Bezpečnost dětí a mladistvých na sociálních sítích

Pavel Kopczyk

Bakalářská práce
2021

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2020/2021

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Pavel Kopczyk**
Osobní číslo:	**A16498**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Prezenční**
Téma práce:	**Bezpečnost dětí a mladistvých na sociálních sítích**
Téma práce anglicky:	**The Safety of Children and Adolescents on Social Networks**

Zásady pro vypracování

1. Uveďte základní terminologii v dané problematice.
2. Rozeberte nejpoužívanější sociální sítě.
3. Popište rizika a nebezpečí při užívání sociálních sítí.
4. Pomocí dotazníkového šetření se zaměřte na množství zneužitelných informací, které o sobě uživatelé sami zveřejňují.
5. Výsledky prezentujte pomocí grafů a formou doporučení.

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

Seznam doporučené literatury:

1. KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 978-802-4755-953.
2. PETROWSKI, Thorsten. *Bezpečí na internetu: pro všechny*. Liberec: Dialog, 2014. Tajemství (Dialog). ISBN 978-807-4240-669.
3. ECKERTOVÁ, Lenka a Daniel DOČEKAL. *Bezpečnost dětí na internetu: rádce zodpovědného rodiče*. Brno: Computer Press, 2013. ISBN 978-802-5138-045.
4. ŠEVČÍKOVÁ, Anna. *Děti a dospívající online: Vybraná rizika používání internetu*. Praha: Grada, 2015. ISBN 978-802-4796-451.
1. ČERNÁ, Alena. *Kyberšikana: průvodce novým fenoménem*. Praha: Grada, 2013. Psyché (Grada). ISBN 978-802-4745-770.

Vedoucí bakalářské práce: **Ing. Dora Kotková, PhD.**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **15. ledna 2021**
Termín odevzdání bakalářské práce: **19. května 2021**

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.
DĚKAN

doc. Mgr. Milan Adámek, Ph.D. v.r.
děkan

Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 15. ledna 2021

Jméno, příjmení: Pavel Kopczyk

Název bakalářské práce: Bezpečnost dětí a mladistvých na sociálních sítích

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/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 diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/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 diplomovou/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 diplomové/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 diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/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 diplomové/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 16. 5. 2021

Pavel Kopczyk v.r.
podpis diplomanta

ABSTRAKT

Bakalářská práce se zabývá problematikou bezpečnosti na sociálních sítích, ochranou osobních údajů, využití, případně zneužití těchto údajů skupinou nebo jedincem. Práce obsahuje základní informace o sociálních sítích Facebook, Instagram, YouTube a Twitter, vysvětlení pojmů jako sociální síť, influencer, YouTube atd.

Náplní praktické části této práce je vytvoření dotazníku a zmapování benevolentnosti uživatelů sociálních sítí ke sdílení svých osobních údajů s naprosto cizími jedinci a míra jejich bezpečného chování na sociálních sítích.

Klíčová slova: Sociální síť, Facebook, Istagram, YouTube, profil, informace.

ABSTRACT

This bachelor thesis looks into problematics of security on various social media, the protection of personal data, its use and its misuse by either an individual or a group. Firstly, this work provides the basics about concrete social media channels, such as Facebook, Instagram, Youtube and Twitter. In this part, the thesis defines fundamental terms, for example it enables a definition for social network, influencer or Youtube amongst others. Secondly, this thesis is analysing the vulnerability of children on the Internet and the quantity of exposure to potential danger. Thereby, the purpose of the practical part of this work is to create a questionnaire and map how users of social networks are benevolent to sharing their personal data with the strangers and whether they behave safely on social networks.

Keywords: Social network, Facebook, Istagram, YouTube, profile, information

PODĚKOVÁNÍ

Rád bych poděkoval Ing. Doře Kotkové, PhD. za cenné připomínky, odborné vedení při zpracování bakalářské práce a své rodině za podporu a shovívavost. Také děkuji pedagogům na základních školách a víceletých gymnáziích za poskytnuté informace v dotaznících, které mi umožnily napsat tuto práci.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Sociální sítě se staly za posledních deset let nedílnou součástí našich životů, především u mladší generace. Děti a mladiství tráví na sociálních sítích značnou část svého volného času. Sociální sítě nabízejí uživatelům komunikaci s přáteli, hraní her, seznámení se s novými lidmi, sdílení dat, získávání informací, možnost vyjádřit se anonymně k jakémukoliv tématu s jakýmkoliv výrokem. V mnoha směrech jsou současné sociální sítě prospěšné, pokud jsou využívány správně.

Děti a mladiství jsou na sociálních sítích nejzranitelnější skupina, především proto, že hůře rozeznávají, a mnohdy podceňují, rizika a nebezpečí sociálních sítí. Na sítích se následkem toho chovají nezodpovědně – přidávají si do přátel téměř kohokoliv, klikají na různé odkazy, jejichž obsah je určen výhradně dospělým, jejich profily bývají veřejné i potenciálním nepřátelům, sdílejí zbytečně příliš mnoho soukromých informací. Snadno se poté stávají oběťmi obtěžování, zneužívání, kyberšikany, vydírání nebo ztráty soukromí a osobních údajů.

Teoretická část bakalářské práce je zaměřena na základní terminologii v oblasti sociálních sítí, jsou zde uvedeny a rozebrány nejpoužívanější sociální sítě. Dále se práce zaměřuje na hrozby a nebezpečí při užívání sociálních sítí, na jejich prevenci a případné řešení následků daných hrozeb.

V praktické části bude pojednáno o sběru a výsledcích empirického materiálu. Byl proveden kvantitativní výzkum a částečně i kvalitativní výzkum. Empirický materiál byl získán formou dotazníkového šetření a dílčí část pomocí profilů na sociálních sítích. Cílem praktické části je zjištění, jak jsou uživatelé na sociálních sítích benevolentní ke sdílení soukromých údajů, zda se chovají na sociálních sítích bezpečně a kolik na nich tráví času.

Cílem této práce je informovat děti a mladistvé o možných rizicích, které sociální sítě představují, jak takovým rizikům předcházet a, jak řešit jejich následky.

TEORETICKÁ ČÁST

1 SOCIÁLNÍ SÍTĚ

Sociální síť je služba provozovaná na internetu. Svým členům umožňuje založit a upravovat vlastní profil a zároveň komunikovat s ostatními členy. Uživatelé mohou kromě komunikace s ostatními také sdílet různé odkazy, videa, fotky a další informace. Drtivou většinu informací na sociálních sítích produkují samotní uživatelé. Dochází k propojení lidí pomocí jejich kontaktů v telefonu, e-mailu nebo na základě shodných pracovních či přátelských vztahů. [1]

V současné době má přístup k internetu 59 % světové populace. Sociální sítě využívá 49 % lidí, což znamená, že více než 83 % lidí, kteří mají internet, využívají sociální sítě. Průměrný uživatel internetu stráví 6 hodin a 43 minut na internetu každý den, z čehož více než jednu třetinu stráví na sociálních sítích. Z toho vyplývá, že sociální sítě jsou velmi podstatnou součástí našich životů. [2]

1.1 Facebook

Facebook je americká internetová společnost se základnou v Kalifornii. Byla založena studenty Harwardu Markem Zuckergergem, Eduardem Savarinem, Dustinem Mozkowitzem a Chrisem Hughesem. Nejdříve to měla být sociální síť pouze pro studenty Harwardu. Díky její oblibě se postupně rozšířila na další vysoké školy. Následně začali tuto sociální síť využívat mladiství starší 13 let. Dnes je na Facebooku více než 2 a půl miliardy minimálně jednou měsíčně aktivních uživatelů.

Na tuto sociální síť se člověk může přihlásit v podstatě z jakéhokoliv zařízení využívajícího internet, jako je počítač, tablet, mobil, některé funkce je možné ovládat pomocí hodinek. Po registraci jsou uživatelé vyzváni k vložení konkrétních informací o sobě, jako např. fotografie či alba s fotografiemi, datum narození, atd. Tyto informace mohou vidět všichni uživatelé, pokud máte nastavený veřejný profil, nebo pouze osoby, které jste si přidali do přátel. Záleží na vašem nastavení soukromí. [3]

1.1.1 Messenger

Facebook Messenger (běžně známý jako Messenger) byla původně aplikace pro bezplatné zasílání zpráv (Facebook Chat) vyvinutá v roce 2008 společností Facebook, Inc. V roce 2011 společnost vydala samostatné mobilní aplikace pro

iOS a Android. V rámci dalšího rozšiřování služeb (např. bezplatné hlasové hovory a videohovory) vyvinula společnost Facebook nové aplikace na různých operačních systémech. Spustila také vyhrazené webové rozhraní (Messenger.com), čímž oddělila zasílání zpráv a zprostředkovávání hovorů od hlavní aplikace na Facebooku, která uživatelům umožňuje používat webové rozhraní.

Uživatelé mohou odesílat a přijímat zprávy, sdílet fotografie, videa, samolepky, animace (tzv. gify), emotikony, zvukové záznamy a soubory. Lidé si oblíbili reagovat na zprávy ostatních uživatelů pomocí vložení jednoho symbolu, hrát hry a využívat tyto atributy také v rámci skupinových konverzací a hraní her. [3]

1.2 Instagram

Instagram je bezplatná online aplikace primárně určena pro sdílení fotografií. Jedná se o jednu z největších sociálních sítí vůbec, oblíbenou zejména mezi dětmi a mladistvými. V roce 2012 byla původní společnost Burbn, Inc., ve které projekt Instagram vznikl, prodána Facebooku.

Instagram umožňuje uživatelům upravovat a nahrávat fotografie a krátká videa prostřednictvím mobilní aplikace. Uživatelé mohou ke každému ze svých příspěvků přidat titulek a tzv. hashtagy pro snadnější/cílené vyhledání příspěvku ostatními uživateli. Hashtag, neboli klíčové slovo, je označován symbolem # a vkládají se do něj slova, která nejlépe vystihují daný příspěvek. Každý příspěvek uživatele se objeví na Instagramu všem, kteří sledují uživatelův profil. Je-li profil uživatele veřejný a je-li příspěvek označen hashtagem, může být zobrazen jakýmkoliv jiným uživatelem. Uživatelé mají možnost nastavit svůj profil také jako soukromý. Příspěvky soukromého profilu uvidí pouze lidé, kterým sledování profilu bylo předem schváleno iniciátorem/autorem příspěvku. Tohle omezení však není zárukou toho, že příspěvek, který uživatel umístí v síti internetu, nebude prostřednictvím jeho schválených sledujících, tzv. followerů, šířen dál k eventuálnímu zneužití.

Obdobně jako u jiných platforem sociálních sítí mohou uživatelé Instagramu používat, komentovat a přidávat do záložek další příspěvky a posílat soukromé zprávy svým přátelům prostřednictvím funkce Instagram Direct. Fotografie lze sdílet na jedné nebo několika dalších sociálních sítích (Twitteru, Facebooku) jediným kliknutím.

Instagram není jen nástrojem pro jednotlivce, ale také pro podniky. Aplikace pro sdílení fotografií nabízí společnostem možnost založit si bezplatný obchodní účet na propagaci své značky a produktů. Společnosti s firemními účty mají přístup k metrikám interakce zdarma. Podle webové stránky Instagramu používá více než 1 milion inzerentů po celém světě Instagram k dosahování obchodních výsledků. Zvláště díky snadnému propojení na jiné sociální sítě má tento trend propagace firem na rozdíl např. od tištěných periodik perspektivu i do budoucnosti. [4]

1.3 Twitter

Twitter je sociální síť, která funguje na základě sdílení krátkých zpráv, videí, obrázků či odkazů. Těmto krátkým sdělením se říká "tweety" (pípnutí). Pokud se některému dalšímu uživateli líbí určitý „tweet", může ho „retweetnout", neboli přeposlat svým sledujícím. Tento způsob vede k rychlému předání zajímavých informací co největšímu počtu lidí. U příspěvků lze použít „@" pro označení jiného uživatele, či hashtag (#) pro členění témat. [5]

1.4 YouTube

YouTube je internetová služba pro sdílení videí. Uživatelům umožňuje sledovat videa zveřejněná jinými uživateli a nahrávat vlastní videa. Tato služba byla vytvořena jako nezávislý web v roce 2005 a už o rok později byla zakoupena společností Google. Videa, která byla nahrána na YouTube, se objevují nejen na webu YouTube, ale mohou být prostřednictvím odkazů zveřejněna také na jiných webech, nejčastěji např. na sociální síti Facebook a různých periodikách. [6]

Sloganem webu YouTube je „Vysílejte sami sebe" [6]. To znamená, že služba YouTube je určena pro všechny, kteří chtějí publikovat svá videa. Z obsahu webu je zřejmé, že drtivou většinu videí skutečně vytvářejí a nahrávají amatéři. Je to dáno jednak tím, že prostředí YouTube je uživatelsky přívětivé, a také tím, že technika umožňující sdílení a nahrání videí je běžně dostupná a má v sobě již zabudované funkce, které výše zmíněné podporují.

Videa YouTube zveřejňují lidé z celého světa, ze všech typů prostředí. Mezi příklady patří amatérské filmy, hudební videa, sportovní přenosy, ukázky služeb, výrobků a další

zábavné či propagační události zachycené na videu. Lidé také používají YouTube ke zveřejňování instruktážních videí, a to v podstatě z jakékoli oblasti lidské činnosti. Najdeme zde například podrobné postupy k vytváření webových stránek, k obsluze počítačů a tiskáren, ke grafickým programům, ale třeba také kuchyňské recepty, návody ke skládání lega, k opravě automobilu atd. Další z možností, jak využít služby YouTube, je skutečnost, že společnost Google nabízí sdílení příjmů z reklamních kliknutí generovaných na stránkách s videem. Podmínkou k uveřejnění reklamy od společnosti Google je určitý počet zhlédnutí a odběratelů konkrétního kanálu YouTube. Někteří uživatelé tak z umístění reklam na svých videích generují finanční zisk.

Závěrem lze konstatovat, že vzhledem k dostupnosti technického vybavení a výše zmiňovanému přívětivému uživatelskému prostředí má tato služba dopad i sociální. Lidé by si měli být vědomi toho, že cokoli, co dělají na veřejnosti, může kdokoli zachytit na video a umístit na YouTube. Hlavní hrdina takového videa se sice může bránit, ale nikdo už mu nezaručí, že inkriminované video z internetu zmizí. [6]

1.5 TikTok

TikTok je sociální síť dříve známá jako musical.ly. Je to mobilní aplikace, na které mohou uživatelé sledovat, nahrávat, či sdílet krátká videa. Aplikaci používají zejména mladí lidé pro zábavu. Na TikToku nalezneme krátká videa od třívteřinových do minutových, kde uživatelé tancují, zpívají, sdílejí různá komická videa, nebo videa, jak něco vyrobit. Aplikace je vlastněna a vyvíjena čínskou společností ByteDance. Kvůli vlastnictví čínskou firmou měla aplikace problém v ostatních státech kvůli obavám o zneužití osobních údajů čínskou vládou. [7]

Závěrem lze konstatovat, že obliba sociálních sítí mezi mladými rok od roku stoupá. Dnešní mládež využívá sociální sítě ve svém volném čase pro zábavu a také v rámci školních povinností pro kontakt se spolužáky, pro domlouvání setkání s kamarády a vrstevníky, a v neposlední řadě i pro vyhledávání nových kontaktů k seznámení. Pro děti a mladistvé jsou sociální sítě již od jejich útlého dětství běžnou součástí jejich životů.

2 ZÁKLADNÍ TERMINOLOGIE V DANÉ PROBLEMATICE

V této kapitole je rozebrána základní terminologie, především bezpečnost jako taková, je vysvětleno, kdo je youtuber a influencer. Jsou objasněny pojmy jako fake news, sexting a kyberšikana.

2.1 Bezpečnost

Slovo bezpečnost pochází z latinského securitas, což znamená jistota, záruka, duševní pokoj. Je to stav, ke kterému dochází, když se subjekt necítí být v ohrožení, a to z hlediska svého zdraví, zájmů, hodnot nebo své existence. Dá se definovat i jako stav beze strachu o sebe, o druhé, o budoucnost či o ztrátu života nebo majetku. [8]

Bezpečnost můžeme rozlišovat na vnitřní a vnější. Vnitřní bezpečnost lze charakterizovat jako tu, kterou můžeme ovlivnit tím, že se budeme neustále připravovat na hrozby, které nás ohrožují, a eliminovat je. Vnější bezpečnost spočívá hlavně na vnějších rizicích, například vojenského či politického rázu. [8] Bakalářská práce se zaměřuje zejména na vnitřní bezpečnost dětí a mladistvých na sociálních sítích, kterou sami děti ovlivňují tím, jak se na sociálních sítích chovají. Ale i rodiče těchto dětí jí mohou ovlivnit tím, že znají hrozby, které sociální sítě skýtají a že své děti na tyto hrozby upozorňují a předcházejí jim.

2.2 Fake news

Fake news, česky falešné zprávy, je označení pro různé dezinformace či hoaxy. Základním stavebním prvkem fake news jsou dezinformace, což znamená záměrně vymyšlené nepravdivé informace. Falešné zprávy jsou vytvářeny účelově a vědomě, nejedná se tedy o chybu či překlep. Jsou vytvářeny za účelem zmanipulovat a ovlivnit příjemce zprávy. Nejčastěji se vyskytují na dezinformačních webech nebo sociálních sítích, kde někteří uživatelé, aniž by jakkoli kontrolovali pravdivost informace, sdílí dezinformace i na ostatních sociálních sítích, tím pádem se bohužel stává, že se smyšlené zprávy šíří rychleji než pravdivé informace. Dalším z důvodů velkého a rychlého šíření hoaxů je snaha o zvýšení výnosů z inzerce (reklamy), kterou si u dezinformačních článků zaplatí různé obchodní společnosti. Dezinformace jsou velmi často o hodně diskutovaných tématech, jako je například migrace, rasismus, vlivu

totalitních zemí, jako jsou Rusko a Čína, na naši vnitřní politiku a naše politiky apod. [9]

2.3 Influencer

Influencer je slovo odvozené z anglického influence, což znamená vliv. Je to osoba, která ovlivňuje významné množství lidí. Většinou se s nimi setkáváme na sociálních sítích, jako je Instagram nebo YouTube. Influenceři na těchto sítích bývají označováni za Instagramery nebo YouTubery, ale mohou to být i různé slavné osobnosti, jako jsou sportovci, herci, politici, rockové hvězdy atd. [10] Pro mnoho z těchto lidí tvoří influencing značnou část příjmů, ať už v podobě propagace různých výrobků či služeb, nebo pouze například díky oblečení, které nosí. Za což jsou odměněni reklamními společnostmi.

2.4 YouTuber

YouTuber je kdokoliv, kdo přidává obsah v podobě videí, kde sám vystupuje, na sociální síť YouTube. Tuto činnost dělá opakovaně.[11]

V dnešním světě se pomalu každé malé dítě chce stát YouTuberem a vydělávat spousty peněz na reklamě. Natočí pár vlastních videí po vzoru svých oblíbených YouTuberů, ale protože jejich videa nemají dostatečnou kvalitu nebo pouze proto, že jejich videa nemají velkou sledovanost, brzy je taková snaha omrzí. Přesto zůstávají pasivními diváky slavných a úspěšných YouTuberů, ať už je hodnota jejich příspěvků jakákoliv.

2.5 Kyberšikana

Kyberšikana se dá chápat jako úmyslné agresivní chování individua nebo skupiny lidí prostřednictvím internetu vůči člověku, který se může jen stěží takovým útokům bránit. Nejčastějšími důvody pro kyberšikanu je odplata, dalším důvodem je, že si to oběť (z pohledu útočníka) zaslouží, a dále, že to byl pouhý žert, který neměl nikomu ublížit. Pojem kyberšikana je velmi úzce spjatý s klasickou šikanou, s jediným rozdílem, že šikana probíhá v reálném svět, útočník verbálně či fyzicky napadá oběť z očí do očí. Zatímco kyberšikana probíhá v internetovém prostředí. [12]

2.6 **Sexting**

Sexting je spojení dvou slov, jedním je sex a druhým texting, což je psaní si s někým. Sexting proto znamená posílání si zpráv, fotek nebo videí, která mají sexuální podtext. [13]

Tato kapitola pojednává o bezpečnosti jako takové. Dále o falešných zprávách, influenceřích a youtuberech. Fake news jsou a budou velkým problémem, protože jsou již vytvářeny tak promyšleně, že se falešná zpráva zdá být na první pohled naprosto pravdivá. Dětí a mladiství jsou velmi důvěřiví a naivní, ještě nemají takové životní zkušenosti, aby se nad zprávou kriticky zamysleli, případně si ji ověřili z jiných zdrojů. Tomu bohužel napomáhají i někteří influenceři a youtubeři, kteří umí velmi sofistikovaně podat falešnou zprávu tak, že je velmi uvěřitelná. Tím že používají ta správná slova a opírají se hlavně o pravdivou část falešné zprávy, zmatou mnoho lidí natolik, že uvěří například, že je země placatá. Dále je v kapitole popsáno co to je kyberšikana a sexting.

3 DĚTI A MLADISTVÍ

Děti, osoby do 15 let, ale především mladiství, osoby od 15 do 18 let, tráví na internetu čím dál více času. Dle evropského průzkumu, který byl zaměřen na děti on-line, tráví děti od 9 do 16 let na internetu průměrně 167 min denně, což je téměř dvojnásobek času, který podle stejného průzkumu na internetu trávili před 10 lety (88 min). Nejvíce času tráví děti sledováním videí, posluchem hudby, komunikací s kamarády a rodinou, navštěvováním sociálních sítí. Čas strávený na internetu dnes bude ještě vyšší, kvůli epidemii, se velká část školních povinností přesunula do internetového prostředí. Čím více času stráví děti na internetu, tím větší je riziko, že se budou muset potýkat s nějakou nepříjemnou situací, ať už to je sexting, kyberšikana apod. Ve většině evropských zemí méně než 10 % mladistvých nahlásilo, že se stali obětí kyberšikany, přibližně pětina z těchto útoků měla velmi nepěkný průběh a na oběti velmi neblahý dopad. V mimořádných situacích může on-line šikana skončit i sebevraždou oběti. [14]

3.1 České děti a mladiství on-line

Téměř všechny děti od 9 let mají denně přístup na internet. Zajímavé je, že některá běžně obávaná rizika české děti příliš nerozruší. Např. 78 % dětí bylo nadšeno a dalších 10 % nebylo rozrušeno po osobním setkání s člověkem, kterého znali pouze z internetu. Většina ze setkání byla s vrstevníky, ale ze 7 % procent se děti setkávaly i s dospělými. [14]

Zajímavé je i šetření České rady dětí a mládeže, kde zjistili mnoho šokujících faktů, jako například, že třetina dotazovaných ví o někom, kdo prodává své nahé fotografie, nebo že čtvrtina dotázaných zažila situaci, kdy jejich spolužák nebo kamarád byl šikanován kvůli svým fotkám zveřejněným na internetu. Ještě více alarmující je ale fakt, že dnešní teenageři si často pořizují svoje nahé fotky nebo videa. Jedna třetina dotázaných poslala své nahé fotky partnerovi a 7 % z nich na to doplatilo. Z důvodu pomsty totiž jejich fotky či videa partner zveřejnil. 12 % dotázaných uvedlo, že poslali svou nahou fotku někomu, kdo je o to požádal, aniž by ho osobně znali, a 9 % respondentů poslalo svou nahou fotku někomu, koho osobně neznají a kdo jim za to zaplatil. [15]

Česká republika se z hlediska bezpečnosti dlouhodobě řadí do první desítky nejbezpečnějších zemí. Snad právě tato skutečnost je důvodem, že se české děti a mladiství necítí být ohroženi a že berou na lehkou váhu rizika, která on-line prostředí přináší.

4 HROZBY SPOJENÉ S UŽÍVÁNÍM SOCIÁLNÍCH SÍTÍ

Hrozeb na sociálních sítích existuje celá řada. V následujících podkapitolách jsou vypsána hlavní nebezpečí, která skýtají sociální sítě a na která je potřeba si dávat pozor.

4.1 Kyberšikana a vydírání

Kyberšikana je účelový útok na jednotlivce nebo na skupinu lidí v rámci kyberprostoru. Mnohdy to začíná jako hloupý vtip, ponižující přezdívky, vulgarismy, nadávky v komentářích, zakládání falešných profilů. Často se pojí s klasickou šikanou. Ti, co jsou šikanovaní off-line, bývají často šikanováni také na internetu. Ale kyberšikana může přijít odkudkoliv a kdykoli. Bohužel s rozvojem moderních technologií a chytrých mobilů se ke kyberšikaně uchyluje čím dál více dětí a dospělých, kteří využívají internetového prostoru sociálních sítí k praktikování tohoto jednání. Některé výzkumy uvádějí, že se s kyberšikanou setkalo až 50 % dětí. Webové stránky a sociální sítě jsou běžnými místy, kde dochází k šikaně na internetu. Kyberšikana se na sociálních sítích vyskytuje formou psychické šikany, k níž lze zařadit provokování, vyhrožování či ponižování, urážení, pomlouvání. Například se jedná o zveřejňování ponižujících záznamů - nedůstojné fotografie či videa buď vložené samotným vlastníkem, nebo uživatelem, jenž chce dotyčného poškodit. Pomlouvání a různé formy ponižování za použití falešných profilů a s tím spojené krádeže identity, či provokace, útoky na uživatele v průběhu on-line komunikace, diskuze, zveřejňování cizích informací s cílem uškodit oběti. Do kyberšikany lze počítat i vyloučení z virtuální komunity. [16]

4.2 Manipulace skrze sociální sítě

Sociální sítě manipulují svými uživateli. Jedná se sice o malou a nenápadnou manipulaci, ale z dlouhodobého hlediska to může být velmi nebezpečné. Již dnes se zdá, že sociální sítě mění svět ve smutnější, mrzutější, čím dál více rozdělující společnost. Zároveň ničí u lidí schopnost rozpoznat pravdu, a to kvůli záplavě lživých, nepravdivých nebo zavádějících příspěvků, které někteří uživatelé bez jakéhokoliv ověření pravdivosti, relevantnosti sdílejí dál.

Společnosti poskytující sociální média získávají zdroje příjmů tím, že nabízejí společnostem údaje o svých uživatelích, kteří jsou pomocí těchto údajů lehce

manipulováni. Nejznámějším příkladem manipulace uživatelů sociálních sítí je společností Cambridge Analytica, která díky informacím o desítkách milionů uživatelů Facebooku významně ovlivnila volby v několika zemích, zejména ve Spojených státech amerických. Společnost využila privátní data uživatelů, na které následně cíleně distribuovala politickou reklamu. [17]

4.3 Deprese, úzkost

S nástupem sociálních sítí, kolem roku 2011, se zejména u dívek, které se narodily po roku 1995 (generace Z), velmi zvýšilo riziko duševních onemocnění, jako například deprese a úzkost, a s tím i riziko sebepoškozování a sebevražd. A to ze tří hlavních důvodů. Prvním je, že mladé dívky se vždy porovnávaly s různými herečkami, modelkami apod., ale na sociálních sítích jsou i jejich kamarádky, vrstevnice, které když použijí nějaký filtr, nebo si upraví rty a oči, tak vypadají mnohem lépe než ve skutečnosti. Kvůli tomu se dnešní mladé dívky mohou cítit, že jsou ošklivé. Dalším důvodem je, že teenagerky nechtějí zůstávat pozadu, být vynechány, nezapadat do kolektivu. Třetím a možná nejdůležitějším důvodem je, že pomocí sociálních sítí se dá lehce šikanovat. Dívky totiž nejsou jako chlapci, kteří si většinou všechno vyřeší osobně, maximálně se někdy poperou. Dívky šikanují ostatní dívky ničením sociálních vztahů, například pomluvami, šířením lží, polopravd apod. a to jim sociální sítě umožňují v podstatě odkudkoli, kdykoli a s anonymitou falešného účtu. I proto se míra duševních onemocnění, jako například deprese u dnešních mladých dívek zvedla z 5 % v roce 2012 na 15 % v roce 2016. Pouze během 4 let se míra těchto duševních onemocnění ztrojnásobila. Což má za následek také větší míru sebepoškozování a v některých případech i sebevraždu deprimované dívky. [18]

Za zmínku stojí šest let starý případ tehdy osmnáctileté hvězdy Instagramu Australanky Esseny O'Neill, která měla na svém instagramovém účtu přes 500 000 sledovatelů (followerů) a jednoho dne se rozhodla emotivně promluvit, že to, co na Instagramu dělá, propaguje, fotí, není skutečné, že už dále nechce být součástí tohoto klamu. Ve svém videu řekla vše o temné stránce sociálních médií a upravila si popisky u svých fotografií na ty „více reálné“. Instagram ji zanechal prázdnou - protože ten, koho lidé obdivovali, nebyla ona -, a s touhou závislou po lajcích. Na svém profilu smazala více než 2000

fotografií, které podle ní nebyly skutečné. Založila webovou stránku, která měla bojovat proti nezdravému kultu sociálních médií. [19]

4.4 Vystavení nevhodnému obsahu

Dnešní malé děti jsou často na sociálních sítích vystavovány nevhodnému obsahu. Nevhodným obsahem se rozumí agresivní, násilné nebo nenávistné příspěvky, sexuální narážky, komentáře nebo obrázky. V průměru 25 % evropských dětí bylo vystaveno nevhodnému obsahu, který je obtěžoval, urážel nebo rozesmutnil během roku 2019. [14]

4.5 Sexting

Děti a mladiství se na sociálních sítích mohou setkat i se sextingem, kdy si přes sociální síť posílají fotografie, videa nebo zprávy se sexuálním kontextem. Dnešní děti a mladiství si posílají takový materiál hlavně v rámci vztahu. Přítel pošle přítelkyni svou intimní fotografii a ona mu pošle svou. Najdou se ale i tací, kteří své intimní fotografie či videa pošlou neznámé osobě dokonce v tentýž den, kdy se s danou osobou v internetovém světě seznámí. Sexting má několik rizik. Největším rizikem je, že pokud někomu pošleme své intimní fotografie, videa či zprávy, nemáme nikdy jistotu, že nebudou zneužity. V případě zveřejnění citlivého materiálu musíme mít na paměti, že už nikdy nepůjde smazat. Děti a mladiství, kteří sextingují, mohou být trestně stíháni za výrobu a jiné nakládání s dětskou pornografií. [13]

4.6 Závislost

Závislost je velký problém u sociálních sítí, protože algoritmy, které sociální sítě využívají, jsou vytvářeny tak, aby byly návykové. Tím pádem čím více času strávíme na sociálních sítích, tím více zvyšujeme riziko, že se na nich staneme závislými. Velkým problémem to může být hlavně u dnešních dětí a mladistvých, protože vyrostly v době, kdy jsou už sociální sítě samozřejmostí. Používají je již od útlého dětství, proto ani nevědí, že jsou na nich závislé.

S tímto problémem se pojí i další hrozby zdravotních problémů, protože celkově děti a mladiství tráví na počítačích a chytrých telefonech mnohem více času než

předchozí generace. Kvůli velkému počtu hodin strávených ve virtuálním světě každý den se zvyšuje riziko zdravotních problémů, jako jsou bolesti hlavy, zad, kloubů, obezita nebo onemocnění očí či šlach. [17]

4.7 Sociální inženýrství

„Internet jako takový je bezpečný, nebezpeční jsou na něm jen lidé.“ [20] Kteří vymýšlejí způsoby, jak dosáhnout „svého“. Sociální inženýrství je proces manipulace lidí za účelem vytěžení informace a uskutečnění určité akce. Útoky jsou vedeny manipulativně, přesvědčivě a bývají uskutečněny buď náhodně, nebo na konkrétní osoby. Sociální inženýři neustále vylepšují své útoky a daleko lépe se umí sžít s prostředím, jelikož jsou často poučeni ze svých chyb. Oběť může být pečlivě vytipována podle věku, pohlaví, zájmů a dalších jiných kritérií. [20]

4.7.1 Ideální dosažení cíle sociálního inženýra

Ideální dosažení cíle sociálního inženýra je velká důvěra ze strany oběti. Pokud se jedná například o sociálního inženýra, který se snaží vylákat z oběti fotky s erotickou tématikou, ideálním stavem pro něj je, když mu oběť věří natolik, že mu sama chce posílat své nahé fotky. Převážně je tohoto stavu dosaženo u chlapců, kteří věří, že doopravdy komunikují s hezkou slečnou, ne se sociálním inženýrem, a sami nabízejí výměnu fotek s erotickou tématikou.

Jelikož sociální inženýři mají neustále modernější finty, odhalení bývá o to těžší. Zajímavé je, jak sociální inženýr dosahuje svého cíle prostřednictvím třetí osoby. Predátor se vydává za třetí osobu, chlapce, který píše náhodné dívce, že prohrál sázku, která spočívala v tom, že musí poslat fotografie své holky ve spodním prádle, a jelikož dotyčný žádnou slečnu nemá, osloví na sociální síti dívky své cílové skupiny s dotazem, zda by mu nějakou takovou fotku nezaslaly, s tím, že jí za její ochotu nabídne finanční odměnu. V očích oběti se jeví jako „slušný kluk“, který je pouze single a prohrál sázku. [20]

4.7.2 Sociální inženýři, nabídky, výmluvy, jejich technika

Útočníci/predátoři ne vždy oslovují pouze zprávou či žádostí o přátelství. Často stačí umístit nějakou výzvu/ dotaz do veřejných diskuzí a chatů, jak tomu bylo donedávna

třeba na serveru Lide.cz, který ukončil k 14.12.2020 po 23 letech svůj provoz. Jeden z důvodů ukončení bylo právě i mnoho falešných profilů se sexuálními podtexty v chatovacích místnostech typu:

„Zajištěný manažer hledá dívku, která by se nechala rozmazlovat.“ [20]

„Hledám klučinu 12-14 let, co se nudí jako já, bez fotky nepsat.“ (Děti si málokdy vymezují hranici, pokud si chtějí jen popovídat).[20]

„Byla jsem se ptát na práci v KFC, ale tam brigádníky nehledají.“ (Nadhozená nabídka, po níž následují nabídky sexu za úplatu. [20]

Sociální inženýři bývají mnohdy blokováni administrátory a je možné na první pohled rozpoznat jejich falešný profil, u jiných je odhalí až znalec v oboru. Nejčastěji jsou to muži mezi 30 až 40 lety, převážně svobodní nebo rozvedení, středoškolského či základního vzdělání. Někteří z nich jsou úplní začátečníci a je možné je odhalit dle napodobující mluvy dítěte. V mnoha případech se jedná o muže s nízkým sebevědomím, postižené jedince.

Druhou skupinou jsou pro změnu muži s velice vysokým intelektem, jako např. učitelé, trenéři, kteří své oběti dobře znají a o to více s nimi můžou manipulovat. Za zmínku stojí případ dvou skautských vedoucích „Piškota a Meluzína“, kteří v rozmezí pěti let zneužili přes 40 svých svěřenců, a to velmi chytrou propracovanou formou. Jelikož vedli chlapecký oddíl Bobrů, přidávali si členy svého oddílu pod falešnými profily dívek na sociálních sítí do přátel, komunikovali s nimi a snažili se z nich vylákat erotické fotografie. Následně je „ony dívky“ vydíraly, že fotografie zveřejní, pokud jim nezašlou další, tentokrát s homosexuální tématikou. Chlapci byli smutní, nevěděli, co dělat, tak se svěřili svým oddílovým vedoucím, kteří jim nabídli „pomoc“, a to takovou, že videa natočí společně s nimi. Soud je následně poslal do vězení na 10 let. Na případu se ukazuje, jak vše bylo propracované do posledního detailu a jak snadné je pro děti věřit „lidem“ na druhé straně internetu, když jsou jim schopny zasílat své nejdůvěrnější fotografie. [20]

4.7.3 **Phishingové útoky**

Existuje také nebezpečí phishingových útoků. Phishing je podvodná technika, která se využívá k získání citlivých informací, jako je např. heslo nebo číslo kreditní karty. Uživatel může obdržet e-mail, který vypadá, že pochází ze sociálních sítí, ale ve skutečnosti vybízí k návštěvě falešných webů, kde uživatel zadá svoje citlivé údaje. Problémem u falešných webových stránek je, že na první pohled vypadají totožně s originální webovou stránkou například internetového bankovnictví. Ti, kteří mají účet na sociálních sítích, jsou často cílem takových útoků. Oběti může být řečeno, aby vložila údaje na podvodný web. [20]

4.7.4 **Pretexting**

Pretexting je technika sociálního inženýrství podobná phishingu, kde se útočník snaží získat důvěrné informace. Hlavním rozdílem je však předem připravený scénář, který útočník používá k ošálení oběti, aby mu sama poskytla své cenné informace. Útočník se většinou vydává za autoritu, jako například správce sociální sítě, policii nebo úřad. Útočník si musí udělat nejdříve průzkum, k čemuž se skvěle hodí sociální sítě - například k zjištění telefonního čísla, něco o přátelích a od přátel dané osoby, kterou sleduje, co se jí líbí a podobně. Poté si připraví scénář, který oběti nebude připadat podezřelý. To znamená, že postava, za kterou se útočník vydává, musí být věrohodná, stejně jako situace, kterou vytvoří. Proto musí útočník o oběti znát co nejvíce co nejkonkrétnějších detailů ještě dříve, než se s obětí seznámí, aby pro něj bylo jednodušší oběť přesvědčit, aby se vzdala svých citlivých údajů. Někteří pretexteři dokonce falšují telefonní číslo nebo e-mailovou doménu, aby vypadali důvěryhodněji. Často pretexteři neútočí pouze na jednotlivce, ale na celé společnosti a firmy, které mají větší finanční prostředky. Například se vydávají za prodejce, kterému společnost pravidelně zasílá platby. Díky informacím z profilů sociálních sítí nebo jiných veřejných zdrojů se jim podaří přesvědčit zaměstnance odpovědného za platby, aby změnil informace o bankovním účtu pro dodavatele. [21]

4.8 Ztráta času a ztráta produktivity

Pro mnoho zaměstnanců je obtížné se v zaměstnání soustředit, musejí být přihlášeni ke svému účtu, zveřejňovat aktualizace apod. Mnoho zaměstnanců kvůli tomu přišlo o práci, jelikož to ovlivňuje jejich produktivitu. [22]

4.9 Krádež identity

Dalším nebezpečím, které mohou weby sociálních sítí představovat, je krádež identity. Na webových stránkách mohou lidé předstírat a měnit o sobě své údaje (např. o věku) a všelijak podvádět, aby jim ostatní uživatelé sdíleli své osobní údaje, stahovali malware (škodlivý software) nebo poskytovali přístup na omezené stránky. Webové stránky sociálních sítí vybízejí uživatele k zadávání a sdílení co největšího množství dat. Útočník může z příspěvků nashromáždit tolik informací, kolik potřebuje, aby naplánoval např. útok pomocí sociálního inženýrství. [22]

4.10 Ztráta soukromí

Osobní údaje zveřejněné na sociální síti může využívat kdokoli, protože jsou přístupné veřejnosti. Webové stránky, jako jsou sociální sítě, pravidelně zálohují své databáze. Proto informace shromážděné o uživateli nebo zveřejněné v průběhu času samy nikdy nezmizí úplně, protože se zálohují a trvale ukládají do webového systému. Lze to považovat za trvale viditelné.

Jakmile jsou jednou informace zveřejněny na sociálních sítích, nejsou již soukromé a mohou být volně přístupné ostatním. Veřejný profil umožňuje ostatním uživatelům vidět a komentovat, vše co na svém profilu zveřejníte.

Některé sociální sítě prodávají data svých uživatelů ostatním organizacím, jako například různým reklamním společnostem. Proto může docházet k narušení soukromí i tímto způsobem. [22]

Závěrem lze tedy konstatovat, že hrozeb spojených s užíváním sociálních sítí je spousta. Nejčastějšími riziky z výše vypsaných jsou manipulace skrze sociální sítě a závislost na sociálních sítích, vystavení nevhodnému obsahu při užívání sociální sítě.

PRAKTICKÁ ČÁST

5 METODOLOGICKÁ VÝCHODISKA

Pro svou práci jsem si zvolil přístup jednak kvantitativní, tím, že jsem vytvořil a oslovil děti a mladistvé formou dotazníkového šetření, a jednak kvalitativní, a to pomocí profilů na sociálních sítích.

V rámci kvantitativní metody sběru dat jsem si stanovil cíl oslovit 200 respondentů ve věku 8 – 18 let. Tuto věkovou kategorii jsem z hlediska zaměření své bakalářské práce vyhodnotil jako nejrizikovější, a to z několika důvodů:

1. jedná o nezletilé

2. sociální sítě používá velmi často

3. lidé v tomto věku jsou nejvíce ovlivňováni vrstevníky – předpokládal jsem, že profily na sociálních sítích jsou otázkou prestiže i fungování v kolektivu

4. vzhledem k malým životním zkušenostem je nejvíce zranitelná

V rámci kvalitativní metody sběru dat jsem byl v užším korespondenčním kontaktu s 20 uživateli sociální sítě Instagram.

6 VÝZKUM

Výzkumná část bakalářské práce spočívala ve vytvoření dotazníkového šetření, kde jsem zjišťoval, jak jsou ostatní uživatelé benevolentní ke sdílení svých osobních informací. Posléze pro potvrzení výsledků dotazníkového šetření jsem vytvořil profily na sociální síti Instagram, pomocí kterých jsem uživatele upozorňoval na některá bezpečnostní rizika a radil, co, kde a s kým lze na sociálních sítích zveřejňovat a co už nikoli.

6.1 Dotazník

V rámci kvantitativní metody sběru dat jsem si stanovil cíl oslovit alespoň 200 respondentů ve věku 8 – 18 let. Na konci dotazníku byla i edukativní část o tom, jak se chovat co nejbezpečněji na sociálních sítích.

Tento cíl jsem naplnil prostřednictvím kontaktování svých bývalých učitelek ze základní školy (ZŠ Štefánikova, Hradec Králové, celkem 25 respondentů) a svých bývalých učitelů z víceletého gymnázia (PSJG Hradec Králové, celkem 24 respondentů). Právě vzhledem ke skutečnosti, že jsem absolvoval víceleté gymnázium, jsem oslovil pro kontaktování respondentů z druhého stupně ZŠ třídní učitelky svých mladších bratrů, kteří jsou ve věku 12 a 14 let (ZŠ Svobodné Dvory, celkem 26 respondentů, a ZŠ Kukleny, Hradec Králové, celkem 25 respondentů). Respondenti vyplňovali dotazník anonymně a vyplnění jim zabralo přibližně 5 minut času. Sběr dat pro dotazník proběhl v době od 2. do 6. 3.2020 o přestávkách.

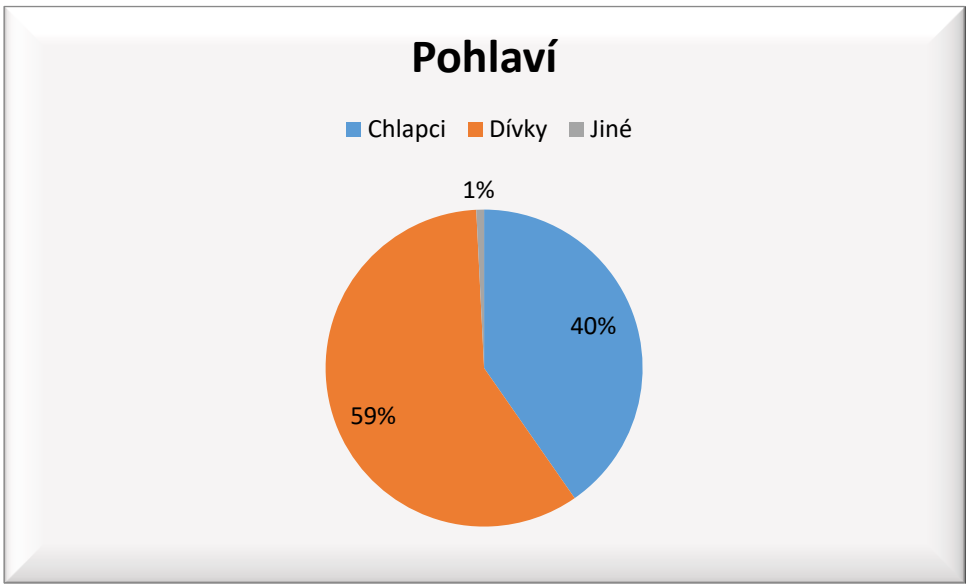
Další 153 odpovědí jsem získal pomocí on-line dotazníku na webu Survio.com, kde jsem tento dotazník odeslal prostřednictvím e-mailu všem vyučujícím z webu Občankáři - Asociaci učitelů občanské výchovy a společenských věd, jež jsem poprosil, aby v rámci výuky požádali své žáky a studenty o jeho vyplnění. Také jsem se přidal do různých facebookových skupin typu: skolaci.com, Učitelky 1. stupně ZŠ sobě (PK), kde mi rovněž byl poskytnut prostor, abych mohl oslovit vyučující, kteří dotazníky rozeslali svým žákům. Oslovení učitelů se mi zdálo jednodušší a účelnější, než oslovovat samotné mladistvé, jelikož mám dojem, že přece jen vztah žák-učitel je více autoritativní a současně pro děti a mladistvé důvěryhodný.

V jedné facebookové skupině můj příspěvek schválen nebyl, jelikož schvalovali jen dotazníky určené pro učitele. Celkově mohu konstatovat, že jsem se ze strany pedagogů setkal s milým a vstřícným přístupem.

Celkově jsem tedy vyhodnocoval 253 dotazníky.

6.2 Tabulky a grafy - vyhodnocení dotazovaných

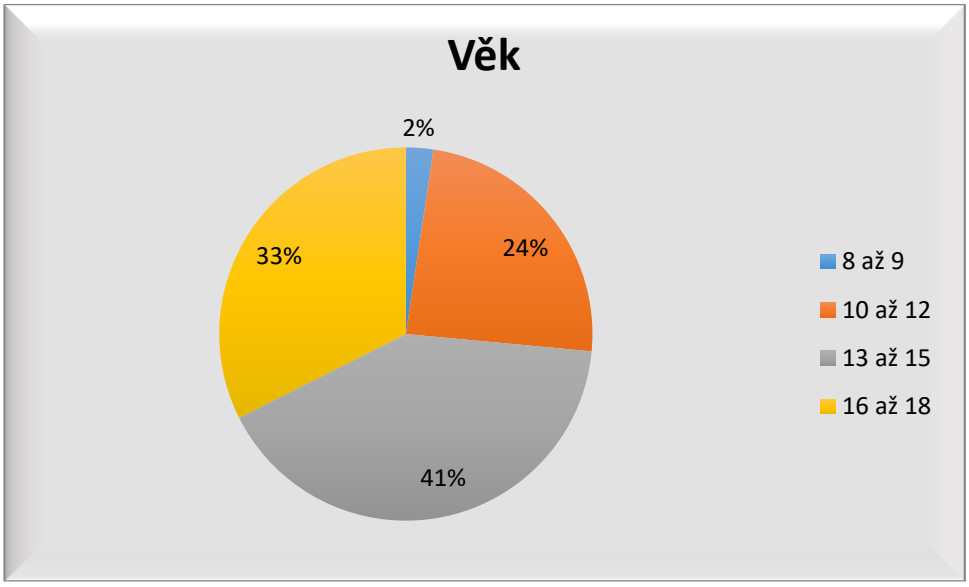
Otázka č. 1 Jakého jsi pohlaví?



Graf 1 Pohlaví

Průzkumu se zúčastnilo celkem 253 osob, z čehož 149 bylo děvčat a 102 chlapců. Dva respondenti uvedli, že se necítí ani jako jedno z výše uvedených pohlaví.

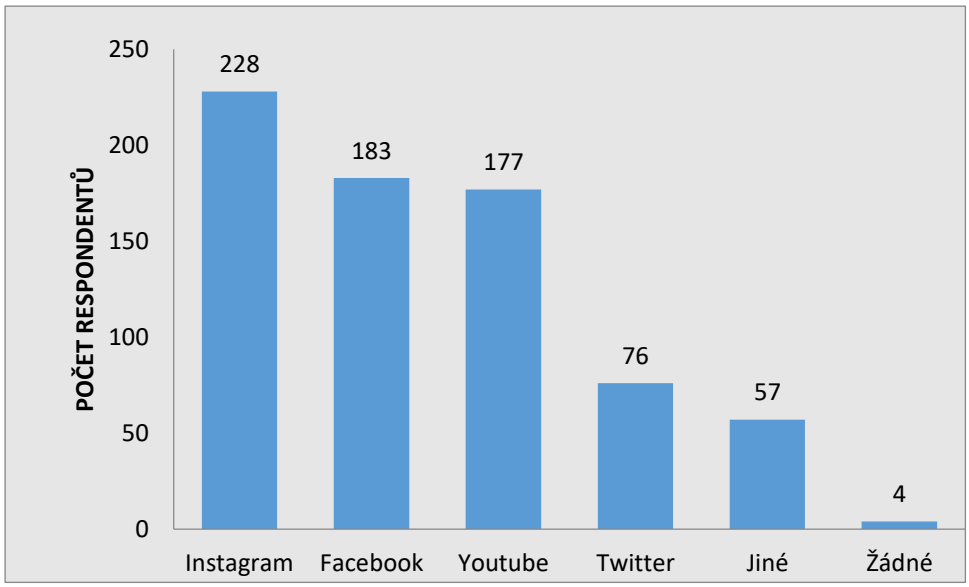
Otázka č. 2 Kolik ti je let?



Graf 2 Věk

Největší skupina respondentů byla ve věku 13-15 let, druhou nejpočetnější skupinou byli mladiství ve věku 16-18, kterých bylo 82. Třetí skupinou byly děti od 10 do 12 let, nejmenší skupinou dotazovaných byly děti ve věku 8-9 let, kterých bylo pouze 6.

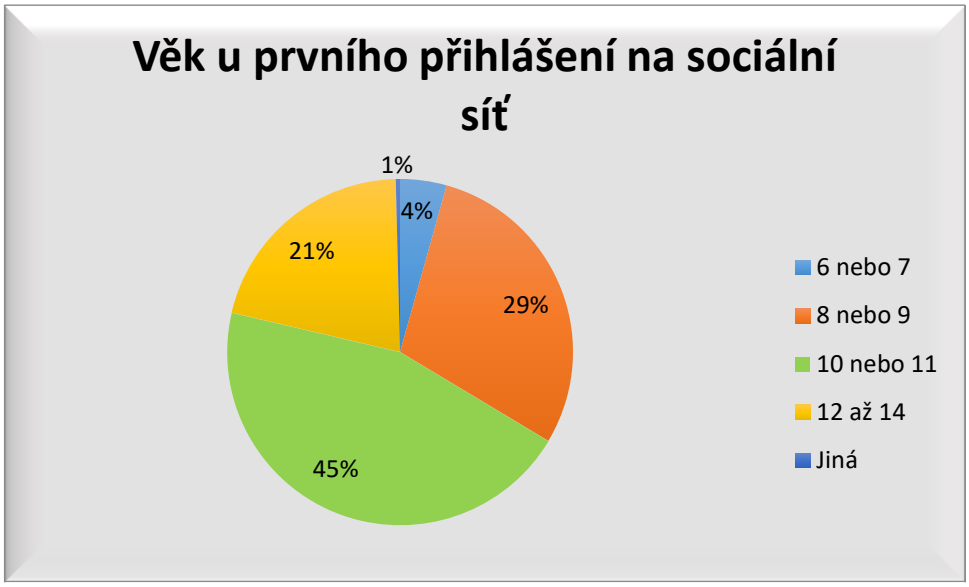
Otázka č. 3 Na které sociální síti máš založený účet? (označ všechny užívané sítě)



Graf 3 Založené účty na sociálních sítích

Z odpovědí na tuto otázku vyplývá, že dnešní děti a mladiství mají hlavně účty na Instagramu (91,2 %) a na Facebooku (73,2 %). Na YouTube má založený účet 70,8 % respondentů, účet na Twitteru 30,4 % dětí a dospívajících. Jiné sociální sítě využívá 22,8 % respondentů, jako jiné většinou respondenti vyplňovali TikTok a Reddit. Čtyři z dotázaných (1,6 %) uvedli, že nemají založený účet na žádné sociální síti.

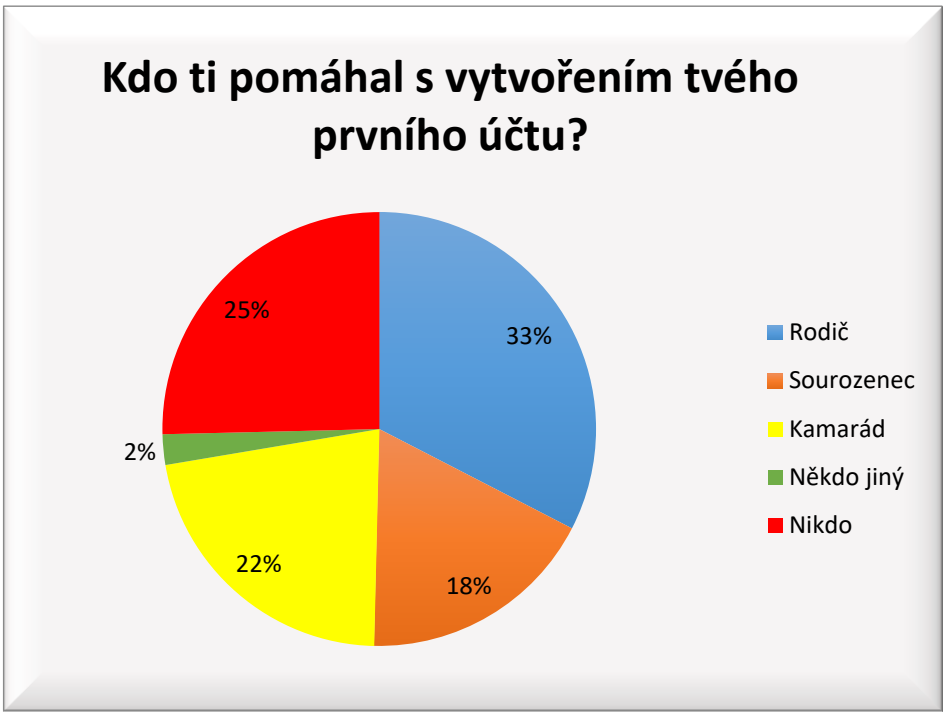
Otázka č. 4 V kolika letech ses poprvé přihlásil na některou ze sociálních sítí?



Graf 4 Věk u prvního přihlášení na sociální síť

Z otázky č. 4 vyplývá, že nejvíce dětí a mladistvých se poprvé přihlašuje na sociální síť ve věku 10 nebo 11 let. Téměř třetina se přihlásila již ve věku 8 nebo 9 let. 53 respondentů uvedlo, že se poprvé přihlásili na sociální síť ve věku 12 až 14 a 11 dospívajících uvedlo, že jsou na sociálních sítích již od 6 nebo 7 let. Jeden respondent uvedl, že se na sociální síť přihlásil již v pěti letech.

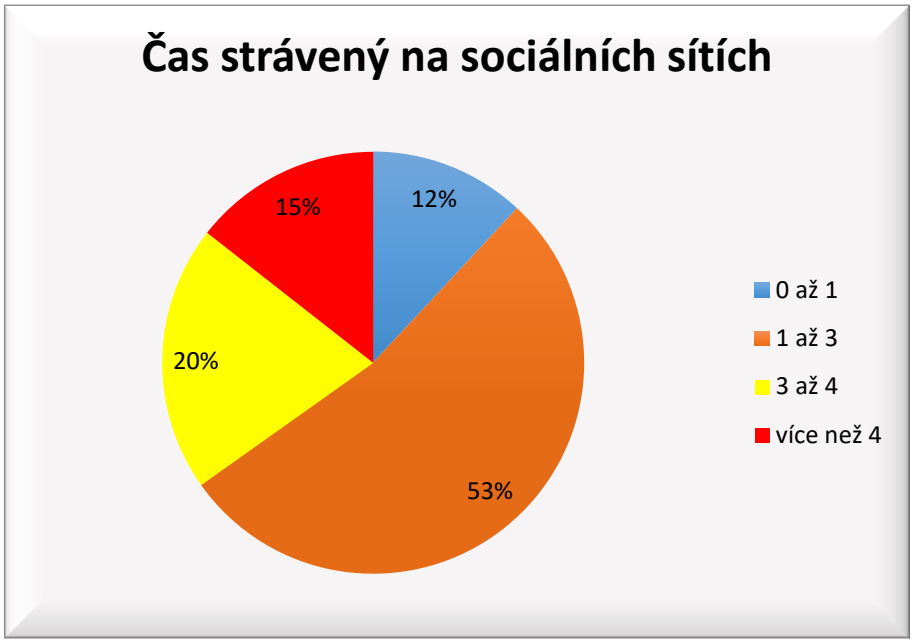
Otázka č. 5 Kdo ti pomáhal s vytvořením tvého prvního účtu?



Graf 5 Pomoc s vytvořením prvního účtu

Z odpovědí na předchozí otázku vyplynulo, že věkový průměr prvního přihlášení na sociální síť je 10,15 roku. Vzhledem k tomu, že většina sociálních sítí má ohraničenou spodní hranici na 13 let věku, a uživatelský účet na sociální síti má 97 % z dotázaných, je zřejmé, že toto pravidlo není dětmi, ale z 33 % dokonce ani rodiči dětí, jak vyplynulo z průzkumu, respektováno.

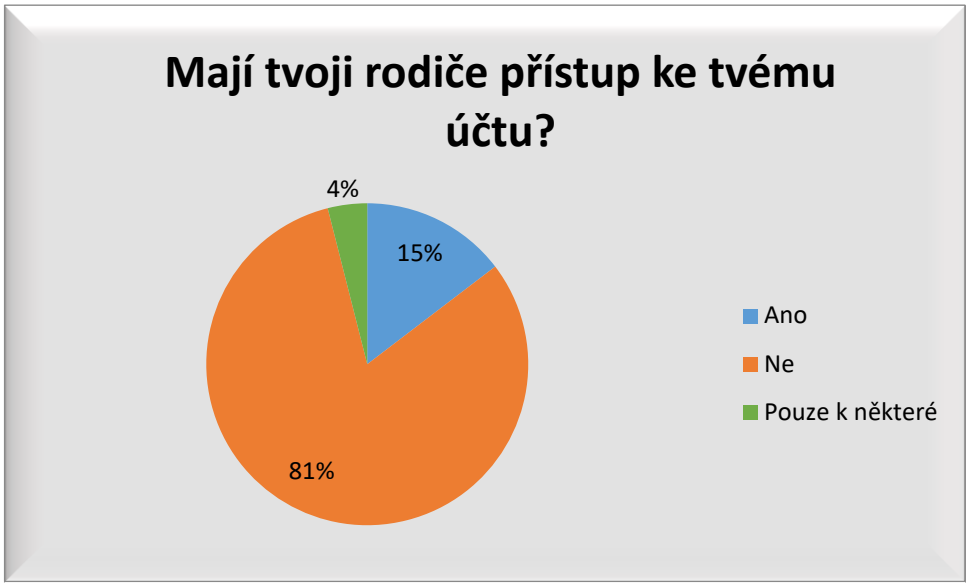
Otázka č. 6 Kolik hodin denně trávíš na sociálních sítích?



Graf 6 Čas strávený na sociálních sítích

Až 53 % uživatelů tráví na sociálních sítích 1–3 hodiny denně. Více než 15 % uživatelů dokonce více než 4 hodiny denně. Můžeme jen polemizovat, zda je to způsobeno současnou pandemickou situací, kdy se děti více „shlukují“ na sociálních sítích, jelikož jim současná vládní omezení jim neumožňují reálný kontakt. 20 % uživatelů zde tráví 3–4 hodiny a pouze 12 % dětí a mladistvých je na sociálních sítích méně než 1 hodinu denně.

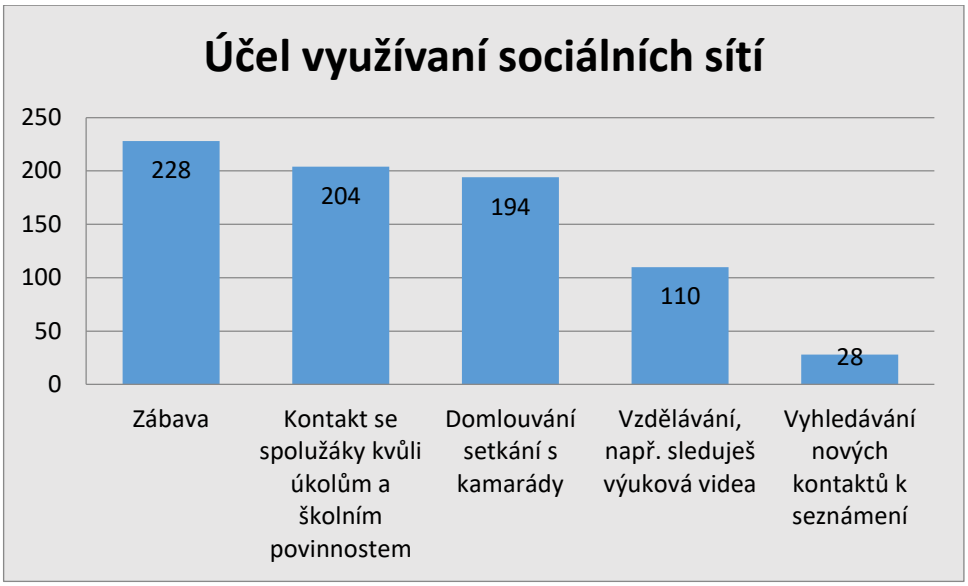
Otázka č. 7 Mají tvoji rodiče přístup ke tvému účtu?



Graf 7 Přístup rodičů k účtu dítěte

Jak z grafu jasně vyplývá, až 81 % rodičů a zákonných zástupců nemá přístup k účtu svého nezletilého dítěte, což je více než 200 z 250 respondentů. 4 % rodičů mají přístup pouze k některým účtům a pouze 15 % rodičů má volný přístup k informacím o účtech svých dětí.

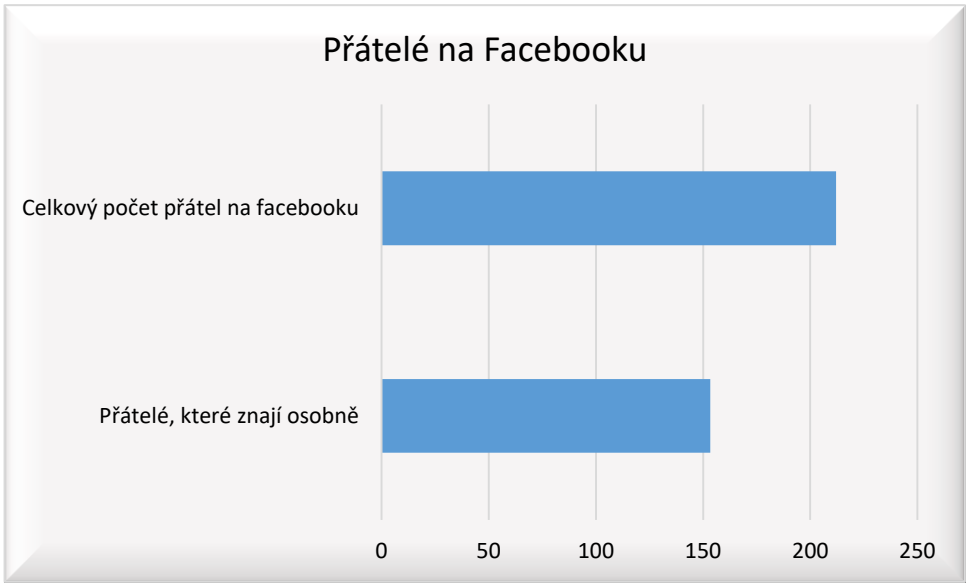
Otázka č. 8 K jakému účelu využíváš sociální sítě?



Graf 8 Účel využívání sociálních sítí

Děti a mladiství nejvíce využívají sociální sítě pro zábavu (90,1 %), dále pro kontakt se spolužáky a kvůli úkolům a školním povinnostem (80,6 %), více než tři čtvrtiny respondentů využívají sociální sítě pro domlouvání setkání s kamarády (76,6 %), poté 43,4 % respondentů sleduje na sociálních sítích různá výuková videa a pouze 11 % dětí a mladistvých využívá sociální sítě k vyhledávání nových kontaktů k seznámení.

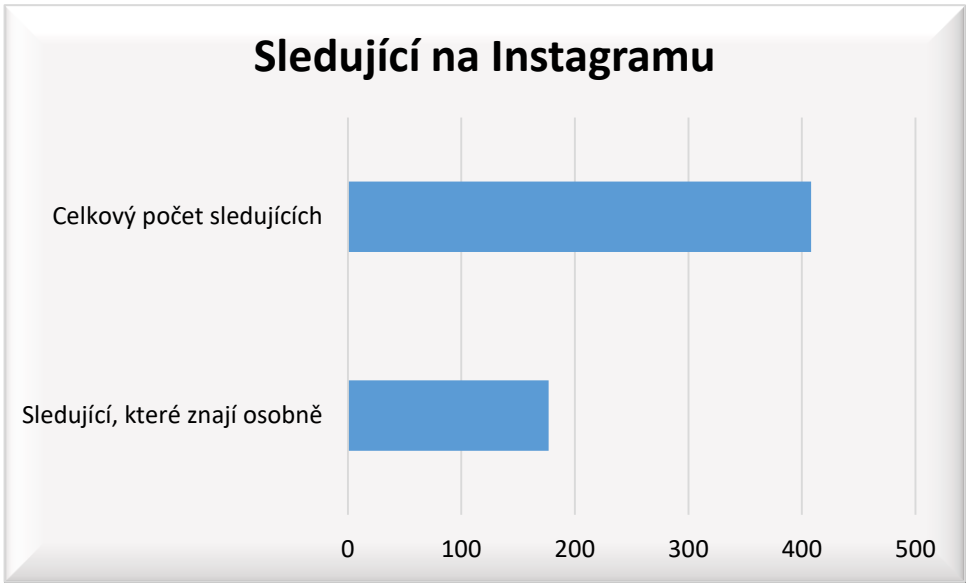
Otázka č. 9 a 10 Kolik máš přátel na Facebooku a kolik z nich znáš osobně?



Graf 9 Přátelé na Facebooku

Z otázek 9 a 10 vyplývá, že děti a mladiství mají v přátelích na Facebooku více než jednu čtvrtinu lidí, které neznají osobně.

Otázka č. 11 a 12 Kolik máš sledujících na Instagramu a kolik z nich znáš osobně?



Graf 10 Sledující na Instagramu

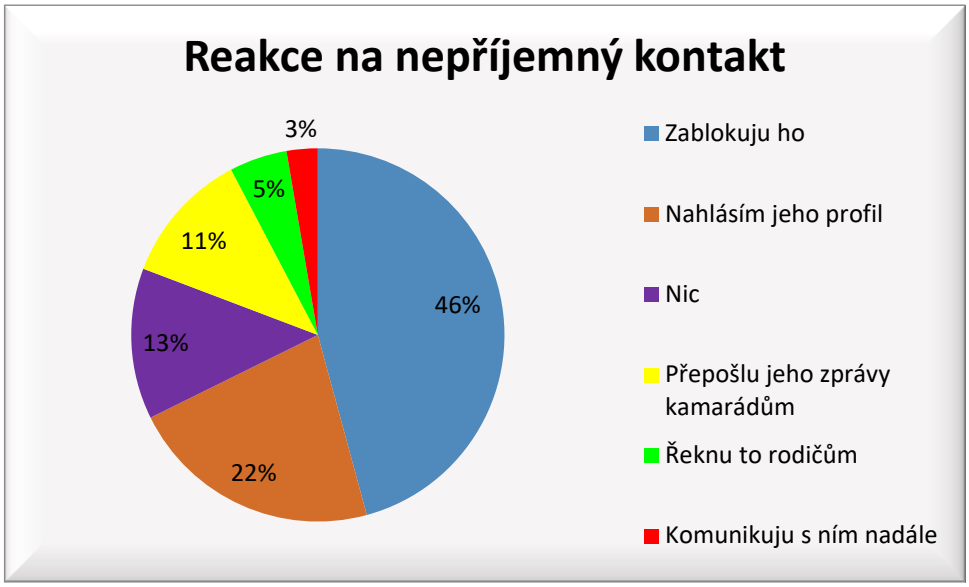
Z otázek 11 a 12 vyplynulo, že respondenti, kteří mají účet na Instagramu, mají v průměru více než 400 sledujících, z nichž znají pouze průměrně přibližně jen polovinu (177).

Otázka č. 13 Kontaktují tě cizí lidé?

Graf 11 Kontakt s cizími lidmi

Na otázku, zda děti a mladistvé kontaktují cizí lidé, odpovědělo 175 (70 %) respondentů kladně a 78 (30 %) záporně, čtyři respondenti vzhledem k tomu, že nemají účet na žádné sociální síti, neodpovídali vůbec.

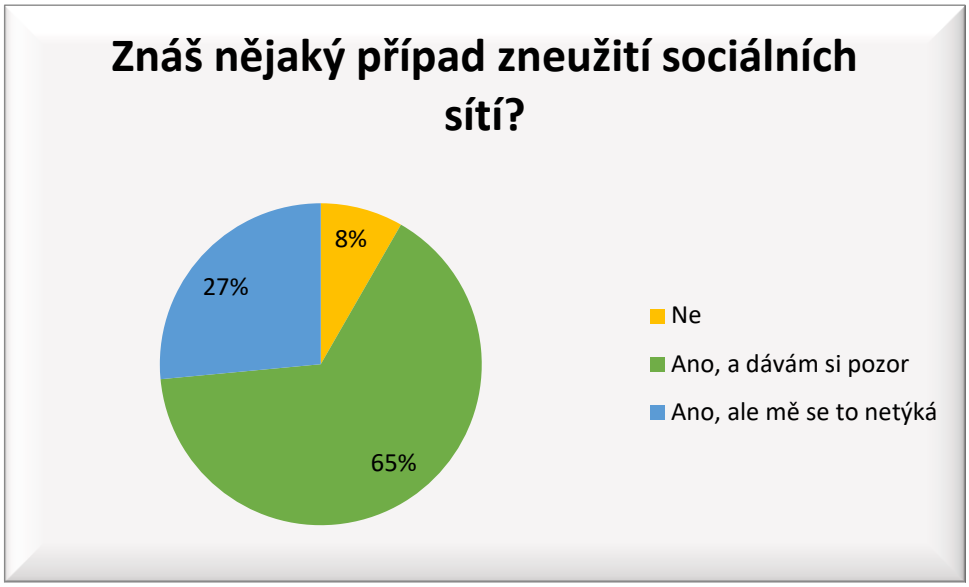
Otázka č. 14 Co uděláš, když je ti takový kontakt nepříjemný?



Graf 12 Reakce na nepříjemný kontakt

Na otázku týkající se reakce na nepříjemný kontakt odpověděla téměř polovina respondentů (46 %), že si kontakt zablokují, což jde velice snadno - volbou zablokovat, odebrat z přátel apod. Zajímavým zjištěním naopak je, že až 3 % dotázaných komunikuje s nepříjemným člověkem (kontaktem) nadále. 22 % procent zúčastněných se zachová zodpovědně, a to tím, že profil nahlásí, tudíž tím vlastně předcházejí tomu, že by nepříjemný kontakt kontaktoval další uživatele sociálních sítí. 11 % respondentů sdílí své nepříjemné zážitky s kamarády, kterým přeposílají jejich zprávy. Zarážející je, že 13 % účastníků výzkumu neudělá vůbec nic z nabízených možností, což se obávám, že je ta nejhorší možnost spolu s 3 %, kteří odpověděli, že komunikují nadále. Pouze 5 % dotázaných řekne tuhle skutečnost rodičům, což je velice malé procento, trochu znepokojující, jelikož rodiče- zákonní zástupci, s kterými děti žijí, si zaslouží více důvěry.

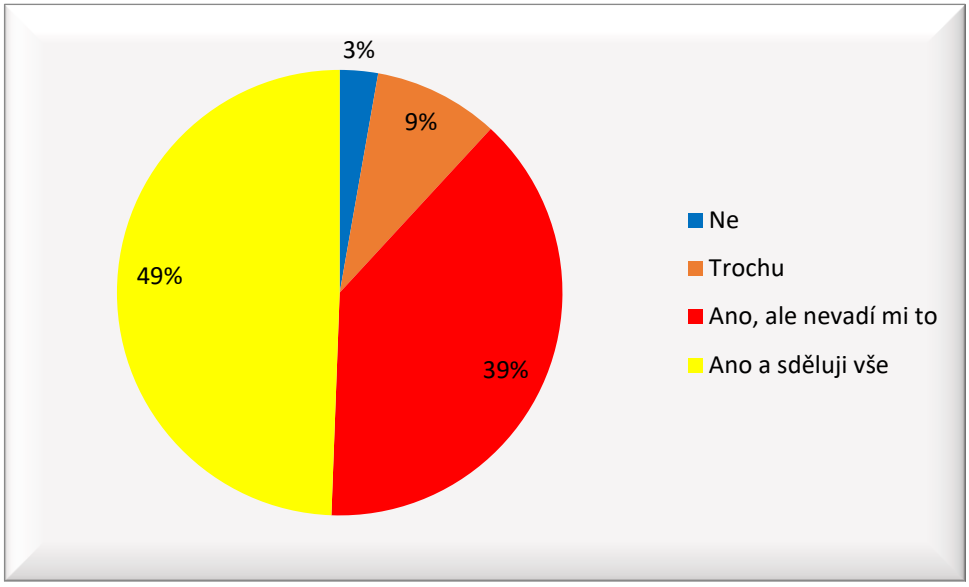
Otázka č. 15 Znáš nějaký případ zneužití sociálních sítí?



Graf 13 Zkušenost s případy zneužití sociálních sítí

Více jak polovina respondentů uvádí, že zná případ zneužití na sociální síti, ale zároveň je opatrná a dává si pozor. Pouze 8 % nezná žádné zneužití na sociální síti a 27 % uživatelů tvrdí, že jich se tohle týkat nemůže.

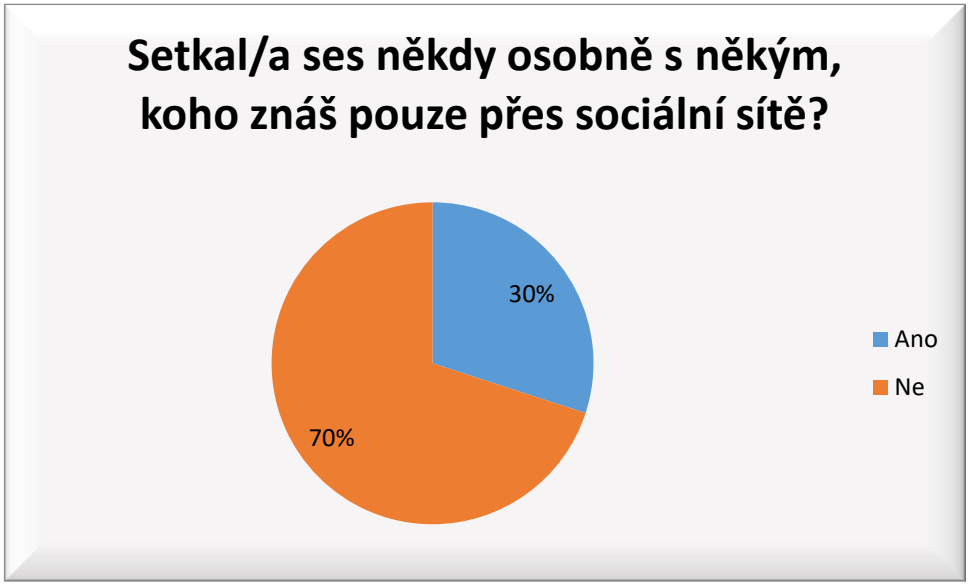
Otázka č. 16 Víš, že používáním sociálních sítí a všech možných aplikací dáváš přístup ke svým soukromým datům, kontaktům, zprávám…?



Graf 14 Přístup k osobním informacím

Jak je z otázky patrné, většina dotázaných moc dobře ví, že dává díky používání sociálních sítí nahlédnout „do svého soukromí“, respektive přístup ke svým soukromým datům. Přímo 49 % dotázaných jasně odpovědělo, že sděluje vše, 39 % uživatelů sociálních sítí to ani nevadí, pouze 9 % si není jisto a odpovědělo „trochu“. Neinformovaná byla pouze 3 % respondentů. Ti odpověděli „ne“.

Otázka č. 17 Setkal/a jsi se někdy osobně s někým, koho znáš pouze skrz sociální sítě?



Graf 15 Setkání s cizí osobou

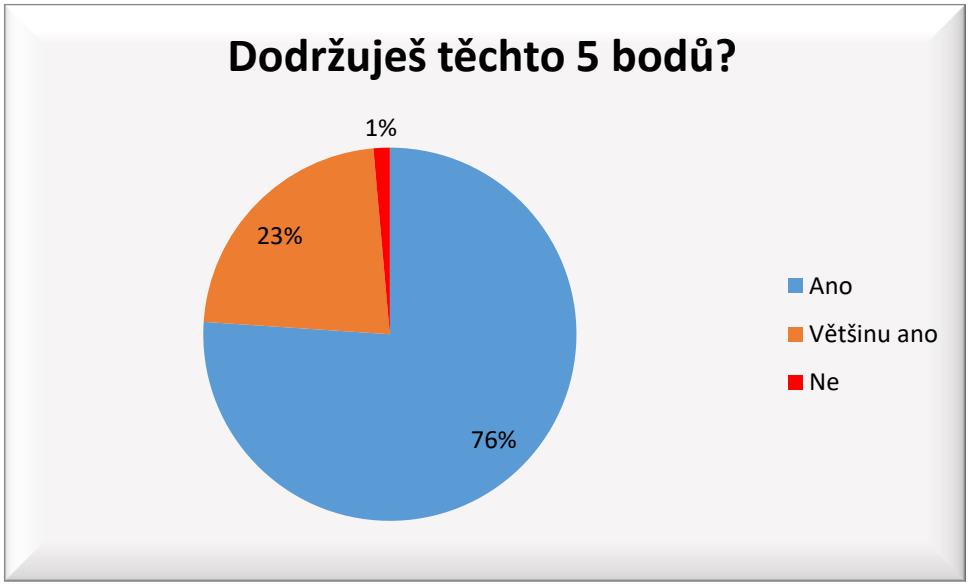
Otázku č. 17 jsem přidal pouze do elektronického dotazníku, tudíž mi na ni odpovědělo pouze 153 respondentů. Odpovědi na tuto otázku jsou poněkud znepokojující, protože 30 % respondentů odpovědělo, že se již setkali s někým, koho poznali pouze na internetu a osobně se s ním nikdy předtím neviděli. Vzhledem k tomu, že na internetu se můžeme vydávat za kohokoli, viz první část mé praktické části, může být takové setkání nebezpečné, zvláště pro děti, které jsou v průměru již od deseti let na sociálních sítích. A jejich rodiče nevědí (a 80 % z nich ani nemůže vědět, pokud jim to děti samy neřeknou), s kým komunikují, respektive s kým se scházejí přes sociální sítě.

Otázka č. 18 Jak se chovat bezpečně na sociálních sítích?

Tato otázka byla také pouze u dotazníku, který jsem rozeslal online formou, tudíž na ni odpovědělo pouze 153 respondentů. V této otázce byl sepsán list pěti základních bodů pro bezpečné používání sociálních sítí.

Pět bodů vypadalo následovně:

1. Mít dostatečně dlouhé heslo, které nikdy nikomu nesmíme prozrazovat.
2. Nezveřejňovat své kompletní údaje, jako adresu, telefonní číslo apod.
3. Nedomlouvat si osobní setkání s někým naprosto neznámým.
4. Neposílat nikomu své fotografie, ani ty nevinné. V žádném případě intimní fotografie.
5. V případě vydírání či šikany se svěřit rodiči, sourozenci nebo alespoň kamarádovi. Nemazat důkazy. Případně nahlásit útočníka přímo správci sociální sítě.



Graf 16 Dodržování 5 bodů pro bezpečné používání sociálních sítí

Na tuto otázku uvedla většina dětí a mladistvých, že dodržují všech těchto pět bodů, 23 % respondentů uvedlo, že dodržuje většinu z těchto pravidel, a pouze 1 % respondentů uvedlo, že těchto pět zásad nedodržuje.

Pokud chceš cokoli připsat, můžeš sem:

Této možnosti, která byla v dotazníku umístěna v závěru, využilo pár respondentů, kteří připsali následující příspěvky:

„myslim si, ze socialni site tu budou uz na vzdy, kdyz se detem nebo nove prihlasenym reknou nejaka jakoby rizika, nebo jak s tim pracovat, tak je to v poradku.. v tehle dobe jsou soc. site podle me dost dulezite, at uz pro pomoc skoly, tak na kontakt s kamardy, kdyz enni moznost chodit ven“

„Já chápu, že plno dětí (ale I dospělích) je závislý a že zpřístupňujeme naše soukromé data, ale bohužel se podle mě v dnešní společnosti nedá 100 % fungovat, pokud nejste alespoň částečně součástí této virtuální reality...dále si také myslím, že sociální sítě nahradí jednou normální zprávy v televizi a stanou se primárním zdrojem informací. Například všichni mí spolužáci a vrstevníci sledujou, co se děje díky informacím, které jim poskytnou jejich sociální sítě. Důležité je poznat, co je pravda.“

„Mluvit o bezpečnosti dětí a mladistvých na sociálních sítích je podle mého názoru hodně důležité. Sama jsem se vším obeznámena a dávám si pozor. Před založením účtu by se každý základní pravidla měl naučit.“

„Myslím, že soc. sítě jsou spíše k užitku než k zneužití. Riziko tam samozřejmě ale je.“

„o bezpečnosti na internetu jsem se hodně dozvěděl z projektu Buď Save Online“

„Nemám důvod, psát si s lidmi, které neznám a nic neznamenají. Když chci s někým mluvit, tak se s ním setkám osobně, nebo skrze hovor/videohovor.“

„byl mi nabídnut sex za peníze nebo peníze za fotky s mými prsy“

„Malí děti, který nemají rozum píšou na soc. sítě hanlivé a urážlivé komentáře nebo posty, myslím si, že by se co nedříve měli sociální sítě pro děti 9-12 zrušit protože podle mě nemají ani páru o tom že je to nevkusné a pokud toto jejich rodiče vidí a nic s tím neudělají tak by se měli stydět a to co nejvíce“

„ otázka reakce na nepříjemný kontakt- nebyla tam možnost, že sem zavolala na linku bezpečí, je zdarma a tam mi právě poradili, ať to řeknu doma a pak si ho blokla.“

„Good luck s bakalářkou doufám, že ti to vyjde šéfe! “

6.3 Vyhodnocení dotazníku

Dotazníkové šetření bylo provedeno u 253 dětí a mladistvých. Z čehož bylo téměř 60 % děvčat, 40 % chlapců. Z tohoto počtu se již dají dělat celkem relevantní závěry. Největší skupinou respondentů byly děti od 13 do 15 let. Nejoblíbenější sociální sítí je mezi dětmi a mladistvými Instagram, který využívá více než 90 % respondentů, na Facebooku to byly tři čtvrtiny, což svědčí o postupném úpadku zájmu ze strany dětí a mladistvých o tuto sociální síť a naopak Instagram se těší veliké popularitě za strany mladých, i když se zdá, že i Instagram už mladí opouštějí a přesouvají se na novější sociální sítě, zejména TikTok. Mám dojem, že pokaždé když se objeví nová sociální síť, jsou právě děti a mladiství na ní jako první. Poté se na sociální síť začnou přihlašovat i rodiče a prarodiče a děti se začnou opět stěhovat na novější sociální síť, kde nemají dospělí takový přehled o jejich aktivitách a kde je rodiče či prarodiče neztrapňují komentáři pod jejich příspěvky nebo označováním na fotkách například z rodinných oslav.

Velmi mě překvapilo, kolik času mladí na sociálních sítích tráví. Pouze 12 % tráví na sociálních sítích maximálně hodinu. Většina respondentů stráví na sociálních sítích od 1 do 3 hodin času, ale 35 % respondentů je aktivních na sociálních sítích více než 3 hodiny a 15 % respondentů uvedlo, že stráví na sociálních sítích více než 4 hodiny denně. Vezmeme-li v úvahu, že se dotazníkového šetření účastnili všichni školou povinní respondenti, kteří školní výukou stráví 4-7 hodin ve všední dny, pak je většina jejich volného času věnována surfování po sítích. Tato skutečnost je do jisté míry dána

současnou situací, kdy je pobyt venku omezen a kdy nefungují žádné off-line mimoškolní aktivity, jako jsou sportovní, hudební, výtvarné nebo dramatické kroužky. Na druhou stranu, jak je popsáno výše, sociální sítě způsobují závislost. Z toho důvodu se domnívám, že trvá-li současný stav takto dlouho, budou se děti a mladiství s virtuálním světem neradi loučit, aby místo toho navštěvovali kroužky nebo sportovali.

U otázky na věk při prvním přihlášení na některou ze sociálních sítí byl průměrný věk přibližně 10 let, což vzhledem k tomu, že většina sociálních sítí stanovuje minimální věkovou hranici pro přihlášení na 13 let, naprostá většina dětí porušuje.

Co se týče ochrany soukromí, mnoho dětí a mladistvých má profil na sociálních sítích nastaven jako veřejný, zbytek má profil nastavený jako soukromý, což znamená, že pouze osoby, které si uživatel přidá do přátel, případně které si do přátel přidají jeho, mohou vidět, co na svém profilu sdílí. Z výsledku dotazníku vyplynulo, že děti a mladiství mají na sociální síti Facebook čtvrtinu přátel, které ani neznají osobně. U sociální sítě Instagram dokonce polovinu svých sledujících. Což znamená, že i pokud mají nastaven profil jako soukromý, stále může velká část neznámých osob vidět, co na svém profilu sdílí. Obzvláště na Instagramu, kde děti schvalují žádosti o sledování téměř komukoli, tudíž poněkud postrádá smysl mít nastavený profil jako soukromý.

Ze zjištěného lze však vyvodit, že se mnohé děti a mladiství na sociálních sítích chovají vcelku bezpečně, znají jednotlivá hrozící nebezpečí a umějí se s nimi vypořádat. Především respondenti, kteří odpovídali na on-line dotazník, kde byla poslední otázka edukativně zaměřena na základních pár bodů o tom, jak se chovat bezpečně na sociálních sítích. Naprostá většina odpověděla, že dodržuje těchto pár základních pravidel.

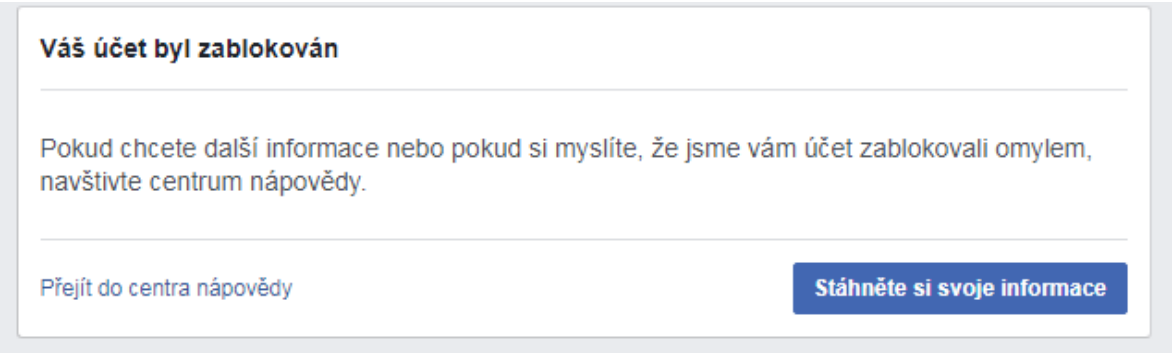
6.4 Průzkum sociálních sítí

Pro hlubší průzkum sociálních sítí jsem založil několik profilů na sociálních sítích. Byl jsem inspirován filmem V Síti, kde se tři dospělé herečky vydávali za dvanáctileté slečny. Vytvoření těchto profilů bylo čistě pro vědecké účely bakalářské práce. Profily byly po dokončení průzkumu, respektive po dvou týdnech smazány. Profily byly vytvořeny pro zjištění, kolik uživatelů sociálních sítí navazuje kontakt s dětmi a mladistvými, a kvůli varování dětí a mladistvých před hrozbami či úskalími sociálních

sítí. V neposlední řadě pro ověření výsledků dotazníkového šetření. Pomocí profilů jsem navazoval konverzaci pouze pozdravem a uživatele jsem k ničemu nevybízel.

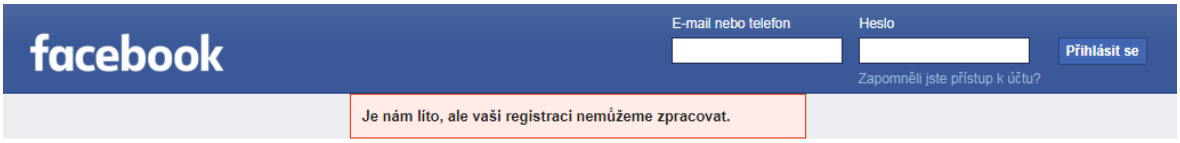
6.4.1 Vytvoření profilu na Facebooku

Z hlediska ověřování nových profilů mi Facebook vyšel jako bezpečný, protože už při vytvoření nového profilu mi hned po rozeslání dvou žádostí o přátelství nahlásil podezřelou aktivitu na mém účtu. Následně jsem se bez ověření telefonního čísla ani nemohl přihlásit.



Obrázek 1 Zablokovaný účet [Screenshot autor – Facebook.com]

Než jsem si pořídil nové telefonní číslo, Facebook můj účet zablokoval (obr. č. 2). Poté už jsem se s tímto novým číslem nemohl ani zaregistrovat, protože na mém zařízení (telefonu, počítači) byla identifikována podezřelá aktivita (obr. č. 2). Registrací bych tedy porušoval jejich zásady ochrany osobních údajů.



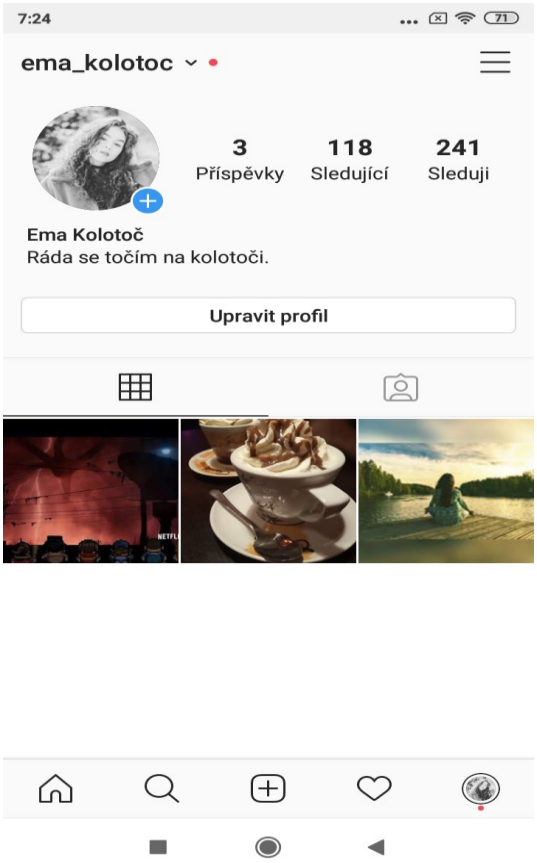
Obrázek 2 Odmítnutí registrace nového účtu [Screenshot autor – Facebook.com]

Následně jsem se ještě pokusil zaregistrovat pomocí prohlížeče TOR[1]. Domníval jsem se, že nebude-li moci Facebook tento účet propojit s mou IP adresou, povolí mi registraci. Ani na tomto prohlížeči se mi to však nepovedlo.

Po konzultaci těchto výsledků s kolegou, který si ještě před pár lety (2016/17) vytvářel spousty profilů, a to pouze pomocí nové e-mailové adresy, jsem došel k závěru, že společnost Facebook velmi zlepšila způsob ověřování nových uživatelů.

6.4.2 Vytvoření falešného profilu na Instagramu

U Instagramu už bylo podstatně jednodušší si vytvořit falešný profil. E-mailová adresa i telefonní číslo sice zůstaly stejné jako u mého soukromého účtu, ale ostatní uživatelé bez využití kontrolních mechanismů na první pohled nezjistí, že se nejedná o můj pravý účet.



Obrázek 3 Ukázka falešného profilu na Instagramu [Screenshot autor – Instagram.com]

[1] Internetový prohlížeč umožňující anonymní komunikaci a pohyb po internetu.

Na Instagramu si nepřidáváte přátele jako na jiných sociálních sítích, ale pouze je sledujete a ostatní mohou sledovat vás. U mladší generace je to i jakýsi ukazatel oblíbenosti, čím více ´followerů´ (lidí, kteří vás sledují) máte, tím jste oblíbenější. Proto jsem se v této praktické části zaměřil hlavně na tuto skupinu. Těmto uživatelům nezáleží na tom, koho sledují či kdo sleduje je. Chtějí hlavně jakousi pozornost, aby se o ně někdo zajímal. Děti a mladiství ve věku od 11 do 17 hledají sami sebe, chtějí patřit do různých skupin, zajímají se hodně o témata, o kterých se stydí mluvit s rodiči, jako např. sexuální život apod.

Na Instagramu jsem si vytvořil celkem 3 profily. Dvakrát jako dívka, jednou jako chlapec. Postupoval jsem tak, že jsem si našel influencera, kterého sledují děti a mladiství, a začal sledovat a oslovovat jeho followery, a to z jednoho profilu jako chlapec a z jednoho jako dívka. Rád bych tu zdůraznil, že jsem uživatele k ničemu špatnému nevybízel, ani jsem nenabádal k žádné protizákonné aktivitě.

Z jednoho dívčího profilu jsem oslovil chlapce i dívky, a to formou pozdravu. Dívky se mnou nekomunikovaly vůbec, z chlapců odpověděla 1/5 oslovených. Z dvanácti chlapců, kteří zareagovali, byla ve dvou případech druhá a v osmi případech třetí věta zaměřena na erotiku. Na poznámku, že mi ještě nebylo patnáct let, reagovali všichni ve smyslu „to mi nevadí“. Po upozornění, že sex do 15 let je trestný čin, byli ve většině případů vulgární. Další komunikaci jsem poté nerozvíjel.

Z chlapeckého profilu jsem opět oslovil chlapce a dívky. Chlapci mi na pozdrav odpověděli pozdravem, a protože jsem dál s nikým komunikaci nerozvíjel, skončila pouhým pozdravem. Dívek, které na pozdrav odpověděly (v celkovém počtu 24), jsem se dotázal, jestli už je někdo vyzval, aby mu poslaly svou „fakt sexy“ fotku. Polovina z nich se mnou i po tomto dotazu komunikovala i nadále. Dvě dívky mi sdělily, že mi fotku pošlou, až pošlu já svou, zbylých 10 v komunikaci pokračovalo ve stylu „A proč?, Jak to myslíš?“. Komunikaci jsem v tomto momentě už vedl stylem, že provádím výzkum, že můj profil je vymyšlený a že by nikdy nikomu takové fotky posílat neměly.

Druhý dívčí profil jsem pouze vytvořil, ale nikoho jsem ani nekontaktoval, ani nezačal sledovat. Neobsahuje ani žádnou fotografii či příspěvek, pouze mé jméno zní anglicky. Za dva týdny jsem měl 35 sledujících.

6.4.3 **Badoo**

V souvislosti se zkoumaným tématem jsem se dozvěděl, že seznamovací servery, mezi které patří Badoo, užívají i nezletilí, dokonce často i mladší 15 let. Spodní věková hranice je sice nastavena na 18 let, ale stejně jako u mnoha jiných sítí není ani zde dodržována.

Založil jsem si tedy profil i na Badoo, kde jsem se vydával za čtrnáctiletou dívku. Za dobu trvání účtu, což bylo 14 dní, mi 2 uživatelé (dle jejich účtu mužského pohlaví) nabízeli peníze za sex a intimní fotografie. Současně se ptali také na mé kamarádky, jestli by chtěly totéž. Dva z nich mi poslali, aniž bych je o to žádal, „své“ fotografie intimních partií.

Závěrem lze říci, že se děti a mladiství chovají na sociálních sítích celkem bezpečně. Během dvou týdnů jsem se díky profilům na sociálních sítích cítil pobouřen, znechucen, potěšen a překvapen. Reakce uživatelů byly opravdu různorodé. Většina uživatelů neodpověděla na můj pozdrav, případně si mě rovnou zablokovala. Byl jsem překvapen uživateli, kteří se mnou komunikovali, hlavně z hlediska jejich slovníku a obecně chováním. Děti a mladiství jsou v internetovém prostředí, mnohem sprostější a drsnější. Některé fráze, které by z očí do očí nikomu neřekli, jim nedělá problém napsat. Na druhou stranu jsem se na sociálních sítích setkal i s uvědomělými a zodpovědnými mladými lidmi, kteří mi po sdělení, že provádím průzkum pro větší bezpečí na sociálních sítích, děkovali za mou snahu.

7 ZNEUŽITELNÉ INFORMACE O UŽIVATELÍCH SOCIÁLNÍCH SÍTÍ

Zneužitelných informací může být několik typů. Spousta uživatelů sociálních sítí uvádí na svém profilu adresu, kde bydlí. Když poté přidají příspěvek, např. v živém vysílání na Facebooku, jak jsou na dovolené s celou rodinou, je pro případného zloděje velmi snadné vykrást jejich dům či byt. Někteří uživatelé sdílejí i s naprosto neznámými lidmi své intimní fotografie, a vůbec je nenapadne, že by je pomocí těchto fotografií mohl někdo následně např. vydírat. Stejně tak však může dopadnout sdílení takových fotografií i s někým, s kým jsem právě ve vztahu. Vztah skončí, což u takto mladých lidí bývá časté, ale fotografie zůstanou. Protějšek je opět může zneužít, rozeslat po síti, zveřejnit.

Velmi mě překvapilo, jak moc jsou někteří uživatelé sdílní, někdy až drzí, co se týče jejich komunikace s okolním světem. I přesto, že jsem se na sociálních sítích vydával za nezletilé dívky či chlapce, někteří uživatelé mi stejně posílali fotky svých intimních partií s nabídkou sexu.

Zneužívat informace o uživatelích může i samotná sociální síť, pokud např. „lajkujeme“ některé příspěvky, sociální síť si nás pomocí různých algoritmů zaškatulkuje do takzvané sociální bubliny. Kromě reklamy a nabídky zboží či služeb může taková virtuální stopa vést ke zneužití v podobě ovlivňování myšlení, názorů i chování prostřednictvím cílení politických sdělení, hoaxů nebo jiných účelově vytvořených dezinformací.

8 JAK SE CHOVAT BEZPEČNĚ NA SÍTÍCH

V této kapitole budou uvedena základní pravidla a tipy, jak se chovat na sociálních sítích co nejbezpečněji.

8.1 Hesla a ukradená identita

Příliš jednoduché heslo může vést k ukradení identity, což je velmi nepříjemná situace, protože vás následně může útočník vydírat, ztrapnit a podobně. Zde je několik tipů pro bezpečné heslo:

- U hesla je dobré se řídit příslovím „na velikosti, respektive délce záleží“, proto by přístupové heslo k účtu na sociální síť mělo být dostatečně dlouhé, minimálně 10 a více znaků s kombinací písmen i čísel (ideálně dávat čísla na začátek a doprostřed hesla).
- Nikdy nepoužívat pro všechny přístupy jedno heslo, pro každou sociální síť mít jiné heslo.
- Heslo nikdy nikomu neprozrazovat.
- Nepoužívat hesla typu:
    - jméno domácího mazlíčka
    - koníčky
    - rok narození, ať už vlastní, nebo někoho z rodiny
    - vlastní jméno nebo jméno partnera
    - název oblíbeného fotbalového klubu, zpěváka, kapely
- Heslo by nemělo dávat žádný smysl. [23] V případě, že nějaký smysl bude dávat, aby bylo snadněji zapamatovatelné, je dobré, aby bylo opravdu velmi dlouhé, např.
  Jedobrésimýtruce,pořádněamýdlemminimálně3krátdenně. Takové heslo by útočníkovi, pokud by se ho snažil prolomit hrubou silou, neboli zkoušením všech možných kombinací písmen, trvalo 26 trestrigintilionů

let [24], což je mnohonásobně více let, než uběhlo vteřin od počátku vesmíru tak, jak ho známe.

8.2 Neprozrazovat své kompletní údaje

Na sociálních sítích by děti nikdy neměly zveřejňovat své kompletní údaje a další citlivé informace, jako je číslo kreditní karty nebo číslo občanského průkazu. Jméno je ještě v pořádku, ale příjmení už je na zvážení. Údaje jako adresa, telefonní číslo, škola nebo třída by již neměly být veřejné na sociálních sítích.

Celkově je dobré udržovat osobní údaje soukromé, protože čím více informací o sobě zveřejníte, tím je vyšší riziko, že někdo použije tyto informace ke krádeži vaší identity, přístupu k vašim soukromým datům nebo k pronásledování. [23]

8.3 Neklikat na podezřelé odkazy

Může se stát, že vám přijde zpráva od sociálního inženýra se „super nabídkou“. Pokud kliknete na odkaz nebo stáhnete nějaký soubor, nebo někam zadáte údaje k platební kartě, můžete mít během okamžiku zavirovaný počítač či peníze stržené z účtu. Je proto velmi důležité dávat si pozor, na které odkazy klikáte a co si stahujete do počítače nebo telefonu. Výborným nástrojem na zjištění, zda je odkaz či soubor bezpečný, je webový server virustotal.com, kde lze po zadání url webové stránky či nahrání podezřelého souboru do minuty zjistit, zda je možné danou webovou stránku či soubor bezpečně otevřít.

8.4 Omezit čas strávený na sítích

Americký autor Jaron Lanier ve své knize doporučuje všem smazat si všechny účty nebo přestat používat sociální sítě alespoň na půl roku, protože systém všech účtů na sociálních médiích se stal postupem času neustálým sledováním a jemnou manipulací neetickým, krutým a nebezpečným. Jako argumenty pro smazání účtů na sociálních sítích uvádí např. ztrácení svobodné vůle, to, že sociální sítě podkopávají pravdu, dále, že vás sociální sítě činí nešťastnými nebo že sociální média ničí schopnost empatie nebo dokonce, že z vás sociální média dělají hlupáka. Proto bychom měli

alespoň zkusit přestat používat sociální sítě, abychom viděli, zda to má na nás pozitivní, či spíše negativní efekt, zdali jsme se nestali již závislými na sociálních sítích apod. [17]

8.5 Nepořizovat a neposílat sextingový obsah

Jak již bylo zmíněno výše, nejlepší a nejúčinnější ochrana proti vydírání, zveřejnění citlivého obsahu, jako jsou vlastní nahé fotografie nebo videa, je nepořizovat a neposílat takový obsah nikdy, nikomu. Ať už to po vás chce přítel/kyně, nebo se jen chcete pochlubit svou krásnou postavou, nikdy nikomu neposílejte takové fotografie. Ani videocall není řešení, protože potenciální útočník si ho může nahrávat nebo dělat snímky obrazovky (screenshoty). Pokud jste dítě nebo mladistvý, je dokonce nelegální vyrábět a distribuovat takový materiál a můžete být za to trestně stíháni.

8.6 Dalších několik tipů pro bezpečné používání sociálních sítí

- Mějte aktualizovaný legální antivirový software
- Nepřidávejte si do „přátel“ neznámé lidi.
- Rodičovský dohled – Zákonní zástupci dětí a mladistvých mají možnosti monitorovat, co jejich děti na sociálních sítích dělají například pomocí mobilních aplikací. Tyto aplikace umožňují rodičům filtrovat nebezpečný obsah na různých stránkách a sociálních sítích. Umožňují vypnout funkce posílání zpráv, omezit přístup nebo dobu používání internetu. Aplikace umožňují rodičům sledovat polohu jejich dětí pomocí systémů GPS zabudovaných do mobilních zařízení. [25]
- Prostudujte si vše o nastaveních ochrany osobních údajů a zabezpečení na sociálních sítích a použijte tyto nástroje. Jsou tam, aby vám pomohly kontrolovat, kdo vidí, co zveřejňujete, a spravovat vaše on-line příspěvky tím nejlepším způsobem.
- Zveřejňujte o ostatních pouze to, co byste chtěli, aby ostatní zveřejňovali o vás.
- Nezapomínejte se odhlašovat.

- Nesetkávejte se s někým, koho znáte pouze z internetu, a už v žádném případě k nikomu nenastupujte do auta.

8.7 Televize Seznam - Bezpečně online, pořad Černota, dokument V síti - Buď Safe

Kvůli případům obětí zneužití a šikany v internetovém světě vzniklo několik internetových platforem, jako např. *Seznam se bezpečně* či *Černota*, které pomáhají v boji s kyberšikanou. Jejich cílem je, aby podobných incidentů již v budoucnu nepřibývalo.

Kvůli pandemii Covid19 se život mladistvých přesunul z velké míry do světa on-line, proto je toto téma ještě více relevantní v dnešní době, kdy uživatelé tráví na internetu ještě více času.

Velmi výstižně rozebírá problematiku zneužívání sociálních sítí jedincem dokument Víta Klusáka *V síti*, jenž vešel do kin na začátku roku 2020 a který dobře vystihuje problém zneužívání sociálních sítí. Dokument byl natočen proto, aby ukázal, kolik se na sociálních sítích vyskytuje takzvaných predátorů, kteří se snaží z nezletilých dívek vylákat intimní fotografie nebo videa a následně je vydírat zveřejněním oněch intimních materiálů. Hlavními aktéry filmu jsou tři plnoleté herečky, které hrají dvanáctileté dívky, jež jsou „loveny v síti“. Film má dvě verze, jednu pro školy, druhou pro širokou veřejnost, která je dostupná od 18 let, s explicitními scénami, kde jsou pouze zakryty obličeje daných útočníků. Velkým plusem je, že díky tomuto dokumentu pronikla velká osvěta tématu o zneužívání sociálních sítí a kyberšikany do široké veřejnosti. Vznikla kampaň zahrnující přednášky, rozhovory s aktérkami, která právě mnoha dospívajícím mohla pomoci. Zároveň se mnoho predátorů z internetového prostředí stáhlo a děti a mladiství si dnes dávají na sociálních sítích větší pozor. [26]

9 ZÁVĚR

Cílem bakalářské práce „Bezpečnost dětí a mladistvých na sociálních sítích“ bylo zmapovat, jak moc jsou mladí lidé sdílní, co se týče jejich soukromých údajů a zda se na nich výše zmínění chovají bezpečně. Zároveň byl kladen velký důraz i na zpětnou vazbu. To znamená, že kromě mapování, zda se děti chovají na sociálních sítích bezpečně, byla do praktické části bakalářské práce zahrnuta snaha o rozšíření znalostí u dětí a mladistvých o hrozbách sociálních sítí a to o tom, jak tyto hrozby minimalizovat. Dílčím cílem bylo tedy informovat děti a mladistvé o možných hrozbách, které sociální sítě představují, jak jim předcházet a jak řešit případné následky, a zároveň zjistit, kolik času tráví na sociálních sítích a které sítě to jsou.

V teoretické části bakalářské práce jsou popsány nejrozšířenější sociální sítě. Dále jsou jasně vymezena rizika při používání sociálních sítí, je zde vysvětlena odborná terminologie a definice, které se vážou na sociální sítě a nebezpečí na nich.

Praktická část byla rozdělena na kvantitativní a kvalitativní výzkum. Jak z kvalitativního, tak kvantitativního průzkumu bylo zjištěno, že většina dětí a mladistvých se chová na sociálních sítích obezřetně. Uvědomují si, jaká rizika sociální sítě skýtají. Vůbec nekomunikují, případně si rovnou zablokují uživatele, kteří jim jsou nepříjemní. Pouze 8 respondentů z 253 s nepříjemným kontaktem komunikuje nadále. Z kvalitativního výzkumu vyšli děti a mladiství, kteří zareagovali na zprávy od „neznámé osoby“ (autora BP), jako vulgární a sexuálně přebujelí, ale na druhou stranu obezřetní mladí lidé.

Z kvantitativního výzkumu vyplývá, že jsou děti a mladiství celkem obezřetní. Většina z dotázaných ví o hrozbách sociálních sítí a dává si pozor. K zamyšlení však zůstává skutečnost, že děti a mladiství tráví na sociálních sítích velkou většinu svého volného času. Průměrně mají děti a mladiství v přátelích na sociální síti Facebook čtvrtinu „přátel“, které ani osobně neznají. V případě sociální sítě Instagram mají i více než polovinu sledujících, které neznají. Dalším bodem k zamyšlení je, že 30 % respondentů uvedlo, že se setkalo s někým, koho poznali pouze prostřednictvím sociální sítě.

Co se týče bezpečí na sociálních sítích, velmi dobrou osvětu tohoto tématu provedl Vít Klusák se svým dokumentem V síti. Dokument poukazuje na to, že se na sociálních

sítích vyskytuje velké množství internetových predátorů, na které je potřeba si dávat pozor. Díky tomuto dokumentu jsou dnešní děti a mladiství mnohem opatrnější při používání sociálních sítí.

Celkově by bakalářská práce mohla být přínosná pro rodiče dětí a mladistvých. Pro obeznámení se, s jakými riziky se na sociálních sítích jejich potomci, ale v podstatě i oni sami mohou setkat.

SEZNAM POUŽITÉ LITERATURY

[1] HAVLOVÁ, Jaroslava. Sociální síť. In: *KTD: Česká terminologická databáze knihovnictví a informační vědy (TDKIV)* [online]. Praha : Národní knihovna ČR, 2003- [cit.2020-03-29]. Dostupné z: https://aleph.nkp.cz/F/?func=direct&doc_number=000015947&local_base=KTD.

[2] KEMP, Simon. Digital 2020. *Wearesocial* [online]. 2020, 30.1.2020 [cit. 2021-02-22]. Dostupné z: https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media

[3] CONSTINE, Josh. Facebook Messenger Launches Free VOIP Video Calls Over Cellular And Wi-Fi. *Techcrunch* [online]. 2015, 27.4.2015 [cit. 2020-03-29]. Dostupné z: https://techcrunch.com/2015/04/27/facebook-messenger-video-chat/

[4] ROUSE, Margaret. Instagram. *SearchCIO: Techtarget* [online]. 2015, 1.5.2017 [cit. 2020-07-03]. Dostlupné z: https://searchcio.techtarget.com/definition/Instagram

[5] Help twitter. *Twitter help center* [online]. [cit. 2021-02-22]. Dostupné z: https://help.twitter.com/en

[6] Youtube: Youtube definition. *Techterms* [online]. 2009, 7.10.2009 [cit. 2020-03-29]. Dostupné z: https://techterms.com/definition/youtube

[7] SCHWEDEL, HEATHER. a Guide to TikTok for Anyone Who Isn't a Teen. *Slate* [online]. 2018 [cit. 2021-02-22]. Dostupné z: https://slate.com/technology/2018/09/tiktok-app-musically-guide.html.

[8] Ochrana osob a majetku. *Slu* [online]. [cit. 2021-02-22]. Dostupné z: https://www.slu.cz/file/cul/63077130-d050-448e-9321-d4e2e246b14c

[9] ŠLERKA, Josef. Dezinformace, fake-news, bulvární zpráva. *Transparency* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.transparency.cz/dezinformace-fake-news-bulvarni-zprava/

[10] ŠLERKA, Josef. Dezinformace, fake-news, bulvární zpráva. *Transparency* [online]. 2019 [cit. 2021-02-22]. Dostupné z: https://www.transparency.cz/dezinformace-fake-news-bulvarni-zprava/

[11] Co je Youtube. *Mioweb* [online]. 2019 [cit. 2020-03-29]. Dostupné z: https://www.mioweb.cz/slovnicek/youtuber/

[12] ČERNÁ, Alena. *Kyberšikana: průvodce novým fenoménem*. Praha: Grada, 2013. Psyché (Grada). ISBN 978-802-4745-770

[13] KOHOUT, Roman a Radek KARCHŇÁK. Bezpečnost v online prostředí. Karlovy Vary: Biblio Karlovy Vary, 2016. ISBN 978-80-260-9543-9

[14] SMAHEL, David, Hana MACHÁČKOVÁ, Giovanna MASCHERONI, Lenka DEDKOVA, Elisabeth STAKSRUD, Kjartan ÓLAFSSON, Sonia LIVINGSTONE a Uwe HASEBRINK. *EU Kids Online 2020* [online]. 2020, 10.2.2020, , 156 [cit. 2021-01-20].Dostupnéz:https://www.lse.ac.uk/media-and-communications/assets/documents/research/eu-kids-online/reports/EU-Kids-Online-2020-10Feb2020.pdf

[15] Zobrazování sexuality a nahoty mladých online. *Česká rada dětí a mládeže* [online]. 2020 [cit. 2021-5-3]. Dostupné z: https://heyzine.com/flip-book/64b1581056.html#page/1

[16] ČERNÁ, Alena. *Kyberšikana: průvodce novým fenoménem*. Praha: Grada, 2013. Psyché (Grada). ISBN 978-802-4745-770

[17] LANIER, Jaron. *10 Argument for Deleting Your Social Media Account Right Now*. 1. Henry Holt and Co., 2018. ISBN 978-1250196682.

[18] LUKIANOFF, Greg a Jonathan HAIDT. The Coddling of the American Mind: How Good Intentions and Bad Ideas Are Setting Up a Generation for Failure. Penguin Press, 2018. ISBN 0735224897.

[19] Australia Instagram star Essena O'Neill quits 'unhealthy' social media. *BBC* [online]. 2015, 3.11.2015 [cit. 2021-04-06]. Dostupné z: https://www.bbc.com/news/world-australia-34707116

[20] KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Praha: Grada Publishing, 2016. ISBN 9788024755953.

[21] FRUHLINGER, Josh. What is pretexting? Definition, examples and prevention. In: *Csoonline* [online]. [cit. 2021-02-23]. Dostupné z:

https://www.csoonline.com/article/3546299/what-is-pretexting-definition-examples-and-prevention.html

[22] What Are The Dangers Of Social Networking?: Top 7 Dangers And Risks Of Social Network Sites. *Roliedema* [online]. [cit. 2021-04-06]. Dostupné z: https://www.roliedema.com/dangers-of-social-networking.html

[23] PETROWSKI, Thorsten. *Bezpečí na internetu: pro všechny*. Liberec: Dialog, 2014. Tajemství (Dialog). ISBN 978-807-4240-669.

[24] How Secure Is My Password. *Security.org* [online]. [cit. 2021-04-06]. Dostupné z: https://www.security.org/how-secure-is-my-password/

[25] Social media. *Staysafeonline* [online]. [cit. 2021-04-12]. Dostupné z: https://staysafeonline.org/stay-safe-online/securing-key-accounts-devices/social-media/

[26] Osvětová kampaň V SÍTI. *Vsitifilm* [online]. 2020 [cit. 2021-5-6]. Dostupné z: https://vsitifilm.cz/

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IG Instagram

TOR The Onion Router

SEZNAM OBRÁZKŮ

SEZNAM GRAFŮ

SEZNAM PŘÍLOH

PŘÍLOHA P I: DOTAZNÍK

Ahoj, jmenuji se Pavel a studuji Bezpečnostní technologie, systémy a management na Univerzitě Tomáše Bati ve Zlíně. Pro bakalářskou práci dělám tento výzkum a prosím tě, abys mi s tím pomohl/a. Vše je anonymní. Děkuji ti.

Dotazník pro cílovou skupinu 8-18 let:

1. Pohlaví:
    a) chlapec
    b) děvče
2. Věk:
    a) 8 – 9
    b) 10 – 12
    c) 13 – 15
    d) 16 – 18
3. Škola:
    a) základní
    b) víceleté gymnázium
    c) jiná, uveď, jaká
4. Máš založený účet na (označ všechny užívané sítě):
    a) Facebook
    b) Instagram
    c) Twitter
    d) YouTube
    e) Jiné
    f) žádné

5. Napiš, v kolika letech ses poprvé přihlásil/a na některou ze sociálních sítí?

a) _____

6. Kdo ti pomáhal s vytvořením tvého prvního účtu?
    a) Rodič
    b) Sourozenec
    c) Kamarád
    d) Někdo jiný, uveď, kdo _____
    e) nikdo
7. Kolik hodin denně trávíš na sociálních sítích?
    a) 0 – 1
    b) 1 – 3
    c) 3 – 4
    d) více než 4
8. Mají tvoji rodiče přístup ke tvému účtu?
    a) ano
    b) ne
    c) mají jen k _____
9. Sociální síť používáš k tomuto účelu:
    a) zábava
    b) vzdělávání, např. sleduješ výuková videa
    c) kontakt se spolužáky kvůli úkolům a školním povinnostem
    d) vyhledávání nových kontaktů k seznámení
    e) domlouvání setkání s kamarády
10. Kolik máš přátel na Facebooku?

b) _____

11. Kolik z přátel na Facebooku znáš osobně?

c) _____

12. Kolik máš sledujících na Instagramu?

d) _____

13. Kolik z těchto sledujících znáš osobně?

e) _____

14. Kontaktují tě cizí lidé?
    a) ano
    b) ne
15. Co uděláš, když je ti takový kontakt nepříjemný?
    a) nahlásím jeho profil
    b) řeknu to rodičům
    c) řeknu to učiteli, protože si o těchto věcech otevřeně povídáme
    d) zablokuju ho
    e) přepošlu jeho zprávy kamarádům
    f) komunikuju s ním nadále
    g) nic
16. Znáš nějaký případ zneužití sociálních sítí?
    a) Ne
    b) Ano, ale mě se to netýká
    c) Ano a dávám si na to pozor
17. Víš, že používáním sociálních sítí a všech možných aplikací dáváš přístup ke svým soukromým datům, kontaktům, zprávám…?
    a) ne
    b) trochu

c) ano, ale nevadí mi to

d) ano a nepovoluji vše

Děkuji ti za vyplnění dotazníku, a kdybys chtěl/a, můžeš cokoli připsat. Sem:

_____

_____

_____