zaznamenána data, o kterých se zmiňuji v teoretické části.

### **4.1 Charakteristika výzkumných metod**

Výzkumná metoda dotazníku nahrazuje strukturovaný rozhovor. Řadí se do kvantitativních metod. Je vyhotoven v písemné formě. Výhodou této metody je získání přehledného množství poskytnutých odpovědí. V dnešní době je hojně využíván dotazník v elektronické formě. Respondent ho jednoduše může vyplnit skrz internet. Cílem u dotazníku je ověřit hypotézy, které se pomocí otázek potvrdí nebo vyvrátí.

Otázky v dotazníku se volí s ohledem na stanovený cíl výzkumné práce. Otázky by měly být srozumitelné, stručné a jednoznačné. Existuje řada způsobů, jakým se odpovídá na otázky. Jedním z nich jsou odpovědi otevřené pro sdělení názoru respondenta. Další možností je vybírat ze škály odpovědí. V poslední řadě se jedná o uzavřené odpovědi, kde jsou jasně dané odpovědi. (Vojtíšek, 2012, s.27-28)

### **4.2 Způsob výběru respondentů**

U dotazníků byl použit cílený výběr respondentů. Dotazník byl určen pro děti a dospívající ve věku od 12 do 17 let. Byl šířen pomocí sociálních sítí a elektronické pošty. Díky tomu se dostal do různých škol, a nejen k jednotlivým žákům dané třídy. Pomocí kontaktů se dostal také do dvou táborových skupin, do skupin s rozdílným zaměřením a zkušenostmi. Dotazníkový vzor je tedy více rozmanitý a široký. Bylo zodpovězeno a zpracováno 123 odpovědí na dotazník. Dotazníkové šetření probíhalo 20 dní.

Respondentům bylo kladeno 14 otázek. Všechny byly uzavřené a byly stanovené odpovědi, z kterých dotazovaní vybíraly. U dvou otázek se jednalo o výběr z více možností. Otázky byly pomyslně rozděleny do dvou částí. První se zaměřovala na prevenci od rodičů a školy, jaký tomu přikládají důraz. Druhá byla cílená na rizikové situace a jak se s nimi

vypořádají dotazování. U dotazníku byla zachována dobrovolnost a anonymita respondentů. Studenti byli informováni o účelu otázek k vyhotovení výzkumu pro bakalářskou práci.

### 4.3 Cíle výzkumu

Hlavním cílem výzkumu je zjistit, zda má edukace, primárně od rodičů nebo školy, pozitivní dopad na prevenci problematického chování na internetu a sociálních sítích. Dílčí cíl jsem stanovila na zmapování chování studentů na sociálních sítích mimo jiné z hlediska potenciálního nebezpečí. Tím jsem si chci ověřit informace, které jsem získala v teoretické části mé bakalářské práce.

### 4.4 Hypotézy

Hypotézy jsou stanoveny na základě informací z teoretické části. Ve velké míře jsem se s takovými tvrzeními setkala od svého okolí. Proto jsem chtěla znát názor a chování od skutečného vzorku osob. Na základě informací jsem sestavila tyto hypotézy, které se díky výzkumu potvrdí nebo vyvrátí.

Pro hlavní cíl byly stanoveny 4 hypotézy. Zaměřují se na edukaci a prevenci v oblasti rizikového chování na internetu a sociálních sítích.

**H1** – Většina studentů, kteří byli edukováni ze strany školy nebo rodičů ohledně problematického chování na internetu, by neporušila pravidla bezpečného chování na internetu.

**H2** – Alespoň 75% studentů, kteří komunikují s rodiči o aktivitách na sociálních sítích a vzdělávají se v rámci bezpečného chování na internetu, by o sobě nesdíleli citlivé informace nebo fotografie.

**H3** – Rodiče, kteří využívají sociální sítě, více vzdělávají své děti ohledně správného chování a nástrah na internetu.

**H4** – Méně jak jedna třetina dotazovaných nebyla edukována ohledně bezpečného chování na sociálních sítích.

Dílčí cíl je ověřit chování studentů na sociálních sítích z různých hledisek. Pro tuto část bylo staveny čtyři hypotézy.

**H1** – Více jak dvě třetiny respondentů si hlídá, co o sobě sdělují na sociálních sítích.

**H2** – Méně jak polovina dotazovaných by poslala svou intimní fotografii bez zaznamenání obličeje.



**H3** – Méně jak 30% respondentů s někým sdílí citlivé informace jako je heslo, číslo nebo adresu bydliště.

**H4** – Většina respondentů neodepisuje na nechtěné zprávy.

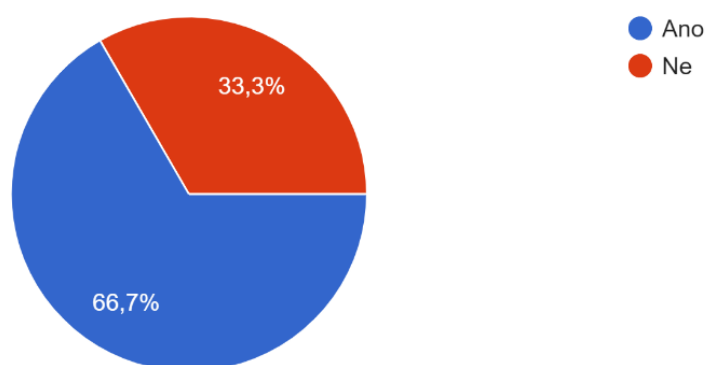
#### 4.5 Záznam a zpracování dat výzkumu

Dotazník byl vyplněn prostřednictvím internetu. K vytvoření byla využita služba společnosti Google. Skrz jejich formuláře byly otázky zadané a vyplněné. Služba sloužila k zaznamenání dat výzkumu. Ke zpracování bylo zvoleno tabulek, grafů i slovní interpretace. Číselné údaje jsou pro přehlednost zaokrouhlené na celá čísla. Následně byla data zpracována a porovnána se stanovenými hypotézami.

#### 4.6 Výsledky dotazníku

##### Otázka č. 1- Používají tvoji rodiče aktivně sociální sítě?

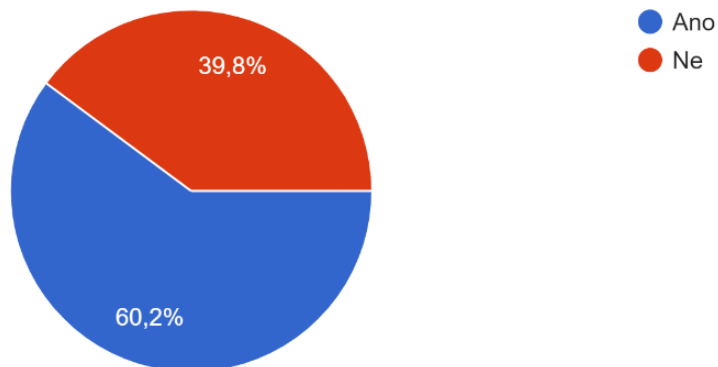
Obrázek 1- Graf znázorňující aktivitu rodičů na sociálních sítích



Ze 123 respondentů odpovědělo 82 kladně a 41 záporně. Procentuálně je zastoupení 66% ku 33%. V této otázce mě zajímalo, zda rodiče mají povědomí o fungování sociálních sítí z vlastní zkušenosti. Z dotazovaného vzorku respondentů vyplývá, že více jak 66% rodičů je aktivně využívá. Lze tak předpokládat, že většina rodičů používá sociální sítě a je schopná předat zkušenosti svým dětem.

## Otázka č.2- Bavili jste se s rodiči, jak se správně chovat na internetu a sociálních sítích?

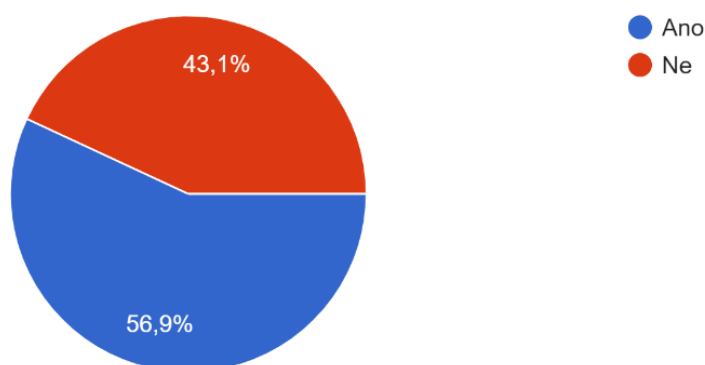
Obrázek 2- Graf znázorňující edukaci ze strany rodičů



V této otázce jsem se zajímala o prevenci ze strany rodičů. Zda se z vlastní iniciativy informují a vzdělávají své děti ohledně správného chování na internetu a s ním spojených sociálních sítích. Z výsledků lze vyčíst, že více jak polovina rodičů udělala základní opatření. Záporně odpovědělo 49 a kladně 74 respondentů. Rozdíl není tak rapidní jako u předchozí otázky a procentuálně činí 60% ku 40%.

## Otázka č. 3- Přišel/a by sis otevřeně promluvit s rodičem, kdyby nastal nějaký problém na sociálních sítích?

Obrázek 3- Graf znázorňující důvěru a komunikaci dětí s rodiči

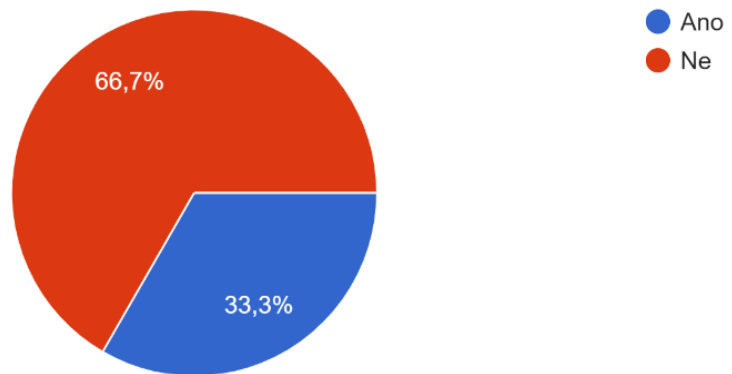


Respondenti na tuto otázku ohledně otevřenosti k rodičům reagovali více kladně. Z výzkumné otázky jsem se chtěla dozvědět otevřenost dětí a dospívajících vůči rodičům při možném vzniku potíží na sociálních sítích. Z celku odpovědělo 57% kladně a 43% záporně.

Otevřenost k rodičům v této oblasti by tak volilo 70 respondentů. Zbýlých 53 osob by se nesvěřilo svým rodičům.

**Otázka č. 4- Sledují rodiče tvoji aktivitu na sociálních sítích? (např. mají tvůj profil ve sledujících nebo se zajímají co tě na sítích baví)**

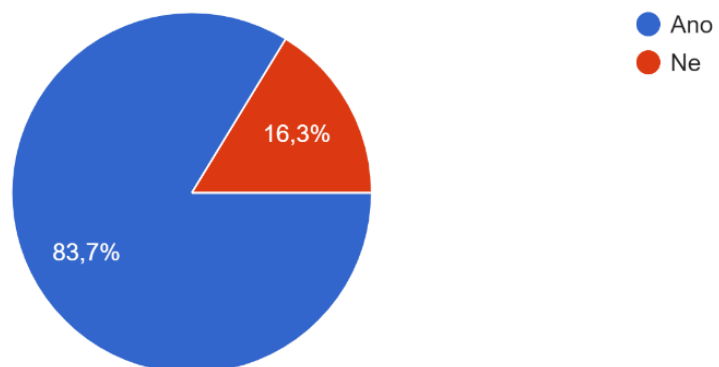
*Obrázek 4- Graf znázorňující zájem rodičů o aktivitě svých dětí na sociálních sítích*



Otázka se zaměřovala na povědomí rodičů o aktivitách svých dětí vykonávaných skrz sociální sítě. Z celkového počtu respondentů odpověděly negativně dvě třetiny, tedy 82 respondentů. Pozitivně odpovědělo pouze 33% respondentů, tedy 41 respondentů. Ze zkoumaného vzorku tedy vyplývá, že rodiče spíše nesledují aktivitu dětí a v tomto ohledu nemají přehled.

**Otázka č. 5- Měl/a si někdy na škole přednášku o tom, jak se chovat na internetu?**

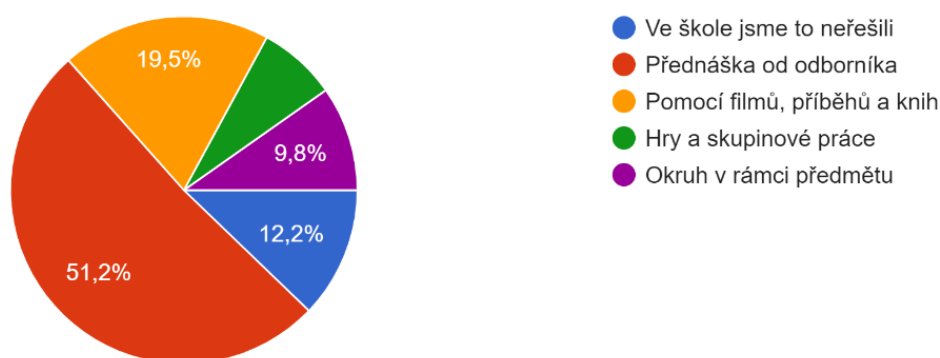
*Obrázek 5- Graf znázorňující prevenci školy v této oblasti*



Z celkového počtu 123 respondentů negativně odpovědělo 20 respondentů tedy 16%. Dokazuje to na většinové povědomí o správném chování uživatelů internetu. Pozitivně odpovědělo 103 respondentů, tedy 84%. Školy respondentů si uvědomují důležitost prevence v této oblasti. Škola tedy ve většině případů své žáky připravuje na jednání a užívání internetu.

#### **Otázka č. 6- Jakou formou tě škola vzdělávala ohledně bezpečného chování na internetu?**

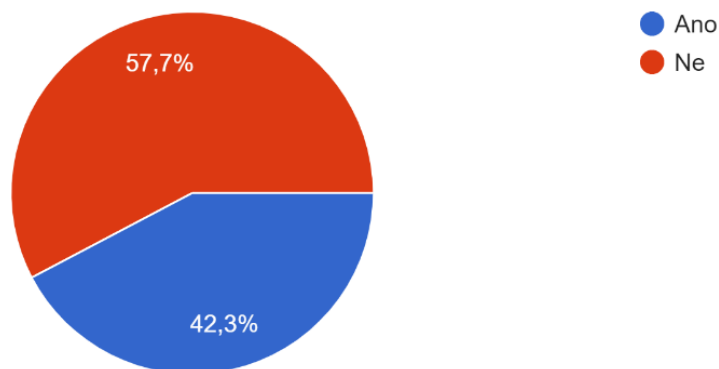
*Obrázek 6- Graf znázorňující formu prevence ve škole*



Výzkum ukázal rozmanitost škol v pojetí prevence. Většina škol zvolila cestu přednášky od odborníka na danou problematiku. Tuto možnost zvolilo 51% dotazovaných. Další používanou metodou je prevence spojená s audiovizuálními materiály a knihami, kterou zažilo 20% respondentů. Z dotazovaných 12% uvedlo, že problematiku neřešili ve škole vůbec. Prevence na školách se provozuje i během předmětů. Tuto odpověď zvolilo 10% respondentů. Pouze 7% respondentů zvolilo volbu více interaktivní pomocí her a skupinové práce.

**Otázka č. 7- Četl/a si někdy informace a materiály o bezpečném chování na internetu?**

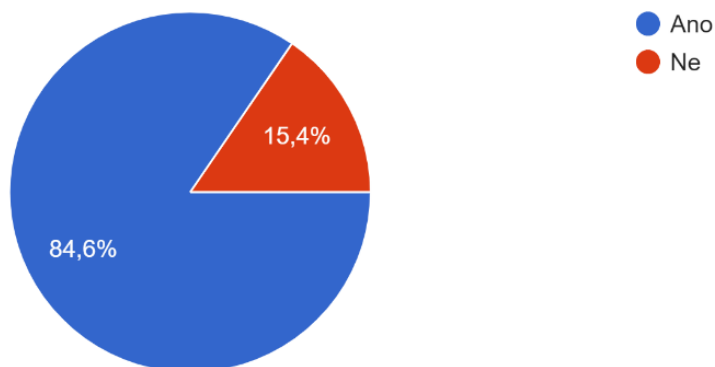
*Obrázek 7- Graf znázorňující samostudium materiálů o bezpečném chování*



Tato otázka dokazuje, že více jak polovina respondentů si sama informace nevyhledává. Z celkového počtu je to 71 dotazovaných (58%), kteří žádný materiál sami nestudovali. Podle mého názoru to dokazuje důležitost prevence a informovanosti ze strany školy a rodičů. Z dotazovaného vzorku si jen 52 respondentů (42%) informace nebo materiály samo vyhledává.

**Otázka č. 8- Hlídáš si soukromí a přemýšlíš co o sobě sdělovat na sociálních sítích?**

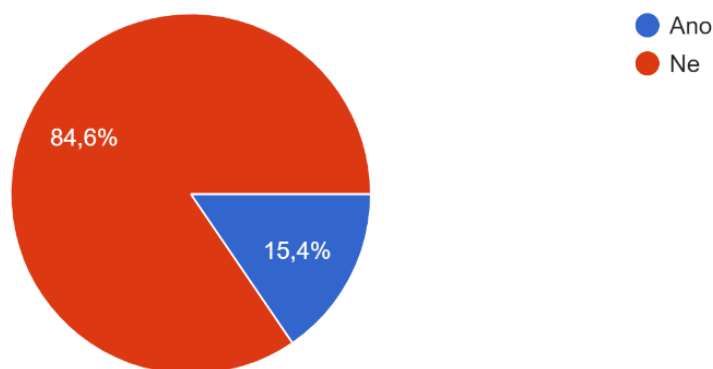
*Obrázek 8- Graf znázorňující opatrnost ve sdílení informací*



Otázka je zaměřená na ochranu soukromí a veřejné sdělování informací o sobě na sociálních sítích. Většina dotazovaných se o tuto složku zajímá a přemýšlí o svém soukromí. V celkovém počtu se jedná o 104 dotazovaných, vyjádřených v procentech 85%. Zbýlých 19 respondentů, tedy 15%, nevěnuje zvláštní pozornost sdíleným informacím.

**Otázka č. 9- Poslal/a bys někomu koho znáš jenom ze sociálních sítí citlivé informace (např. telefonní číslo, adresu kde bydlíš apod.)**

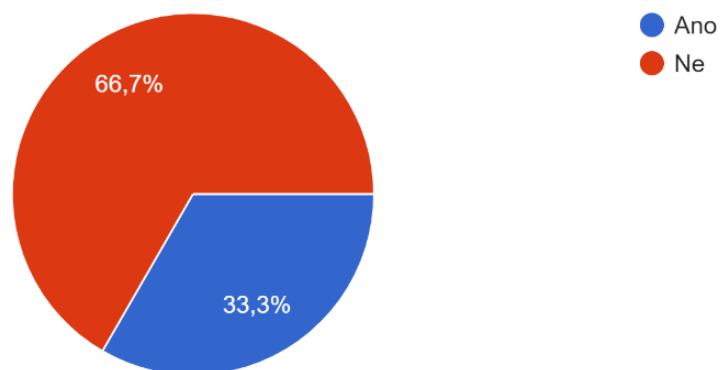
*Obrázek 9- Graf znázorňující ochranu citlivých informací*



Zde převládá jasný postoj k ochraně informací. Respondenti na tuto otázku v 85% odpověděli, že by žádné informace typu adresa nebo telefonní číslo nesdělili. Tedy z 123 dotazovaných osob by 104 reagovalo negativně. Naopak 15% respondentů by některé informace uživatelům poslalo, z dotazovaných je to 19 osob.

**Otázka č. 10- Otevřel/a si někdy podezřelý obsah/odkaz, který ti někdo poslal?**

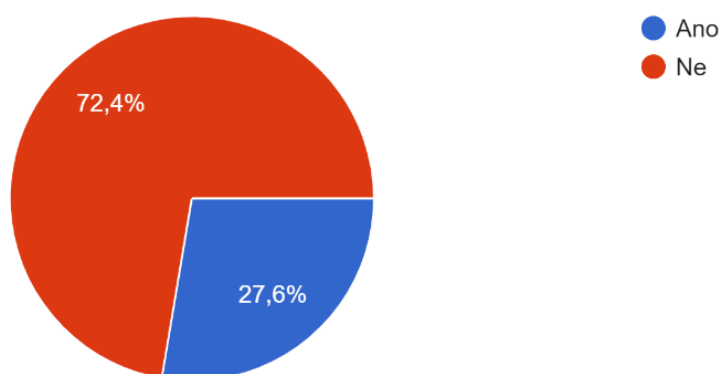
*Obrázek 10- Graf znázorňující obezřetnost při otevírání souborů*



Tato otázka se zaměřuje na ochranu proti napadení nebo podvodům na internetu. Jedna třetina dotazovaných má zkušenost s podezřelým obsahem nebo odkazem. S takovým jednáním se setkalo 41 respondentů. Dvě třetiny, tedy 82 osob, by se takovému jednání vyhnulo.

**Otázka č. 11- Setkal/a si se někdy osobně s člověkem, kterého si znal/a pouze přes sociální sítě, aniž by o tom někdo věděl?**

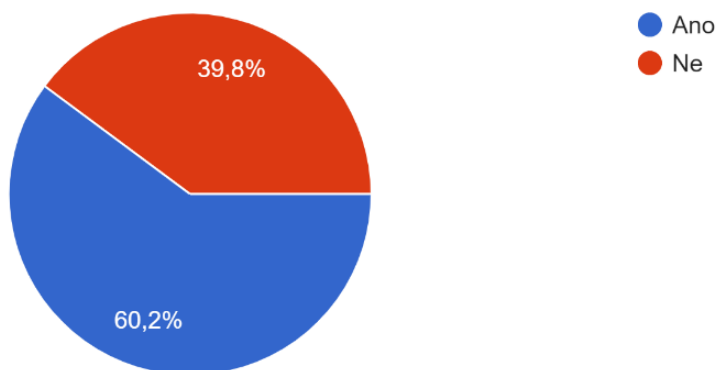
*Obrázek 11- Graf znázorňující opatrnost při osobním kontaktu*



Výzkumná otázka se zaměřuje na osobní kontakt s neznámou osobou. Výsledky dokazují, že 72% dotazovaných by se neseťkalo s neznámou osobou. Takto by jednalo 84 respondentů. Výzkum uvedl, že 28% má zkušenost se stykem s neznámou osobou a takto by jednalo 34 osob.

**Otázka č. 12- Máš v telefonu fotografie, co by nikdo jiný neměl vidět?**

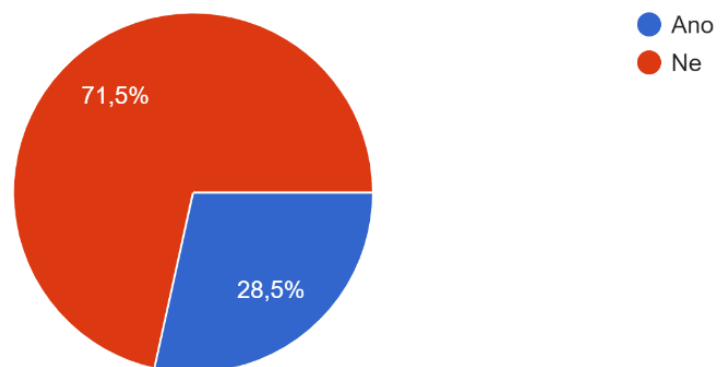
*Obrázek 12- Graf znázorňující výskyt citlivých fotografií*



Počet respondentů reagujících kladně je 60%, tedy více než polovina. 74 respondentů tedy vlastní tajné fotografie, které by se daly zneužít nebo by je mohly ohrozit. 40% respondentů, tedy 49 osob, nemá v telefonu citlivé fotografie. Výzkum ukazuje, že mnoho respondentů bere mobilní telefon jako trezor.

### Otázka č. 13- Poslal/a by si někomu s kým jsi v kontaktu intimní fotografie bez obličeje?

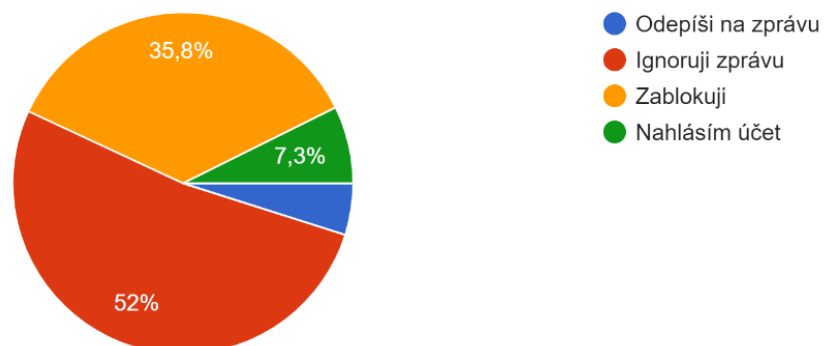
Obrázek 13- Graf znázorňující zaslání intimní fotografie



V této otázce převládá názor nesdílení intimních fotografií. Více jak polovina dotazovaných přesně 72% (88 osob) by fotografii neposlala. Zato 29% (35 osob) by ji bez zaznamenání obličeje zaslala. Z mého pohledu ukazuje výzkum atraktivitu zakázaných fotografií, kterou si dospívající a děti zpestřují konverzace.

### Otázka č. 14- Jak reaguješ na nevhodné zprávy od cizích lidí?

Obrázek 14- Graf znázorňující reakci na nevhodné zprávy





Reakce na nevhodné zprávy jsem rozdělila do čtyř skupin. Nejvíce početná byla odpověď ignorování zprávy. Takto odpovědělo 52% respondentů. Tuto možnost vyplnilo 64 osob. Na nevyžádanou zprávu reagují přehlédnutím. Dále 36% dotazovaných uvedlo že konverzaci zablokují, aby jim uživatel nemohl zasílat další zprávy. Druhou z možností uvedlo 44 respondentů. Ve třetí skupině osoby nahlásí účet, ze které zpráva přišla technické podpoře sociální sítě. Reakci používá 7% a takto reaguje 9 respondentů z celkového počtu. V neposlední řadě by na některé zprávy respondenti odpověděli. Z dotazovaných se takto vyjádřilo 5%, pouze 6 osob.

## 4.7 Analýza výsledků výzkumné části

V této části je provedena analýza získaných dat z výzkumné části a data jsou dále zpracovaná pro ověření hypotéz. Výsledky jsou zaznamenány formou grafů a tabulek. Následně jsou výsledky popsány a srovnány s hypotézami a jejich předpoklady. Hypotézy jsou rozděleny do dvou částí. První část je zaměřena na prevenci a edukaci studentů. Druhá je zaměřena na rizikové chování a chování studentů.

### 4.7.1 Hypotézy k hlavnímu cíli

**H1 – Většina studentů, kteří byli edukováni ze strany školy nebo rodičů ohledně problematického chování na internetu, by neporušila pravidla bezpečného chování na internetu.**

První hypotéza obsahuje myšlenku, že většina studentů, kteří prošli edukací ohledně bezpečného chování na internetu, nebude porušovat pravidla bezpečného chování na internetu. Tato analýza byla rozdělena do dvou kroků. První je zaměřená na výsledky bezpečného chování na internetu při edukaci od rodičů a druhá od školy. V návaznosti na to jsou porovnány data od edukovaných a needukovaných studentů.<sup>1</sup>

První část analýzy se zaměřuje na výsledky studentů edukovaných od rodičů. Z dotazníkových otázek toto řeší otázka č. 2. Proto jsou porovnávány výsledky studentů, kteří odpověděli na tuto otázku ano vs ti, kteří odpověděli ne. Tyto dva vzorky studentů se porovnávají v jejich chování a reakcí na problematické chování.

---

<sup>1</sup> První dva sloupce v tabulkách ukazují data edukovaných studentů, proto zkratka edu. Zbylé dva sloupce jsou pro data needukovaných studentů.

Porušování bezpečného chování na internetu bylo studováno v otázkách 8, 9, 10, 11 a 13. Předpokladem tedy je, že edukovaní studenti budou na tyto otázky odpovídat správně ve větším procentu případů.

**Výsledky dotazníkové šetření pro edukované/needukované studenty od rodičů jsou následující:**

*Tabulka 1- Pro edukované/needukované studenty od rodičů*

Otázky	ANO (edu)	NE (edu)	ANO	NE
Hlídáš si své soukromí a přemýšlíš co o sobě sdělovat na sociálních sítích?	93%	7%	71%	29%
Poslal/a bys někomu koho znáš jenom ze sociálních sítí citlivé informace? (např. telefonní číslo, adresu kde bydlíš apod.)	14%	86%	18%	82%
Otevřel/a si někdy podezřelý obsah/odkaz, který ti někdo poslal?	26%	74%	45%	55%
Setkal/a si se někdy osobně s člověkem, kterého si znal/a pouze přes sociální sítě aniž by o tom někdo věděl?	24%	76%	33%	67%
Poslal/a by si někomu s kým jsi v kontaktu intimní fotografii bez obličeje?	20%	80%	41%	59%

Z výsledků v této tabulce je viditelné, že u každé otázky většina studentů odpověděla tak, že by neporušila pravidla bezpečného chování na internetu.

1. 93% edukovaných studentů si hlídá své soukromí a přemýšlí co o sobě sdělovat na sociálních sítích.
2. 86% edukovaných studentů by neposlalo někomu koho zná jenom ze sociálních sítí citlivé informace.
3. 74% edukovaných studentů nikdy neotevřelo podezřelý obsah/odkaz, který jim někdo poslal.
4. 76% edukovaných studentů by se nikdy nesetkalo s člověkem, kterého by znali jenom přes sociální sítě aniž by o tom někdo věděl.
5. 80% edukovaných studentů by neposlalo někomu s kým je v kontaktu intimní fotografii bez obličeje.

Z výsledků tabulky lze tedy jednoznačně říct, že v části edukovaných studentů od rodičů byla hypotéza potvrzena.

Druhá část analýzy sleduje stejné otázky jako první s tím rozdílem, že sleduje edukaci od školy, která je obsažena v otázce č.5. V druhém kroku srovnává edukované

a needukované studenty. Otázky ve kterých se sleduje rizikové chování na internetu jsou stejné jako v první části.

**Výsledky dotazníkové šetření pro edukované/needukované studenty od školy jsou následující:**

*Tabulka 2- Pro edukované/needukované studenty od školy*

Otázky	ANO (edu)	NE (edu)	ANO	NE
Hlídáš si své soukromí a přemýšlíš co o sobě sdělovat na sociálních sítích?	86%	14%	75%	25%
Poslal/a bys někomu koho znáš jenom ze sociálních sítí citlivé informace? (např. telefonní číslo, adresu kde bydlíš apod.)	17%	83%	5%	95%
Otevřel/a si někdy podezřelý obsah/odkaz, který ti někdo poslal?	37%	63%	15%	85%
Setkal/a si se někdy osobně s člověkem, kterého si znal/a pouze přes sociální sítě aniž by o tom někdo věděl?	26%	74%	35%	65%
Poslal/a by si někomu s kým jsi v kontaktu intimní fotografii bez obličeje?	26%	74%	40%	60%

Z výsledků v této tabulce je viditelné, že u každé otázky většina studentů odpověděla tak, že by neporušila pravidla bezpečného chování na internetu.

1. 86% edukovaných studentů si hlídá své soukromí a přemýšlí co o sobě sdělovat na sociálních sítích.
2. 83% edukovaných studentů by neposlalo někomu koho zná jenom ze sociálních sítí citlivé informace.
3. 63% edukovaných studentů nikdy neotevřelo podezřelý obsah/odkaz, který jim někdo poslal.
4. 74% edukovaných studentů by se nikdy nesetkalo s člověkem, kterého by znali jenom přes sociální sítě aniž by o tom někdo věděl.
5. 74% edukovaných studentů by neposlalo někomu s kým je v kontaktu intimní fotografii bez obličeje.

Z výsledku tabulky lze tedy také konstatovat, že v části edukace od školy byla hypotéza potvrzena.

V rámci dodatečných zjištění a srovnání s needukovanými studenty lze také říct, že edukace je užitečná a funkční. V jednotlivých odpovědích se lišily výsledky až o několik desítek procent.

V obou případech, tedy edukace od školy i rodičů, byla hypotéza č.1 potvrzena.

**H2 Alespoň 75% studentů, kteří komunikují s rodiči o aktivitách na sociálních sítích a vzdělávají se v rámci bezpečného chování na internetu, by o sobě nesdíleli citlivé informace nebo fotografie**

Druhá hypotéza se věnuje myšlence, že studenti, kteří komunikují s rodiči o aktivitách na sociálních sítích a vzdělávají se v rámci bezpečného chování na internetu, by se o sobě nesdíleli citlivé informace nebo fotografie.

Komunikace s rodiči je v otázkách 2 a 3. Pokud tedy student odpověděl na otázku č. 2 nebo na otázku č. 3 ano, je v rámci analýzy veden tak, že komunikuje s rodiči o aktivitách na sociálních sítích. Vzdělávání o bezpečném chování na internetu je v otázce č.7. Studenti, kteří na tuto otázku odpověděli ano, jsou v analýze vyhodnocováni, jako že se vzdělávají.

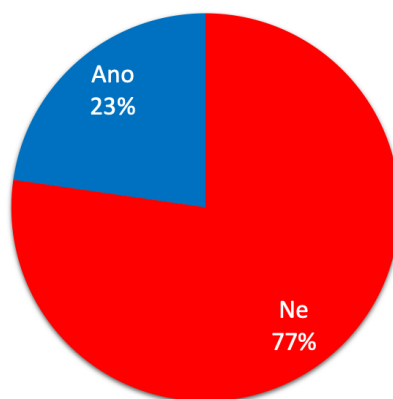
Porovnání jsou v oblasti otázek o sdílení citlivých informací, které jsou obsažené v otázce č. 9 a posílání citlivých fotografií v otázce č. 13.

Analýza vyhodnocuje u studentů, kteří komunikují s rodiči o aktivitách na soc. sítích a zároveň se vzdělávají, jestli by sdíleli citlivé informace nebo fotografie. Dodatečně pak analýza srovnává tuto skupinu se skupinou studentů, kteří se s rodiči nebaví o aktivitách na sociálních sítích a nevzdělávají se v rámci bezpečného chování na internetu.

První část analýzy se věnuje otázce odeslání intimní fotografie bez obličeje.

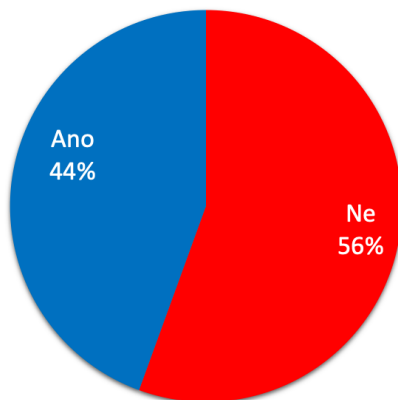
*Obrázek 15- Graf znázorňující variantu komunikují s rodiči a sebevzdělávají se*

**Poslal/a by si někomu s kým jsi v kontaktu intimní  
fotografii bez obličeje?  
(varianta komunikují s rodiči, vzdělávají se)**



Obrázek 16- Graf znázorňující variantu nekomunikují s rodiči a nevzdělávají se

**Poslal/a by si někomu s kým jsi v kontaktu intimní  
fotografii bez obličeje?  
(varianta NEkomunikují s rodiči, NEvzdělávají se)**



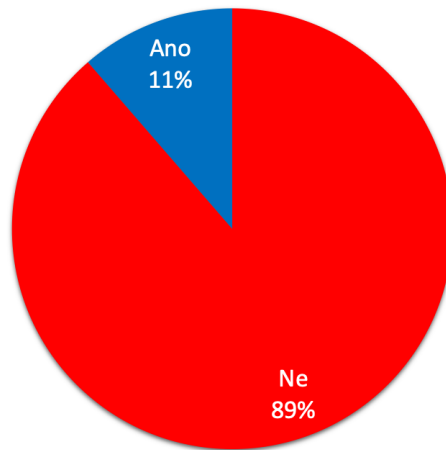
77% respondentů, kteří komunikují s rodiči nebo se vzdělávají v oblasti bezpečnosti by neposlalo někomu s kým je v kontaktu intimní fotografii bez obličeje. Tento výsledek potvrzuje hypotézu.

V dodatečném šetření bylo dále zjištěno, že se velmi liší výsledky studentů, kteří komunikují s rodiči a vzdělávají se oproti těm, kteří nekomunikují a nevzdělávají se (detail viz výše). V prvním případě by fotku neposlalo 77% studentů, ale v tom druhém už pouze 56%. Je tedy viditelné, že komunikace s rodiči a vzdělávání se o bezpečném chování na internetu má svůj velký význam a studenti se díky těmto informacím chovají lépe na sítích a vystavují se méně rizikům.

Druhá část analýzy se věnuje sdílení citlivých informací.

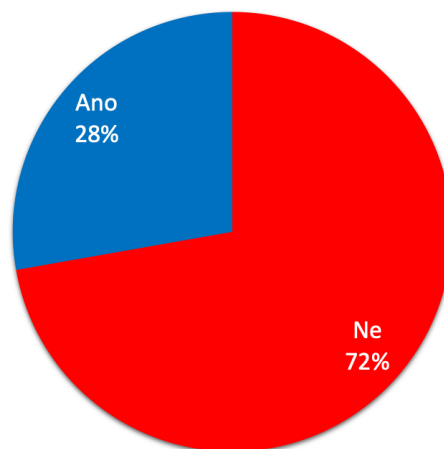
Obrázek 17- Graf znázorňující variantu komunikují s rodiči a sebevzdělávají se

**Poslal/a bys někomu koho znáš jenom ze sociálních sítí  
citlivé informace?  
(varianta komunikují s rodiči, vzdělávají se)**



Obrázek 18- Graf znázorňující variantu nekomunikují s rodiči a nevzdělávají se

**Poslal/a bys někomu koho znáš jenom ze sociálních sítí  
citlivé informace?  
(varianta NEkomunikují s rodiči, NEvzdělávají se)**



89% respondentů, kteří komunikují s rodiči a vzdělávají se, odpovědělo, že by neposlalo někomu, koho zná jen ze sociálních sítí, citlivé informace. Hypotéza tedy byla opět potvrzena.

V dodatečném šetření bylo dále zjištěno, stejně jako u předchozí otázky, že jsou odlišné výsledky u studentů, kteří nekomunikují s rodiči a nevzdělávají se v rámci bezpečného chování na internetu. V tomto případě odpovědělo 72% procent, že by neposlalo citlivé informace. Číslo je stále velmi vysoké, nicméně i tak je opět vidět pozitivní vliv komunikace s rodiči a sebevzděláváníí.

Obě části analýzy potvrzují hypotézu č.2. To znamená, že více jak 75% studentů, kteří komunikují s rodiči o aktivitách na sociálních sítích a vzdělávají se v rámci bezpečného chování na internetu, by o sobě nesdělili citlivé informace nebo fotografie.

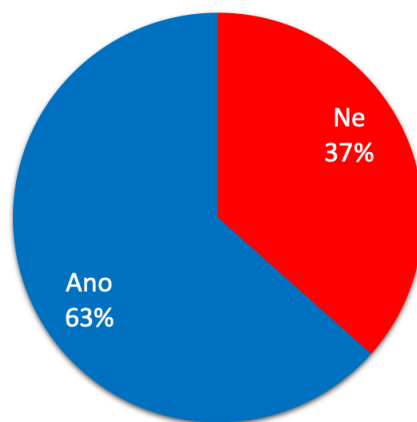
### **H3 – Rodiče, kteří využívají sociální sítě, více vzdělávají své děti ohledně správného chování a nástrah na internetu.**

Třetí hypotéza sleduje rodiče, kteří využívají sociální sítě a vzdělávání jejich dětí. Předpokládá se, že rodiče využívající sociální sítě se budou více zabývat edukací u svých dětí. Porovnání budou s rodiči, kteří na sociálních sítích nejsou.

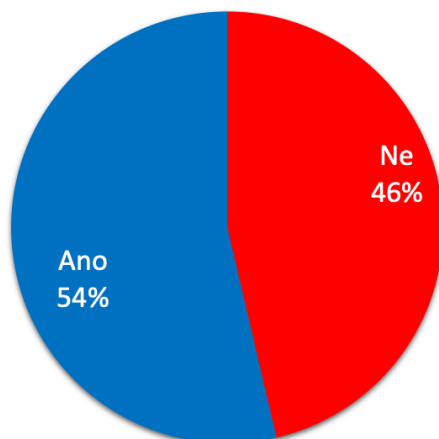
Využívání sociálních sítí je řešeno v otázce č. 1. a edukace dětí ohledně chování na internetu v otázce č. 2. Výsledné grafy jsou tak dva, kde základní rozdílem je u rodičů využívání/nevyužívání soc. sítí.

*Obrázek 19- Graf znázorňující prevenci rodičů, kteří využívajících sociální sítě*

#### **Bavili jste se s rodiči jak se správně chovat na internetu a sociálních sítích? (varianta - rodiče využívají sociální sítě)**



**Bavili jste se s rodiči jak se správně chovat na internetu a sociálních sítích?  
(varianta - rodiče nevyužívají sociální sítě)**



Výsledky jsou následující:

63% dětí řeklo, že se s rodiči bavili o tom, jak se správně chovat na internetu a sociálních sítích a 37% odpovědělo, že ne.

U rodičů, kteří sítě nepoužívají, byla čísla nižší, ačkoliv rozdíl není tolik výrazný. 54% dětí odpovědělo, že se s rodiči bavilo o tom, jak se správně chovat na internetu a sociálních a 46% odpovědělo, že ne.

Je zde tedy vidět určitá pozitivní vazba mezi využíváním soc. sítí u rodičů a následnou komunikací s dětmi, nicméně rozdíl je pouhých 9%.

Hypotéza byla výsledky potvrzena. Tedy že rodiče více vzdělávají své děti, pokud sami využívají sociální sítě.

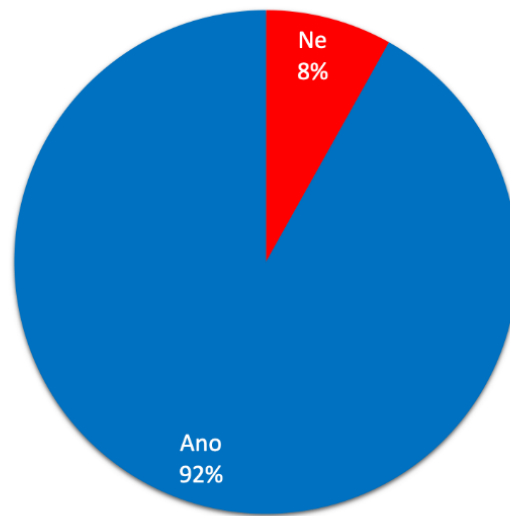
**H4 – Méně jak jedna třetina dotazovaných nebyla edukována ohledně bezpečného chování na sociálních sítích.**

Tato hypotéza pracuje s edukací studentů od rodičů (otázka č. 2) a od školy (otázka č. 5). Předpokladem hypotézy je, že méně jak 1/3 studentů nebyla od těchto dvou zdrojů edukována. Edukováni studenti jsou ti, kteří tedy odpověděli ano buď na otázku č. 2 nebo na otázku č. 5., stačí tedy alespoň jedna kladná odpověď.



Obrázek 21- Graf znázorňující edukaci ohledně bezpečného chování

**Studenti byli edukováni ze strany školy nebo rodičů ohledně bezpečného chování na internetu**



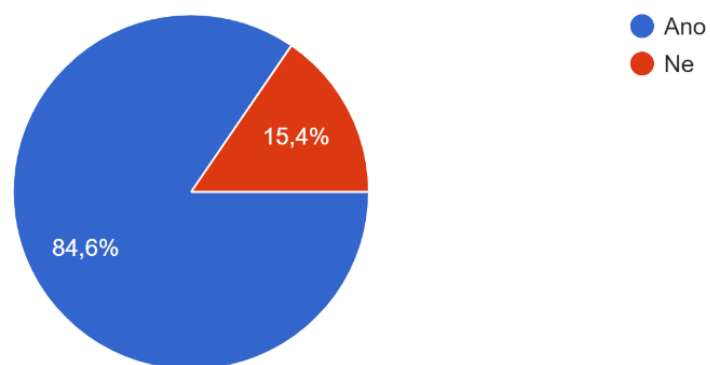
92% respondentů odpovědělo, že byli edukováni ohledně bezpečného chování na internetu a hypotéza tak byla potvrzena. Výsledky také dokazují, jak je prevence klíčovým tématem rodičů a škol.

## 4.7.2 Hypotézy k vedlejšímu cíli

**H1 – Více jak dvě třetiny respondentů si hlídá soukromí a co o sobě sdělují na sociálních sítích.**

Tato hypotéza předpokládá, že více než 2/3 respondentů si hlídá co o sobě sděluje na sociálních sítích. Hypotéza je zaměřena na fotografie a příspěvky, které sdělují na svých profilech. Otázka se také zaměřuje na nastavení soukromí na sociálních sítích. Tato problematika je řešena v otázce č. 8.

Obrázek 22- Graf znázorňující ochranu soukromí a sdílených informací na profilu

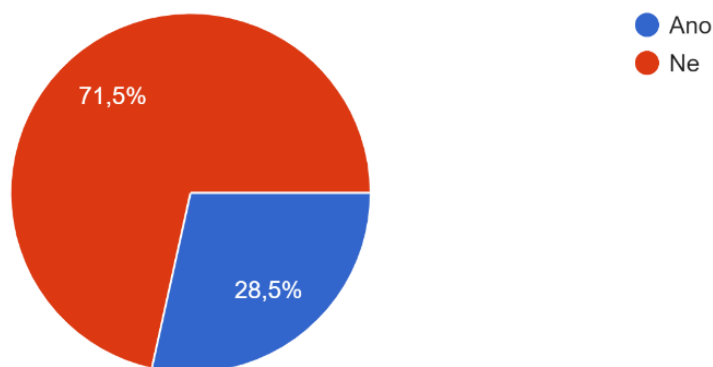


84% respondentů odpovědělo, že si hlídá své soukromí a přemýšlí co o sobě sděluje na sociálních sítích. Hypotéza tak byla výzkumnou otázkou potvrzena.

**H2 – Méně jak polovina dotazovaných by poslala svou intimní fotografii bez zaznamenání obličeje.**

Tato hypotéza předpokládá, že méně než 50% studentů by poslalo svou intimní fotografii bez zaznamenání svého obličeje. Číslo bylo dáno relativně vysoké, protože sdílení intimních fotografií je dost lákavá oblast, které se studenti rádi zúčastňují. Edukace bezpečného chování je podle ostatních výsledků na dobré úrovni, ale zasílání lechtivého obsahu by mohli studenti vnímat jinak a považovat ho za nerizikové. Tato hypotéza má vazbu na otázku č. 13.

Obrázek 23- Graf znázorňující zaslání intimní fotografie

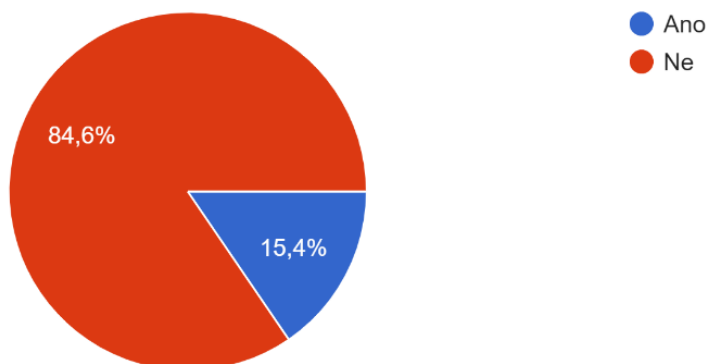


72% respondentů odpovědělo, že by neposlalo intimní fotografii bez obličeje. Pouze 28% by tak svou intimní fotografii poslalo. Hypotéza tak byla potvrzena a předpoklad byl překonán o velký rozdíl.

**H3-Méně jak 30% respondentů by sdílela s někým koho zná jenom ze sociálních sítích citlivé informace jako je telefonní číslo, adresu bydliště apod.**

Tato hypotéza se věnuje tématu sdílení citlivých informací a předpokládá, že pouze méně jak 30% studentů by tyto citlivé informace s někým sdílelo. Je zde velký předpoklad, že si respondenti hlídají soukromí. Vstupy pro hypotézu jsou vedené v otázce č. 9.

Obrázek 24- Graf znázorňující sdílení citlivých informací

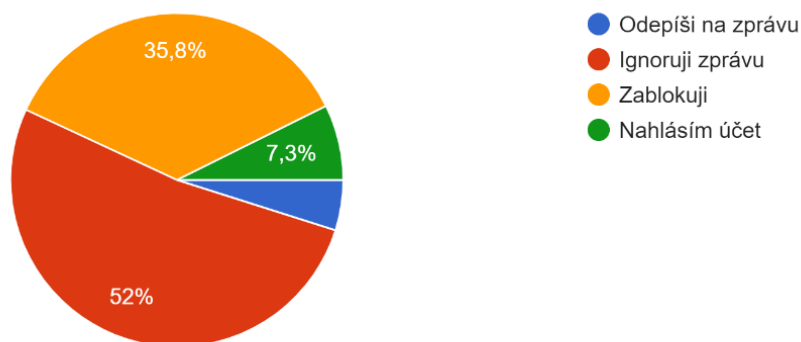


85% respondentů odpovědělo, že by neposlalo své citlivé informace někomu, koho zná jenom přes sociální sítě. Tzn. pouze 15% by své citlivé informace poslalo přes sociální sítě, což je číslo menší než 30%. Hypotéza tak byla potvrzena.

#### H4-Většina respondentů neodepisuje na nechtěné zprávy.

Hypotéza č. 4. se věnuje tématu reakce na nechtěné zprávy. Předpokladem je, že většina respondentů vzhledem k široké edukaci v tomto tématu neodpovídá na nechtěné zprávy. Odepisování na zprávy řeší otázka č. 14.

Obrázek 25- Graf znázorňující reakce na zprávy



5% respondentů odpovědělo, že na zprávu odepíšou

7% respondentů odpovědělo, že nahlásí účet

39% respondentů odpovědělo, že uživatele zablokují

52% respondentů odpovědělo, že zprávu ignorují

Z toho vyplývá, že celkově pouze 5% studentů by na zprávu odpovědělo. Hypotéza tak byla potvrzena. Respondenti se v tomto případě ve většině shodli na bezpečném postupu.

#### 4.8 Shrnutí výzkumné části

V analýze výzkumných otázek, byly potvrzeny všechny stanovené hypotézy. Hlavní cíl výzkumné části byl naplněn. Byl prokázán pozitivní dopad prevence na problematiku chování na internetu a sociálních sítích, kdy hlavním zdrojem prevence je edukace od rodičů nebo školy. Z praktické části je vidět, jaký pozitivní vliv má na děti a dospívající prevence a edukace v oblasti bezpečného chování na internetu. Od školy se prevence a edukace dostalo 84% dotazovaným.

Velmi významný byl u analýzy rozdíl mezi studenty, kteří byli edukováni v tématu bezpečného chování a těmi, kteří nebyli. Výsledky otázek týkajících se rizikového chování a správných odpovědí na ně se leckdy lišily i o desítky procent.

Mile mě překvapilo, že na edukaci mají velký podíl i rodiče. Informují své děti v této oblasti a vytváří důvěryhodný prostor pro svěřeni se v případě problémů. Z analýzy dat vyplynulo, že u respondentů má edukace od rodičů dobrý vliv na bezpečné chování na internetu.

Díky dílčímu cíli jsem si ve výzkumné části ověřila daty chování studentů na sociálních sítích mimo jiné z hlediska potenciálního nebezpečí. Tím jsem si chtěla ověřit informace, které jsem získala a prezentovala v teoretické části mé bakalářské práce.

Zaskočila mě informace, že rodiče nesledují aktivitu svých dětí. Nemají tedy přehled o tom, co se na profilech dětí objevuje. Respondenti ve 2/3 odpověděli, že se rodiče nezajímají, co je na sítích baví a nejsou ve sledujících jejich profilu.

Další zajímavostí je výsledek výzkumu, který ukazuje, jaké citlivé informace se skrývají v telefonech dětí a dospívajících. Výsledek mluví o 60%, kteří by nechtěli ukázat svou fotogalerii někomu jinému. Důležité ovšem je, že by citlivé fotografie ve většině neposlali dál.

## Diskuze

V této části zhodnotím výsledky závěrečné práce. V teoretické části jsem se věnovala postupně rizikům online světa, abych zjistila, kde se děti a dospívající mohou stát obětmi útoků nebo se setkat s nevhodným chováním. V praktické části jsem se pak v první polovině zabývala prevencí tohoto rizikového chování pomocí edukace ze strany školy nebo rodičů. Mým cílem bylo zjistit, jak velký vliv má edukace na prevenci těchto aktivit.

Díky výzkumu se potvrdily všechny stanovené hypotézy. Výsledky dotazníku poukázaly na velmi dobrou informovanost dětí a dospívajících. Školy se ve velké míře zabývají prevencí této problematiky. Bohužel mám z výsledků pocit, že edukace je spíše povrchová. Většina respondentů měla pouze přednášku od odborníka. Myslím si, že by bylo vhodné studenty vzdělávat v oblasti bezpečnosti na internetu více do hloubky. V rámci studia ke kapitole prevence jsem otevřela mnoho materiálů, které mohou učitelé k výuce prevence využívat. První věc, co mě zarazila, je, že se s edukací o internetu může začínat již v nízkém věku dětí. U malých dětí se dají využívat příběhy, pohádky nebo hry. Dále se prevence může provádět velice zajímavě přes skupinové či interaktivní aktivity. Metod a materiálů je spousta pro různé věkové skupiny. Jen by je školy mohly více využívat, protože přednášku si děti jinak jen odsedí a nijak zvlášť se aktivně nezapojí.

Z mého výzkumného vzorku vyšlo, že velké procento, přesně 92%, bylo edukováno ohledně bezpečného chování na internetu buď ze strany školy nebo rodičů. Výsledky ukázaly, jak velký vliv má prevence od rodiny. Obzvláště data, která poukazují na to, že prevence od rodičů funguje lépe než ta od školy. Rizikové chování bylo nižší než u respondentů edukovaných ze strany školy. Z výzkumu také vyšlo, že se velký počet rodičů nijak aktivně nezajímá, co jejich děti na sociálních sítích dělají. Podle respondentů jejich profily nesledují a neptají se na jejich aktivity a obecně události v online světě. Přesto děti v rodičích cítí útočiště a svěřily by se jim, kdyby vznikl nějaký problém nebo by se setkaly s rizikovým chováním.

V části věnované samotným rizikům většinou odpovědi respondentů korespondovaly s pravidly bezpečného chování na internetu. Překvapily mě výsledky hlavně dvou otázek ohledně zasílání fotografií a fotografií v telefonu. Intimní fotografii bez zaznamenání obličeje by poslalo 29% respondentů (35 osob). To je poměrně velké množství na to, že se jedná o nezletilé respondenty. Skoro ve všech knihách, článcích a materiálech se píše, jak snadno se takových fotografií dá zneužít. Přesto si dospívající tímto způsobem zpestřují

konverzace. To samé platí i u nevhodných fotografií, které ve 40% respondenti mají v telefonu, ale nechtěli by je nikomu ukázat. V obou případech se vystavují velkému riziku zneužití fotografií s možným následkem vydírání.

Samozřejmě mě díky výsledkům dotazníku napadají další otázky, na které bych se teď chtěla doptat. Více bych se třeba chtěla dozvědět o zasílání nechtěných zpráv. Například co v nich je napsáno, kolik z dotazovaných obdrželo intimní fotografii nebo kolik uživatelů jim píše.

Velice zajímavé by bylo prozkoumat i rizikové chování s přihlédnutím ke kraji respondentů. Informovanost o této problematice může být rozdílná i z tohoto hlediska. S vyšším počtem respondentů by byl ukazatel výsledku z mého pohledu daleko rozmanitější.

Myslím si, že velmi zajímavý výzkum by byl i z pohledu druhé strany od rodičů. Jak oni vnímají tuto problematiku, zda se s problematickým chováním na internetu sami nsetkali nebo zda se opravdu nezajímají o dění na sociálních sítích u svých dětí. Protože z vlastní zkušenosti vím, že děti tohle mohou vnímat rozdílně. Rodiče je třeba sledují a děti o tom nemusí vědět, nebo třeba využívají falešný účet. Mohou také mít zapnuté aplikace rodičovské kontroly a sledovat co navštěvují.

Celkově lze říct, že edukace dětí ohledně bezpečného chování na internetu je jak pro školy, tak rodiče velkým tématem. Většina rodičů (60%) se edukaci věnuje a snaží se dětem předat informace jak se správně chovat na internetu. Naprostá většina škol (84%) vzdělává své studenty v tomto tématu. Většina těchto aktivit je ovšem prováděna pasivní formou. 51% aktivit jsou přednášky a 20% filmy, což nutně vede k nižší angažovanosti dětí. Nicméně i tak je vidět, že vzdělávání má pozitivní dopad, jak ukázaly výsledky, kde bylo srovnáváno rizikové chování edukovaných a needukovaných dětí. Pravděpodobnost rizikového chování byla u needukovaných studentů v několika oblastech vyšší o více než 20% v porovnání s edukovanými. Se vzděláváním by bylo tedy vhodné pokračovat i ze strany školy. Ideálně ovšem s rozšířením aktivit a zatraktivněním formy, kterou se tyto informace studentům předkládají.

## Závěr

Svou bakalářskou práci jsem psala na téma rizikového chování na internetu se zaměřením převážně na sociální sítě. V práci jsem se zaměřila především na děti a dospívající, kteří využívají sociální sítě nejvíce. Cílem práce bylo mimo jiné přiblížit rizika, kterým jsou děti a dospívající v dnešní době vystaveny.

Veškeré získané informace jak z teoretické, tak praktické části, jsou přínosné pro mé vzdělání a následné zaměstnání. Toto téma se vyvíjí velice rychle, a proto by se měla i rozvíjet prevence na školách. Díky vzdělání mohu vykonávat pozici metodika prevence či výchovného poradce, kteří se s tímto druhem rizik setkávají velice často. Má závěrečná práce mě obohatila o důležité informace, jak situacím předcházet a následně i řešit.

V teoretické části jsem proto z počátku rozvedla základní informace o sociálních sítích. Následně jsem rozepsala rizika, která se v dnešním online světě odehrávají. Práci jsem cíleně směřovala na děti a dospívající, kteří se v mnoha případech stávají obětí. O škodlivém a nebezpečném chování jsem jednotlivě napsala nezbytné informace a rozepsala, jak se snadno může stát uživatel obětí kybernetické kriminality.

V teoretické části jsem se seznámila s mnoha novými poznatky. Například manipulace s obětí, což je téma, které jsem měla možnost prozkoumat z různých příkladů rizikového chování. Pachatel využívá různých metod a způsobů, jak oběti ublížit nebo ji uškodit. Dále jsem pronikla do preventivních zásad, které napomáhají k obraně uživatelů sociálních sítí a internetu. Zjistila jsem jaké situace mohou nastat a jaké dopady může mít nerozvážené jednání.

V praktické části jsem využila získaných informací a na základě toho vytvořila dotazníkové šetření a sestavila hypotézy. Cílem výzkumu bylo zjistit, zda má edukace, primárně od rodičů nebo školy, pozitivní dopad na prevenci problematického chování na internetu a sociálních sítích. Dílčí cíl jsem stanovila na zmapování chování studentů na sociálních sítích mimo jiné z hlediska potenciálního nebezpečí. Z výzkumu vyplynulo, že edukace má pozitivní dopad na prevenci v oblasti rizikového chování na internetu a sociálních sítích. Z výzkumu také vyplynulo, že většina dotazovaných prošla edukací a v online prostoru se pohybují vesměs bezpečně.

Stanovené cíle mé bakalářské práce byly naplněny. Byla přiblížena rizika online prostředí a praktická část se zabývala prevencí a jejími dopady na rizikové chování.



## Seznam použité literatury a dalších informačních zdrojů

### Použitá literatura

ESSAU, Cecilia A. a Paul H. DELFABBRO. *Adolescent Addiction: Epidemiology, Assessment, and Treatment*. Druhé vydání. Elsevier Science, 2020. ISBN 978-0-12-818626-8.

CHATFIELD, Tom. *Digitální svět: 50 myšlenek, které musíte znát*. Slovar, 2013. ISBN 978-80-7391-720-3.

KOPECKÝ, Kamil a Veronika KREJČÍ. *Rizika virtuální komunikace: Příručka pro učitele a rodiče* [online]. Olomouc: NET UNIVERSITY, s.r.o, 2010 [cit. 2023-04-27]. ISBN 978-80-254-7866-0. Dostupné z: <https://www.e-bezpeci.cz/index.php/ke-stazeni/tiskoviny/14-rizika-internetove-komunikace-prirucka-pro-rodice-a-ucitele/file>

KOPECKÝ, Kamil a kol. *Rizikové formy chování českých a slovenských dětí v prostředí internetu* [online]. Olomouc: Vydavatelství Univerzity Palackého, 2015 [cit. 2023-04-24]. ISBN 978-80-244-4868-8. Dostupné z: <https://www.e-bezpeci.cz/index.php/ke-stazeni/odborne-studie/75-rizikove-chovani-ceskych-a-slovenskych-deti-v-prostredii-internetu-2015-monografie/file>

KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně na internetu: Průvodce chování ve světě online*. Praha: Grada, 2016. ISBN 978-80-247-5595-3.

ROGERS, Vanessa. *Kyberšikana: Pracovní materiály pro učitele a žáky i studenty*. Praha: Portál, 2011. ISBN 978-80-7367-984-2.

ŠEVČÍKOVÁ, Anna a kol. *Děti a dospívající online: vybraná rizika používání internetu*. Praha: Grada, 2014. ISBN 978-80-247-5010-1.

### Internetové zdroje

BEZPEČNĚ ONLINE. Desatero. *Bezpečně online* [online]. 2016 [cit. 2023-06-05]. Dostupné z: <https://bezpecne-online.ncbi.cz/surfuj-bezpecne/item/433-desatero-bezpecne-online>

BUĎ SAFE ONLINE. *Pro média* [online]. [cit. 2023-06-21]. Dostupné z: <https://www.avast.com/cz/besafeonline/pro-media>

BURÝŠEK, Jiří. Fakta: Kyberšikanu trestní právo nezná. Objevuje se ale čím dál častěji. *Seznam Zprávy* [online]. 11.10. 2020 [cit. 2023-04-16]. Dostupné z:

<https://www.seznamzpravy.cz/clanek/fakta-kybersikanu-trestni-pravo-nezna-objevuje-se-ale-cim-dal-casteji-123355>

BURDOVA, Carly. What Is Cyberstalking and How to Stop It. *Avast* [online]. 2022 [cit. 2023-05-07]. Dostupné z: <https://www.avast.com/c-cyberstalking>

ČESKÁ BANKOVNÍ ASOCIACE. Nejčastější typy podvodů. *Kybertest* [online]. 2022 [cit. 2023-05-14]. Dostupné z: <https://www.kybertest.cz/nejcastejsi-typy-podvodu>

ČT 24. Počet podvodů na internetu stále roste. Jen loni lidé přišli o více než dvě miliardy. *ČT 24* [online]. 13.2.2023 [cit. 2023-05-12]. Dostupné z: <https://ct24.ceskatelevize.cz/domaci/3564580-pocet-podvodu-na-internetu-stale-roste-jen-loni-lide-prisli-o-vice-nez-dve-miliardy>

DĚTSKÉ KRIZOVÉ CENTRUM. *Jaké služby poskytujeme* [online]. [cit. 2023-06-21]. Dostupné z: <https://www.ditekrize.cz/o-detskem-krizovem-centru/>

DOLEŽALOVÁ, Pavlína. Snapchat: děcka, žijte přítomností – ale opatrně!. *Linka bezpečí* [online]. 2018 [cit. 2023-05-05]. Dostupné z: <https://www.linkabezpeci.cz/-/snapchat-decka-zijte-pritomnosti-ale-opatrne>

E-BEZPEČÍ. Alarmující nárůst případů vydírání (sextortion) v kyberprostoru, E-Bezpečí bojuje v první linii. *E-bezpečí* [online]. 3.6.2023 [cit. 2023-06-22]. Dostupné z: <https://www.e-bezpeci.cz/index.php/rizikove-jevy-spojene-s-online-komunikaci/socialni-site/3310-alarmujici-narust-pripadu-vydirani-sextortion-v-kyberprostoru-e-bezpeci-bojuje-v-prvni-linii>

E-BEZPEČÍ. *Základní informace o projektu* [online]. [cit. 2023-06-21]. Dostupné z: <https://www.e-bezpeci.cz/index.php/o-projektu/oprojektu>

EMPEY, Charlotte. Jak si nastavit silné heslo. *Avast* [online]. 31. 1. 2019 [cit. 2023-06-05]. Dostupné z: <https://blog.avast.com/cs/jak-si-nastavit-silne-heslo>

ESET. 4 nejčastější podvody na českém internetu. *Dvojklik.cz* [online]. 21.9.2022 [cit. 2023-05-12]. Dostupné z: <https://www.dvojklik.cz/4-nejcastejsi-podvody-na-ceskem-internetu/>

ESET. Sexting je běžný pro třetinu z nás, není ale bez rizika. *Dvojklik.cz* [online]. 24. 8. 2022 [cit. 2023-05-05]. Dostupné z: <https://www.dvojklik.cz/sexting-je-bezny-pro-tretinu-z-nas-neni-ale-bez-rizika/>

GEORGIEV, Deyan. How Much Time Do People Spend on Social Media in 2023?. *Techjury* [online]. 10. 7. 2023 [cit. 2023-07-22]. Dostupné z: <https://techjury.net/blog/time-spent-on-social-media/>

INTERNETEM BEZPEČNĚ. Desatero dobrého kybernetického rodiče: Je třeba se stát zodpovědným online rodičem. *Internetem bezpečně* [online]. [cit. 2023-06-12]. Dostupné z: <https://www.internetembezpecne.cz/internetem-bezpecne/rodice/desatero-dobreho-kybernetickeho-rodice/>

INTERNETEM BEZPEČNĚ. TikTok: Co byste měli vědět o nejrychleji rostoucí sociální síti dneška. *Internetem bezpečně* [online]. 23.10.2019 [cit. 2023-03-11]. Dostupné z: <https://www.internetembezpecne.cz/tiktok-co-byste-meli-vedet-o-nejrychleji-rostouci-socialni-siti-dneska/>

JSNS. Semináře, webináře a kurzy pro vyučující. Jeden svět na školách [online]. [cit. 2023-06-12]. Dostupné z: <https://www.jsns.cz/vzdelavani-vyucujicich/seminare-kurzy>

JSNS.CZ. *O nás* [online]. [cit. 2023-06-21]. Dostupné z: <https://www.jsns.cz/o-jsns/o-nas>

KLEMENT, Vítězslav. Marketákův průvodce po sociálních sítích: Instagram. *Mediaguru* [online]. 29. března 2022 [cit. 2023-03-11]. Dostupné z: <https://www.mediaguru.cz/clanky/2022/03/marketakov-pruvodce-po-socialnich-sitich-instagram/>

KOPECKÝ, Kamil. Strategie manipulace dětí v online prostředích se zaměřením na tzv. kybergrooming. *Pediatric pro praxi* [online]. 2015, 15.7.2015, **16**(5) [cit. 2023-04-28]. Dostupné z: <https://www.pediatricpropraxi.cz/pdfs/ped/2015/05/09.pdf>

KOPECKÝ, Kamil. Stručný úvod do problematiky online vydírání českých dětí se zaměřením na tzv. sextortion. *Pediatric pro praxi* [online]. 2014, **15**(6) [cit. 2023-05-06]. Dostupné z: <https://www.pediatricpropraxi.cz/pdfs/ped/2014/06/07.pdf>

KOPECKÝ, Kamil. Co je syndrom FoMO. *E-bezpečí* [online]. 4. 4. 2017. [cit. 2023-05-16]. Dostupné z: <https://www.e-bezpeci.cz/index.php?view=article&id=1229>

KOPECKÝ, Kamil. Úloha primární prevence aneb Jak informovat o rizikových jevech spojených s internetem. *E-bezpečí* [online]. 2017 [cit. 2023-05-22]. Dostupné z: <https://www.e-bezpeci.cz/index.php/rodicum-ucitelum-zakum/1235-uloha-prevence>

KOPECKÝ, Kamil. Netiketa, pravidla slušného chování uživatelů internetu. *E-bezpečí* [online]. 23. 5. 2021 [cit. 2023-05-28]. Dostupné z: <https://www.e-bezpeci.cz/index.php/2-uncategorised/2219-netiketa-pravidla-slusneho-chovani-uzivatelu-internetu>

LINKA BEZPEČÍ. *O nás* [online]. [cit. 2023-06-21]. Dostupné z: <https://www.linkabezpeci.cz/o-nas>

LIVINGSTONE, Sonia a Leslie HADDON. *EU Kids Online: Final Report* [online]. 2009 [cit. 2023-04-03]. Dostupné z: <http://eprints.lse.ac.uk/24372/1/EU%20Kids%20Online%20final%20report%202009%28lsero%29.pdf>

MORAVČÍK, Ondřej. Vývoj registrované kriminality v roce 2022. *Policie České republiky* [online]. 13.1.2023 [cit. 2023-05-9]. Dostupné z: <https://www.policie.cz/clanek/vyvoj-registrovane-kriminality-v-roce-2022.aspx>

NGSS. 10 rad pro bezpečné chování na internetu. *NGSS* [online]. 17. 3. 2020 [cit. 2023-06-06]. Dostupné z: <https://www.ngss.cz/clanek/54-10-rad-pro-bezpecne-chovani-na-internetu>

O'CONNELL, BRIAN. History of Snapchat: Timeline and Facts. *TheStreet* [online]. 28.2.2020 [cit. 2023-03-13]. Dostupné z: <https://www.thestreet.com/technology/history-of-snapchat>

O2 CHYTRÁ ŠKOLA. Kybergrooming. *O2 Chytrá škola* [online]. [cit. 2023-05-02]. Dostupné z: <https://vyuka.o2chytraskola.cz/clanek/25/kybergrooming/14364>

O2 CHYTRÁ ŠKOLA. Kyberstalking. *O2 Chytrá škola* [online]. [cit. 2023-05-07]. Dostupné z: <https://vyuka.o2chytraskola.cz/clanek/26/kyberstalking/14369>

O2 CHYTRÁ ŠKOLA. *O nás* [online]. [cit. 2023-06-21]. Dostupné z: <https://o2chytraskola.cz/o-nas>

POLICIE ČR. Kyberkriminalita. *Policie České republiky* [online]. 2019 [cit. 2023-04-18]. Dostupné z: <https://www.policie.cz/clanek/kyberkriminalita.aspx>

PORTÁLDIGI. Netiketa aneb slušnost platí všude. *PortálDigi* [online]. 13. 12. 2018 [cit. 2023-05-28]. Dostupné z: <https://portaldigi.cz/netiketa-aneb-slusnost-plati-vsude/>

RECMANOVÁ, Alena. Pravidla netikety. *Medium* [online]. 30. 11. 2017 [cit. 2023-05-29]. Dostupné z: <https://medium.com/edtech-kisk/pravidla-netikety-ea92f7c3e58b>

SADÍLKOVÁ, Zuzana. Děti a digitální technologie. *Psychiatrie pro praxi* [online]. 2020 [cit. 2023-05-17]. Dostupné z: <https://www.psychiatriepropraxi.cz/pdfs/psy/2021/01/14.pdf>

SATRAPA, Pavel. Netiketa. *Lupa.cz* [online]. 31. 3. 2005 [cit. 2023-05-29]. Dostupné z: <https://www.lupa.cz/clanky/netiketa/>

SMAHEL, D., MACHACKOVA, H., MASCHERONI, G., DEDKOVA, L., STAKSRUD, E., ÓLAFSSON, K., LIVINGSTONE, S., and HASEBRINK, U. *EU Kids Online 2020: Survey results from 19 countries*. [online]. 2020 [cit. 2023-04-15]. Dostupné z: <https://www.eukidsonline.ch/files/Eu-kids-online-2020-international-report.pdf>

STÁTNÍ ZDRAVOTNÍ ÚSTAV. Netolismus: závislost na tzv. virtuálních drogách. *Nzip.cz* [online]. [cit. 2023-05-14]. Dostupné z: <https://www.nzip.cz/clanek/259-netolismus>

VANÍČKOVÁ, Vanda. YouTube, spojenec při rozvoji gramotností. *Metodický portál RVP.CZ* [online]. 21. 1. 2019 [cit. 2023-03-12]. Dostupné z: <https://clanky.rvp.cz/clanek/s/Z/21979/YOUTUBE-SPOJENEC-PRI-ROZVOJI-GRAMOTNOSTI.html>

VIEWEGOVÁ, Martina. Netolismus. *Internetem bezpečně* [online]. 5. 11. 2019 [cit. 2023-05-14]. Dostupné z: <https://www.internetembezpecne.cz/netolismus/>

VOJTÍŠEK, Petr. *Výzkumné metody* [online]. Praha, 2012 [cit. 2023-06-26]. ISBN 978-80-905109-3-7. Dostupné z: [https://skoly.praha.eu/files/=84121/Skripta\\_-\\_V%C3%BDzkumn%C3%A9\\_metody.pdf](https://skoly.praha.eu/files/=84121/Skripta_-_V%C3%BDzkumn%C3%A9_metody.pdf)

Zákon č. 40/2009 Sb. *Zákony pro lidi* [online]. 2009 [cit. 2023-04-18]. Dostupné z: <https://www.zakonyprolidi.cz/cs/2009-40#f3920268>

ZORMANOVÁ, Lucie. Kyberšikana v České republice a v zahraničí. *Metodický portál RVP.CZ* [online]. 15.10.2019 [cit. 2023-04-13]. Dostupné z: <https://clanky.rvp.cz/clanek/c/Z/22075/kybersikana-v-ceske-republice-a-v-zahranici.html>

## Seznam obrázků a tabulek:

Obrázek 1- Graf znázorňující aktivitu rodičů na sociálních sítích .....	41
Obrázek 2- Graf znázorňující edukaci ze strany rodičů .....	42
Obrázek 3- Graf znázorňující důvěru a komunikaci dětí s rodiči.....	42
Obrázek 4- Graf znázorňující zájem rodičů o aktivitě svých dětí na sociálních sítích.....	43
Obrázek 5- Graf znázorňující prevenci školy v této oblasti .....	43
Obrázek 6- Graf znázorňující formu prevence ve škole.....	44
Obrázek 7- Graf znázorňující samostudium materiálů o bezpečném chování .....	45
Obrázek 8- Graf znázorňující opatrnost ve sdílení informací .....	45
Obrázek 9- Graf znázorňující ochranu citlivých informací.....	46
Obrázek 10- Graf znázorňující obezřetnost při otevírání souborů .....	46
Obrázek 11- Graf znázorňující opatrnost při osobním kontaktu .....	47
Obrázek 12- Graf znázorňující výskyt citlivých fotografií .....	47
Obrázek 13- Graf znázorňující zaslání intimní fotografie.....	48
Obrázek 14- Graf znázorňující reakci na nevhodné zprávy .....	48
Obrázek 15- Graf znázorňující variantu komunikují s rodiči a sebevzdělávají se .....	52
Obrázek 16- Graf znázorňující variantu nekomunikují s rodiči a nevzdělávají se.....	53
Obrázek 17- Graf znázorňující variantu komunikují s rodiči a sebevzdělávají se .....	54
Obrázek 18- Graf znázorňující variantu nekomunikují s rodiči a nevzdělávají se.....	54
Obrázek 19- Graf znázorňující prevenci rodičů, kteří využívajících sociální sítě .....	55
Obrázek 20- Graf znázorňující prevenci rodičů, kteří nevyužívají sociální sítě .....	56
Obrázek 21- Graf znázorňující edukaci ohledně bezpečného chování.....	57
Obrázek 22- Graf znázorňující ochranu soukromí a sdílených informací na profilu.....	58
Obrázek 23- Graf znázorňující zaslání intimní fotografie.....	59
Obrázek 24- Graf znázorňující sdílení citlivých informací .....	59
Obrázek 25- Graf znázorňující reakce na zprávy .....	60

Tabulka 1- Pro edukované/needukované studenty od rodičů .....	50
Tabulka 2- Pro edukované/needukované studenty od školy.....	51