Sociální sítě a jejich bezpečnost z pohledu mladistvých

Veronika Jordánová, DiS.

Bakalářská práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Veronika Jordánová, DiS.**
Osobní číslo:	**A16019**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Informační technologie v administrativě**
Forma studia:	**prezenční**
Téma práce:	**Sociální sítě a jejich bezpečnost z pohledu mladistvých**
Téma anglicky:	**Security of Social Networks from the Point of Adolescents**

Zásady pro vypracování:

1. **Vysvětlete co jsou sociální sítě a jaký je jejich účel.**
2. **Popište hrozby na sociálních sítích.**
3. **Věnujte se i pojmům jako je kyberšikana a stalking v souvislosti se sociálními sítěmi.**
4. **Vytvořte dotazníkové šetření.**
5. **Proveďte průzkum sociálních sítí (co lidé sdílí veřejně).**
6. **Vyhodnoťte dotazníkové šetření s průzkumem sociálních sítí.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BLINKA, Lukáš. Online závislosti: jednání jako droga? : online hry, sex a sociální sítě: diagnostika závislosti na internetu: prevence a léčba. Vydání 1. Praha: Grada, 2015, 198 s. Psyché. ISBN 978-80-210-7975-5.**
2. **BOYD, Danah. Je to složitější: sociální život teenagerů na sociálních sítích. Vydání první. Přeložil Lukáš NOVÁK. Praha: Akropolis, 2017, 301 s. ISBN 978-80-7470-165-8.**
3. **HOLLÁ, Katarína. Sexting a kyberšikana. Vydanie: prvé. Bratislava: Iris, 2016. 165 stran.**
4. **KOŽÍŠEK, Martin a Václav PÍSECKÝ. Bezpečně n@ internetu: průvodce chováním ve světě online. Praha: Grada Publishing, 2016, 175 s. ISBN 978-80-247-5595-3.**
5. **PETROWSKI, Thorsten. Bezpečí na internetu: pro všechny. Liberec: Dialog, 2014, 243 s. Tajemství. ISBN 978-80-7424-066-9.**
6. **ŠEVČÍKOVÁ, Anna. Děti a dospívající online: vybraná rizika používání internetu. Praha: Grada, 2014, 183 s. Psyché. ISBN 978-80-210-7527-6. Dostupné také z: http://www.grada.cz/deti-a-dospivajici-online_7905/kniha/katalog/.**

Vedoucí bakalářské práce: **Ing. Lukáš Králík**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **30. listopadu 2018**

Termín odevzdání bakalářské práce: **15. května 2019**

Ve Zlíně dne 7. prosince 2018

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. Ing. Martin Sysel, Ph.D.
garant oboru

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 15. 05. 2019

Veronika Jordánová, DiS, v.r.
podpis diplomanta

ABSTRAKT

Cílem bakalářské práce je zjistit jak vnímají sociální sítě a jejich bezpečnost mladiství (ve věku 10 – 18 let) a také co na sociálních sítích sdílí veřejně. V teoretické části práce jsou rozebrány pojmy jako sociální sítě, historie, a pojmy s tím spojené. V praktické části je vytvořen dotazník zaměřený na sociální sítě, jejich bezpečnost z pohledu dětí základní školy a mladistvých. V praktické části se také nachází srovnání výsledků dotazníku s průzkumem sociálních sítí, který byl stanoven na základě výsledků z dotazníkové šetření.

Klíčová slova: sociální sítě, bezpečnost, mladiství, dotazník

ABSTRACT

The aim of this bachelor thesis is to get acquainted with how the social networks and their safety will perceive adolescents (aged 10 - 18 years). In the theoretical parts are given terms such as social networks, history and concepts In the practical part is created a questionnaire focused on social networks, their safety from the perspective of primary school children and adolescents In the practical part there is also a comparison of the results of the questionnaire with the survey of social networks, which was based on the results of the questionnaire survey

Keywords: social network, security, adolescents, questionnaire

Poděkování:

Děkuji svému vedoucímu Ing. Lukáši Králíkovi za cenné rady a vedení po celou dobu zpracování bakalářské práce. Dále bych chtěla poděkovat všem, kteří se zapojili do dotazníkového šetření, které je nedílnou součástí této bakalářské práce.

„*Svoboda jednoho končí tam, kde svoboda druhého začíná.“* John Stuart Mill.

OBSAH

ÚVOD

Sociální sítě jsou nedílnou součástí dnešního světa, především pro generaci Z, případně generaci Y (mileniálové). Tyto dvě generace v podstatě vyrůstaly za přítomnosti sociálních sítí a internetu celkově. Bakalářská práce se soustředí především na bezpečnost těchto sítích, a jak tuto bezpečnost vnímá právě generace Z. V dnešní době si asi nikdo nedokáže představit život bez moderních technologií (chytré telefony, počítače, neomezený přístup na internet téměř kdekoliv a kdykoliv).

Pro starší generace může být tento jev až nepochopitelný, proč má někdo potřebu sdílet se světem své pocity, myšlenky, fotografie sebe, své rodiny, své osobní informace. Pro generace, které v tomto vyrůstaly už od mala je však naprosto normální otevřeně sdílet své myšlenky, někteří si tímto dokáží vydělat dost peněz, aniž by museli chodit denně do „normální“ práce.

Nejdříve byly sociální sítě spíše lokální a až nástupem nejznámější sociální sítě Facebook.com se rozšířily celosvětově. Díky tomuto není problém být v kontaktu de facto nepřetržitě s kýmkoliv, kdekoliv na světě, v jakémkoliv časovém pásmu. Můžeme mít kamaráda z Afriky, kamarádku z USA, komunikovat s rodinou na druhé straně zeměkoule. Je však vždy na druhé straně opravdu ten člověk, který si myslíme? Opravdu komunikujeme s kamarádkou, která je stejně stará jako my a má podobné zájmy? I těmito otázkami se bakalářská práce zabývá. Sociální sítě totiž nejsou jen o reálných přátelích či kamarádech. Na druhé straně může klidně sedět naprostý opak stejně staré kamarádky, ale například daleko starší muž či žena, kteří se za stejně starou kamarádku pouze vydávají.

Sociální sítě dnes používá drtivá většina lidí, i když někteří pouze jen pro komunikaci s ostatními – například Messenger od sociální sítě Facebook, ten totiž může používat i člověk, který nevlastní profil na Facebooku.

Kvůli sociálním sítím je všude tolik informací, kterým téměř nelze uniknout. Dokáží je lidé filtrovat tak, aby si uměli z každé informace odnést to, co je relevantní? Dokáží to mladiství? Opravdu je nutné být neustále s někým v kontaktu? Jsou tyto sítě vůbec bezpečné? I těmito otázkami se bude bakalářská práce zabývat.

I. TEORETICKÁ ČÁST

1 SOCIÁLNÍ SÍTĚ – CO JE TO SOCIÁLNÍ SÍŤ

Sociální síť je služba na internetu, která svým členům umožňuje vytvářet profily (veřejné, soukromé, firemní) a na těchto profilech nabízí prostor pro sdílení obsahu (fotografie, videa, pocity, myšlenky). Obsah na sociálních sítích je z většiny tvořen jejími uživateli. Pomocí sdílení příspěvků, diskusních fór můžou vytvářet obsah a komunikovat. Oblíbeným druhem jsou diskusní fóra na dané téma (koníčky, politika, vaření, sex,…), kde si lidé navzájem vyměňují názory, zkušenosti a rady. [1]

Největší boom zažily sociální sítě v období „neomezeného internetu“. Díky tomu měli uživatelé jednodušší a daleko levnější přístup na sociální sítě. Do té doby byl mobilní internet velmi drahý a lidí tudíž využívali sociální sítě především z domova nebo v práci. Jelikož měli najednou internet v mobilních zařízeních a sociální sítě okamžitě přístupné, tento trend se velmi rychle rozmohl. Největší celosvětovou sociální sítí je Facebook. [1]

1.1 Historie sociálních sítí

Výraz sociální síť jako první použil J. A. Barnes, profesor londýnské univerzity, v roce 1954 při studování sociálních vazeb mezi rybáři v Norsku. Jeho závěr byl, že celou společnost můžeme definovat jako množinu bodů, kde jsou některé propojeny vzájemnými vztahy. Tato množina pak utváří celkovou síť vztahů, neboli sociální síť. [2]

K sociální síti jak ji známe dnes, bylo však ještě hodně daleko. Až za dalších 24 let (v roce 1978) vznikl systém Bulletin Board System (BBS). Tento systém umožňoval jako vůbec první posílání textových zpráv. Systém byl však velmi pomalý, vždy mohl být přihlášený jen jeden uživatel. Pokud tedy lidé chtěli takhle chatovat, mohla se jim tato výměna zpráv protáhnout klidně i na celé hodiny. Tento problém vyřešil finský student Jarkko Oikarinen, který v roce 1988 vytvořil první Internet Relay Chat (IRC) jménem OuluBox. Právě tato aplikace dala vzniknout základu všem dnešním chatovacím aplikacím a serverům. Byla totiž první, která umožňovala komunikovat s ostatními v reálném čase. [2]

V roce 1997 vznikla první sociální síť, která umožnila vytvořit si vlastní okruh přátel, prohlížet jejich profily a vzájemně komunikovat. Ne, ještě to nebyl Facebook, ale sociální síť jménem SixDegrees.com. Bohužel, i přes to, že SixDegrees.com používalo přes milion uživatelů a firma zaměstnávala víc než 100 lidí, v roce 2001 kvůli finančním problémům musela skončit. Zakladatel projektu SixDegrees.com Andrew Weinreich po čase prohlásil, že SixDegrees předběhla svou dobu. [2]

Známější sociální sítí je MySpace vytvořena lidmi, kteří pracovali na první seznamce Freindsteru. MySpace kromě vytváření profilů a propojování se s přáteli nabídl i vlastní chatovací službu - instant messenger). MySpace nepodporoval pouze založení profilu, ale profil si mohl uživatel v grafickém rozhraní upravit, přidat fotografie a později i propojit s hudební scénou. V roce 2006 měl MySpace přes 100 milionů registrovaných uživatelů. Bohužel, slavné dny MySpace se blížily konci od roku 2004, kdy student z Harvadské Univerzity Mark Zuckerberg představil svoji sociální síť pro studenty Harvardu jménem TheFacebook.com. [2]

1.2 Pravdivost údajů na sociálních sítích

Na sociální sítě může napsat každý uživatel, co uzná za vhodné. Může také využívat přezdívky a nemusí užívat pouze své pravé jméno. Provozovatelé těchto sociálních sítí nemají moc prvků, jak správnost těchto údajů ověřit. Vystupovat pod svým pravým jménem nás dělá dohledatelnými. Mohou nás najít naši přátelé, bývalí spolužáci, kolegové z práce ale i naprosto cizí lidé. [1]

Je však důležité si uvědomit, že i když budou lidé na sociálních sítích vystupovat pod přezdívkou, neznamená to, že je v případě porušení zákonů či etických norem nelze dohledat. Navíc ani všechny sdílené fotografie nemusí odpovídat realitě. Na sociálních sítích chtějí lidé vystupovat lépe než v reálném světě. Fotografie si upravují, nastavují kompozici, jen velmi málo sdílených fotografií odpovídá skutečnosti. [1]

1.3 Facebook

V roce 2004 založil mladý student Mark Zuckerberg sociální síť TheFacebook.com pro studenty Harvardu, aby zde mohli komunikovat a sdílet informace. TheFacebook.com se rychle rozšířil do celého světa a nyní jej využívá více než dvě miliardy lidí. [2]

Název The Facebook vznikl nejspíš podle letáků, které se rozdávaly na Harvardské univerzitě studentům, kteří nastoupili do prvních ročníků, takzvané „facebooks". Letáky byly rozdávány proto, aby se studenti lépe a rychleji seznámili mezi sebou. A právě toto inspirovalo zakladatele k založení sociální sítě TheFacebook.com. S vytvořením sociální sítě pomáhali další lidé - spolubylící Marka Zuckerberga, Kirkland – Andrew McCollum, Dustin Moskovitz, Chris Hughesem a Eduard Saverin. [4]

O založení Facebooku byl v roce 2010 natočen i film The Social Network, kde se popisuje založení této největší, revoluční sociální sítě a všechny problémy okolo. Ve filmu se ukazuje, co všechno k založení Facebooku vedlo, popisuje také neshody s bratry Winklevossovými. [3]

(Zajímavostí ohledně Facebooku je také výběr modré barvy, důvod je takový, že zakladatel Mark Zuckerberg trpí červeno - zelenou barvoslepostí a proto je Facebook modrý. Modrou barvu totiž vidí nejlépe.) Pro založení účtu na sociální síti Facebook je potřeba mít minimálně 13 let (z důvodu platných zákonů Spojených států amerických) a e-mailovou adresu. [4]

Obrázek 1: logo Facebook.com [13]

1.4 Instagram

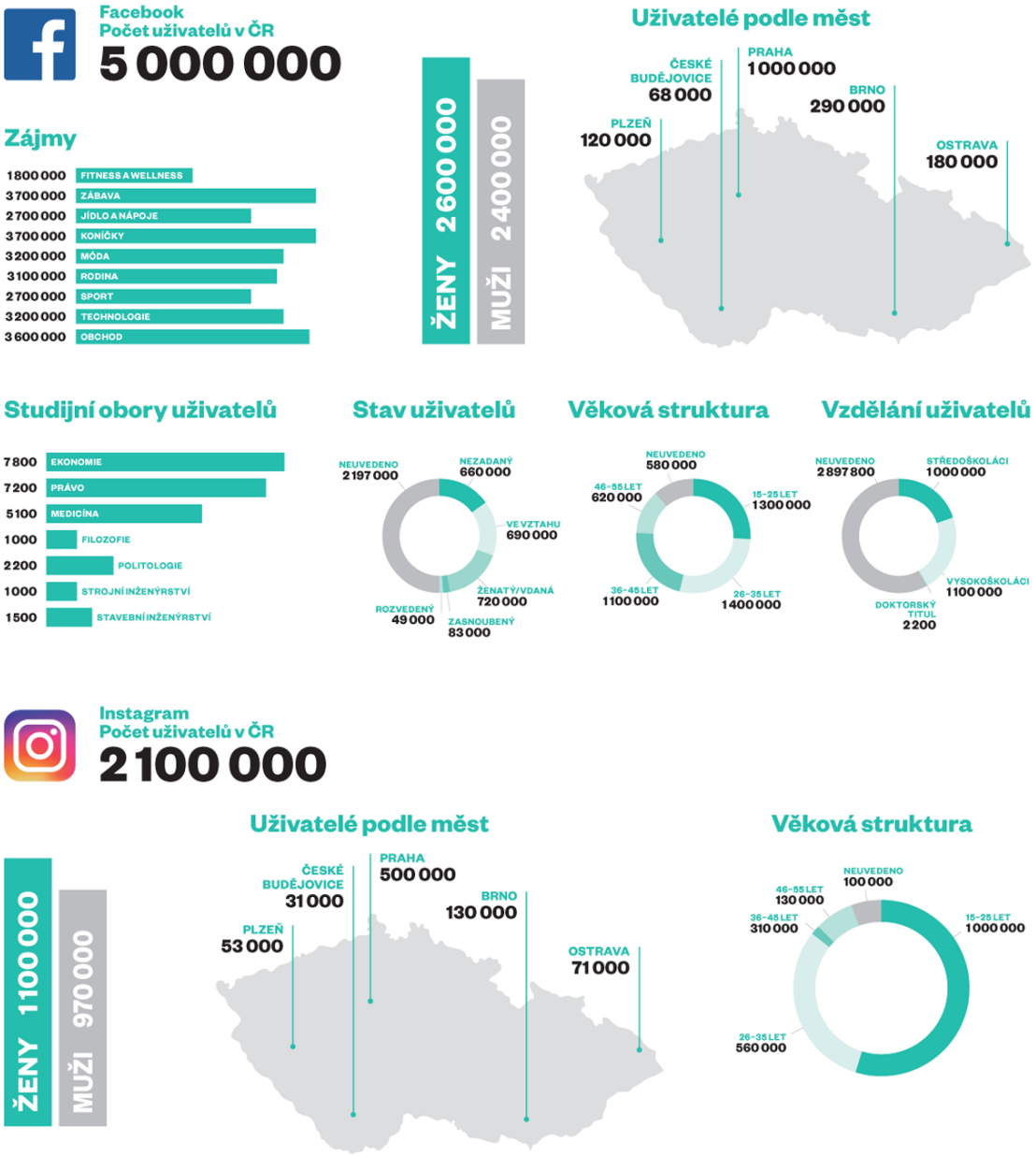
Instagram je nejznámější mobilní aplikací pro sdílení fotek a krátkých videí, který vznikl v roce 2010. Toto se ještě posílilo v momentě, kdy v roce 2012 koupil Instagram Facebook za jednu miliardu dolarů. Instagram vznikl až po větších sociálních sítích - Twitter, Facebook, Flickr, Tumblr a podobné platformy pro sdílení fotografií. Oficiální motto Instagramu zní „rychlé sdílení fotografií", což vystihuje hlavní myšlenku celé této platformy - vyfotit, označit # (hashtag, rychlý jednoslovný popisek, heslo). Pomocí hashtagů lze následně příspěvek (fotografii) jednoduše vyhledat. [2]

Obrázek 2: logo Instagram [14]

Založení účtu na Instagramu je rychlejší a jednodušší, obzvláště pokud nový uživatel přichází a má účet na Facebooku. V tomto případě vybere pouze fotografii, kterou chce použít na svém profilu, zvolí si uživatelské jméno, případně pár vět o sobě. Nového uživatele pak Instagram upozorní na osoby se kterým je v kontaktu na Facebooku a ty mu pak doporučí pro sledování (anglicky follow). Pokud se uživatelé navzájem sledují (followers) vidí všechny své příspěvky. [2]

Každý uživatel si určuje sám, koho bude sledovat, osoby či účty (firemní, reklamní účty) a tím si vytváří vlastní obsah své sítě. Publikovat své fotografie na této sociální síti je opět velmi jednoduché. Pomocí chytrého telefonu pořídí uživatel fotografii, kterou následně může pomocí přednastavených filtrů upravit. Filtry změní barevnost, upraví kontrast, jas, stíny případně přidají rámeček nebo fotografii oříznou. Nakonec uživatel přidá k fotografii popisek za pomocí užití symbolu # a přidáním hesla (#MeToo - přiznání žen, které byly někdy sexuálně obtěžovány, převážně známými osobnostmi). Pokud uživatel toto heslo použije u svého příspěvku a má veřejný profil, kdokoli podle něj může příspěvek dohledat. Všechny příspěvky s #MeToo se budou sdružovat pod tento hashtag. Velmi to zjednodušuje následné vyhledávání. [2]

Navíc Instagram nabízí i tzv. sdílení příběhů (InstaStories), kde uživatel nahraje fotografii či krátké video (maximálně 15 sekund), které po 24 hodinách zmizí. Důležité je dodat, že nic co uživatel sdílí na sociální síti, nikdy úplně nezmizí nebo se nesmaže. [2]



Obrázek 3: počet uživatelů na Instagramu a Facebooku [21]

Na obrázku 3 jsou znázorněny statistiky počtu uživatelů, jejich věku a místa bydliště na Instagramu a Facebooku z časopisu Marketing a Media, kde se několik článků věnuje sociálním sítím. [21]

1.5 Twitter

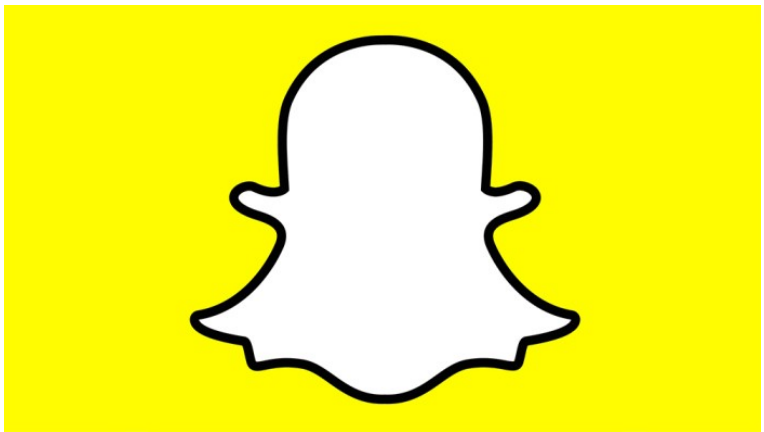
V roce 2006 byla založena další sociální síť a to Twitter a první příspěvek od zakladatele zněl: „just setting up my twttr.” v překladu „právě si nastavuji svůj Twitter.” Kouzlo této sociální sítě je právě v rychlosti a jednoduchosti sdílených příspěvku, tzv.

„tweetů". Dnes už mohou uživatelé sdílet i fotografie či videa, původní myšlenkou bylo psaní rychlých, krátkých textů. Původně měl jeden tweet maximálně 140 znaků, což Twitter nedávno navýšil na 280 znaků. Při založení účtu na Twitteru není nutné zadávat skutečné jméno či fotografii, jak je to při založení Facebooku. Twitter má přes 330 milionů aktivních uživatelů. [2]

Obrázek 4: logo Twitter [15]

1.6 Snapchat

Sociální síť Snapchat je specifická svým konceptem. Podstata této sociální sítě je v nahrávání krátkých videí či fotografií (tzv. „snapy"), které pak uživatel rozesílá mezi své kamarády na této sociální síti. Uživatel může poslat „snap" pouze jednomu, výběru přátel nebo všem, „snap" se zobrazí pouze na určenou dobu (například 10 - 20 sekund), po uplynutí této doby fotografie či video zmizí. [2]



Obrázek 5: logo Snapchat [16]

1.7 Youtube

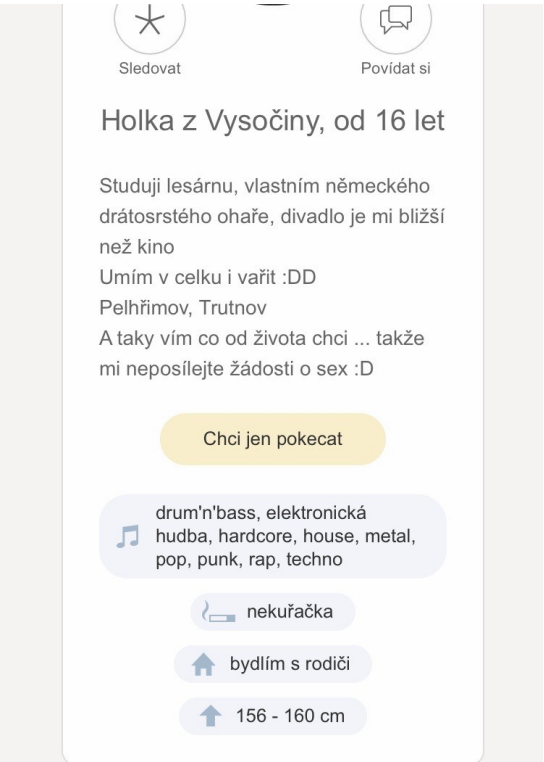
Další sociální sítí je server Youtube.com, kam uživatelé nahrávají svá domácí videa na různá témata. Nejčastější témata jsou životní styl, kosmetika, móda a herní videa. Herní videa jsou videa, kde jsou natočené postupy z hraní her, odběratelé se dívají na to, jak kterou hru daný Youtuber hraje. Youtuber - člověk, který pravidelně přidává videa na určité téma a následně si tímto vydělává peníze. [5]

Když v září roku 2018 oznámil největší český Youtuber Jiří Král, který má na Youtube více než jeden milion odběratelů, že se svojí tvorbou na Youtube končí, různá média se začala předhánět v prorokování konce této sociální sítě v České republice. V dnešní době se spousta umělců z Youtube přesouvá i na jiné sítě, kde mohou také předávat informace, většinou spíše mladším generacím (generace Y a Z). [5]

Obrázek 6: logo Youtube.com [17]

1.8 Lidé.cz

Lidé.cz je čistě česká sociální síť, kterou provozuje portál Seznam.cz. Podstatou sítě Lidé.cz je tvorba profilů, kam mohou uživatelé nahrávat fotky, videa a prostřednictvím této sítě komunikovat s ostatními. Nejoblíbenější jsou diskusní fóra na různá témata (geografické chaty, různé koníčky či zájmy). Lze se zde také zaregistrovat do seznamky, která nabízí desítky tisíc inzerátů, které jsou rozděleny do různých kategorií, seznamku lze propojit také se svým již vytvořeným profilem. Profil na Lidé.cz si můžou založit osoby od 16 let. Prohlížet profily lze i bez registrace či přihlášení. [19]



Obrázek 7: ukázka profilu z webu
Lidé.cz [22]

1.9 Badoo

Badoo je sociální síť, která je přímo určena pro seznamování s lidmi ze svého okolí, ale také z celého světa. Princip Badoo funguje tak, že rozesílá e-maily kontaktům již registrovaných uživatelů. Tohle vše bohužel činí bez svolení uživatelů. Na této seznamce je povolena registrace osobám starším 18 let. [20]

1.10 Influencer (marketing)

Influencer je člověk, který tvoří obsah na sociálních sítích, v dnešní době má především Intagram velký vliv na své sledující. Tohoto vlivu začaly využívat různé firmy k propagaci svých výrobků, kdy je tato reklama pro ně daleko levnější než například spot v televizi a s daleko větším dopadem. Influencer marketing využívá především toho, že konkrétního influencera sleduje určitá skupina lidí, tím pádem je reklama přesně cílená a také důvěryhodná. Sledující influencerům věří, že daná věc je opravdu taková, jakou ji popisují. Což nemusí být vždy pravda, nyní je trh přesycen jak influencery, kteří nad tímto druhem placených spoluprací nepřemýšlí a takzvaně berou všechno za různých podmínek,

tak i opačnými případy, kdy si každý pečlivě zvolí, jakou značku chce na trhu reprezentovat. [5]

Ovšem i zde se objevují problémy, například když influencer reklamu neoznačí. Ve všech ostatních mediích je ze zákona dáno, že každá reklama musí být označena. Na Instagramu by se mělo využívat možnosti přidat označení „Placené partnerství", případně přidat do popisku minimálně hashtag #ad, #sponzored, #sponzorováno, #reklama a tak podobně. Hlavně z důvodu, aby si sledující mohl sám rozhodnout, zda věří, že je to opravdu tak skvělé jak Infuencer prezentuje nebo se jedná o reklamu, kterou má zaplacenou a nemusí tedy vše v příspěvku být pravda. [5]

Chování generací X, Y, Z na internetu se liší hlavně v užívaných sociálních sítích. Podle agentury Ipsos, která vytvořila studii o Generaci Z, generace X (39 - 52 let) komunikuje převážně přes e-mail a postupně objevuje sociální sítě či diskusní fóra, 14 % sleduje Youbery, 11 % sleduje instagramisty a 11 % se inspiruje od bloggerů.

Mileniálové, mladší generace Y (24 - 38 let), nejvíce komunikují přes Facebook nebo Whatsapp, 20 % sleduje youtubery, 23 % sleduje instagramisty a 15 % se inspiruje od bloggerů.

Nejmladší generace Z (4 - 23 let), jinak také smart generace, se narodila do světa sociálních sítí. Generace Z si lépe dokáže chránit soukromí na internetu, na Facebooku spíše sledují co se děje než aby tvořili vlastní obsah. Využívají mnoho komunikačních platforem, sledují influencery a jako jediná generace přiznávají, že se při nákupu nechají ovlivnit doporučením na sociálních sítích, 54 % sleduje youtubery, 44 % sleduje instagramisty a 32 % se inspiruje od bloggerů. [5]

2 HROZBY NA SOCIÁLNÍCH SÍTÍCH

Potencionální riziko ztráty osobních údajů se zvyšuje s množstvím aktivit na internetu. Nikdo by neměl své osobní údaje lehkomyslně sdělovat a poskytovat ostatním. Pokud nastavení soukromí účtu je jen základní, mohou tyto údaje uniknout například i z Facebooku a jiných sociálních sítí. V tomto případě pak může zjistit každý uživatel osobní údaje z nezabezpečeného účtu. [6]

Pokud se jedná o ochranu dětí na internetu, měli by rodiče věnovat velkou pozornost tomu, co jejich děti sdílí veřejně, případně posílají svým kamarádům. Za účty na sociálních sítích se mohou skrývat nejenom kamarádi či známí, ale také úplně cizí osoby, které navíc mohou mít i jiné úmysly než si jen s dětmi povídat. Mohou zde například pedofilové hledat uspokojení svých tužeb případně další lidé s různými problémy. [6]

Doporučení pro rodiče dětí, jak se na sociálních sítích chovat:

- nikdy neprozrazovat kompletní informace o své osobě, především adresu, školu, telefonní číslo aj.,
- neposílat žádné své fotografie, případně nastavit soukromí na příspěvcích, aby je mohli vidět opravdu jen přátelé,
- poučit děti o tom, že ne každý může být tím, za koho se na sociální síti vydává, například Jana z Brna, která uvádí, že je jí 13 let, může ve skutečnosti být klidně Jan z Prahy, kterému je 31 let a nemá zrovna dobré úmysly,
- nikdy se s nikým neznámým nedomlouvat na osobní schůzce.

Toto jsou extrémní příklady, s čím se mohou děti na internetu setkat, ale nejsou ojedinělé. [6]

2.1 Popis nejčastějších hrozeb

Největším problém je bezesporu únik dat ze sociálních sítí a jejich následné zneužití. K tomuto může dojít například špatným zvolením hesla. Bezpečnost hesel je velkým problémem. Každý uživatel má nespočet účtů a k nim přihlašovacích údajů, od bankovní karty až po e-mailové účty, sociální sítě, účty na e-shopech a jiných serverech. Při větším množství hesel a různých věcí, které je potřeba si pamatovat, má člověk tendence si určité věci zjednodušovat. A to platí i při tvorbě či vymýšlení nových hesel. [6]

2.1.1 Phishing

Phishing je složenina z anglických slov „phreaking" a „fishing", volně přeloženo to znamená nabourávání se například do telefonů a lovit oběti. Jedná se o zákeřnou formu internetových podvodů. Phishing je využíván pro získávání citlivých údajů od obětí. Základní myšlenkou je rozesílání zpráv, které se na první pohled zdají jako reálné - například od banky, ze sociální sítě nebo internetového obchodu. Tyto e-maily se pod různými záminkami snaží vylákat přístupové údaje, přihlašovací jméno či heslo, PIN ke kartám nebo údaje do internetového bankovnictví. [6]

Hacker vytvoří autentickou webovou stránku, která je ovšem falešná, většinou nelze rozeznat od originálu. Následně rozešlou e-maily s odkazem na tuto stránku - například sociální sítě a požadavkem na přihlášení. V momentě, kdy se uživatel na této podvodné stránce přihlásí svými údaji, získává hacker volný přístup k účtům, osobním údajům a jiným informacím. [6]

2.1.2 Vishnig

Vishing – spojení slov voice a phishing, je podvodná technika, která má pomocí manipulace vytáhnout z obětí jejich přístupové údaje k různým účtům. Toto probíhá přes telefon. Většina má již poměrně dobře zabezpečený e-mail proti spam e-mailům či různým hoaxům. Jednodušeji mohou podlehnout právě vishingu přes telefon, pokud je telefonát dobře připraven a promyšlen. V tomto případě je těžší rozeznat podvodných telefonát, jelikož útočník je velmi dobře připraven a většinou má další doplňující informace, které získal pomocí sociálních sítí. [12]

2.1.3 Malware

Škodlivé aplikace, programy, které jsou určeny pro vniknutí nebo zneužití systému, sítě v nejhorším případě ke zničení systému. Sociální sítě jsou ideálním prostředí pro šíření malware. Útoky mohou být různé, vždy záleží na záměru autora. [6]

Rozdělení malware:

- Backdoor - tyto programy usilují o přístup do počítačů. tzv. zadní vrátka. Nepovolané osoby získají při infikování počítače tímto druhem viru přístup ke všem souborům a programům.

- Červ - šíří se počítačem a infikuje všechny soubory, maže soubory z pevného disku, dokáže se šířit ne jenom v jednom počítači ale také na jiné počítače.
- Ransomware / Scareware - tyto viry pracují na principu výhružek a s jejich pomocí se z uživatelů snaží vylákat peníze.
- Spyware - prohledává nakažený počítač a zneužívá údaje, které nalezne (přístupové údaje, hesla, údaje o kreditních kartách, osobní informace).
- Trojský kůň - program, který se zdá užitečný, ve skutečnosti v sobě nese i další program - vir, který napadá počítač. [6]

2.1.4 Tvorba hesla

Thorsten Petrowski ve své knize Bezpečně na internetu pro všechny dělí lidi podle kreativity při vytváření hesel na:

- Naivkové - tento typ lidí se řídí heslem „Čím jednodušší, tím lepší". Nejoblíbenější hesla jsou typu – „heslo", „12345",
- Rodinné typy - hesla typu křestní jméno manželky, babičky, dětí,
- Sportovní fanoušci - oblíbené sportovní týmy (hokejové, fotbalové, basketbalové, atd…),
- Tradicionalisté - hesla odvozená z minulosti uživatele,
- Hračičkové – „chytřejší" druhy hesel, většinou s přidruženým číslem. [6]

Nejoblíbenějších deset hesel:

1. jména domácích mazlíčků
2. koníčky
3. rodné příjmení matky
4. den narození někoho z rodiny
5. vlastní narozeniny
6. jméno partnera
7. vlastní jméno
8. název oblíbeného sportovního klubu

9. oblíbená barva
10. název základní školy [6]

Chyby při tvorbě hesla jsou různé, někteří lidé zvolí heslo příliš jednoduché. Další zvolí velmi krátké heslo, což zmenšuje čas k prolomení hesla, každý další znak navíc prodlužuje čas potřebný k prolomení hesla. Někdo mění heslo každý týden, někdo naopak téměř vůbec, což je opět špatně zvolená strategie ochrany hesel a údajů. Problémem může být také ukládání hesel do nezašifrovaných souborů. Například Microsoft Word ukládá informace do dočasných souborů, z nichž může kdokoli získat informace, i přesto, že je soubor smazaný. Nejhorší variantou je ovšem použití stejných hesel v různých účtech. [6]

2.1.4.1 Vytvoření správného hesla

Pro vytvoření silného hesla je potřeba najít správnou kombinaci, pokud možno s užitím minimálně deseti znaků. V nejlepším případě by heslo nemělo dávat smysl a žádné konkrétní slovo. Vymyslet správné heslo a jedinečnou kombinaci není vždy úplně jednoduché, důležité je, aby heslo bylo dostatečně silné, musí však být zapamatovatelné. Dobrou pomůckou pro takovou tvorbu hesla je vymyslet větu, například vystihující záliby a z ní následně poskládat heslo. [6]

Například: „Oblíbené květiny jsou tulipány a růže.” Ze slov pak použít jednotlivá první písmena - OkJtAR. Přidáním zvláštních znaků a čísel dosáhneme velmi silného hesla - např. OkJtAR-_-9173. [6]

Ke každému účtu by mělo být unikátní heslo, nikdy nepoužívat stejné heslo pro více účtů. V tomto případě je jednodušší dostat se do ostatních účtů v případě uhádnutí nebo objevení jednoho hesla.

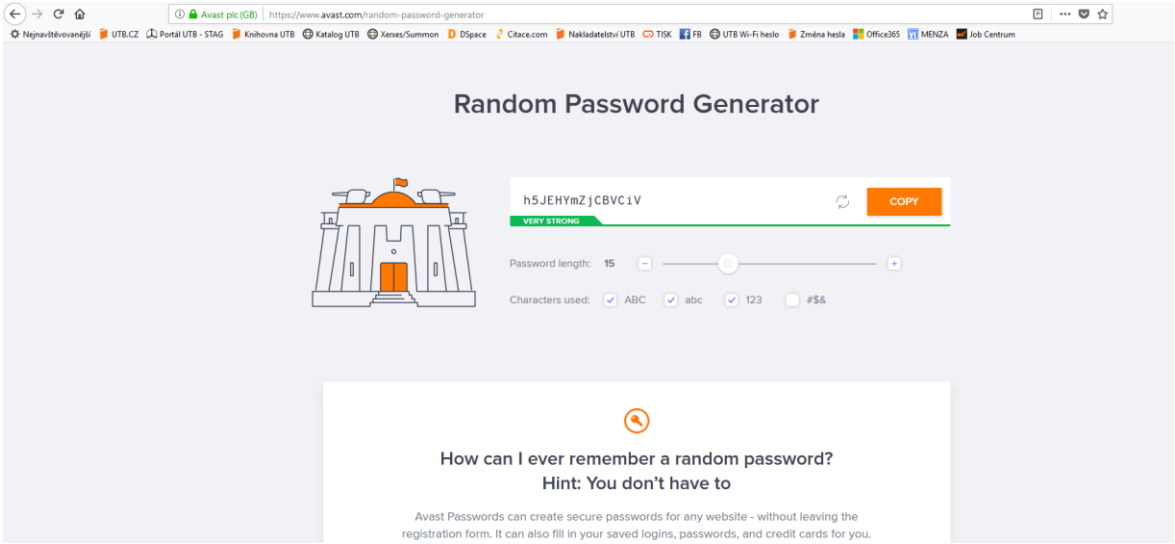
Zásady pro vytvoření hesla:

1. čím delší, tím lepší - minimum 12 znaků
2. použití velkých a malých písmen
3. použití speciálních znaků a čísel
4. častá změna. [10]

Použitím silného hesla ztížíme hackerům přístup k našim účtům. Druhy útoků, které se objevují nejčastěji:

- **útok hrubou silou** - útočník pomocí automatického software zkouší všechny možné kombinace znaků, dokud nenajde tu správnou kombinaci. Všechna hesla, která jsou kratší než 9 - 12 znaků jsou snáze prolomitelná. Tyto útoky mohou také používat filtry či masky, díky čemuž se dokáží k heslu dopracovat ještě rychleji.
- **slovníkový útok** – na rozdíl od útoku hrubou silou využívají hackeři slovník - seznam slov - což znamená, že pokud je jako heslo použito existující slovo, je velkou pravděpodobností, že se ve slovníku objeví. [11]

Pro jistotu, že nové heslo bude opravdu silné a bezpečné lze najít na internetu generátory hesel, které z náhodných písmen, čísel a znaků vytvoří odolné heslo proti útokům. Takový generátor nabízí například i Avast.com (https://www.avast.com/random-password-generator). [11]



Obrázek 8: generátor hesel od avast.com [18]

3 KYBERŠIKANA A STALKING

Kyberšikana (cyberbullying) jednoduše řečeno šikana na internetu pomocí sociálních sítí a chytrých telefonů. Avšak na kyberšikaně není nic jednoduchého. Kyberšikana může být horší než klasická šikana hned z několika důvodů. Hlavním důvodem je, že oběť nemá možnost ji předvídat, nevidí na útočníka a forma může být daleko útočnější a častější než v reálném světě. Aby se dalo označení kyberšikana použít musí být oběť napadána systematicky a opakovaně jedincem případně skupinou. Kyberšikana může být také spojena s šikanou v reálném světě, která může zahrnovat například slovní nadávky, fyzické útoky, pomluvy či ponižování. Kyberšikana může mít několik forem útoku na oběť - vyhrožování, zveřejňování fotografií / nahrávek / videí, zastrašování, vydírání, krádež identity, nabourání se na účty na sociálních sítích. [1]

Jedním z aspektů kyberšikany je opakovatelnost. Tento aspekt je však nejobtížněji dokazatelný. V online světě je zranění způsobené kyberšikanou špatně rozpoznatelné, nelze na něj nahlížet tak jako na zranění způsobena šikanou klasickou (jedná se o fyzická i psychická zranění). Toto se děje například sdílením ponižující fotografie. Každé sdílení, přeposlání může být bráno jako další zranění oběti. [7]

Agresorovi v rámci kyberšikany nelze zamezit nebo zabránit v konání a přístupu k oběti, případně jen velmi omezeně. Neexistuje čas, kdy by agresor nemohl poslat e-mail, SMS zprávu, zveřejnit video / fotografii / příspěvek. Oběť může využít technické postupy pro zablokování agresora (blokování, nahlášení nevhodného obsahu), avšak agresor může vytvořit další a další nezablokované účty. [7]

Za formu kyberšikany může být považován i druh jménem sexting. V případě, že se jedná o nedobrovolné šíření obrázků, videí, textů se sexuální tématikou prostřednictvím internetu, kde mohou být dlouhodobě dostupné a opakovaně na oběť tímto způsobem útočit. [8]

3.1 Sexting

Sexting je druh chování, kdy dospívající mládež a mladí dospělí chtějí rozvíjet posíláním fotografií či videí svoje vztahy. Dobrovolný sexting je formou sexuální aktivity dospívajících a dospělých, tímto mohou uspokojovat svou sexuální zvědavost. Někteří mladí využívají sexting pro přilákání objektu jejich zájmu. [8]

Nátlakový sexting na druhé straně může představovat formu sexuálního obtěžování a nese vyšší riziko zneužití. Self-sexting je druh sextingu, kdy osoba, která materiál poskytuje je zároveň i aktérem na fotografiích. Peer-sexting znamená sdílení obrázků mezi vrstevníky. [8]

Nátlakový nebo také nedobrovolný sexting může zahrnovat i určitou míru obtěžování nebo nátlaku. Příkladem může být, když chlapec nutí dívku, aby mu poslala fotografii intimního charakteru s argumentem, že pokud tak neučiní tak ho dostatečně nemiluje. [8]

V romantickém vztahu dvou lidí může být sexting brán jako normální věc, zpestření všedních dní, případně také jako forma experimentování. Toto můžeme nazvat jako konsenzuální sexting, který se vyskytuje nejenom u dospívající ale i u dospělých jedinců. Opakem je sexting nonkonsenzuální neboli nedobrovolný. Dalším druhem sextingu může být takový, kdy jednotlivec zasílající intimní fotografie touží po pozornosti. Dospívající se snaží upoutat pozornost rozesíláním intimních fotografií s erotickým obsahem. Ovšem v každém případě se k takovým fotografiím může vždy dostat třetí osoba, pro kterou nebyly určeny. V horším případě třetí osoba může tyto fotografie dále distribuovat, což může znamenat problémy pro osobu, která je na těchto fotografiích. [8]

3.2 Kybergrooming

Chování uživatelů na internetu, jehož cílem je pomocí moderních technologií vzbudit v dítěti či dospělém pocit důvěry a následně jej vylákat na schůzku. Například zneužití dětí a mladistvých k jinému účelu, například terorismu může být bráno jako forma kybergroomingu. Nejdůležitějším krokem při kybergroomingu je vzbuzení důvěry oběti. Útočník oběť oslovuje především podle volně dostupných údajů na internetu - na profilu oběti na sociální síti. Dle toho pak vzbuzuje důvěru například stejnými koníčky, názory případně podobnými problémy. [1]

Pro vzbuzení důvěry si útočníci vytváří falešnou identitu obsahující více svých profilů, které vypadají jako pravé, sdílí na nich fotky, například z kroužků a vytváří si tak svůj vlastní svět. Při oslovení obětí si většinou najdou nějakou záminku - koníček, kroužek, film, hudbu a dle toho pak oběti oslovují s konkrétní otázkou, která vypadá jako z okruhu přátel oběti. Takový falešný profil lze snadno odhalit, pokud bude člověk věnovat pozornost detailům. Mezi takové detaily patří například doba založení účtu, minimum přátel nebo přátelé pouze z jedné

skupiny (například chlapci okolo patnácti let), dvojsmyslné popisky či údaje. Sofistikované a vyumělkované fotografie, minimální počet fotografií zachycující běžný denní život. [1]

Útočník vzbuzuje dojem, že mu na oběti záleží, nabízí různé druhy odměn například za zaslání nahých, intimních či sexuálních fotografií. Nabídky mohou být různé, finanční, nebo třeba koupě lístků na oblíbenou kapelu, pomoc s úkolem, zaplacení dovolené aj. V rámci tohoto chování může mít oběť pocit, že si s neznámým buduje silný kamarádský vztah a neznámému na oběti opravdu záleží. Z tohoto může vzniknout emoční závislost oběti na útočníkovi. Oběť se začne svěřovat se svými problémy, trápeními. Oběť se také může jednoduše do útočníka zamilovat, děti mají tendenci se zamilovat pouze na základě základních či vizuálních informací. [1]

Jednou z posledních fází kybergroomingu je nabídka osobního setkání, které ve většině případů má proběhnout někde, kde se oběť nebude moci dovolat pomoci - uzavřené místnosti, auto, sklep, příroda. Poslední etapu a také tou nejhorší je zneužití, napadení či obtěžování dítěte. Toto je čím dál častější, bohužel oběti si tuto skutečnost ve většině případů nechávají pro sebe a nehlásí ji. Ochranou může být dostatečná prevence a důvěra mezi dětmi a rodiči či učiteli.

Oběťmi jsou nejčastěji děti ve věku 11 - 17 let, poměrově rovnoměrné mezi pohlavími. Ohroženější skupinou jsou blond dívky ve věku 13 - 14 let, chlapci pak zhruba o rok mladší se zájmem o sport. [1]

3.3 Stalking

Nebo jinak také nebezpečné pronásledování se může popsat jako nezdravý zájem od nevyžádané osoby o oběť. Často to mohou být bývalí partneři, lidé jejichž city nejsou opětovány. Jejich chování se vyznačuje manipulací, citovým vydíráním (pomocí velkého množství zpráv) či pokusy o setkání pod různými záminkami. [1]

V trestním zákoníku České republiky se od 1. ledna 2010 objevil nový trestný čin a to Nebezpečné pronásledování v § 354. A jeho popis zní:

"§ 354 *Nebezpečné pronásledování*

(1) Kdo jiného dlouhodobě pronásleduje tím, že

a) vyhrožuje ublížením na zdraví nebo jinou újmou jemu nebo jeho osobám blízkým,

b) vyhledává jeho osobní blízkost nebo jej sleduje,

c) vytrvale jej prostřednictvím prostředků elektronických komunikací, písemně nebo jinak kontaktuje,

d) omezuje jej v jeho obvyklém způsobu života, nebo

e) zneužije jeho osobních údajů za účelem získání osobního nebo jiného kontaktu,

a toto jednání je způsobilé vzbudit v něm důvodnou obavu o jeho život nebo zdraví nebo o život a zdraví osob jemu blízkých, bude potrestán odnětím svobody až na jeden rok nebo zákazem činnosti.

(2) Odnětím svobody na šest měsíců až tři roky bude pachatel potrestán, spáchá-li čin uvedený v odstavci 1

a) vůči dítěti nebo těhotné ženě,

b) se zbraní, nebo

c) nejméně se dvěma osobami.” [9]

Mezi projevy stalkingu patří například snaha o poškození pověsti oběti pomocí šíření nepravdivých informací, vyhrožování fyzickým útokem na oběti případně na jejich blízké. Stalker se také často vydává za oběť a tvrdí, že se mu oběť mstí. [1]

Přehnaný zájem, nevyžádané zprávy na sociálních sítích nebo seznamovacích serverech je potřeba okamžitě řešit. Jako první krok se doporučuje kontaktovat administrátory serveru, na kterém se tady to děje. Ti by měli takové poznatky vyhodnotit a případně oznámit policii spolu s obětí. Administrátoři mohou na serverech stalkera zablokovat, případně jinak hlídat. [1]

Stalking nemusí probíhat pouze přes sociální sítě, velmi často se přesouvá do všech rovin, kde se oběť pohybuje. V reálném světě oběť sleduje, čeká na ni na místech, která ví, že navštěvuje (například před prací v čas, kdy oběť končí a odchází) a následně pokračuje i na sociálních sítích či jinde na internetu. Toto se dá vyřešit změnou návyků, například změnit čas příchodu a odchodu z práce, či školy, použít jinou cestu než normálně. Oběť by také měla obeznámit rodinu a blízké o tom, že se to děje, s největší pravděpodobností budou stalkerem též kontaktováni. Oběť by neměla chodit sama, odpovídat na zprávy stalkera, nechodit na žádné schůzky se stalkerem. Při podání trestního oznámení na policii je dobré mít všechny konverzace, dokumenty, výpisy volání a jiné důkazy. [1]

3.4 Rozdíl mezi kyberšikanou, sextingem a stalkingem

V každém případě se jedná o druhy kyberšikany. Kyberšikana je nadřazena sextingu i stalkingu. Zároveň jsou jednotlivě velmi závažnými problémy, stalking trestným činem. Jediným druhem, který může být i dobrovolným je sexting, zde jde primárně o zasílání intimních fotografií či videí. Kyberšikanou se stává v momentě, kdy tyto fotografie zveřejní útočník bez vědomí oběti, případně rozesílá dalším lidem. [9]

Nejčastěji se lze setkat se sextingem, který bývá zpravidla dobrovolný, minimálně na začátku, kdy případné oběti samy od sebe tyto fotografie či videa sdílejí. V případě dalšího šíření těchto fotografií či videí se jedná o kyberšikanu. I když byly fotografie rozeslány dobrovolně, pořád jsou majetkem osoby, která na nich je a ne osoby, která je šíří dál. [9]

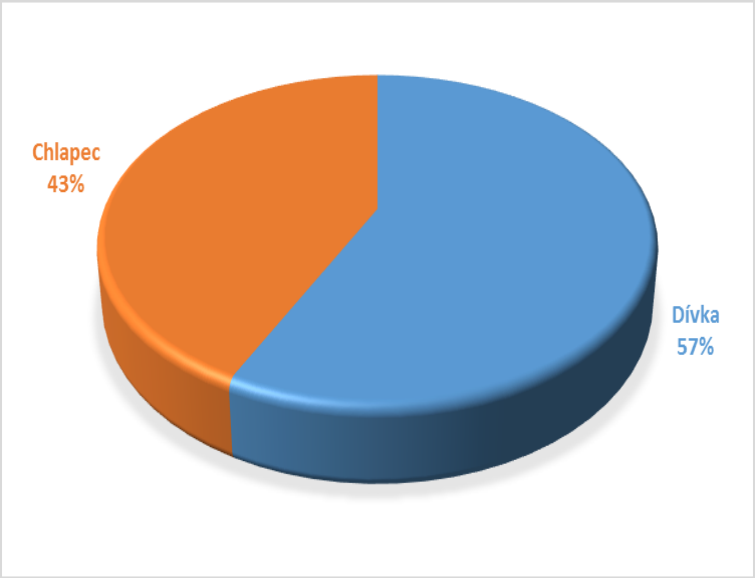
II. PRAKTICKÁ ČÁST

4 METODY PRŮZKUMU

Metody výzkumu pro účely této bakalářské práce byly stanoveny jako kvantitativní výzkum pomocí dotazníkového šetření a následný průzkum sociálních sítí. Dotazníky byly rozeslány na druhý stupeň základní školy Želatovská 8 v Přerově, pomocí paní Mgr. Markéty Krajňakové Ph.D. Na tuto základní školu se odeslalo 45 dotazníků a všech 45 dotazníku se vrátilo vyplněných, tzn. 100 % návratnost. Všechny tyto vytištěné dotazníky byly ručně zadány do online verze dotazníku na webu vyplnto.cz. Tento online dotazník byl také rozeslán na další školy s žádostí o vyplnění. Celkový počet respondentů je 94.

Dotazník obsahuje 30 otázek zaměřených na používání sociálních sítí mladistvými (10 - 18 let), také na to jak se na sociálních sítích chovají, co sdílejí a s kým. V poslední části dotazníku jsou otázky na kyberšikanu, která je velkým tématem tak jako šikana běžná (face to face). Většina otázek byla uzavřená, případně polouzavřená. Pouze dvě otázky byly otevřené, kde mohli respondenti vyjádřit své poznatky či zkušenosti, tyto otázky nebyly povinné.

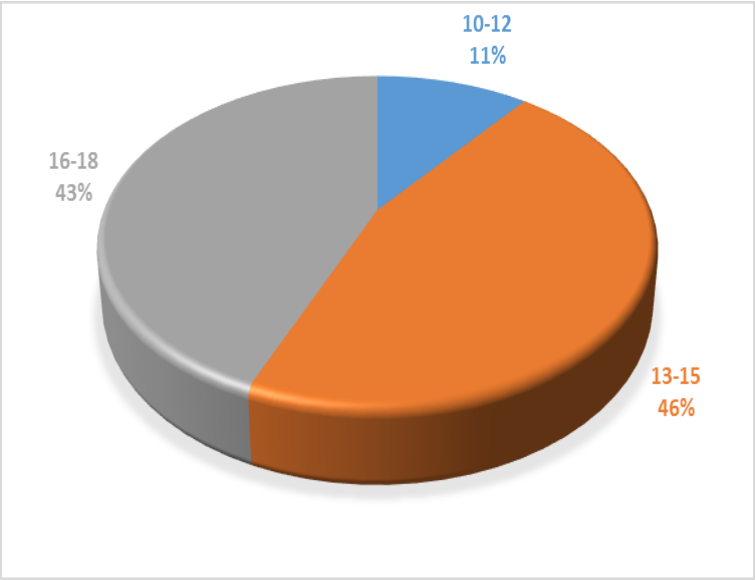
1. otázka - Pohlaví



Graf 1: Pohlaví

Z 94 respondentů bylo 54 dívek a 40 chlapců.

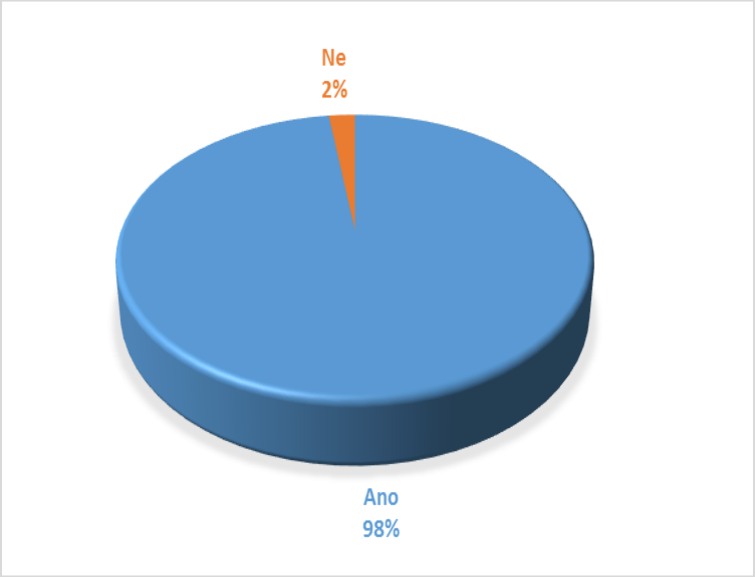
2. Druhá zjišťovací otázka byla na věk.



Graf 2:Věk

Z 94 respondentů bylo ve věkovém rozmezí 10 - 12 let 10 respondentů, 13 - 15 let 43 respondentů a 16- 18 let 41 respondentů.

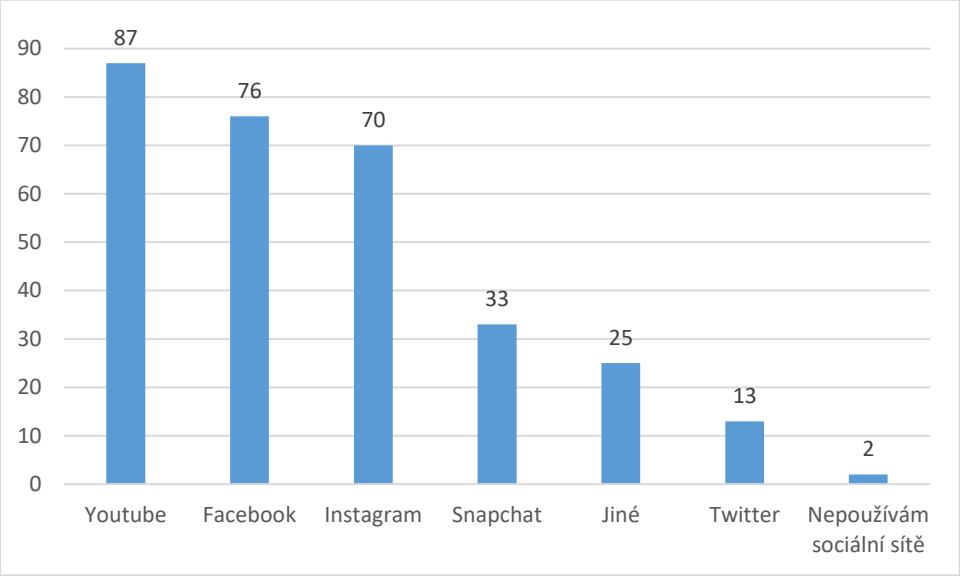
3. Víte, co jsou sociální sítě?



Graf 3: Víte, co jsou sociální sítě?

Na tuto otázku odpověděla jedna dívka 16 - 18 let, že neví, co jsou sociální sítě a pak jeden chlapec ve stejné věkové skupině.

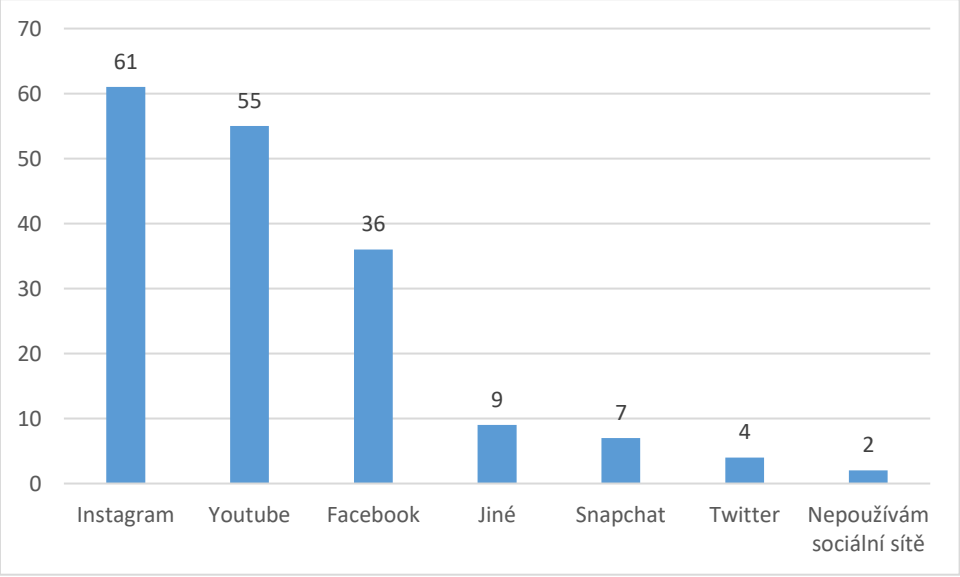
4. Jaké sociální sítě používáte?



Graf 4: Jaké sociální sítě používáte?

Nejčastěji zmíněnou sociální síť Youtube používá 87 respondentů z 94, Facebook a Instagram poté zabírají druhou a třetí příčku. Nejméně se používá sociální síť Twitter. Snapchat kde se posílají fotografie či krátká videa (princip jako Instagram stories, avšak Snapchat toto využíval jako první) používají mladiství čím dál méně. Z toho vyplývá, že na posílání mizejících příspěvků využívají nejvíce Instagram.

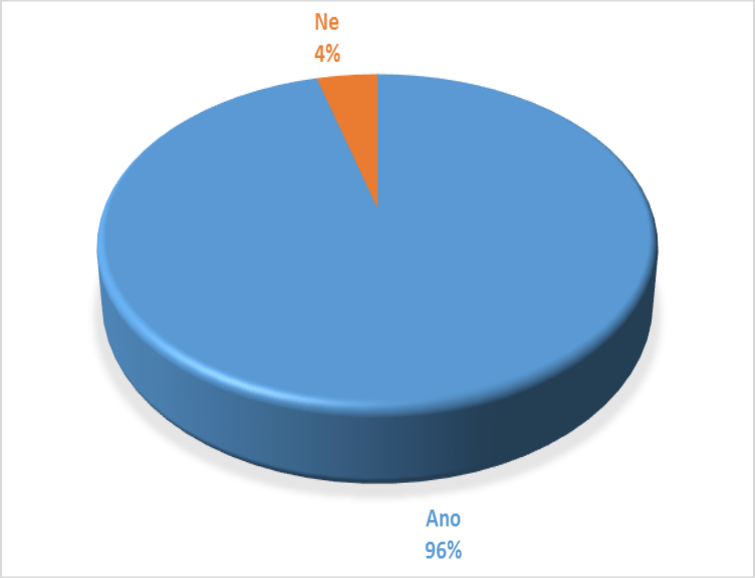
5. Jaké sociální sítě používáte nejčastěji?



Graf 5: Které sociální síte používáte nejčastěji?

Nejvíce dotázaných odpovědělo, že nejčastěji používají Instagram, jako druhou nejčastější síť uváděli Youtube a následně pak Facebook. Minimum odpovědělo, že nejvíce využívají Twitter, který dle výsledků dotazníku není v České republice ve věkové skupině 10 - 18 let vůbec oblíbený a téměř nikdo jej nepoužívá.

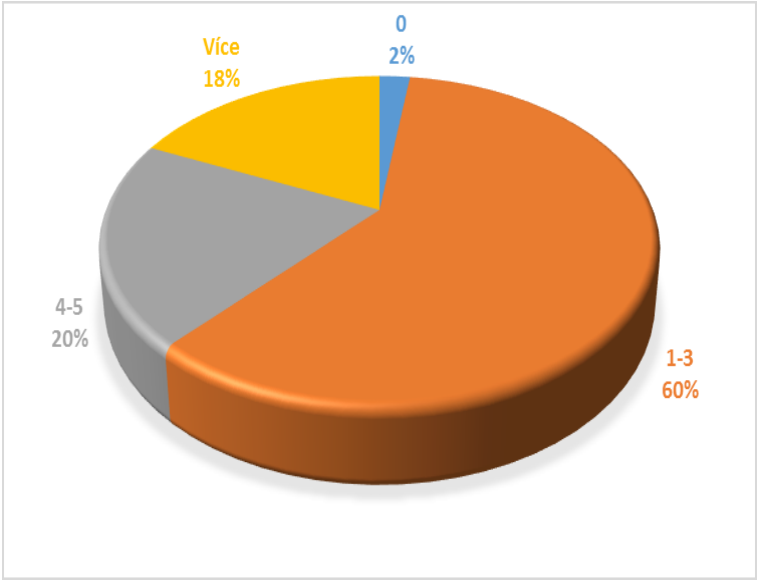
6. Vlastníte telefon / tablet s připojením na internet?



Graf 6: Vlastníte telefon / tablet s připojením na internet?

Tato otázka byla položena hlavně z důvodu toho, zjistit, zda mají žáci přístup k sociálním sítím takřka neomezeně nebo jestli jsou vázáni na Wi - Fi sítě, případně na povolení rodičů doma na počítači. Telefon s připojením na internet nevlastní chlapec 16 - 18 let, chlapec 13 - 15 let, dívka 16 - 18 let, která zároveň uvedla, že sociální sítě nevyužívá vůbec, a chlapec 16 - 18, který rovněž uvedl, že sociální sítě nepoužívá.

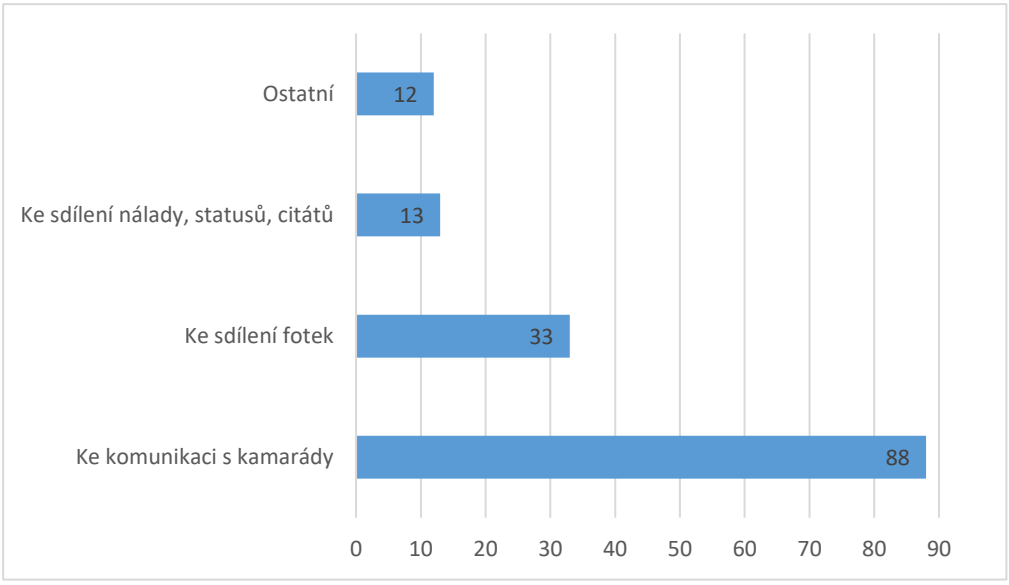
7. Kolik hodin denně trávíte na sociálních sítích?



Graf 7: Kolik hodin denně trávíte na sociálních sítích?

Nejvíce dětí odpovědělo, že na sociálních sítích tráví čas v rozmezí 1 – 3 hodin (60 %), což není hodně, znepokojující je spíše 20 % dětí, které tráví na sociálních sítích 4 - 5 hodin denně a 18 % dokonce více jak 5 hodin denně. Což v rychlém přepočtu na aktivní hodiny žáka základní školy druhého stupně je téměř celý volný čas, který netráví ve škole případně na kroužcích.

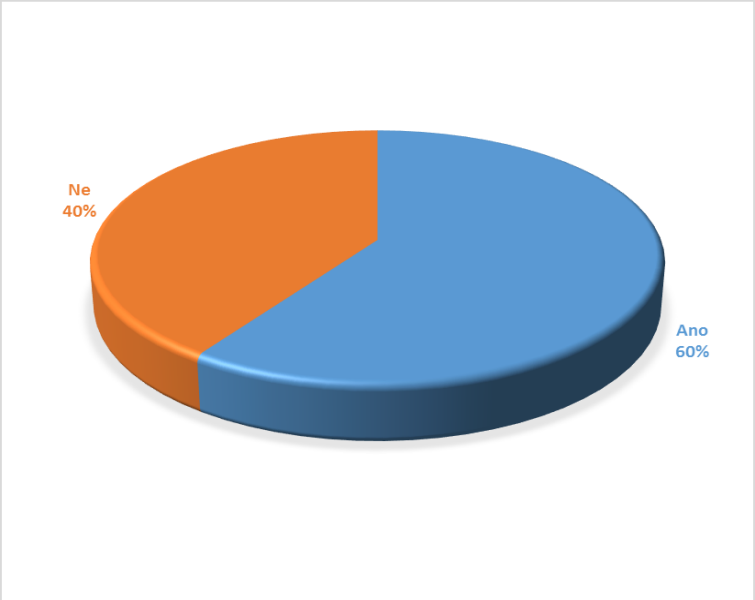
8. K čemu sociální sítě používáte?



Graf 8: K čemu sociální sítě používáte?

Tato otázka nabízela pár odpovědí, ale také možnost vyplnit vlastní. Nejvíce respondetnů odpovídalo, že využívají sociální sítě ke komunikaci s kamarády, případně ke sdílení fotek, nálady, statusů či citátů. Překvapivé je, že zde pouze 3 lidé odpověděli, že sledují Youtube, ale přitom v otázce číslo 4 i 5 bylo odpovězeno více jak 40 krát, že používají Youtube… Některé odpovědi nejspíše měly být spíše vtipné – například chlapec 16 – 18 let uvedl, že sociální sítě používá k lovení ryb.

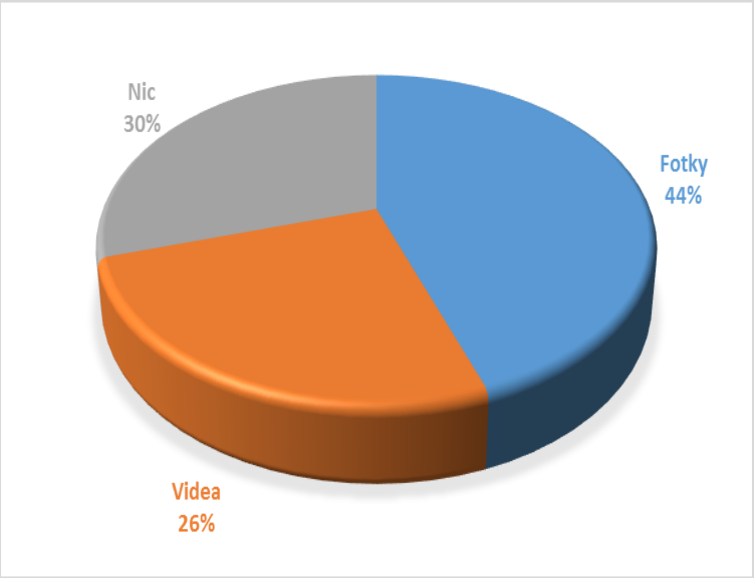
9. Pokud používáte Instagram / Snapchat, využíváte možnosti Stories? (zveřejnění fotky či videa, které po 24 hodinách "zmizí")



Graf 9: Pokud používáte Instagram / Snapchat, využíváte možnosti Stories? (zveřejnění fotky či videa, které po 24 hodinách "zmizí")

Funkce Instagramu - Instastories je funkce umožňující sdílet krátká videa (do 15 sekund) a fotky, které jsou viditelné pouze 24 hodin od uveřejnění. Instagram také nabízí možnost poslat tuto fotku či video pouze svým vybraným přátelům, kdy příspěvek zmizí ihned po přehrání, ne až po 24 hodinách.

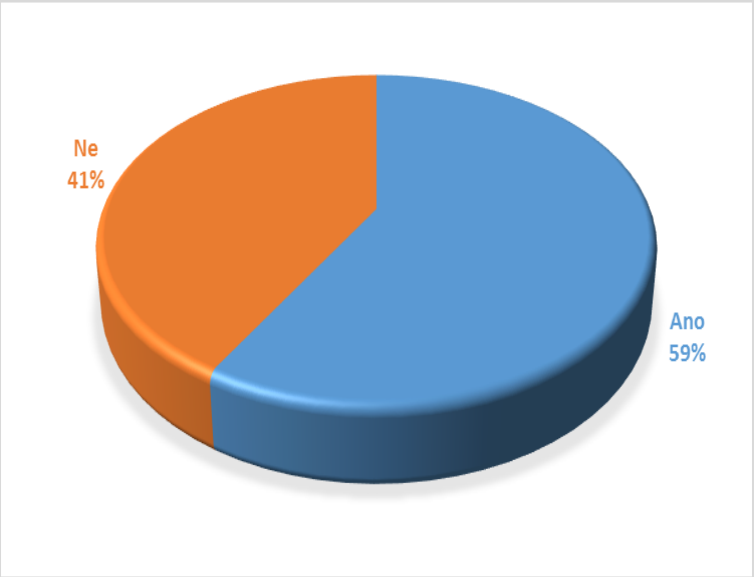
10. Pokud používáte Instastories, sdílíte zde:



Graf 10: Pokud používáte Instastories, sdílíte zde:

Z oslovených respondentů odpovědělo 57, že sdílí fotky, 33 videa a 38 z nich vybralo odpověď nic.

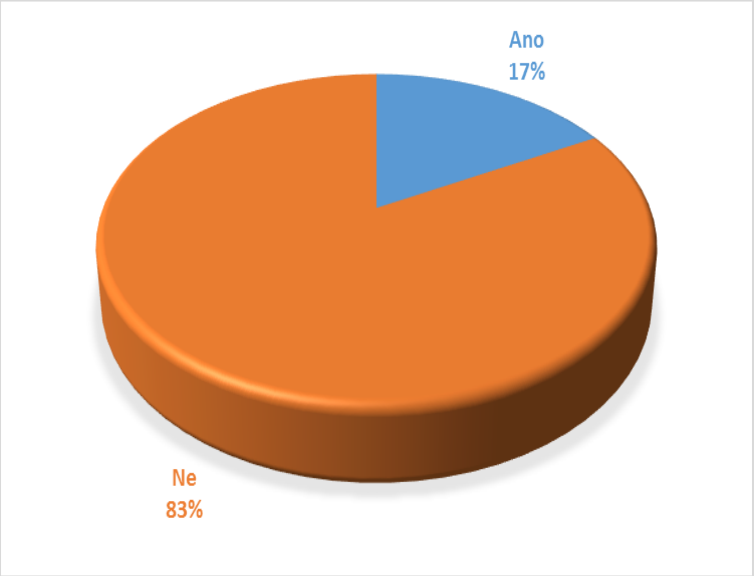
11. Sdílíte fotky sebe? (selfies, fotky s kamarády)



Graf 11: Sdílíte fotky sebe? (selfies, fotky s kamarády)

Na grafu lze vidět, že odpovědi byly relativně vyrovnané, 39 mladistvých odpovědělo, že ne a 55 že ano.

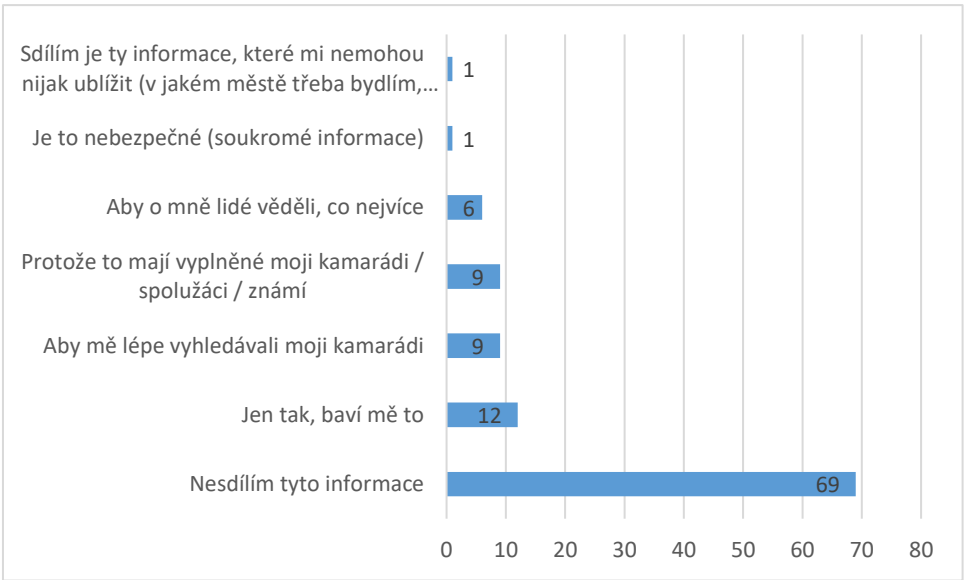
12. Sdílíte svoje konkrétní informace? (bydliště, školu, kterou navštěvujete, svoji rodinu)



Graf 12: Sdílíte svoje konkrétní informace?
(bydliště, školu, kterou navštěvujete, svoji rodinu)

Touto otázkou se dotazník přesouvá spíše do části, kde se zjišťuje, jak moc si mladiství dávají pozor na to, co sdílí veřejně a co ne. Spousta z nich se vyjádřila tak, že z odpovědí vyplývá, že nad tím přemýšlí a nesdílí veškeré informace, které by sdílet mohli.

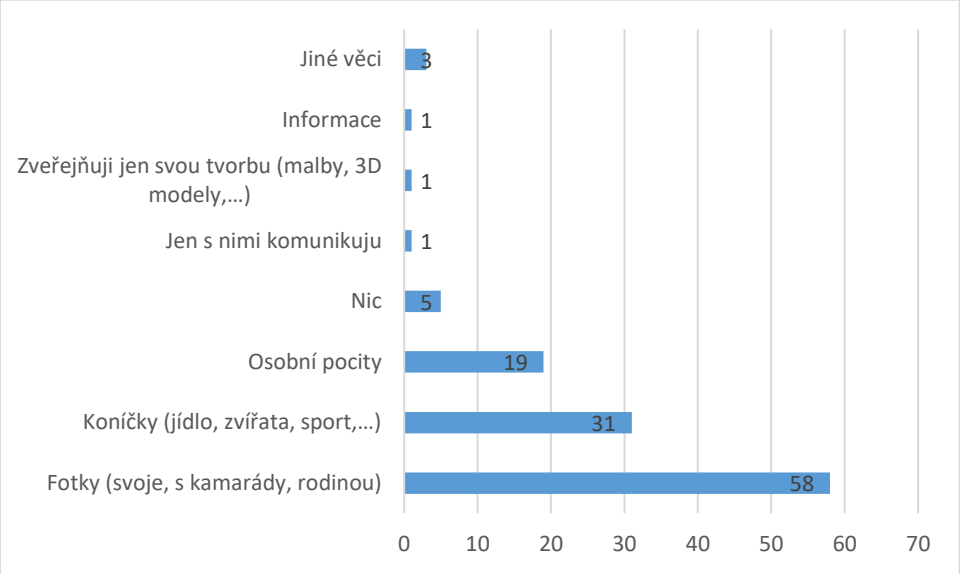
13. Pokud ano, proč tyto informace sdílíte?



Graf 13: Pokud ano, proč tyto informace sdílíte?

Zde byly odpovědi opět dány, ale respondent mohl odpovědět i jinak, jak uznal za vhodné. 69 dětí odpovědělo, že tyto informace nesdílí, což může svědčit o tom, že přemýšlí nad tím, co je vhodné sdílet s internetovým světem a co vhodné již není. Dívka 16 – 18 let uvedla, že sdílí jen ty informace, které ji nemohou ublížit, jako je například město, kde bydlí, ale konkrétnější informace nesdílí. Toto může vypadat jako neškodná informace, ovšem nemusí tomu tak být. Pokud někdo zná konkrétní město, kde dotyčná / ý bydlí a je to menší město, není zpravidla moc těžké si dál zjistit další informace a dostat k tomuto člověku blíž, případně jej jinak kontaktovat.

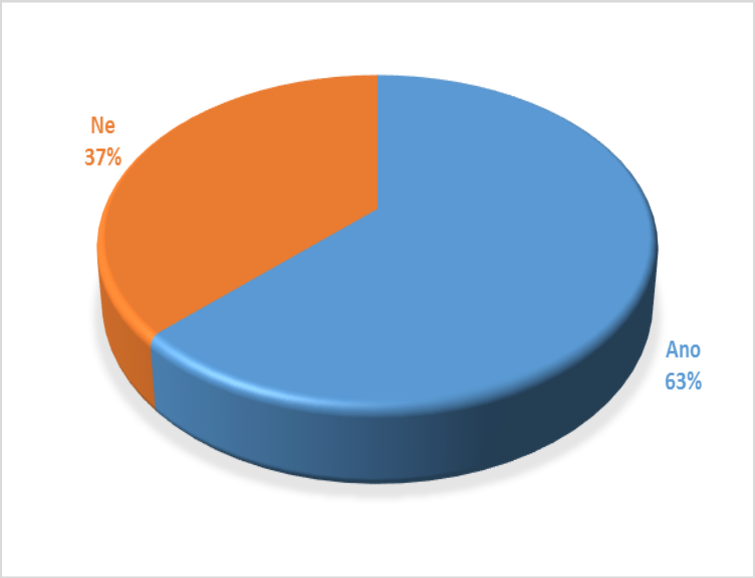
14. Co nejvíce sdílíte na sociálních sítích?



Graf 14: Co nejvíce sdílíte na sociálních sítích?

Největší počet dětí odpovědělo, že sdílí své fotky – fotky s kamarády, s rodinou, menší počet potom sdílí různé své koníčky, minimum sdílí své osobní pocity a jen jedna studentka ve věku 16 -18 let sdílí jen svou tvorbu – 3D modely, malby a jiné.

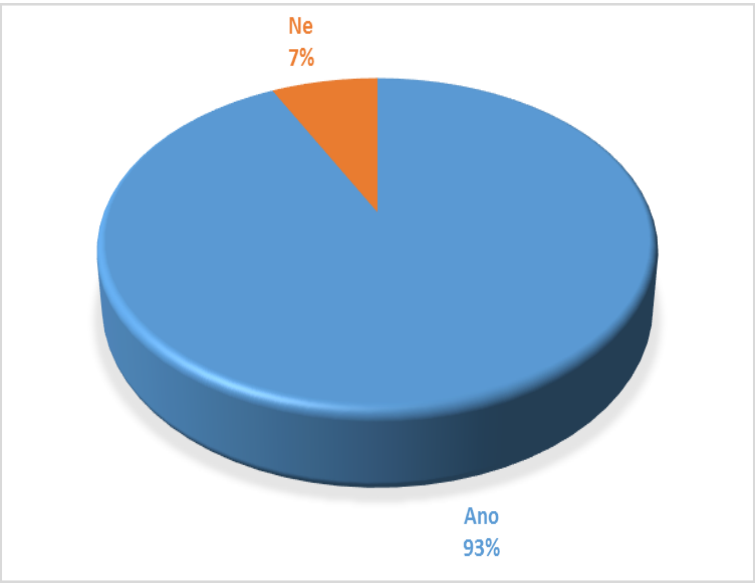
15. Označujete své přátele na fotkách?



Graf 15: Označujete své přátele na fotkách?

Označování kamarádů, rodiny, známých se může zdát jako neškodný počin, nemusí tomu však tak být. Pro stalkery a jiné osobnosti pohybující se na internetu je toto nejjednodušší způsob jak získat dodatečné informace nejenom o objektu zájmu, ale také o jeho koníčcích, přátelích, rodině a tak podobně.

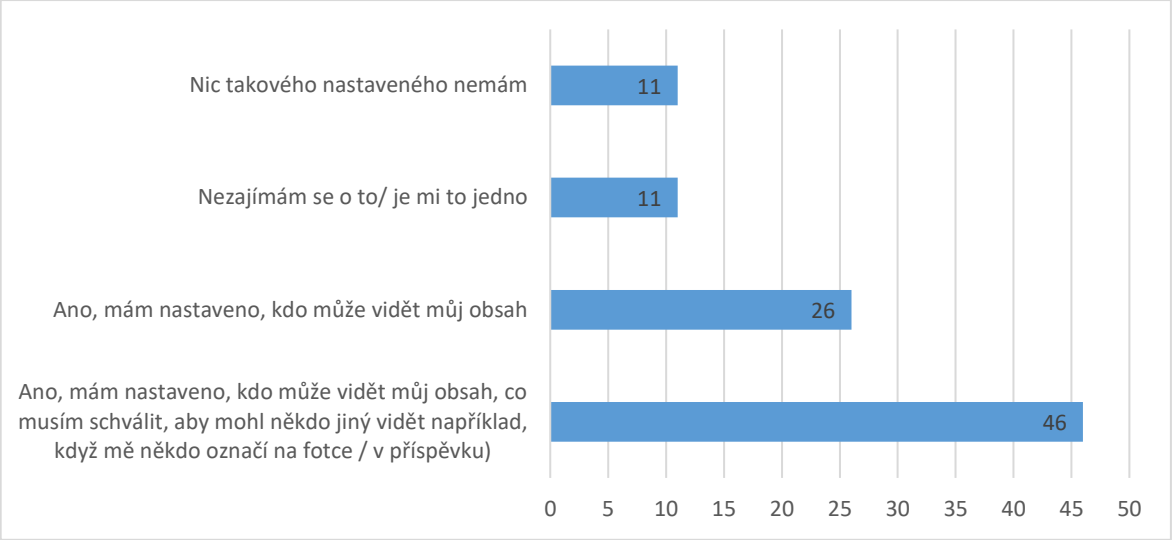
16. Víte, jak si ochránit své soukromí na těchto sociálních sítích?



Graf 16: Víte, jak si ochránit své soukromí na těchto sociálních sítích?

Na tuto otázku odpovědělo, že neví jak si soukromí ochránit 7 mladistvých, 3 dívky 16 -18 let, 3 chlapci 13 – 15 let a jeden chlapec 16 – 18 let.

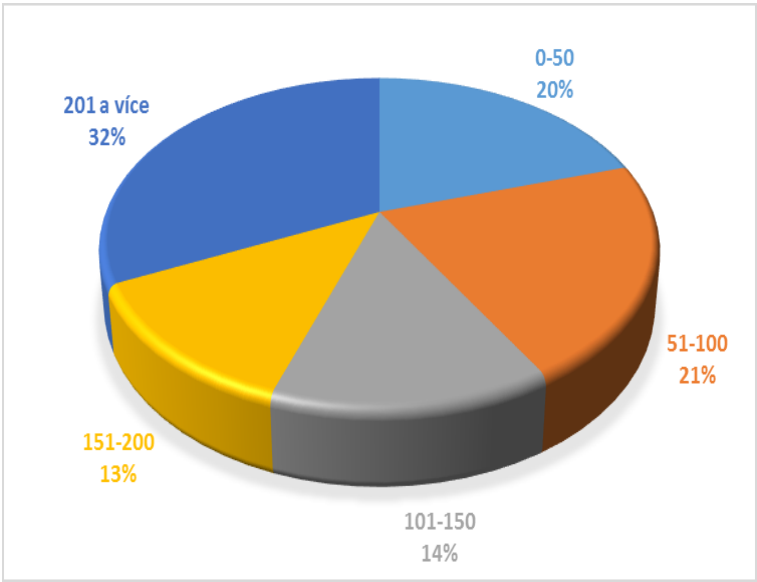
17. Chráníte si soukromí na sociálních sítích pomocí nastavení?



Graf 17: Chráníte si soukromí na sociálních sítích pomocí nastavení?

Poměrně překvapivý se zdá výsledek toho, jak si mladiství chrání soukromí. Předpoklad výsledku této anketní otázky byl, že si mladiství chrání soukromí pomocí nastavení ve většině případů. Zde je vidět, že sice téměř polovina má nastaveno, kdo může jejich obsah vidět a schvalování příspěvků, ovšem také 22 dětí odpovědělo, že je to buď vůbec nezajímá a je jim to jedno nebo, že nic takového nastaveného nemají.

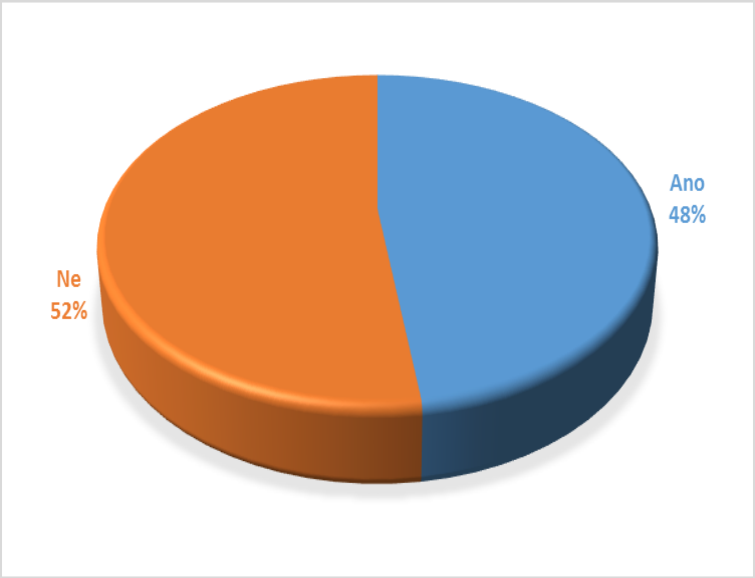
18. Kolik máte na Facebooku / Instagramu přátel?



Graf 18: Kolik máte na Facebooku / Instagramu přátel?

Tato otázka měla zjistit, kolik přátel mladiství obvykle mají na těchto sociálních sítích. Rozmezí čísel mohlo být větší a to z důvodu, že nejvíce (32 % dotázaných) odpovědělo, že mají více jak 201 přátel, předpoklad byl takový, že mají v přátelích pouze lidi, které znají a v rozmezí 10 – 18 let nemají tolik možností, kde kamarády hledat (zatím pouze základní škola, případně víceleté gymnázium, nějaké kroužky a jiné aktivity).

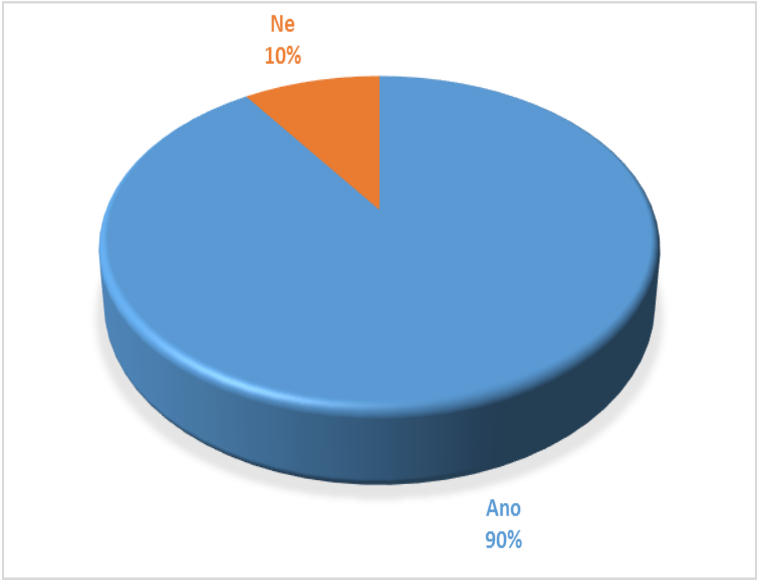
19. Znáte všechny tyto lidi osobně?



Graf 19: Znáte všechny tyto lidi osobně?

Zjištění, že více jako polovina mladistvých nezná všechny lidi, které mají na svých sociálních sítích, je poměrně znepokojující. Může to být pozvánka do jejich soukromí pro všechny druhy lidí, ať už pro neškodné jedince, tak i pro stalkery, agresory a jiné další typy lidí.

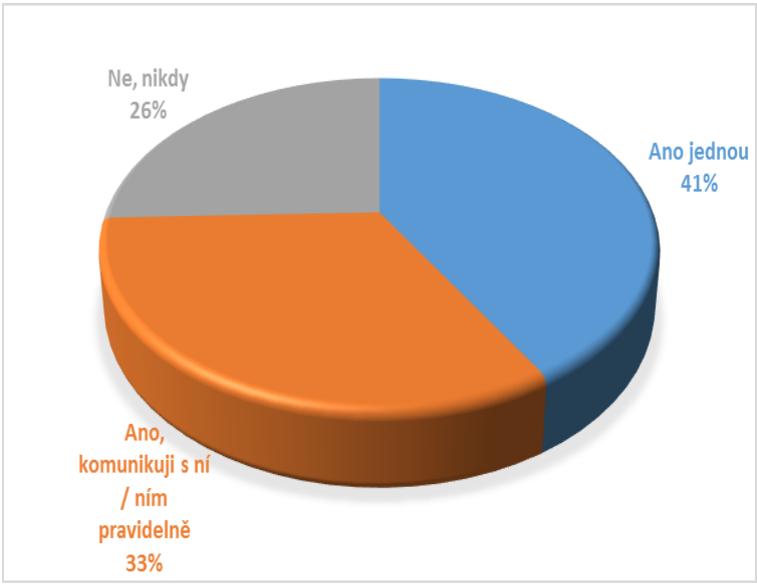
20. Myslíte si, že se na sociálních sítích může člověk stát závislým?



Graf 20: Myslíte si, že se na sociálních sítích může člověk stát závislým?

Na grafu číslo 20 lze vidět, že 10 % (9 mladistvých) dotázaných si myslí, že se na sociálních sítích nemůže člověk stát závislým. Jedná se především o chlapce (čtyři chlapci ve věkové skupině 13 – 15, jeden 10 -12 a jeden 16 – 18 let) a tři dívky, všechny ve věkové kategorii 16 – 18 let.

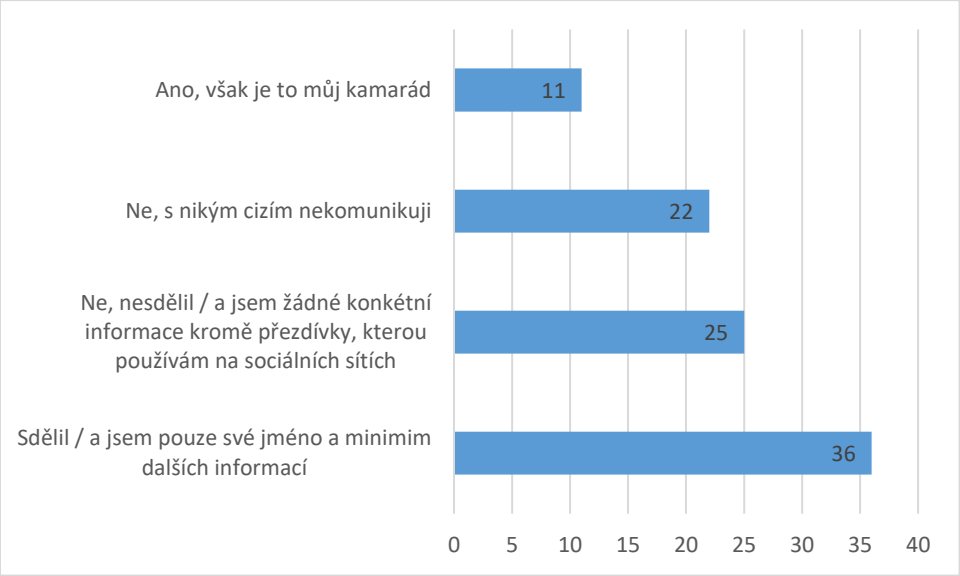
21. Komunikovali jste někdy s člověkem, kterého jste nikdy neviděli v reálném světě?



Graf 21: Komunikovali jste někdy s člověkem, kterého jste nikdy neviděli v reálném světě?

Na grafu 21 je znázorněno, že téměř polovina respondentů někdy ve svém životě komunikovala s někým, koho nikdy neviděla v reálném životě a to že 33 % dětí komunikuje s tímto člověkem pravidelně je opravdu znepokojující. Nejmenší počet dětí odpovědělo, že s takovým člověkem nikdy nekomunikovalo (24 z 94 dotázaných).

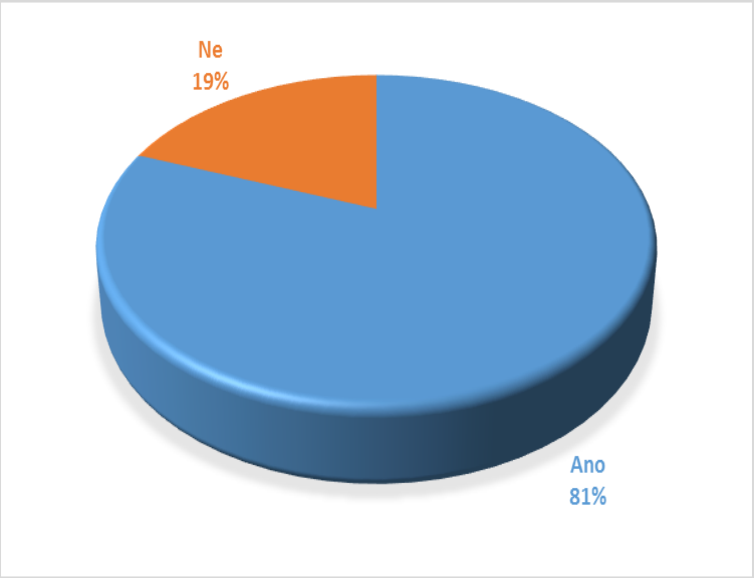
22. Sdělujete tomuto neznámému kamarádovi své osobní údaje (věk, bydliště, školu, do které chodíte, informace o rodině,…)?



Graf 22: Sdělujete tomuto neznámému kamarádovi své osobní údaje (věk, bydliště, školu, do které chodíte, informace o rodině,…)?

Výsledek této otázky je opět překvapivý, i když se na první pohled může zdát, že minimum sděluje své konkrétní informace (11 dětí) není to „pouze“ 11 dětí, které uvedly, že tyto informace sdělují, jelikož je to jejich kamarád, což samo o sobě může být problémem, ale také 36 dětí, které některé z těchto informací sdělily někomu, koho nikdy neviděly. Internet se může zdát být bezpečným místem, kde nikdo nevidí, kdo za monitorem sedí, co si myslí, jak vypadá. Ale když takhle přemýšlejí děti ve věku 10 – 18 let, jak mohou přemýšlet dospělí jedinci? Úplně stejně.

23. Zažili jste někdy Vy nebo někdo ve Vašem okolí kyberšikanu? (šikana, která probíhá na internetu, na sociálních sítích pomocí komentářů, sdílení našich fotek, zesměšňování apod.)



Graf 23: Zažili jste někdy Vy nebo někdo ve Vašem okolí kyberšikanu?

V dnešní době bohužel šikana neprobíhá jen v reálném světě, například ve škole, ale především na internetu. Více jak 80 % z dotazovaných se někdy s kyberšikanou setkalo, což může být také způsobeno tím, že na internetu si obecně může „útočník“ připadat více skrytý a méně na očích než kdyby šikana probíhala na veřejnosti.

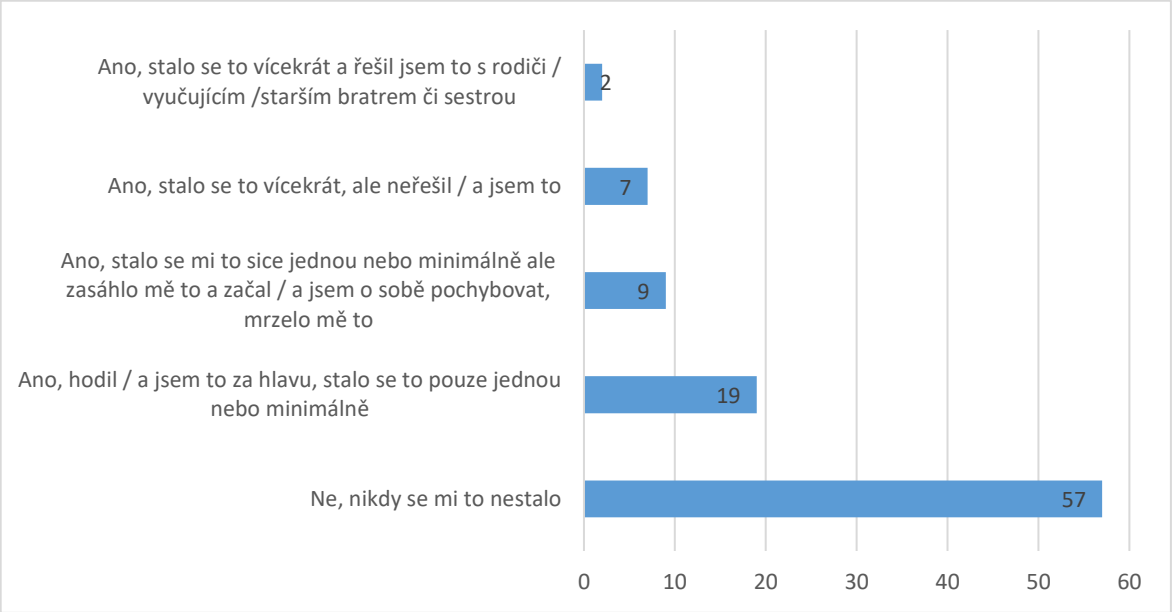
24. Pokud ano, jak tato kyberšikana probíhala? Otázka číslo 24 nebyla povinná, respondenti měli odpovědět dle svých zkušeností.

- beneš mě vyfotil :((chlapec 16 -18).
- Smáli se mi pod fotkama, že jsem tlustý (chlapec 13 – 15).
- Na bývalého spolužáka, který má Aspergerův syndrom si dotyčný udělal jeho profil. Kyberšikana probíhala formou sdílení nepravdivých informací, zesměšňování apod. (chlapec 16 – 18).
- Znásilňování (chlapec 16 – 18).
- Vyhrožování (dívka 16 – 18).
- Pomluvy (chlapec 13 – 15).
- sdílením videa mě s nevhodným obsahem (dívka 13 – 15).

- nechci zmiňovat (dívka 13 – 15).
- jen označování v urážlivých příspěvcích a nadávky v jedné anonymní aplikaci (dívka 13 – 15).

pozn.: Odpovědi jsou autentické, tak jak je respondenti zadali do dotazníku.

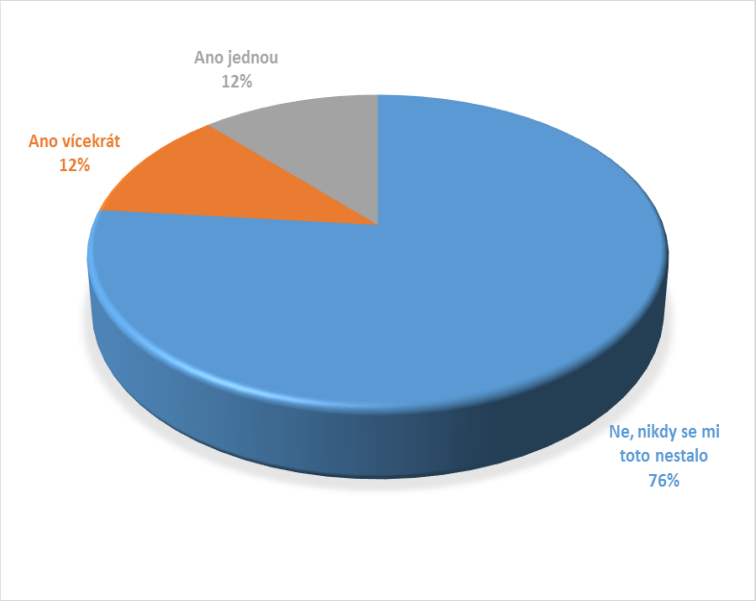
25. Zažili jste někdy zesměšnění na sociální síti? Někdo nelichotivě okomentoval Vaši fotku, status, cokoli? A jak jste se s tím vypořádali?



Graf 24: Zažili jste někdy zesměšnění na sociální síti? Někdo nelichotivě okomentoval Vaši fotku, status, cokoli? A jak jste se s tím vypořádali?

Na otázku 23. odpovědělo 81 %, že se s kyberšikanou na sociálních sítích setkalo, na otázku 25 dopovědělo 57 respondentů, že jim se to nikdy nestalo. Toto může být způsobeno tím, že tomuto byli pouze svědky na cizích profilech. Dětí, které zažily nějaké posměšky, ale nezasáhlo je to, bylo 19, těch co to neřešily i přes to, že se to stalo opakovaně 7 a pouze 2 děti tento problém řešily s někým dospělým.

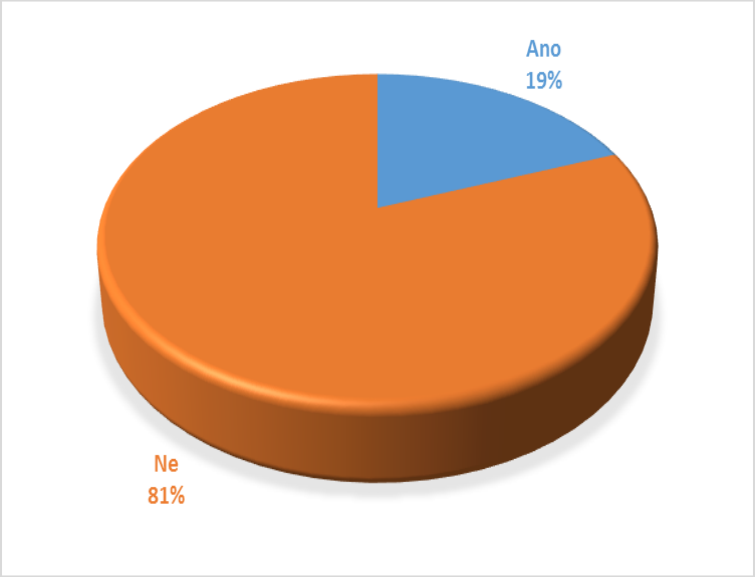
26. Stalo se Vám někdy, že na Vás cíleně na internetu útočil jeden člověk / skupina lidí? Zesměšňující fotky, nepříjemné zprávy?



Graf 25: Stalo se Vám někdy, že na Vás cíleně na internetu útočil jeden člověk / skupina lidí? Zesměšňující fotky, nepříjemné zprávy?

Odpovědi ano jednou a ano vícekrát mají stejný počet odpovědí a to 11. Ne, nikdy se mi toto nestalo, odpovědělo 72 respondentů. I tyto odpovědi korespondují s ostatními otázkami položenými výše ohledně kyberšikany a zesměšňování.

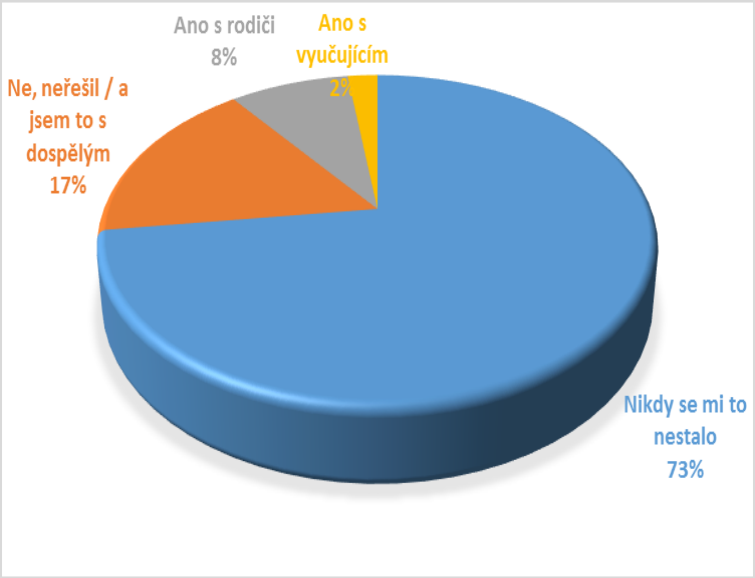
27. Byl to někdo, koho znáte / jste znali z reálného života?



Graf 26: Byl to někdo, koho znáte / jste znali z reálného života?

Více než 80 % odpovědí bylo záporných, pouze 18 dětí má zkušenosti s tím, že je na internetu obtěžoval někdo jim známý.

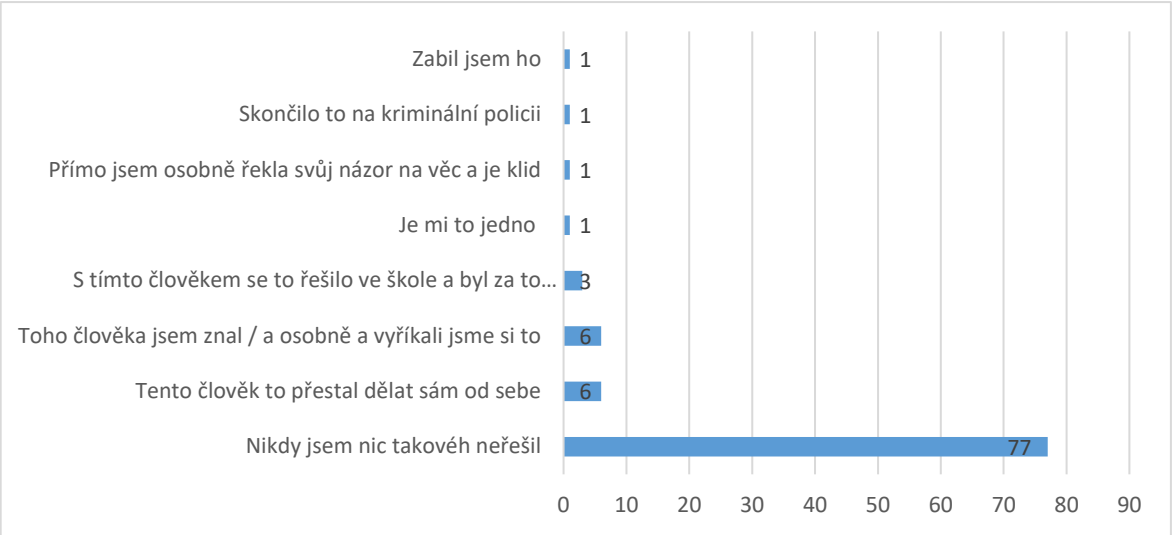
28. Řešili jste tuto věc s někým dospělým?



Graf 27: Řešili jste tuto věc s někým dospělým?

Většina mladistvých nikdy tento problém neřešila, více jak 70 % z důvodu, že se jim to nikdy nestalo, 17 % se toto stalo, ale s dospělým jej nikdy neřešili. Dohromady pouze 10 % dotázaných řešilo kyberšikanu s dospělými, ať už s rodiči nebo s vyučujícím.

29. Jak jste tuto věc řešili?



Graf 28: Jak jste tuto věc řešili?

V otázce 29 byl také prostor pro vlastní odpovědi, ale pouze 4 mladiství tuto možnost využili, zbylých 90 vybralo z nabízených odpovědí, opět nejvíce vybralo možnost, že nikdy nic takového nemuseli řešit. Nejspíš opět jedna odpověď, která nejspíš měla být vtipná, od chlapce 16 – 18 let, který uvedl, že sociální sítě používá k lovení ryb, uvedl také, že kyberšikanu řešil tím, že dotyčného zabil.

30. Pokud se Vám něco takového stalo, co byste doporučil tomu, kdo je šikanován? Pokud ne, odpovídat nemusíte. Otázka číslo 30 nebyla povinná, respondenti měli odpovědět dle svých zkušeností.

- Ať danou záležitost okamžitě řeší, protože mlčet je to nejhorší, co může udělat. Může vést až k depresím či k něčemu mnohem horšímu. (chlapec 16 – 18).
- Blokovat si všude tu osobu (dívka 13 – 15).
- Dal bych mu přes hubu (chlapec 10 – 12).
- Je to sice blbé, ale měl by to ten člověk říct, aby mu dospělí pomohli. (chlapec 13 - 15).
- Musí se umět bránit (chlapec 13 – 15).
- Pokud by mě někdo urážel tak bych ho/ji ignoroval. Pokud by se mě někdo snažil zesměšnit fotkou či videem tak bych tuto věc nahlásil. (chlapec 13 – 15).

- Proti kyberšikaně je nejjednodušší obrana si daného člověka zablokovat. Na všech sociálních sítích to lze. Pokud by to pokračovalo, je vhodné ho nahlásit a případně řešit přes rodiče/policii. Ale nejlepší je utnout to hned na začátku blokováním (dívka 16 – 18).
- Rozhodně to říct někomu dospělému (dívka 16 – 18).
- Řekli to rodičům nebo učitelce (chlapec 13 – 15).
- Řešit to přes školu a následně si zrušit účet na sociálních sítích. A snažit se, aby v reálném životě taky nevypadal jako snadný terč pro šikanu (vystupovat sebevědoměji, umět reálně komunikovat,…), (dívka 16 – 18).
- Říct to co nejdřív dospělým - rodičům. (dívka 16 – 18).
- Určitě to nahlásit, v horších případech rovnou policii, v žádném případě nejednat bez rozmyšlení (například na toho člověka hned zaútočit, mohlo by se to potom vymstít). (dívka 16 – 18).
- Určitě se nebát to říct někomu kdo je vám blízký a pomůže vám to řešit. Není se čeho bát (dívka 16 – 18).
- Zmlátit ho/poprosit někoho silného, ať ho zmlátí (chlapec 13 – 15).

pozn.: Odpovědi jsou autentické, tak jak je respondenti zadali do dotazníku.

5 ROVNÁNÍ PRŮZKUMU S REALITOU

Největším problémem dnešní doby a užívání sociálních sítí je to, že si uživatelé často neuvědomují, že vše co je jednou na internetu tam zůstane i když fotky či příspěvky uživatelé smažou. Vždy může být někdo, kdo si udělal printscreen fotky či příspěvku a vlastník o tom nemusí být ani informován. Spousta uživatelů má sociální sítě něco jako svůj vlastní deníček, kam sdílejí všechny své pocity, zážitky, nálady, fotky či videa. Neuvědomují si, že tohle může vidět celý internet a tím pádem vlastně úplně všichni, kteří k němu mají přístup.

5.1 Nejčastější chyby ve sdílení obsahu

Nejhorší chybou je veřejné sdílení informací o tom, kde se dotyčný pohybuje, myšleno v momentě, kdy odjede například na dovolenou. Není výjimkou, že sdílí například foto a popis, že jsou nyní na určitý čas mimo domov. Toto může mít nedozírné následky. Ne všichni lidé, které máme v přátelích, nebo nás sledují na našich profilech, jsou čestní. Tyhle informace můžeme v podstatě vnímat jako doslovnou pozvánku k vniknutí do našeho domu a odcizení věcí či peněz. Sdílení místa či polohy také napomáhá různým stalkerům k tomu, aby byli oběti ještě blíže v momentě, kdy se oběť nepohybuje na obvyklých místech.

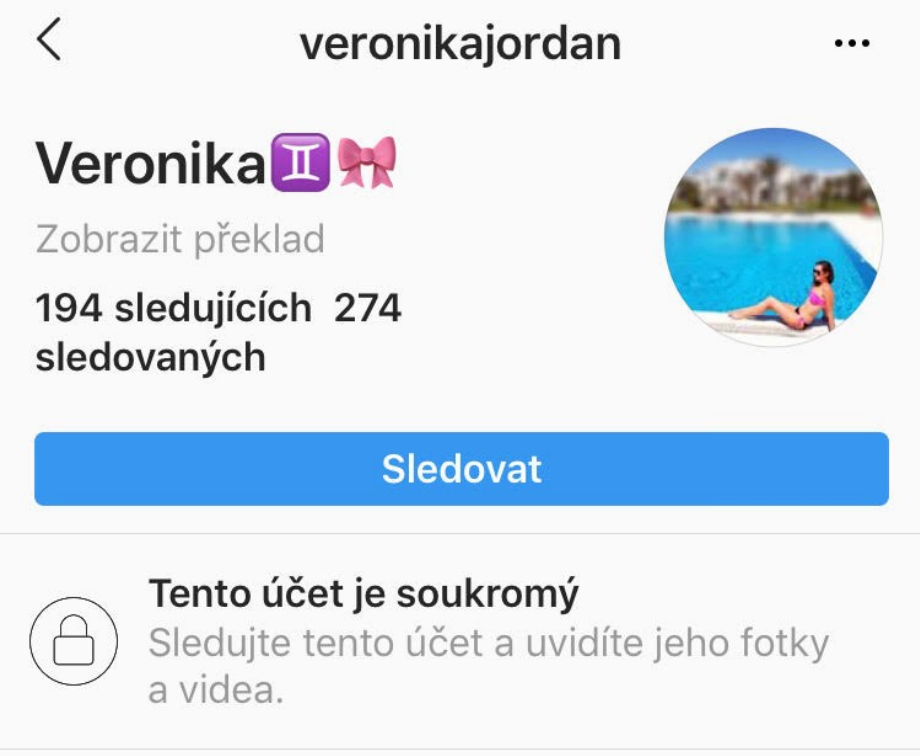
5.2 Srovnání

Pro potřeby bakalářské práce a výzkumu, co osoby sdílí veřejně, byl založen falešný účet jak na Facebooku tak i na Instagramu. Faceboook a Instagram z dotazníkového šetření vyšly jako jednoznačně nejpoužívanější, proto byl vytvořen účet na těchto dvou sociálních sítích.

Z průzkumu známých, přátel, rodiny, spolužáků a kolegů zatím jednoznačně vychází, že na sociální síti Facebook veřejně téměř nic nesdílí. Ovšem na Instagramu už je to zajímavější. Prozatím se z průzkumu zdá, že na Facebooku si lidé dávají pozor, jak na nastavení tak na to, co sdílí veřejně a co ne na rozdíl od Instagramu, kde jejich hranice ve sdílení opadají a jsou více otevření. Spousta z nich má na Instagramu také otevřený účet, který tím pádem může navštívit kdokoli a sledovat, co dělají, jaké fotky přidávají.

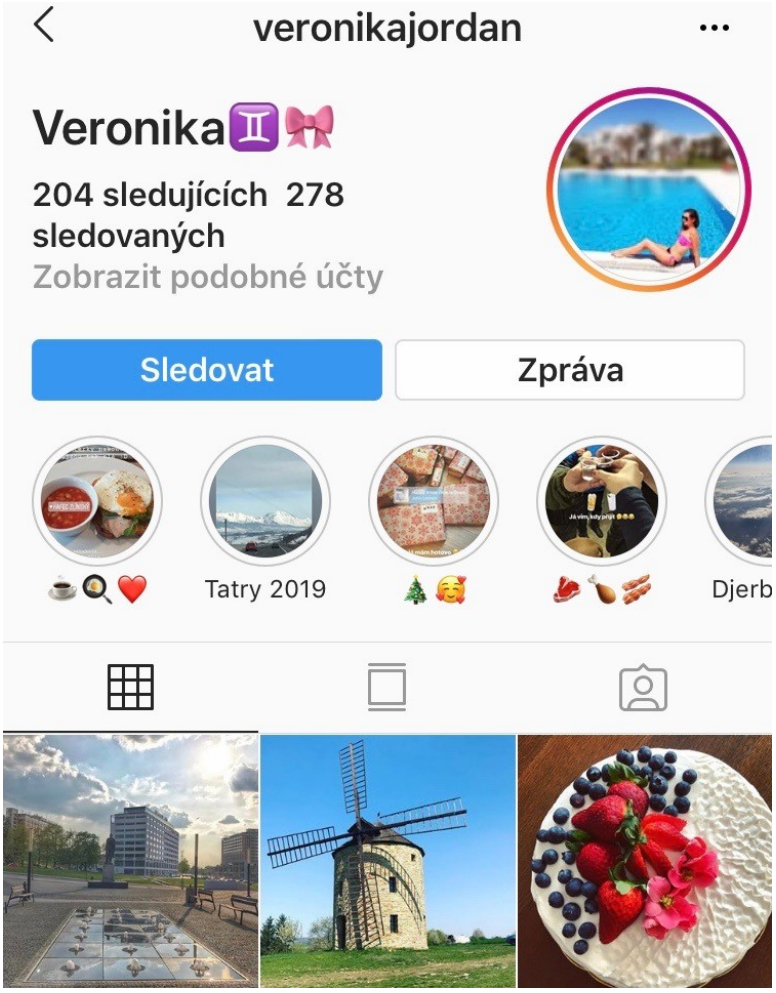
Na Instagramu může mít uživatel pocit určitého „bezpečí" z pohledu například užívání instastories, což jsou fotky či videa sdílená pouze na 24 hodin, po kterých „zmizí". Samozřejmě nic na internetu jen tak nezmizí, ale může to dodat pocit, že už to následně nikdo neuvidí.

Pokud je na Instagramu nastavený účet jako soukromý, nelze na něm nic sledovat, dokud to vlastník profilu neschválí. Pokud se tak nestane, máme přístup pouze k profilové fotce a přezdívce. Na Facebooku je toto nastavení méně jednoznačné, musíme nastavit přesně, co chceme, aby neznámý na našem profilu viděl - ve většině případů je to pouze profilový obrázek a úvodní fotka profilu, případně nějaké soutěže, které musí být sdíleny veřejně. Na osobní informace jsou uživatelé skoupí v rámci sdílení veřejného obsahu.



Obrázek 9: ukázka soukromého účtu a Instagramu

Na obrázku číslo 9 lze vidět Instagramový účet, který je nastaven jako soukromý, vidíme pouze profilový obrázek, pokud je nastaven a pár informací, které si může vlastník profilu upravit dle svých potřeb, názorů a jiných. Aby někdo cizí mohl tento účet sledovat, musí nejdříve požádat o možnost tento účet sledovat. Je pak pouze na vlastníkovi účtu, zda tuto žádost povolí nebo nepovolí. V případě, že je žádost povolena vidí uživatel vše, co je na profilu zveřejněno.



Obrázek 10: ukázka veřejného profilu na Instagramu

Na desátém obrázku je ukázka z veřejného profilu na Instagramu. Tyto profily může navštívit a sledovat fotky, či videa kdokoli a nemusí dotyčný profil ani sledovat. Majitel profilu tudíž nemá téměř žádné informace o tom, kdo jeho profil prohlíží. Uživatelé Instagramu jsou v tomto ohledu hodně otevření a moc nedbají na to, kdo jejich účet sleduje.

Toto může být ovlivněno také Influencer marketingem, kdy si tito lidé vydělávají pomocí sdílení příspěvků na sociálních sítích a ostatní se jim chtějí vyrovnat. Co je přeci těžkého na vydělávání si peněz pomocí těchto sítí? Z tohoto důvodu mohou mít profily otevřené a hledat co nejvíce followers s vidinou jednoduchého výdělku.

Z dotazníkového šetření vzešly informace spíše takové, že mladiství toho moc nesdílí, že přemýšlí nad tím, co sdílí veřejně. Což svým způsobem vzešlo i z průzkumu sociálních sítích pomocí falešného účtu.

Obrázek 11: ukázka veřejného profilu na Instagramu (slečna 8 let)

Na obrázku číslo 11 lze vidět příklad, kdy má slečna otevřený účet a už jen její popis je děsivý. Slečna (v tomto případě snad ještě holčička) zde sdělila všechny možné informace, díky kterým je možné ji zkontaktovat s podobnými zájmy. Tento profil je otevřený a jsou na něm i osobní fotografie.

Obrázek 12: ukázka veřejného profilu na Instagramu (slečna 12 let)

Další ukázka veřejného profilu 12 leté slečny, která zde sděluje, kde bydlí, do jaké třídy chodí a také její koníčky. Všechny tyhle informace jsou velmi nebezpečné, i když se to nemusí na první pohled zdát.

Obrázek 13: ukázka veřejného profilu na Instagramu (slečna 11 let)

Ukázkové veřejné profily byly vybrány zcela náhodně při průzkumu sociálních sítí. Na obrázku číslo 13 je nejvíce zarážející, že 11 letá slečna si zadá do popisu sebe (svého profilu), že je svobodná.

Falešný účet vytvořený na sociální síti Facebook byl bohužel smazán, ale předtím byl proveden průzkum, ze kterého vzešlo, že sociální síť Facebook není tak populární. Zde už lidé moc věcí nesdílí, minimálně ne veřejně. Což bylo základním sledovaným ukazatelem – co lidé sdílí veřejně. Na sociální síti Facebook veřejně sdílí hlavně příspěvky s různými druhy soutěží, případně prosby o sdílení ztraceného člověka, případně zvířete.

ZÁVĚR

Při psaní bakalářské spatřil světlo světa připravovaný dokument s názvem @v_siti_film (oficiální Instagram). Jedná se o dokumentární film o zneužívání dětí na internetu. Momentálně je ve fázi hledání finanční podpory na www.hithit.cz. Na oficiálním instagramovém profilu jsou k prohlédnutí trailery z připravovaného filmu. Jedná se o dokument, kde se 3 dospělé dívky vydávají na sociální síti za 12 leté slečny. Během pár hodin se s nimi spojí nespočet dospělých mužů, kteří i přes to, že vědí kolik slečnám je (opravdu si myslí, že pouze 12) po nich chtějí video hovory se sexuální tématikou, v dokumentu dokonce k několika takovým video hovorům dojde.

S tvůrcem filmu Vítem Klusákem byl na téma přípravy filmu zveřejněn rozhovor v DVTV, kde popisuje, jak film vznikal a proč je důležité, aby tento film vidělo co nejvíce lidí.

Dokument má být vytvořen hlavně jako poslání pro dívky a jejich rodiče, kteří by měli vědět, co jejich děti na internetu dělají. Rodiče by také měli vědět, co v případě, že něco takového zjistí, udělat.

Bohužel pouze pár procent obětí se s tímto problémem někomu svěří. To vzešlo i z dotazníku, byť ohledně kyberšikany, kde se pouze pár jedinců někomu svěřilo. Rodiče, učitelé i děti by se měli v tomto ohledu více vzdělat, aby měli přehled o tom, co v takové situaci dělat a na co mají právo.

Nebezpečí sociálních sítí může být demonstrováno například na tzv. „modré velrybě“, kdy tato „hra“ připravila o život spoustu dětí. A to jen pro to, že se šířila přes sociální sítě a děti plnily, co po nich někdo na internetu chtěl. Dětem bylo vyhrožováno, pokud nesplnily všechny požadované úkoly, které nezřídka končily i smrtí dotyčného.

Je nutné si uvědomit, jak moc můžou být sociální sítě nebezpečné. Nejenom pro děti, mladistvé, ale i pro dospělé jedince. V posledních dnech vychází stále více článků na téma bezpečnost na sociálních sítí a začíná se o tomhle problému veřejně mluvit, což je důležité.

Lidé se v tomto směru musí vzdělávat a vědět, co s čím se mohou na sociálních sítích setkat. Rodiče by měli se svými dětmi mluvit a vysvětlit jim, že ony nedělají nic špatného, pokud jsou oběťmi různých věcí na sociálních sítích.

SEZNAM POUŽITÉ LITERATURY

[1] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016, 175 s. ISBN 978-80-247-5595-3.

[2] *Než přišel Facebook. Stručný průvodce historií sociálních sítí. - Internet pro všechny* [online]. Praha, 2017 [cit. 2019-04-25]. Dostupné z: http://www.internetprovsechny.cz/nez-prisel-facebook-strucny-pruvodce-historii-socialnich-siti/

[3] *The Social Network (2010)|ČSFD.cz* [online]. Praha, 2010 [cit. 2019-03-19]. Dostupné z: https://www.csfd.cz/film/262711-the-social-network/prehled/

[4] *Fenomén jmeném Facebook: prostá sociální síť, nebo tichý vizionář? - Buď FIT* [online]. Praha, 2017 [cit. 2019-03-13]. Dostupné z: https://casopis.fit.cvut.cz/tema/2-17-socialni-site/fenomen-jmenem-facebook-prosta-socialni-sit-tichy-vizionar/

[5] *Marketing & Media*. Praha: Forum Media, 2018, **2018**(40).

[6] PETROWSKI, Thorsten. *Bezpečí na internetu: pro všechny*. Liberec: Dialog, 2014, 243 s. Tajemství. ISBN 978-80-7424-066-9

[7] ŠEVČÍKOVÁ, Anna. *Děti a dospívající online: vybraná rizika používání internetu*. Praha: Grada, 2014, 183 s. Psyché. ISBN 978-80-210-7527-6. Dostupné také z: http://www.grada.cz/deti-a-dospivajici-online_7905/kniha/katalog/

[8] HOLLÁ, Katarína. *Sexting a kyberšikana.* Vydanie: prvé. Bratislava: Iris, 2016. 165 stran.

[9] BOYD, Danah. *Je to složitější: sociální život teenagerů na sociálních sítích.* Vydání první. Přeložil Lukáš NOVÁK. Praha: Akropolis, 2017, 301 s. ISBN 978-80-7470-165-8.

[10] *Defend Against Password Hacking| Veracode* [online]. Burlington MA, 2019 [cit. 2019-04-13]. Dostupné z: https://www.veracode.com/security/password-hacking

[11] *Jak si nastavit silné heslo* [online]. Praha, 2019 [cit. 2019-04-13]. Dostupné z: https://blog.avast.com/cs/jak-si-nastavit-silne-heslo

[12] *Co je vishing? -Správa.sítě.eu* [online]. Praha, 2016 [cit. 2019-05-13]. Dostupné z: https://www.sprava-site.eu/vishing/

[13] *Facebook* [online]. 2019 [cit. 2019-05-13]. Dostupné z: https://cs-cz.facebook.com/

[14] *New Instagram Logo 2019* [online]. Sydney, 2019 [cit. 2019-05-13]. Dostupné z: https://www.edigitalagency.com.au/instagram/new-instagram-logo-png/

[15] *Twitter logo Sketch freebie* [online]. Paris, 2019 [cit. 2019-05-13]. Dostupné z: https://www.sketchappsources.com/free-source/114-twitter-logo.html

[16] *Snapchat Tweaks iOS App to After Redesign Backlash - Variety* [online]. 2019 [cit. 2019-05-13]. Dostupné z: https://variety.com/2018/digital/news/snapchat-ios-app-changes-1202806822/

[17] *YouTube* [online]. 2019 [cit. 2019-05-13]. Dostupné z: https://eu.usatoday.com/story/tech/talkingtech/2019/01/25/youtube-stop-recommending-conspiracy-videos-misinform-users/2677506002/

[18] *Random Password Generator* [online]. Praha, 2019 [cit. 2019-05-13]. Dostupné z: https://www.avast.com/random-password-generator

[19] *Lidé|Sociální sítě* [online]. Česká republika, 2010 [cit. 2019-05-14]. Dostupné z: http://www.socialnisite.123abc.cz/lide

[20] *Sociální sítě* [online]. Praha: ČVUT [cit. 2019-05-15]. Dostupné z: https://www.fd.cvut.cz/personal/cvrceant/

[21] *Sociální sítě v ČR - září 2018|Marketing&Media. www.mam.cz* [online]. Praha: Forum Media, 2018, 2018 [cit. 2019-05-15]. Dostupné z: https://mam.cz/c1-66277810-socialni-site-v-cr-zari-2018

[22] *Lide.cz - Seznamka a chat* [online]. Praha: Seznam.cz, 2019 [cit. 2019-05-16]. Dostupné z: https://www.lide.cz/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BBS Bulletin Board System.

IRC Internet Relay Chat.

SEZNAM OBRÁZKŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK

Dotazník – bezpečnost sociálních sítí

Veronika Jordánová

Dobrý den,

Tímto Vás chci poprosit o vyplnění dotazníku níže. Dotazník Vám zabere pár minut a mne pomůže k napsání bakalářské práce. Dotazník je zaměřen na sociální sítě a jejich bezpečnost z pohledu mladistvých.

Děkuji za pomoc. Dotazník je anonymní. U každé otázky vyberte alespoň jednu odpověď.

1) Pohlaví
    a) Chlapec
    b) Dívka
2) Věk
    a) 10 – 12
    b) 13 – 15
    c) 16 – 18
3) Víte, co jsou sociální sítě?
    a) Ano
    b) Ne
4) Jaké sociální sítě používáte?
    a) Facebook
    b) Instagram
    c) Snapchat
    d) Youtube
    e) Twitter
    f) Jiné
    g) Nepoužívám sociální sítě
5) Kterou sociální síť používáte nejčastěji?
    a) Facebook
    b) Instagram
    c) Spnapchat
    d) Youtube

e) Twitter

f) Jiné

g) Nepoužívám sociální sítě

6) Vlastníte telefon / tablet s připojením na internet?

a) Ano

b) Ne

7) Kolik hodin denně strávíte na sociálních sítích?

a) 0

b) 1 – 3

c) 4 – 5

d) Více

8) K čemu sociální sítě používáte?

a) Ke komunikaci s kamarády (chat, messenger, direkt message, aj.)

b) Ke sdílení fotek

c) Ke sdílení nálady, statusů, citátů

9) Pokud používáte Instagram / Snapchat, využíváte možnosti Stories? Zveřejnění fotky či videa, které po 24 hodinách „zmizí“?

a) Ano

b) Ne

10) Pokud ano, zveřejňujete zde:

a) Fotky

b) Videa

c) Nic

11) Sdílíte fotky sebe? Selfies, fotky s kamarády?

a) Ano

b) Ne

12) Sdílíte svoje konkrétní informace? Bydliště, školu, kterou navštěvujete, svoji rodinu?

a) Ano

b) Ne

13) Pokud ano, proč?

    a) Aby o mně lidé věděli, co nejvíce

    b) Aby mě lépe vyhledávali moji kamarádi

    c) Protože to mají vyplněné moji kamarádi / spolužáci / známí

    d) Jen tak, baví mě to

    e) Vlastní

14) Co nejvíce sdílíte na sociálních sítích?

    a) Fotky (svoje, s kamarády, rodinou)

    b) Koníčky (jídlo, zvířata, sport,…)

    c) Osobní pocity

    d) Jiné

15) Označujete své přátele na fotkách?

    a) Ano

    b) Ne

16) Víte jak si ochránit své soukromí na těchto sociálních sítích?

    a) Ano

    b) Ne

17) Chráníte si soukromí na sociálních sítích pomocí nastavení?

    a) Ano, mám nastaveno, kdo může vidět můj obsah, co musím schválit, aby mohl někdo jiný vidět (například když mě někdo označí na fotce / v příspěvku)

    b) Ano, mám nastaveno, kdo může vidět můj obsah

    c) Nezajímám se o to / je mi to jedno

    d) Nic takového nastaveného nemám

18) Kolik máte na Facebooku / Instagramu přátel?

    a) 0 – 50

    b) 51 – 100

    c) 101 – 150

    d) 151 – 200

    e) 201 a více

19) Znáte všechny tyto lidi osobně?

    a) Ano

    b) Ne

20) Myslíte si, že se na sociálních sítích může člověk stát závislým?

    a) Ano

    b) Ne

21) Komunikovali jste někdy s člověkem, kterého jste nikdy neviděli v reálném světě?

    a) Ano jednou

    b) Ano, komunikuji s ní / ním pravidelně

    c) Ne, nikdy

22) Sdělujete tomuto neznámému kamarádovi své osobní údaje (věk, bydliště, školu, do které chodíte, informace o rodině,…?

    a) Ano, však je to můj kamarád

    b) Sdělil / a jsem pouze své jméno a minimum dalších informací

    c) Ne, nesdělil/a jsem žádné konkrétní informace kromě přezdívky, kterou používám na sociálních sítích

    d) Ne, s nikým cizím nekomunikuji

23) Zažili jste někdy vy nebo někdo ve Vašem okolí kyberšikanu? (šikana, která probíhá na internetu, na sociálních sítích pomocí komentářů, sdílení našich fotek, zesměšňování apod.)

    a) Ano

    b) Ne

24) Pokud ano, jak tato kyberšikana probíhala? Prosím popište.

    a)

25) Zažili jste někdy zesměšnění na sociální síti? Někdo nelichotivě okomentoval Vaši fotku, status, cokoli? A jak jste se s tím vypořádali?

    a) Ano, hodil / a jsem to za hlavu, stalo se to pouze jednou, nebo minimálně

    b) Ano, stalo se to sice jednou nebo minimálně, ale zasáhlo mě to a začal / a jsem o sobě pochybovat, mrzelo mě to

    c) Ano, stalo se to vícekrát, ale neřešil / a jsem to

    d) Ano, stalo se to vícekrát a řešil / a jsem to s rodiči / vyučujícím / starším bratrem či sestrou

    e) Ne, nikdy se mi to nestalo

26) Stalo se Vám někdy, že na Vás cíleně na internetu útočil jeden člověk / skupina lidí? Zesměšňující fotky, nepříjemné zprávy?

    a) Ano jednou

    b) Ano vícekrát

    c) Ne nikdy se mi toto nestalo

27) Byl to někdo, koho znáte / jste znali z reálného života?

    a) Ano

    b) Ne

28) Řešili jste tuto věc s někým dospělým?

    a) Ano s rodiči

    b) Ano s vyučujícím

    c) Ne, neřešil / a jsem to s dospělým

    d) Nikdy se mi to nestalo

29) Jak jste tuto věc řešili?

    a) Toho člověka jsem znal / a osobně a vyříkali jsme si to

    b) Tento člověk to přestal dělat sám od sebe

    c) S tímto člověkem se to řešilo ve škole a byl za to pokárán

    d) Nikdy jsem nic takového neřešil

30) Pokud se Vám něco takového stalo, co byste doporučil tomu, kdo je šikanován? Pokud ne, odpovídat nemusíte. Prosím vypište.

PŘÍLOHA P II: OBSAH DISKU CD

prilohy_dotaznik_data.csv

prilohy_dotaznik_data_ciselniky.pdf

prilohy_dotaznik_data_1-94.pdf

fulltext.pdf