ZÁPADOČESKÁ UNIVERZITA V PLZNI

FAKULTA EKONOMICKÁ

Bakalářská práce

Bezpečnost na sociálních médiích

Security on Social Media

Veronika Jánská

Plzeň 2019

ZÁPADOČESKÁ UNIVERZITA V PLZNI
Fakulta ekonomická
Akademický rok: **2018/2019**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Veronika JÁNSKÁ**
Osobní číslo:	**K16B0100P**
Studijní program:	**B6208 Ekonomika a management**
Studijní obor:	**Management obchodních činností**
Název tématu:	**Bezpečnost na sociálních mediích**
Zadávající katedra:	**Katedra marketingu, obchodu a služeb**

Zásady pro vypracování:

1. Definujte pojmy internet a sociální média a demonstrujte, jakou roli na nich hraje bezpečnost.
2. Uveďte výhody, nevýhody a rizika, která působí na uživatele internetu a sociálních médií.
3. Pomocí vhodných nástrojů analyzujte problematiku bezpečnosti na internetu a sociálních médiích u vybrané cílové skupiny uživatelů.
4. Na základě provedené analýzy navrhněte zlepšující opatření.

Rozsah grafických prací: **neuveden**

Rozsah kvalifikační práce: **40-60**

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

Seznam odborné literatury:

- **BEDNÁŘ, Vojtěch.** *Marketing na sociálních sítích: prosaďte se na Facebooku a Twitteru.* **Brno: Computer Press, 2011. ISBN 978-80-251-3320-0.**
- **KOŽÍŠEK, Martin a PÍSECKÝ, Václav.** *Bezpečně n@ internetu: průvodce chování ve světě online.* **Praha: Grada Publishing, 2016. ISBN 978-80-247-5595-3.**
- **PETROWSKI, Thorsten a KURKA, Tomáš.** *Bezpečí na internetu: pro všechny.* **Liberec: Dialog, knižní velkoobchod a nakladatelství, 2014. ISBN 978-80-7424-066-9.**

Vedoucí bakalářské práce: **Ing. Michal Mičík, Ph.D.**
Katedra marketingu, obchodu a služeb

Datum zadání bakalářské práce: **23. října 2018**

Termín odevzdání bakalářské práce: **23. dubna 2019**

Doc. Ing. Michaela Krechovská, Ph.D.
děkanka

Západočeská univerzita v Plzni
L.S.
Fakulta ekonomická

Ing. Jan Tlučhoř, Ph.D.
vedoucí katedry

V Plzni dne 23. října 2018

Čestné prohlášení

Prohlašuji, že jsem bakalářskou práci na téma

„*Bezpečnost na sociálních médiích*“

vypracovala samostatně pod odborným dohledem vedoucího bakalářské práce za použití pramenů uvedených v přiložené bibliografii.

V Plzni, dne ……..

.....

podpis autora

Poděkování

Jako první bych chtěla poděkovat především vedoucímu mé bakalářské práce, Ing. Michalu Mičíkovi, Ph.D., za trpělivost a skvělé rady při zpracovávání a dále také paní Ing. Biňovcové, že mi umožnila v rámci vyučovací hodiny diskutovat se studenty.

Obsah

Úvod 8
Teoretická část 10
1 Internet 10
1.1 Pojem Internet 10
1.2 Vznik Internetu, jeho historie a důležitá data 11
1.3 Web 2.0 12
1.4 Web 3.0 13
1.5 Právní aspekty 13
1.6 Netiketa 14
2 Sociální média 15
2.1 Definice 15
2.2 Sociální sítě 17
2.3 Česká sociální média 19
2.4 Mezinárodní sociální média 20
2.4.1 Facebook 20
2.4.2 Instagram 22
2.4.3 Twitter 23
2.4.4 Ask.fm. 24
2.4.5 LinkedIn 25
2.4.6 YouTube 25
2.5 Výhody a nevýhody využívání sociálních médií 26
2.5.1 Výhody 26
2.5.2 Nevýhody 27
2.6 Dezinformace a hoaxy 29
3 Bezpečnost a rizika používání sociálních médií 33
3.1 Bezpečnost 33
3.2 Rizika a riziková chování na sociálních médiích 33
3.2.1 Phishing 34
3.2.2 Kybergrooming 36
3.2.3 Kyberšikana 37
3.2.4 Sexting 38
3.2.5 Kyberstalking 39
3.2.6 Krádež identity 40

3.3 Obrana proti rizikům 41
3.4 Projekty, které pomáhají 42
3.4.1 Linka Bezpečí 42
3.4.2 Bezpečný internet 43
3.4.3 Seznam se bezpečně 43
3.4.3 Bílý kruh bezpečí 43
3.4.4 E-bezpečí 44
4 Vlastní výzkum 45
4.1 Dotazníkové šetření 45
4.1.1 Výsledky 46
4.1.2 Souhrnný report 59
4.2 Focus group 60
4.2.1 Výsledky 60
5 Preventivní opatření a doporučení 63
Závěr 68
Seznam obrázků 69
Seznam tabulek 70
Použité zdroje 71
Seznam příloh 78
Abstrakt 87
Abstract 88

Úvod

Bakalářská práce se zabývá fenoménem, který je v současné době stále více rozšířený – sociálním médiím a sítím a především bezpečností na nich. Sociální média a profil na nich má v dnešní době téměř každý, proto je potřeba znát nástrahy a rizika, která mohou při využívání těchto komunikačních prostředků hrozit**.** V práci jsou zmíněná rizika, která jsou nejzávažnější a měla by se jim věnovat pozornost - kyberšikana, sexting, kybergrooming, vydírání, phishing a stalking.

Cílem této práce je navrhnout opatření a doporučení, která by měla sloužit jako prevence a pomoci předcházet těmto rizikům.

Práce je rozdělena do dvou částí – teoretické, která poskytuje teoretický podklad a praktické, která obsahuje dotazníkové šetření, metodu focus group a již zmíněná doporučení a preventivní opatření.

Teoretická část je rozdělená do tří kapitol. V první kapitole je popsán v první řadě Internet, jeho vznik, historie, Web 2.0 a Web 3.0, dále jsou zde popsány právní aspekty a netiketa, neboli pravidla chování na internetu. Další kapitola je zaměřena na sociální média. V první řadě jsou popsána sociální média, sociální sítě a poté vybrané příklady českých sociálních médií a mezinárodních sociálních médií. Další částí jsou výhody a nevýhody na sociálních médiích a poslední podkapitolou je, zdali vše, co se na Internetu píše, lze označit jako pravdivé a důvěryhodné. Poslední kapitolou teoretické práce je již samotná bezpečnost na Internetu. Je zde popsána bezpečnost, jednotlivá bezpečností rizika, která na sociálních médiích mohou hrozit, jak se proti těmto rizikům bránit a preventivní projekty, které mají za cíl pomáhat v boji proti těmto rizikům.

Praktická část je rozdělena do dvou částí. První část je zaměřena na vlastní výzkum mezi studenty pomocí dvou metod – metodou focus group a dotazníkového šetření. Nejdříve jsou jednotlivé metody popsány, je také popsán způsob jejich zpracování a poté již samotné výsledky metod, které byly pro výzkum použity a souhrnný report z dotazníkového šetření. Dotazníkové šetření je aplikováno na studenty středních a vysokých škol a cílem této metody je zjistit, jak se studenti chovají na Internetu, kolik času na něm tráví a jestli znají rizika, která je na sociálních médiích mohou potkat. Dále jestli znají projekty, které jim mohou v případě nastání některého z rizik pomoci. Součástí dotazníkového šetření jsou také

hypotézy, které budou pomocí vhodné metody testovány a přijaty, nebo v opačném případě označeny za nepotvrzené. Metoda focus group je prováděna na střední škole na vzorku 16 studentů (2 skupiny po 8) a cílem je doplnit otázky z dotazníkového šetření. Druhá část je zaměřena na navržená doporučení a preventivní opatření, která by mohla napomoci menšímu výskytu bezpečnostních rizik.

Teoretická část

1 Internet

1.1 Pojem Internet

Dle Sklenáka můžeme Internet označit jako: „*globální informační systém, který je logicky propojen do jednoho celku prostřednictvím adresního prostoru založeného na protokolu IP (Internet Protocol) nebo jeho následných rozšířeních"* (Sklenák, 2001, s. 181).

Pro Internet se také používá jeho zkrácená verze net, nebo ho také můžeme nazvat „síť sítí". Internet umožňuje přenášet data z jednoho počítače do druhého a tvoří ho velké množství počítačů. Pro mnoho uživatelů je ale Internet zejména elektronická pošta (email), který už téměř nahradil poštovní služby. Elektronická služba je jednou z nejpoužívanějších služeb Internetu (imip.cz, 2011).

Je nutno podotknout, že Internet jako celek nikdo nevlastní ani přímo neřídí. Funguje díky tomu, že všichni lidé na světě mají společný zájem na tom být propojeni. Mít svou síť, ze které se uživatel nedostane nikam dál nebo se dostane jen do části Internetu, je k ničemu. A tak nebyla jiná možnost - lidé se domluvili na společné síti. Samozřejmě zde plně funguje tržní mechanismus – a to konkurence, boj o zákazníka a v neposlední řadě také úmrtnost slabých. Pokud je některá firma úspěšná, má kvalitní síť a kvalitní propojení do zbytku Internetu, slušné ceny a pěkný vztah se zákazníky, tak roste, má obrat, zisky a další zákazníci se jen hrnou. Pokud je naopak jiná firma neschopná, má špatné a pomalé připojení, trpí výpadky, je drahá, nekomunikuje se zákazníky apod., tak zákazníci snadno odejdou ke konkurenci a taková firma časem s velkou pravděpodobností zkrachuje (datacentrum.wedos.com, 2010).

Internet se stal běžnou součástí života, a protože nemá žádného majitele, je nutné ho nějakým způsobem koordinovat. Pro tyto účely existuje několik nadnárodních organizací, zde uvedené například ICANN (Internet Corporation for Assigned Names and Numbers) či IANA (Internet Assigned Numbers Authority), které různé věci centrálně evidují, koordinují, vymýšlí, zavádí standardy apod. Cílem je především eliminace politických vlivů, což bohužel není zcela možné. V článku se uvádí, že např. ICANN je ještě stále pod dohledem vlády USA (datacentrum.wedos.com, 2010).

Internet poskytuje celou řadu služeb. Dle Dostála (2011) lze mezi ně řadit následující:

- Web (informace na webových stránkách, které jsou vzájemně propojeny pomocí hypertextových odkazů).
- Email.
- On-line komunikaci (možnost psát nebo telefonovat lidem z celého světa).
- Elektronickou konferenci (možnost zasílat si vzájemně příspěvky pomocí elektronické pošty).
- Přenos souborů mezi FTP serverem a FTP klientem.

1.2 Vznik Internetu, jeho historie a důležitá data

Za rok vzniku Internetu je většinou považován rok 1969, kdy v souvislosti s experimentálním ověřováním možností přenosů byla vytvořena síť ARPANET. Přestože šlo o vládní výzkum, který byl financovaný z armádních zdrojů, byla síť po vydařeném otestování zkoumaných principů předána do správy akademické obce. Postupným připojováním dalších akademických sítí k původní síti ARPANET, začal být tento propojený systém označován jako - „Internet“ a to v 80. letech minulého století (Jansa a kolektiv, 2016).

V současné době je Internet často považován pouze za soubor www stránek. Přitom, jak bylo výše uvedeno, síť Internet, respektive její předchůdce, fungoval od 70. let 20. století až do roku 1991 bez služby World Wide Web. Ta je tedy službou podstatně mladší, než celá síť Internet a je pouze jednou z jejích nadstaveb. Mezi další služby můžeme řadit elektronickou poštu (neboli e-mail), službu FTP (File Transfer Protocol), nebo v minulosti více používané BBS nebo Gopher (Jansa a kolektiv, 2016).

U zrodu Internetu v moderní podobě stáli v roce 1962 zejména Licklider a Welden Clark, kteří jako první popsali, jak by měla taková celosvětová a otevřená síť vypadat. Dle jejich slov by se síť měla skládat z počítačů propojených s pomocí širokopásmových komunikačních sítí (imip.cz, 2011).

První Internet byl čistě nekomerční, propojoval výzkumné ústavy, pracoviště a sloužil zejména k propojení univerzit. V 80 a 90 letech minulého století se historie Internetu mění a vyvíjí a začínají se objevovat první komerční poskytovatelé internetových služeb. To stálo

za zrodem zkratky ISP (Internet Service Provider aneb poskytovatel internetových služeb) (imip.cz, 2011).

Odhaduje se, že v roce 1993 se s využitím Internetu přenáší přibližně 1% veškerého telekomunikačního provozu. Rok 2000 ale vykazuje 51% podíl informací proudících díky Internetu, o 7 let později už ale přes Internet proudí přes 95% veškerých informací (imip.cz, 2011).

Mezi důležitá data v historii Internetu řadíme rok 1969 – již zmíněný - vytvoření sítě ARPANET, rok 1972 – založení centrální agentury pro správu internetového prostoru IANA, 1982 – v tomto roce byly zavedeny formální standarty protokol TCP/IP, v tomto roce byl také zaveden protokol pro odesílání emailových zpráv SMTP, dále rok 1990 – první internetový vyhledávač Archie, 1991 – zavedení internetové služby World Wide Web (Web 1.0), 1995 – on-line prodejce knih Amazon.com a online aukční a obchodní portál eBay, 1998 – vyhledávač Google, v roce 2001 otevřená encyklopedie Wikipedie, 2003 – Skype pro telefonování přes Internet, o rok později sociální síť Facebook a v roce 2005 YouTube pro sdílení videa (imip.cz, nedatováno).

V dnešní době je na Internetu možné dělat téměř cokoliv. Studenti si díky němu hledají informace pro své vzdělání, dospělí si díky němu mohou najít práci. Pomocí Internetu je také možné zjistit si informace pro cestování, naplánovat si dovolenou. Dále umožňuje sledovat videa, filmy, číst elektronické knihy, poslouchat písničky. Pro podnikatele je skvělou příležitostí jak se prosadit, ale nejen pro ně, také pro muzikanty, umělce a neziskové organizace. Internet je pro spoustu lidí příležitostí a stále častěji se využívá v mobilním telefonu.

Podle průzkumu, který zrealizovala společnost Gemius S.A. v rámci projektu Net monitor *Češi online 2018* , v roce 2018 je na Internetu 7,9 milionů Čechů a 61% si ho prohlíží z mobilního zařízení. 49% se věnuje na Internetu školním, nebo pracovním věcem a nejčastěji navštěvovanou obsahovou kategorií je zpravodajství (netmonitor.cz, 2018).

1.3 Web 2.0

Obsah webu ale nemusí být jen statický a bez toho, aniž by do něj nemohli uživatelé sami přispívat. Proto se stále častěji setkáváme s termínem „Web 2.0“. Aniž by uživatel uměl

programovat a psát složité kódy, může tak sám přispívat do obsahu Internetu a tvořit ho (Dostál, 2011).

Od Webu 1.0 (World Wibe Web) se Web 2.0 liší především tím, že vlastník je v roli moderátora – návštěvníci webu se aktivně podílejí na jeho obsahu. Interakce je vítána, web je propojen na sociální profily a uživatelé mezi sebou mohou komunikovat (uhk.cz, 2014).

Web 2.0 se stává stále více oblíbenějším, jelikož se lidé rádi dělí o své zážitky, pocity a sdílejí své názory. Technologie, které jsou pro Web 2.0 typické, jsou sociální sítě (Facebook, Instagram..), Sdílení videa (YouTube, Stream.cz), Wiki (Wikipedia), Blogy (Blog.cz) a MashUp (Google News) (Dostál, 2001).

1.4 Web 3.0

Stále častěji se hovoří o Webu 3.0. Neexistuje pro něj zatím přesná definice, ale podstatou bude získat kontext od uživatele a být schopen poskytnout nejužitečnější informace o hledaném výrazu či věci, což Web 2.0 nedokáže, ten vyhledá informace, které jsou nejoblíbenějším výsledkem vyhledávání. Web 3.0 lze přirovnat k asistentovi umělé inteligence, který svému uživateli rozumí a dokáže vše personalizovat (techopedia.com, 2019).

Dalším rozdílem mezi Webem 2.0 a Webem 3.0, je, že když si uživatel chce najít informace o dovolené, hledá levné lety a ubytování, musí se podívat na spoustu informací na webu, které porovnávají různé výběry, a hledání může trvat hodiny. Weboví asistenti nebo vyhledávače Webu 3.0 budou proto umět prezentovat tyto informace velmi inteligentním způsobem pomocí přesných a příznivých návrhů a to na základě profilu uživatele (techopedia.com, 2019).

1.5 Právní aspekty

Zneužití osobních údajů je závažné riziko, které uživateli Internetu na sociálních médiích hrozí. Zákon č. 101/2000 Sb., o ochraně osobních údajů vymezuje práva každého tohoto uživatele na ochranu před neoprávněným zásahem do soukromí a povinnosti při zpracování osobních údajů.

Osobní údaj dle § 4 písm. a) zákona je „*jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu*“ (business.center.cz, nedatováno).

25. května 2018 v rámci celé Evropské unie vstoupilo v platnost Obecné nařízení o ochraně osobních údajů (GDPR). Toto nařízení značně posiluje současnou úroveň ochrany osobních dat. Pro firmy které stále více využívají sociální sítě pro svůj marketing, to znamená výrazné snížení shromažďování osobních údajů bez vědomí uživatele nebo obchodování s databázemi osobních údajů získaných na sociálních sítích. Identifikace a profilování návštěvníků webových stránek za účelem jejich následného marketingového oslovení nebude tak možné bez toho, aniž by k tomu daná fyzická osoba dala svůj předchozí souhlas (retailnews.cz, 2017).

1.6 Netiketa

Netiketa je pojem, který se skládá ze slova NET (jako síť) a ETIKETA. Jedná se o pravidla slušného chování, kterými by se uživatelé Internetu měli řídit (Eckertová, Dočekal, 2013).

Etiketa na síti se skládá z těchto pravidel (Král, 2015):

- Komunikují spolu lidé, a proto je třeba se na Internetu chovat slušně.
- Pokud se při komunikaci vyskytují nějaké chyby, je třeba snažit se je tolerovat. Chyby dělají všichni, i ti nejchytřejší.
- Respektovat soukromí ostatních a brát ohled na druhé.
- Nezneužívat situaci, kdy toho jeden umí více než ostatní a je lépe informován, ale naopak, snažit se ochotně pomáhat.
- Neporušovat autorská práva.
- Nerozesílat spam, hoax, nebo reklamu, které jen zahlcují Internet. A určitě ne žádný malware.
- Pokud uživatel rozesílá a sdílí s někým videa, obrázky, musí tak dělat v odpovídající podobě (např. přes servery typu Úschovna).
- Snažit se psát stručně, výstižně, ale správně.

- Při komunikaci se chovat dle pravidel platných pro toho, s kým se komunikuje. Dnes je možné komunikovat s lidmi z celého světa, je tedy potřeba znát základní pravidla komunikace s cizinci.

2 Sociální média

2.1 Definice

Spojení sociální média se skládá ze dvou různých slov. Slovo sociální zde znamená, že lidé mezi sebou mohou sdílet a předávat si informace jeden od druhého a druhé slovo média odkazuje na nástroj komunikace, v tomto případě na Internet (televize, rozhlas a podobně, jsou zástupci tradičních forem médií). Z těchto dvou odlišných pojmů lze definovat, že sociální média jsou webové komunikační nástroje, které lidem umožňují vzájemné propojení pomocí sdílení a komunikace (lifewire.com, 2019).

Sociální média lze poznat podle některých typických prvků (lifewire.com, 2019):

- Lze si na webu vytvořit uživatelský účet.
- Možnost přizpůsobení a nastavení profilu.
- Aktualizování informací.
- Možnost komentovat jiné příspěvky.
- Hodnocení nebo hlasování.

Sociální média ale nejsou novým pojmem. Lidé si mezi sebou předávají doporučení, myšlenky a názory už po staletí. V moderní historii k tomuto sdílení informací lidé používali diskuse z očí do očí, dopisy, telefon nebo nejvíce používaný email. Je zde ale spousta nových výhod a možností, co nám nabízejí sociální média, jak je známe dnes. Jsou to především jednoduchost, transparentnost a přístupnost (Smih, Wollan, Zhou, 2011).

Schopnost sdílet fotografie, názory, události atd. v reálném čase změnila způsob, jakým lidé žijí, jak se prezentují a také způsob, jakým firmy mohou podnikat. Obchodníci, kteří využívají sociální média jako nástroj marketingu, vykazují měřitelné výsledky. Je ale potřeba média používat s opatrností, s péčí a respektem (thebalancesmb.com, 2018).

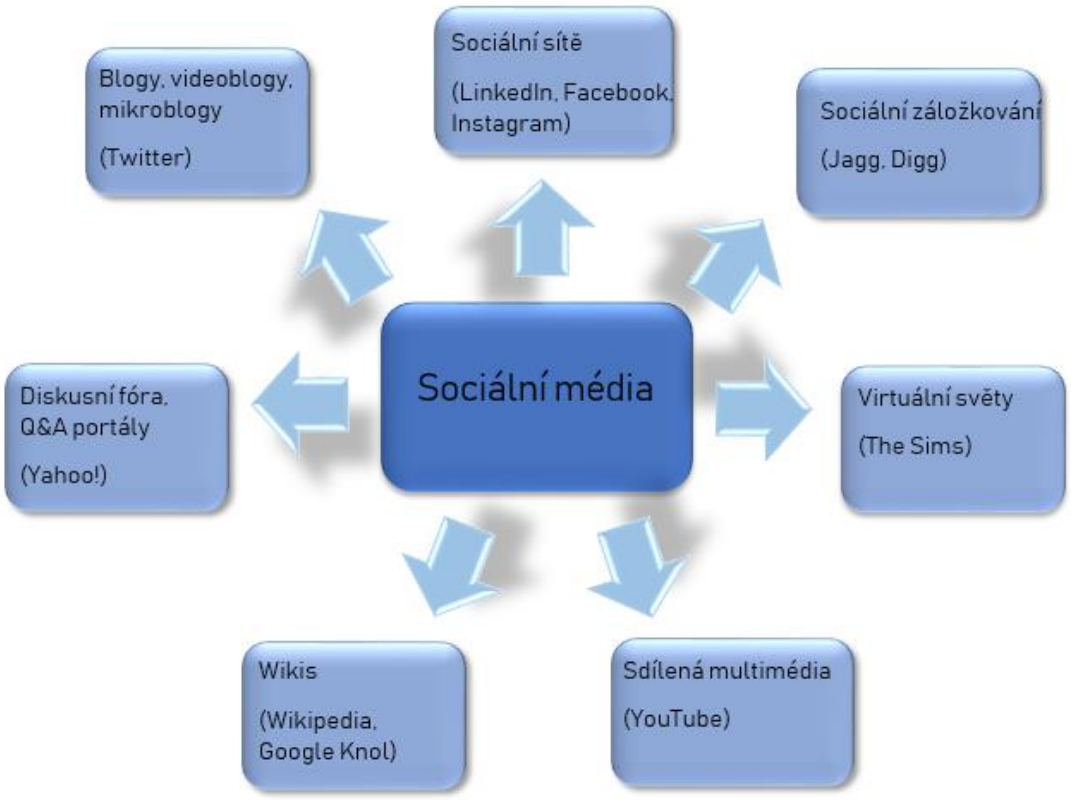
Sociální média lze dělit z mnoha hledisek, ale mnoho služeb se svými funkcemi překrývá, takže toto členění může být trochu zavádějící. Blogy podle některých odborníků spadají pod sociální sítě, někdo dokonce vidí za blogy a video blogy něco úplně jiného. Je důležité dělit členění ze dvou hledisek, jak podle marketingové taktiky, tak z hlediska zaměření. Podle zaměření lze sociální média dělit následovně (Janouch, 2013):

- Sociální sítě – do nich spadají videa, blogy, fotky, chaty, audio a diskuse.
- Stránky, kde se hlasuje o kvalitě obsahu.
- Zprávy – nejrůznější weby, na kterých jsou zveřejňovány zprávy a uživatelé sociálních médií na ně mohou sami přispívat svými komentáři nebo je sdílet.
- Sociální záložkovací systémy – sdílení informací, a především článků, pomocí veřejných záložek.
- Business sítě – ty slouží především pro propojení lidí z byznysu (především se jedná o vyšší či nejvyšší management).

Členění z hlediska marketingové taktiky bývá ale přehlednější a dle tohoto členění jsou také častěji vykonávány průzkumy používání sociálních médií (Janouch, 2013):

- Sociální sítě – LinedIn, Facebook, Instagram.
- Blogy, videoblogy a mikroblogy – Twitter.
- Diskusní fóra a Q&A portály - Yahoo!
- Wikis – Wikipedia. Google Knol.
- Sdílená multimédia – YouTube.
- Virtuální světy – The Sims.
- Sociální záložkování – Jagg, Digg.

Obrázek č. 1 - Rozdělení sociálních médií



Zdroj: Vlastní zpracování dle Janoucha, 2013

Mezi 15 nejpoužívanějších sociálních médií k lednu roku 2019 patří na prvním místě Facebook, dále YouTube, Twitter, Instagram, LinkedIn, Reddit, VK, Tumblr, Pinterest, Google+, Flickr, meetup, Ask.fm, LiveJournal, myspace (ebizmba.com, 2019).

V České republice mezi nejoblíbenější sociální média řadíme na prvním místě Facebook, dále YouTube, Instagram, LinkedIn, Twitter a Snapchat. Začínají se ale probouzet a získávat si stále větší popularitu sociální média jako Pinterest (s počtem něco kolem 200 tisíc uživatelů), nebo Tinder (linkedin.com, 2017).

2.2 Sociální sítě

Sociální sítě jsou jedním ze sociálních médií a velmi oblíbenou internetovou službou. V roce 2009 byly sociální sítě (někdy se pro ně uvádí zkratka SNS neboli Social Networking Sites) mezi mladými lidmi nejvíce oblíbeným a v některých zemích dokonce nejvíce používaným nástrojem pro komunikaci. Sociální sítě jsou využívány zejména pro

komunikaci a sebereprezentaci jejich uživatelů a jednotlivé profily zde jde propojovat mezi přáteli. Na sociálních sítích je možné vytvářet různé skupiny, přidávat se do jiných, lze sdílet vlastní fotografie, videa, sledovat profily svých přátel a komentovat jejich příspěvky (Ševčíková a kolektiv, 2014).

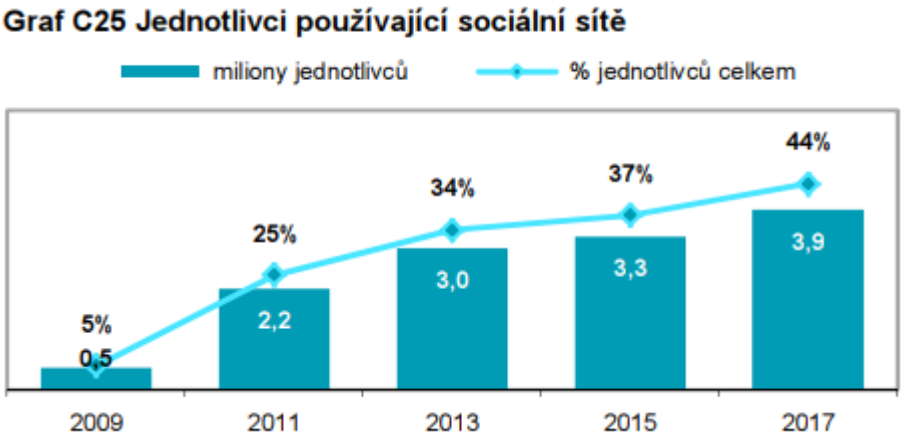
Rozmach sociálních sítí nastal v období tzv. „neomezeného Internetu“, který byl do té doby pro mnohé uživatele příliš drahý a ne úplně dostupný. V Současné době je největší celosvětovou sítí služba Facebook, kterou v roce 2016 využívalo 1,5 miliard uživatelů (Kožíšek, Písecký, 2016).

Sociální sítě patří mezi aplikace Webu 2.0, takže tato aplikace je od počátku založena na obsahu, který tvoří samotní uživatelé. Neexistuje zde žádná redakce, která by obrázek nebo příspěvek musela před publikováním schválit. Obsah publikují samotní uživatelé a sami ho i distribuují. Obsah na sociální síti je rozdělen na primární a sekundární. Jako primární lze označit ten, který vytvoří uživatel a dá k dispozici další uživatelům a sekundární je vše, čím přispívají ostatní uživatelé (komentáře) (Bednář, 2011).

Mezi lidmi, kteří žádnou síť nevyužívají, panuje názor, že sociální sítě využívají jen mladí lidé, což ale bývá často rozšířený omyl. Statistiky ukazují, že v roce 2014 bylo na Facebooku přes 46% lidí starších 35 let (Král, 2015).

Na následujícím obrázku č. 2 lze vidět, že od roku 2009 do roku 2017 se počet jednotlivců používajících sociální sítě zvýšil z 5% na 44%.

Obrázek č. 2 - Jednotlivci používající sociální sítě



Zdroj: ČSÚ, 2018

Podle marketingového výzkumu z října roku 2016 prováděný společností Focus, sociální síť využívá téměř 46 % populace, z toho 26 % lidí má profil na některé sociální síti. Nejvíce uživatelů má Facebook (42 %) a s velkým odstupem následuje YouTube, Google+, Instagram a další. Téměř polovina uživatelů Facebooku ho navštěvuje denně, navzdory sdílení aktuálních zpráv a novinek, Facebook zůstává nadále platformou orientovanou spíše na zábavu a virální obsah. Více než 80 % se na sociální sítě připojují přes jedno, maximálně přes dvě zařízení, nejčastěji se jedná o notebook nebo netbook, ze kterých na sítě vstupuje 70 % uživatelů. 63 % lidí se připojuje ze svého smartphonu (FOCUS – Marketing a Social Research, 2016).

V roce 2011 realizovala česká společnost Seznam.cz průzkum mezi 12400 uživateli. Cílem bylo zjistit, jaké osobní údaje vkládají na své profily na sociálních sítích a proč. 19,8 % uvedlo, že v profilech schválně neuvádějí pravdivé informace, nebo je alespoň zkreslují. V dotazníku také uvedli, že nevlastní pouze jeden profil, ale průměrně zhruba 2,7 profilů na sociálních sítích. Anonymitu na internetu si chválí 63 % respondentů a 20 % dotázaných uvedlo, že se obávají prozrazení údajů u svých přátel (Kožíšek, Písecký, 2016).

2.3 Česká sociální média

Před nástupem sociální sítě Facebook bylo v České republice několik velkých sociálních médií.

Mezi ty nejznámější můžeme řadit (Kožíšek, Písecký, 2016):

- Lidé.cz - nejznámější česká seznamovací síť, která se po změně konceptu v roce 2014 zaměřila spíše na uživatelské profily, soukromé chaty a diskusní fóra.
- Xchat.cz - kdysi hojně využívaná síť, která v současné době využívá hlavně chatovací služby.
- Libimseti.cz – komunitní portál nabízející profily, seznamku, chat i diskusní fóra.
- Spolužáci.cz – portál sloužící k setkávání současných ale i bývalých spolužáků v uzavřených skupinách. 2. 9. 2018 byla ale tato služba ukončena.
- ČSFD.cz – největší sociální síť zaměřená na fanoušky filmů a seriálů.
- Štěstí.cz – seznamka zaměřená na starší uživatele Internetu.
- Seznamka.cz – patří mezi nejstarší české služby nabízející seznámení prostřednictvím inzerátů.

2.4 Mezinárodní sociální média

Zahraniční média byly nedávno pro české uživatele kvůli jazykové bariéře docela nezajímavé, s lokalizací služeb se ale vše změnilo. Atraktivní se staly především z důvodu intuitivních mobilních verzí s využitím nových technologií a nejnovějších trendů. Mezi oblíbená mezinárodní sociální média kromě níže uvedených dále řadíme Whattsapp, Google +, Pinterest, Flickr, Tumblr, Snapchat a Skype (Kožíšek, Písecký, 2016).

2.4.1 Facebook

Sociální síť Facebook patří k největším webovým službám a počet uživatelů stále roste. Je přeložena do více než osmdesáti jazyků včetně češtiny. Tato služba byla založena Markem Zuckerbergem, zpočátku jako studentský komunitní projekt na Harvardské univerzitě. Později se ale rozšířila na ostatní univerzity a postupně se otevřela i pro ostatní. Výhodou služby je interakce mezi uživateli, sdílení obsahu nebo komunikační nástroje (Král, 2016).

Facebook je v dnešní době nejrozšířenější sítí. Uživatelé na něm mohou se svými přáteli sdílet fotky, statusy, videa a nově i příběhy, které jsou vidět po dobu 24 hodin a poté zmizí.

Zde je stručný přehled historie a některé zajímavé milníky (Walter, 2013):

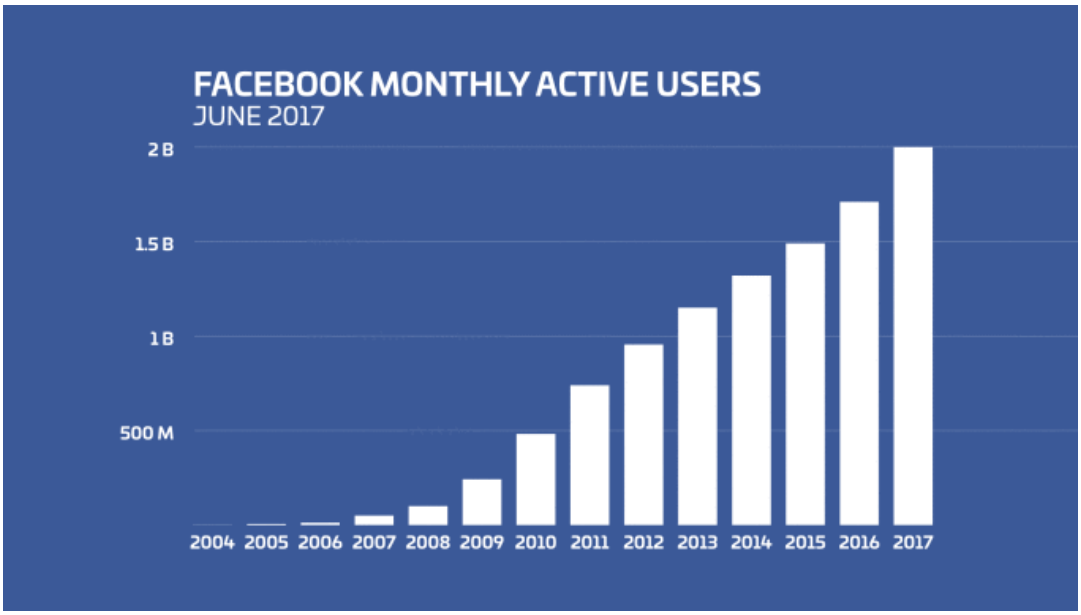
- V roce 2004 Zuckerberg s pomocí svých přátel spustil síť Facebook. Po třech týdnech měla stránka více než 6 tisíc uživatelů. Během jednoho měsíce se počet zvýšil na 10 tisíc, zatímco za další měsíc již měla dalších 30 tisíc uživatelů.
- V září roku 2004 Facebook představil dvě nejzásadnější vylepšení – Skupiny a Zeď. Myšlenka zdi si získala rychlou oblibu.
- Koncem listopadu téhož roku Facebook přesáhl jeden milion uživatelů.
- 20.9.2005 firma oficiálně přijala jméno Facebook.
- Na pozdim roku 2005 Facebook představil jednu z nejúspěšnějších funkcí – možnost nahrávat fotografie, které je možno i tagovat.
- V roce 2008 označil časopis *Time* Zuckerberga za jednoho z nejvlivnějších lidí planety.
- V březnu roku 2010 se stránka stala v USA webovou stránku číslo jedna.
- V dubnu téhož roku Facebook zavedl tlačítko To se mi líbí (Like).
- V září roku 2012 překročil počet uživatelů jednu miliardu.

Neexistuje žádná sociální síť, která by získala větší globální podíl na počtu uživatelů Internetu. Facebook se stal uznávanou platformou hlavně pro ty, kdo milují shromažďování různých videí, obrázků, informací na jednom místě. Také zde můžeme najít profily různých politiků, umělců a značek, takže uživatel má pocit, že jim je blíž. Facebook se stal nenahraditelnou součástí struktury webu a v současnosti dominuje digitálnímu prostředí. BBC World Service jako největší mezinárodní vysílací síť osloví 188 milionu lidí. Podíváme-li se ale na denní dění na Facebooku, vidíme, že toto číslo značně zaostává. Podle statistik zveřejněných Facebookem v roce 2012, se toto číslo pohybuje kolem 526 miliónů uživatelů denně (Walter, 2013).

V roce 2017 přesáhl 2 miliardy účtů, k roku 2018 má Facebook 2,13 miliard uživatelů a v České republice má účet na Facebooku přes 5 milionů uživatelů (feedit.cz, 2018).

Na obrázku č. 3 lze vidět vývoj počtu uživatelů Facebooku od roku 2004 do června 2007.

Obrázek č. 3 - Vývoj počtu uživatelů Facebooku do června roku 2017



Zdroj: sproutsocial.com, 2018

Facebook je mediálním kanálem a systémem identity. Facebookový profil se stává internetovým ekvivalentem pasu umožňujícím prokázání vlastní identity v on-line světě. Různé webové stránky uživatelům nabízejí, aby se k nim připojili právě pomocí těchto

profilů na facebooku a v tomto režimu poté mohou přecházet od jedné stránky ke druhé (Walter, 2013).

Značkám a zadavatelům reklamy umožňuje Facebook globální platformu, která jim pomáhá oslovit své současné, ale i potenciální zákazníky, s výjimkou Číny, kde Facebook zastoupen není. Jako platforma Facebook vytvořil celý nový soubor ekonomických příležitostí, které třetím stranám, podnikům, i jednotlivcům, umožňují významným způsobem rozšiřovat vlastní způsoby interakce v prostředí on-line (Walter, 2013).

V Roce 2018 měla společnost Facebook dva skandály, které se týkaly úniku dat. První z nich se týkal analytické společnosti Cambridge Analytica, která prý nepatřičným způsobem získala data téměř 87 uživatelů Facebooku a to prostřednictvím aplikací, které tito lidé a jejich známí používali. Společnost Cambridge Analytica byla obviněna z toho, že data která získala, použila k ovlivnění a zmanipulování voleb. Svou činnost tedy v roce 2018 ukončila. Díky této aféře s únikem dat se Facebook potýkal s velkým poklesem svých akcií a přerušení reklamy, či úplný odchod z této sítě oznámily například společnosti Elona Muska, časopis Playboy, nebo německá banka Commerzbank (eurozpravy.cz, 2018).

Druhý, o několik měsíců později, se týkal bezpečnostní chyby, díky které se mohli na účty uživatelů dostat hackeři a získat přístupové údaje a další informace. Přitom bylo napadeno více než 50 milionů účtů a dalších 40 milionů bylo v ohrožení. Facebook byl nucen zresetovat přístupové tokeny (díky kterým se na účet nemusíme pořád přihlašovat) k 90 milionům účtům, které se opět musely přihlásit do určité platformy, protože byly v rámci bezpečnostního opatření odhlášeny. Majitelům účtů tak přišlo oznámení, ale heslo měnit nemuseli, protože k tomu se hackeři nikdy nedostali (letemsvetemapplem.eu, 2018).

2.4.2 Instagram

Sociální síť Instagram je dnes jednou z nejoblíbenějších sociálních sítí. Byla spuštěna v roce 2010 a slouží především ke sdílení obrázků ale i videí s lidmi po celém světě. Díky hastagům se obrázek objeví u uživatele na druhém konci světa. Instagram umožňuje fotky také upravovat díky svým grafickým filtrům a udělat tak obrázek podstatně hezčí. Uživatelé si mezi sebou mohou také chatovat, nebo sdílet příběhy, buď se svými blízkými přáteli, nebo se všemi, kdo na profil narazí. V roce 2012 Instagram odkoupila společnost Facebook za jednu miliardu dolarů. Instagram se stává stále více oblíbenou aplikací a od roku 2013 do

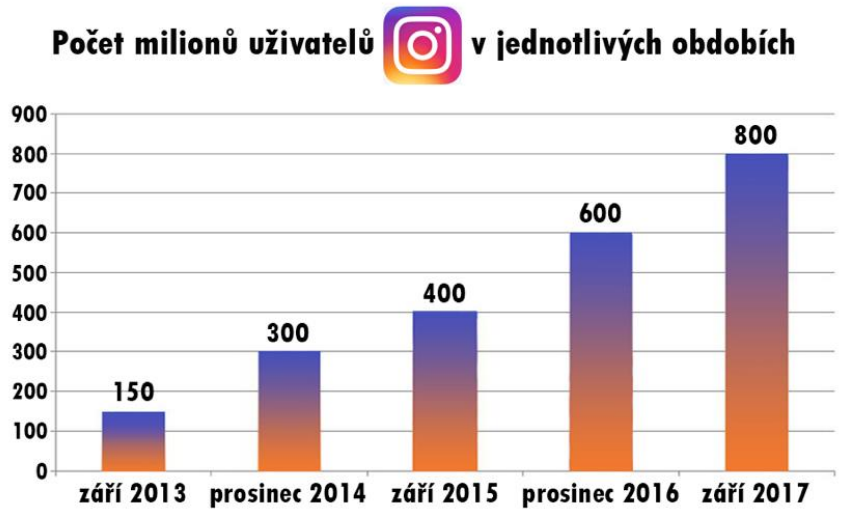
roku 2017 vzrostl počet aktivních uživatelů skoro 9x a to na 800 milionu aktivních uživatelů měsíčně (m-journal.cz, 2018).

Instagram je jednou z nejprogresivnějších sociálních médií. Po zavedení Insta stories se mnoho uživatelů ze Snapchatu přesunulo právě na Instagram. Stále nabízí více rozšířených funkcí a možností.

V České republice v roce 2017 má účet na této sociální síti něco přes 1,3 milionů lidí. Největší počet uživatelů má věková skupina 18 – 24 let (37 %) a dále lidé ve věku 25 – 34 let (27 %). Mezi uživateli převažují ženy (55 %) (anvenies.cz, 2018).

Následující obrázek číslo 4 ukazuje vývoj počtu uživatelů od roku 2013 do roku 2017.

Obrázek č. 4 – Vývoj počtu uživatelů Instagramu do roku 2017



Zdroj: anvenies.cz, 2018

2.4.3 Twitter

Toto sociální médium umožňuje uživatelům psát krátké zprávy, tzv. tweety o délce maximálně 280 znaků. Tweety jednotlivých lidí mohou sledovat jejich odběratelé, ale i lidé, kteří je nesledují, pokud mají veřejný profil. V České republice není Twitter až tak rozšířený, svou oblibu na něm nachází hlavně politici, média a firmy. Twitter se ale v poslední době stává stále více oblíbenou sociální sítí. Rostoucí popularita Twitteru se dá vysvětlit tím, že na ní přibývá čím dál více známých osobností a mnohdy na něj přispívají

více než na Facebook a ostatní sociální sítě. K roku 2018 je na Twitteru celosvětově 330 miliónů uživatelů (zive.cz, 2018).

Podle průzkumu společnosti Per Analytics, který zkoumal k čemu se Twitter používá, lze tweety rozdělit na:

- Zprávy
- Spam
- Propagace sebe sama
- Bezvýznamné bláboly
- Konverzace
- Retweety

Přes 40 % tweetů jsou jen bláboly, konverzační tweety zaujaly 2. místo (38 %) a vše ostatní je pod 10 %. Tweety se zprávami jsou až na posledním místě s 3,6 % (Janouch, 2013).

2.4.4 Ask.fm.

Lotyšská specifická sociální síť, kterou využívají především mladí uživatelé, slouží k psaní anonymních, nebo neanonymních otázek na zeď uživatele. Ten může a nemusí na ně odpovědět a sdílet je na svou zeď. Ask.fm je propojen i s jinými sociálními médii, např. Facebookem kde dotazy mohou být zobrazeny na profilech a „lajkovány“ (Kožíšek, Písecký, 2016).

Otázka ochrany soukromí na této síti řešená není. Otázky a odpovědi na ně vidí všichni a tu možnost mají i neregistrovaní uživatelé. Není zde žádný mechanismus pro nahlášení ilegálního obsahu, šikany, nebo obtěžování. Nelze zde ani nastavit úroveň ochrany soukromí a chybí užitečné rady pro mladé a začínající uživatele, jak se vyhnout možným problémům a rizikům, proto je tato síť velmi riziková a často bývá zmiňována právě v souvislosti se šikanou či nevhodným chováním.

2.4.5 LinkedIn

LinkedIn je profesně orientovaná sociální síť. Její uživatelé na ní publikují své pracovní životopisy, spojují se se svými kolegy nebo lidmi, se kterými v pracovním životě v minulosti spolupracovali. Služba slouží také pro hledání práce a pracovníků a jsou na ní aktivní pracovní agentury. LinkedIn vznikla v roce 2003 a v roce 2016 Microsoft oznámil, že tuto platformu odkoupí za 26 miliard dolarů, která byla v té době ztrátová. K roku 2017 má LinkedIn 500 milionů uživatelů, služby ale využívá měsíčně pouze 25% z nich (rychlofky.cz, 2017).

Velkou výhodou této sítě je, že pracovní vztah zde nelze navázat tak jednoduše. Dotyční s tímto propojením musí souhlasit. Vytváří se tak síť vzájemně ověřených vazeb. Na LinkedIn je také zajímavá funkce LienkdIn Answers, kde uživatelé mohou klást různé dotazy, na které lze téměř ve většině případů očekávat rozumnou odpověď. Otázky se většinou týkají odborných a obchodních záležitostí (Janouch, 2015).

Počet uživatelů v České republice v roce 2018 přesáhl 1,5 miliónů účtů. Dominují na něm muži a největšími zaměstnavateli na LinkedIn jsou Škoda Auto, T-mobile, O2 CZ a ČEZ (linkedin.com, 2017).

2.4.6 YouTube

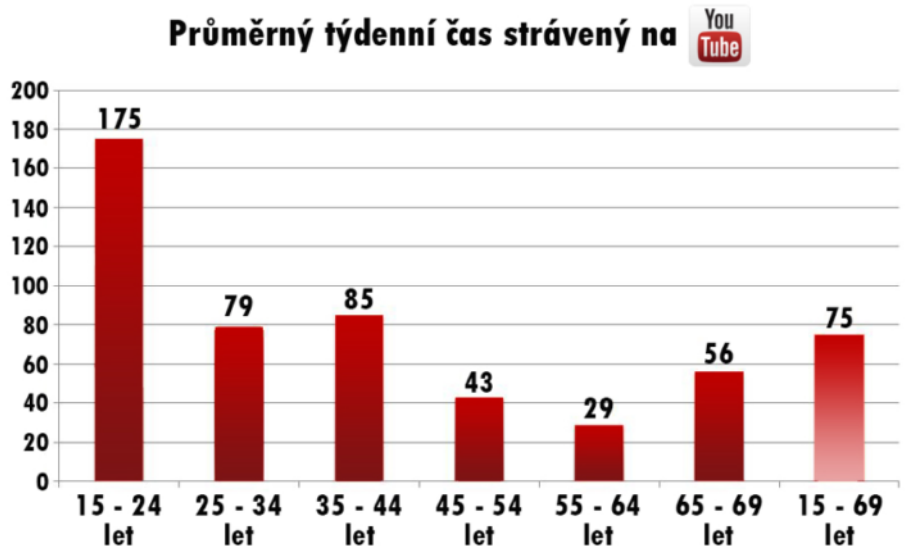
Služba YouTube je největší sítí, která umožňuje svým uživatelům sdílet, nahrávat a prohlížet videa. Internetový obsah lze také kromě samostatného serveru sdílet i na jiných webových stránkách, na sociálních sítích, nebo na různých blozích. Denně shlédnou lidé kolem 2 miliard videí a stovky tisíc lidí je nahrávají. Každou minutou je na YouTube nahráno více než 24 hodin videí. Služba YouTube je pro uživatele zadarmo, veškeré finance vycházejí z reklamy (Aktuálně.cz, 2011).

Začátek YouTube se datuje k roku 2005 a za vytvoření této služby stojí tři zakladatelé - Chad Hurley, Steve Chen a Jawed Karim. Hlavní podíl ve společnosti mají první dva. Poslední zmiňovaný, i přesto, že byl součástí týmu, který byl u zrodu YouTube a tím, kdo s originální myšlenkou přišel, se dostal do pozadí. Rozhodl se totiž pokračovat ve studiích na Stanfordské univerzitě a ve společnosti dále působil pouze jako poradce (Aktuálně.cz, 2011).

YouTube je k roku 2011 lokalizovaný v 25 zemích a 38 jazycích. Jeho uživatelé jsou obvykle lidé mezi 18 a 54 lety a poměr pohlaví je mezi uživateli stejný. Pro porovnání, v roce 2018 se na YouTube nahraje každou minutu 400 hodin videí a měsíčně je navštěvují 1,8 miliard uživatelů (Smartmania.cz,2018).

Na obrázku č. 5 lze vidět průměrný čas strávený na YouTube. Nejvíce času na něm tráví uživatelé ve věkové skupině 15-24 let, naopak nejméně uživatelé mezi 55-64 lety (anvenies.cz, 2018).

Obrázek č. 5 - Průměrný týdenní čas strávený na YouTube v minutách v roce 2017 dle věku



Zdroj: anvenies.cz, 2018

2.5 Výhody a nevýhody využívání sociálních médií

Facebook, Instagram a další sociální média jsou fenoménem 21. století a dnes je využívá téměř každý. Nesou sebou řadu výhod ale i nevýhod. Zde jsou uvedeny některé z nich.

2.5.1 Výhody

- **Komunikace**. Největší podstata sociálních médií. Lidé spolu mohou komunikovat z celého světa kdykoliv a odkudkoliv. Uživatel může své myšlenky a nápady sdílet s velkým množstvím přátel a udržovat s nimi stále kontakt a to především s lidmi, se kterými není možné se vidět (list25.com, nedatováno).

- **Možnost vzdělávání**. Na sociálních médiích mohou studenti, učitelé (ale nejenom ti), sledovat odborníky a specialisty v oboru, ve kterém se chtějí zdokonalovat a učit se od nich bez toho aniž by za to museli platit (techmaish.com, 2016).
- **Marketing**. Dnes jsou na sociálních médiích miliardy lidí a tak by měly být zahrnovány do marketingu každého podnikatele, či firmy, která chce být úspěšná. Firma k tomu může využít například influencery, kteří jejich produkt či službu na některé sociální sítí zpropagují, nebo si mohou na sociálních médiích vytvořit svůj profil a informovat tak své potenciální nebo stálé zákazníky, pořádat různé soutěže. Propagují zde však také různé nevládní, neziskové a dobrovolné organizace, které si takto zase mohou zajistit větší podporu a sdílení. Podnikům sociální média také umožňují dělat průzkumy mezi spotřebiteli a zjistit tak cenné informace pro další působení na trhu (list25.com, 2017).
- **Povědomí.** Sociální média také vytvářejí povědomí a inovují způsob života lidí. Pomáhají lidem objevovat nové a inovativní přípravky, které jim mohou usnadnit život. Ať už pomocí již výše zmíněných influencerů nebo reklamy (techmaish.com, 2016).
- **Boj proti kriminalitě.** Policisté a vláda mohou využít sociální média k nalezení zločinců, k boji proti kriminalitě a ke zlepšení situace v oblasti kriminality ve své zemi (legit.ng, 2019).
- **Informovanost.** V dnešní době skoro každý kdo ráno vstane, jako první shlédne sociální média a jelikož skoro veškerá informační média mají na Facebooku či Twitteru svůj profil, je možné tak sledovat aktuální dění a zprávy přímo na nich. Sociální média také mohou pomoci při ověřování informací, jelikož jak v televizních tak tištěných médiích mohou být nepravdivé informace. Facebook má i tu funkci, že v případě zemětřesení, teroristických útoku nebo podobných situacích umožní informovat přátele, že jsou v pořádku a mimo ohrožení a to pouze pomocí pár kliků (techmaish.com, 2016).

2.5.2 Nevýhody

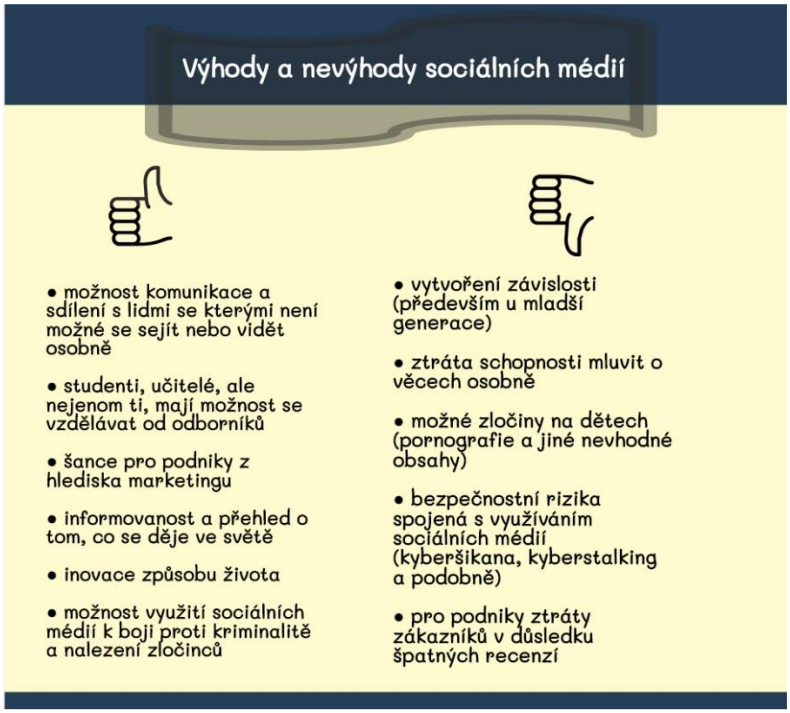
- **Závislost.** Tato nevýhoda převažuje spíše u mladší generace, která na nich tráví většinu svého volného času. Spousta z nich by ale tento čas mohla věnovat mnohem produktivnějším aktivitám. Někteří si neumějí život bez sociálních médií ani představit a spoustě z nich mohou tyto média značně zasahovat do běžného života (techmaish.com, 2016).
- **Ztráta schopnosti mluvit o věcech osobně.** Tím, že lidé spolu stále více a častěji komunikují na sociálních médiích prostřednictvím online chatu a zpráv, spoustu lidí tak tuto komunikaci využívá k řešení problémů. Někteří lidé tak nejsou schopni vyjádřit

svůj názor nebo řešit problém s člověkem osobně bez využití sociálních médií. Tím, že spolu lidé mluví a komunikují prostřednictvím sociálních médií, také ztrácejí schopnost chápat a rozpoznat pocity a emoce toho druhého (rootsofaction.com, 2014).

- **Reputace.** Sociální média mohou snadno někomu zničit pověst tím, že o něm nějaký uživatel sdílí nebo píše falešný příběh, který se může dostat k velkému množství lidí. Podobně i podniky mohou utrpět ztráty v důsledku špatné pověsti přenášené přes sociální média (špatné recenze od zákazníků a podobně) (techmaish.com, 2016).
- **Zločiny na dětech**. Využití sociálních médií může vystavit jednotlivce různým formám obtěžování nebo nevhodnému kontaktu. To platí zejména pro dospívající a mladší děti. Pokud rodiče neúplně filtrují obsah webu, děti by mohly být vystaveny pornografii nebo jinému nevhodnému obsahu (lovetoknow.com, nedatováno).
- **Bezpečnostní rizika**. Při využívání sociálních médií hrozí uživatelům bezpečnostní rizika. Ať už jde o zneužití osobních údajů, různé formy podvodů, vydírání, kyberšikanu, nebo kyberstalking, rizik, které uživateli sociálních médií hrozí, je mnoho a ne vždy jde ovlivnit jejich nastání.

  Na obrázku č. 6 lze tyto výhody a nevýhody vidět v grafickém znázornění.

Obrázek č. 6 - Výhody a nevýhody sociálních médií



Zdroj: Vlastní zpracování, 2019

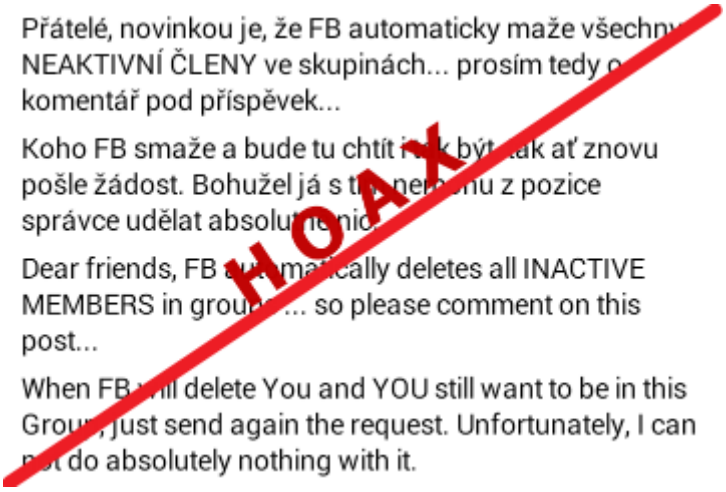
2.6 Dezinformace a hoaxy

Jednou z možností na sociálních médiích je, že kdo si na nich založí profil, může si do obsahu a na svůj profil dávat téměř co chce, vyjma některých obsahů, které jsou trestné (šíření pornografie apod.). Tato možnost s sebou ale také nese další věc – ne všechno, co daný člověk na sociální sítě dá, musí být pravdou. Ať už se jedná o údaje, které na ně uživatel vložil (vyšší/nižší věk, falešné jméno), tak o informacích a statusech, které na svůj profil sdílí.

Jedním z běžných jevů na Internetu a sociálních médiích je hoax. Lze ho označit jako zbytečnou řetězovou zprávu, která se šíří bleskovou rychlostí a využívá neinformovanost a důvěru rozesílatelů. I když existuje řada druhů hoaxů, mají jeden znak společný – nabádají k dalšímu rozesílání a sdílení. Jedná se například o e-mail začínající slovy „pošli tento e-mail dalším pěti kamarádkám, nebo budeš mít 10 let smůlu“. Hoaxy ale mohou mít různý obsah. Může se jednat o informace zábavné, varující před nebezpečím, falešné prosby o pomoc a petice, citově vydírající, nebo varující před virovým ohrožením. Některé hoaxy ale mohou sloužit i ke zneužití osobních údajů, a to proto, že při přeposílání hoaxu lidé většinou nechávají předešlé příjemce ve zprávě. Takto Internetem běží dlouhý seznam e-mailových adres, což zvyšuje riziko toho, že je někdo zneužije (Gregor, Vejvodová, 2018).

Jedním z příkladů hoaxů (viz obrázek č. 7 níže) je zpráva, která vybízela členy skupiny, aby okomentovali příspěvek, jinak je Facebook automaticky smaže jako neaktivního člena. Facebook ale sám od sebe neaktivní členy nemaže, ale jen měnil způsob, jakým jsou uživatelé do skupin pozváni. Dříve mohli členové pozvat své přátele, aby se stali členy skupin a ti se jimi poté automaticky stali. Podle nových pravidel jsou ale tito uživatelé přesunuti do sekce pozvaných a libovolný člen skupiny je musí schválit. Jedná se tedy o špatnou interpretaci zprávy. První výskyt tohoto hoaxu byl letos v lednu (hoax.cz, 2019).

Obrázek č. 7 - Příklad hoaxu



Zdroj: hoax.cz, 2019

Dalším z jevů vyskytujících se převážně v médiích a na sociálních sítích jsou fake news. Novým pojmem fake news označujeme již staré a známé dezinformace. Tento termín proto, protože jsou úmyslně nepravdivé, nebo zavádějící. Autor má jediný cíl – zmanipulovat a ovlivnit příjemce těchto informací (Gregor, Vejvodová, 2018).

Dezinformace se objevují v médích téměř každý den a k jejich rozmachu dopomohl Internet a sociální sítě, pomocí nichž se tyto klamavé informace dostanou k většímu počtu lidí. U nás nejčtenějším deníkem je bulvární Blesk. Nejvíce se totiž prodávají skandály, nebo zákulisní informace. Toho si samozřejmě nemohli nevšimnout novináři, ani známé osobnosti, které toho využívají ve svůj prospěch (Gregor, Vejvodová, 2018).

Jako příklad dezinformací ve světě lze uvést příklad z USA. Těsně před prezidentskými volbami vyšla řada dezinformací a manipulativních informací. Tyto informace zahltily Facebook a Twitter. Jejich obsahem byla především lživá informace o tom, že jednoho z kandidátů, Donalda Trumpa, podporuje sám papež, nebo o připravované žalobě FBI na Hillary Clintonovou. Za těmito dezinformacemi stáli makedonští teenageři, kteří si tak vydělávali prostřednictvím zobrazování reklamy (rozhlas.cz, 2016).

Dezinformace se ale šíří také v Česku. Například z oblasti zdravotnictví, sem patří konspirační teorie o škodlivosti očkování. Dále známá dezinformace o tom, že Česko chce zrušit písmeno Ř, která se objevila na webu Weeks.cz. (info.cz, 2018) Dále vytvářené

falešné citáty významných osobností jako např. Karla IV, nebo Jana Wericha. Lze najít také falešné citáty, které jdou přímo proti konkrétnímu politikovi nebo politickému subjektu (viz obrázek č. 8 níže). Nejznámějšími dezinformačními weby v ČR jsou Sputnik, Svět kolem nás, Lajkit, nebo Parlamentní listy (rozhlas.cz, 2016).

Obrázek č. 8 - Falešný citát sdílený podporovatelem SPD a Miloše Zemana, který sdílelo 6.5 tisíce lidí

Zdroj: info.cz, 2018

V České republice dezinformace znepokojují 73 % uživatelů Internetu. U nás se této problematice věnuje Ministerstvo vnitra, které k tomuto účelu zřídilo speciální oddělení. Tématem se zabývala i bezpečnostní rada státu, evropský akční plán ale musí schválit senátoři a poslanci (seznamzpravy.cz, 2019).

V boji proti dezinformacím v ČR vzniklo několik projektů. Jedním z nich je stránka demagog.cz, která ověřuje informace a výroky českých předních politiků a to pomocí dohledávání primárních zdrojů. Snaží se poukazovat zejména na nepravdivá a manipulativní vyjádření, která křiví veřejný prostor. Za dobu jejich fungování byly ověřeny už tisíce výroků. Projekt se dočkal i některých ocenění, např. v roce 2012 Novinářská cena, či Křišťálová lupa. Demagog vychází především z fungujících organizací jako PolitiFact, nebo FactCheck.org (demagog.cz, 2012).

Dalším projektem, který se snaží zamezit dezinformacím je publicistický web Manipulátoři.cz. Věnují se oblasti politického marketingu, PR a komunikačních strategií. Zastávají názor, že skrývání faktů nemůže přinést nic dobrého a jejich cílem je vytvořit otevřenou neideologickou platformu a faktickou diskusi (manipulatori.cz).

Posledním projektem, je projekt zvolsi.info, který jako oba předchozí projekty bojuje proti fake news a manipulacím. Projekt založili studenti z Masarykovy univerzity v roce 2016 a sepsali *Surfařův průvodce po internetu*, který čtenářům poslouží jako takový jednoduchý návod, jak se ve světě medií neztratit a nenechat se zmanipulovat. Také vystupují na školách a snaží se studentům své rady předat i osobně (zvolsi.info.cz, 2019).

3 Bezpečnost a rizika používání sociálních médií

3.1 Bezpečnost

Internetová bezpečnost je relativně mladý pojem. Začala se řešit až na přelomu 80 a 90 let 20. století, i když k propojování počítačů docházelo již dříve. Doba kdy uživatelům hrozila „jen“ zavirovaná disketa je bohužel už minulostí (Eckertová, Dočekal, 2013).

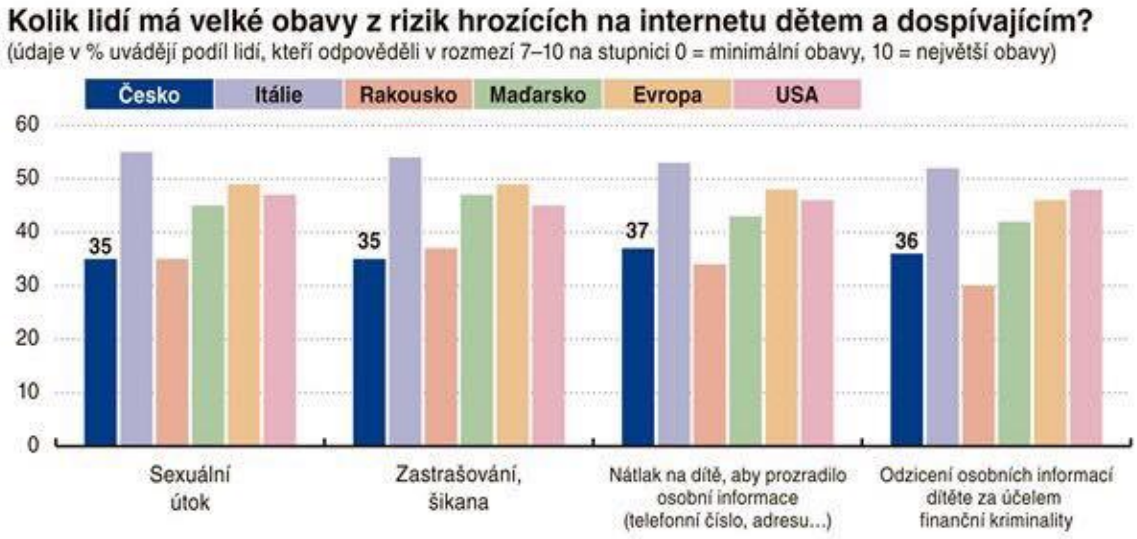
Nebezpečí na Internetu a sociálních médiích stále roste. Stále se objevuje více možností, jak si útočník může najít cestu k oběti. Největší chyba, které se uživatelé Internetu dopouštějí, je, že jsou přesvědčeni, že tohle se jim nikdy stát nemůže. Ale i člověk, který se snaží chovat na Internetu bezpečně, se tou obětí klidně může stát. Je proto třeba být opatrný a znát rizika, která uživatele mohou na Internetu a hlavně – na sociálních médiích – potkat, protože některá z nich do značné míry lze svým chováním ovlivnit a omezit nebo v opačném případě zvýšit pravděpodobnost jeho nastání.

3.2 Rizika a riziková chování na sociálních médiích

Riziko lze označit jako nežádoucí událost, která může, ale také nemusí nastat. Můžeme ho chápat také jako pravděpodobnost výskytu negativního jevu, které je důsledkem určitého chování, či vystavení se nějaké nechtěné situaci (Ševčíková a kolektiv, 2014).

Podle průzkumu Europ Assistance, kterého se zúčastnilo přes 7000 respondentů z Evropy a USA ukazuje, že Češi mají největší obavy z rizika, že bude vyvíjen nátlak na jejich dítě, aby prozradilo své osobní údaje. V porovnání s ostatními zeměmi - nejvíce se těchto rizik obávají Italové a nejméně Rakušané. Další rizika, kterých se Češi obávají, lze vidět na obrázku č. 9 (idnes.cz, 2019).

Obrázek č. 9 - Obavy z rizik hrozících na Internetu



Zdroj: idnes.cz

Rizik, která uživatele na sociálních sítích mohou potkat, je spousta. Je potřeba je znát, umět na ně reagovat a především snažit se na sociálních médiích chovat tak, aby nedocházelo k jejich prohlubování. V následujících podkapitolách jsou uvedeny a popsány rizika, která značným způsobem mohou uživatele sociálních médií ohrozit.

3.2.1 Phishing

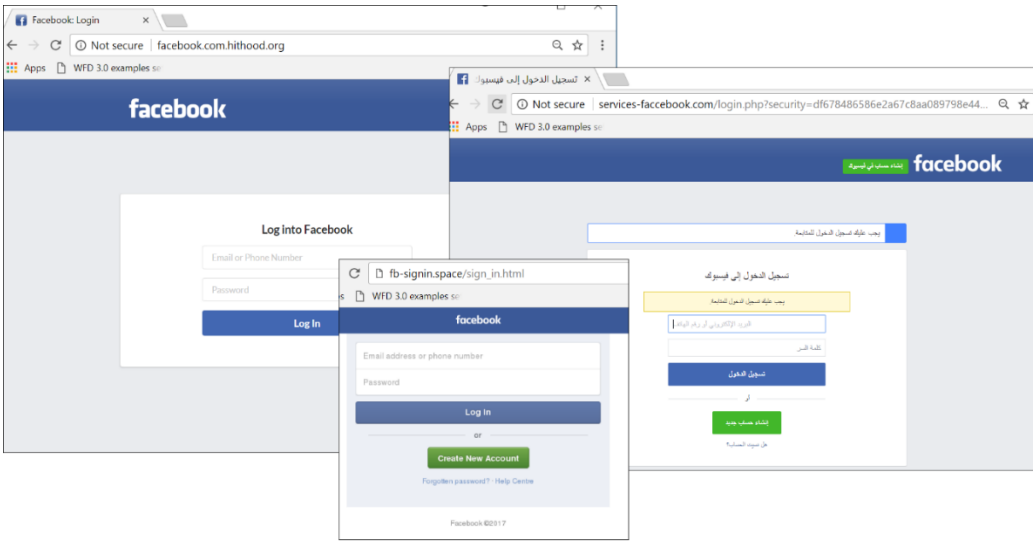
První z rizik, které při používání sociálních médiích hrozí, je phishing. Jedná se o složeninu anglických výrazů ..phreaking“ a „fishing“. Zatímco slovo „fishing“ opravdu znamená rybaření, slovo ,,phreaking“ je odovozené slovo z „phone freaking“, neboli telefonování. V USA, v dobách, kdy elektronika začínala, bylo velice populární ,,nabourání “ do telefonních systémů. Předchůdci novodobých hackerů díky tomu mohli telefonovat bez poplatků. Základní myšlenka phishingu je vytáhnout z oběti přihlašovací údaje, hesla, PINy ke kartám, bankovní údaje a tak dále pod nejrůznějšími záminkami. Využívá přitom oblíbených sociálních sítí, banky, internetové obchody a rozesílá zprávy, které se zdají býti dost věrohodné. Často používají upozornění na nedostatečné údaje zabezpečení počítače, a aby se zabezpečení vylepšilo, uživatel musí uvést právě výše uvedené údaje (Petrowski, 2014).

Zadáním přihlašovacích údajů do formuláře na takto podvodných webových stránkách je uživatel v podstatě předává útočníkovi k dispozici, aniž by o tom sám věděl a ten je poté využije ke svému prospěchu. Poslední dobou se zprávy s phishingovým odkazem šíří přes sociální sítě a mnohdy i zkušený uživatel může mít problém s tím, tento druh podvodu odhalit (internetembezpecne.cz, nedatováno).

Je třeba tyto útoky včas rozpoznat. Někdy lze phishing poznat už jen podle samotného názvu v předmětu e-mailu (osamělé ženy, XXX, apod.). Bohužel existují i velmi rafinované typy přesvědčivých e-mailů. Další pomůckou jak tento podvod odhalit může být koncovka e-mailové adresy. Pokud napíše e-mail někdo s adresou, která je těžce identifikovatelná, např. manueldf@dfgetf.vr, s největší pravděpodobností se jedná o phishing. Je třeba si také uvědomit, že seriózní společnosti by nikdy své klienty nenutily zasílat jim důležité údaje emailem (channelworld.cz, 2018).

Na následujícím obrázku č. 10 lze vidět příklad phishingového útoku, který chtěl vylákat přihlašovací údaje na Facebook.

Obrázek č. 10 - Příklady stránek phishingu, které napodobují přihlašování do služby Facebook



Zdroj: securelist.com, 2018

3.2.2 Kybergrooming

Dalším rizikem, se kterým se uživatelé Internetu mohou setkat, je kybergrooming. Jedná se o situaci, kdy se pachatel snaží se svou obětí komunikovat, kontaktovat ji přes sociální sítě, nebo jiným způsobem, získat si především její důvěru a tím ji přimět k osobní schůzce. Nejvíce jsou tímto ohrožovány děti, protože získat si důvěru u dětí je nejsnazší. Pachatel se chce s osobou setkat za účelem zneužití, prostitucí, zmanipulování, nebo přijmout ji k nějakému trestnému činu. Za kybergrooming se ukládá trest odnětí svobody až na 2 roky (Jansa a kolektiv, 2016).

Většinou útočníci využívají více profilů, aby působili důvěryhodně. Nejen, že si vytvoří svůj profil, ale vytvoří si i profil svých kamarádů, čímž se snaží dokázat pravost a získat si důvěru. Na své profily vkládají zajímavé fotografie a obsah a oběť tedy může snadněji podlehnout, než kdyby profil byl prázdný a nicneříkající (Kožíšek, Písecký, 2016).

Pachatelé se snaží svou oběť nalákat. Může jít o nabídku dobití kreditu, nebo vstupenky na koncerty a festivaly, zaplatit to, co oběť zrovna potřebuje – například nový telefon, nebo může slíbit setkání s nějakou celebritou, kterou předstírá, že zná (Kožíšek, Písecký, 2016).

Nelze určit, jaké osoby se stávají kybergroomery, nebo co je příčinou jejich jednání. Může se jednat o osoby s nízkým sociálním statusem, ale i vysoce postavené a vzdělané jedince. Mezi útočníky ale převažují osoby, které dosud nebyly trestány. Kybergroomer se může bavit experimentováním s více lidmi najednou a zůstat pouze u virtuální komunikace, nebo může směřovat k fyzickému zneužití oběti (Eckertová, Dočekal, 2013).

Dítě se většinou nechá vylákat na schůzku, protože se domnívá, že na druhém konci sedí opravdu celebrita nebo její idol. Těší ji, že si celebrita vybrala zrovna jeho a konverzace se může časem změnit z nezávazné na domluvu schůzky v reálném světě. Kybergoomer vždy přizpůsobuje obsah zpráv dané situaci a věku oběti. Mnohdy se oběť nechá zlákat, protože o tomto nebezpečí nemá dostatek informací a naivně si myslí, že kybergoomer je opravdu ten, za koho se vydává. Z průzkumu *EU Kids Online 2011* vyplývá, že se děti nebojí seznamovat a udržovat kontakt na Internetu s lidmi, které nikdy neviděli naživo. Celkem je to 30 % dětí ve věku 9-16 let a velké procento z nich souhlasí po nějaké době i s osobní schůzkou aniž by to předem ohlásily rodičům (Eckertová, Dočekal, 2013).

Příklady těchto útoků můžeme nalézt po celém světě a stále je jich větší množství. V České republice za zmínku stojí příběh kybergoomera Pavla Hovorky, který pracoval jako ostraha a přispíval dětským domovům. Své oběti, mladé chlapce, většinou kontaktoval a vyhledával na seznamovacích portálech. Se svými obětmi si nějaký čas dopisoval a poté je pozval k sobě do práce, kde je nutil k pohlavnímu styku, některé z nich také vydíral a chtěl po nich nahé fotografie, za které nabízel peníze. Obtěžoval takto více než 20 chlapců (iDnes.cz, 2009).

3.2.3 Kyberšikana

Na Internetu je běžné, že se ne vždy všichni se všemi shodnou. Mohou se hádat veřejně do komentářů, nebo si i zanadávat. Toto chování ale může přerůst v něco mnohem silnějšího a uživatelé se mohou stát aktéry nebo oběťmi šikany. Kyberšikana, na rozdíl od klasické šikany, je formou častější a oběť ji nemá šanci předvídat (Louie Stowell, 2017).

Cílem kyberšikany je oběť ponížit, zesměšnit, zastrašit, nebo jinak ji ublížit za pomocí moderní technologie (Internet, mobily..). Aby se mohlo skutečně hovořit o kyberšikaně, je nutné, aby probíhala opakovaně, aby oběť byla napadena cíleně a to buď jednou osobou, nebo skupinou. Někdy je kyberšikana spojena i s klasickou šikanou, kdy je osoba napadána i fyzicky (Kožíšek, Písecký, 2016).

Pod kyberšikanu spadají činnosti jako zasílání výhružných SMS, e-mailů nebo jiných zpráv, například na sociálních médiích, dále sem patří činnosti jako zveřejňování videí online (většinou ty, které mají oběť ponížit), přeposílání osobních informací a fotek bez souhlasu, zasílání sexuálních snímků, o které ale příjemce nemá zájem a v neposlední řadě také zřizování falešných účtů za účelem zesměšnění (Louie Stowell, 2017).

Někdy pod kyberšikanu spadá i tzv. Happy Slapping, jinak řečeno natáčení fyzického útoku. Jedná se o útok na náhodně vybranou osobu, například kolemjdoucího v parku. Jeden z aktérů napadne oběť a další to vše natáčí. Cílem je získat originální dokument, který poté budou moci zveřejnit na některých portálech pro sdílení videa. Happy Slapping se rozšířil především ve Velké Británii, kde zvláštní kategorií se zde stalo napadání fyzicky slabých, především opilých bezdomovců. Motivem zde bývá přijetí do různých skupin a gangů – útočníci mají pocit moci a cítí se dobře v partě silných (Eckertová, Dočekal, 2013).

Oběťmi kyberšikany se v kolektivu velmi často stávají ti, kteří nejsou moc populární, nebo ti, kteří jsou ostatními odmítány. Většinou jde o plaché, stydlivé, nejisté a úzkostné děti, které se výrazně vybočují a jsou něčím jiní, například výrazná barva vlasů, styl oblékání, rovnátka, brýle apod (Ševčíková a kolektiv, 2014).

Účinky kyberšikany jsou mnohdy mnohem závažnější než u klasické šikany a to zejména proto, že oběť neví, kým je napadána, kdo za tím vším stojí, jestli je to člověk z jejího okolí, nebo někdo, koho vůbec nezná, dále také proto, že do kyberšikany se může zapojit více agresorů a ponížení oběti může sledovat více lidí (internetembezpecne.cz, nedatováno).

Podle výzkumu rizikového chování uživatelů Internetu, které realizovalo e-bezpečí a Seznam.cz, 13,70% někdy zažilo ponižování a ztrapňování pomocí šíření fotografií. Bezmála 18% někdy zažilo vyhrožování a zastrašování a s verbálními útoky se setkalo více než 30% dotazovaných (Kožíšek, Písecký, 2016).

3.2.4 Sexting

Pod pojmem sexting se skrývá složenina dvou slov – texting a sex. Označuje situaci, kdy uživatel vědomě zasílá vlastní či jen sdílí odhalené fotografie, videa, nebo texty s erotickou tématikou pomocí komunikačních technologií. Je třeba si uvědomit, že v mnoha případech tyto fotografie a jiné materiály nezůstanou jen mezi nimi, ale začnou se šířit – buď mezi kamarády, nebo přímo veřejně na Internetu. Zpráva z Internet Watch Foundation z roku 2012 uvádí, že až 88% citlivých obrázků a videí jsou zveřejněny na jiném než původním zdroji (Eckertová, Dočekal, 2013).

Mezi dospívajícími je takové dopisování každodenní realitou. Dospívající „sextují“, když chtějí upoutat pozornost, chtějí projevit zájem anebo dát partnerovi najevo svou oddanost. Problém ale přichází ve chvíli, kdy jejich vztah skončí. Bývalý partner, který má tyto materiály stále uložené v telefonu nebo počítači, je může velmi jednoduše zveřejnit na sociálních médiích nebo je rozesílat e-mailem. Podobných případů přibývá a některé z nich už dokonce skončily sebevražedným pokusem, kdy oběť neunesla ponížení způsobené zveřejněním jejich intimních fotografií (safeinternet.cz, 2012).

Jedním z příkladů, kdy fotografie zaslané v soukromém chatu byly zneužity, je případ, kdy se na Facebooku vytvořila skupina „Pražské roztahovačky“, na kterou členové skupiny

přidávali fotografie, které jim dívky zaslaly. Většinou tato fotografie byla doplněna o popisek, o jakou dívku jde, její jméno a popis. K této skupině se postupně přidala i další města jako Olomouc nebo Brno. Tuto kauzu ještě více podpořila média, která o ní začala informovat. Někteří uživatelé se snažili tyto skupiny nahlásit, avšak podle služby bylo toto jednání v pořádku. Poté se do situace vložila policie, která zjišťovala, zda se jedná o trestný čin, ale povětšinou byla věc odložena s odůvodněním, že fotografie, které se objevovaly na skupinách, byly uveřejněny samotnými oznamovatelkami na jiných veřejných internetových službách (Kožíšek, Písecký, 2016).

V roce 2017 realizoval projekt e-bezpečí ve spolupráci s O2 výzkum, který byl zaměřený na rizikové faktory v prostředí Internetu u českých dětí. Z průzkumu vyšlo, že 74 % respondentů považuje sexting za velmi rizikový. Ukázalo se také, že sexting mezi dětmi stále roste. V porovnání s rokem 2012 vzrostl o 42 % na dnešních 15 %. Motivací pro sexting je u 63 % dětí upoutání pozornosti, 61 % má jako motivaci flirtování a 46 % si díky tomu chce získat přátele. Nástroje, které pro sexting využívají, jsou především Facebook (65,73 %), dále Facebook messenger (54,13 %) a Snapchat (50,93 %). Co je ale alarmující – v případě zneužití obsahu zaslaných v rámci sextingu by o tom více než 30 % nikomu neřeklo. Pouze 38, 83 % respondentů by to oznámilo rodičům (e-bezpeci.cz, 2017).

3.2.5 Kyberstalking

Pokud osoba narušuje soukromí jiné osoby, dlouhodobě ji pronásleduje, vyhledává její přítomnost, omezuje ji a vyvolává v ní pocity jako strach, úzkost a paniku, jedná se o stalking. Při využití Internetu (například sociální média, email..) a mobilního telefonu se hovoří o kyberstalkingu (Eckertová, Dočekal, 2013).

V dnešní době je snadné si o člověku zjistit na sociálních médiích spoustu informací. Existují na to i speciální stránky, například stalkface.cz, do které stačí vložit odkaz na facebookový profil a pak už jen stačí vybrat, co o dané osobě chce uživatel vědět (například fotky, stránky a příspěvky, které lajkuje a podobně). To dává samozřejmě možnost stalkerům zjistit si o osobě co nejvíce údajů.

Kyberstalking jak je již uvedeno výše, znamená stalking na Internetu. Stejně jako kyberšikana, tak i kyberstalking se může pojit s tradičním stalkingem v reálném životě. Může docházet k přímým či nepřímým výhružkám, fyzickému pronásledování oběti, čekání

na oběť například před školou, před domem a podobně. Dále také stalker může vyhrožovat fyzickým útokem na osoby blízké oběti. Dále mezi projevy patří snaha o poškození pověsti oběti a očernění prostřednictvím šíření nepravdivých informací (Kožíšek, Písecký, 2016).

V České republice je toto pronásledování označeno jako trestný čin nebezpečného pronásledování, za který lze udělit 1 až 3 roky odnětí svobody. Do tohoto trestného činu také spadá vytrvalé kontaktování právě prostřednictvím elektronických komunikací, kdy oběť má obavu o svůj život nebo zdraví a také život blízkých (Jansa a kolektiv, 2016).

Většinou se stalkerem stane člověk, který je nevyrovnaný, nesouhlasí s ukončením vztahu, cítí se ublížený, nebo že je s ním nespravedlivě zacházeno. Často to také bývají osamělí lidé. Někdy pro ně oběť může být objektem sexuální touhy, toužící po intimitě a vztahu. Jsou posedlí a mají rádi pocit kontroly nad svou obětí (jdidoklubu.cz, 2016).

Pronásledovanými lidmi bývají celebrity – díky dostupným informacím snadno stalker najde, kde se nachází, dále bývalí partneři – ti se obětmi stávají vůbec nejčastěji, dále také známí stalkera, kolegové z práce, spolupracovníci – především kvůli závisti nebo nesnášenlivosti a cizí lidé, u kterých jde často o sexuální motiv (jdidoklubu.cz, 2016).

3.2.6 Krádež identity

Posledním uvedeným rizikem, se kterým se na Internetu uživatel může setkat, je krádež identity. Stále roste počet případů podvodů, kdy se uživatelé Internetu snaží vystupovat pomocí falešné identity nebo své informace zkrášlují. Někteří z nich mají svou vymyšlenou identitu promyšlenou do detailů, takže i pro odborníky je někdy těžké ji rozpoznat. Mnozí z nich se tak vydávají za celebrity, producenty, lékaře, investory, nebo za normální lidi ať už jde o známé nebo cizí. Tito lidé používají metody sociálního inženýrství, takže velmi dobře znají metody, které na první pohled přesvědčí člověka o jeho pravosti (Kožíšek, Písecký, 2016).

S krádeží identity se setkáváme už odjakživa. V současné době se změnila jen její podoba. Namísto fyzického vydávání se za někoho jiného pomocí ukradených listin a dokumentů, nebo zevnějškem, dnes jsme uváděni v omyl na základě počítačové masky (bezpecnyinternet.cz, nedatováno).

Krádež identity se řadí mezi kriminální činy, kdy cílem útočníka je získat citlivé údaje své oběti a poté se za oběť vydávat. Motivací může být poškození dobrého jména, finanční zisk, nebo motivem může být i pomsta. Útočník může odcizit heslo, podrobnosti o kreditní kartě, nebo číslo občanského průkazu. Velmi dobrým zdrojem jsou právě profily na sociálních sítích a podobných oblíbených službách (eset.com, nedatováno).

3.3 Obrana proti rizikům

Pokud už se uživatel s některým z rizik setká a stane se obětí některého z nich, je důležitě vědět, jak se v takovém případě zachovat, na koho se obrátit a jak se z této nepříjemné situace dostat.

Pokud se uživatel stal obětí podvodného e-mailu a sdělil své důvěrné údaje třetí osobě, je v první řadě nutné ihned kontaktovat svou banku, ovšem oficiální cestou, například přes hotline. Pokud si to uvědomil včas, může zkusit své údaje oficiální cestou urychleně změnit, aby se k nim útočník nedostal. Bohužel, na většinu těchto případů se přijde až po delší době. Jelikož se jedná o trestný čin, je také dobré nahlásit to na Polici ČR a podat trestní oznámení na neznámého útočníka. Většina prohlížečů také umožňují nahlásit phishing, pokud si právě prohlíží stránku snažící se vylákat údaje, takže lze využít i tuto možnost (bezpecnyinternet.cz, nedatováno).

Pokud se někdo dostane do takové situace, že ho někdo sleduje, vydírá, obtěžuje, nebo jinak napadá - především by si to neměl nechávat pro sebe. Měl by se svěřit buď rodičům, kamarádům, nebo někomu komu věří, anebo využít některou z anonymních cest – například linku bezpečí, nebo některou z poraden. Pokud je obětí žák/student, lze se obrátit na školu, která ví, jak dále postupovat. Je důležité s útočníkem nekomunikovat, v žádném případě neodpovídat a nesnažit se ho prosit o to, aby toho nechal. Je třeba tohoto člověka zablokovat a ukládat si všechny zprávy, nebo příspěvky které o uživateli sdílel nebo rozesílal.

Pokud je uživateli vyhrožováno, že pokud neodpoví, něco udělá (například mu smaže účet, nebo si na něj někde počká), ani zde by se nemělo na takové zprávy odpovídat. Většinou se oběť lekne, a pokud ji útočník vydírá, dělá přesně to, co po ni požaduje. Ale je třeba si uvědomit, že s tím útočník nepřestane a oběť se tak bude točit v kruhu, ze kterého se nedostane, pokud s ním komunikaci neutne a nepožádá o pomoc.

Pokud někdo uveřejnil fotografii s citlivým obsahem, kterou mu uživatel zaslal, je třeba řešit situaci okamžitě, aby nedošlo k jejímu dalšímu rozesílání. Je potřeba také kontaktovat správce stránek a požádat ho o smazání příspěvku, do žádosti uvést co nejvíce podrobností s důkazem, že se jedná skutečně o osobu, která je na fotografii. Je důležité se neobracet na subjekty, které slibují stažení obsahu z Internetu a jsou placené – jedná se o podvodné stránky (Kožíšek, písecký, 2016).

Ve všech těchto případech je třeba smířit se s tím, že se uživatel stal obětí a že se tomu (ve většině případů) nedalo vyhnout. Uživatel by si to neměl pokládat za vinu, jako se to v některých případech stává. Měl by se z této situace poučit a snažit se v této oblasti vzdělávat, aby v případě dalšího napadení už věděl, co dělat, nebo pokud by se obětí stal někdo z jeho okolí, aby mu mohl poradit a pomoci.

V následující kapitole jsou uvedeny projekty, které popisují, jak se proti těmto rizikům bránit a na které se lze obrátit.

3.4 Projekty, které pomáhají

V České republice existuje řada projektů, které mají za cíl eliminovat bezpečnostní rizika, vzdělávat uživatele Internetu v této problematice a především snažit se pomoct, pokud k některému z nich dojde.

3.4.1 Linka Bezpečí

Pro pomoc lze využít Linku bezpečí, která je největší a nejdéle fungující linkou pro děti a mladistvé do 26 let po celém území ČR. Denně se na tuto linku obrací 700 dětí a mladých lidí. Číslo na tuto linku je snadno zapamatovatelné – 116111 a nejčastějšími důvody pro využití je šikana ve škole, hádky s kamarády, nebo proto, že si nemají o důležitých věcech s kým promluvit nebo se někomu svěřit. Tato linka je zdarma, anonymně a nonstop – 365 dní v roce a 24 hodin denně. Funguje zde i rodičovská linka, na kterou se mohou obracet i rodiče, když mají obavy o své děti (linkabezpeci.cz, nedatováno).

Osoba, která se potřebuje svěřit, nebo poradit, může využít již výše zmíněné telefonní číslo a zavolat, nebo může využít e-mail pomoc@linkabezpeci.cz, nebo přímo na webových stránkách linkabezpeci.cz online chat. Pro vstup na chat je potřeba se zaregistrovat (vytvořit

si přezdívku a heslo) a délka chatu je omezena denně na 90 minut (linkabezpeci.cz, nedatováno).

V roce 2007 se na linku bezpečí s problémy s Internetem obrátilo 40 dětí. Nejčastěji děti řeší kyberšikanu, obtěžování přes sociální sítě, sexting, vydírání, nebo zneužití osobních údajů. V roce 2018 toto číslo vzrostlo na 624 dětí, proto linka bezpečí spustila společně s ČSOB a nadací O2 netradiční kampaň, která je zaměřena na kyberbezpečnost. Projekt je šířen pomocí videí, která lze nalézt jak na YouTube, tak na webové adrese hustalida.cz (linkabezpeci.cz, 2018).

3.4.2 Bezpečný internet

Tento projekt vznikl s cílem ukázat možná rizika spojená s využíváním Internetu a především také způsoby, jak se jim bránit. Bezpečný internet se snaží oslovit různé cílové skupiny – začínající uživatele, pokročilé uživatele, rodiče, děti, ale také školy a pro všechny tyto skupiny jsou vytvořeny speciální kurzy (pro pokročilé uživatele například jak si ochránit data, jak nakupovat přes Internet a podobně). Je také možné využít online poradnu, kde lze bezplatně zaslat dotaz pomocí formuláře na webové stránce bezpecnyinternet.cz (bezpecnyinternet.cz, nedatováno).

3.4.3 Seznam se bezpečně

Projekt Seznam se bezpečně založila společnost Seznam.cz a hlavním důvodem pro vznik tohoto projektu byla sebevražda 15 leté dívky kvůli úniku jejích nahých fotografií. Projekt nabízí tři filmy, které upozorňují na rizika spojená s používáním Internetu. První díl je zaměřený na rizika s online seznamováním, druhý se věnuje kyberšikaně a sociálnímu inženýrství a třetí popisuje případ zneužití 39 dětí skautskými vedoucími. Díky tomuto projektu také byly natočeny spoty - pro mladší *Křečci v síti* a pro starší *Desatero s Benem*. Tyto filmy a videa lze nalézt na portálu Stream.cz. Kromě filmů a spotů projekt uskutečňuje výjezdy do škol a snaží se jim rizika Internetu odlehčenější formou představit (jsns.cz, nedatováno).

3.4.3 Bílý kruh bezpečí

Dalším z projektů, který se snaží pomáhat, je Bílý kruh bezpečí. Tato pomoc je poskytována prostřednictvím bezplatné nonstop linky 116 006 – pro oběti kriminality a domácího násilí, dále celostátními sítěmi BKB, centrálami BKB v Praze, intervenčního centra v Brně,

klíčových sociálních pracovníků a linky 257 317 110 – nonstop linky pro oběti a svědky trestných činů. Ročně eviduje Bílý kruh bezpečí více než 12 000 kontaktů (bkb.cz, 2009).

Mezi další činnosti Bílého kruhu bezpečí patří přednášky, výcviky, semináře, vlastní projekty a účast na mezinárodních projektech, zahraniční spolupráce – členství ve Victim Support Europe a v neposlední řadě také spolupráce s nestátními organizacemi (bkb.cz, 2009).

3.4.4 E-bezpečí

Posledním projektem zde zmíněným je e-bezpečí. Jedná se o celorepublikový projekt zaměřený na prevenci, výzkum, vzdělávání, intervenci a osvětu spojenou s rizikovým chováním na Internetu. Tento projekt se specializuje především na kyberšikanu, sexting, kybergrooming, kyberstalking, rizika sociálních sítí, hoaxy, online závislosti a zneužití osobních údajů (e-bezpeci.cz, 2008).

Základní činností projektu je terénní práce s různými cílovými skupinami, přednášky, vzdělávací akce zaměřené na prevenci a podobné činnosti s nimi související. Představa o problematice je předváděna na základě modelových situací, které skutečně mohou nastat a na příkladech skutečných kauz (e-bezpeci.cz, 2008).

Celkem prošlo výcvikem projektu E-Bezpečí přes 60 000 žáků základních a středních škol, proškoleno bylo více než 10 000 dospělých a byla poskytnuta pomoc více než 2500 obětem kybernetické kriminality (e-bezpeci.cz, 2008).

4 Vlastní výzkum

V předchozích kapitolách v teoretické části je popsána mimo jiné bezpečnost na sociálních médiích. Následující kapitoly obsahují vlastní výzkum zaměřený na tuto problematiku. Pro tento výzkum byly využity dvě metody – dotazníkové šetření a metoda focus group. Obě tyto metody mají za cíl zjistit, zdali se studenti cítí na Internetu bezpečně a zdali znají rizika, která je na sociálních médiích mohou potkat. Metoda focus group tato zjištění ještě doplňuje o vlastní názory studentů. Na základě zjištěných dat budou navržena doporučená opatření v rámci prevence.

4.1 Dotazníkové šetření

První metodou, která je v této práci využita pro zjištění dat, je dotazníkové šetření. Dotazník je zaměřený na studenty středních a vysokých škol. Dotazování probíhalo ve dvou formách - přes portál survio.com a v papírové podobě (viz příloha A), která byla využita pro studenty střední školy, kde byla aplikována i metoda focus group. Dotazování probíhalo v elektronické podobě na sociální síti Facebook. Dotazník byl umístěn na několika školních skupinách a soukromém profilu a dotazování probíhalo od 19. 2. 2019 do 19. 3. 2019. Vzhledem k tomu, že dotazníkové šetření zodpovědělo 150 respondentů, nelze výsledky výzkumu zobecňovat pro všechny studenty.

Cílem dotazníku bylo zjistit, zda se uživatelé Internetu cítí na sociálních mediích bezpečně a jestli znají rizika, která se jich nebo jejich blízkých mohou týkat, co nejčastěji na Internetu dělají, dále kolik času tráví na sociálních médiích, proč tyto média používají a zdali jim doba na nich přijde užitečná a v neposlední řadě také jestli je podle nich veřejnost obeznámena s nebezpečím, které jim může hrozit, jaká skupina je dle nich nejvíce ohrožena a jestli znají alespoň nějaké projekty, které mají za cíl těmto rizikům předcházet nebo jejich obětem pomoc je řešit.

Dále byly zkoumány závislosti mezi některými otázkami. Pro zkoumání asociací byla vybrána neparametrická statistická metoda Kendallovo Tau, jelikož k dispozici není tolik dat, aby mohl být použit Test chí-kvadrát nezávislosti v kontingenční tabulce. Tento koleračí koeficient se používá pro měření síly vztahu dvou proměnných a je používán pro pořadová data (Hendl, 2015).

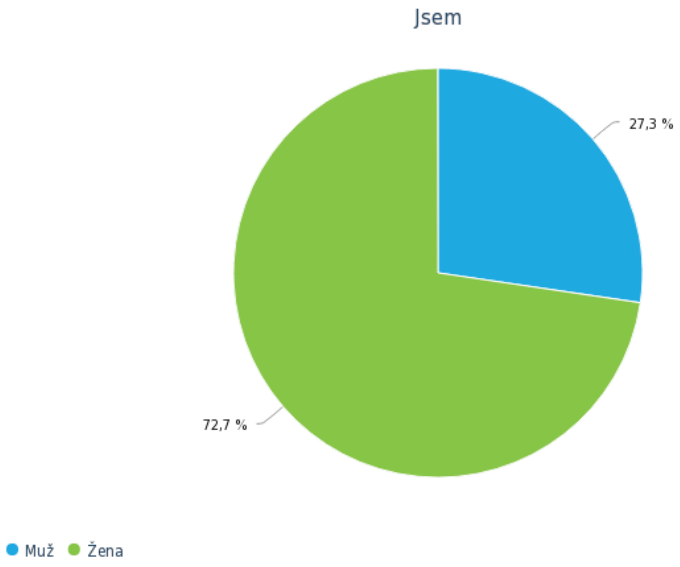
Pomocí Kendallova Tau byly testovány následující hypotézy:

- **H1**: Existuje asociace mezi důvěrou v informace uvedených na Facebooku a na internetové stránce.
- **H2**: Existuje asociace mezi věkem respondenta a dobou strávenou na sociálních médiích.
- **H3**: Existuje vzájemný vztah mezi tím, zdali si respondenti píší na Internetu s cizími lidmi a tím, jestli jim to přijde běžné a normální
- **H4**: Mezi vzděláním respondenta a jeho povědomí o rizicích, které ho na sociálních médiích mohou ohrozit, existuje vztah.

4.1.1 Výsledky

Na dotazníkové šetření odpovědělo celkem 150 studentů, z toho 109 žen a 41 mužů. Grafické znázornění lze vidět na obrázku č. 11.

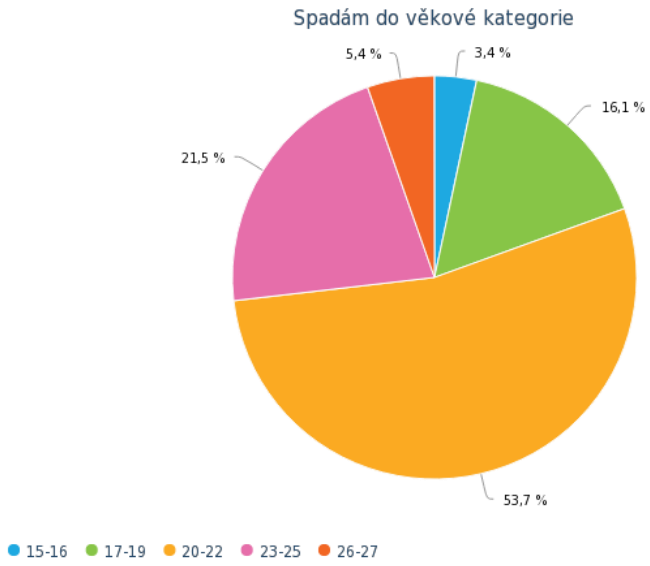
Obrázek č. 11 - Pohlaví studentů



Zdroj: Výsledky vlastního výzkumu, 2019

Nejvíce zastoupenou věkovou skupinou jsou studenti ve věku od 20-22 let, kterých je v celkovém počtu 80 a tvoří 53,7 % všech respondentů.

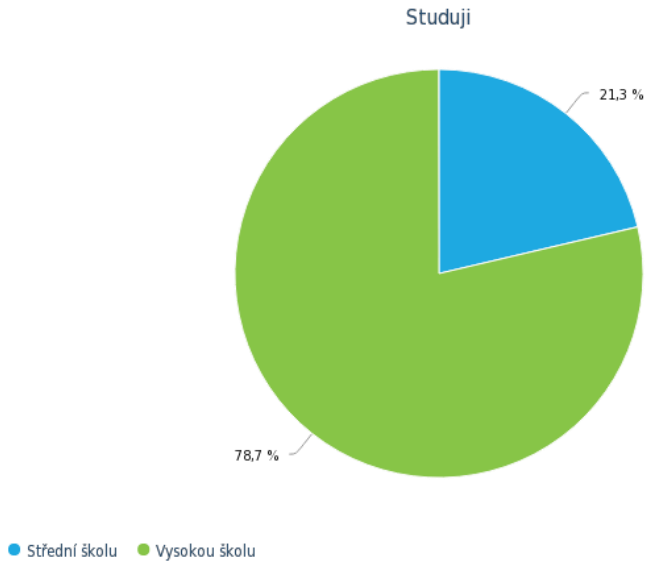
Obrázek č. 12 - Věk studentů



Zdroj: Výsledky vlastního výzkumu, 2019

Celkem 118 z celkového počtu respondentů studuje vysokou školu.

Obrázek č. 13 - Typ školy

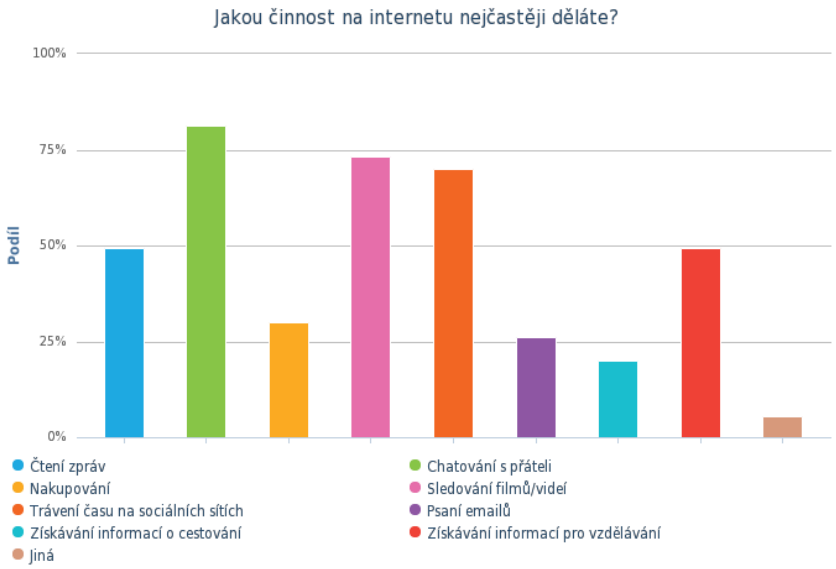


Zdroj: Výsledky vlastního výzkumu, 2019

Následující otázka se již týkala Internetu a to konkrétně co nejčastěji na Internetu respondenti dělají. Z grafu vyplývá, že nejčastější aktivitou je chatování s přáteli, oproti tomu nejméně respondenti na Internetu získávají informace o cestování. V dalších

odpovědích uváděli že, na Internetu pracují, nebo hrají online hry. Souhrnný přehled veškerých odpovědí poskytuje obrázek č. 14.

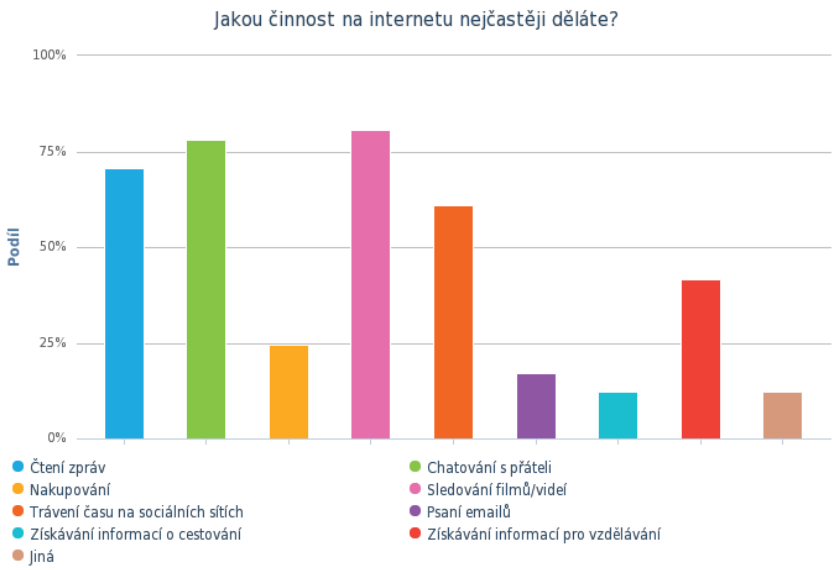
Obrázek č. 14 - Nejčastější aktivita na Internetu



Zdroj: Výsledky vlastního výzkumu, 2019

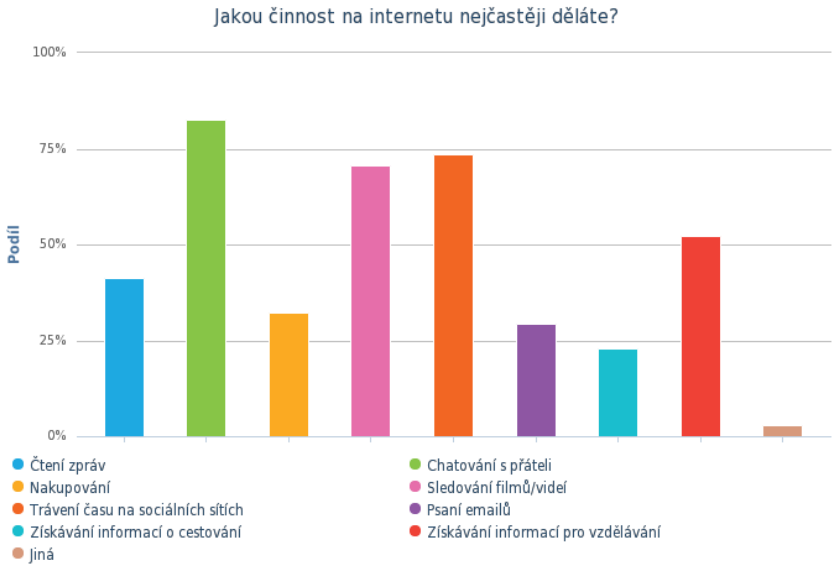
Když ale porovnáme muže a ženy, na následujících grafech můžeme vidět, že muži častěji sledují filmy a méně tráví čas na sociálních sítích (viz obrázek č. 15), než ženy (viz obrázek č. 16). Ženy také méně čtou zprávy, více píší e-maily a také si více získávají informace pro vzdělávání.

Obrázek č. 15 - Nejčastější aktivita u mužů



Zdroj: Výsledky vlastního výzkumu, 2019

Obrázek č. 16 - Nejčastější aktivita u žen



Zdroj: Výsledky vlastního výzkumu, 2019

Další dvě otázky byly zaměřené na důvěru respondentů k informacím uvedeným na Internetu. První otázka se týkala důvěry v informace na Facebooku a druhá v informace uvedené na internetové stránce (např. politické strany, cestovní agentury apod.). Z tabulky č. 1 lze vidět, že informacím uvedeným na Facebooku nevěří nikdo a spíše věří jen 50 z nich (ze 150 responzí). Naopak informacím na internetové stránce věří 15 studentů a spíše jim

věří 88 (ze 150 responzí). Lze tedy říci, že studenti spíše věří informacím uvedeným na internetové stránce.

Tabulka č. 1 - Počet respondentů s důvěrou v informace uvedené na Facebooku a na internetové stránce

	Pokud je informace uvedená na Facebooku, pak ji:	*Pokud je informace uvedená na internetové stránce, pak ji:*
Věřím	0	15
Spíše věřím	50	88
Nedokážu odpovědět	43	31
Spíše nevěřím	49	12
Nevěřím	8	4

Zdroj: Vlastní zpracování, 2019

Mezi těmito dvěma otázkami byla také zkoumána závislost pomocí Kendellova Tau. Na základě p-hodnoty, která v případě těchto dvou otázek vyšla 0,000001, se dá tvrdit, že mezi zkoumanými proměnnými existuje závislost, jejíž velikost byla změřena Kendallovým Tau jako 0,438. Na tomto základě je tedy **H1** přijata.

Na následující tabulce č. 2 lze vidět, která sociální média studenti znají a která z nich sami využívají. Mezi tři nejvíce známá sociální média se zařadil Facebook, YouTube a Instagram. Naopak mezi nejméně známé patří sociální média – Spolužáci.cz, Ask.fm a Líbimseti.cz. Mezi nejpoužívanějšími médii lze vidět opět Facebook, YouTube a Instagram a naopak mezi nejméně používanými jsou Spolužáci.cz (které k lednu roku 2019 byly zrušeny, takže je využívat již nelze) dále Libimseti.cz, Lidé.cz a Ask.fm. Lze tedy obecně říci, že studenti více používají zahraniční média.

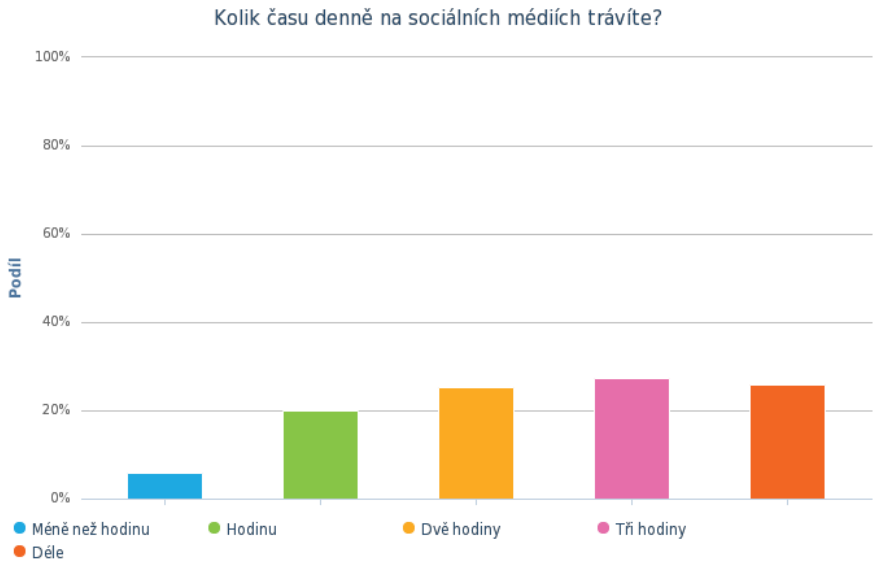
Tabulka č. 2 - Počet studentů, kteří znají a využívají daná sociální média

	Student sociální médium zná	*Student sociální médium využívá*
Facebook	147	146
YouTube	147	141
Instagram	145	120
Twitter	142	29
ČSFD	130	70
Lidé.cz	117	4
Spolužáci.cz	112	0
LinkedIn	70	16
Ask.fm	96	7
Libimseti.cz	53	1

Zdroj: Vlastní zpracování, 2019

Studenti tráví na sociálních médiích nejčastěji 3 hodiny (celkem 27,3 % z nich). Naopak nejméně častou odpovědí bylo méně než hodinu. Déle než tři hodiny na sociálních médiích tráví 26 % respondentů. Pomocí Kendallova Tau bylo zkoumáno, zdali existuje vztah mezi věkem a dobou strávenou na sociálních médiích. Na základě p-hodnoty, která v případě těchto dvou otázek vyšla 0,8055864, lze tvrdit, že mezi zkoumanými proměnnými závislost neexistuje. Na tomto základě tedy **H2** nebyla přijata a lze konstatovat, že věk na dobu strávenou na Internetu vliv nemá.

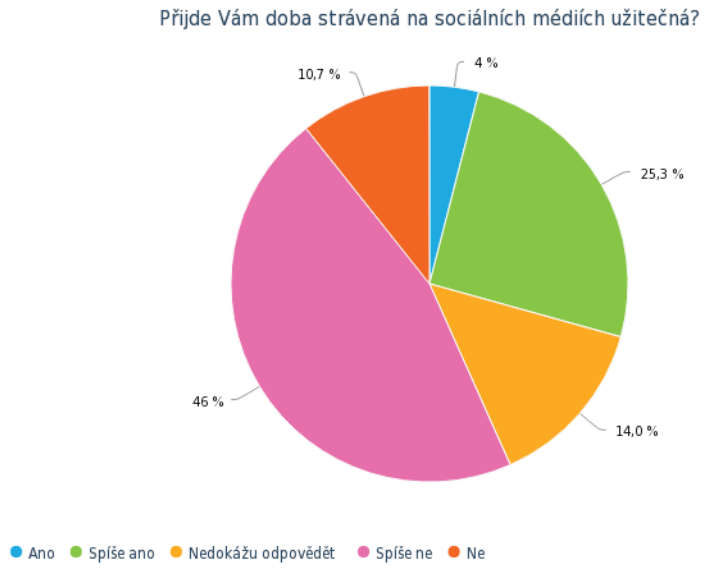
Obrázek č. 17 - Kolik času studenti na sociálních médiích tráví



Zdroj: Výsledky vlastního výzkumu, 2019

46 % respondentům přijde doba, kterou na sociálních médiích tráví, neužitečná. Naopak užitečná a spíše užitečná přijde jen necelým 30 % studentům. Procentuální znázornění lze vidět na obrázku 18. 33 % Respondentům, kteří na předchozí otázku, kolik času na sociálních tráví, odpověděli déle než tři hodiny, doba na sociálních médiích přijde neužitečná. Naopak téměř 35 % z nich odpovědělo spíše užitečná a užitečná.

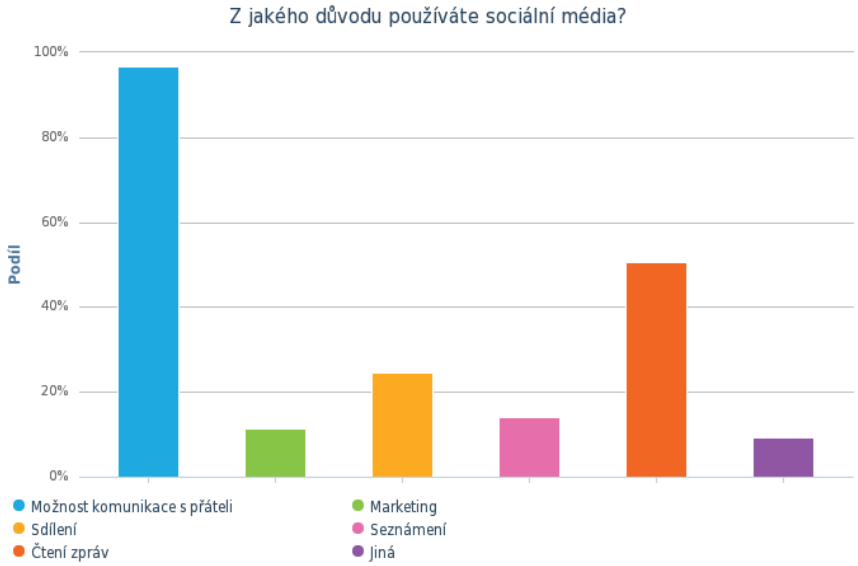
Obrázek č. 18 – Užitečnost doby strávené na sociálních médiích



Zdroj: Výsledky vlastního výzkumu, 2019

Podle respondentů, sociální média mají spíše výhody. Celkem si to myslí 43,3% z nich. Nevýhody uvedlo pouze 6% a mezi nejčastější důvody používání sociálních médií patří možnost komunikace s přáteli. Uvedlo ji celkem 96,7%. Další častou aktivitou na síti je čtení zpráv a možnost sdílení. Nejméně častou aktivitou na síti je poté marketingová aktivita. Mezi jinými důvody, proč respondenti využívají sociální média, se objevilo sledování trendů v kosmetice, nebo využívání sociálních médií ke své práci či pro zábavu.

Obrázek č. 19 - Důvody používání sociálních médií



Zdroj: Výsledky vlastního výzkumu, 2019

Následující tabulka č. 3 znázorňuje počet studentů, kterým vadí psát si na sociálních médiích s cizími lidmi a také jestli jim to přijde běžné a normální. Psát si s cizími lidmi vadí celkem 25,3% respondentů a spíše vadí 31,3 %. 22 % studentů to nepřijde normální. Mezi těmito otázkami byla zkoumána závislost – zdali těm, kterým vadí psát si na sociálních médiích s cizími lidmi, to přijde běžné a normální. Na základě p-hodnoty, která v případě těchto dvou otázek vyšla 0,000001, se dá tvrdit, že mezi zkoumanými proměnnými existuje závislost, jejíž velikost byla změřena Kendallovým tau jako 0,495. Na tomto základě je tedy **H3** přijata.

Tabulka č. 3 - Počet studentů, kteří si píší s cizími lidmi na sociálních médiích a zdali jim to přijde běžné a normální

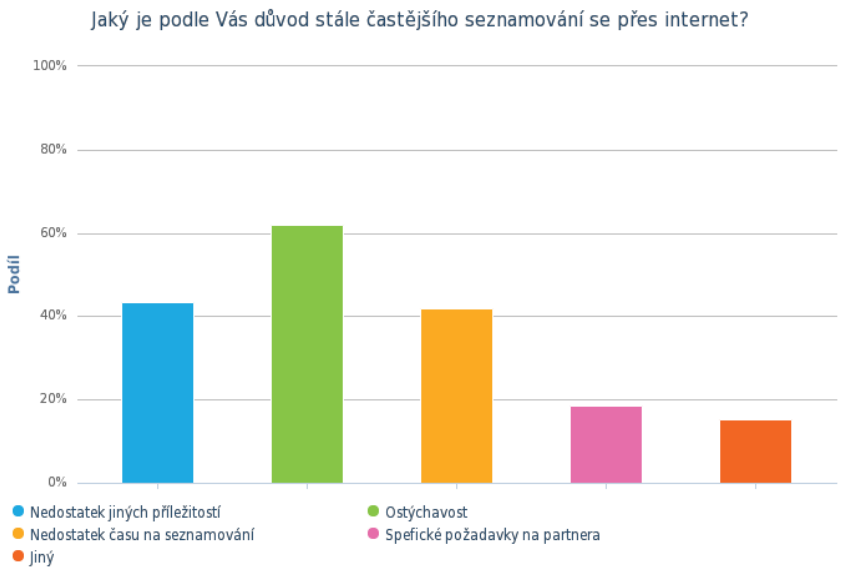
	Vadí Vám psát si na sociálních médiích s cizími lidmi?	*A přijde Vám toto psaní běžné a normální?*
Ano	38	16
Spíše no	47	36
Nedokážu odpovědět	16	22
Spíše ne	41	54
Ne	8	22

Zdroj: Vlastní zpracování, 2019

Přes Internet se někdy seznámilo celkem 48,7 % respondentů. Důvody, které mohou vést ke stále častějšímu seznamování se přes Internet lze vidět na grafickém znázornění níže. Mezi nejčastější důvody podle studentů lze řadit ostýchavost, nedostatek jiných příležitostí,

nebo nedostatek času pro seznamování běžnou cestou. Mezi jinými odpověďmi se objevil například strach z oslovení, nedostatek sociálních dovedností v realitě, nebo z důvodu usnadnění, pohodlnosti, či dokonce lenosti. Názorný přehled všech odpovědí veškerých odpovědí poskytuje obrázek č. 20.

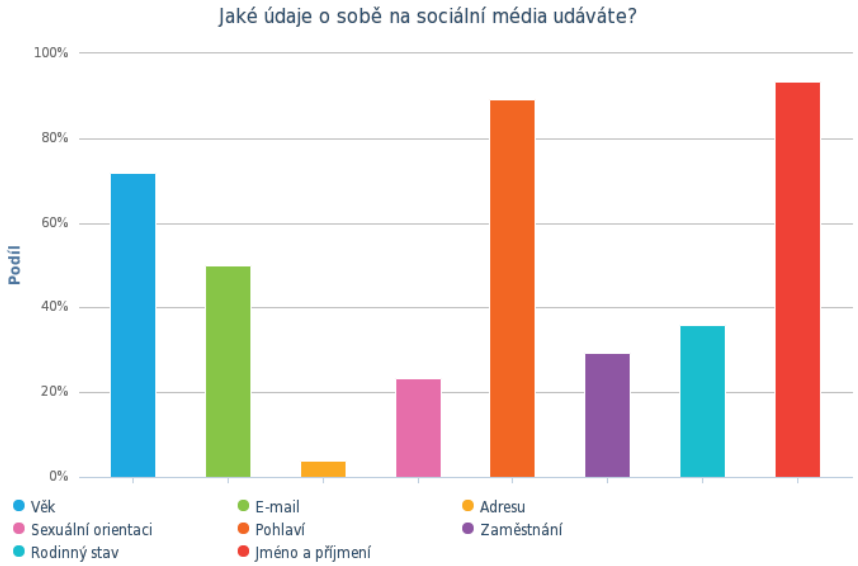
Obrázek č. 20 - Důvody pro seznamování se na Internetu



Zdroj: Výsledky vlastního výzkumu, 2019

Pravdivé osobní údaje o sobě na sociální média udává přes 80 % studentů. Mezi údaje, které o sobě na sociální média uvádějí, patří jméno a příjmení, které uvádí 93,3 % respondentů, dále pohlaví (89,3 %) a svůj věk (72 %). Naopak údaje, které udává jen malé procento, je sexuální orientace a adresa, kterou uvádí jen 4 % z dotazovaných. Veškeré odpovědi a četnosti jejich udávání zachycuje obrázek č. 21.

Obrázek č. 21 - Jaké údaje o sobě uživatelé udávají



Zdroj: Výsledky vlastního výzkumu, 2019

Další otázky už byly zaměřené na bezpečnost na sociálních médiích. První z nich se dotazovala, zdali se studenti cítí na Internetu bezpečně. Ano a spíše ano uvedlo 53,3 % z nich. Následující tabulka č. 4 znázorňuje rozdíly této otázky mezi vysokoškolskými studenty a středoškolskými (hodnoty v tabulce jsou uvedené v %, jelikož byl rozdílný počet vysokoškolských a středoškolských studentů). Bylo zkoumáno, zdali má vzdělání vliv na pocit bezpečí. Na základě p-hodnoty, která v případě těchto dvou otázek vyšla 0,7805245, se dá tvrdit, že mezi zkoumanými proměnnými závislost neexistuje a na základě tohoto zjištění tedy **H4** nebyla přijata. V tabulce č. 4 lze vidět, že výrazné rozdíly mezi vysokoškolskými a středoškolskými studenty v pocitu bezpečí nejsou.

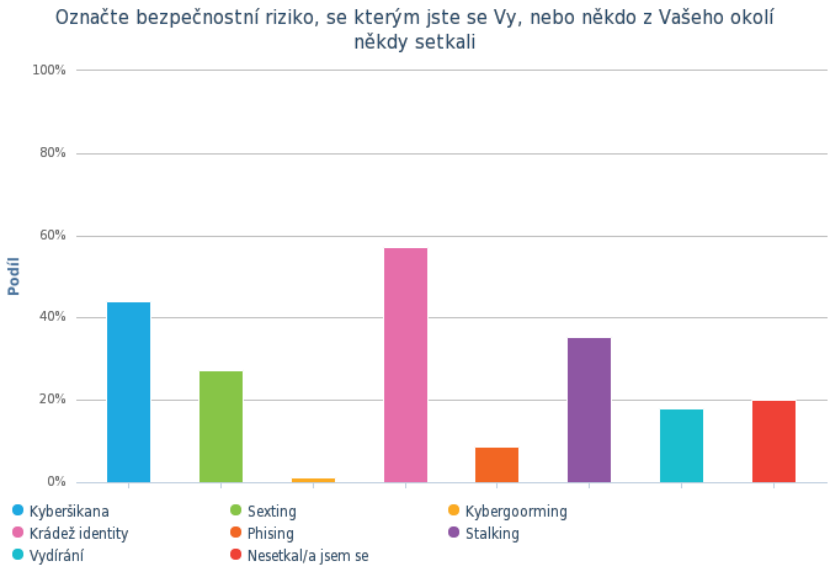
Tabulka č. 4 - Procentuální vyjádření počtu studentů VŠ a SŠ studia a jejich pocit bezpečí na Internetu

	Cítíte se na Internetu bezpečně? (VŠ student)	*Cítíte se na Internetu bezpečně? (SŠ student)*
Ano	9,3 %	3,1 %
Spíše ano	45,8 %	43,8 %
Nedokážu odpovědět	14,4 %	31,3 %
Spíše ne	22,9 %	18,8 %
Ne	7,6 %	3,1 %

Zdroj: Vlastní zpracování, 2019

Bezpečností rizika, která je na sítích mohou potkat, zná 96 % respondentů. Mezi bezpečnostní rizika, se kterými se studenti, nebo někdo v jejich okolí někdy setkali, patří na prvním místě krádež identity, dále kyberšikana a stalking. Naopak s kybergroomingem má zkušenost jen 1,3 % studentů a phishingem 8,7 %. S žádným z uvedených rizik se nesetkalo pouze 20 % studentů. Souhrnný přehled veškerých odpovědí poskytuje obrázek č. 22.

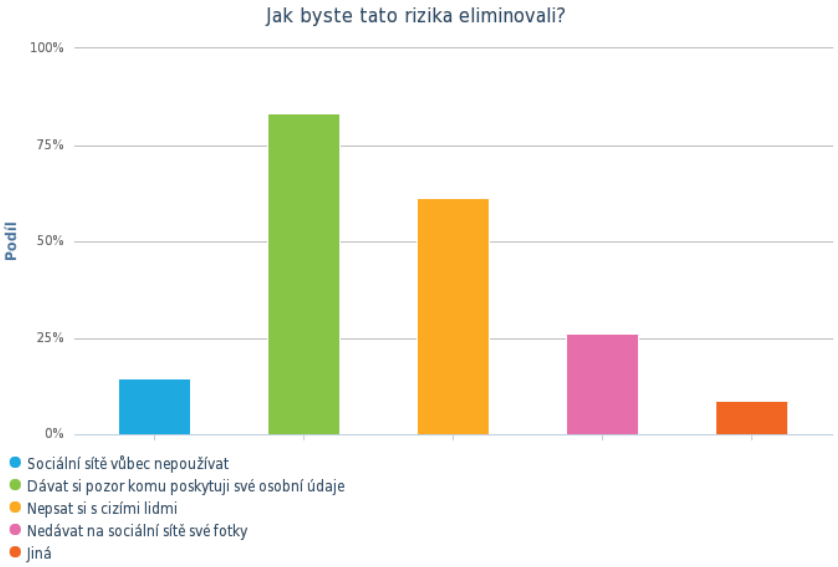
Obrázek č. 22 - Bezpečností rizika, se kterými se studenti, nebo někdo v jejich okolí někdy setkali



Zdroj: Výsledky vlastního výzkumu, 2019

Nejvíce ohroženou skupinou na sociálních médiích je skupina 15 let a méně. Uvedlo ji celkem 86,7 % respondentů, druhou nejvíce ohroženou skupinou jsou uživatelé mezi 16-18 lety (6,7 %) a na třetím místě lidé starší 41 let, kterou uvedlo 6 %. Veřejnost s riziky, které uživatele na sociálních médiích mohou potkat, obeznámena spíše není, myslí si to 48 % z dotázaných. Pouhých 24 % si myslí, že spíše ano, nebo ano. Na otázku, jak by tyto rizika eliminovali, odpovídali většinou dávat si pozor na to, komu poskytovat své údaje, nebo nepsat si s cizími lidmi. 14,7 % si myslí, že řešením je sociální sítě vůbec nepoužívat. Dále studenti uváděli přidávat si jen lidi, které znají, nerozesílat intimní fotografie, zabezpečit si své účty a lépe své účty kontrolovat. Obrázek č. 23 znázorňuje grafické zobrazení možné eliminace rizik.

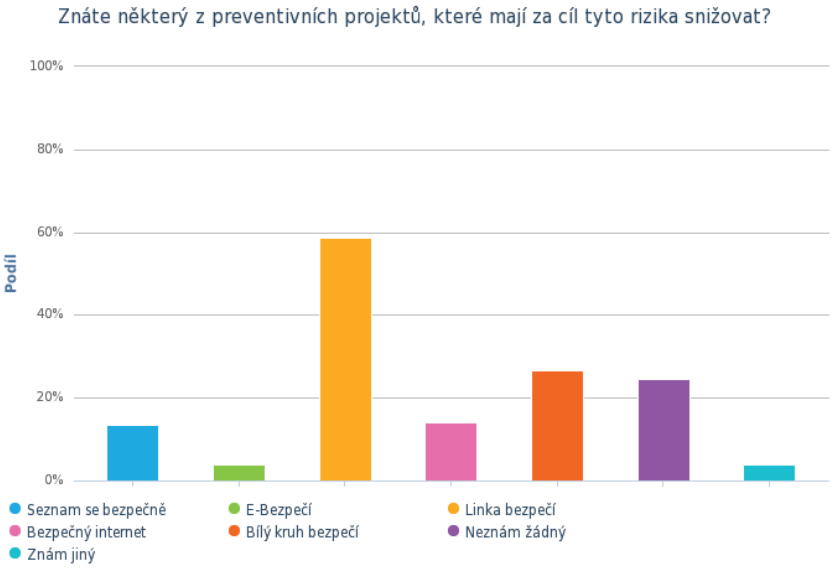
Obrázek č. 23 - Jak eliminovat rizika spojená s užíváním sociálních médií



Zdroj: Výsledky vlastního výzkumu, 2019

Předposlední otázka se zaměřila na projekty, které se snaží na tyto rizika upozorňovat a pomáhat jejich eliminaci. Na obrázku č. 24 lze vidět, že více než polovina respondentů zná linku bezpečí a Bílý kruh bezpečí, který zná 26,7 %. Vůbec žádný z projektů nezná 24,7 %.

Obrázek č. 24 - Znalost projektů zaměřujících se na bezpečností rizika



Zdroj: Výsledky vlastního výzkumu, 2019

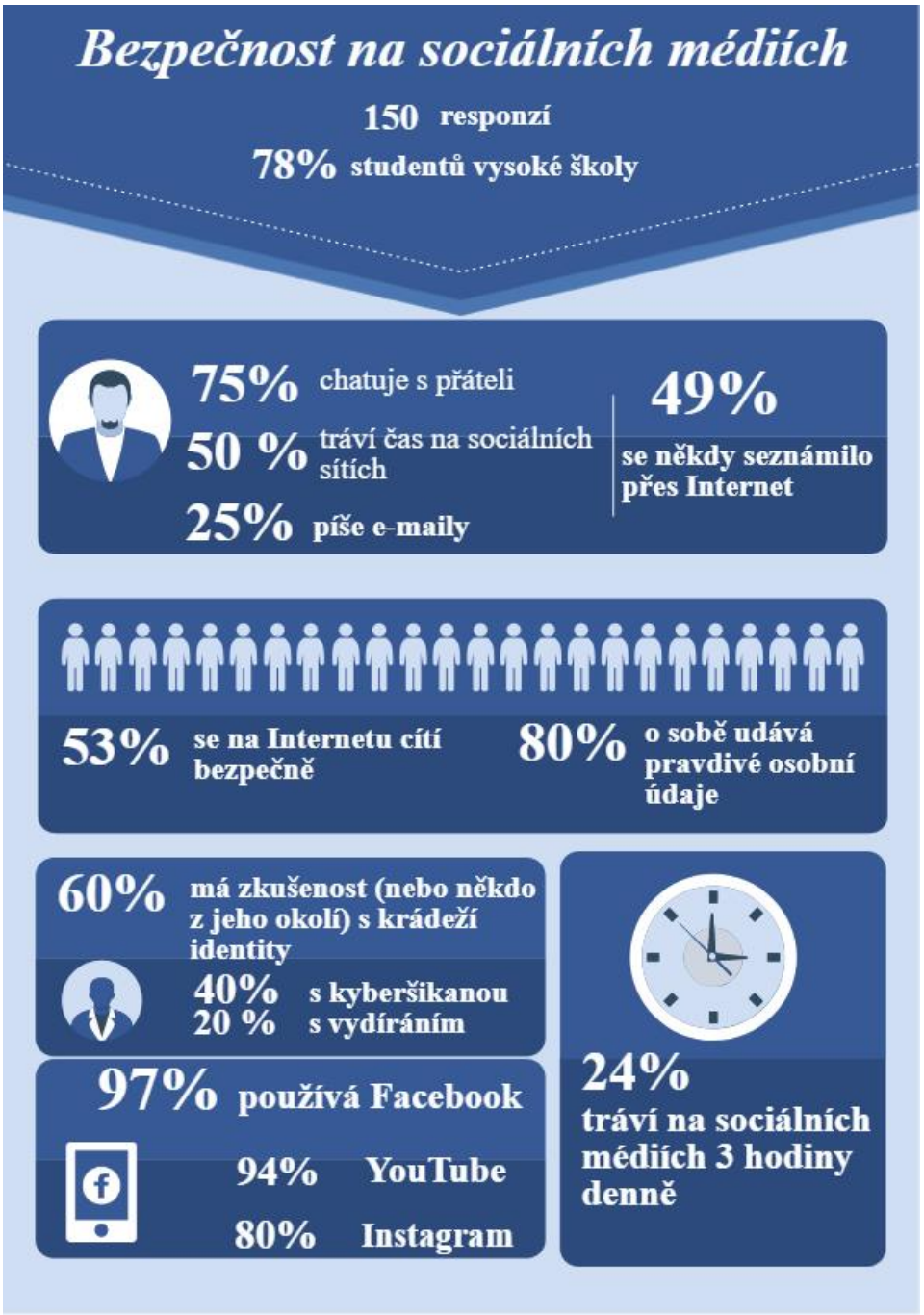
Poslední a zároveň první otevřenou otázkou byl názor studentů na to, jaká je podle nich budoucnost sociálních médií. Budoucnost podle velké části respondentů bude především ve

stále se zvyšující komunikaci přes sociální média. Čím dál méně se budou lidé scházet osobně a lidé nebudou schopni mezi s sebou komunikovat mimo síť. Většina z nich uvedla, že sociální média se dále budou rozvíjet, budou stále populárnější a budou více využívané ve všech oblastech (práce, obchod). Bude růst vliv influencerů a využití sociálních médií v marketingu. S růstem popularity sociálních medií ale podle některých přímo úměrně rostou i bezpečnostní rizika s nimi spojená, která ale nebudou společností řešená, dokud se nestane něco zásadního. Také se lidé pomocí sociálních médií budou stále více seznamovat on-line. Bude to stále větší zdroj informací, které ale budou stále více vzdálenější pravdě. Sociální média jejich uživatele budou stále více ovládat a většina lidí si bez nich nebude moct svůj život představit a co hůř – ani nebudou chtít. Buducnost také vidí v nové nejvyužívanější platformě, jelikož Facebook začíná mít spoustu nedostatků. Buď může být nahrazen Instagramem, který je nejprogresivnější sociální sítí, nebo úplně novou.

4.1.2 Souhrnný report

Pro přehlednou interpretaci dotazníkového šetření byl vytvořen report, ve kterém jsou shrnuty výsledky. Procenta jsou pro větší přehlednost zaokrouhlena.

Obrázek č. 25 - Report z dotazníkového šetření



Zdroj: Vlastní zpracování, 2019

4.2 Focus group

Druhá z metod, která byla pro zjištění dat použita, je metoda focus group. Jedná se o metodu, kdy se s několika respondenty vede diskuse na dané téma a měla by trvat přibližně jednu hodinu.

Diskuse byla provedena se studenty střední školy v Rakovníku, z Masarykovy obchodní akademie, konkrétně studenty 3. ročníku. Studenti byli rozděleni na dvě skupiny po 8 a obě pohlaví byla zastoupena ve stejném poměru. Nejdříve byly probírané doplňující otázky k dotazníku, který studenti dostali k vyplnění a poté otázky, které byly rozděleny do čtyř oblastí – závislost na sociálních médiích, Facebook, obsah na síti a důvěra v přátele, které na sociální síti mají. Cílem této diskuse bylo doplnit otázky z dotazníku, seznámit studenty s problematikou bezpečnosti na sociálních médiích a zachytit jejich názory a domněnky vůči tomuto tématu. Pracovní list k metodě je v příloze B.

4.2.1 Výsledky

Nejdříve výsledky otázek, které doplňovaly dotazník. Studenti nejčastěji na internetu tráví čas na sociálních médiích, čtou zprávy, novinky ze světa a sledují on-line seriály. Téměř polovina z nich uvedla, že nejčastěji sledují dění ve sportu a vyhledávají si informace pro vzdělávání. Důvěru ale v sociální sítě nemají, informace uvedené na Facebooku jsou pro ně nedůvěryhodné, vnímají je spíše jako marketingový tah nebo hoax a věří spíše informacím, které jsou uvedené na internetové stránce. Jedna studentka jako příklad uvedla, že se jí ne jednou stalo, že na facebookové stránce obchodu byly rozdílné ceny, než na internetové. Informace, které nejčastěji na Internetu vyhledávají, jsou informace o počasí, informace do školy, nebo o cestování. Studenti většinou tráví na sítích déle než tři hodiny a to hlavně proto, že sledují videa na YouTube, ale záleží na dni, o víkendu je to déle než o všední dny. Doba strávená na sociálních médiích jim ale užitečná nepřijde – většinou spíše prokrastinují a některým z respondentů to přijde jako ztráta času. Na otázku, co užitečnějšího by místo toho mohli dělat, odpověděli učení, sportování, nebo osobní setkání s člověkem, se kterým si na síti píší.

Z průzkumu také vyplývá, že sociální média pro většinu respondentů mají více výhod, než nevýhod. Jsou mezi nimi rychlost, možnost plánování akcí, sledování událostí co se dějí v okolí, možnost shlédnutí seriálu zadarmo, nebo sportovní informace. Mezi nevýhodami se objevil fakt, že si o Vás může kdokoli cokoli zjistit a bezpečnostní rizika z toho plynoucí.

Studenti na sítě o sobě většinou uvádějí pravdivé osobní údaje, ale údaj, který by na sociální média nikdy nedali, je pravý věk, bydliště, nebo telefonní číslo. Své vztahy na sociálních sítích také nezveřejňují a to hlavně pro to, že je to zásah do jejich soukromí. Přes internet se ale seznamují, dokonce někteří z nich uvedli, že si díky nim našli partnera. Mají kolem sebe také lidi, kteří zcela běžně využívají portály pro seznamování – většinou badoo nebo tinder, oni sami ale tento způsob seznamování nevyužili.

Nejvíce ohrožená věková skupina je 15 a méně, je to dáno tím, že takto mladí uživatelé sociálních sítí se na nich nedokáží tak orientovat, snáze uvěří, jsou naivnější a mají skony k tomu odpovídat cizím lidem.

Rizika, se kterými se na sociálních sítích nejvíce setkávají, jsou krádež identity, většinou na Instagramu a kyberšikana, Většinou se tato rizika dají ovlivnit svým chováním například tím, že uživatelé nebudou na svůj profil uvádět fotografie a odepisovat cizím lidem.

V druhé části focus group otázky spadaly do 4 okruhů, jak již bylo zmíněno – závislost na sociálních médiích, Facebook, důvěru a obsah na síti.

Většina studentů je na sociálních sítích závislá a nedokáže si bez nich svůj běžný den představit. Zrušit by si ho ale dokázali, někteří o tom i uvažovali, ale nakonec se rozhodli pro používání, hlavně pro to, že by nebyli schopni sledovat dění ve skupinách ve kterých jsou členy (například skupina jejich ročníku). Studenti také uvedli, že by se cítili mimo hru, pozvánky na akce a domlouvání se na ně probíhá většinou právě přes sociální sítě a tak by o tyto informace byly ochuzeny. Pokud nemají delší dobu připojení, nervózní se ale necítí, možná jen mají starost, jestli jim někdo nepsal. Na otázku, které komunikaci dávají přednost, zda-li osobní, nebo na sociálních médiích, odpověděli, že záleží na tom s kým. S důležitými lidmi, kamarády a partnery se raději setkávají osobně.

Další okruh byl věnován Facebooku. Facebook je podle většiny respondentů nejrozšířenější sociální síť. Všichni jí mají a běžně používají, i když Facebook podle nich bude brzo nahrazen jinou platformou (Instagramem). Důvodem proč se tak může stát, uvádějí větší přehlednost instagramu a nedostatky, které Facebook má. Hlavním důvodem proč Facebook používají je možnost komunikace, sledování událostí a skupiny, do kterých se mohou přidávat. Na Facebook si většinou přidávají lidi, které osobně znají, nebo znají od vidění (například studenty z vyšších ročníků). Hlavní výhodu Facebooku vidí v možnosti komunikace a možnosti sestavit si vlastní plán akcí (událostí).

Co se týče obsahu, který na sociální sítě přidávají, většinou se jedná o aktualizaci profilové fotky, kterou mění v průměru jednou za měsíc, dále sdílení videí z youtube, většinou písníčky, nebo zprávy ze světa (novinky). Nejvíce obsahu přidávají na Instagram a to na insta story, většinou denně. Přímo na profil pak fotky přidávají 1x týdně.

Posledním podtématem, o kterém se hovořilo, byla důvěra v lidi, které na sociálních médiích respondenti mají. Ať už jejich přátelům, nebo followerům, studenti spíše věří. Profilům, kterým ale nedůvěřují, jsou profily, které nemají profilovou fotku, nebo které na profilu mají jen jednu, nebo dvě fotografie. Uvádějí, že takové profily jim přijdou nedůvěryhodné, nebo falešné. Na sociálních médiích přesto, že svým přátelům důvěřují, se ale veřejně na profilu nesvěřují, jen pár z nich po chatu, pokud je to neodkladné a důležité.

5 Preventivní opatření a doporučení

Jak bylo zjištěno z dotazníkového šetření, veřejnost podle respondentů spíše není obeznámena s nebezpečím, jaké je může na Internetu potkat. Proto poslední částí praktické práce jsou doporučení a preventivní opatření, které by mohly napomoct k tomu, aby k těmto rizikům docházelo co nejméně. Na prevenci je potřeba myslet jak z pohledu uživatele sociálních médií, rodiče (v případě nižší věkové skupiny), tak i školy.

Uchovávat si své soukromí

První a zároveň jedna z nejdůležitějších věcí, je uchovávat si své soukromí. Je třeba si svůj profil nastavit tak, aby vyhovoval požadavkům uživatele a cítil se bezpečně. Upravit si své osobní údaje a zveřejňovat jen ty, které chce, aby viděli jeho přátelé. Také je důležité si své profily nastavit jako soukromé, nehrozí tak, aby údaje viděli cizí lidé. Je vhodné, udávat o sobě jen informace, jaké si dané sociální médium žádá, většinou je to jméno, email a věk. Svou adresu, rodinný stav, nebo telefonní číslo většinou není nutné udávat – a pokud ano, lze je nastavit soukromě, ovšem nedávnému problému s únikem dat, se kterým se potýkal Facebook, by se dalo předejít jedině tím, Facebook si vůbec nezakládat.

Nesdílet svou polohu

Ať už sdílení polohy přes sociální média soukromě (messenger) nebo veřejně (instastory) může být nebezpečné a pokud má uživatel veřejný profil a jeho příběhy může vidět tedy kdokoliv, je lepší svou polohu raději vůbec nesdílet. Je to nejsnadnější způsob jak si stalker může najít cestu k oběti. Instagram ale umožňuje nastavení příběhů pouze pro blízké přátele, do kterých je možné si zvolit jen lidi, které uživatel chce, aby příběh viděli a proto v případě sdílení polohy je rozumné využít právě tuto funkci.

Psát si jen s důvěryhodnými osobami

Dalším, velmi důležitým bodem, je psát si s lidmi, ke kterým uživatel chová důvěru. Jak je ve výsledcích focus group psáno – lidé nejčastěji nevěří profilům, které mají v albu jen jednu fotografii. Je třeba si na tyto lidi dávat pozor, protože většinou se jedná o profily falešné. Tento profil se snaží vždy tuto domněnku vyvrátit, ale pokud má uživatel potřebu si s ním psát, může ho poprosit o fotku se specifickou věcí (např. s ovladačem v ruce nebo s datem, na které je dobře vidět) aby dokázal, že je to opravdu on. Pokud se jedná o osobu, která již profil má, tak je dobré ho nahlásit – jedná se totiž o krádež identity. Častým případem to teď bývá právě na Instagramu.

Být obezřetní při schůzce naslepo

Na Internetu je možné setkat se se spoustou lidí, mezi kterými se bohužel mohou objevit podvodníci nebo útočníci. V situaci, kdy osoba, se kterou uživatel udržuje virtuální kontakt a se kterou si nějaký čas píše a která poté požaduje osobní setkání, je dobré být na pozoru. Nikdy není jisté, kdo za počítačem na druhé straně sedí a co po dotyčné osobě opravdu požaduje. Pokud má na schůzce zájem i druhá strana, určitě je třeba sejít se na veřejném místě, ideálně ve dne a ještě s někým „při ruce“, kdyby se cokoliv stalo. Určitě je dobré o této schůzce říct kamarádům, nebo rodičům.

Pozor na Fotografie

Když uživatelé vkládají fotografie na svůj profil, měli by u toho být opatrní. Pokud není na fotografii sám, měl by se nejdřív zeptat, jestli osoba, která se s ním na fotce nachází, s uveřejněním souhlasí. Je také samozřejmé, že fotografie, na kterých je uživatel jen v plavkách, nebo které působí vyzývavě, akorát zvyšují riziko, že je někdo zneužije, takže je lepší, takové fotografie vůbec nepřidávat. Posílat je někomu soukromě do chatu – jen pokud toho člověka uživatel opravdu zná, avšak ani tady se riziko dalšího rozesílání nevylučuje. Pokud uživatel dá na Internet fotografii, kterou po nějaké době (může to být týden, měsíc, rok..) vyhodnotí jako nevhodnou, nebo kterou na svém profilu dále nechce mít, může ji smazat, ale nebude mít záruku, že se nešíří dále po Internetu. Existuje na to ale služba TinEye, do které lze nahrát tuto fotografii a tato služba najde, kde se daná fotografie ještě nachází. Také existuje podobná služba přímo od Google, kde jdou místo textu nahrát obrázky a stejně jako TinEye Google vyhledá, na jakých webových stránkách se tato fotografie nachází.

Myslet na to, že obsah přidaný na Internet je většinou nevratný

Vše, co na Internet uživatel přidá, mnohdy nelze vrátit. Lze sice tento obsah smazat, nebo upravit ale nikdy není jistota, že to někdo jiný nevyfotil, nebo neuložil a v budoucnu nepoužije proti osobě, která příspěvek napsala. Proto je třeba promýšlet co na Internet sdílet a co ne. Někdy si uživatelé neuvědomují, že informace, které o sobě na sociálních médiích uvádějí, mohou vidět i subjekty, o kterých vůbec nepřemýšleli, že by se k nim mohli dostat. Většinou jde o zaměstnavatele, kteří si o svých zaměstnancích stále více zjišťují informace na sociálních médiích a je to v praxi stále více běžnější metodou, jak si získat o potenciálním uchazeči co nejvíce informací.

Rodič jako vzor

Při prevenci je třeba také myslet na aktéry těchto bezpečnostních rizik, ne jen na jeho oběti. Velkou roli hraje v těchto případech rodič, který by měl být pro své dítě vzorem – pozitivním vzorem. Měl by s ním především komunikovat a snažit se aby měl o těchto rizicích povědomí. Také by měly být děti poučeni, že není správné ubližovat jiným lidem a když něco takového uvidí u jiných, aby to rychle nahlásili a nebyli přihlížejícími (tohle platí především pro věkovou skupinu 15 a méně).

Preventivní semináře a interaktivní cvičení na základních školách

Z dotazníkového šetření vyplývá, že nejvíce ohroženou skupinou na Internetu bývají žáci základních škol (15 let a méně). Proto by se na základních školách měly konat preventivní opatření v rámci seminářů jak pro žáky, tak pro rodiče. Na českých základních školách probíhá těchto projektů spousty, avšak při provádění focus group někteří studenti uvedli, že to byla „jen" hodinová přednáška, kterou si poslechli a nic moc si z ní neodnesli. Proto by bylo vodné dělat na škole pravidelné projekty, které se této problematiky týkají a zapojit do nich samotné žáky prostřednictvím interaktivních cvičení. Z dotazníkového šetření také vychází, že studenti (nebo někdo z jejich okolí) se nejvíce setkávají s kyberšikanou a krádeží identity, proto by bylo vhodné zaměřit tyto cvičení především na tyto rizika a věnovat jim větší pozornost.

Být obezřetný k informacím na sociálních médiích

Ne vše, co se na Internetu píše, je pravdivé, jak už bylo popsáno v teoretické části. Proto je třeba si informace ověřovat z více zdrojů, znát dezinformační weby a znát také projekty, které na tyto weby a dezinformace upozorňují. Je vhodné si na vše udělat vlastní názor a posoudit, zdali je informace věrohodná a nešířit hoaxy dál.

Vytvářet silná hesla

Dalším velmi důležitým bodem jsou silná hesla. Je potřeba si svůj učet dobře zabezpečit a nastavit si takové heslo, které nelze snadno uhádnout. Mezi nevhodná hesla, která se nedoporučují používat, se řadí jména svých domácích mazlíčků, poštovní směrovací číslo, nebo jména svých blízkých. Je třeba si nastavit heslo, které bude přiměřené dlouhé a bude obsahovat všechny možné znaky od velkých písmen přes číslice až po písmena s háčky. Také by heslo nemělo být stejné na více účtech a už vůbec by se nemělo nikomu prozrazovat a zvyšovat tak riziko jeho zneužití. Na Internetu jsou některé generátory, které dokáží

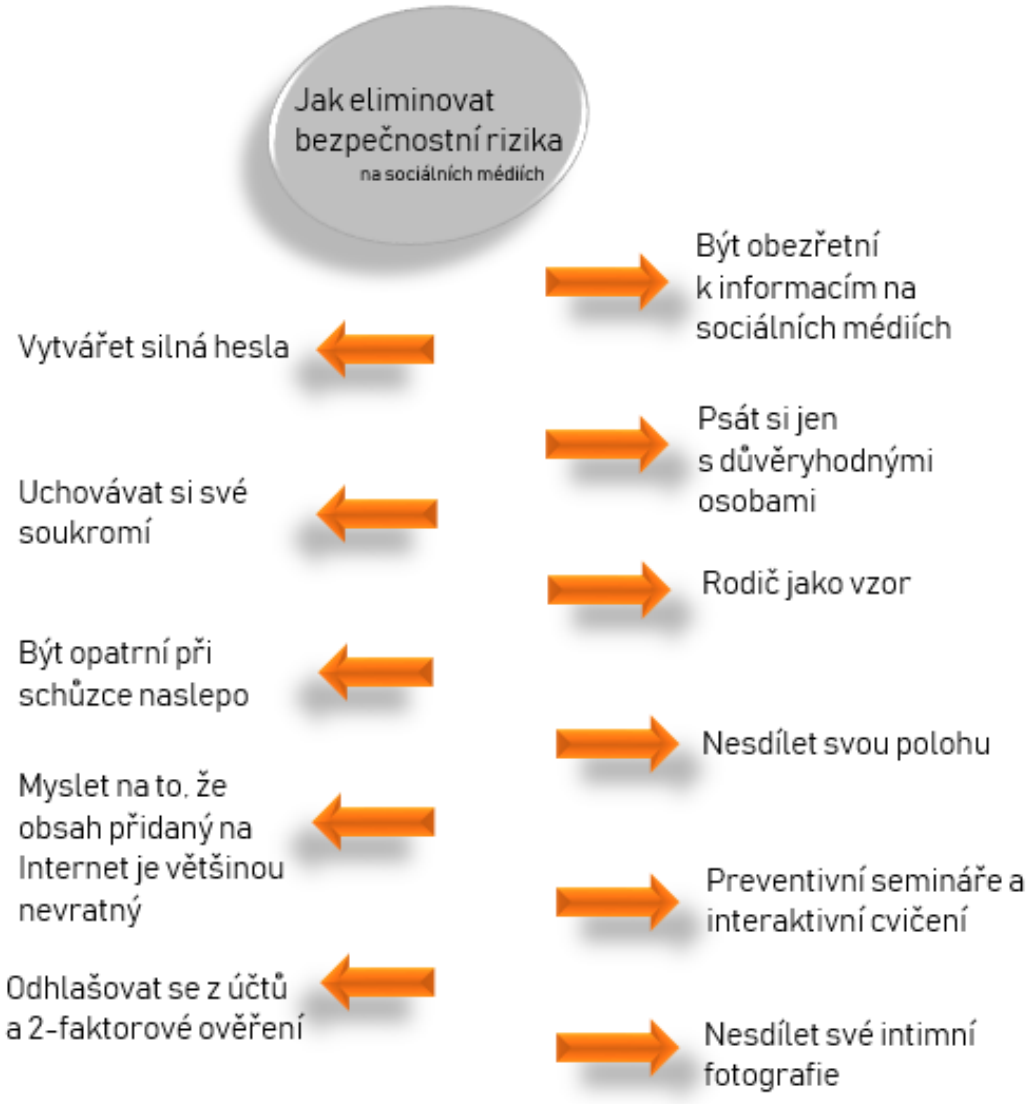
vytvořit silné a náhodné heslo, které si zároveň lze zapamatovat. Je jím například stránka Xkpaswd.net.

Odhlašovat se z účtů a 2-faktorová autentifikace

Při používání sociálních médií na jiném počítači než na zařízení uživatele je důležité dbát na odhlašování se ze všech účtů, na kterých se při užívání jiného zařízení uživatel přihlásil. Eliminuje se tak riziko jejich zneužití. Kromě hesla je důležité také myslet na 2-faktorovou autentifikaci a při přihlašování nepoužívat jen heslo, ale například nechat si poslat SMS s kódem, které ověřují, že jde opravdu o majitele účtu.

Na následujícím obrázku č. 26 lze pro shrnutí vidět všechna navržená doporučení, která by mohla napomoct k eliminaci rizik hrozících na sociálních médiích.

Obrázek č. 26 - Model preventivních opatření



Zdroj: Vlastní zpracování, 2019

Závěr

Cílem práce bylo pomocí vhodných metod zjistit, zdali se uživatelé Internetu cítí na sociálních médiích bezpečně, zdali jsou obeznámeni s riziky, která je na sociálních médiích mohou potkat a na základě toho navrhnout opatření a doporučení, jak se těmto rizikům vyvarovat. Autorka postupovala dle zásad bakalářské práce a v teoretické části byly vymezeny pojmy jako Internet, sociální média, výhody a nevýhody sociálních médií, bezpečnost na Internetu a rizika spojená s využíváním sociálních médií.

Praktická část je rozdělena na tři části. V první je popsáno a vyhodnoceno dotazníkové šetření. Celkem odpovědělo 150 studentů vysokých a středních škol. Byl vytvořen i souhrnný report, který obsahuje souhrnné zjištění z tohoto dotazníkového šetření. Bylo zjištěno, že polovina studentů se na Internetu cítí bezpečně a většina z nich rizika, která na sociálních médiích hrozí, zná. Nejvíce se studenti setkali (nebo někdo z jejich okolí) s kyberšikanou nebo krádeží identity.

Další části byla metoda focus group, která doplnila dotazníkové šetření. Bylo aplikováno na studenty středních škol, kteří nejdříve byli obeznámeni s riziky, která jim povětšinou byla již známá, a pro úplnost jim byl k diskusi poskytnut slovníček pojmů, který obsahoval všechny rizika s krátkým vysvětlením. Poté následovala již samotná diskuse, díky které se autorka dozvěděla detailnější odpovědi.

Třetí částí byla již doporučení a opatření, která by měl uživatel sociálních médií, a především věková skupina 16 let a méně (podle respondentů nejohroženější skupina), dodržovat. Mezi navržená doporučení se řadilo vytváření silných hesel, dvoufázové přihlašování, uchovávání soukromých informací, nezveřejňování intimních fotografií, psaní si jen s lidmi, kterým studenti věří a uskutečňování preventivních seminářů a cvičení na školách, jelikož z dotazníkového šetření také vyplynulo, že veřejnost obecně s riziky obeznámena není.

Seznam obrázků

Obrázek č. 1 - Rozdělení sociálních médií.....17
Obrázek č. 2 - Jednotlivci používající sociální sítě 18
Obrázek č. 3 - Vývoj počtu uživatelů Facebooku do června roku 2017.....21
Obrázek č. 4 – Vývoj počtu uživatelů Instagramu do roku 2017.....23
Obrázek č. 5 - Průměrný týdenní čas strávený na YouTube v minutách v roce 2017 dle věku 26
Obrázek č. 6 - Výhody a nevýhody sociálních médií 28
Obrázek č. 7 - Příklad hoaxu.....30
Obrázek č. 8 - Falešný citát sdílený podporovatelem SPD a Miloše Zemana, který sdílelo 6.5 tisíce lidí 31
Obrázek č. 9 - Obavy z rizik hrozících na Internetu 34
Obrázek č. 10 - Příklady stránek phishingu, které napodobují přihlašování do služby Facebook 35
Obrázek č. 11 - Pohlaví studentů.....46
Obrázek č. 12 - Věk studentů 47
Obrázek č. 13 - Typ školy 47
Obrázek č. 14 - Nejčastější aktivita na Internetu 48
Obrázek č. 15 - Nejčastější aktivita u mužů.....49
Obrázek č. 16 - Nejčastější aktivita u žen 49
Obrázek č. 17 - Kolik času studenti na sociálních médiích tráví 51
Obrázek č. 18 – Užitečnost doby strávené na sociálních médiích 52
Obrázek č. 19 - Důvody používání sociálních médií.....53
Obrázek č. 20 - Důvody pro seznamování se na Internetu.....54
Obrázek č. 21 - Jaké údaje o sobě uživatelé udávají 55
Obrázek č. 22 - Bezpečností rizika, se kterými se studenti, nebo někdo v jejich okolí někdy setkali 56
Obrázek č. 23 - Jak eliminovat rizika spojená s užíváním sociálních médií.....57
Obrázek č. 24 - Znalost projektů zaměřujících se na bezpečností rizika 57
Obrázek č. 25 - Report z dotazníkového šetření.....59
Obrázek č. 26 - Model preventivních opatření 67

Seznam tabulek

Tabulka č. 1 - Počet respondentů s důvěrou v informace uvedené na Facebooku a na internetové stránce.....50
Tabulka č. 2 - Počet studentů, kteří znají a využívají daná sociální média 51
Tabulka č. 3 - Počet studentů, kteří si píší s cizími lidmi na sociálních médiích a zdali jim to přijde běžné a normální 53
Tabulka č. 4 - Procentuální vyjádření počtu studentů VŠ a SŠ studia a jejich pocit bezpečí na Internetu 55

Použité zdroje

Tištěné zdroje

BEDNÁŘ, Vojtěch. Markeing na sociálních sítích: Prosaďte se na Facebooku a Twitteru. Brno: Computer Press, 2011. ISBN 978-80-251-3320-0.

DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

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

GREGOR, Miloš, Petra VEJVODOVÁ a ZVOL SI INFO. *Nejlepší kniha o fake news!!!*. Brno: CPress, 2018. ISBN 978-80-264-1805-4.

HENDL, Jan. *Přehled statistických metod: Analýza a metaanalýza dat.* 5. vyd. Praha: Portál, 2015. ISBN 978-80-262-0981-2.

JANOUCH, Viktor. *Internetový marketing: Prosaďte se na webu a sociálních sítích*. Brno: Computer Press, 2013. ISBN 978-80-251-2795-7.

JANSA, Lukáš, OTEVŘEL, Petr, ČERMÁK, Jiří, MALIŠ, Petr, HOSTAŠ, Petr, MATĚJKA, Michal, MATĚJKA, Jan. *Internetové právo*. Brno: Computer Press, 2016. ISBN 978-80-251-4664-4.

KOŽÍŠEK, Martin a Václav PÍSECKÝ. *Bezpečně n@ internetu: průvodce chováním ve světě online*. Computer Press, 2016. ISBN 978-80-247-5595-3.

PETROWSKI, Thosten. *Bezpečně na internetu pro všechny*. Dialog: Liberec, 2014. ISBN 978-80-7424-066-9.

STOWELL, Louie. *Bezpečnost dětí na internetu*. Praha: Svojtka & Co., 2017. ISBN 978-80-256-2083-0.

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

WALTER, Ekaterina. *Mysli jako Zuckerberg: Pět podnikatelských tajemství šéfa firmy Facebook*. Praha: Management Press, 2013. ISBN 978-80-7261-264-2.

Internetové zdroje

AKTUÁLNĚ.CZ. *YouTube.* [online]. aktualne.cz, 2011. [cit. 22.2.2019]. Dostupné na: https://www.aktualne.cz/wiki/zahranici/youtube/r~i:wiki:1147/?redirected=1554124549

BEZPEČNĚ ONLINE. *O co jde když se řekne sexting?* [online]. saferinternet.cz, 2012. [cit. 17.3.2019]. Dostupné na: https://bezpecne-online.saferinternet.cz/pro-rodice-a-ucitele/teenageri-a-komunikace/item/37-o-co-jde-kdyz-se-rekne-sexting

bezpečný internet.cz. [online]. bezpecnyinternet.cz, n.d. [cit. 4.4.2019]. Dostupné na: http://www.bezpecnyinternet.cz/

BEZPEČNÝ INTERNET.CZ. *Krádež identity a jak se ji bránit.* [online]. bezpecnyinternet.cz, n.d. [cit. 21.3.2019]. Dostupné na: http://www.bezpecnyinternet.cz/pokrocily/ochrana-prav/kradez-identity.aspx?kurz=true

BEZPEČNÝ INTERNET.CZ. *Co dělat, pokud se stanu obětí phishingu?* [online]. bezpecnyinternet.cz, n.d. [cit. 1.4.2019]. Dostupné na: http://www.bezpecnyinternet.cz/zacatecnik/prochazeni-webu/obeti-phishingu.aspx

BILAL, Ahmad. *10 Advantages and Disadvantages of Social Media for Society.* [online]. techmaish.com, 2016. [cit. 5.4.2019]. Dostupné na: https://www.techmaish.com/advantages-and-disadvantages-of-social-media-for-society/

Bílý kruh bezpečí. [online]. bkb.cz, 2009. [cit. 4.4.2019]. Dostupné na: https://www.bkb.cz/

BUSSINESSCENTER.CZ. *Zákon o ochraně osobních údajů.* [online]. Bussinescenter.cz, 1998. [cit. 1.2.2019]. Dostupné na: https://business.center.cz/business/pravo/zakony/oou/cast1h1.aspx#par4

BURDOVÁ, Michaela. *Kyberstalking? Nebezpečné pronásledování!* [online]. jdidoklubu.cz, 2016. [cit. 19.3.2019]. Dostupné na: https://www.jdidoklubu.cz/Kyberstalking-Nebezpecne-pronasledovani-P7027602.html

CLAYWELL, Charlie. *Advantages and Disadvantages of Social Networking.* [online]. lovetoknow.com, n.d. [cit. 5.4.2019]. Dostupné na: https://socialnetworking.lovetoknow.com/Advantages_and_Disadvantages_of_Social_NetworNetw

COMGUARD. *Pozor, je to phishing!* [online]. channelworld.cz, 2018. [cit. 5.4.2019]. Dostupné na: https://channelworld.cz/press-room/pozor-je-to-phishing-21282

ČAMBALA, Lukáš. *YouTube má rekordní počet uživatelů. Každou minutu nahrávají stovky hodin obsahu.* [online]. smartmania.cz, 2018. [cit. 22.2.2019]. Dostupné na: https://smartmania.cz/youtube-ma-rekordni-pocet-uzivatelu-kazdou-minutu-nahravaji-stovky-hodin-obsahu/

ČERNÁ, Zuzana. *Kdo bude Čechy chránit před fake news? To zatím není jasné, ale řeší se to na nejvyšší úrovni.* [online]. seznamzpravy.cz, 2019. [cit. 10.3.2019]. Dostupné na: https://www.seznamzpravy.cz/clanek/kdo-bude-cechy-chranit-pred-fake-news-to-zatim-neni-jasne-ale-resi-se-to-na-nejvyssi-urovni-66823

ČSÚ. *Informační společnost v číslech.* [online]. czso.cz, 2018. [cit. 5.4.2019]. Dostupné na: 6.https://www.czso.cz/documents/10180/61601892/061004-18_C.pdf/d972dac5-2c5b-4330-9280-12e219604519?version=1.0

DATACENTRUM WEDOS. *Co je to Internet a jak funguje?* [online]. datacentrum.wedos.com, 2010. [cit. 27.1.2019]. Dostupné na: https://datacentrum.wedos.com/a/17/co-je-internet-jak-funguje.html

Demagog.cz. [online]. Demagog.cz, 2012. [cit. 10.4.2019]. Dostupné na: https://demagog.cz/

DEMIDOVA, Nadezdha, SHCHERBAKOVA, Tatyana, VERGELIS. *Maria. Spam and phishing in Q1 2018.* [online]. securelist.com, 2018. [cit. 15.3.2019]. Dostupné na: https://securelist.com/spam-and-phishing-in-q1-2018/85650/

ČTK. *Únik dat z facebooku se týká až 87 milionů uživatelů.* [online]. eurozpravy.cz, 2018. . [cit. 18.3.2019]. Dostupné na: https://eurozpravy.cz/veda-a-technika/internet/219915-unik-dat-z-facebooku-se-tyka-az-87-milionu-uzivatelu/

DOSTÁL, Jiří. *Internet druhé generace pro učitele.* [online]. Olomouc: Univerzita Palackého, 2011 [cit. 20.3.2019]. ISBN 978-80-224-2779-9. Dostupné na: https://books.google.cz/books?id=RPCmxttiGIC&printsec=frontcover&dq=dost%C3%A1l+internet&hl=cs&sa=X&ved=0ahUaahUah5mnnqLhAhWEL1AKHQr2B70Q6AEIKDAA#v=onepage&q=dost%C3%A1l%20iiiinter&f=false

E-bezpečí. [online]. e-bezpeci.cz, 2008. [cit. 5.4.2019]. Dostupné na: https://www.e-bezpeci.cz/

E-BEZPEČÍ.CZ. Výzkum *Sexting a rizikové seznamování českých dětí v kyberprostoru (2017)*. [online]. e-bezpeci.cz, 2017. [cit. 18.3.2019]. Dostupné na: http://o2.e-bezpeci.cz/#vyzkum

EBIZMBA.COM. *Top 15 Most Popular Social Networking Sites | January 2019.* [online]. Ebzimba.com, 2019. [cit. 15.3.2019]. Dostupné na: http://www.ebizmba.com/articles/social-networking-websites

ESET.COM. *Krádež identity*. [online]. eset.com, n.d. [cit. 21.3.2019]. Dostupné na: https://www.eset.com/cz/kradez-identity/

FEEDIT.CZ. *Nejnovější čísla pro Facebook a Instagram v ČR*. [online]. feedit.cz, 2018. [cit. 10.2.2019]. Dostupné na: https://feedit.cz/2018/09/24/nejnovejsi-cisla-pro-facebook-a-instagram-v-cr/

FILIP, Jiří. *Facebook postihl obří únik dat. Hackeři se mohli zmocnit informací z 50 milionů účtů*. [online]. letemsvetemapplem.cz, 2018. [cit. 15.2.2019]. Dostupné na: https://www.letemsvetemapplem.eu/2018/09/28/facebook-postihl-obri-unik-dat-hackeri-se-mohli-zmocnit-informaci-z-50-milionu-uctu/

FOCUS. *Uživatelé sociálních sítí v ČR*. [online]. focus-agency.cz, 2016. [cit. 10.2.2019]. Dostupné na: https://www.focus-agency.cz/files/contentFiles/socialni-site-2016-cz.pdf

HOAX.CZ. *Facebook - automatické mazání neaktivních členů skupin.* [online]. hoax.cz, 2019. [cit. 9.3.2019]. Dostupné z: http://www.hoax.cz/hoax/facebook---automaticke-mazani-neaktivnich-clenu-skupin/

HUDSON, Mathew. *What is Social Media?* [online]. thebalancesmb.com, 2018. [cit. 14.3.2019]. Dostupné na: https://www.thebalancesmb.com/what-is-social-media-2890301

IDNES.CZ. *Důvěřují a neprověřují. Čechům bezpečnost na internetu moc neříká* [online]. iDnes.cz, 2019. [cit. 15.3.2019]. Dostupné na: https://www.idnes.cz/ekonomika/domaci/internet-bezpecnost-cesi-pruzkum-zneuziti.A190213_457221_ekonomika_rts

IDNES.CZ. *Soud potrestal zneužití jednadvaceti chlapců osmi lety vězení.* [online]. iDnes.cz, 2009. [cit. 16.3.2019]. Dostupné na: https://www.idnes.cz/zpravy/cerna-kronika/soud-potrestal-zneuziti-jednadvaceti-chlapcu-osmi-lety-vezeni.A090205_101224_krimi_jba

IMIP.CZ *Co je Internet?* [online]. Imip.cz, 2011. [cit. 27.1.2019]. Dostupné na: http://www.imip.cz/

IMIP.CZ *Internet historie.* [online]. Imip.cz, 2011. [cit. 27.1.2019]. Dostupné na: http://www.imip.cz/internet-historie/

INTERNETEM BEZPEČNĚ. *Kyberšikana.* [online]. internetemebezpecne.cz, n.d. [cit. 17.3.2019]. Dostupné na: https://www.internetembezpecne.cz/internetem-bezpecne/rizika-online-komunikace/kybersikana/

JAVŮREK, Karel. *Twitter je poprvé v historii v zisku, počty aktivních uživatelů ale nerostou.* [online]. zive.cz, 2018. [cit. 19.2.2019]. Dostupné na: https://connect.zive.cz/clanky/twitter-je-poprve-vhistorii-v-zisku-pocty-aktivnich-uzivatelu-ale-nerostou/sc-320-a-191729/default.aspx

JSNS.CZ. *Seznam se bezpečně.* [online]. jsns.cz, n.d. [cit. 4.4.2019]. Dostupné na: https://www.jsns.cz/projekty/medialni-vzdelavani/bulletin-medialni-vzdelavani/predstavujeme/seznam-se-bezpecne

Linka bezpečí. [online]. linkabezpeci.cz, n.d. [cit. 3.4.2019]. Dostupné na: https://www.linkabezpeci.cz/

LORENC, Jakub. *Jak se daří jednotlivým sociálním sítí v České republice?* [online]. linkedin.com, 2017. [cit. 10.3.2019]. Dostupné na: https://www.linkedin.com/pulse/jak-se-daří-jednotlivým-sociálním-sítí-v-české-republice-jakub-lorenc/

LUKWAGO J. *How Facebook Managed To Reach 2 Billion Monthly Active Users.* [online]. newslexpoint.com, 2017. [cit. 18.3.2019]. Dostupné na: https://newslexpoint.com/facebook-hits-2-billion-monthly-users/

NATIONS, Daniel. *What Is Social Media?* [online]. Lifewire.com, 2019. [cit. 14.3.2019]. Dostupné na: https://www.lifewire.com/what-is-social-media-explaining-the-big-trend-3486616

NĚMEČKOVÁ, Kateřina. *Čísla hovoří jasně: rok 2017 byl pro Instagram nebývale úspěšný.* [online]. focus-age.cz, 2018. [cit. 19.2.2019]. Dostupné na: https://www.focus-age.cz/m-journal/aktuality/cisla-hovori-jasne--rok-2017-byl-pro-instagram-nebyvale-uspesny__s288x13398.html

Manipulátoři.cz. [online]. Manipulatori.cz, n.d. [cit. 10.3.2019]. Dostupné na: https://manipulatori.cz/

MÁCA, Roman. *Dezinformace, maily, falešné citáty. Studie ukazuje, jak se v Česku ovlivňují volby.* [online]. info.cz, 2018. [cit. 9.4.2019]. Dostupné na: https://www.info.cz/cesko/dezinformace-maily-falesne-citaty-studie-ukazuje-jak-se-v-cesku-ovlivnuji-volby-36815.html

PAVLÁT, Martin. *Řeč čísel: Aneb, jaký byl rok 2017 pro sociální média.* [online]. anvenies.cz, 2018. [cit. 19.2.2019]. Dostupné na: https://anvenies.cz/rec-cisel-aneb-jaky-byl-rok-2017-pro-socialni-media/

PRICE-MITCHEL, Marylin. *Disadvantages of Social Networking: Surprising Insights from Teens.* [online]. rootsofaction.com, 2014. [cit. 5.4.2019]. Dostupné na: https://www.rootsofaction.com/disadvantages-of-social-networking/

RETAILNEWS.CZ. *GDPR se nevyhne ani internetu a sociálním sítím*. [online]. Retailnews.cz, 2017. [cit. 1.2.2019]. Dostupné na: https://retailnews.cz/2017/09/08/gdpr-se-nevyhne-ani-internetu-a-socialnim-sitim/

RYCHLOFKY.CZ. *Linkedin má 500 milionů registrovaných účtů a pouze 25 % z nich měsíčně službu používá*. [online]. rychlofky.cz, 2017. [cit. 19.2.2019]. Dostupné na: https://rychlofky.cz/2017/04/24/linkedin-ma-500-milionu-registrovanych-uctu-a-pouze-25-z-nich-mesicne-sluzbu-pouziva/

SKLENÁK, Vilém. *Data, informace, znalosti a Internet.* [online]. Praha: C. H. Beck, 2001 [cit. 20.3.2019]. ISBN 80-7179-409-0. Dostupné z: https://books.google.cz/books?id=UJh-gLdTH8IC&printsec=frontcover&dq=sklen%C3%A1k&hl=cs&sa=X&ved=0ahUKEwjq26bbbbOnKLhAhXNjqQ-TC8wQ6AEIKDAA#v=onepage&q=sklen%C3%A1k&f=false

SMITH, Nick, WOLLAN, Robert, ZHOU, Catherine. *The Social Media Management Handbook.* [online]. New Jersey: John Wiley & Sons, 2011. [cit. 14.3.2019]. ISBN 978-0-470-65124-7. Dostupné na: https://books.google.cz/books?id=DltMsBQvDP0C&pg=PT7&lpg=PT7&dq=smith+wollan+you+book&source=bl&ots=TaERvRgZZb&sig=ACfU3U0Clha8nDPuZ7DfOG5gz0UuHpvKUu&hl=cs&sa=X&ved=2ahUKEwia8ca14anhAhWj2eAKHbQXDZMQ6AEwCHoECAgQAA#v=onepage&q=smith%20wollan%20you%20book&f=false

TECHNOPEDIA. *Web 3.0.* [online]. Technopedia, 2019. [cit. 20.3.2019]. Dostupné na: https://www.techopedia.com/definition/4923/web-30

WEAVER, E. *25 Advantages Of Social Media That Are Good To Keep In Mind.* [online]. list25.com, 2017. [cit. 5.4.2019]. Dostupné na: https://list25.com/25-advantages-of-social-media-that-are-good-to-keep-in-mind/3

ZÁRUBOVÁ, Zuzana. *Web 2.0.* [online]. Wiki CR, 2014. [cit. 20.3.2019]. Dostupné na: https://fim2.uhk.cz/wikicr/web/index.php/home/9-ict/110-web-20

ZLATOVSKÝ, Michal, KOČÍ, Petr. *Žebříček českých neověřených článků: dezinformační texty mají nad pravdivými navrch.* [online]. rozhlas.cz, 2016. [cit. 10.3.2019]. Dostupné na: https://interaktivni.rozhlas.cz/dezinformace/

Zvol si info. [online]. BRUNO & ZENI, 2019. [cit. 10.3.2019]. Dostupné z: https://zvolsi.info/

Seznam příloh

Příloha A – dotazníkové šetření

Příloha B – pracovní list k metodě focus group

Příloha A – dotazníkové šetření

Dotazníkové šetření

V rámci mé bakalářské práce na téma Bezpečnost na sociálních sítích, jsem jako jednu z metod průzkumu pro získání informací zvolila dotazníkové šetření, které se zaměřuje na sociální média, Internet, jeho rizika a bezpečnost. Věnujte prosím několik minut jeho vyplněním. Pokud bude něco nejasného, ráda zodpovím případné dotazy.

1. Jsem:
   - □ Muž
   - □ Žena

2. Studuji:
   - □ Střední školu
   - □ Vysokou školu

3. Spadám do věkové kategorie:
   - □ 15-16
   - □ 17-19
   - □ 20-22
   - □ 23-25
   - □ 26-27

4. Jakou činnost na internetu nejčastěji děláte? (možnost více odpovědí)
   - □ Čtení zpráv
   - □ Chatování s přáteli
   - □ Nakupování
   - □ Sledování filmů/videí
   - □ trávení času na sociálních sítích
   - □ psaní emailů
   - □ získávání informací o cestování
   - □ získávání informací pro vzdělávání
   - □ jiná: _____

5. Pokud je informace uvedena na Facebooku (např. politické strany, cestovní agentury..), pak ji:
   - □ Věřím

□ Spíše věřím
□ Nedokážu odpovědět
□ Spíše nevěřím
□ Nevěřím

6. Pokud je informace uvedena na internetové stránce (např. politické strany, cestovní agentury..), pak ji:
   □ Věřím
   □ Spíše věřím
   □ Nedokážu odpovědět
   □ Spíše nevěřím
   □ Nevěřím

7. Která sociální média znáte?
   □ Facebook
   □ Instagram
   □ Twitter
   □ YouTube
   □ Ask.fm
   □ LinkedIn
   □ Lidé.cz
   □ Líbímseti.cz
   □ Spolužáci.cz
   □ ČSFD.cz

8. A kterou z nich sami využíváte?
   □ Facebook
   □ Instagram
   □ Twitter
   □ YouTube
   □ Ask.fm
   □ LinkedIn
   □ Lidé.cz
   □ Líbímseti.cz
   □ ČSFD.cz

9. Kolik času denně na sociálních médiích trávíte?
   □ Méně než hodinu
   □ Hodinu
   □ Dvě hodiny
   □ Tři hodiny
   □ Déle

10. Přijde Vám doba strávená na sociálních médi užitečná?

□ Ano
□ Spíše ano
□ Nedokážu odpovědět
□ Spíše ne
□ Ne

11. Myslíte si, že sociální média mají více výhod, nebo nevýhod?
□ Výhody
□ Spíše výhody
□ Nedokážu odpovědět
□ Spíše nevýhody
□ Nevýhody

12. Z jakého důvodu používáte sociální média? (možnost více odpovědí)
□ Možnost komunikace s přáteli
□ Marketing
□ Sdílení
□ Seznámení
□ Čtení zpráv
□ jiná: _____

13. Vadí Vám psát si na sociálních médiích s cizími lidmi?
□ Vadí mi to
□ Spíše mi to vadí
□ Nedokážu odpovědět
□ Spíše mi to nevadí
□ Nevadí

14. V návaznosti na předchozí otázku - přijde Vám psaní na sociálních médicích s cizími lidmi běžné a normální?
□ Přijde mi to běžné a normální
□ Spíše mi to přijde běžné a normální
□ Nedokážu odpovědět
□ Spíše mi to nepřijde běžné a normální
□ Nepřijde mi to běžné a normální

15. Seznámili jste se někdy díky sociálním médiím s někým, kdo je Váš kamarád dodnes?
□ Ano
□ Ne

16. Jaký je podle Vás důvod stále častějšího seznamování se přes internet? (možnost více odpovědí)
□ Nedostatek jiných příležitostí
□ Ostýchavost
□ Nedostatek času na seznamování

□ Specifické požadavky na partnera
□ jiný: _____

17. Dáváte na sociální média pravdivé osobní údaje?
□ Ano
□ Spíše ano
□ Nedokážu odpovědět
□ Spíše ne
□ Ne

18. Jaké údaje o sobě na sociální média udáváte?
□ Jméno a příjmení
□ Věk
□ E-mail
□ Adresu
□ Sexuální orientaci
□ Pohlaví
□ Zaměstnání
□ Rodinný stav
□ jiné: _____

19. Cítíte se na internetu bezpečně?
□ Ano
□ Spíše ano
□ Nedokážu odpovědět
□ Spíše ne
□ Ne

20. Která věková skupina je podle Vás při využívání sociálních médidích nejvíce ohrožena?
□ 15 a méně
□ 16-18
□ 19-25
□ 26-30
□ 31-40
□ 41 a více

21. Je podle Vás dostatečně veřejnost obeznámena s nebezpečím, které se vyskytuje na sociálních médiích?
□ Ano
□ Spíše ano
□ Nedokážu odpovědět
□ Spíše ne
□ Ne

22. Znáte možná rizika, která Vás na sociálních médiích mohou potkat?

□ Ano
□ Spíše ano
□ Nedokážu odpovědět
□ Spíše ne
□ Ne

23. Označte bezpečnostní riziko, se kterým jste se Vy, nebo někdo z Vašeho okolí někdy setkali:
□ Kyberšikana
□ Sexting
□ Kybergrooming
□ Krádež identity
□ Phishing
□ Stalking
□ Vydírání
□ Nesetkal/a jsem se

24. Jak byste tato rizika eliminovali? (možnost více odpovědí)
□ Sociální sítě vůbec nepoužívat
□ Dávat si pozor na to, komu poskytuji osobní údaje
□ Nepsat si s cizími lidmi
□ Nezveřejňovat na sociálních sítích své fotky
□ jinak: _____

25. Znáte některý z preventivních projektů, které mají za cíl tyto rizika snižovat?
□ Seznam se bezpečně
□ E-bezpečí
□ Linka bezpečí
□ Bezpečný internet
□ Bílý kruh bezpečí
□ Neznám žádný
□ Znám jiný: _____

26. Jaká je podle Vás budoucnost sociálních médií?
_____
_____
_____

Děkuji za vyplnění.

Příloha B – pracovní list k focus group

Focus group

1. Rozdání dotazníků, vysvětlení, ujištění o tom, že dotazník je anonymní + rozdání slovníčků pojmů
2. Po vyplnění shrnutí dotazníku, optat se, zda bylo vše jasné, zda všemu rozuměli, zda jim všechny otázky vyhovovaly a nebyly některé moc citlivé
3. Otázky – doplňující k otázkám z dotazníku + otázky mimo dotazník
4. V případě času debata (pokud bude - vlastní zkušenost s rizikem)

Doplňující otázky k dotazníku:

Jakou činnost na Internetu nejčastěji děláte – Proč zrovna tato činnost, děláte i jinou činnost?

Pokud je informace uvedena…na fb – proč ji věříte/nevěříte? + které informace na fb nejčastěji vyhledáváte? (o politice, média)

Pokud je informace uvedena na internetové stránce – proč ji věříte/nevěříte? + které informace na internetu nejčastěji vyhledáváte? (o škole, o počasí)

Kolik času na sociálních médiích trávíte? – pokud déle, kolik?

Přijde Vám doba strávená na sociálních médiích užitečná? – Pokud ne, proč? Co užitečnějšího by se dalo na Internetu dělat?

Myslíte si, že sociální média mají více výhod, nebo nevýhod? – Uveďte výhody a nevýhody sociálních sítí

Jaké údaje o sobě na sociální média udáváte? – Jaké údaje byste na síť o sobě nikdy nedali?

Seznámili jste se někdy s někým přes internet, kdo je Váš kamarád dodnes? - Našli jste si někdy díky sociálním sítím partnera?

Která skupina je na internetu nejvíce ohrožena? – Proč si myslíte, že zrovna tato?

Je podle Vás dostatečně veřejnost obeznámena s nebezpečím, které se vyskytuje na sociálních médiích? – Pokud Vaše odpověď byla „Ne“, jak by se tato situace dala řešit, napadají Vás nějaká opatření? (např. semináře na středních/základních školách)

Rizika na sociálních médiích – Napadají Vás kromě uvedených ještě nějaká rizika, se kterými byste se mohli setkat? + dají se tyto rizika nějak ovlivnit svým chováním?

Otázky, které se k dotazníku nevztahují:

ZÁVISLOST NA SOCIÁLNÍCH MÉDIÍCH

Myslíte si, že jste na sociálních médiích závislí? Dokázali byste se jich vzdát?

Přemýšleli jste někdy o zrušení účtu?

Cítíte se nervózní / nesvůj, když nemáte možnost připojení na soc. média?

Myslíte si, že díky sociálním médiím ztrácíme schopnost komunikovat s lidmi „face to face“ ?

Jakému typu komunikace dáváte přednost? (osobní, sociální sítě)

FACEBOOK

Myslíte si, že Facebook může být v blízké budoucnosti ohrožen jinou platformou? (díky stále větším nedostatkům)

Přidáváte si na Facebooku jen lidi, které znáte?

Co si myslíte, že je největší výhodou Facebooku?

DŮVĚRA

Důvěřujete lidem, které máte na sociálních médiích? (svým followers, přátelům na fb)

Svěřujete se lidem na sociálních médiích?

OBSAH NA SÍTI

Jaký obsah vkládáte na sociální média a jak často?

Abstrakt

JÁSNKÁ, Veronika. *Bezpečnost na sociálních médiích*. Bakalářská práce. Plzeň: Fakulta ekonomická ZČU v Plzni, 78 s., 2019.

Klíčová slova: Internet, Sociální média, bezpečnost, rizika

Tato bakalářská práce se zabývá bezpečností na sociálních médiích a riziky, které na sociálních médiích mohou hrozit. Práce je rozdělena do dvou částí – teoretické a praktické. V teoretické části autorka popisuje základní pojmy z oblasti Internetu, sociálních médií a bezpečností na nich. Praktická část je poté rozdělena do tří částí. Nejdříve autorka provedla dotazníkové šetření mezi studenty, kde cílem bylo zjistit, jak bezpečně se na sociálních médiích cítí a s jakými bezpečnostními riziky se již setkali. Druhá část praktické práce je zjišťovaní dat pomocí metody focus group, která doplnila výsledky z dotazníkového šetření. Na závěr, poslední částí práce, jsou navržená doporučení a opatření, která by měla sloužit jako prevence a napomoct k eliminaci těchto rizik.

Abstract

JÁNSKÁ, Veronika. Security on Social Meida. Bachelor thesis. Pilsen: Faculty of Economic, University of West Bohemia. 78 s., 2019.

Key words: Internet, Social media, safety, risks

This Bachelor thesis deals with Security on Social Media and risks that social media may have. The thesis is divided into two main parts – theoretical and practical. In the theoretical part the author defíines basics concepts of Internet, social media and the security on them. The practical part is divided into three parts. First, the author conducted a questionnaire survey among students, where the aim was to find out how safe they feel about social media and what security risks they have already encountered. The second part of the practical part is finding out the data using the focus group method, which completed the results from the questionnaire survey. In conclusion, the last part of the thesis are suggested recommendations and measures that should serve as prevention and help to eliminate these risks.