Univerzita Hradec Králové

Přírodovědecká fakulta

Katedra informatiky

Internetové sociální sítě a jejich využívání žáky středních škol

Diplomová práce

Autor: Bc. Markéta Marková

Studijní program: N1101 Matematika

Studijní obor: Učitelství pro střední školy – informatika
Učitelství matematiky pro střední školy

Vedoucí práce: doc. RNDr. Štěpán Hubálovský, Ph.D.

Hradec Králové červen 2015

Univerzita Hradec Králové

Přírodovědecká fakulta

Zadání diplomové práce

Autor:	**Bc. Markéta Marková**
Studijní program:	N1101 Matematika
Studijní obor:	Učitelství pro střední školy – informatika Učitelství matematiky pro střední školy
Název práce:	Internetové sociální sítě a jejich využívání žáky středních škol
Název práce v AJ:	Online social networks and their use by secondary school students
Cíl a metody práce:	Cílem teoretické části práce je popsat nejrozšířenější sociální sítě, možnosti jejich využití a bezpečnostní rizika spojená s jejich užíváním. Cílem praktické části práce je pomocí dotazníkového šetření zjistit, které sociální sítě a jak často žáci středních škol používají, zdali si uvědomují možná rizika a vědí, jak jim předcházet, případně jak je řešit.
Garantující pracoviště:	Katedra informatiky Přírodovědecká fakulta
Vedoucí práce:	doc. RNDr. Štěpán Hubálovský, Ph.D.
Oponent:	PhDr. Michal Musílek, Ph.D.
Datum zadání práce:	26. 3. 2014
Datum odevzdání práce:	

Prohlášení

Prohlašuji, že jsem diplomovou práci vypracovala samostatně a že jsem v seznamu použité literatury uvedla všechny prameny, z kterých jsem vycházela.

V Hradci Králové dne Markéta Marková

Poděkování

Tímto děkuji vedoucímu diplomové práce doc. RNDr. Štěpánu Hubálovskému Ph.D. za odborné vedení diplomové práce, cenné rady a připomínky, které mi pomohly k vypracování práce.

Anotace

MARKOVÁ, M. *Internetové sociální sítě a jejich využívání žáky středních škol.* Hradec Králové, 2015. Diplomová práce na Přírodovědecké fakultě Univerzity Hradec Králové. Vedoucí bakalářské práce doc. RNDr. Štěpán Hubálovský Ph.D. 84s.

Diplomová práce se zaměřuje na internetové sociální sítě a jejich využívání žáky středních škol. Cílem teoretické části je popsat nejrozšířenější druhy sociálních sítí, možnosti jejich využití a popsat bezpečnostní rizika, která jsou s jejich užíváním spojené. Cílem praktické části je pomocí dotazníkového šetření zjistit četnost využívání sociálních sítí žáky středních škol, jejich zkušenosti s nimi a podvědomí žáků o rizicích spojených s užíváním sociálních sítí.

Klíčová slova

internetové sociální sítě, nebezpečí na sociálních sítích, kyberšikana, kybergrooming, kyberstalking, projekty na ochranu dětí

Abstract

MARKOVÁ, M. *Online social networks and their use by secondary school students.* Hradec Králové, 2015. Diploma Thesis at Faculty of Science University of Hradec Králové. Thesis Supervisor doc. RNDr. Štěpán Hubálovský Ph.D. 84p.

Diploma thesis focuses on online social networks and the use of secondary school students. The aim of the theoretical part of the thesis is description of the most common types of social networks, their using and describtion of the security risks that are associated with above problem. The aim of the practical part is provide questionnaire survey for determination of the frequency of use of social networks between secondary school students, their experience with them and subconscious students about the risks associated with the use of social networks.

Keywords

social networks, danger of social network, cyberbullying, cyber grooming, cyberstalking, projects for children proteciton

Obsah

Úvod

Internetové sociální sítě jsou bezesporu fenoménem dnešní doby. Používají je miliardy lidí po celém světě. Sociální sítě se neustále mění a přizpůsobují novým trendům a požadavkům uživatelů. Záměrem jejich tvůrců je získat co největší uživatelskou základnu. Virtuální prostor, do kterého díky sociálním sítím vstupujeme, na nás působí tak, že nemá hranice ani omezení. Můžeme se, díky nim během vteřiny spojit s lidmi, kterým chceme něco sdělit a to bez ohledu na to, kde se právě nacházejí. Sociální sítě se staly součástí každodenního života mnoha z nás a lze bezpochyby říci, že výrazně ovlivňují životy lidí v naší společnosti. V současné době je v České republice rozšířeno a hojně používáno několik takovýchto služeb. Velkou část uživatelů sociálních sítí tvoří mladí lidé. Nezřídka se stává, že využívají i více různých sociálních sítí a tráví na nich spoustu volného času.

Cílem teoretické části práce je vytvořit literární rešerši v oblasti dané problematiky. Především seznámit čtenáře s pojmem internetové sociální sítě, s jejich typy, možnosti jejich využití a také s bezpečnostními riziky, které jsou s jejich užíváním přímo spjatá. Cílem praktické části práce je pomocí dotazníkového šetření zmapovat chování studentů středních škol na sociálních sítích, zjistit jejich preference určitých služeb i to, jak hodně času tráví na sociálních sítích a v neposlední řadě jestli si uvědomují a znají bezpečnostní rizika, která je mohou potkat.

Práce je strukturovaná do pěti kapitol. V úvodu první kapitoly se zabývám pojmem sociální síť, jeho prvotním významem i tím, jak tento pojem nejčastěji používáme dnes. Dále stručně popisuji historii a vývoj sociálních sítí, možnosti rozdělení sociálních sítí podle různých kritérií, jejich výhody a nevýhody a jak často jsou dnes používané. V druhé kapitole se zabývám konkrétními u nás nejčastěji používanými sociálními sítěmi. Snažím se popsat jejich základní charakteristiky a myšlenky. Ve třetí kapitole upozorňuji na rizika, se kterými se mohou žáci středních škol, při používání sociálních sítí setkat. Především se zaměřuji na kyberšikanu, kybergrooming a kyberstalking. Ve čtvrté kapitole připomínám fakt, že nejlepším řešením je problémům a nežádoucím situacím pomocí

preventivní činnosti předcházet. V druhé části kapitoly pak seznamuji čtenáře s projekty a organizacemi, které mohou pomoci při řešení výše zmíněných negativních jevů. V poslední páté kapitole analyzuji data pořízená pomocí dotazníkového šetření, kterého se zúčastnili právě žáci středních škol.

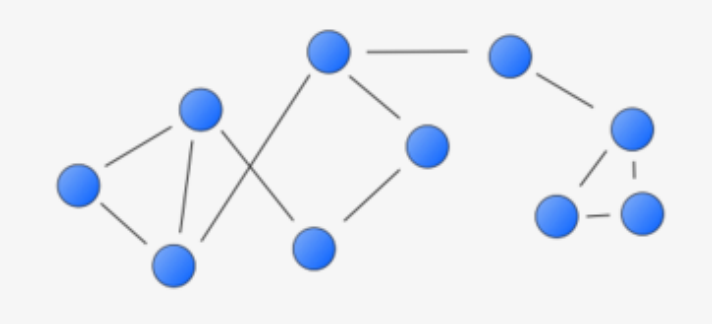
Práce je určena především pro žáky středních škol a jejich učitele, kterým by mohla pomoci při preventivní činnosti a osvětě na školách. Stejně tak je vhodná i pro rodiče, kteří nemají příliš zkušeností s informačními a komunikačními technologiemi a zajímají se o bezpečnost svých dětí na sociálních sítích potažmo na internetu.

1 Sociální síť

Ačkoliv se dnes s pojmem sociální síť setkáváme především ve spojitosti s internetem, poprvé jej použil v roce 1954 sociolog J. A. Barnes. Dle jeho definice je sociální síť určitá skupina lidí, kterou spojují rodinné vztahy, práce nebo koníčky [1].

Později sociologové tento pojem zpřesňují například A. Pavlíček uvádí: *„Sociologie definuje sociální síť jako propojenou skupinu lidí, kteří se navzájem ovlivňují, přičemž mohou být příbuzní. Sociální síť se tvoří na základě společných zájmů, rodinných vazeb nebo z jiných více pragmatických důvodů, jako je např. ekonomický, politický či kulturní zájem“* [2].

Sociální síť si můžeme představit jako strukturu uzlů znázorňujících jednotlivce případně skupiny či organizace. Tyto uzly propojují vazby určující vzájemné vztahy např. rodina, přátelství, zájem, fyzický kontakt či víra (viz obr. 1).



Obr. 1: Diagram sociální sítě [3]

Jak již bylo zmíněno výše, v současné době je pojem sociální sít často spjatý s internetem. Máme pak většinou na mysli tzv. internetové sociální sítě, které jsou momentálně velmi rozšířené například: Facebook, Twitter, Google+. Slovní spojení „sociální síť“ je překladem z anglického „Social Network“. Za ekvivalentní, byť méně používané, lze považovat termíny „společenská síť“ případně „komunitní síť“.

Pojem „internetové sociální sítě“ je dnes běžně zkracovaný pouze na „sociální sítě“. Takto zkrácený jej můžeme používat, je-li z kontextu zřejmé, že nedojde k záměně pojmů.

1.1 Internetová sociální síť

Internetová (webová) sociální síť je webová služba, která sdružuje uživatele. Ti spolu díky ní mohou komunikovat a sdílet informace např. obrázky, fotografie, videa a články.

V roce 2007 dvě internetové socioložky Danah Boydová a Nicole Ellisonová v článku Social network sites: Definition, history, and scholarship definovaly termín sociální sítě následovně:

„Sociální sítě jsou webové služby, které lidem umožňují:

1. *založit si veřejný či polo-veřejný profil v rámci daného systému,*
2. *vytvořit seznam dalších uživatelů, s nimiž jsou spojeni,*
3. *prohlížet a procházet tento seznam kontaktů jakož i seznamy ostatních uživatelů v daném systému“* [4].

Podle předešlé definice můžeme říci, že všechny sociální sítě spojuje několik základních znaků:

- Propojování uživatelů – každý uživatel tvoří aktivně nebo pasivně „síť“ přátel nebo odběratelů.
- Profil – stránka, na které jsou uvedené základní údaje uživatele. Obvykle zde nalezneme jméno a příjmení uživatele, profilovou fotografii, věk a místo bydliště. Někdy se můžeme setkat i s dalšími informacemi jako je telefonní číslo, e-mail, zájmy, informace o škole a o zaměstnání a další fotografie a videa. Profil je vytvářen samotným uživatelem a jeho aktivitou na sociální síti. Podobu profilu může uživatel neustále ovlivňovat a upravovat.
- Komunikace – obvykle probíhá dvěma způsoby. První je pomocí tzv. přímých zpráv, tyto zprávy vidí jen odesílatel a příjemce. Druhý způsob je veřejný. Uživatel zveřejní zprávu všem svým přátelům případně odběratelům najednou obvykle tím, že ji umístí na vlastní profil [5].

1.2 Historie a vývoj sociálních sítí

Předchůdce sociálních sítí se objevuje již v 80. letech 20. století. Jednalo se o skupiny lidí, které pomocí mailů podporovaly své sociální vztahy.

Dne 2. 10. 1971, byl poslán první vzkaz na vzdálený počítač. Uživatelé této služby byli vojáci v síti ARPA NET. Dalším důležitým momentem bylo vytvořeno Internet Relay Chat (IRC – chat přes internet) finským studentem Jarkem Ojkarinnenem. Jednalo se o systém, který umožňoval komunikaci v reálném čase [6].

Rendy Conrad v roce 1995 představil službu classmates.com, kterou někteří považují za první sociální síť dnešního typu. Bylo nutné se do sítě registrovat na webových stránkách a poté uživatel mohl vyhledávat a udržovat vztahy mezi spolužáky a studenty. Tato sociální síť je dodnes funkční, její uživatelé pocházejí převážně z USA a Kanady [3].

Na počátku roku 1997 je spuštěn server sixdegrees.com, zakladatel služby je právník Andrew Weinreich. Síť byla jedinečná tím, že žádala po uživatelích používání jejich pravého jména. Dalším významným prvkem byl online profil každého uživatele založený na jeho skutečné identitě. Sixdegrees byla první internetová firma, která se pokoušela zmapovat skutečné vztahy mezi živými lidmi. Tato síť měla však i své nedostatky, například do uživatelských profilů nebylo možné nahrávat fotografie. Navíc v této době nebyly ani příliš rozšířené digitální fotoaparáty. Síť sixdegrees.com byla v mnohém revoluční a naznačila směr dalšího vývoje sociálních sítí [7].

Po roce 2000 se začalo objevovat stále více nových sociálních sítí např. švédská síť pro náctileté LunarStorm, korejská síť Cyworld nebo pracovní síť Ryze. V únoru roku 2003 byl spuštěn web amerického programátora Jonathana Abramse. Jeho sociální síť Friendster se stala okamžitým hitem, během měsíce měla několik milionů uživatelů. Kdo se chtěl k síti připojit, potřeboval pozvánku od stávajícího uživatele. Společnost trvala na tom, aby její uživatelé používali svou skutečnou identitu. Sociální síti Friendster nakonec uškodila její vlastní popularita. Lidé, kteří síť spravovali, nebyli schopni zajistit její plynulý chod a sociální síť pod náporem uživatelů nebyla schopná provozu [7].

Rychlý úspěch sociální sítě Friendster přispěl ke spuštění velkého množství dalších sociálních sítí. Z těch, které jsou u nás poměrně známé, jmenujme obchodní (pracovní) síť LinkedIn, jenž vznikla v květnu 2003. Další u nás objevující se sítí je MySpace. Tato síť byla spuštěna 15. srpna 2003 a byla velmi inspirovaná službou

Friendster. Hlavním rozdílem bylo, že služba MySpace nepožadovala po svých uživatelích uvedení jejich skutečné identity [7].

Dne 4. 2. 2004 byla spouštěna sociální síť Facebook. V roce 2006 se poprvé objevuje sociální síť Twitter. O pět let později v roce 2011 představuje společnost Google svou sociální síť Google+.

Sociální sítě jsou velmi oblíbený fenomén dnešní doby. Díky tomu neustále vznikají nové, odlišující se myšlenkou, funkcemi nebo okruhem cílových uživatelů.

1.3 Druhy sociálních sítí

Sociální sítě můžeme dělit podle několika kritérií. Každý uživatel však může danou sociální síť užívat dle vlastních potřeb, tedy odlišně od původně zamýšleného využití.

- **Sociální sítě zaměřené na profil:** Služby této sociální sítě jsou organizovány především kolem profilů jejich uživatelů. Profily uživatelů bývají mnohdy podrobné, obsahují velké množství informací – jméno a příjmení, fotografie, detaily zájmů případně oblíbené a neoblíbené věci. Do této kategorie můžeme zařadit sociální sítě typu Facebook, MySpace, atd.
- **Sociální sítě zaměřené na obsah**: Profil uživatele je stále důležitý a může obsahovat dosti informací, ale důležitější je obsah příspěvků. Příkladem těchto sítí může být YouTube nebo Instagram. Existuje spousta uživatelů, kteří aktivně nepřidávají obsah na tyto sítě, ale sledují příspěvky svých přátel případně dalších pro ně zajímavých lidí.
- **Víceuživatelské virtuální prostředí** (Multi User Virtual Environment): Virtuální světy, které vznikly propojením principu sociálních sítí a víceuživatelských her. Jednotliví uživatelé spolu komunikují prostřednictvím avatarů. (Avatar je vytvořená virtuální postava reprezentující uživatele v daném virtuálním prostředí.) Příkladem těchto sítí je Second Life nebo World of Warcraft.
- **Mikro-blogovací sociální sítě:** Služby, které umožňují publikovat pouze krátké zprávy a to buď veřejně, nebo v rámci uživatelových kontaktů a skupin. U nás je nejpoužívanější sítí tohoto typu Twitter [8].

Některé zdroje uvádějí dělení sítí na **obecné** a **specializované**. Za obecné jsou považovány sítě, v nichž mají uživatelé různorodé vazby (např. Facebook, Twitter,…). Naproti tomu specializované sítě jsou zaměřené na určité skupiny lidí např. na sportovce (dame-sport.cz) nebo matky (modrykonik.cz) [5].

Dále můžeme rozlišovat sítě **otevřené**, k jejich používání se stačí pouze zaregistrovat, a **uzavřené,** do nich je přístup nějakým způsobem omezen, např. musíme být členy určité skupiny případně dostat od člena skupiny pozvánku. V otevřené síti mohou vznikat menší uzavřené podsítě [5].

1.4 Výhody a nevýhody sociálních sítí

Jeden z hlavních důvodů proč lidé sociální sítě používají je komunikace a udržování kontaktů. Uživatelé spolu mohou v reálném čase komunikovat a to bez ohledu na místo, kde se právě nachází. Sociální sítě spojují lidi, kteří by se jen těžko mohli reálně potkat, nebo jsou vzájemně geograficky nedosažitelní. Také umožňují uživatelům kontaktovat případně navazovat spojení s mediálně známými osobnostmi, neboť někteří populární a významní lidé na sociálních sítích komunikují se svými příznivci.

Mezi další důvody, proč lidé navštěvují sociální sítě, patří:

- možnost sdílení vlastního obsahu (statusů, fotografií, videí, atd.) s přáteli, případně odběrateli,
- plánování rozmanitých společenských událostí a akcí (od oslav narozenin až po koncerty známých skupin),
- získávání informací a to nejen o ostatních uživatelích, ale i o světě ve kterém žijeme (získávání informací o článcích internetových periodik, o televizních stanicích a jejich pořadech, atd.).

Používání sociálních sítí může mít však i negativní dopady. Nejvíce ohroženou skupinou jsou děti a mladiství a to nejen proto, že tráví na internetu, potažmo sociálních sítí mnoho času, ale také příliš nerozlišují mezi on-line a off-line světem, neboť se narodili v době, kdy je internet samozřejmostí. U mladistvých je častým problémem jejich potřeba prezentovat sám sebe, což může vést k přehnanému sebeodkrývání a následnému zneužití těchto údajů další osobou [4].

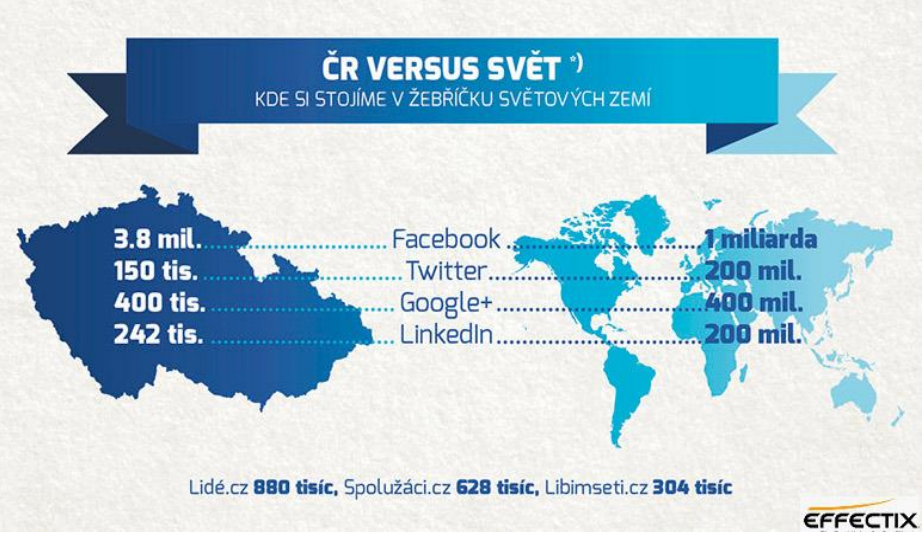
Možné nevýhody užívání sociálních sítí řadíme:

- kyberšikana,
- kybergrooming,
- kyberstalking,
- závislost,
- sexting, zneužití osobních informací apod.

Více se rizikům, se kterými se mohou žáci středních škol na sociálních sítích setkat, budeme věnovat v kapitole 3 Rizika spjatá s používáním sociálních sítí.

1.5 Návštěvnost sociálních sítí

Sociální sítě jsou momentálně velmi oblíbené a to nejen v České republice, ale i v zahraničí (viz obr. 2) a jejich obliba stále roste.



Obr. 2: Počet uživatelů sociálních sítí (březen 2013) [9]

Podle výzkumu MML-TGI, který mapoval návštěvnost zahraničních sociálních sítí českými uživateli ve druhém a třetím kvartálu roku 2014, je bezesporu nejnavštěvovanější sociální sítí Facebook. Podle výzkumu ji týdně navštívilo 3,35 mil. uživatelů. Druhou nejnavštěvovanější sítí v České republice byla v tomto období sociální sít zaměřená na sdílení videí YouTube, jejíž týdenní návštěvnost činila 2,03 mil. osob. Nejrychleji rostoucí sociální sítí je podle průzkumu TML-TGI Google+, jejíž návštěvnost se oproti předcházejícím dvou čtvrtletím zvýšila o 50 % na 0,53 mil. uživatelů [10].

2 Nejpoužívanější sociální sítě v ČR

Dříve u nás byly populární české sociální sítě jako libimseti.cz (sdílení a hodnocení fotografií, seznamka,…), lide.cz (chatovací server, blogy,…), a spoluzaci.cz (komunikace mezi současnými i bývalými spolužáky). Poslední dvě jmenované patří společnosti Seznam. Obliba českých sítí neustále klesá.

V současnosti nejnavštěvovanější sociální sítí v České republice je Facebook, z tohoto důvodu si dovolím věnovat této sociální sítí ve své práci více prostoru. Mezi hojně navštěvované sociální sítě patří i Google+, Youbute, Instagram, Twitter.

2.1 Facebook

Obr. 3: Mark Zuckerberg [11]

Facebook založil dne 4. února 2004 student Harvardské univerzity Mark Zuckerberg se spolužáky Dustinem Moskovitzem, Crisem Hugnesem a Eduardem Severinem [11]. Služba nacházející se na webové adrese www.Thefacebook.com byla určena pro studenty Harvardské univerzity a ačkoliv obsahovala jen minimum funkcí, stala se ihned velmi oblíbenou [7]. Již v březnu téhož roku ji její zakladatelé rozšířili na univerzity Stanford, Columbia a Yale [11].

O necelých čtrnáct měsíců později dne 20. května 2005 se společnost oficiálně přejmenovala na Facebook a přemístila se na doménu www.facebook.com [7]. Postupně byla sociální síť spuštěna na středních školách v USA. Nakonec se společnost rozhodla otevřít registraci, od 26. září 2006 [11] již nebyl k přihlášení nutný e-mail některé z amerických vysokých nebo středních škol, od tohoto dne se mohl k této síti připojit kdokoliv starší 13 let.

David Kirkpatrick popisuje ve své knize Facebook následovně:

„Facebook sjednocuje svět. Stal se z něj most mezi kulturami, zvláště mezi mladými lidmi. I přes své skromné začátky se stal technologickým vůdcem s jednoznačným

vlivem v celé oblasti moderního života. Jeho členové postupují napříč generacemi, regiony, jazyky i třídami. Facebook mění mezilidskou komunikaci, prodej výrobků, kontakt mezi vládami a obyvateli, a dokonce i fungování společností. Mění charakter politického aktivismu a v některých státech začíná ovlivňovat i samotnou demokracii" [7].

Sám Facebook se popisuje následovně:

„Naším cílem je umožnit lidem sdílení a vytvářet otevřenější a propojenější svět. Každý den se lidé scházejí na Facebooku, aby si vyměňovali svoje příběhy, podívali se na svět očima druhých, spojili se s přáteli a zapojili se do nejrůznějších akcí. Konverzace, které se odehrávají na Facebooku, jsou zrcadlovým obrazem různorodosti komunity tvořené více než miliardou lidí" [12].

Vzhledem ke statistikám, které Facebook uvádí, lze říci, že se mu jeho cíl daří naplňovat. K 31. prosinci 2014 má 1,39 miliardy uživatelů, kteří jsou aktivní minimálně jednou měsíčně, denně je pak aktivních 890 milionů uživatelů. Přibližně 82,4 % každodenně aktivních uživatelů nepochází z USA ani z Kanady [11].

Kdo chce začít Facebook používat, musí se zaregistrovat na úvodní stránce služby (viz obr. 4). Kromě jména a příjmení je třeba zadat e-mailovou adresu nebo číslo mobilního telefonu, datum narození a pohlaví. Na jednu e-mailovou adresu případně na jedno telefonní číslo lze založit pouze jeden profil. Datum narození je nutné zadat především pro kontrolu věku uživatele.

Obr. 4: Úvodní strana www.facebook.com [13]

Registrací souhlasí uživatel s podmínkami používání mimo jiné s těmito body:

„Neposkytnete na Facebooku falešné osobní informace ani bez povolení nevytvoříte účet pro nikoho jiného. Nebudete vytvářet více než jeden osobní účet. Pokud váš účet deaktivujeme, nevytvoříte bez našeho svolení jiný. Nebudete službu Facebook používat, pokud je vám méně než 13 let. Nebudete službu Facebook používat, pokud jste odsouzeným sexuálním delikventem. Nesdělíte nikomu své heslo, neumožníte nikomu přístup ke svému účtu ani nepodniknete žádné jiné kroky, které by mohly ohrozit bezpečnost vašeho účtu…" [14]. Při používání služby se však běžně můžeme setkat s uživateli, kteří tyto pravidla porušují.

Po registraci uživatel obvykle začíná vyplněním vlastního profilu. Spektrum informací, které o sobě můžeme sdělit je opravdu široké. Začíná právě u jména a příjmení zadaného při registraci, profilovou a úvodní fotografií. Obě tyto fotografie můžeme měnit, zároveň mají tyto tři údaje nastavené soukromí jako veřejné, toto implicitní nastavení není možné měnit. Dalšími údaji, které může uživatel na svém profilu zveřejnit, jsou: datum narození, pohlaví, kontakty, místo bydliště, adresa, vzdělání a práce, aktuální partnerský stav, rodinné vztahy, zájmy, oblíbené knihy a filmy, seznam přátel a další.

Na Facebooku je u drtivého množství informací možné nastavit soukromí. Můžeme tedy určit, kdo jednotlivé informace uvidí. Máme možnost si vybrat z možností „Veřejný" (informace zůstanou viditelné pro všechny uživatele Facebooku), „Přátelé" (informace budou viditelné pouze pro přátele daného uživatele), „Přátelé kromě známých" (informace budou viditelné pro přátele, kromě těch které uživatel přesunul do seznamu „Známý"), „Jenom já" (informace uvidí pouze uživatel), a „Vlastní nastavení" (zde si může viditelnost informací upravit uživatel podle svého přání, například si vybrat, které seznamy jeho přátel příspěvky uvidí a které nikoliv). Stejné nastavení soukromí platí jak pro informace, které na profil uživatel umístí, tak i pro veškerý obsah, který na internetové sociální síti Facebook sdílí. Nesmíme však zapomínat, že ať je naše nastavení soukromí sebelepší stále, pro nás platí podmínky používání služeb Facebook tedy i bod 2.1 a 2.4 těchto podmínek:

„2.1 …udělujete nám nevýhradní, přenosnou, převoditelnou, celosvětovou bezúplatnou (royalty-free) licenci na použití veškerého obsahu podléhajícího vašemu

DV (duševní vlastnictví), který zveřejníte na Facebooku nebo v návaznosti na něj (Licence k DV). Tato licence k DV končí, jakmile svůj obsah podléhající DV odstraníte ze svého účtu, s výjimkou případů, kdy jste tento obsah sdíleli s ostatními…

2. 4 Pokud publikujete obsah nebo informace s použitím nastavení Veřejné, znamená to, že povolujete všem (včetně osob mimo službu Facebook) přístup k těmto informacím, jejich použití a jejich spojení s vámi (tj. s vaším jménem a profilovou fotkou)" [14].

Proto by měli být uživatelé obezřetní při zveřejňování informací a sdílení obsahu. Obecně se uživatelům radí, nenahrávat na sociální sítě obsah, u něhož by jim vadilo, že bude veřejně přístupný.

Aby mohl uživatel službu využívat, potřebuje se spojit s dalšími lidmi. Facebook k tomu poskytuje dva nástroje. Prvním je uzavření „přátelství" s určitým uživatelem. Nejprve musí uživatel odeslat potencionálnímu příteli „žádost o přátelství", pokud ji zvolený uživatel příjme, stávají se z těchto dvou lidí „přátelé". Mezi těmito uživateli se vytváří oboustranné spojení. Uživatelé jsou tak upozorňováni na činnost toho druhého. Služba umožňuje maximální počet „přátel" 5000. Přátele může uživatel rozdělovat do seznamů například podle toho, odkud daného člověka zná, jeden přítel může být členem více seznamů. Druhá možnost je vybraného uživatele „Sledovat". Tento uživatel musí nejprve odsouhlasit, že může být sledován. Při této volbě se vytváří jednostranné spojení, sledující uživatel vidí na své „zdi" vše co sledovaný uživatel sdílí na svém profilu jako veřejné. Obráceným směrem však toto spojení nefunguje. „Zeď" je místo, kde se zobrazují uživatelovy příspěvky a aktuální aktivity těch s kterými je propojen.

Na Facebooku je několik funkcí, které usnadňují komunikaci. Je možné sdílet fotografie, videa, nálady a statusy. Je možné posílat pomocí chatu zprávy vybraným uživatelům a komentovat obsah, který ostatní sdílí. Také lze vytvářet případně se přidávat do skupin. Ve skupinách se sdružují, které něco spojuje např. zájem, politický názor atd. V dané skupině spolu mohou uživatelé sdílet a komentovat si vzájemně obsah a zároveň nemusí být „přátelé". Dále mohou uživatelé této sociální sítě vytvářet pozvánky na různé akce a události. Mohou být pozváni a oznámit

pomocí Facebooku organizátorovi, zda přijdou nebo ne. Zároveň vidí, kdo další pozvání přijal.

Jedna z funkcí, které se mohou zdát trochu kontroverzní, je sledování polohy uživatele. Pokud si uživatel nevypne tuto službu, pak Facebook sleduje, z jakého místa se uživatel přihlašuje. Zaměření polohy bývá v tomto případě velmi podrobné a ostatní mohou vidět, kde se uživatel právě nachází. Další podobnou funkcí je mapa, ta je umístěná v profilu uživatele. Pokud uživatel vloží fotografii s označením polohy, kde byla vyfocena, případně je na nějaké takové fotografii označen, zakreslí se toto místo do mapy na jeho profilu. Přidává-li uživatel nebo jeho přátelé fotografie často, je pak na mapě vidět, kde se uživatel obvykle pohybuje. Tyto služby však poskytují i jiné sociální sítě.

Facebook se 24. května 2007 změnil na platformu. To znamená, že začal umožňovat, aby cizí aplikace běžely na stránkách jejich služby. Tím se výrazně rozrostl počet úkonů, které lze na Facebooku vykonávat. Nejpopulárnějšími aplikacemi se stali hry, někteří uživatelé si zakládali profily právě jen kvůli nim. Ukázalo se, že lidé rádi hrají s lidmi, které znají a soutěží s nimi [7]. Za tyto výhody však uživatel platí sdílením informací s těmito aplikacemi. Pokud chce uživatel nějakou aplikaci začít používat, musí souhlasit s tím, že jí poskytuje přístup k osobním údajům. V některých případech, uživatelé povolují aplikaci, že bude v rámci nastaveného zabezpečení zveřejňovat zprávy na uživatelově profilu. Tím se uživatelovy osobní údaje dostávají do rukou třetí strany.

Jednou z hlavních ideologií Facebooku a Marka Zackerberga je transparentnost. Každý uživatel na této síti má mít vytvořený jen jeden profil, založený na jeho skutečné identitě. Vazby, které síť vytváří, mají pouze kopírovat vazby z reálného světa. Ověření identity uživatelů má být provedeno pomocí přátel uživatele. Pouze pokud bude uživatel používat své pravé jméno, budou ho jeho přátelé moci vyhledat a spojit se s ním. Pokud člověk vystupuje pod pravým jménem, je pak opatrnější a díky tomu se nesetkáváme tak často s vulgaritou a nežádoucím chováním jako v anonymních sítích. Všechno by mělo vést k transparentnosti, s tím spojené větší odpovědnosti, ale i toleranci a pochopení [7]. Jak moc je možné tuto ideologii naplnit, ukáže až čas. Nicméně s jistotou můžeme říct, že službě Facebook

se daří denně propojovat miliony uživatelů a učit je postupně odkrývat své soukromí.

2.2 Google+

Google+ je sociální síť vytvořená společnosti Google. Není to první zkušenost této společnosti v dané oblasti. Od roku 2004 do roku 2014 provozovala sociální síť Orkut, ta však nebyla v České republice příliš rozšířená, bohatou uživatelskou základnu měla hlavně v Indii a Brazílii [15].

Obr. 5: Logo služby Google+ [16]

Služba Google+ dostupná na webové stránce plus.google.com byla spuštěna dne 28. června 2011. Tato sociální síť určitým způsobem zastřešuje a propojuje služby, které již bylo možné na Google používat před jejím vznikem. Sám Google o službě říká:

„V roce 2011 jsme představili projekt Google+, jehož cílem bylo vnést na internet pestrost a jemné nuance lidské komunikace a vylepšit celý vyhledávač Google tím, že do něj začleníme uživatele i s jejich vztahy a zájmy“ [17].

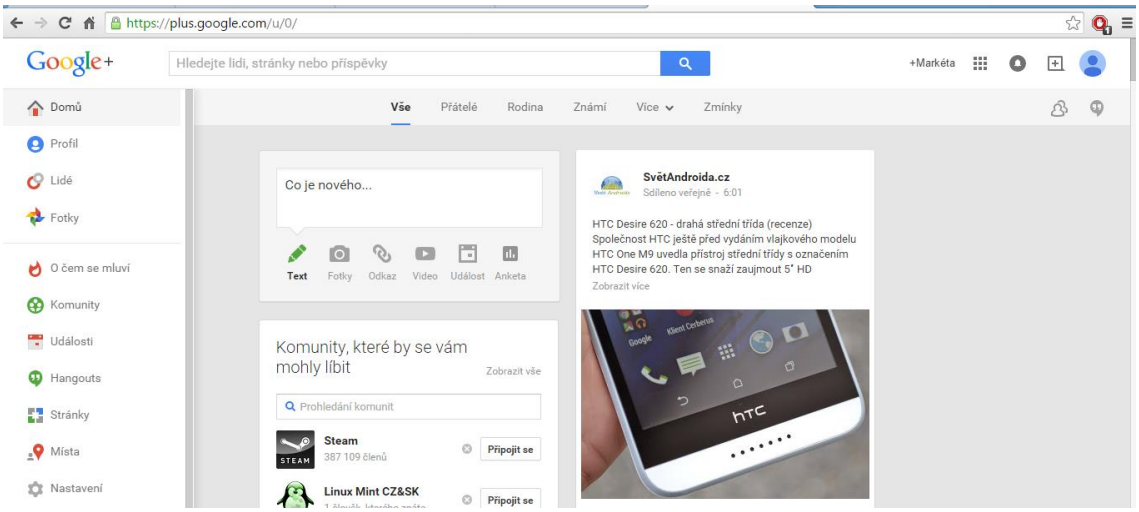
Na sociální síti Google+ bylo ke dni 18. 10. 2014 vytvořeno přes 2 miliardy profilů [18]. Google+ tak dosti výrazně předčil svého největšího konkurenta sociální síť Facebook v počtu založených účtů, nikoliv však v počtu užití. Velké množství uživatelů má sice založený profil na sociální síti Google+, ale zároveň tuto službu nevyužívá. Těm, kdo již měli založený účet u společnosti Google, byl automaticky založen profil ve službě Google+, jedná se například o uživatele služby Gmail. Pokud chcete využívat některé služby společnosti Google mimo jiné službu YouTube (více kapitola 2.3), jste mnohdy tlačeni do založení profilu na sociální síti Google+. Proto nelze srovnávat počet založených účtů na Google+ s počtem aktivních uživatelů Facebooku.

Pokud sociální síť chceme začít používat, je nutné se zaregistrovat a souhlasit s touto podmínkou umožňující společnosti využívat obsah, který uživatel nahraje na sociální síť:

„Pokud nahrajete, odešlete, uložíte nebo přijmete obsah do nebo prostřednictvím našich služeb, poskytujete společnosti Google (…) celosvětově platnou licenci k užití,

hostování, uchovávání, reprodukování, upravení, vytvoření odvozených děl (…), komunikaci, publikování, provozování a zobrazování na veřejnosti a distribuci takového obsahu. (…) Licence přetrvává i poté, co přestanete naše služby používat…“ [19].

Po registraci si uživatel tvoří profil. Ten je rozdělena na několik částí. První část „Něco o mně“ zpravidla obsahuje jméno a příjemní, fotografii, případně další informace jako je datum narození, vztah, práce, vzdělání, bydliště, kontaktní údaje, lidé, které má uživatel v kruzích a kteří mají v kruzích jeho. V profilu jsou další stránky například s příspěvky, fotografiemi, videi atd. Díky tomuto rozdělení je profil uživatele přehledný.



Obr. 6: Domovská stránka služby Google+ [16]

Uživatel rozděluje lidi, s kterými je ve spojení, pomocí tzv. kruhů, což jsou vlastně tematické skupiny. Přednastavené kruhy jsou: rodina, přátelé, známí a sledování. Každý uživatel si může vytvořit další kruhy podle potřeby. Jeden uživatel může být umístěn do více kruhů. Lidi, kteří uživatele zajímají, si přidá do kruhů a vidí, co daný uživatel na sociální síti sdílí. Neprobíhají tu žádné žádosti. Každého uživatele si tak může přidat do kruhů kdokoliv.

Při vkládání obsahu si lze zvolit, s kým se má sdílet. První možnost je sdílet Veřejně, tedy že uživatelův obsah uvidí všichni používající sociální síť Google+ a zároveň se zobrazí na domovské stránce lidí, kteří mají uživatele v kruzích. Další možností je určení sdílení podle kruhů. Uživatel pak může zvolit, že bude svůj

obsah sdílet jen s lidmi, které umístil do určitého kruhu, např. rodina případně pouze s jednotlivci. Nastavení soukromí u příspěvků je tak rychlé a snadné.

Kromě komunikace s lidmi v kruzích se také může uživatel přidávat do různých komunit. V komunitách lze komunikovat a sdílet obsah i s lidmi, které nemá ve svých kruzích. Komunity mají vždy nějaké téma nebo zaměření. Založit libovolnou komunitu může jakýkoliv uživatel sítě.

Mezi oblíbené funkce na Google plus patří Hangouts, umožňuje uživatelům posílat nejen textové zprávy a obrázky, ale i zahajovat hlasové hovory. Další oblíbená funkce je nahrávání fotografií. Google+ uživateli umožňuje upravovat fotografie, a především je nahrávat do cloudu od Google. Často je tato služba používána na mobilních telefonech pomocí aplikace Google+ Photos [19].

Sociální síť Google+ působí na první pohled poměrně složitě. Když se v ní člověk zorientuje, zjistí, že je dosti variabilní a v celku přehledná. Výhodou je spojení s nástroji společnosti Google jako jsou kalendář nebo mapy.

2.3 YouTube

YouTube je služba umožňující sdílení a komentování videí. Její zařazení mezi sociální sítě není úplně jednoznačné, obsahuje však několik sociálních prvků. K této službě mohou přistupovat i neregistrovaní uživatelé a přehrávat si libovolná videa. Zaregistrovaný uživatel může dále nahrávat vlastní video-obsah na svůj kanál a zveřejňovat na něm další informace. Odebírat obsah ostatních uživatelů, komentovat ho a hodnotit ho palcem nahoru (líbí) nebo palcem dolů (nelíbí).

Obr. 7: Zakladatelé služby YouTube: Chad Hurley, Stave Chen a Jawed Karim [20]

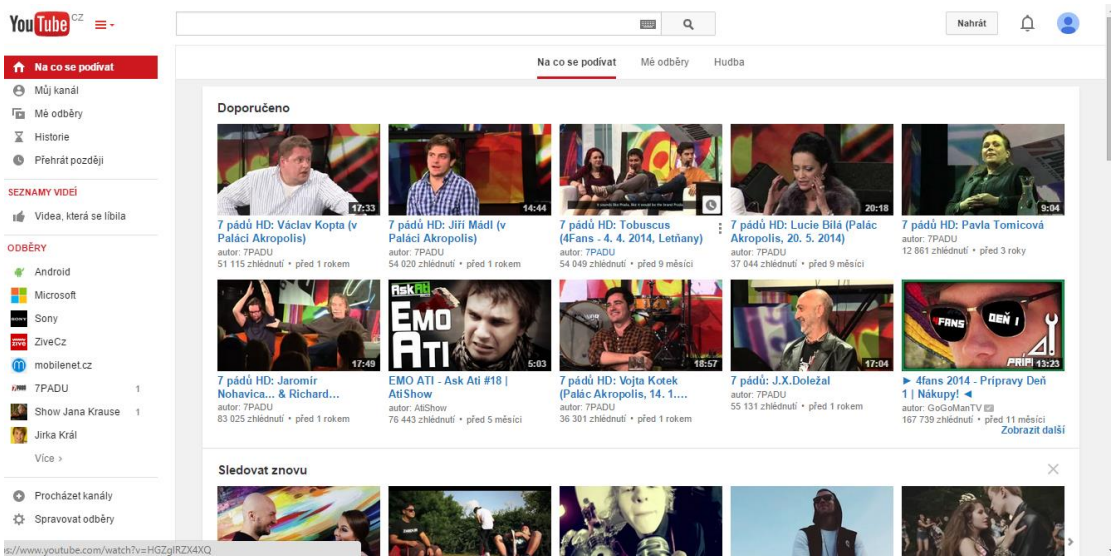
Vznik YouTube se datuje na 14. února 2005, kdy byla ve Spojených státech zaregistrovaná internetová doména youtube.com. V květnu se na webových stránkách objevila služba umožňující sdílení videí. Kromě amatérských videí se brzy začaly na stránkách objevovat i hudební klipy a pirátské kopie filmů,

což pomohlo sociální síti k rychlejšímu růstu. Službu YouTube vytvořili Chad Hurley, Stave Chen a Jawed Karim (viz obr. 8) [20].

Na podzim roku 2006 koupila službu YouTube společnost Google za 1,65 miliardy dolarů. Dne 9. 10. 2008 byla služba lokalizována pro Českou republiku. Nyní je velmi úspěšná. Za jednu minutu bývá na server nahráno až 300 hodin nových videí. YouTube má více než miliardu uživatelů z celého světa. V České republice navštíví každý měsíc tuto sociální síť okolo 4,2 milionu uživatel [21].

V listopadu 2013 proběhla integrace YouTube se službou Google+. Uživatelé, kteří od této chvíle chtějí komentovat a hodnotit videa na YouTube, musí mít založený profil na sociální síti Google+. Těm, kteří vlastnili účet na sociální síti YouTube před touto integrací, byl automaticky vytvořen účet na Google+. Protože v té době už byla služba YouTube třetí nejnavštěvovanější webovou stránkou na světě (po google.com a facebook.com), byl tento krok velmi kritizován [22].

Přo přihlášení na YouTube tak dnes používáme stejné přihlašovací údaje jako při přihlašování do ostatních služeb Google (např. Gmail, Google+).

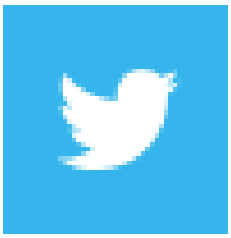


Obr. 8: Úvodní stránka služby YouTube přihlášeného uživatele [23]

Specifickou skupinou uživatelů na YouTube jsou tzv. YouTubers (česky také YouTubeři). To jsou uživatelé, kteří natáčejí autorská videa, mají na svém kanálu hodně odběratelů a na svých videích velké množství zhlédnutí. Těmto uživatelům

pak nabízí YouTube spolupráci a určité finanční odměny podle počtu zhlédnutí jejich videí. I v České republice je několik takových uživatelů.

2.4 Twitter



Obr. 9: Logo služby Twitter [24]

Twitter (český překlad štěbetání nebo cvrlikání ptáků) je mikro-blogovací sociální síť, kterou založili 21. března 2006 Jack Dorsey, Noah Glass, Evan Williams a Biz Stone [24]. Na Twittru lze publikovat libovolné zprávy, které však mají maximální délku 140 znaků. Tento rozsah nebyl vybrán náhodně. Prvotní myšlenka k založení sociální sítě se zrodila již v roce 2000. Jack Dorsey přemýšlel o službě, která umožní sdílení zpráv (statusů) odkudkoliv a kdykoliv, což v této době umožňovaly hlavně SMS zprávy. Standardní délka jedné SMS byla 160 znaků. Volných 20 znaků bylo ponecháno do zálohy. Toto redukování délky zpráv se zachovalo dodnes, přestože většina uživatelů přistupuje k Twitteru přes internet [25]. Dnes je možné sdílet i fotografie a krátká videa. Novinkou je podpora skupinového chatu uživatelů.

Statusy, které na Twitteru sdílíme s ostatními, se obvykle nazývají Tweety. Člověk, který uživatele sleduje je odběratel neboli follower. Na každý Tweet je možné odpovědět. Odpověď se pak zobrazí ve tvaru @jméno uživatele, na kterého reagujeme, poté následuje samotná zpráva. Další možnost je Retweet příspěvku, což znamená přeposlání daného příspěvku svým followerům. Také si můžeme Tweet oblíbit (přidat k oblíbeným), případně ho poslat v soukromé zprávě pouze vybraným uživatelům. Každý uživatel si může zvolit veřejný nebo soukromý profil. Veřejný profil může odebírat kdokoli. Uživatel, který má nastavený profil jako soukromý, musí každému followeru povolit odběr.

Funkcí, kterou zpopularizoval Twitter a poté se velmi rychle rozšířila po celém internetu, je tzv. hashtag. Hashtag je slovo nebo fráze označená symbolem #. Dnes můžeme slovo uvedené za tímto znakem označit za klíčové slovo daného příspěvku. Pomocí hashtagů je možné uspořádat velké množství dat napříč všemi jednotlivými uživateli Twitteru, pomáhá zlepšit indexování obsahu a slouží k rychlejšímu vyhledání informací o vybraném tématu.

Společnost Twitter na svých webových stránkách uvádí, že má měsíčně 288 milionů aktivních uživatelů, kteří napíší 500 milionů Tweetů denně [26].

2.5 Instagram

Instagram je sociální síť určená ke sdílení fotografií pomocí mobilních telefonů. Fotografie je možné upravovat pomocí filtrů, nastavení například kontrastu, jasu, sytosti atd. Od roku 2013 je možné na Instagram nahrávat i videa v maximální délce 15 sekund [27]. Každý uživatel má vlastní profil, na kterém jsou kromě základních informací zveřejněných uživatelem viditelné sdílené fotografie a videa.

Obr. 10: Logo služby Instagram [27]

Na Instagramu je mnoho prvků podobných jako na Twitteru. Uživatel má možnost nastavit si profil jako soukromý nebo veřejný. Pokud je účet soukromý, uvidí uživatelův nahraný obsah jenom lidé, které schválí. Na domovské stránce se uživateli zobrazují vlastní fotky a fotky uživatelů, které sleduje. Všechny fotografie lze označit titulkem a hashtagy. Uživatelé mohou sdílený obsah komentovat a označit ho jako „To se mi líbí“. Instagram nabízí také službu Instagram Direct, díky které lze posílat fotografie nebo videa pouze vybraným uživatelům.

Autory této sociální sítě jsou Kevin Systrom a Mike Krieger [28]. Aplikaci Instagram bylo nejprve možné používat pouze na mobilních telefonech s operačním systémem iOS, poprvé se objevil v App Store (internetový obchod aplikací určený pro iOS společnoti Apple) 6. 10. 2010 a během prvních dvou měsíců získal 10 milionů uživatelů. Až v dubnu roku 2012 byl Instagram spuštěn i pro operační systém Android. Uživatelé Windows Phone museli na aplikaci čekat do listopadu roku 2013. Významnou událostí pro sociální síť Instagram byla její akvizice společností Facebook, která se uskutečnila 9. 4. 2012. Dne 21. 12. 2012 byl Instagram spuštěn v 25 jazycích a to včetně české lokace [27].

Služba umožňuje přidávat k fotografiím geografickou polohu a sestavovat tak mapu míst, na kterých fotografujeme. Dnes je také možné prohlížení profilů uživatelů Instagramu pomocí webových stránek www.instagram.com. Na webu

jsou však služby omezené, např. není možné vkládat fotografie. Jedná se pouze o doplněk k samotné aplikaci určené pro chytré mobilní telefony.

Podle statistik, které aktuálně uvádí společnost Instagram na svých webových stránkách [27], má služba 300 milionů uživatelů, kteří jsou alespoň jednou za měsíc aktivní, více jak třicet miliard sdílených fotografií a denně průměrně zveřejněných 70 milionů snímků.

3 Rizika spjatá s používáním sociálních sítí

Jak už bylo uvedeno výše, používání sociálních sítí s sebou nese kromě nesporných výhod i určitá rizika. Tato rizika jsou úzce spjata s riziky používání internetu jako takového, nelze je proto striktně oddělit. S určitými negativními jevy se však na sociálních sítích můžeme setkávat častěji než s jinými. Je důležité je znát, vědět jak jím předcházet a jak je případně řešit. Není však potřeba tato rizika nějak démonizovat. Špatné věci se na internetu potažmo sociálních sítí skutečně dějí, stejně tak se však dějí i při jakýchkoliv jiných aktivitách člověka.

Nebezpečí tkví především v tom, že rizikovou skupinou jsou děti a mladiství. Důvodů je hned několik. Velký podíl na tom, proč jsou více vystaveni negativním jevům na sociálních sítích má to, jak se zde chovají. Jsou často důvěřivější, méně zodpovědní a ne vždy domýšlejí důsledky svých činů. Nepřemýšlejí příliš nad tím, jak je informace, které sami zveřejní, mohou v případě zneužití poškodit [29].

Dále jsou pro ně důležité nové technologie a neustálé připojení k internetu. Nepoužívání internetových sociálních sítí případně dalších aplikací může vést k tzv. sociálnímu vyloučení (vyloučení jedince ze skupiny a jejich aktivit).

Komunikace a kontakt s vrstevníky je pro dospívající velmi důležitý. Jedná se o potřeby, které měli adolescenti vždy. Osvojení si dovednosti mezilidského kontaktu je v tomto věku zásadní a vede k vyššímu sebevědomí a pocitu samostatnosti [30]. Proto je přirozené, že dochází k přesouvání těchto aktivit i do online světa.

Barbora Krčmářová také upozorňuje na potřeby motivující lidské chování v dospívání, které je možné na internetu snadno naplňovat, což vede adolescenty k častému připojení k síti. Jedná se o potřeby:

- **Nalezení vlastní identity** – je snadné zde experimentovat, vydávat se za někoho jiného a postupně si tvořit představu o tom, kým chceme být.
- **Touha patřit do skupiny** – právě na sociálních sítích je mnoho vrstevníků, s kterými lze být neustále ve spojení, i když právě není možné setkat se s nimi osobně.

- **Vztahy s opačným pohlavím** – na internetu je možné zkoušet mnoho interakcí s opačným pohlavím (konverzace, flirt, námluvy,…).
- **Sounáležitost** – není problém najít lidi se stejnými koníčky a zálibami.
- **Separace od rodiny** – oddělení od některých zvyků rodiny, vede k pocitu soběstačnosti a dospělosti. Tuto potřebu může částečně naplňovat využívání moderních technologií, převážně když je rodiče příliš nepoužívají.
- **Ventilace frustrace** – svěřit se s pocitem zklamání lidem, kteří prožívají podobné trápení [31].

Na webových stránkách Projektu bezpecne-online.cz se dočteme, že lze aktivitu adolescentů na sociálních sítích shrnout do následujících 6 bodů:

1. prezentovat se;
2. najít vrstevníky, které zajímá stejná hudba nebo filmy, diskutovat s nimi o nich a posílat si odkazy;
3. navazovat kontakty s novými lidmi (např. přáteli přátel);
4. prohlížet stránky kamarádů (zjišťovat co právě dělají, sledovat jejich diskuse s ostatními), aktualizovat vlastní stránky (profily);
5. komunikovat se spolužáky;
6. kontaktovat kamarády, možnost spojení s více přáteli najednou [32].

Při pohybování na internetu a sociálních sítích mají někteří uživatelé sklon oddělovat virtuální svět od světa reálného. Objevuje se pak u nich pocit, že co se děje ve světě virtuálním, není skutečné a mají zde tendenci zříkat se zodpovědnosti za své činy. Tento jev se někdy označuje jako disociace ve spojitosti s používáním internetu [30].

Alena Černá a kol. upozorňují na tzv. disinhibiční efekt, s kterým se můžeme také setkat a vysvětluje ho následovně: Pojem *„disinhibiční efekt označuje chování na internetu, při němž máme menší zábrany a nedomýšlíme důsledky svého jednaní natolik, jak bychom činili v offline světě. Za tímto jevem stojí vnímaná anonymita a neviditelnost, které jsou typické pro internetovou komunikaci. Disinhibice se projevuje dvojím způsobem. V některých situacích může podporovat agresivní chování na internetu, v jiných naopak větší míru sebeodhalování, jakož i projevů podpory a pochopení pro druhé“* [30].

Na internetu tedy komunikujeme s lidmi jinak než při osobním setkání. Disinhibiční efekt ovlivňuje uživatele dvěma způsoby:

Jeden typ uživatelů má sklony vyjadřovat se vulgárně a hrubě převážně proto, že se nebojí následků plynoucích z jejich chování. Na internetu si připadají skrytě a nepostižitelně. To však pro běžného uživatele nemusí být vždy pravda. Jak je například uvedeno na internetových stránkách projektu Bezpečný internet.cz: *„Anonymní internet je mýtus, nikdo není zcela anonymní. Většina provozovatelů udržuje logy k jednotlivým uživatelským účtům a ty pak na základě žádostí předává policii. Informace získané z připojení, mohou významně přispět k dopadení pachatele“* [33]. Bohužel, ne vždy se pachatele podaří odhalit, navíc chování uživatele nemusí být tak závažné, aby se jím policie České republiky mohla zaobírat.

Druhý typ uživatelů větší anonymita zbavuje strachu, díky tomu jsou schopni více komunikovat a seznamovat se s novými lidmi, nebojí se odmítnutí. Jak již bylo uvedeno, někdy také dochází ke zvýšenému sebeodhalování. Sebeodhalování je sdělování osobních informací druhým lidem. Ve spojitosti se sociálními sítěmi, do sebeodhalování řadíme i to, co o sobě uživatel uvede na svých profilech a účtech. Uživatelé jsou pak ochotni sdělit nejen své osobní údaje, ale také své názory, zážitky, životní postoje, osobní údaje svých blízkých a přátel apod. V reálném životě míra sebeodhalování roste s důvěrou a pevností vztahu. Abychom druhému člověku sdělili něco, co považujeme za intimní, je potřeba určitá dávka odvahy a pocitu bezpečí. Ten lze na internetu, díky již zmíněném pocitu anonymity, najít poměrně snadno. Proto některým uživatelům nedělá problém se mnohem více odhalit, ukázat všechny své stránky a říct, co si opravdu myslí [31]. Dochází k situacím, kdy se uživatel se svými problémy raději svěří cizí osobě než někomu blízkému, a to hlavně proto, že se s daným člověkem v reálném životě nesetká a nebojí se tolik případného odsouzení či negativních reakcí [30].

Národní centrum bezpečného internetu ve svém metodickém materiálu pro pedagogické pracovníky s názvem Ochrana osobních údajů a osobnosti vytvořeného v rámci projektu Škola bezpečně online: Zvýšení kvality vzdělávání v oblasti bezpečného užívání internetu v Pardubickém kraji uvádí princip zvyšujících se rizik. Podle tohoto materiálu lze za nejohroženějšího uživatele

internetu označit osamělého a separovaného člověka s potřebou vztahu a komunikace, který využívá sociální sítě, a zároveň je nezodpovědný, neinformovaný a ignorující možná rizika [34].

3.1 Kyberšikana a online obtěžování

Kyberšikana (kybernetická šikana) a online obtěžování je jakýsi fenomén dnešní doby výrazně spojený právě s rozšířením sociálních sítí. Pojmy kyberšikana a online obtěžování jsou dnes mnohdy slučované. Z hlediska dopadů tohoto chování je však žádoucí je rozlišovat. Chceme-li tyto pojmy definovat, potřebujeme nejdříve porozumět pojmu šikana někdy označované jako tradiční (školní) šikana.

Anna Ševčíková a kol. [4] a Alena Černá a kol. [30] uvádějí specifikaci pojmu šikana od Dana Olweuse:

„Šikana sestává ze tří hlavních kritérií:

1. *jde o úmyslné agresivní jednání;*
2. *toto jednání je opakované;*
3. *mezi obětí a agresorem existuje mocenská nerovnováha.“*

Mocenskou nerovnováhou je v tradiční šikaně myšlena například vyšší fyzická nebo sociální zdatnost agresora.

Tuto definici lze považovat jako základní, odlišuje šikanu od pouhé agrese. Alena Černá upozorňuje, že je třeba vzít v potaz i další faktory. Mimo jiné to, že oběť agresorovo jednání nijak nevyprovokovala a k útokům dochází v prostředí, které není snadné opustit (třída, škola, atd.) [30].

Kyberšikana je moderní a dynamicky se vyvíjející fenomén, proto je těžké definovat tento pojem s konečnou platností. Definice kyberšikany vychází z předcházejících tří kritérií šikany a přidává čtvrté, fakt, že vše probíhá v elektronické podobě. Kvůli specifičnostem virtuálního světa však některá předcházející kritéria nabývají zcela odlišného významu [4].

Kamil Kopecký a kol. definují kyberšikanu jako: „*individuální či skupinově úmyslné zneužívání informací či elektronické komunikace vedoucí k záměrnému*

a opakovanému obtěžování, nebo ohrožování jedince či skupiny šířením poškozujících textů, obrázků apod.“ [35].

Kritériem, na které by nemělo být při definování kyberšikany zapomínáno, je fakt, že oběť vnímá situaci jako nepříjemnou a ubližující [4].

Alena Černá zmiňuje základní prvky kyberšikany [30]:

- Používání informační a komunikační technologie.
- Opakování se – zde je opakovanost chápána jinak než v případě klasické šikany, dochází zde k tzv. opakované újmě, kterou nemusí zajišťovat agresor, ale publikum, například opakovaným sdílením ponižujícího příspěvku na sociálních sítích nebo jeho komentováním [4].
- Záměrnost ublížit ze strany agresora.
- Mocenská nerovnováha mezi obětí a agresorem – zde už neplatí, že daná nerovnováha je daná fyzickou nebo sociální převahou. U kyberšikany tuto nerovnováhu spatřujeme v tom, že mnohdy nelze zamezit agresorovi kontaktu s obětí, s ohledem na to, jak je pro nás v dnešní době používání informačních a komunikačních technologií důležité. O mocenské nerovnováze také můžeme mluvit, pokud oběť neví, kdo je agresor.
- Jednání je obětí vnímáno jako nepříjemné a ubližující.

Pokud nejsou splněny všechny podmínky pro definici kyberšikany pak obvykle mluvíme „pouze“ o online obtěžování. Uvádí se, že online obtěžování nemá tak zraňující dopad na oběť, ale mohou se objevit i případy, ve kterých má toto jednání vážné následky. Je vhodné tyto termíny oddělovat a dané jevy nezaměňovat. Čímž je možné se vyvarovat použití nevhodných a neúčinných preventivních a intervenčních programů [30].

Příkladem online obtěžování je:

- jednorázový útok,
- útok, při kterém nebylo úmyslem druhého poškodit,
- útok, jenž potenciální oběť nepovažuje za nepříjemný nebo ubližující [4].

Nejednotnost s definicí pojmu kyberšikana a případného zavedení pojmu online obtěžování se promítá v odlišnosti výsledků jednotlivých výzkumů mapujících rozšířenost kyberšikany v České republice. Podle průzkumu realizovaného v rámci projektu E-bezpečí s názvem Nebezpečí internetové komunikace IV konaného v letech 2012–2013, jehož respondenti byli žáci základních a středních škol, se setkalo s kyberšikanou z pozice oběti 50,69 % dětí [36]. Naproti tomu podle výzkumu realizovaného v rámci projektu Copingové strategie kyberšikany u adolescentů zveřejněného ve zprávě Online obtěžování a kyberšikana, který probíhal v letech 2011–2012 v Jihomoravském kraji, udává, že „jen" 6 % žáků ve věku 12–18 let se stalo oběťmi kyberšikany [37]. Takto velký procentuální rozdíl mezi oběma výzkumy byl způsoben právě rozdílným chápáním pojmu kyberšikana.

Šikana a kyberšikana mají mnoho společného, proto není příliš vhodné chápat kyberšikanu jako samostatný problém spojovaný pouze s moderními technologiemi. Někteří autoři považují kyberšikanu za určité rozšíření šikany tradiční [30], v jiných zdrojích je kyberšikana chápána jako druh psychické šikany [38]. Návaznost kyberšikany na tradiční šikanu potvrzuje i výzkum realizovaný v rámci projektu Copingové strategie kyberšikany. Při šetření bylo zjištěno, že děti, které jsou oběťmi kyberšikany, jsou v 71 % případů také obětí tradiční školní šikany [37].

Kybernetická šikana se od tradiční šikany liší prostorovou neomezeností (příkoří se oběti neděje pouze na určitých místech např. ve škole, ale díky moderním technologiím ji provází všude včetně domova), časovou neomezeností (nekončí, trvá prakticky nepřetržitě, dokud má oběť zapnutý internet nebo mobilní telefon), širokými dopady (pomocí sociálních sítí je jakýkoliv obsah velmi rychle a snadno šiřitelný, neomezuje se pouze na určitou skupinu lidí), obtížnou rozpoznatelností (nepůsobí viditelná zranění), anonymitou (agresor se může skrývat za neznámými profily) [39].

Kyberšikana má určité charakteristické projevy, které v některých případech vycházejí i z tradiční šikany.

Nejčastějšími projevy jsou:

Zveřejnění ponižující fotografie nebo videa: Ponižující fotografie nebo videa může agresor získat třemi způsoby. První možnost je, že mu daný obsah poskytne přímo oběť, například proto, že agresorovi důvěřuje případně proto, že ji agresor vydírá. Také je možné, že daný obsah agresor oběti ukradne obvykle z mobilního telefonu nebo počítače. Nezřídka se pak stává, že ponižující obsah agresor vyfotografuje nebo natočí sám. Někdy tento materiál dále upravuje (fotomontáž, editace videa), aby výsledný obsah byl co nejvíce ponižující [38].

V některých případech se setkáváme i s chováním, které se označuje jako Happy Slapping v českém překladu „Veselé fackování". Dříve se jednalo o fyzické napadení nic netušící mnohdy neznámé oběti, kterou útočníci zfackovali, a zároveň celou situaci včetně reakce oběti nahrávali většinou na mobilní telefon [30]. Dnes se tento jev ještě rozšířil. Za Happy Slapping považujeme natáčení fyzického nebo sexuálního útoku. Cílem je získat šokující, originální a ponižující video, které útočníci vystavují na internetu a většinou touží po vysokém počtu zhlédnutí [40].

Pomlouvání a urážení: Útočník se obvykle snaží poškodit dobrou pověst oběti a také narušit její vztahy s ostatními. Agresor také někdy vytváří profil na sociální síti, blog nebo speciální internetovou stránku, na které uvádí nepravdivé informace o oběti, snaží se jí zesměšnit a poškodit.

Odhalení cizího tajemství: Hlavním cílem tohoto jednání je poškodit oběť. Tajemství zná útočník ve většině případů přímo od oběti, ta mu ho buď sama prozradí, nebo je útočník z oběti vyláká. Obvykle předstírá, že má o oběť skutečný zájem a že mu na ní záleží.

Vyloučení z online skupiny: Záměrné vyloučení jedince z určité online skupiny, do které by chtěl či měl patřit. I přesto, že toto jednání nenese prvek agrese, může být pro oběť zraňující a to především kvůli nenaplnění potřeby mladých lidí být členem určité skupiny a podílet se na ní. Například pokud má třída založenou vlastní skupinu na sociální síti, ve které si spolužáci často povídají, řeší záležitosti týkající se školy, případně si pomáhají s domácími úkoly a pouze oběti je odepřen přístup do této skupiny a to i přesto, že by se zřejmě chtěla stát členem.

Krádež cizí identity, zneužití cizího účtu: Útočník zjistí přístupové údaje k elektronickým účtům oběti. Následně může manipulovat s profily (publikováním lživých informací), vydávat se za oběť a rozesílat jejím jménem nevhodný obsah (urážení jejich přátel, veřejné rasistické projevy,…), zneužít osobní údaje a seznam kontaktů (přihlašování se do různých služeb, objednávání v e-shopech,…), mazat kontakty a zprávy.

Obtěžování a sledování (kyberharašení a kyberstalking): Obtěžováním neboli kyberharešením označujeme chování, kdy agresor zaplavuje oběť různými zprávami - například SMS na mobilní telefon, nebo zprávy, kdykoliv se oběť připojí k nějaké službě. Oběť z nějakého důvodu není schopná nepříjemnou konverzaci ukončit [30].

Kyberstalking je chování, při němž pachatel pronásleduje oběť prostřednictvím informačních a komunikačních technologií. Tomuto jevu se budeme podrobněji věnovat v podkapitole 3.2 Kyberstalking.

Vyhrožování, zastrašování, vydírání: Chování objevující se i při tradiční šikaně. Rozdílem je, že při kyberšikaně dochází k těmto jevům ve virtuálním prostředí.

Kybernetická šikana je obvykle realizována pomocí sociálních sítí, mobilních telefonů (jednak k posílání SMS a MMS, také k focení a natáčení oběti) a e-mailových zpráv. Někdy také pomocí instant messengerů, speciálně vytvořených internetových stránek a blogů.

Aktérem kyberšikany je oběť, agresor (útočník) a publikum. Každý z aktérů, ať už se kyberšikany zúčastňuje dobrovolně či nedobrovolně, vědomě nebo nevědomě, hraje důležitou roli a jeho chování může průběh kyberšikany ovlivnit.

Pokud je kyberšikana jen pokračováním školní šikany, pak je oběť obvykle fyzicky nebo sociálně méně zdatná a často se něčím odlišuje od ostatních, například vzhledem. Neznamená to, že každý takový žák je automaticky vystaven kyberšikaně, důležitou roli hrají především mezilidské vztahy ve skupině a chování okolí.

Oběti kyberšikany můžeme podle Aleny Černé a kol. [30] rozdělit na čtyři typy. První dva jsou odvozeny z tradiční šikany, jedná se o tzv. pasivní oběť

a oběť-provokatéra. Pasivní obětí bývají fyzicky slabší, nespolečenští žáci, kteří nemají příliš přátel, a proto je snadné je napadat, příliš se nebrání a málokdo se jich zastane. Oběť-provokatér na sebe naopak strhává pozornost, chová se agresivně nebo jinak negativně působí na své okolí, to pak mívá pocit, že si šikanu/kyberšikanu vlastně zaslouží. Třetím typem je agresor, který se sám stane obětí. Může se jednat o pomstu šikanované/kyberšikanované oběti nebo kohokoliv jiného, kdo na internetu viděl útok. Poslední typem jsou žáci, kteří se ničím neodlišují, dokonce mohou být ve skupině i oblíbení. V online prostředí se ale stávají zranitelní a jsou pro agresora snadno přístupní, může to být způsobeno nižšími znalostmi v oblasti informačních a komunikačních technologií. Agresor pak často zneužívá osobní informace, které o sobě sama oběť na internetu zveřejnila.

V metodickém materiálu pro pedagogické pracovníky Kyberšikana ve školním prostředí vydaného Národním centrem bezpečnějšího internetu [39] upozorňují, že se profil agresora v průběhu školní docházky může měnit. Profil agresora studující střední školu pak sestavili následovně:

„*Agresorem se častěji stává žák:*

- *málo úspěšný, ale s vysokou potřebou sebeprosazení;*
- *s vysokým sebevědomím;*
- *který se s šikanou setkal na základní škole, ať už v roli agresora, svědka nebo oběti;*
- *s rozvíjející se disociální poruchou osobnosti nebo probíhajícím psychickým onemocněním;*
- *pocházející z majetné rodiny nebo jehož rodiče mají významné společenské postavení, pokud žije s představou vlastní výjimečnosti a beztrestnosti a ztrácí kontakt s realitou;*
- *s nezralým nebo negativně nastaveným hodnotovým systémem*.“

Agresorem kyberšikany tedy nemusí být fyzicky silný nebo společensky neoblíbený žák, který si pomocí ponižování druhých snaží zvýšit sebevědomí. Může se jednat i o oblíbeného a sebevědomého člověka, neuvědomujícího si dopady svého chování. Obecně lze však pozorovat u všech agresorů nižší míru empatie, útočník se neumí vžít do pocitů oběti.

V některých případech může docházet k tzv. kokpit efektu. Kokpit efekt přirovnává jednání kyberagresorů k jednání letců shazujících bomby na obydlené oblasti. Protože nevidí faktické dopady a utrpení, jaké způsobují, nepociťují výrazný pocit viny za své jednání. Podobně agresor jednající prostřednictvím informačních a komunikačních technologií nevidí, jaké má jeho chování skutečné dopady na oběť a neuvědomuje si tak v plném rozsahu, jak moc oběti ubližuje [30].

Posledním aktérem kyberšikany je publikum. Jedná se vlastně o kohokoliv, kdo je svědkem útoku. Pokud je takový útok veden na sociální síti, pravděpodobně bude diváků velké množství. Z každého diváka se tak může stát tzv. sekundární útočník [38], pokud například pomáhá s šířením tohoto zraňujícího obsahu. Může jít o vědomé ale i nevědomé podporování kyberšikany. Uživatel shlédne vtipné video a pak se ho rozhodne sdílet se svými přáteli, mnohdy uživatele ani nenapadne, že se jedná o kyberšikanu a že hlavnímu aktérovi způsobuje každé zhlédnutí bolest. Kromě nevědomých šiřitelů, existují samozřejmě i diváci, kteří záměrně a s cílem oběti ještě více ublížit, šíří takovýto materiál.

To, jakým způsobem se publikum postaví ke kyberšikaně, kterou vidí, může často ovlivnit vývoj celé situace. Pokud se zvedne vlna nevole vůči agresorovi a uživatelé proti tomuto jednání otevřeně vystoupí, pak je pravděpodobné, že útočník nebude dále motivovaný v kyberšikaně pokračovat a ohrožovat tak svoje společenské a sociální postavení. Pokud však diváci zůstávají nečinní a tiše tolerují dané chování, nebo přímo podporují agresora například komentováním a sdílením, pak je velká pravděpodobnost rozšíření kyberšikany.

Bez nadsázky lze říci, že sociální sítě jsou ideálním místem pro kyberšikanu. Jakýkoliv příspěvek mohou vidět miliony uživatelů. Nyní se zamysleme nad modelovým příkladem tradiční školní šikany, jenž se rozšíří i na kyberšikanu. Pro agresora je velmi jednoduché zveřejnit na sociální síti jakoukoliv ponižující fotografii nebo video oběti. Během chvíle může tento obsah vidět většina spolužáků oběti. Pokud někdo z přihlížejících obsah sdílí je možné, že ho během pár hodin uvidí většina žáků ze školy, kterou oběť navštěvuje, ale také další obyvatelé města, v kterém žije. Kdokoliv může tento materiál komentovat a útok tak dále podporovat, v tento moment už ztrácí agresor nad útokem kontrolu a neovlivní, kde všude se obsah objeví. Agresor může také odesílat oběti zprávy,

které ji mají zastrašit, může ji vydírat a hrozit zveřejněním nějakým způsobem kompromitujícího obsahu. Dále může veřejně oběť urážet, zesměšňovat a vyzývat ostatní, aby se přidali. Na některých sociálních sítích může agresor založit skupinu, podněcující k ublížení a nenávisti oběti. Důsledky tohoto jednání mohou být pro oběť fatální.

Jak již bylo zmíněno výše, kyberšikanu lze považovat za druh psychické šikany, s tím souvisí i psychologické dopady na oběť. Kamil Kopecký a kol. vyjmenovávají nejzávažnější potíže, které ji mohou potkat: „*tenze, strach, stres; pokles sebehodnocení, sebedůvěry, depresivní a neurotické potíže, poruchy spánku, snížení frustrační tolerance, pocit neřešitelnosti situace, ztráta životní pohody, zkratkovité jednání, zvyšující se agrese, celková psychická nestabilita, trauma a posttraumatická stresová porucha atd.*“ Dlouhodobě neřešená kyberšikana, tak může oběť výrazně poznamenat.

Dojde-li ke kyberšikaně, lze formulovat jednoduché doporučení podle, kterého by se měli děti a dospívající v pozici oběti řídit:

1. Svěřit se dospělé osobě, které oběť důvěřuje.
2. Uložit důkazy - přirozenou reakcí člověka je zraňující obsah mazat. Pro pozdější dokazování kyberšikany a usvědčení pachatele, je však důležité jednotlivé projevy útoku uschovat (e-mail, SMS), případně pořizovat a ukládat Print Screen obrazovky. Pokud dítěti pomáhá dospělá osoba, je vhodné, aby si důkazy ukládala k sobě a oběť je nemusela uchovávat a zvětšovat tak vlastní trápení.
3. Ignorace útočníka – na útočníka není dobré nijak reagovat, jakýkoliv atak agresora většinou vede k dalšímu útoku.
4. Použít technická řešení – blokovat agresora případně ho nahlásit administrátorovi služby, nahlásit nevhodný obsah a požadovat jeho stažení, upravit nastavení zabezpečení vlastního účtu atd.

Pokud je kyberšikana přesahem školní šikany, je žádoucí, aby se do jejího řešení zapojila škola. Dále je často vhodné využít pomoci vládních a soukromých institucí [30].

3.1.1 Řešení kyberšikany ve školním prostředí

Pokud se škola o kyberšikaně dozví, musí se jí zabývat. Nejprve mapuje situaci, aby mohla zvolit správný postup řešení. Důležité je, zdali se kyberšikana týká přímo jejího žáka, jak se o ní škola dozvěděla a zda se děla přímo během vyučování [41].

Ministerstvo školství mládeže a tělovýchovy v Metodickém doporučení k primární prevenci rizikového chování u dětí a mládeže [41] uvádí postup, kterým by se měly školy při řešení kyberšikany řídit:

„1. ***Zajistěte ochranu oběti:*** *Kontaktujte operátora mobilní sítě nebo zřizovatele www stránek, profilu…atd.*

2. ***Zajistěte dostupné důkazy s podporou IT kolegy***
3. ***Důkladně vyšetřete a žádejte odbornou pomoc****: Vyšetřete všechny souvislosti se zjištěným incidentem. Zajistěte si podporu a pomoc externího pracovníka (IT expert, PPP, policie,….). Kontaktujte a spolupracujte s MySpace, Facebookem, nebo jakýmkoli jiným webovým prostředím, kde ke kyberšikaně došlo.*
4. ***Opatření:*** *Zvolte takové opatření a řešení, které je odpovídající závažnosti prohřešku a důsledkům, které agresor způsobil.*
5. ***Informujte a poučte rodiče****: Informujte rodiče oběti i rodiče kyberagresora. Postup a zásady sdělování informací jsou stejné jako u „klasické šikany" (např. NE konfrontace oběti a agresora). Poučte rodiče o tom, koho mohou (je vhodné) kontaktovat (Policie ČR, OSPOD, PPP, právní zástupce atd.). Některé případy kyberšikany nespadají do kompetence školy.*
6. ***Žádejte konečný verdikt a informace****: Při zapojení a následně celém prošetření případu trvejte na konečném stanovisku všech zainteresovaných institucí (PČR…) a dalších subjektů (rodiče).*
7. ***Postihy****: Při postizích agresorů postupujte v souladu se Školním řádem a již vypracovaným krizovým plánem."*

Při řešení kyberšikany je dobré pamatovat, že vychází z pokřivených mezilidských vztahů v dané skupině. Proto je nutné pracovat s celou třídou v rámci prevence, ale i řešení kyberšikany, je nutné usilovat o zlepšení klimatu a vztahů ve třídě.

3.2 Kybergrooming

V dnešní době není neobvyklé seznamovat se na internetu s novými lidmi. Někdy nás nový přítel zaujme natolik, že ho chceme potkat osobně. Takováto setkání jsou dnes poměrně častá a většina z nich s sebou nenese výrazné riziko, byť mohou přinést určitá zklamání. Může se však stát, že ačkoliv si myslíme, že člověka, s kterým jsme se seznámili přes internet, již známe a důvěřujeme mu, ve skutečnosti si píšeme s někým, kdo nám chce ublížit. Může se tak jednat o tzv. kybergrooming.

Kybergrooming definuje Kamil Kopecký následovně: „*Termín kybergooming označuje chování uživatelů internetu (predátorů, kybergoomerů), které má v oběti vyvolat falešnou důvěru a přimět ji k osobní schůzce.*“ A dále dodává: „*Výsledkem této schůzky může být sexuální zneužití oběti, fyzické násilí na oběti, zneužití oběti pro dětskou prostituci, k výrobě dětské pornografie apod.*“ [42].

Kybergooming je v drtivé většině zaměřen proti dětem a mladistvým, kteří tráví hodně volného času například na sociálních sítích nebo jiných internetových službách umožňujících online komunikaci a často si zde hledají nové přátele. Můžeme říct, že obvykle se obětí kdybergoomingu stává dítě nebo mladistvý ve věku 11–17 let. Častěji se jedná o dívky než chlapce. Mnohdy jde o jedince s nízkým sebevědomím, kteří se cítí osaměle a touží po lásce a pozornosti, dále bývají zvýšeně sugestibilní a otevření manipulaci [43].

Pachatelem se častěji stávají muži než ženy. Blíže je však nejsme schopni charakterizovat, jelikož se jedná o různorodou skupinu lidí s nízkým i vysokým společenským statusem [42]. Často je útočník označován za pedofila, to je však mnohdy velmi nepřesné. Pedofilie je porucha sexuální preference, která se projevuje sexuálním zaměřením na děti bez znaků dospívání obvykle ve věku 5–12 let. Zde se jedná spíše o hebefilii nebo efebofilii, tedy sexuální náklonost k dospívajícím dívkám nebo chlapcům. I tyto deviace jsou někdy považovány za rizikové [43].

Psychická manipulace oběti v rámci kybergoomingu bývá dlouhodobější. Běžně se pohybuje v rozmezí 3 měsíců až několika let. V tomto čase probíhá několik etap útoku:

První etapou je příprava na kontakt s dítětem. Útočník si zpravidla vytvoří falešnou identitu, obvykle předstírá, že je jen o něco málo starší než oběť.

V druhé etapě útočník kontaktuje oběť a snaží se o navázání a prohloupení vztahu. Obvykle používá různé techniky například tzv. efekt zrcadlení, kdy předstírá, že má stejné zájmy, problémy, názory apod. jako oběť. Čímž v ní vzbuzuje pocit přátelství, sounáležitosti a potlačuje tak strach z komunikace s neznámou osobou. Snaží se získat co nejvíce informací o své oběti, může si tak sestavovat její profil. Chce znát její tajemství. Často oběť uplácí a poskytuje jí různé dárky (např. kredit do mobilního telefonu, digitální fotoaparát,…), postupně se snaží snižovat zábrany zaváděním sexuálního obsahu do konverzace. Útočník mnohdy usiluje o získání fotografií nebo videozáznamu obnažené oběti. Predátor se také snaží o její izolaci od okolí. Ve většině případů vyžaduje po oběti, aby neřekla o jejich přátelství rodičům ani nikomu jinému. Útočník se často stává „nejlepším přítelem" oběti, ta se mu svěřuje se všemi starostmi a má k němu plnou důvěru.

Třetí etapou je příprava na osobní schůzku. Útočník připravuje oběť na to, že na setkání přijde někdo starší, než je její virtuální kamarád například „jeho otec nebo bratr". Pokud oběť se schůzkou nesouhlasí, může dojít k vydírání prostřednictvím obsahu, který útočníkovi zaslala sama oběť.

Poslední čtvrtou etapou je samotná schůzka. K sexuálnímu či jinému zneužití oběti nemusí dojít hned při první schůzce, útočník může pokračovat v manipulaci a zaútočit až po několika osobních setkáních. V případě, že pachatel zaútočí na oběť, může ji pomocí manipulace nebo vydírání přesvědčit k opakovaným schůzkám [42].

Národní centrum bezpečného internetu v Metodickém materiálu pro pedagogické pracovníky Kybergrooming a kyberstalking upozorňuje na následky, s kterými se může oběť potýkat: *„Dojde-li v rámci kybergoomingu k vydírání a zneužívání intimních materiálů oběti nebo dokonce k fyzickému zneužití prožívání a chování dítěte, může být poznamenáno posttraumatickou stresovou poruchou. Ta se může*

projevit v mnoha oblastech jako: obavy z budoucnosti, vymizení radosti, úzkost, pocity opuštěnosti, poruchy spánku a problémy s příjmem potravy, pocity únavy a vyčerpání, tendence k úniku z reality, somatické poruchy, nepřátelské reakce, odmítání i nejbližších, pocity viny, dotírající vzpomínky na událost [43].

Nejúčinnější obranou před kybergroomingem je prevence. Je důležité seznamovat především děti a mladistvé s touto problematikou a informovat je o možnosti internetové manipulace a to i v rámci výuky na základní a střední škole. Kopecký uvádí základní pravidla, jejichž dodržování žáky před kybergroomingem může ochránit:

1. Nezapomeň, že informace, které uživatelé na internetu zveřejňují, nemusí být pravdivé, kdokoliv zde může lhát.
2. Všímej si, odlišných odpovědí. Pokud někdo lže, je možné že si nebude pamatovat, co všechno si vymyslel.
3. Zpozorni, nabádá-li tě někdo k tomu, aby vaše komunikace zůstala tajná. Takové chování je velmi podezřelé.
4. Nepřijímej ani neodesílej obsah sexuální povahy.
5. Nesděluj neznámým lidem své osobní údaje ani je nezveřejňuj na svých profilech a účtech.
6. Nikdy nechoď na osobní schůzku s člověkem, kterého znáš pouze z internetu bez vědomí rodičů.
7. Důkladně zvaž, s kým si na internetu budeš povídat a o čem. Mohlo by se stát, že tě osoba, s kterou jsi si anonymně povídal/a na internetu vystopuje i v reálném světě [44].

Velmi důležité jsou dobré vztahy a komunikace v rodině. V takovém případě je výrazně větší šance, že se postižené dítě a mladistvý svěří rodičům nebo nějakému blízkému dospělému. Aby o útoku kybergroomera oběť někomu pověděla je velmi důležité a mnohdy to usnadňuje řešení celé situace. V momentě, kdy si oběť uvědomí ohrožení, je dobré zachovat klid, přesto je nutné situaci řešit, nelze spoléhat na to, že se vyřeší sama. Oběti se doporučuje zajistit důkazy a ukončit konverzaci s útočníkem, nejlépe ho blokovat. Nakonec nahlásit útok na policii a také poskytovateli služeb, při jejichž používání k napadání došlo. Tím lze alespoň částečně znesnadnit kybergroomerovi jeho další útoky [43].

3.3 Kyberstalking

Pro vysvětlení pojmu kyberstalking je dobré si nejprve definovat pojem stalking. Kopecký a Krejčí uvádějí: *„Stalking označuje opakované, dlouhodobé, systematické a stupňované obtěžování, které může mít řadu různých forem a různou intenzitu“* [42].

Útočník oběť často pronásleduje a omezuje. Také jí a jejím blízkým vyhrožuje a snaží se v oběti vzbudit pocit strachu. Stalking se většinou projevuje posíláním SMS zpráv, zanecháním vzkazů na sociálních sítích, telefonováním, posíláním nevyžádaných dárků atd. [43]. Je nutné dodat, že oběť o toto jednání nestojí a obtěžuje jí.

„Kyberstalking je chování jednotlivce, skupiny nebo organizace, které využívá infomační a komunikační technologie k pronásledování a obtěžování jiné osoby, skupiny či organizace“ [45].

Obětí se může stát kdokoliv napříč sociálním a ekonomickým spektrem. Ve většině případů se stává, že oběť útočníka (stalkera) osobně zná, ne vždy však tuší, že právě on je její pronásledovatel. Spíše výjimečně oběť stalkera osobně nezná, tito útočníci často hledají své oběti právě na sociálních sítích [42].

Stalkerem se častěji stávají muži než ženy. Útočící ženy jsou však považovány za přemýšlivější, cílevědomější a důslednější, proto jsou označovány za více nebezpečné [43].

Útočníky můžeme dělit na několik typů: **bývalý partner** (nejedná se pouze o partnerský vztah ale například i o vztah pracovní nebo obchodní), **uctívač** (touží po vztahu s obětí a předpokládá, že je tato tužba vzájemná, oběti jsou často populární osobnosti), **neobratný nápadník** (útočník je obvykle narcistické povahy, domnívající se, že je pro každého přitažlivý, touží po vztahu, zároveň však nedokáže navázat s nikým vztah zpravidla kvůli špatným sociálním a komunikačním schopnostem), **ublížený pronásledovatel** (usiluje o pomstu, z pocitu skutečné nebo domnělé újmy, kterou mu oběť způsobila) [43].

Kopecký a Krejčí přidávají ještě typ Kyberstalker (útočník používající k napadení informační a komunikační technologie), tento typ útočníka však není striktně

vyhraněný. Kyberstalking se jako doprovodný atak oběti může objevit u jakéhokoliv typu útočníka. Existuje i skupinka kyberstalkerů, kteří pronásledují svoji oběť výhradně pomocí informačních a komunikačních technologií, v těchto případech obvykle nedochází k fyzickému napadení oběti [42].

Cílem útočníka často bývá získat: totální kontrolu a moc nad obětí (chce oběť vlastnit a ovládat), nebo péči a starost o oběť (přeje si vztah s obětí), nebo chce zničit blaho oběti z důvodů zášti a nepřátelství (obvykle si přeje zničení rodinných, pracovních nebo společenských vztahů oběti, v extrémních a ojedinělých případech se může snažit donutit oběť k sebevraždě) [43].

Pronásledování bývá velmi traumatizující a pro oběť může znamenat dlouhodobé následky. Mezi nejčastější patří: deprese, úzkost, ztráta sebeúcty, pocit zranitelnosti, ztráta důvěry, posttraumatická stresová porucha, poruchy spánku, nadměrná bdělost, sebevražedné myšlenky a pokusy, sklon k užívání drog a alkoholu apod. [45].

Kyberstalking je tedy určitá forma stalkingu, ten je v České republice od roku 2010 vymezen jako trestný čin „nebezpečné pronásledování". Aby bylo možné útočníka ze stalkingu obvinit, musí být splněné následující podmínky: „*1. Musí být jednoznačné, že pronásledovatel tak činí proti vůli oběti. 2. Pronásledování musí být intenzivní. 3. Pronásledování musí být dlouhodobé (min. 4 – 6 týdnů)"* [42].

Při řešení kyberstalkingu je dobré postupovat podobně jako při řešení kyberšikany a kybergroomingu. Tedy zablokovat kyberstalkera a nezapomenout uschovat důkazy. Při pocitu ohrožení kontaktovat Policii České republiky. Ve většině případů však bude řešení kyberstalkingu úzce souviset s řešením stalkingu. Kolář a Krejčí v takovém momentu radí: „*Přerušit osobní kontakty s pronásledovatelem, vyhýbat se místům možného setkání, změnit své návyky, snažit se projevy pronásledování evidovat a zdokumentovat. Vyhledat pomoc, mimo domov se pohybovat s další osobou, nosit u sebe legální prostředky pro svou obranu a nikde nezveřejňovat své osobní údaje. Dále je dobré kontaktovat odborné instituce a v případě pocitu intenzivního strachu kontaktovat Policii ČR"* [42].

3.4 Nadměrné používání internetu a závislost

Dnes o závislosti na internetu, hlavně sociálních sítích a počítačových hrách, slýcháváme poměrně často. Proto je na začátku této podkapitoly důležité upozornit na fakt, že závislost na internetu není uznána v diagnostickém manuálu MKN-10 (Mezinárodní kvalifikace nemocí). Lze tedy říct, že se nejedná o oficiální psychickou poruchu [4]. Závislost na internetu nemá mnoho společného se závislostí na drogách nebo alkoholu. Mnohem blíže připomíná například gamblerství, jedná se o tzv. „návykové a impulzivní poruchy". Anna Ševčíková dále uvádí, že se aktuálně v České republice pro potřebu diagnostiky závislosti na internetu používá podle manuálu MKN-10 diagnóza F 63.8 „jiné impulzivní a návykové poruchy".

Na webových stránkách kliniky adiktologie 1. lékařské fakulty a VFN Univerzity Karlovy v Praze definují závislost na internetu následovně:

„Obecně se závislost na internetu definuje jako nadměrné používání internetu, které s sebou přináší do života jedince psychologické, sociální, pracovní nebo školní komplikace. Výzkumy ukázaly, že si člověk nevybuduje „závislost na internetu" obecně, ale spíše na konkrétních internetových aplikacích nebo webech. Mezi nejnávykovější aplikace či webové stránky patří ty, které umožňují obousměrnou komunikaci" [46].

Závislost na internetu je někdy také označována jako netolismus, což je závislost na tzv. virtuálních drogách (např. sociálních sítí nebo počítačových hrách).

Odborníci se shodují, že abychom vůbec mohli mluvit o závislosti na internetu, musí být naplněno 6 kritérií, které stanovil Mark Griffiths.

Kritérii jsou:

1. význačnost – daná aktivita se stane nejdůležitější aktivitou v životě jedince,
2. změna nálady – spojené s prováděním dané činnosti,
3. zvyšování tolerance – potřeba prodlužování činnosti, k dosažení stejného uspokojení jako dříve,
4. abstinenční příznaky – nepříjemné pocity v případě, že danou činnost nelze provádět,

5. konflikt – zvýšená doba činnosti přináší konflikty v mezilidských vztazích, intrapsychický konflikt (např. pocit ztráty kontroly), případně konflikty s dalšími aktivitami, kterým se uživatel věnoval,
6. rekurence (relaps, recidiva) – návrat k problémovému chování i po delší době abstinence [4].

Pokud není splněno těchto šest kritérií, nemluvíme o závislosti, ale pouze o nadměrném užívání internetu.

Mezi nejrizikovější aplikace internetu, na kterých si děti a adolescenti vytvářejí snadno závislost, patří sociální sítě a další webové stránky a programy umožňující online komunikaci. Není důležité, jestli uživatel pomocí těchto nástrojů komunikuje s lidmi, které zná z reálného světa nebo pouze s virtuálními přáteli. Problém nastává v momentě, kdy tato činnost začne narušovat jeho skutečné osobní vztahy s rodinou či blízkými a přátelství udržované prostřednictvím internetu se pro uživatele stanou důležitějšími než ty ostatní. Zvýšeně rizikovou oblastí je také hraní online her především těch, které využívají víceuživatelské virtuální prostředí. Hráči spolu v těchto hrách komunikují a spolupracují na plnění úkolů, díky čemuž se posouvají ve hře. U některých uživatelů může docházet k tzv. přetížení informacemi. Tak označujeme chování řízené nutkáním vyhledávat velké množství informací na internetu. Tyto informace však uživatel není schopný nikdy všechny využít. Samozřejmě se mohou objevit i další rizikové oblasti [45].

Nadměrné užívání internetu potažmo závislost není přímo spjata s úrovní počítačových znalostí jedince [31]. Tento jev potkává začátečníky mající pouze základní znalosti stejně jako pokročilé uživatele, kterým nejsou informační a komunikační technologie nijak cizí. Obecně lze říci, že závislostí jsou ohroženi zejména ti, pro něž je využívání internetu a jeho aplikací útěkem od problémů z reálného světa. Jedním z hlavních důvodů je to, že na internetu lze snadno uspokojovat rozličné potřeby jedince.

Americký psycholog Abraham Maslow uspořádal lidské potřeby do tzv. „pyramidy potřeb“ (viz obr. 11) [47]. Potřeby jsou zde hierarchicky upořádané do jednotlivých pater. Abychom mohli postoupit do vyššího patra, je nutné naplnit potřeby, které jsou uvedeny níže. Na internetu je plnění potřeb mnohdy snadnější než v reálném životě a případný nezdar člověka nezraňuje v takové míře. Potřeby, které není schopen uživatel internetu naplnit, obvykle potlačuje.

Obr. 11: Pyramida potřeb Abrahama Maslowa [47]

Příklady uspokojování potřeb na sociálních sítích:

Fyziologické potřeby (např. hlad, žízeň) – Tyto potřeby jako jediné uživatel obvykle potlačuje.

Bezpečí a jistota – V těžkých chvílích někteří utíkají před problémy do virtuálního světa. V případě, že se uživatel setká s něčím nepříjemným na sociálních sítích, může z nich odejít nebo nereagovat, to mu dává určitý pocit bezpečí.

Láska a sounáležitost – Na sociálních sítích se člověk setkává se svými přáteli, ať už je zná z osobního života nebo pouze díky internetu. Má tak neustáli pocit, že někam patří. Mnoho lidí se dnes také pomocí moderních technologií seznamuje s potencionálními partnery a snaží se zde najít lásku.

Úcta a uznání – Uživatel prožívá, pokud jeho názory a příspěvky na sociální síti sklízí pozitivní ohlasy. Díky tomu si zvyšuje sebevědomí.

Seberealizace – Nachází se na vrcholu pyramidy. Jedná se o potřebu pravdy, dobroty, estetické potřeby, spravedlnosti, sebevyjádření atd. [45]. Říci svůj názor

a svoji myšlenku na cokoliv, je jedna se základních věcí, kterou nám sociální sítě dovolují. K naplnění této potřeby, tak může docházet prakticky neustále.

K uspokojování potřeb může samozřejmě docházet také například v online hrách. Proto jsou právě tyto služby z hlediska závislosti rizikovější než některé jiné aplikace internetu.

Netolismus a nadužívání internetu může mít různé fyzické a psychické dopady. Nejohroženější skupinou jsou děti, u kterých může mít časté sezení u počítače za následek zhoršení pohybového vývoje a zaostávání v sociálních dovednostech. Mezi časté důsledky závislostí patří: poruchy spánku, bolesti spojené se zvýšenou zátěží určité části těla (záda, krk, hlava), problémy se zrakem (suché a namožené oči), bolest rukou a zápěstí (syndrom karpálního tunelu), změna váhy (v důsledku špatného stravování hrozí jak příbytek i úbytek váhy), zanedbávání osobní hygieny [45].

Při léčbě závislosti na internetu není primárním cílem abstinence. Je nutné si uvědomit, že internet je dnes zcela běžnou součástí života, přestat ho zcela využívat je tedy nežádoucí. Výsledkem léčby je získání kontroly nad vlastním chováním v on-line světě. Obecně se považuje za žádoucí ukončení používání problémových aplikací a zároveň běžné používání ostatních služeb. Odborná pomoc spočívá zejména v psychoterapii, kterou může doprovázet i farmakoterapeutický zásah (např. antidepresiva) [45]. V případě léčby dětí je vhodná systematická rodinná terapie, zapojení jiných aktivit do života nemocného a samozřejmě také práce s jeho motivací [4].

3.5 Další možná rizika

3.5.1 Sexting:

Pojem sexting označuje zasílání či sdílení obsahu s erotickým a sexuálním podtextem. Často jde o intimní fotografie a videa případně o sexuálně orientované komentáře. Tento fenomén se objevuje hlavně u dospívajících [39]. Obvykle dochází k zasílání těchto materiálů mezi vrstevníky např. v rámci partnerských vztahů, v některých případech děti a mladiství posílají takovýto obsah za určité benefity (např. kredit do mobilního telefonu, dárky) cizím lidem [31]. Kdokoliv kdo

takovýto materiál získá, má možnost ho využít k vydírání. Pokud dojde ke zveřejnění materiálu na internetu, může se zde zobrazovat několik let, případně se může objevit i na stránkách s pornografickým obsahem. Šiřitel sextingu tak riskuje, že přijde o dobrou pověst a důvěryhodnost, což může ovlivnit jeho další budoucnost. Pořizováním jakýchkoliv intimních fotografií, videí či jiných záznamů osob mladších 18 let i samotným nezletilým se občan České republiky může dopouštět trestného činu výroby a jiného nakládání s dětskou pornografií [43].

3.5.2 Zneužití osobních údajů:

Kyberagresoři zneužívají osobní údaje, které o sobě uvede mnohdy sama oběť. Na sociálních sítích uživatelé sdílejí mnoho informací a některé zdánlivě nevinné mohou pachatelovi velmi dobře posloužit. Tyto údaje mohou být zneužité k obohacení (například pokud uživatel na sociální síti oznámí, že odjíždí na dovolenou, nebo z ní sdílí fotografie a přitom má v profilu uvedenou adresu bydliště), k psychickému násilí (vydírání a již zmíněná kyberšikana, kybergrooming a kyberstalking), ke krádeži identity a podvodům v rovině majetkové nebo osobní, případně k cílené agresivní reklamně [34].

3.5.3 Phishing

Jedná se o podvodné většinou e-mailové útoky na uživatele s cílem získat důvěrné informace. E-mailová zpráva se snaží navodit u oběti pocit, že se jedná o zprávu z organizace, jejíž služby využívá. Nejčastěji útočník předstírá, že jde o zprávy z banky uživatele, ale může se jedna i o jiné služby například sociální sítě. V textu podvodného e-mailu je uveden odkaz, který po kliknutí uživatele přesměruje na stránky podvodníka, vypadající jako oficiální stránky služby. Zde má z určitého důvodu oběť zadat osobní informace (čísla účtů, kreditních karet, přístupových údajů a hesel) většinou pod záminkou aktualizace osobních údajů. Všechna zadaná data však získá podvodník a může je kdykoliv zneužít [48].

3.5.4 Hoax

Hoax je poplašná zpráva, která obvykle varuje před neexistujícím problémem, vyvolává paniku nebo obtěžuje adresáta. Obsahem hoaxu bývá popis nebezpečí nebo viru a jeho dopad na infikovaný počítač (od zformátování disku až po výbuch

počítače), varování z důvěryhodných zdrojů (předstírá varování např. FBI) a výzva k dalšímu rozesílání. Rozesíláním takovýchto zpráv uživatel porušuje pravidla Netikety [49].

4 Prevence a pomoc

4.1 Prevence

Nejlepší obranou proti všem rizikům spojeným s používáním sociálních sítí a internetu obecně je, jak už bylo řečeno, prevence. Je důležité pracovat s rizikovou skupinou dětí a mladistvých, poukazovat na možné problémy a nepříjemnostmi, které je mohou potkat. Vést je k bezpečnějšímu používání internetu a v neposlední řadě jim pomoci a poradit, pokud se setkají s problémem, který by neměli řešit sami.

Důležitou roli zde hrají rodiče, rozhodující jsou vztahy, které ovlivňují, zdali se dítě rodičům svěří s problémem. Druhým faktorem je počítačová gramotnost rodičů, jestli jsou schopni adekvátně posoudit závažnost situace a technicky řešit daný problém.

Škola obvykle zastává velkou část preventivní činnosti a to především rozšiřování okruhu vědomostí v souvislosti s těmito tématy. Pokud se rodič postiženého dítěte neorientuje v oblasti informačních a komunikačních technologií, pak může pedagog pomoci s řešením technické stránky problémů lépe.

V rámci prevence před kyberútokem je dobré se řídit následujícími pěti pravidly.

1. Chovat se slušně k ostatním uživatelům a respektovat Netiketu.
2. Nebýt příliš důvěřivý a nezapomínat, že kdokoliv může lhát.
3. Nikomu nesdělovat citlivé a osobní informace, které by mohly být zneužity.
4. Přečíst si a dodržovat pravidla služeb, které na internetu používáme.
5. Seznámit se s možnými riziky, se kterými se můžeme při elektronické komunikaci setkat [38].

Na internetových stránkách projektu Bezpečný internet.cz autoři uvádějí následujících 10 rad pro bezpečné používání sociálních sítí:

„Rady pro bezpečné používání sociálních sítí:

1. *Neuvádějte na veřejném profilu telefonní číslo nebo adresu.*
2. *Neposílejte nikomu svoji intimní fotografii, nikdy nevíte, kde se může objevit.*

3. *Udržujte hesla (k e-mailu i jiná) v tajnosti, nesdělujte je ani osobě blízké či kolegovi v práci.*
4. *Nikdy neodpovídejte na neslušné, hrubé nebo vulgární maily a vzkazy.*
5. *Nedomlouvejte si schůzku přes internet, aniž byste o tom neřekli někomu jinému.*
6. *Nevěřte každé informaci, kterou na internetu získáte.*
7. *Když s někým nechcete komunikovat, nekomunikujte.*
8. *Nesdělujte informace typu, kdy jedete na dovolenou, po návratu by vás mohlo čekat překvapení.*
9. *Při používání webové kamery buďte obezřetní, kdokoli může na druhé straně hovor nahrávat.*
10. *Než cokoli potvrdíte, přečtěte si podmínky užívání"* [50].

Dodržování těchto pravidel může nejen dítě nebo mladistvého uchránit před nežádoucími a bolestivými životními zkušenostmi. Je důležité určitá pravidla používání internetu vštěpovat dětem již od útlého věku.

4.2 Pomoc

V České republice funguje několik projektů, které mohou oběti pomoc při řešení nepříjemné situace a to nejen radou. Mnohdy organizace pomůže řešit problém rychleji a efektivněji, než by byl schopen jedinec sám.

Mezi nejznámější organizace patří:

4.2.1 E-bezpečí (www.e-bezpeci.cz)

Projekt E-Bezpečí je zaměřen na prevenci, vzdělávání, výzkum a osvětu spojenou s rizikovým chováním na internetu. Zabývá se hlavně kyberšikanou, sextingem, kybergroomingem, kyberstalkingem, dalšími riziky na sociálních sítích, hoaxem a spamem a zneužitím osobních údajů v prostředí elektronických médií. Se všemi těmito jevy se lze seznámit na internetových stránkách projektu E-bezpečí. Je realizován Centrem prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci ve spolupráci s dalšími organizacemi [51].

Důležitou součástí projektu je poradna, kde může kdokoliv anonymně požádat o pomoc. V rámci poradny pracují poradci pro oblast IT technologií, poradci pro oblast práva, pracovníci Policie ČR, pracovníci OSPOD (orgány sociálně-právní ochrany dětí), pracovníci z oblasti prevence kriminality a další. Pracovníci

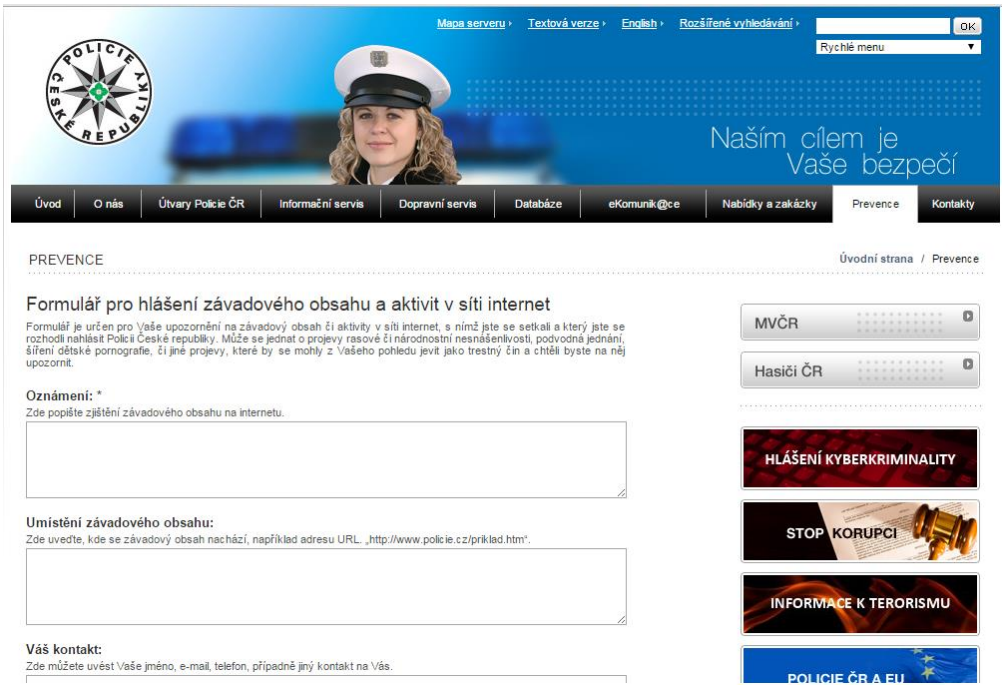
například dokáží pomoci s blokací závadného obsahu na sociální síti Facebook [52].

4.2.2 Linka bezpečí

Sdružení linka bezpečí nabízí odbornou bezplatnou pomoc dětem do 18 let a studentům do 26 let. V rámci své činnosti zřídila internetovou stránku www.pomoc-online.cz, na které seznamuje čtenáře s možnými riziky používání internetu. Na Lince bezpečí se dítěti nabídne kvalifikovaná rada i v této oblasti. Mimo to může dítě požádat o radu prostřednictvím e-mailu pomoc@linkabezpeci.cz případně v určených hodinách může psát na Chat Linky bezpečí. Rodiče, pedagogové případně ostatní dospělí mohou využít tzv. Rodičovské linky [53].

4.2.3 Policie ČR

V případě podezření na spáchání trestného činu na internetu je možné na takovéto jednání upozornit přímo na internetových stránkách Policie České republiky (http://aplikace.policie.cz/hotline) prostřednictvím „Formuláře pro hlášení závadového obsahu a aktivit v síti internet“. Oznámení je možné podat i anonymně [54].



Obr. 12: Formulář pro hlášení závadného obsahu [54]

4.2.4 Bezpečný internet.cz (www.bezpecnyinternet.cz)

Projekt Bezpečný internet.cz se zabývá riziky, která jsou spojená s používáním internetu. Projekt si klade za cíl být pomocníkem a rádcem všech uživatelů bez omezení věku a snaží se pokrýt celou škálu možných problémů. Jedná se o nekomerční projekt založený společnostmi Česká spořitelna, Microsoft a Seznam.cz, dalšími partnery jsou: cz.nic, hoax.cz, Policie ČR, advokátní kancelář Pierstone a společnost Quastasoft, podnikající v oblasti informačních technologií. Na webových stránkách projektu je možné využít poradnu. Uživatel má možnost, nahlédnou do již zodpovězených dotazů, případně poslat dotaz vlastní. Pokládání není anonymní, odesílatel však po vyřešení může zakázat dotaz veřejně zobrazovat [55].

5 Využívání sociálních sítí žáky středních škol

5.1 Metodologie práce

Hlavním cílem mé diplomové práce je zjistit, jaké sociální sítě žáci středních škol preferují, jak je využívají a zda si uvědomují možná rizika, se kterými se při této činnosti mohou setkat. Také jsem se zajímala o to, jestli si chrání svoje soukromí a zdali jim vadí nebo nevadí bavit se či scházet s cizími lidmi. V neposlední řadě mě zajímalo, zda je tomuto tématu věnován prostor při hodinách informatiky, jestli se žáci mohou přihlašovat na sociální sítě i ve škole a zda se škola zapojuje do případného řešení problémů.

K získání potřebných údajů jsem využila metodu anonymního dotazníku vlastní konstrukce, který byl směřován žákům středních škol. Dotazník byl šířen v elektronické podobě prostřednictvím serveru www.vyplnto.cz. Výzkumné šetření probíhalo v období od 26. 02. 2015 do 12. 03. 2015. Celkem se zúčastnilo 221 středoškolských studentů. Velkou část respondentů tvořili žáci Jiráskova Gymnázia v Náchodě, menší podíl pak studenti čtvrtého ročníku Gymnázia Lanškroun a studenti jiných škol. Díky způsobu šíření dotazníku ho mohl vyplnit kdokoliv. Abych zajistila, že získaná data budou pouze od studentů středních škol, zařadila jsem na začátek dotazníku otázku ošetřující tento problém. Vyplňující, kteří nejsou žáky středních škol, tak nemohli odpovídat na ostatní otázky a z vyhodnocování dotazníku byli zcela odstraněni.

Při vyhodnocování dotazníků jsem se snažila najít odpovědi na následující otázky:

Chodí na setkání s cizími lidmi častěji ženy než muži?

Zveřejňují o sobě na internetových sociálních sítích žáci 4. ročníku méně informací než ostatní žáci?

Setkávají se žáci, kteří tráví na sociálních sítích více jak 3 hodiny denně s kyberšikanou častěji než ostatní?

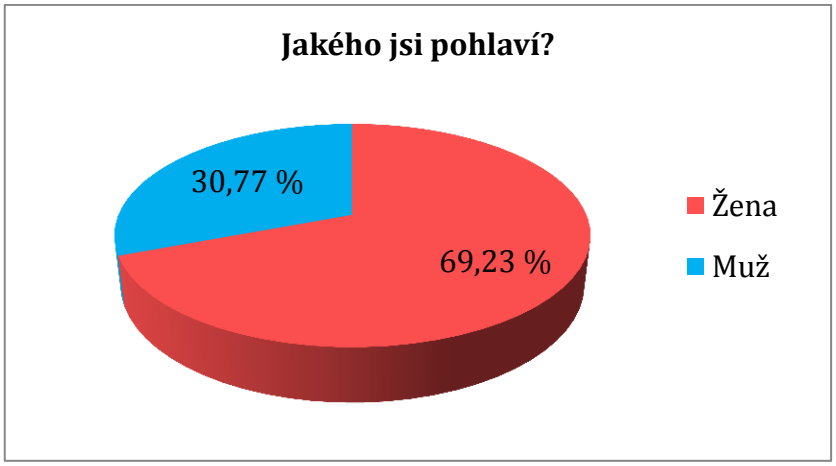
Dotazník se skládá celkem z 22 otázek. Právě 17 otázek je uzavřených, 4 polouzavřené a 1 otevřená. Některé otázky přímo navazují na určité odpovědi.

Proto jsem volila rozvětvený dotazník. Každý respondent tak odpovídal na 7–22 otázek.

Na začátek dotazníku jsem umístila 3 segmentační otázky. Jejich výsledky podrobněji ukazují, jaká skupina respondentů se do průzkumu zapojila.

Otázka č. 1: „Jakého jsi pohlaví?“

Otázka zjišťující poměr dotazovaných žen a mužů. Dotazníkového šetření se zúčastnilo 153 žen a 68 mužů.

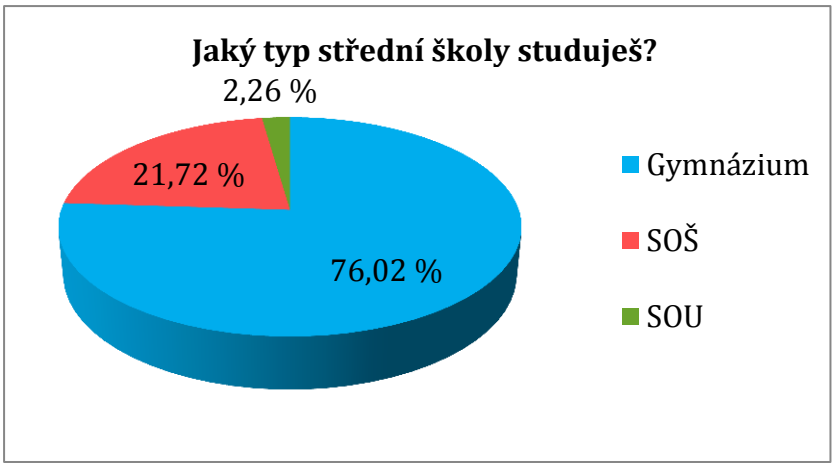


Graf 1: Pohlaví žáků

Otázka č. 2: „Jaký typ střední školy studuješ?“

Tuto otázku jsem do dotazníku zahrnula, abych zjistila, jestli se žáci studující různé typy středních škol chovají na sociálních sítích odlišně nebo je jejich chování totožné. Protože však byli respondenti z jednotlivých typů škol zastoupeni velmi nerovnoměrně, nebylo možné objektivně posuzovat rozdíly mezi chováním jejich žáků.

Gymnázium označilo jako školu, kterou studuje 168 respondentů, střední obornou školu 48 respondentů a střední odborné učiliště pouze 5 odpovídajících.

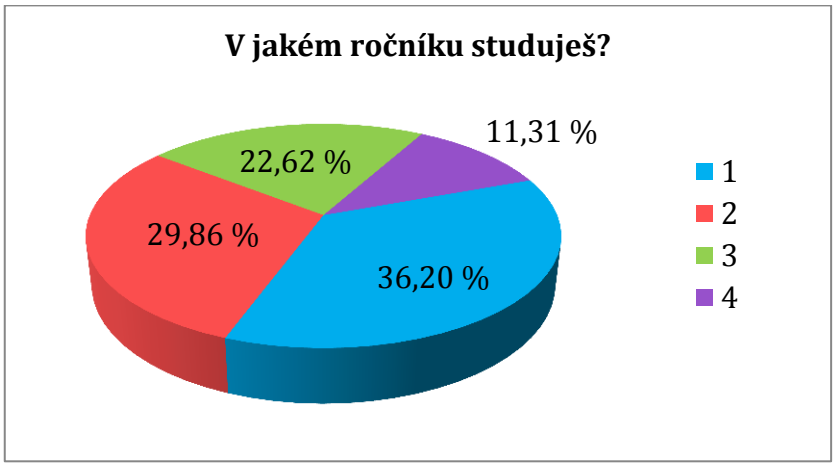


Graf 2: Typ střední školy

Otázka č. 3: „V jakém ročníku studuješ?“

Kromě typu střední školy jsem sledovala i ročník, který žáci právě studují. Což dává možnost analyzovat, jestli se chování žáků na sociálních sítích v průběhu čtyř let studia mění.

Nejvíce označovaná opověď byla 2. ročník, který studuje 80 respondentů, dále 1. ročník, který zvolilo 66 respondentů, následován 4. ročníkem s 50 respondenty, nejméně respondentů navštěvuje 3. ročník - přesně 25.



Graf 3: Ročník studia

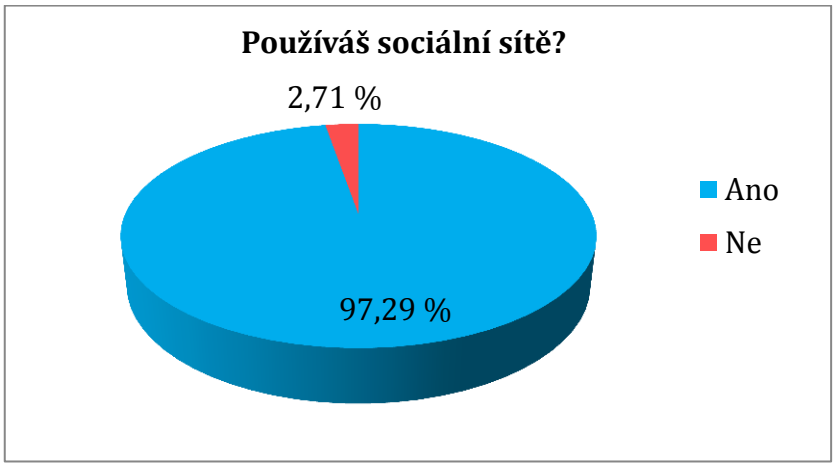
5.2 Analýza získaných údajů

Následující otázky se již přímo týkají mého průzkumu.

Otázka č. 4: „Používáš sociální sítě?“

Sociální sítě jsou v dnešní době fenoménem a nejrozšířenější jsou právě mezi mladými lidmi. Proto mě nepřekvapilo, když 215 respondentů odpovědělo „Ano“ a pouze 6 „Ne“

Protože některé další otázky se vztahovaly pouze k uživatelům sociálních sítí, zvolila jsem v tomto místě větvení dotazníků. Žáci, kteří odpověděli záporně, pokračovali otázkou č. 16.

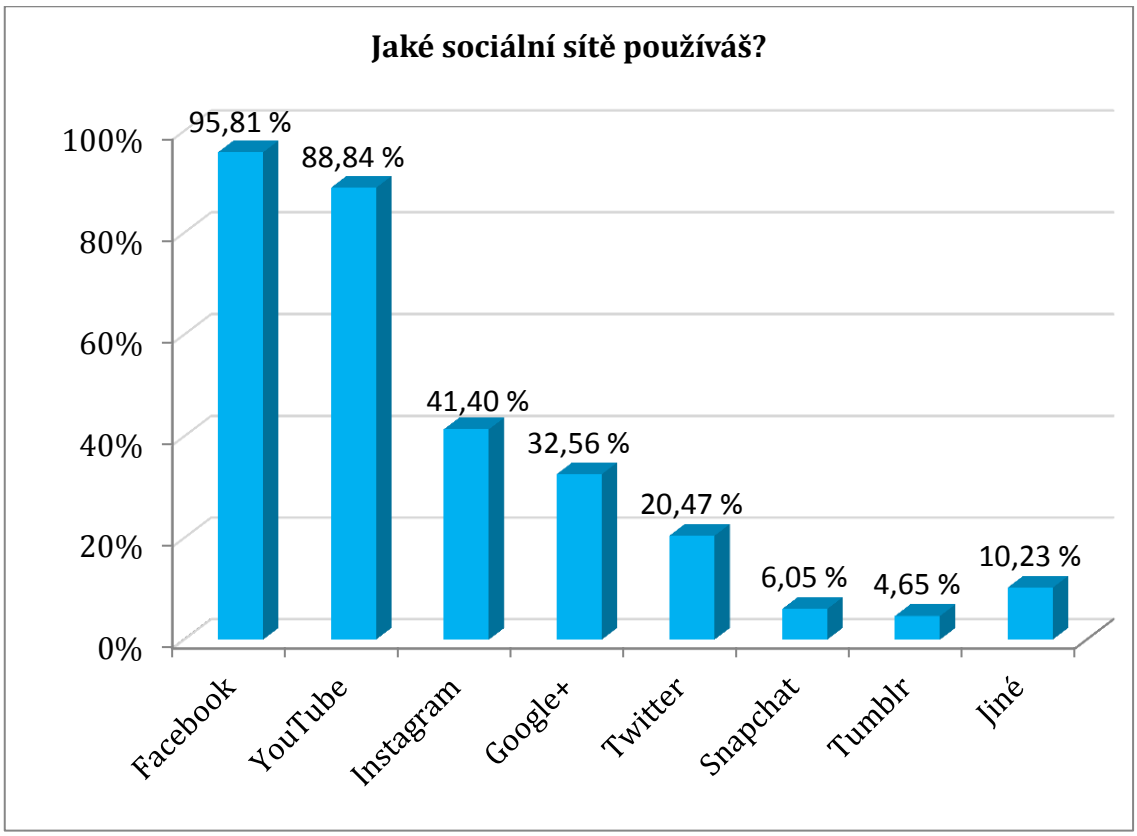


Graf 4: Využívání sociálních sítí

Otázka č. 5: „Jaké sociální sítě používáš?“

V dnešní době existuje celá řada sociálních sítí. Nejrozšířenější je u nás bezesporu Facebook. Obecně však platí, že mladí lidé jsou ochotni více experimentovat a zkoušet nové služby. Zajímalo mě, jaké sítě jsou mezi středoškoláky nejrozšířenější. Protože jeden uživatel může používat několik sociálních sítí, umožnila jsem v této otázce volit více odpovědí, proto je jejich procentuální součet větší než 100 %. Tuto otázku jsem zvolila jako polouzavřenou a to hlavně proto, aby respondenti mohli zadat všechny sociální sítě, které využívají a nebyli omezeni pouze výběrem těch nejrozšířenějších.

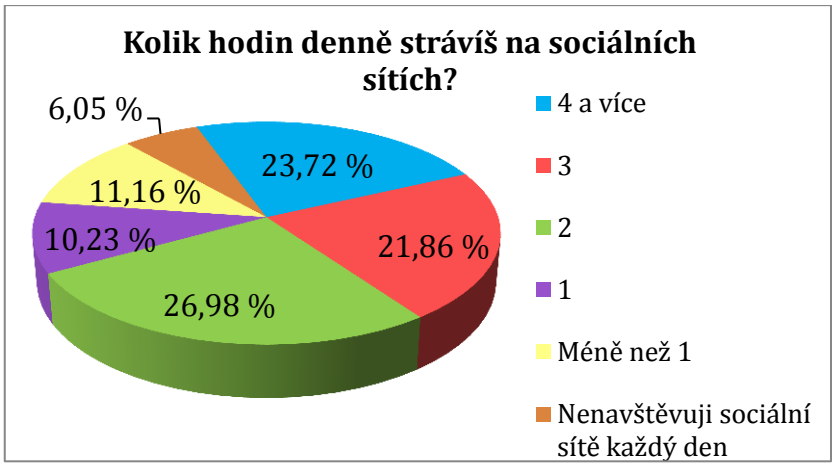
Nebylo velkým překvapením, že nejvíce konkrétně 206 respondentů uvedlo, že využívá sociální síť Facebook. Dále pak YouTube používá 191 respondentů, Instagram 89 respondentů, Google+ 70 respondentů, Twitter 44 respondentů. Možnost „Jiné“ zvolilo 35 respondentů. Nejčastěji pak zmiňovali Snapchat 13 respondentů a Tumblr 10 respondetů.



Graf 5: Typy sociálních sítí

Otázka č. 6: „Kolik času denně strávíš na sociálních sítích?“

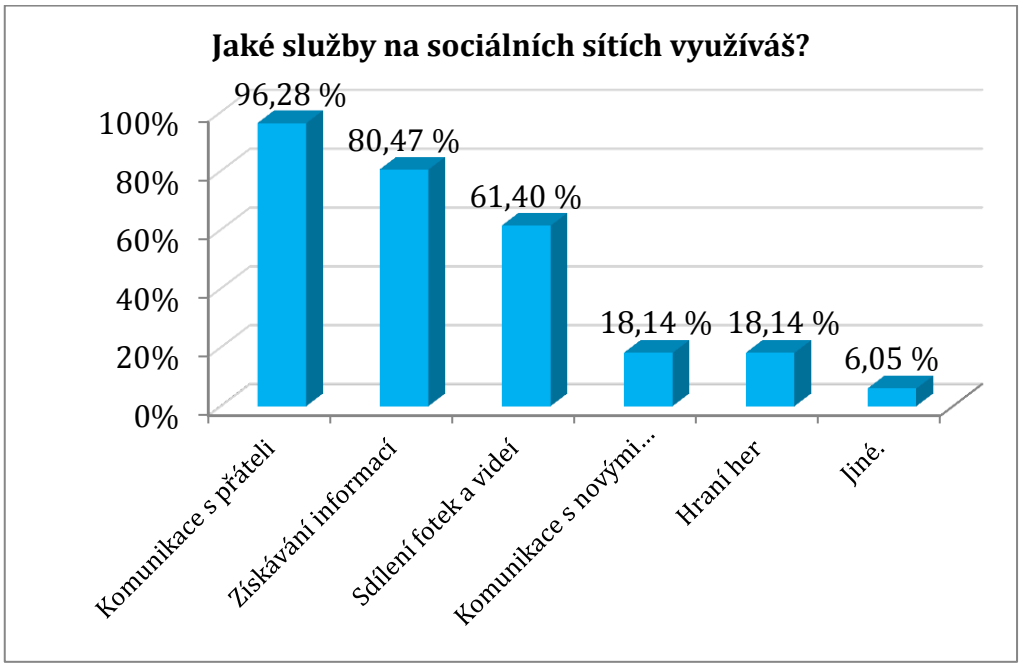
Tato otázka zjišťuje, kolik času jsou žáci středních škol zvyklí trávit na sociálních sítích. Dvě hodiny denně na nich tráví 58 odpovídajících, 4 a více hodin 51 odpovídajících, 3 hodiny 47 odpovídajících, méně než hodinu 24 odpovídajících, jednu hodinu denně 22 odpovídajících a pouze 13 odpovídajících nenavštěvuje sociální sítě každý den. Je tedy zřejmé, jak jsou u mladých lidí sociální sítě populární a kolik jsou ochotni jim věnovat času.



Graf 6: Čas strávený na sociálních sítích

Otázka č. 7: „Jaké služby na sociálních sítích využíváš?“

Na sociálních sítích je možné dělat více činností, zajímalo mě, čemu se věnují středoškoláci nejvíce. U otázky bylo možné vybrat více než jednu odpověď. Zároveň byla tato otázka polouzavřená, každý respondent tak mohl zvolit možnost „Jiné“ a dopsat vlastní odpověď.



Graf 7: Způsob užívání sociálních sítí

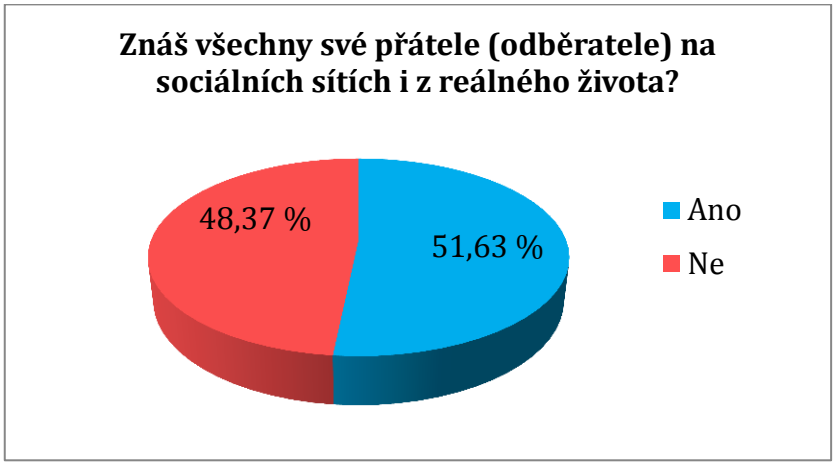
Data ukázala, že: 207 respondentů používá sociální sítě ke komunikaci s přáteli, 173 respondentů získává na sociálních sítích informace (např. o aktuálním dění), 132 respondentů sdílí fotografie a videa, 39 respondentů používá sociální sítě

k seznamování se a komunikaci s novými lidmi, 39 respondentů hraje na socích sítích hry a 13 respondentů využívá sociální sítě i k jiným činnostem, např. poslouchání hudby, prohlížení obrázků, organizování společenských akcí, příprava do školy apod.

Otázka č. 8: „Znáš všechny své přátele (odběratele) na sociálních sítích i z reálného života?“

Touto otázkou jsem chtěla zjistit, zda se žáci středních škol zajímají o to, kdo je na sociálních sítích sleduje a zda jsou ochotní komunikovat a sdílet svoje obsahy s cizími lidmi.

Odpovědi ukazují spíše neopatrnost žáků. Všechny své přátele (příp. odběratele nebo sledující) zná pouze 111 respondentů, ostatní tedy 104 respondentů uvedlo, že všechny neznají.

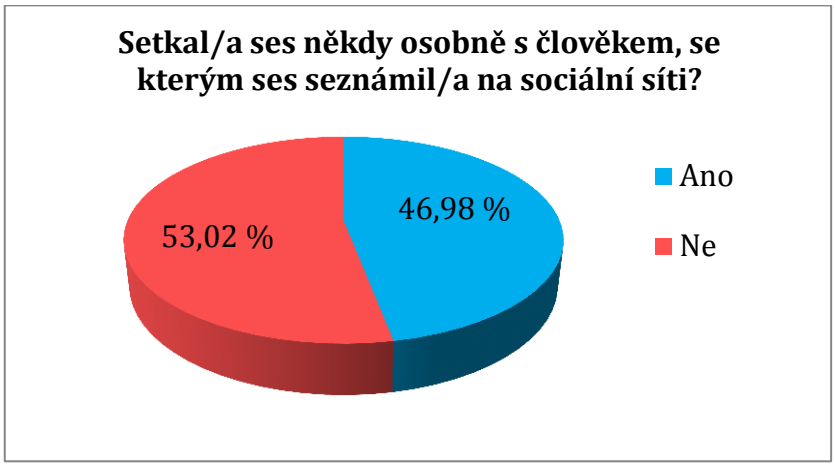


Graf 8: Znalost všech přátel (odběratelů)

Otázka č. 9: „Setkal/a ses někdy osobně s člověkem, se kterým ses seznámil/a na sociální síti?

Uzavřená otázka č. 9 vyšetřuje, zda jsou žáci ochotni setkávat se s cizími lidmi, které znají pouze ze sociálních sítí. Ukazuje se, že i přes možné nebezpečí plynoucí z tohoto chování se 101 respondentů s někým cizím již setkala. Zbylých 114 respondentů zatím nikoliv (viz graf 9). Překvapivé pro mě bylo, že se s cizími lidmi častěji setkávají muži v 57,35 % případu (přesně 39 z 68 mužů), než ženy, které se takto zachovali v 40,52 % případů (konkrétně 62 ze 153 žen). Odpověď

na otázku „Chodí na setkání s cizími lidmi častěji ženy než muži?“ zní: Ne, ženy se s cizími lidmi setkávají méně často než muži.

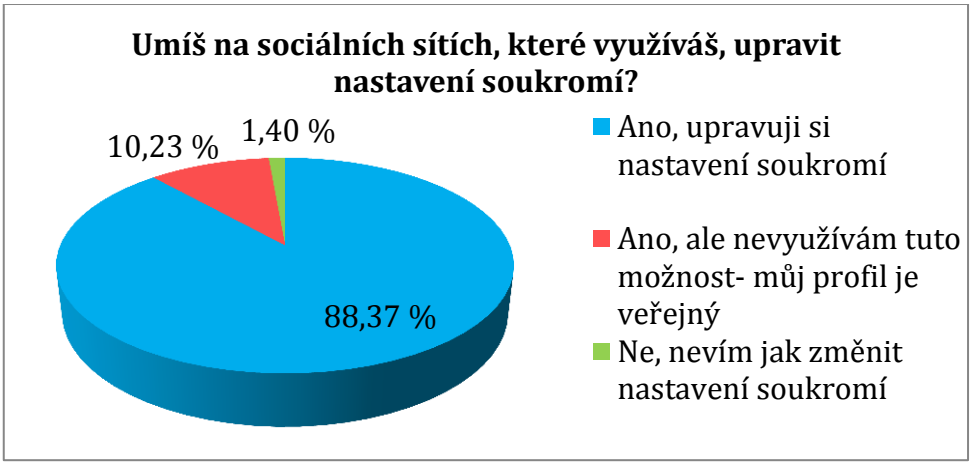


Graf 9: Setkávání se s cizími lidmi

Otázka č. 10: „Umíš na sociálních sítích, které využíváš, upravit nastavení soukromí?“

Uzavřená otázka, zabývající se problémem viditelnosti soukromého obsahu. Často lze na sociálních sítích vidět profily (účty) s nenastaveným soukromím.

Výsledky dotazníku ukazují, že žáci středních škol nemají technické problémy s nastavením soukromí a pokud mají svůj profil nastavený jako zcela veřejný, bývá to jejich vědomé rozhodnutí. Celkem 190 respondentů si upravuje nastavení soukromí, 22 respondentů ví, jak si soukromí nastavit, ale nevyužívá tuto možnost a pouze 3 respondenti uvedli, že nevědí jak toto nastavení provést.

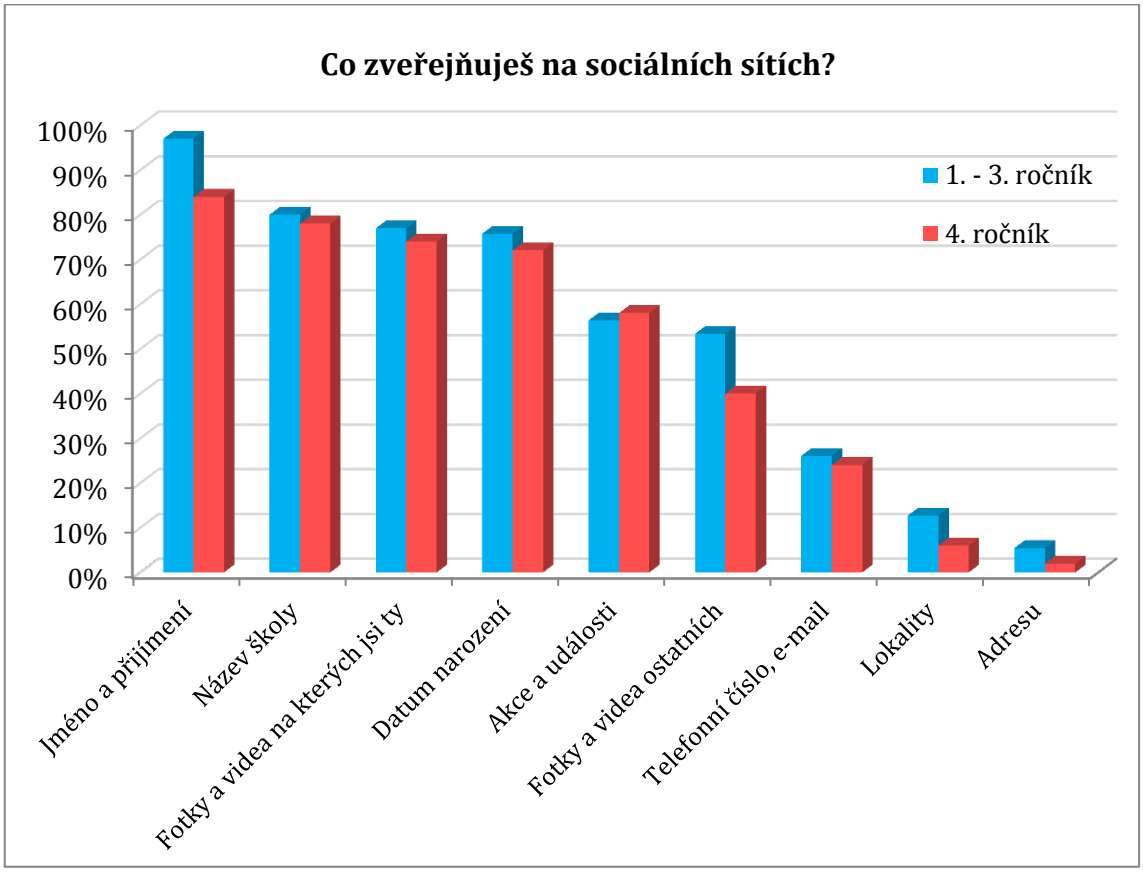


Graf 10: Nastavení soukromí

Otázka č. 11: „Co zveřejňuješ na sociálních sítích?“

Na sociálních sítích lze uvádět velké množství informací, proto jsem volila polouzavřenou otázku s možností více odpovědí.

Z 215 respondentů, kteří používají sociální sítě, na nich zveřejňuje 202 (93,95 %) pravé jméno a příjmení, 171 (79,53 %) název školy, kterou studuje, 164 (76 28 %) fotografie a videa, zachycující jí/jeho, 161 (74,88 %) datum narození, 122 (56,74 %) akce a události, kterých se plánuje zúčastnit, 108 (50,23 %) fotografie a videa dalších lidí (např. rodiny, přátel,…), 55 (25,58 %) telefonní číslo nebo e-mail, 24 (11,16 %) lokality, ve kterých se pravidelně pohybuje, 10 (4,65 %) adresu, jeden respondent (0,47 %) volil možnost jiné a pouze dva uživatelé (0,94 %) nezveřejňují na sociálních sítích žádné osobní údaje.



Graf 11: Zveřejňování osobních informací – porovnání ročníků

Abych mohla odpovědět na otázku: „Zveřejňují o sobě na internetových sociálních sítích žáci 4. ročníku méně informací než ostatní žáci?“ potřebovala jsem zjistit, jestli se v této oblasti mění chování uživatelů během dospívání. Jak je vidět

na grafu 11, žáci čtvrtých ročníků o sobě skutečně sdělují méně informací. Největší pokles okolo 13 % je u zveřejňování fotografií a videí ostatních lidí a pravého jména a příjmení. 6% pokles je pak možné vidět u zveřejňování lokalit, v kterých se osoba často pohybuje. Oproti tomu je mírný 1,64% nárůst možné sledovat ve sdílení akcí a událostí, kterých se žák plánuje zúčastnit. Celkově lze říci, že žáci 4. ročníků oproti ostatním žákům zveřejňují skutečně méně osobních informací.

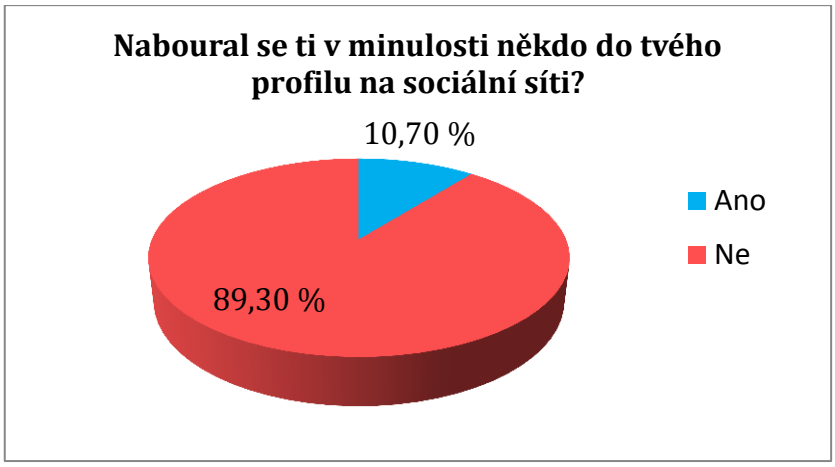
Otázka č. 12: „Zná někdo další přihlašovací údaje k tvým profilům na sociálních sítích?“

I přesto, že jsou uživatelé neustále upozorňováni, aby nikomu nesdělovali své přihlašovací údaje k jednotlivým službám (např. při používání sociální sítě Facebook se toto jednání přímo rozchází s jejich podmínky užití), tak 28 z 215 respondentů přiznalo, že někdo další zná jejich přihlašovací údaje.

Graf 12: Sdělování přihlašovacích údajů

Otázka č. 13: „Naboural se v minulosti někdo do tvého profilu na sociální síti?“

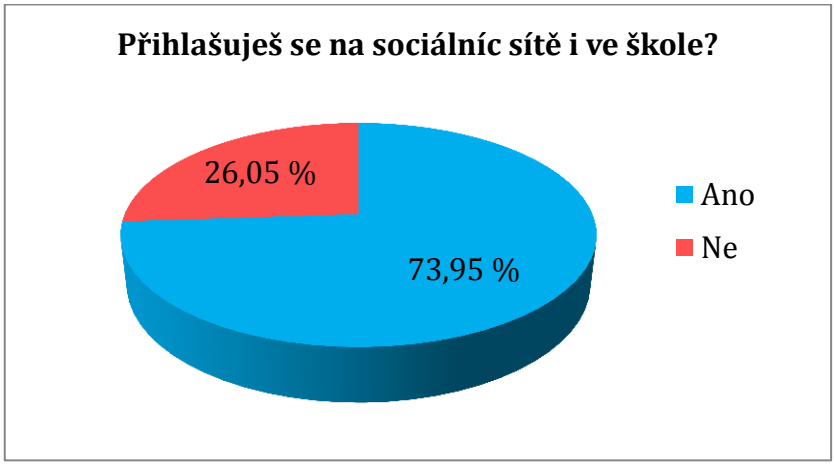
Nepříjemnou zkušeností, která může uživatele sociálních sítí potkat, je krádež a případné zneužití účtu. Podle výsledků průzkumu se s tímto setkalo 23 z 215 respondentů.



Graf 13: Zkušenost se zneužitím účtu

Otázka č. 14: „Přihlašuješ se na sociální sítě i ve škole?“

V některých případech se školy nechtějí zapojovat do řešení kyberšikany. Jejich časným argumentem je, že se kyberšikana mnohdy neodehrává v době, kterou žáci tráví ve škole. Odpovědi v dotazníkovém šetření však ukazují, že 159 z 215 žáků používajících sociální sítě na ně přistupuje i ze školy (viz graf 14). Na tuto otázku přímo navazuje otázka č. 15, která byla položena pouze žákům, kteří odpověděli kladně. Zbývajících 56 respondentů pokračovala otázkou č. 16.



Graf 14: Používání sociálních sítí ve škole

Otázka č. 15: „Z jakého zařízení se ve škole na sociální sítě přihlašuješ?“

Zajímalo mě, jestli žáci přistupují ve škole na sociální sítě pouze z vlastního zařízení, nebo jestli využívají i školní. Ukázalo se, že pouze ze školního zařízení (počítače, notebooku,…) přistupuje k sociálním sítím 27 žáků, ze školního

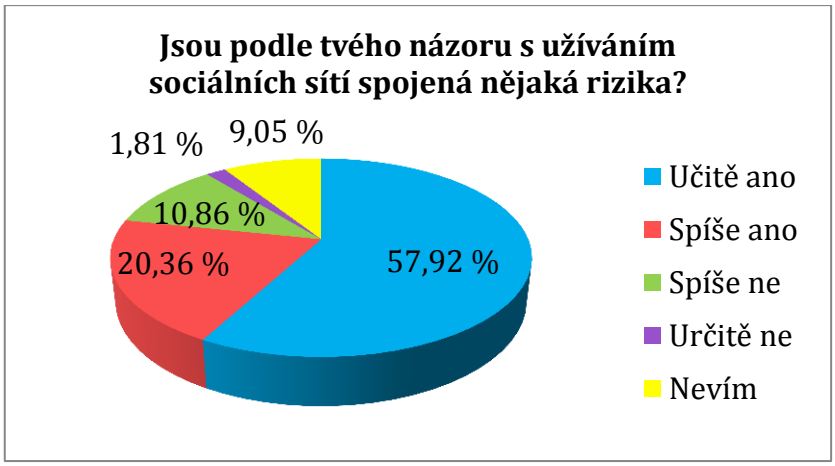
i vlastního zařízení 77 žáků a pouze z vlastního zařízení (telefonu, tabletu,…) 55 žáků.

Graf 15: Připojování se k sociálním sítím

Zvážíme-li chování všech zúčastněných respondentů dotazníku, lze říci, že se ze školního zařízení přihlašuje na sociální sítě 47,06 % žáků středních škol. Nelze tedy nikdy vyloučit, že pokud je dítě obětí kyberšikany, nedochází k útokům během času, který žák tráví ve škole.

Otázka č. 16: „Jsou podle tvého názoru s užíváním sociálních sítí spojená nějaká rizika?“

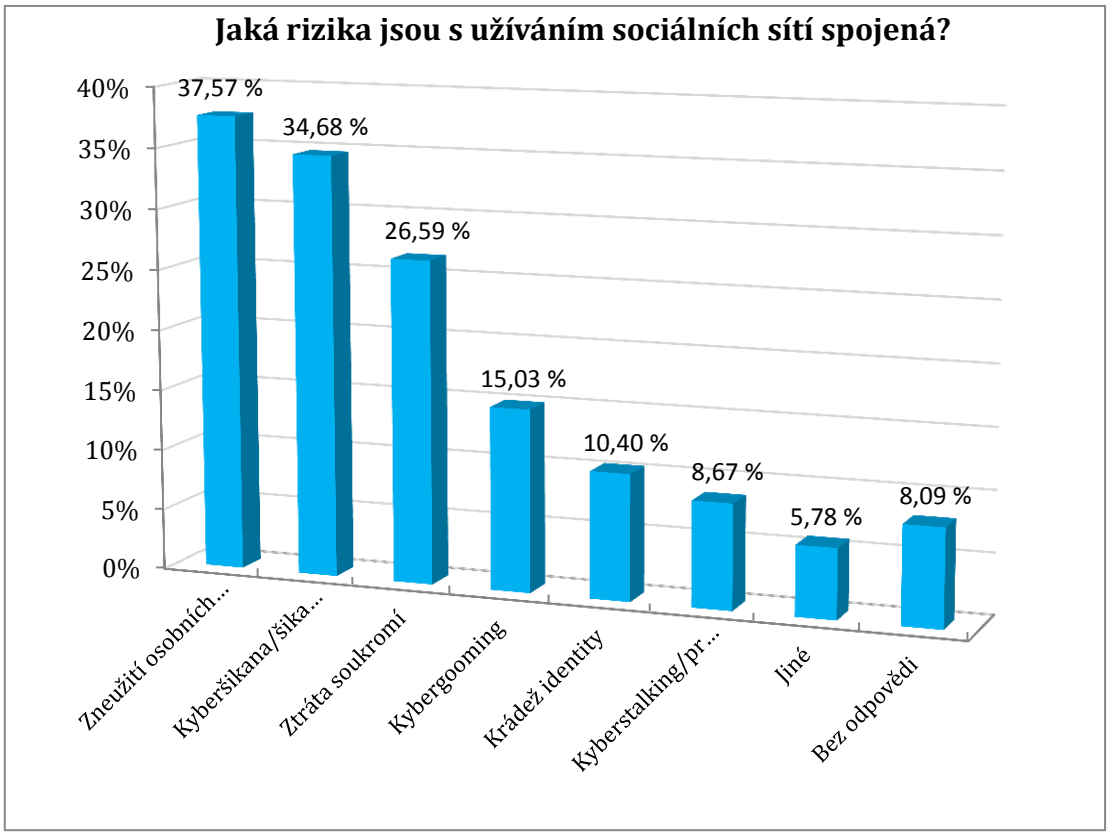
Výsledky dotazníku naznačují, že si středoškolští žáci uvědomují určitá nebezpečí, s kterými se mohou setkat při používání sociálních sítí. Odpověď „určitě ano“ zvolilo 128 respondentů, „spíše ano“ 45 respondentů, „spíše ne“ 24 respondentů, „určitě ne“ 4 respondenti, „nevím“ odpovědělo 20 respondentů. Na otázku č. 17 odpovídali pouze respondenti, podle nichž mohou být sociální sítě nebezpečné. Ostatní pokračovali na otázku č. 18.



Graf 16: Výskyt rizik na sociálních sítích

Otázka č. 17: „Jaká rizika jsou s užíváním sociálních sítí spojená?“

Snažila jsem se zjistit, co žáci považují za skutečné nebezpečí na sociálních sítích, aniž bych jim některé problémy přímo podsouvala. Proto jsem v tomto případě volila otevřenou otázku. Následně jsem odpovědi rozdělila do několika skupin. Každý respondent mohl napsat více odpovědí.

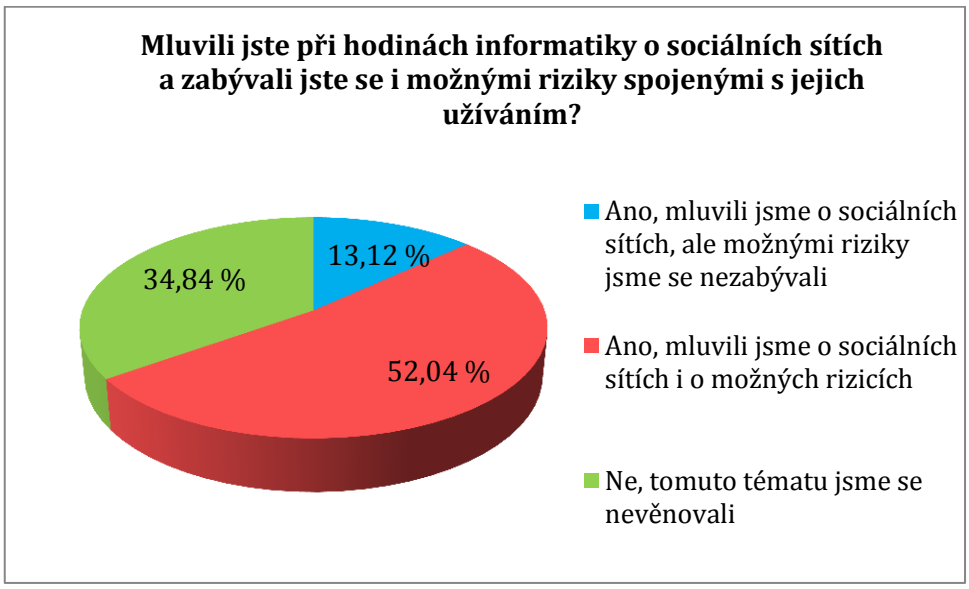


Graf 17: Častá rizika na sociálních sítích

Jako největší riziko respondenti vidí: zneužití osobních informací a soukromého obsahu 65, kyberšikanu a šikanu 60, ztrátu soukromí 27, krádež identity a zneužití profilu 18, kyberstalking a pronásledování 15, jiné 10, 14 respondentů na tuto otázku neodpovědělo.

Otázka č. 18: „Mluvili jste při hodinách informatiky nebo jiného předmětu o sociálních sítích a zabývali jste se i možnými riziky spojenými s jejich užíváním?“

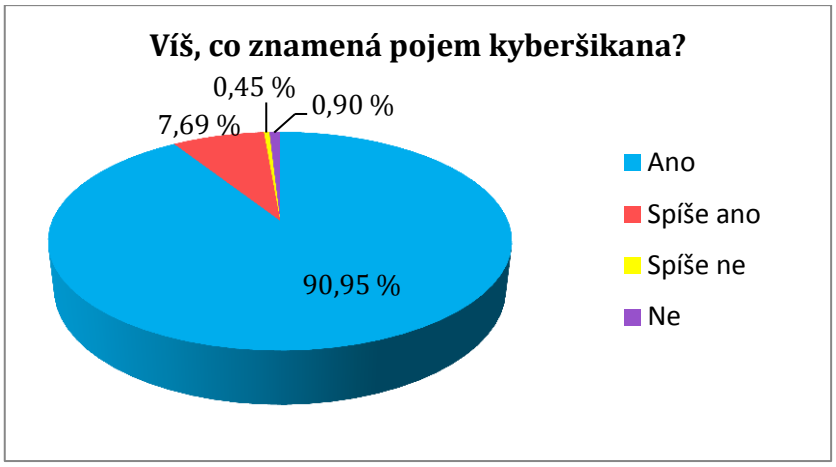
Jako nejlepší způsob boje proti kyberšikaně a dalším negativním jevům na sociálních sítích se považuje prevence. Zajímalo mě, jestli se tomuto tématu věnují učitelé pří výuce informatiky případně jiných předmětů. 115 žáků zvolilo možnost „ano, mluvili jsme o sociálních sítích i o možných rizicích“, 29 žáků vybralo odpověď „Ano, mluvili jsme o sociálních sítích, ale možnými riziky jsme se nezabývali“ a 77 žáků odpovědělo „ne, tomuto tématu jsme se nevěnovali“.



Graf 18: Prevence ve školách

Otázka č. 19: „Víš, co znamená pojem kyberšikana?“

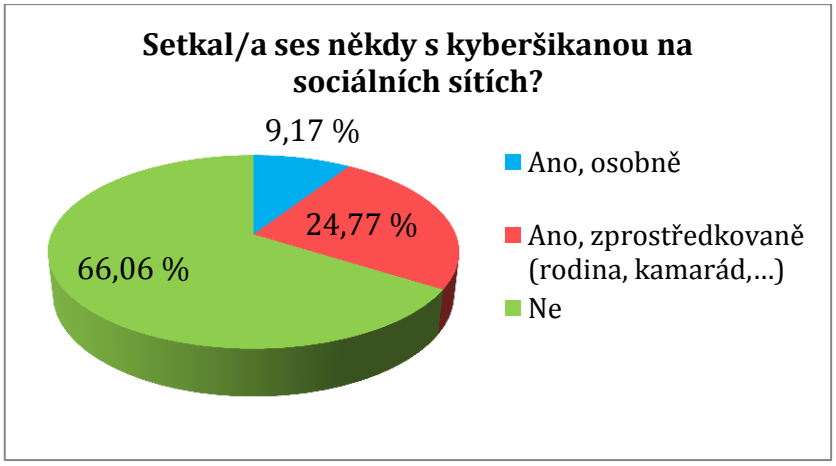
Pojem kyberšikana byl drtivé většině respondentů znám. „Ano“ odpovědělo 201 odpovídajících, „spíše ano“ 17 odpovídajících, pouze jeden odpovídající uvedl „spíše ne“ a 2 uvedli, že nevědí co pojem kyberšikana znamená. I v tomto místě se dotazník větvil, žáci, kteří neznali význam tohoto pojmu, pokračovali otázkou č. 22.



Graf 19: Pojem kyberšikana

Otázka č. 20: „Setkal/a ses někdy s kyberšikanou na sociálních sítích?“

Jak bylo uvedeno v teoretické části práce, kyberšikana se definuje různě a to ovlivňuje výsledky výzkumů jejího rozšíření. Zjišťovala jsem, kolik respondentů se z kyberšikanou setkalo. Odpověď „ano, osobně“ zvolilo 20 respondentů. Druhou možnost „ano, zprostředkovaně (rodina, kamarád,…)“ vybralo 54 respondentů. Zbývajících 144 respondentů odpovědělo, že se s kyberšikanou nesetkalo.



Graf 20: Zkušenost s kyberšikanou

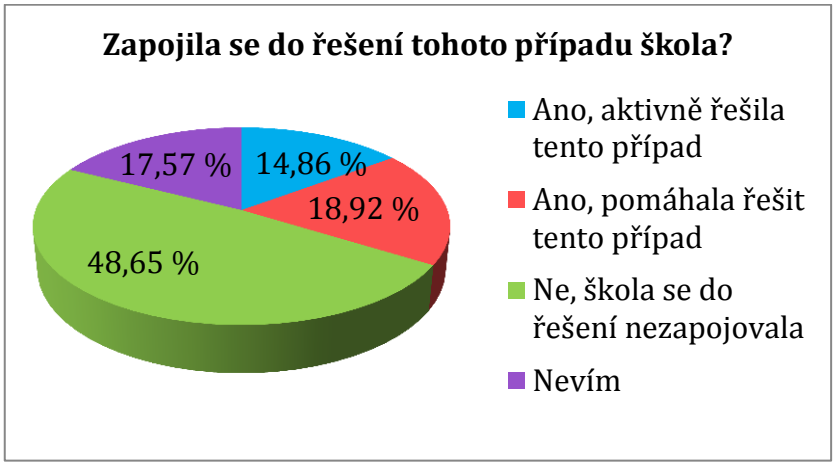
V předešlé podkapitole jsem položila otázku: „Setkávají se žáci, kteří tráví na sociálních sítích více jak 3 hodiny denně s kyberšikanou častěji než ostatní?“

Při hledání odpovědi jsem vycházela z výsledků otázek č. 6 a č. 20. Vzhledem k tomu, že žáků, kteří se osobně s kyberšikanou setkali, bylo z celého spektra pouze 20 (9,17 %), je třeba tyto výsledky brát spíše orientačně. Nicméně sesbíraná

data ukazují, že se s kyberšikanou osobně setkává 12 z 99 žáků, kteří tráví na sociálních sítích více než 3 hodiny denně, tedy 12 % z nich. Naproti tomu s kyberšikanou se setkává 8 ze 122 žáků, kteří tráví na sociálních sítích méně jak tři hodiny denně, tedy 6,6 % z nich. Kladnou odpověď na výše uvedenou otázku, tak potvrzuje více než 5% rozdíl v četnosti této situace.

Otázka č. 21: „Zapojila se do řešení tohoto případu škola? (zastoupená např. učitelem, výchovným poradcem, apod.)“

Tato otázka se zobrazila pouze respondentům, kteří se někdy s kyberšikanou setkali. Z nich 11 odpovědělo „ano, aktivně řešila tento případ“, 14 odpovědělo „ano, pomáhala řešit tento případ“, 36 respondentů pak udalo odpověď „ne, škola se do řešení tohoto případu nezapojovala“ a 13 respondentů nevědělo, jak se daná situace nakonec řešila.



Graf 21: Řešení kyberšikany ve škole

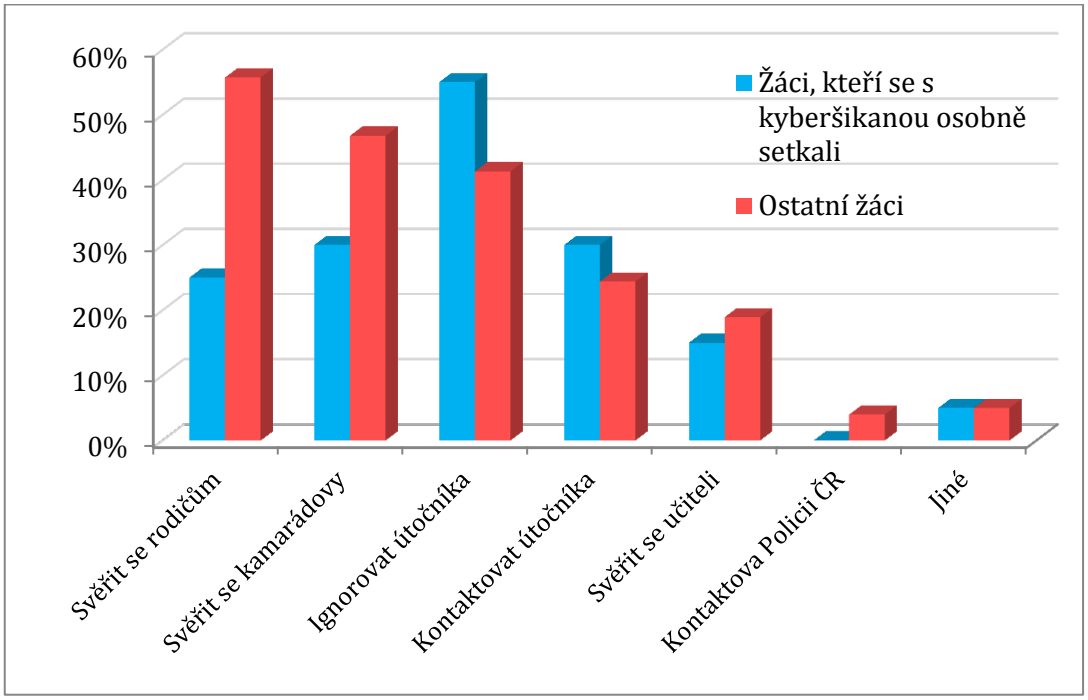
Otázka č. 22: „Jak jsi kyberšikanu řešil/a? Případně jak bys postupoval/a, kdyby ses s kyberšikanou osobně setkal/a?“

Zajímalo mě, jaký postup volili kyberšikanovaní žáci, když se s tímto problémem setkali. A také to, co považují za správné řešení kyberšikany ti, co se s ní zatím osobně nesetkali. U této otázky bylo možné zvolit více možností, zároveň se jednalo o polouzavřenou otázku, respondenti tedy mohli napsat i jiné řešení.

Nejčastěji volenými opatřeními byli: „povědět o útoku rodičům“ 117 respondentů (52,94 %), „povědět o útoku kamarádovi“ 100 respondentů (45,25 %), „ignorovat

a blokovat útočníka“ 94 respondentů (42,53 %), „kontaktovat útočníka a vysvětlit si to s ním“ 55 respondentů (24,89 %), „povědět o útoku učiteli“ 41 respondentů (18,55 %), „kontaktovat Policii ČR“ 8 respondentů (3,62 %), jiný postup (např. pomstu, nahlášení správci služby apod.) by volilo 11 respondentů (4,98 %).

V grafu 22 jsem rozdělila zvlášť odpovědi žáků, kteří museli kyberšikanu osobně řešit od odpovědí čistě teoretických od těch žáků, kteří se s tímto problémem zatím osobně nepotkali. Lze pozorovat určité rozpory v těchto odpovědích. Je zjevné, že většina žáků tuší, že nejlepší řešení je svěřit se někomu blízkému nejlépe dospělému. Ale ve chvíli, kdy se jedinec v dané situaci v pozici oběti ocitne, raději volí jiné metody a řeší problém sám.



Graf 22: Řešení kyberšikany - porovnání

Závěr

Díky průzkumu jsem potvrdila, že internetové sociální sítě využívá většina žáků středních škol prakticky bez rozdílů pohlaví, typu střední školy nebo ročníku studia. Nebylo překvapením, že většina žáků používá sociální síť Facebook, zároveň se ukázalo, že spolu s ním využívají i služeb dalších sociálních sítí a tráví na nich často několik hodin denně.

Dozvěděla jsem se, že žáci jsou si vědomi možných rizik, která jsou s užíváním sociálních sítí spjatá, umějí si změnit nastavení soukromí na svých účtech a přemýšlí nad tím, které údaje o sobě zveřejní a které nikoli. Na druhou stranu mě ale překvapilo, že téměř polovina žáků je ochotná scházet se s cizími lidmi, které znají pouze prostřednictvím sociálních sítí.

Také jsem se snažila zjistit, jak z pohledu žáka přistupuje k této problematice jeho škola. Výsledky dotazníkového šetření ukázaly, že ze školního zařízení se někdy k sociálním sítím přihlašuje téměř polovina žáků. Také se ukázalo, že s kyberšikanou se setkalo ať už osobně nebo zprostředkovaně každé třetí dítě. S ohledem na tyto výsledky ukazující na problémy, u kterých nelze vyloučit, že se mohou odehrávat i během pobytu dítěte ve škole, je lehce znepokojivé, že o rizicích spojených s užíváním sociálních sítí nebyla v rámci výuky seznámena téměř polovina žáků.

Pokud jde o samotné řešení kyberšikany ukazuje se, že žáci ví, jak nejlépe postupovat. Ovšem v momentě, kdy se jich tento problém skutečně dotýká, často přehodnocují situace a zachovají se odlišně.

Pro zmapování situace ohledně využívání sociálních sítí žáky středních škol jsem využila metodu anonymního dotazníku především proto, že tímto způsobem lze získat potřebné informace od relativně velké a různorodé skupiny respondentů.

Teoretická část mé diplomové práce je nejprve věnována sociálním sítím, jejich stručné historii, jejich rozdělením, výhodám a nevýhodám a popularitě, které se dnes těší. V dalších kapitolách představuju nejvíce využívané sociální sítě v České republice a jejich základní vlastnosti. Poté se věnuji rizikům, která mohou

při používání sociálních sítí žáky potkat, i tomu jak se jim bránit a kde je možné hledat pomoc.

Jsem přesvědčená, že je potřeba o těchto problémech otevřeně mluvit, neboť s nárůstem popularity takovýchto služeb je velká pravděpodobnost, že se setkáme i s nárůstem obětí, na které budou směřované útoky právě pomocí sociálních sítí nebo jiných služeb internetu.

Tato práce má především informativní charakter, shrnuje danou problematiku, která se dnes může dotknout každého uživatele a upozorňuje právě na žáky středních škol, neboť ti jsou často velmi ohroženi, a návyky, které si v souvislosti s používáním sociálních sítí budují, je budou mnohdy provázet i v dospělosti.

Pevně věřím, že stanovený cíl diplomové práce jsem splnila. Toto téma je bezesporu velmi aktuální a nabízí spoustu možností pro další studium. Bylo by například zajímavé studovat názory pedagogů, případně rodičů na danou problematiku.

Použitá literatura

[1] Social network Definition from PC Magazine Encyclopedia. *Technology Product Reviews, News, Prices & Downloads | PCMag.com | PC Magazine* [online]. © 1996-2015 [cit. 2015-02-18]. Dostupné z: http://www.pcmag.com/encyclopedia/term/55313/social-network

[2] PAVLÍČEK, Antonín. *Nová média a sociální sítě*. V Praze: Oeconomica, 2010, 181 s. ISBN 978-802-4517-421.

[3] SLÁMOVÁ, Hana. ISP IV - Komunikace v malých skupinách a sociální sítě. *Hana Slámová - VOŠIS, VŠE, UISK, U3V* [online]. 13. 4. 2010 [cit. 2015-02-20]. Dostupné z: http://www.joomla.slamow.com/informace-a-spolecnost/prednasky/86-isp-iii-komunikace-v-malych-skupinach.html

[4] ŠEVČÍKOVÁ, Anna a kol. *Děti a dospívající online: Vybraná rizika používání internetu*. Praha: Grada, 2014, 183 s. Psyché. ISBN 978-802-4750-101.

[5] Sociální sítě 2.díl, společné prvky. *Webové stránky zdarma | BANAN.CZ = webové stránky zdarma a hosting* [online]. [2009] [cit. 2015-03-01]. Dostupné z: http://www.banan.cz/serialy/Socialni-site/Socialni-site-2-dil-spolecne-prvky

[6] Sociální sítě - Historie sociálních sítí. *Sociální sítě* [online]. © 2014 [cit. 2015-02-20]. Dostupné z: http://www.socialnisite.estranky.cz/clanky/historie-socialnich-siti.html

[7] KIRKPATRICK, David. *Pod vlivem Facebooku: příběh z nitra společnosti, která spojuje svět*. Překlad Helena Danihelková, Jiří Huf, Ondřej Doseděl. Brno: Computer Press, 2011, 320 s. ISBN 978-80-251-3573-0.

[8] Digizen - Social networking - Report - What are social networking services. *Digizen - Home* [online]. © 2005-2015 [cit. 2015-02-21]. Dostupné z: http://www.digizen.org/socialnetworking/sn.aspx

[9] Sociální sítě. *Infografika: Česko a internetová reklama | Effectix Doba Webová* [online]. 2012 [cit. 2015-03-01]. Dostupné z: http://www.doba-webova.com/

[10] MML: Facebook je největší sítí v ČR, dvojkou YouTube | MediaGuru. *MediaGuru: reklama, marketing a média očima Gurua* [online]. 22. 12. 2014 [cit. 2015-04-14]. Dostupné z: http://www.mediaguru.cz/2014/12/mml-facebook-je-nejvetsi-siti-v-cesku-dvojkou-je-youtube/#.VS1tStysWZV

[11] Company Info. *Newsroom* [online]. © 2015 [cit. 2015-03-01]. Dostupné z: http://newsroom.fb.com/company-info/

[12] Zásady koumunity. *Facebook* [online]. © 2015 [cit. 2015-03-01]. Dostupné z: https://www.facebook.com/communitystandards/

[13] *Facebook* [online]. © 2015 [cit. 2015-03-01]. Dostupné z: www.facebook.com

[14] Podmínky. *Facebook* [online]. 30. 1. 2015 [cit. 2015-03-04]. Dostupné z: https://www.facebook.com/legal/terms

[15] NĚMEC, Petr. Google po deseti letech ukončí sociální sít Orkut. *Root.cz: Informace nejen ze světa Linuxu* [online]. 1. 7. 2014 [cit. 2015-03-10]. ISSN 1212-8309. Dostupné z: http://www.root.cz/zpravicky/google-po-deseti-letech-ukonci-socialni-sit-orkut/

[16] *Google+* [online]. [2011] [cit. 2015-03-11]. Dostupné z: https://plus.google.com/

[17] Společnost: Google. *Google* [online]. [1998], [2011] [cit. 2015-04-10]. Dostupné z: http://www.google.com/intl/cs_cz/about/company/

[18] KASÍK, Pavel. Google+ má přes dvě miliardy uživatelů, více než Facebook. *Technet.cz: Technika kolem nás* [online]. 23. 11. 2014 [cit. 2015-03-11]. Dostupné z: http://technet.idnes.cz/google-plus-dve-miliardy-uzivatelu-d60-/sw_internet.aspx?c=A141021_204910_sw_internet_pka

[19] Smluvní podmínky společnosti Google: Ochrana soukromí a smluvní podmínky. *Google* [online]. 14. 4. 2014 [cit. 2015-03-11]. Dostupné z: https://www.google.com/intl/cs_ALL/policies/terms/

[20] Jak to bylo nebylo, YouTube slaví 10. narozeniny. *Mediamania.cz: Reklama, marketing a média* [online]. 13. 2. 2015 [cit. 2015-03-12]. Dostupné

z: http://mediamania.tyden.cz/rubriky/on-line/jak-to-bylo-nebylo-youtube-slavi-10-narozeniny_333378.html

[21] YouTube oslavil 10 let. Kam se portál za poslední dekádu posunul?. *YouTuberi.net: Komunita pro všechny české youtubery* [online]. 16. 2. 2015 [cit. 2015-03-12]. Dostupné z: http://youtuberi.net/youtube-oslavil-10-let-kam-se-portal-za-posledni-dekadu-posunul/

[22] RYLICH, Jan. Nepovedená integrace YouTube a Google Plus. *Ikaros* [online]. 2013, ročník 17, číslo 12 [cit. 2015-03-12]. urn:nbn:cz:ik-14245. ISSN 1212-5075. Dostupné z: http://ikaros.cz/node/14245

[23] *YouTube* [online]. © 2015 [cit. 2015-03-12]. Dostupné z: https://www.youtube.com/

[24] ČIČÁK, Matěj. Twitter oslavil šesté narozeniny, podívejte se na původní náčrtek. *Živě.cz: O počítačích, IT a internetu* [online]. 26. 3. 2012 [cit. 2015-03-16]. Dostupné z: http://www.zive.cz/bleskovky/twitter-oslavil-seste-narozeniny-podivejte-se-na-puvodni-nacrtek/sc-4-a-162974/default.aspx

[25] Twitter vznikl před pěti lety. *Informace, testy a novinky o hardware, software a internetu: CHIP.cz* [online]. 14. 3. 2011 [cit. 2015-03-20]. Dostupné z: http://www.chip.cz/trendy/twitter-vznikl-pred-peti-lety/

[26] Our mission: To give everyone the power to create and share ideas and information instantly, without barriers. *About Twitter: About* [online]. © 2015 [cit. 2015-03-20]. Dostupné z: https://about.twitter.com/company

[27] Layout Instagram. *Instagram* [online]. 2015 [cit. 2015-03-21]. Dostupné z: https://instagram.com/press/

[28] About Us. *Instagram* [online]. 2015 [cit. 2015-03-21]. Dostupné z: https://instagram.com/about/us/

[29] Děti a rizika sociálních sítí. *Informační portál - Šance Dětem* [online]. 3. 2. 2014 [cit. 2015-04-01]. Dostupné z: http://www.sancedetem.cz/srv/www/content/pub/cs/clanky/deti-a-rizika-socialnich-siti-112.html

[30] ČERNÁ, Alena, Lenka DĚDKOVÁ, Hana MACHÁČKOVÁ, Anna ŠEVČÍKOVÁ a David ŠMAHEL. *Kyberšikana: průvodce novým fenoménem*. Editor Alena Černá. Praha: Grada, 2013, 150 s. Psyché. ISBN 978-80-247-4577-0.

[31] *Děti a jejich problémy III: sborník studií*. Praha: Sdružení Linka bezpečí, 2010, 142 s. ISBN 978-80-254-6840-1. Dostupné z: http://www.vyzkum-mladez.cz/zprava/1378730622.pdf

[32] Co teenagery na sociálních sítích tak baví?. *Bezpečně online* [online]. [2011] [cit. 2015-04-17]. Dostupné z: http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-teenagery-na-socialnich-sitich-tak-bavi.html

[33] Rizika sociálních sítí. *Bezpečný internet* [online]. [2012] [cit. 2015-04-17]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/socialni-site/rizika.aspx

[34] *Ochrana osobních údajů a osobnosti: Metodický materiál pro pedagogické pracovníky* [online]. Národní centrum bezpečnějšího internetu, 2012, 42 s. [cit. 12. 4. 2015]. Dostupné z: www.ncbi.cz/category/6-metodiky-ucebni-materialy?download=40

[35] KOPECKÝ, Kamil. *Rizika internetové komunikace v teorii a praxi* [online]. Olomouc: Univerzita Palackého v Olomouci, 2013, 190 s. [cit. 2015-04-18]. ISBN 978-80-244-3595-4. Dostupné z: www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/47-rizika-internetove-komunikace-v-teorii-a-praxi-2013

[36] SZOTKOWSKI, René, Kamil KOPECKÝ a Veronika KREJČÍ. *Nebezpečí internetové komunikace IV* [online]. Olomouc: Univerzita Palackého v Olomouci, 2013, 177 s. [cit. 2015-04-10]. ISBN 978-80-244-3912-9. Dostupné z: www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/58-rizika-internetove-komunikace-iv-2012-2013

[37] MACHÁČKOVÁ, Hana, Alena ČERNÁ, Lenka DĚDKOVÁ, Anna ŠEVČÍKOVÁ a Eva BLAŽKOVÁ. *Online obtěžování a kyberšikana: Zpráva projektu „Copingové strategie kyberšikany u adolescentů* [online]. Brno: Fakulta sociálních studií Masarykovy univerzity, 2012, 18 s.[cit. 2015-04-10]. Dostupné

z: http://www.cyberpsychology.eu/team/storage/2012-Machackova-Online_obtezovani_a_kybersikana.pdf

[38] KREJČÍ, Veronika. *Kyberšikana: kybernetická šikana* [online]. Olomouc, 2010, 72 s. [cit. 2015-04-05]. ISBN 978-80-254-7791-5. Dostupné z: http://www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=14%3Akybersikana-sudie

[39] *Kyberšikana ve školním prostředí: Metodický materiál pro pedagogické pracovníky* [online]. Národní centrum bezpečnějšího internetu, 2012, 44 s.[cit. 2015-04-15]. Dostupné z: http://www.ncbi.cz/category/6-metodiky-ucebni-materialy?download=38

[40] ECKERTOVÁ, Lenka a Daniel DOČEKAL. *Bezpečnost dětí na Internetu: rádce zodpovědného rodiče*. Brno: Computer Press, 2013, 224 s. ISBN 978-802-5138-045.

[41] *Metodické doporučení k primární prevenci rizikového chování u dětí a mládeže* [online]. 2010 [cit. 2015-04-29]. Dokument MŠMT č.j.: 21291/2010-28. Dostupné z: www.msmt.cz/uploads/Priloha_7_Kybersikana.doc

[42] KOPECKÝ, Kamil a Veronika KREJČÍ. *Rizika virtuální komunikace: příručka pro učitele a rodiče* [online]. Olomouc: Net University, 2010 [cit. 2015-04-29]. ISBN 978-80-254-7866-O. Dostupné z: www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=10%3Abrozura

[43] *Kybergrooming a kyberstalking: Metodický materiál pro pedagogické pracovníky* [online]. Národní centrum bezpečnějšího internetu, 2012, 34 s. [cit. 2015-04-29]. Dostupné z: www.ncbi.cz/category/6-metodiky-ucebni-materialy ?download=37

[44] KOPECKÝ, Kamil. *Kybergrooming: nebezpečí kyberprostoru* [online]. Olomouc: Net University, 2010, 16 s.[cit. 2015-04-29]. ISBN 978-80-254-7573-7. Dostupné z: www.e-nebezpeci.cz/index.php/ke-stazeni/materialy-pro-studium-studie-atd?download=5:kybergrooming-studie

[45] *Děti a online rizika: sborník studií*. Praha: Sdružení Linka bezpečí, 2012, 178 s. ISBN 978-80-904920-3-5. Dostupné z: http://old.linkabezpeci.cz/data/articles/down_738.pdf

[46] Jak se závislost na internetu definuje?. *Online adiktologická poradna* [online]. 28. 11. 2010 [cit. 2015-04-29]. Dostupné z: http://poradna.adiktologie.cz/article/zavislost-na-internetu/jak-se-zavislost-na-internetu-definuje/

[47] KOPECKÝ, Kamil. Úvod do problematiky netolismu. *Projekt E-bezpečí* [online]. 17. 10. 2011 [cit. 2015-04-29]. Dostupné z: http://www.e-bezpeci.cz/index.php/temata/dali-rizika/331%E2%80%93uvod-do-problematiky-netolismu

[48] Co je to phishing. *Hoax* [online]. © 2000-2015 [cit. 2015-04-29]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing

[49] Co je to hoax. *Hoax* [online]. © 2000-2015 [cit. 2015-04-29]. Dostupné z: http://www.hoax.cz/hoax/co-je-to-hoax

[50] Rady pro bezpečné používání sociálních sítí. *Bezpečný internet: Rady pro bezpečnost na internetu* [online]. [2012] [cit. 2015-04-29]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/socialni-site/rady.aspx

[51] *Projekt E-bezpečí* [online]. Centrum prevence rizikové virtuální komunikace Pedagogické fakulty Univerzity Palackého v Olomouci, © 2008 - 2015 [cit. 2015-04-29]. Dostupné z: http://e-bezpeci.cz/

[52] *Poradna E-bezepčí: pro oblast rizikového chování na internetu* [online]. Centrum prevence rizikové virtuální komunikace PdF UP Olomouc, 2008-2014 [cit. 2015-04-29]. Dostupné z: http://poradna.e-bezpeci.cz/

[53] *Úvodní strana: pomoc-online_cz* [online]. [2007] [cit. 2015-04-29]. Dostupné z: http://www.pomoc-online.cz/

[54] Formulář pro hlášení závadového obsahu a aktivit v síti internet. *Úvodní strana: Policie České republiky* [online]. © 2015 [cit. 2015-04-29]. Dostupné z: http://aplikace.policie.cz/hotline/

[55] *Bezpečný internet: Rady pro bezpečnost na internetu* [online]. [2012] [cit. 2015-04-29]. Dostupné z: http://www.bezpecnyinternet.cz

Seznam obrázků

Seznam grafů

Seznam příloh

Příloha č. 1 – Dotazník pro žáky středních škol

Vážení žáci středních škol,

jsem studentkou posledního ročníku Přírodovědecké fakulty Univerzity Hradec Králové. Tento dotazník je součástí mé diplomové práce a klade si za cíl zjistit, jaké sociální sítě žáci středních škol nejčastěji používají a zdali se při jejich používání nesetkali s negativní zkušeností.

Děkuji za vyplnění Bc. Markéta Marková

1. Jakého jsi pohlaví?
   - ☐ žena
   - ☐ muž

2. Jaký typ střední školy studuješ?
   - ☐ Gymnázium
   - ☐ Střední odborná škola
   - ☐ Střední odborné učiliště

3. V jakém ročníku studuješ?
   - ☐ 1.
   - ☐ 2.
   - ☐ 3.
   - ☐ 4.

4. Používáš sociální sítě?
   - ☐ Ano
   - ☐ Ne */pokračuj otázkou č. 16*

5. Jaké sociální sítě používáš? (Možno zvolit více odpovědí.)
   - ☐ Facebook
   - ☐ Google+
   - ☐ Instagram
   - ☐ Twitter

☐ YouTube

☐ Jiné. Jaké?

_____

6. Kolik času denně strávíš na sociálních sítích?

   ☐ 4 hodiny a více

   ☐ 3 hodiny

   ☐ 2 hodiny

   ☐ 1 hodina

   ☐ Méně než 1 hodinu

   ☐ Nenavštěvuji sociální sítě každý den

7. Jaké služby na sociálních sítích využíváš? (Možno zvolit více odpovědí.)

   ☐ Komunikace s přáteli

   ☐ Komunikace s novými lidmi (seznamování)

   ☐ Sdílení fotografií a videí

   ☐ Získávání informací (např. o aktuálním dění)

   ☐ Hraní her

   ☐ Jiné. Jaké?

   _____

8. Znáš všechny své přátele (odběratele) na sociálních sítích i z reálného života?

   ☐ Ano

   ☐ Ne

9. Setkal/a ses někdy osobně s člověkem, se kterým ses seznámil/a na sociální síti?

   ☐ Ano

   ☐ Ne

10. Umíš na sociálních sítích, které využíváš upravit nastavení soukromí?

    ☐ Ano, upravuji si nastavení soukromí

☐ Ano, ale nevyužívám tuto možnost – můj profil je veřejný

☐ Ne, nevím jak změnit nastavení soukromí

11. Co zveřejňuješ na sociálních sítích? (Možno vybrat více odpovědí.)

☐ Pravé jméno a příjmení

☐ Datum narození

☐ Adresu

☐ Telefonní číslo nebo e-mail

☐ Název školy, kterou studuješ

☐ Lokality, ve kterých se pravidelně pohybuješ

☐ Fotografie a videa, na kterých jsi ty

☐ Fotografie a videa dalších lidí (např. přátel, rodiny, …)

☐ Akce a události, kterých se plánuješ zúčastnit

☐ Jiné údaje. Jaké?

_____

☐ Nezveřejňuji na sociálních sítích žádné osobní údaje

12. Zná někdo další přihlašovací údaje k tvým profilům na sociálních sítích?

☐ Ano

☐ Ne

13. Naboural se v minulosti někdo do tvého profilu na sociální síti?

☐ Ano

☐ Ne

14. Přihlašuješ se na sociální sítě i ve škole?

☐ Ano

☐ Ne */pokračuj otázkou č. 16*

15. Z jakého zařízení se ve škole na sociální sítě přihlašuješ?

☐ Ze školního zařízení (počítače, notebooku,…)

☐ Z vlastního zařízení (telefonu, tabletu, notebooku,…)

☐ Ze školního i vlastního zařízení

16. Jsou podle tvého názoru s užíváním sociálních sítí spojená nějaká rizika?
    - ☐ Určitě ano
    - ☐ Spíše ano
    - ☐ Spíše ne *(pokračuj otázkou č. 18)*
    - ☐ Určitě ne *(pokračuj otázkou č. 18)*
    - ☐ Nevím *(pokračuj otázkou č. 18)*

17. Jaká rizika jsou s užíváním sociálních sítí spojená?

    _____

    _____

18. Mluvili jste při hodinách informatiky nebo jiného předmětu o sociálních sítích a zabývali jste se i možnými riziky spojenými s jejich užíváním?
    - ☐ Ano, mluvili jsme o sociálních sítích i o možných rizicích
    - ☐ Ano, mluvili jsme o sociálních sítích, ale možnými riziky jsme se nezabývali
    - ☐ Ne, tomuto tématu jsme se nevěnovali

19. Víš, co znamená pojem kyberšikana?
    - ☐ Ano
    - ☐ Spíše ano
    - ☐ Spíše ne *(pokračuj otázkou č. 22)*
    - ☐ Ne *(pokračuj otázkou č. 22)*

20. Setkal/a ses někdy s kyberšikanou na sociálních sítích?
    - ☐ Ano, osobně
    - ☐ Ano, zprostředkovaně (rodina, kamarád,…)
    - ☐ Ne *(pokračuj otázkou č. 22)*

21. Zapojila se do řešení tohoto případu škola? (zastoupená např. učitelem, výchovným poradcem,…)
    - ☐ Ano, aktivně řešila tento případ
    - ☐ Ano, pomáhala řešit tento případ

☐ Ne, škola se do řešení tohoto případu nezapojovala

☐ Nevím

22. Jak jsi kyberšikanu řešil/a? Případně jak bys postupoval/a, kdyby ses s kyberšikanou osobně setkal/a? (Možno vybrat více odpovědí.)

☐ Ignorovat útočníka

☐ Kontaktovat útočníka a vysvětlit si to s ním

☐ Povědět o útoku rodičům

☐ Povědět o útoku učiteli

☐ Povědět o útoku kamarádovi

☐ Jinak. Jak?

_____