UNIVERZITA JANA AMOSE KOMENSKÉHO PRAHA

BAKALÁŘSKÉ KOMBINOVANÉ STUDIUM

2013-2017

BAKALÁŘSKÁ PRÁCE

Klára Hrušková

Bezpečnost a bezpečnostní rizika v prostředí internetu

Praha 2017

Vedoucí bakalářské práce: Mgr. Iskanderová Tatiana, Ph.D.

JAN AMOS KOMENSKY UNIVERSITY PRAGUE

BACHELOR COMBINED STUDIES

2013-2017

BACHELOR THESIS

Klára Hrušková

The safety and security risks on the Internet

Prague 2017

The Bachelor Thesis Work Supervisor: Mgr. Iskanderová Tatiana, Ph.D.

Prohlášení

Prohlašuji, že předložená bakalářská práce je mým původním autorským dílem, které jsem vypracovala samostatně. Veškerou literaturu a další zdroje, z nichž jsem při zpracování čerpala, v práci řádně cituji a jsou uvedeny v seznamu použitých zdrojů.

Souhlasím s prezenčním zpřístupněním své práce v univerzitní knihovně.

V Praze dne 10. 9. 2017 Klára Hrušková

Anotace

Cílem práce „Bezpečnost a bezpečnostní rizika v prostředí internetu “ je analyzování současného chování uživatelů internetu se zaměřením na sociální sítě a internetové bankovnictví. První polovina práce je věnovaná teoretické části s vymezením základních pojmů dané problematiky. V druhé části je popsán výzkum a jeho výsledky. Cílem praktické části je porovnání hypotéz s reálnými výsledky zkoumání.

Klíčová slova

Antivirový program, bezpečnost, kyberkriminalita, internet, internetové bankovnictví, osobní údaj, sociální síť

Annotation

The aim of the thesis "The safety and security risks on the Internet" is to analyze the current behavior of Internet users, with a focus on social networks and Internet banking. The first part is devoted to theory and focuses on the basic concepts of the issue. The second part describes the research and its results. Its aim is to compare theory with reality.

Keywords

Antivirus softwarem, cybercrime, internet, internet banking, security, social network, personal data

ÚVOD

Internet je slovo, které v dnešní době ovládá vše. Kdo není na internetu, jako by neexistoval. Internet využíváme v práci i v soukromém životě, stal se nedílnou součástí každého jedince. Najdeme na něm veškeré informace, které aktuálně potřebujeme. Přes internet sdělujeme svému okolí naše pocity, názory, úspěchy. Bohužel nežijeme v ideálním světě a naše informace mohou sloužit jako podnět k trestné činnosti nebo jen k účelům, které nám mají ublížit. Tato práce se zaměřuje na zjištění, zda jsou si dnešní uživatelé vědomi rizik, která jsou spojena s užíváním internetu se zaměřením na sociální sítě a internetové bankovnictví.

Nedílnou součástí života každého jedince jsou sociální sítě. Je to místo, kde se každý může realizovat podle svých představ. Lidé se tu sdružují podle svých zálib, zaměstnání, rodinných příslušníků, názorů a postojů. Navzájem se chlubí svými dětmi, úspěchy, majetkem, fotkami a zážitky. Všechny výše uvedené příklady jsou pouze ty příjemné věci, ale existují i stinné stránky sociálních sítí, protože páchat trestné činy nebo někomu ubližovat přes internet je snadné. K životu na internetu je potřeba pouze profil na sociální síti a připojení k internetu. Žádná fyzická námaha zde není potřeba, ale zato následky mohou být nedozírné. Někdy mohou vést až k vraždě či sebevraždě oběti. Pachatelé často používají falešné profily. Člověk by měl být opatrný, dávat pozor, s kým si píše a komu sděluje svoje osobní věci. Ve výzkumu bude zjišťováno, do jaké míry jsou uživatelé obezřetní a jaké informace o sobě sdělují ostatním uživatelům internetu. Jedním z hlavních bodů výzkumu je zjistit, zda respondenti byli obětí nějakého trestného činu nebo jim bylo ublíženo prostřednictvím sociálních sítí, a jak jim tato skutečnost pomohla změnit jejich současné chování.

Druhým zaměřením práce je bezpečnost internetového bankovnictví. V dnešní době existuje spousta podvodných emailů, zpráv a internetových stránek, které se snaží z uživatele zjistit jeho přihlašovací údaje do internetového bankovnictví. Bude zjišťováno, zda se s tímto jevem respondenti setkali a zda používají antivirové programy, které by je před útoky na internetu dostatečně ochránily.

Práce je zaměřena na aktuální témata dnešní doby. V bakalářské práci bylo nejvíce čerpáno ze zdrojů na internetu. Autorka se snažila najít důvěryhodné stránky k čerpání informací. Byly navštíveny oficiální stránky sociálních sítí nebo stránky, kde je garance od Ministerstva České republiky a Ministerstva školství a tělovýchovy. Tyto stránky jsou využívány převážně učiteli a výchovnými poradci.

Cílem práce je zjistit a popsat specifika chování na internetu z hlediska bezpečnosti používání sociálních sítí a internetového bankovnictví.

TEORETICKÁ ČÁST

1 DEFINICE MASOVÉ A INTERNETOVÉ KOMUNIKACE

Definice masové komunikace

„Masová komunikace“ je termín, který vznikl koncem 30. let 20 století. Termín vyvolává mnoho pocitů, zabarvení a rysů, proto není možné přesně vysvětlit jeho definici, na které by se dalo shodnout. I přesto se našlo pár definic, které můžeme použít. Gerberova definice z roku 1967 říká, že „*masová komunikace je sociální interakce prostřednictvím sdělení*“[1], kde pojem masový znamená velký počet nebo množství a komunikace nabývá významu příjímání a vysílaná sdělení. Další definice podle Janowitze (1986) říká: „*Masová komunikace zahrnuje instituce a postupy, jimiž specializované skupiny využívají technické prostředky pro šíření symbolického obsahu směrem k rozsáhlému, nesourodému a široce rozptýlenému publiku.*“ [2] V tomto případě znamená komunikace přenos a to z pohledu podavatele, nikoli v celé šíři významu, které známe.

Masová komunikace neznamená to samé jako masová média. Masová média jsou postupy a technologie, které umožňují masovou komunikaci. Každý den se setkáváme s masovou komunikací, styk s komunikací je velmi pestrý a dobrovolný. Komunikaci z většiny utváří kultura a nároky daného člověka, každý jedinec má totiž jiný způsob života a sociální prostředí. K vzniku nových vztahů založených na komunikaci dopomáhají nové technologie. Z výše uvedeného vyplývá, že masová komunikace je od samého počátku více představa než samotná realita života.

Pojem „masa“ má rozdílné výklady, vždy závisí na úhlu pohledu vykládajícího. Převládá myšlenka, že masa znamená něco negativního. Slovníková definice vysvětluje masu jako seskupení, v němž se ztrácí osobnost. To je blízko tomu, co říkají

[1] MCQUAIL, Denis. *Úvod do teorie masové komunikace*. Vyd. 2. Praha: Portál, 1999. s.31. ISBN 80-717-8714-0.
[2] tamtéž

sociologové. Masová komunikace v sobě ukrývá kontakt mezi jedním podavatelem a mnoho příjemci, vše probíhá zároveň a spontánně, se stejným vlivem. To jiným formám komunikace chybí.[3]

Internetová komunikace

Internetová komunikace je komunikace, která je nejnovějším a nejrychleji se rozvíjejícím způsobem komunikace mezi jedinci. Mezi její výhody patří rychlost a finanční nenáročnost. Důležitá je i dostupnost, která záleží na připojení k internetu, ale to v dnešní době není takový problém.

Můžeme rozlišovat dva typy komunikace. První je asynchronní komunikace. To je ta, u které není potřeba ihned reagovat. Nejčastějším typem je emailová komunikace. Druhý typ je synchronní komunikace, která naopak vyžaduje okamžitou reakci na zaslanou zprávu. Můžeme se s ním setkat v podobě chatů (např. ICQ, Skype, Messenger na Facebooku apod.) Některé z chatovacích nástrojů můžeme mít nainstalované přímo v mobilním zařízení, čímž se docílí nejrychlejšího dosahu danému adresátovi.

V dnešní době již můžeme přes internetovou komunikaci zasílat nejen jednoduché zprávy, ale i soubory různého typu (dokumenty, fotografie, hudební soubory) nebo projevovat svoje pocity pomocí malých obrázků a animací, které jsou k dispozici u každého chatu.[4]

[3] MCQUAIL, Denis. *Úvod do teorie masové komunikace*. Vyd. 2. Praha: Portál, 1999. ISBN 80-717-8714-0.
[4] *Jak na internet* [online]. [cit. 2017-03-04]. Dostupné z: https://www.jaknainternet.cz/page/1236/komunikace-pres-internet/

2 VZNIK A VÝVOJ INTERNETU

Historie internetu začíná rokem 1957, kdy tehdejší Sovětský svaz vypustil do vesmíru Spuntik, první umělou družici země. Spojené státy americké byly v šoku, protože Sovětský svaz je předběhl i v atomové a vodíkové bombě. USA se snažilo zlikvidovat náskok a roku 1962 dalo podnět ke vzniku speciální vládní agentury ARPA (Advanced Researcg Projects Agency – úřad pro pokročilé výzkumné projekty). Agentura řešila nejdůležitější problém té doby, a to propojení vzdálených velitelských stanovišť v případě konfliktu nebo propojení vědeckých pracovišť. Tím vznikla myšlenka počítačové sítě, která by umožňovala komunikaci pomocí uzlů. Roku 1966 byly získány dotace na vývoj sítě ARPA, získal je Bob Taylor. Jeho projekt bude znám jako ARPANET.

Zlomový byl rok 1969. Je nainstalován první uzel ARPANETu (IMP). Koncem roku byly vytvořeny další tři uzly na kalifornské a utažské univerzitě a také na Stanfordském výzkumném institutu. V roce 1971 měla již síť dvacet uzlů a o rok později třicet sedm. Začaly se rodit myšlenky o dalším použití a začaly pokusy s elektronickou poštou. O rok později, roku 1972, Ray Tomlinson vyvíjí první emailový program. Na toto navazuje rok 1973, kdy vzniká první podoba internetu tak, jak ho znám dnes. [5]

Roku 1975 provoz ARPANETU vzrůstá. Síť mohou využívat nejen vývojáři a univerzity, ale i běžní uživatelé. 1986 – Propojení výzkumných ústavů v celé zemi přes centra, kde se nacházejí super výkonné počítače, k tomuto přispěla Národní vědecká nadace National Science Foundattion (NSF). Tato vysokorychlostní síť se nazývala NSFNET a přenosová rychlost byla 56kb/s. V roce 1987 vznikl pojem Internet a v síti bylo propojeno 27 000 počítačů.

[5] KRAS, P. *Internet: V Kostce užití v běžném životě*. Havlíčkův Brod: Fragment, 2001. ISBN 80-7200-493-X.

První připojení Československé republiky bylo roku 1990, kdy se připojila k síti zvané BITNET. A roku 1991 se Československo připojuje na Internet, byly propojeny školy a vědecká pracoviště.

ARPANET skončil roku 1990, v tomto roce se událo ještě dokončení funkční verze http 0.9, jazyku HTML, dokončení prvního prohlížeče, webového serveru a webové stránky. 6. srpna 1991 Tim Bertners-Lee odeslal hypertextový odkaz na server do internetové diskuze. A také byl nasazen WWW v laboratoři v CERNu. Byl to opravdu velký mezník ve vývoji. Poté šel vývoj rychle kupředu. V roce 1992 se na Internet připojuje Bílý dům v USA. Na ČVUT v Praze došlo k připojení Československa na Internet a na web byla nahrána první fotografie. Na přelomu roků 1992 a 1993 vzniká celorepubliková síť CESNET se středy v Brně a Praze. Města byla mezi sebou propojena pevnou linkou. A již v březnu roku 1993 měl CESNET celkem jedenáct uzlů po celé ČR.

Internet se začal komercionalizovat a roku 1996 již měl na světě 55 milionů uživatelů. O 2 roky později má připojení už 80 zemí světa a přes milion uživatelů. V České republice vznikají národní domény .cz, z.s.p.o. Roku 2000 byl v České republice schválen zákon o elektronickém podpisu. A na celém světě je již 600 milionů uživatelů sítě internet. O 5 let později vzrostl počet uživatelů na 900 milionů a roku 2009 jich bylo již 1,8 miliardy. Následující rok byla překročena hranice 2 miliard. Ve Finsku byl schválen zákon, který říká, že každý člověk má nárok na internet. V České republice byl přijat Zákon o kybernetické bezpečnosti roku 2004.[6]

[6]Benešovská, M.: *Historie internetu v datech*. Helloworld.cz [online]. ©2017 [cit. 2017-03-01]. Dostupné z: http://www.helloworld.cz/historie-internetu-v-datech/

3 SOCIÁLNÍ SÍTĚ: HROZBY A BEZPEČNOST

Podle sociologie je sociální síť propojená skupina lidí, kteří se navzájem ovlivňují, aniž by na to měl vliv jejich příbuzenský vztah. Skupiny jsou utvářeny na základě společných zájmů, názorů, rodinných vazeb nebo jiných více prospěšných důvodů. J.A. Barnes byl sociolog, který již v roce 1954 používal termín sociální síť. V té době to byl pouze pojem, který sloužil k popisu sociálních struktur spojených pomocí atributů, jako je náboženství, rasa, zájmy, přátelství atd. Jiná definice sociální sítě, která je založena na webových technologiích a zveřejnil ji Boyd a Ellison v roce 2007 v Journal of Computer-Mediater Communucation říká, že sociální síť je služba založená na webových technologiích, která nabízí jedincům používajícím sociální síť tři základní možnosti:

1) Vybudovat v rámci určité sítě veřejný či polo-veřejný profil uživatele

2) Definovat seznam dalších uživatelů v rámci této sítě, se kterými je daný jedinec propojen. Povaha a pojmenování těchto propojení se mohou v různých sítích lišit.

3) Síť umožní uživatelům zobrazit a procházet seznam uživatelů, s nimiž jsou spojeni, a zároveň procházet tyto seznamy i u jiných uživatelů

V druhé generaci internetových služeb neboli webu 2.0, se pojmem sociální síť rozumí každá soustava, která je schopna vytvářet a udržovat síť kontaktů navzájem propojených. Všichni uživatelé sociálních sítí charakterizují svoje vlastnosti, které podle svého uvážení zveřejní pro ostatní uživatele. Lidé se mohou uvnitř každé sítě vyhledávat a shlukovat do skupin. Další z možností je zveřejňování informací, sdílení fotografií, psaní statusů. Mezi největší problém patří bezpečnost a pravdivost údajů uživatelů.[7]

[7] PAVLÍČEK, A. *Nová média a sociální sítě*. 1.vyd. Praha: Oeconomica, 2010. ISBN 978-80-245-1742-1

3.1 SOCIÁLNÍ SÍTĚ

Facebook

Facebook, modrá sociální síť, patří mezi nejrozšířenější na světě. Slouží ke komunikaci uživatelů z celého světa. Facebook nabízí mnoho služeb, které se postupem času vyvíjely ke spokojenosti uživatelů.

Tato sociální síť vznikla 4. února 2004 pod názvem „The Facebook“. Zakladatelem je Mark Zuckerberg, který v době realizace nápadu studoval na Harvardské univerzitě. Během svého studia vytvářel řadu sociálních sítí pro své spolužáky, např. Facemach, Coursematch sítě, kde mohli studenti hodnotit jiné studenty a prohlížet fotografie ostatních. Žádná z nich ale neměla takový úspěch jako Facebook. Původně stránka sloužila k poznání studentů na Harvardu mezi sebou. Stránka se mezi studenty univerzity rozšířila velmi rychle, během jednoho měsíce síť používala více než polovina z nich. V srpnu 2005 byla zakoupena adresa facebook.com a síť se začala šířit i mezi ostatní univerzity v USA, a poté i mezi americké střední školy. Od září 2005 stránky začali používat i studenti škol z celého světa, rok poté ji už používali i nestudující obyvatelé a registrovala se široká veřejnost. [8]

Pro zaregistrování na facebook.com je nutné vyplnit údaje, jako je jméno, příjmení, emailovou adresu nebo telefonní číslo, heslo, datum narození a pohlaví. Podmínkou pro registraci je minimální věk 13 let, nicméně tento údaj není bohužel žádným způsobem kontrolovaný. Síť je možné navštěvovat z počítače nebo pomocí aplikace v telefonu.

Mezi nejzákladnější funkce patří chat, kdy můžeme komunikovat s více uživateli naráz. Slouží k tomu nástroj zvaný Messenger, který lze používat i samostatně, aniž bychom byli připojeni na samotnou síť. Lze si zvolit i skupinovou komunikaci a psát si v určitých skupinách, které si uživatelé sami zvolí. Další služba, která je poskytována, je sdílení fotografií a videí. Na svém profilu může uživatel vkládat odkazy z jiných webových stránek, vytvořit alba fotek pro dobrou přehlednost. Nebo je možné jen

[8] Phillips, S. *A brief history of Facebook* [online]. © 2007 [cit. 2017-02-04]. Dostupné z: http://inventors.about.com/od/fstartinventions/a/Facebook.htm

přidávat momentální myšlenky a psát je do prostoru, který se nazývá zeď. K dispozici je zeď, na které jsou vidět příspěvky všech přátel v seznamu a zeď, na které se nachází jen osobní příspěvky. U každého přípěvku, fotky nebo sdíleného souboru může člověk vyjádřit svůj pocit pomocí reakčních smajlíků nebo napsat komentář.

Další užitečnou funkcí jsou události. Každý uživatel má právo vytvořit událost a zvát na ni své přátele nebo udělat událost veřejnou pro všechny uživatele sociální sítě. Pozvaní pak mají možnost se k pozvánce vyjádřit pomocí tlačítek – mám zájem, zúčastním se nebo ignorovat. Událostí může být cokoli od oslavy narozenin až po divadelní představení. Mezi další přednosti Facebooku patří připomínání narozenin přátel. Na svém profilu si každý uživatel může nastavit jakoukoli úroveň soukromí. Nastaví si, co chce, aby viděli ostatní uživatelé, které má i nemá v přátelích. [9]

Aktuálně na světě existuje více než 1,86 miliardy aktivních uživatelů (údaj z února 2017), což je nárůst oproti minulému roku o 17 %. V Evropě je uživatelů Facebooku zhruba 307 milionů. Nejčastějšími uživateli jsou lidé ve věku 25 až 34 let, kterých je 29,7 %, a více stránku využívají ženy (76 %). Průměrná doba, kterou uživatel stráví svou návštěvou, je 20 minut denně. Za každou jednu sekundu přibude dalších 5 nových profilů. Existuje ovšem až 83 milionů falešných profilů. Svoje profily tu mohou mít i populární osobnosti, a tím komunikovat se svými fanoušky. 50 % procent náctiletých uvádí, že po probuzení se přihlásí na Faceboook, aby zjistili, co se událo nového.[10]

Twitter

Sociální síť vyznačující se modrým opeřencem se zaměřuje pouze na komunikaci uživatelů mezi sebou. Princip je charakterizován jako sms brána, protože příspěvek (tweet) může mít pouze 140 znaků textu. Na Twitteru se nežádá

[9] Bellis, M. *Who Invented Facebook?* [online]. [cit. 2017-02-04]. Dostupné z: http://inventors.about.com/od/fstartinventions/a/Facebook.htm
[10] NOYES, D. *The Top 20 Valuable Facebook Statistics*. [online] ©2017 [cit. 2017-02-04]. Dostupné z: https://zephoria.com/top-15-valuable-facebook-statistics/

o přátelství, pouze se sledují (follow) ostatní uživatelé po kliknutí na tlačítko „sledovat“ u konkrétního uživatele. [11]

Twitter začal fungovat v roce 2006, kdy společnost Odeo hledala nové nápady pro své tvoření. Jack Dorsey přišel na myšlenku posílání krátkých zpráv, které by umožňovalo uživateli komunikovat se skupinou lidí. První půlrok roku 2006 byl ve znamení testování ve firmě Odeo a veřejně byla síť spuštěna až v červenci. V roce 2007 se Twitter stal vlastní společností. [12] V říjnu 2016 měl Twitter zaregistrovaných 317 milionů uživatel, každý den jich je aktivních okolo 100 milionů. Je to výborný nástroj pro získávání nejnovějších informací, které se nejdříve objevují tady, a až poté v médiích. Spousta celebrit a politiků má svůj účet právě zde a velmi aktivně komunikují se svými obdivovateli a sdělují svoje názory.[13]

Instagram

Instagram je mobilní aplikace, která je zaměřena na sdílení fotek mezi uživateli. K základním funkcím patří filtry, kdy před nahráním fotky je možné fotku upravovat do podoby, která je vyhovující. Ostatní uživatelé mohou fotografie hodnotit a komentovat. Na podzim 2016 přibyla další funkce nazývaná Instastories, jejímž účelem je informovat ostatní uživatele, o tom, co daný člověk právě dělá. Fotografie nebo videa jsou zde přístupná pouze 24 hodin, poté se ztratí. Aplikace slouží pouze ke sdílení fotek, videí, neslouží ke komunikaci uživatelů samotných. Příspěvky na Instagramu je možno i popsat, nejvíce se používá znak označující mřížku zvaný „hashtag“. Ten se napíše pod nahraný soubor a napíše se # a za hashtag se začne psát cokoliv, co chce uživatel sdělit. Čím atraktivnější hashtagy jsou pod fotografií, tím více se zatraktivní daný profil a získá více odběratelů, kteří daný profil sledují. Pokud se do vyhledávání zadá dané slovo z hashtagů, tak se uživateli zobrazí všechny příspěvky na

[11] Mazancová, M. *Sociální sítě pro začátečníky: Které vybrat?* [online]. ©2011 [cit. 2016-02-04]. Dostupné z: http://www.internetprovsechny.cz/socialni-site-pro-zacatecniky-ktere-vybrat/
[12] Neznámý, *The History of Twitter* [online]. [cit. 2017-02-04]. Dostupné z: http://profilerehab.com/twitter-help/history_of_twitter
[13] SMITH, C., *350+ Amazing Twitter statistics and facts (November 2016)* [online]. ©2014 [cit.2016-02-04]. Dostupné z: http://expandedramblings.com/index.php/march-2013-by-the-numbers-a-few-amazing-twitter-stats/

Instagramu s daný slovem. Této vlastnosti hodně využívají firmy pro své reklamní kampaně buď na svých profilech nebo prostřednictvím populárních lidí. [14]

Aplikace byla spuštěna 6. října 2010 pouze pro uživatele operačního systému Apple, dnes je již dostupná pro všechny uživatele. Instagram se začal rychle šířit a narůstal počet lidí, kteří ho využívali. V dubnu roku 2012 koupil Instagram Mark Zuckerberg, zakladatel sítě Facebook, za jednu miliardu dolarů. Tím se rozšířilo působení a uživatelé mohou nahrát své fotografie současně na Facebook i Instagram. Momentálně je počet aktivních uživatelů za měsíc zhruba 150 milionů lidí z celého světa a za den se nahraje 55 milionů nových fotografií. [15] K vytvoření profilu v aplikaci stačí uložit aplikaci do mobilního zařízení a mít založený účet na již zmiňovaném Facebooku nebo případně účet založit přes emailovou adresu. [16]

Google+

Google+ je sociální síť od společnosti Google, má podobný účel a charakter jako Facebook. Sdružuje totiž uživatele podle určitých skupin, které nazývá kruhy. Všechny nové přátele, které si člověk přidá, musí zařadit do určitého kruhu – rodina, škola, práce atd. Potom už stačí jen sdílet nějakou informaci, fotografii, odkazy nebo videa na svém profilu a vybrat si, s kterým kruhem přátel bude informaci sdílet. V kruhách lze mít i známé osobnosti. I zde je možnost vyjádřit svůj názor k vloženým příspěvkům, a to tlačítkem "To se mi líbí" nebo „+1". Síť je propojena s ostatními službami a aplikacemi společnosti Google.

Stránka byla spuštěna 28. června 2011 jako testovací provoz a oficiální plné spuštění proběhlo v listopadu téhož roku. Již po čtyřech týdnech provozu měl Google 125 milionů uživatelů a čísla stále stoupají.

[14] Máťa, *Co je instagram* [online] ©2015 [cit.2017-02-05]. Dostupné z: https://www.cestujsnadno.cz/co-je-instagram/
[15] WARCHAR, P., *Jak vznikl Instagram? Od nuly až k Facebooku* [online] ©2005 [cit.2016-02-05] Dostupné z: http://www.instagram.cz/jak-vznikl-instagram-od-nuly-az-k-facebooku/362
[16] Instagram, *Instagram* [online] [cit.2017-02-05] Dostupné z: https://help.instagram.com/182492381886913

Další sociální sítě

Last.fm je sociální síť, která se specializuje na hudební videa a hudbu. S ostatními uživateli tu lze sdílet hudbu, kterou konkrétní člověk poslouchá. Stránka sama také doporučuje hudební novinky, které by neměly uživateli uniknout. Můžete se zde dočíst vše o novinkách v hudbě nebo zdarma stahovat skladby. Nedílnou součástí sítě jsou žebříčky oblíbenosti a kategorie třídění hudby. Mezi další orientovanou sociální síť na hudbu je Songkick, která je zaměřena na fanoušky koncertů a festivalů. Uživatelé zde naleznou také informace o plánovaných akcích a hodnocení proběhlých akcí od ostatních uživatelů.

Svůj rodokmen si mohou uživatelé vytvořit na stránkách Geni.com nebo MyHeritage. Mimo jiné je zde možné sdílet obrázky a videa nebo si s dalšími členy rodiny posílat vzkazy. MyHeritage má navíc i funkci na rozpoznání obličeje, takže člověk může podle fotografií zjistit, komu z rodiny je nejvíce podobný.

České sociální sítě

V českých podmínkách bylo vytvořeno několik sociálních sítí, které jsou hodně využívány veřejností. I přesto, že jsou pouze pro české uživatele, mají svoji popularitu. Spolužáci.cz je síť pro snadnou komunikaci spolužáků ve třídách, možnost sdílet vzkazy, fotografie nebo dokumenty. Pro přihlášení je nutné mít emailovou adresu na portále Seznam.cz. Podobně funguje i síť jménem Lidé.cz. Zde lidé navazují kontakty napříč pohlavími a věkovými kategoriemi, bez ohledu na to, z jaké části naší republiky pochází. Stejně jako Spolužáci.cz patří i tato síť portálu Seznam.cz,. Server nabízí přidávat na svůj osobní profil fotografie, mít svůj vlastní fotopříběh, zasílat uživatelům zprávy nebo diskutovat s ostatními.

Jako další sítě lze jmenovat server Ukažse.cz, který slouží jako fotoseznamka, a zároveň uživatelé mohou hrát i hry. Mnohem oblíbenější je Libímseti.cz, kde se uživatelé navzájem hodnotí, kdo se komu líbí.[17]

[17] Kubeš, R. *Sociální sítě nejsou jen Facebook. Podívejte se i na ty české* [online]. 2009 [cit. 2017-02-27]. Dostupné z: http://technet.idnes.cz/socialni-site-nejsou-jen-facebook-podivejte-se-i-na-ty-ceske-p4e-/sw_internet.aspx?c=A091017_234210_tec_reportaze_vse

3.2 BEZPEČNOST NA SOCIÁLNÍCH SÍTÍCH

Internet nepatří nikomu, a proto může být z pohledu uživatele anonymní, bohužel tomu tak ale není. Z hlediska zákonodárství je toto území na sociálních sítích vymezeno jurisdikcí. Na prvním místě je zajistit citlivé informace uživatelů, které se dostávají na internet, při registracích do sítí. Jsou to především jméno, příjmení, pohlaví, email, datum narození. Tyto údaje nikdo neověřuje. V podmínkách je většinou pouze minimální věk uživatele, který také není kontrolován. Tyto údaje ověří pouze samotný uživatel, který údaje zadal, a to většinou přes emailovou adresu. Na adresu, kterou budoucí uživatel zadal při registraci, přijde potvrzovací odkaz, na nějž stačí pouze kliknout, a profil je dokončen. Všechny tyto údaje mohou být tedy smyšlené.[18]

Při užívání sociálních sítí je možnost si nastavit své soukromí. V praxi to znamená, že uživatel na svůj profil vyplní datum narození, číslo mobilního telefonu, pracovní místo, náboženské vyznání, bydliště apod., a poté si může zvolit, kdo údaje uvidí. Mezi možnosti nastavení soukromí patří, že údaje uvidí pouze uživatelovi přátelé, přátelé přátel nebo všichni uživatelé sítě. Proto je potřeba si důkladně rozmyslet, které údaje o sobě zveřejňovat a komu povolit, aby je viděl. Toto nastavení soukromí podporují některé sítě v čele s Facebookem, Twitterem a Googlem+. Je ovšem nutné dávat si pozor, protože některé z těchto údajů jsou citlivé osobní údaje, které upravuje Zákon č. 101/2000 Sb, o ochraně osobních údajů. A podle § 4 písmene a) je *„osobním údajem 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.“*[19] Toto tedy znamená, že i profilová fotografie s adresou, jménem a příjemním je osobním údajem. Sdílením všech těchto informací může uživatel svoji osobu velmi ohrozit, a pokud sociální sítě používá mládež, která buď nemá na sítích co udělat kvůli svému nízkému věku nebo není upozorněna a poučena, může to mít špatné následky.

[18] PAVLÍČEK, A. *Nová média a sociální sítě*. 1.vyd. Praha: Oeconomica,2010. ISBN 978-80-245-1742-1
[19] Zákon č. 101/2000 Sb. ze dne 4. dubna 2000, o ochraně osobních údajů, In: *Sbírka zákonů České republiky*. 2000, Dostupné z: http://zakony-online.cz/?s20&q20=51

Licenční podmínky

Licenční podmínky jsou dokument, který musí schválit každý uživatel sítě při registraci. Pokud je neodsouhlasí, není možné vytvořit daný profil. Tento souhlas je většinou přijat bez důkladného přečtení, což není správné. Podmínky totiž upravují použití dané stránky, zacházení s citlivými údaji uživatele, práva a povinnosti smluvních stran, povinnosti a práva poskytovatele služby. Během užívání se mohou tyto podmínky změnit. Většina sítí má podobné podmínky užívání.

Facebook například změnil podmínky naposledy k 30. lednu 2015 a všichni uživatelé je museli přijmout. V těchto podmínkách se doporučuje, aby si uživatel přečetl veškeré zásady používání dat a pečlivě s nimi nakládal. Pro názornost by bylo dobré na některé z podmínek upozornit. Všichni uživatelé dávají Facebooku právo na veškeré jejich fotografie a videa. Pokud bude uživatel obsah sdílet jako veřejný, tak uděluje povolení všem uživatelům Facebooku, včetně samotného Facebooku, k tomuto obsahu, který se může používat společně s profilovou fotografií, jménem a příjmením. Pokud uživatel bude sdílet nějaké nápady, myšlenky ohledně Facebooku, tak se zříká jakéhokoli honoráře, pokud bude tato připomínka zrealizována. Dále se každý uživatel zavazuje, že nebude šířit viry, škodlivé kódy, nepoužije stránku k nezákonným činnostem, nebude šířit pornografii, nahotu, jakékoli podněty k násilí, diskriminovat ostatní a obtěžovat jiné uživatele. Dále se zavazuje, že se bude k ostatním uživatelům chovat přiměřeně k jejich udanému věku na profilu apod. V případě, že by chtěl některý z uživatelů podat trestní oznámení na společnost Facebook, musí navštívit Spojené státy americké a žalobu podat pouze osobně u soudů v okrese Northern District v Kalifornii. Soud se bude řídit zákony dané v Kalifornii, na zákony jiných států nebude brán zřetel. Dále podmínky Facebooku upravují reklamu následovně: „*Povolujete nám použít vaše jméno, profilovou fotku, obsah a informace ve spojení s komerčním, sponzorovaným nebo souvisejícím obsahem (například značku, která se vám líbí), který poskytujeme nebo zprostředkováváme. To třeba znamená, že nás tímto opravňujete, abychom mohli za poplatek firmám nebo jiným subjektům zobrazovat vaše jméno nebo profilový obrázek s vaším obsahem nebo informacemi, aniž bychom vás museli jakkoli finančně*

odškodnit. Pokud jste pro svůj obsah nebo informace vybrali konkrétní skupinu příjemců, budeme při použití vaši volbu respektovat.“[20]

3.3 HROZBY NA SOCIÁLNÍCH SÍTÍCH

„Kyberprostor (do češtiny přejato z anglického Cyberspace) je označení pro virtuální realitu interaktivního počítačového světa. Laicky řečeno je kyberprostor veškerý Internet jako takový“.[21] V Kyberprostoru se rozvíjí kriminalita se specifickým názvem kyberkriminalita, tj. termín pro trestné činy, které se odehrávají v kyberprostoru. Nejčastěji jsou kriminalitou postiženy bankovní účty a sociální sítě.

Kyberzločinci své chování činí z různých důvodů (rozchod, vyhazov z práce, msta apod.). Dnešní doba je doba počítačů. Každý druhý jedinec na světě vlastní počítač a připojení k internetu, čímž zanechá na internetu svou stopu. Proto je tak jednoduché se dopustit kyberzločinu a případů neustále přibývá. Mezi specifické případy kyberkriminality patří a pro účely tématu bakalářské práce jsou: kybergrooming, kyberšikana, kyberstalking a kyberterosismus.[22] Další specifickým nebezpečím jsou sexting.

Kyberšikana

Kyberšikana je velký problém, který nejvíce postihuje dětské kolektivy a rychle se šíří ve školách. Kyberšikana se vyznačuje tím, že k ní dochází přes komunikační a informační technologie pomocí počítačů a mobilních telefonů. Napomáhají k tomu nejvíce sociální sítě. Kyberšikana má za účel stejné věci jako klasická šikana, tzn. ublížit a ponížit, ale používá k tomu jiné prostředky. Oběť se nemusí s agresorem vůbec setkat.

---

[20] *FACEBOOK* [online] © 2017 [cit.2017-02-11] Dostupné z: https://www.facebook.com/legal/terms/update
[21] *Kyberprostor*. Správa sítě [online]. ©2016 [cit. 2017-02-26]. Dostupné z: http://www.spravasite.eu/kyberprostor/
[22] *Kyberkriminalita*. Správa sítě [online]. [cit. 2017-02-26]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx

Mezi nejzákladnější znaky kyberšikany patří anonymita agresorů, ti se tudíž méně bojí dopadení. Útok může být časově neomezený po celých 24 hodin, stačí pouze připojení k internetu. Obětí se může stát kdokoli, roli tu nehraje fyzická a psychická vyspělost jedince. Tato forma šikany je těžko zjistitelná pro okolí postiženého – nejsou žádné viditelné příznaky. Pomocí internetu se dá oslovit široká veřejnost a informace jsou lehce a rychle šířitelné. Proto tyto útoky nevyžadují tolik úsilí, ale lze jimi více ublížit než klasickou šikanou. Agresor může rozesílat podvodné zprávy, upravené fotografie nebo videa, komentovat příspěvky svých obětí na sociálních sítích. Toto může trvat i několik měsíců než se dopadne pachatel, protože profil agresora může být falešný. [23]

Kyberstalking

Patří mezi nejnebezpečnější kyberkriminální zločiny. Stalking v překladu znamená lov nebo pronásledování, jedinec který se tomuto zločinu věnuje se nazývá kyberstalker. Ti se snaží různými systematickými technikami a způsoby dlouhodobě psychicky útočit na svoji vyhlídnutou oběť. Většinou to bývají osamělí a zoufalí lidé, kteří jsou mnohdy fascinovaní svými oběťmi. Mohou trpět duševní poruchou, jako jsou paranoia nebo schizofrenie. Tyto nemoci bývají hlavní příčinou, proč se lidé ke kyberstalkingu uchylují. Navzdory tomu bývají tito jedinci velmi inteligentní a své chování jsou schopni velmi dobře skrýt.[24]

Mezi základní projevy nebezpečného stalkingu patří opakované a dlouhodobé pokusy o kontaktování pomocí veškerých nástrojů na internetu. Ze začátku může být posílaný obsah neškodný a příjemný. S postupem času začnou být zprávy urážející a oběti začnou mít strach. V rámci snahy o kontakt je využíván i pocit viny. V dalším případě stalker demonstruje svoji moc a sílu tím, že obětem vyhrožuje a vyvolává pocit strachu a obav o sebe či jeho blízké tak, že píše oběti zprávy typu: vím, kde bydlíš, vidím tě, co máš na sobě….). Patří sem fyzické pronásledování v reálném světě (cesta

[23] *CO JE TO KYBERŠIKANA A JAK SE PROJEVUJE? Http://www.bezpecne-online.cz* [online]. [cit. 2017-02-25]. Dostupné z: http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybersikana-a-jak-se-projevuje.html

[24] *Kyberstalking*. Správa sítě [online]. ©2006 [cit. 2017-02-25]. Dostupné z: http://www.sprava-site.eu/kyberstalking/

z/do práce, na nákup, čeká na oběť před domem apod.). Výjimku netvoří ani vyhrožování násilím nebo smrtí. Pronásledovatel se zcela snaží kontrolovat život oběti. Pronásledovaná oběť může být v nejhorším případě i obětí sexuálně motivované vraždy. Mezi méně nebezpečné varianty kyberstalkingu patří očernění oběti na internetu šířením nepravdivých informací o okolí oběti (v práci, v okolí bydliště). Projevuje se to tím, že si útočník vytvoří falešný profil/internetovou stránku a pomocí těchto nástrojů šíří nepravdivé informace ve snaze snížit důvěryhodnost oběti.[25]

Kybergrooming

Kybergrooming je pojem, který označuje chování pachatele, jenž si na internetu vytipuje svoji oběť a snaží se získat její důvěru tím, že si buduje blízký vztah za účelem vylákat oběť na osobní schůzku, kde je oběť zneužita.

Nejsnadněji se do této situace dostávají děti a mladiství, protože se cítí osaměle, vyhledávají na internetu kamarády, a tak je snadné získat jejich důvěru pomocí dobře zvolených slov prostřednictvím falešného profilu. Pachatelé zjišťují od obětí jejich adresu, telefonní číslo, emaily, s kým bydlí, zda mají sourozence apod. Zároveň se pachatelé velmi často vydávají za někoho jiného. Pokud se snaží vylákat například malého chlapce, tak se sami vydávají za podobně starého chlapce se stejnými zálibami. U starších dětí se pak vydávají za podobně staré kamarády, většinou se to týká dívek, které hledají první lásky. Hlavním rysem chování je trpělivost, pachatelé udržují kontakt dlouhou dobu. Pevně si budují již výše zmíněnou důvěru, tu získají i malými dárky. Součástí je i vydírání. Od obětí pachatel často získává intimní fotografie, které jsou předmětem vydírání, a oběť po té udělá cokoli, co útočník vyžaduje. Do tohoto spadá i opakované osobní setkání, kde pachatel oběť zneužívá.[26]

[25] *Co je to stalking a cyberstalking*. E- bezpečí [online]. ©2008 [cit. 2017-02-25]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/stalking-a-kyberstalking/66-23
[26] *CO JE TO KYBERGROOMING?*. E- bezpečí [online]. [cit. 2017-02-25]. Dostupné z: http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybergrooming.html

Sexting

Sexting je chování, kdy důvěřiví uživatelé internetu posílají nebo sdílení svoje intimní materiály a následně jsou těmito materiály vydíráni. Je to jeden z nejrozšířenějších jevů v rámci komunikace na internetu u mladých lidí. Ti se buď chtějí pochlubit, nebo sdílet fotografie se svými současnými partnery, případně jsou z nich vylákány výměnou za pachatelovu fotografii, která ovšem nemusí k příjemci nikdy dorazit nebo je falešná.[27]

Hoax

Pojem Hoax je pro mystifikující a falešnou zprávu, nespadá do trestných činů. Hoax se často šíří pomocí emailové komunikace, jako tzv. řetězový email. Nejrychlejší způsob šíření je však přes sociální sítě pomocí sdílení informace. Hoax může mít v sobě škodlivý program, případně může obsahovat vir. Nejvíce tím trpí uživatel, u kterého to může mít dopad na jeho psychickou stránku. Falešné zprávy totiž mohou způsobit paniku veřejnosti, ať už se jedná o smrt celebrity, teroristický útok na jejich zemi apod.[28]

[27] Letochová,K.: *Sexting aneb Černobílá budoucnost*. E- bezpečí [online]. ©2013 [cit. 2017-02-26]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/sexting/601-sexting-cernobilabudoucnost
[28] *Hoax*. Správa sítě [online]. ©2016 [cit. 2017-02-26]. Dostupné z: http://www.sprava-site.eu/hoax/

4 INTERNETOVÉ BANKOVNICTVÍ: HROZBY A BEZPEČNOST

V České republice jako první banka, která chtěla provozovat internetové bankovnictví, byla Rodinná záložna. Bylo to v polovině 90. let 20. století, ta ovšem zkrachovala. Poté nápad převzala Družstevní záložna Fio (dnešní Fio banka) a začala nabízet klientům internetové bankovnictví. 4. května 1998 začala na českém trhu působit Expandia Bank, ta klientům nabízela plné ovládání jejich účtů pomocí internetu.[29]

Internetové bankovnictví patří do přímého bankovnictví – další odvětví jsou telefonní, mobilní a domácí bankovnictví. Pro používání internetového bankovnictví stačí mít pouze připojení na internet a internetový prohlížeč v počítači (na rozdíl od homebankingu, kde je potřeba nainstalovat speciální program). Už i chytré mobilní telefony umožňují použít prohlížeč a připojit se do bankovnictví. Banky mají i přímo k tomuto účelu aplikace. Co vše lze na internetovém bankovnictví ovládat, závisí na konkrétní bance. Ovládání účtu spočívá v přístupu na účet, kontrole stavu účtu, měnění a rušení trvalých příkazů, posílání plateb apod. Některá bankovnictví umí úplně nahradit schůzku v bance a vše zadat přes bankovní operace z domova.[30]

Prostředí internetu nemusí být vždy bezpečné, proto se banky snaží maximálně ochraňovat přenášené údaje a údaje klientů. Banky používají následující bezpečnostní prvky:

Autentizační kalkulátor – má čtyři podobné druhy, automaticky vygenerovaný kód po otevření, zadání PIN kódu a následné zobrazení vygenerovaného kódu, PIN kód a detailní data platby a čtvrtý kalkulátor, který pracuje s debetní čipovou kartou, požaduje PIN i emaily platby.

---

[29] *Internetové bankovnictví* [online]. [cit. 2017-03-02]. http://www.mesec.cz/bankovni-ucty/prime-bankovnictvi/internetove-bankovnictvi/pruvodce/

[30] *Přímé bankovnictví* [online]. [cit. 2017-03-02]. Dostupné z: http://www.mesec.cz/bankovni-ucty/prime-bankovnictvi/internetove-bankovnictvi/pruvodce/prime-bankovnictvi-2/

Autentizační SMS – Tento způsob funguje pro potvrzení platby. Na mobilní telefon uživatele přijde autentizační SMS kód, který se vlastnoručně napíše při potvrzení platby.

Autentizační SMS – šifrovaná sms – Pro potvrzení je také zaslána SMS, která je šifrovaná. Také se ručně dopíše do příslušného pole, ale pro tuto funkci je nutné mít SIM kartu podporující bankovní operace.

Podpisový certifikát – Operace na internetu se stvrzujícím podpisovým certifikátem, který je uložen v počítači. Je to heslem chráněný soubor, bývá to USB, CD, DVD apod.

Podpisový certifikát na čipové nebo optické kartě – je kombinace podpisového certifikátu a čipové nebo optické karty, kdy musí být podpisový certifikát na dané kartě. Jiným způsobem nelze bankovní operaci uskutečnit.

Mezi méně časté způsob patří TAN kódy, kdy banka zašle uživateli kód, který je unikátní bývá šesti místný, ten se potvrdí při bankovní operaci.[31]

4.1 HROZBY A BEZPEČNOST

Sociální inženýrství je v internetovém prostředí název pro styl psychologicky vedené manipulace. Manipulace má za úkol z lidí získat osobní informace, které jsou později různým způsobem zneužity. Tento pojem se používá i pro jiné manipulace, ale v případě internetu se jedná hlavně o napadení počítačů, tabletů, mobilních telefonů a jiné.

V kyberprostoru se za sociální inženýrství považují veškeré metody, které přesvědčují oběti o daném stupni důvěry pro úspěšné završení předem připraveného a promyšleného kyberkriminálního prostoru. Jedinci, kteří se věnují sociálnímu inženýrství, jsou zdatní profesionálové v umění klamu lidí. Jeden

[31] *Internetové bankovnictví* [online]. [cit. 2017-03-02]. http://www.mesec.cz/bankovni-ucty/prime-bankovnictvi/internetove-bankovnictvi/pruvodce/

z nejznámějších
a nejslavnější hackerů je Kevin Mitnick. Nejznámější techniky sociálního inženýrství jsou: pharming, phisning, vishing, pretexting a Evil Twin.[32]

Pretexting

Je označování pro vytvořený smyšlený scénář, který má přesvědčit oběť k dobrovolnému vydání informací, které chce daný hacker získat. Jedná se o významnou část sociálního inženýrství, protože zločinci tuto techniku musí dokonale ovládat. V praxi se využívá hojně u kyberzločinů, kde se pachatelé vydávají za jiného člověka. Je to v metodách podvodných telefonátů nebo vishingu, ale také u kybergroomingu.[33]

Phishing

Slovo phishing je složeno ze slov password harvesting fishing a doslovný překlad znamená sběr hesel rybařením. Tak jsou označovány podvodné emailové zprávy, které mají vypadat jako emaily odeslané uživatelům bank. Sdělení bývá napsáno v angličtině nebo česky s pravopisnými chybami. Email obsahuje odkaz na propojení s falešnými stránkami bank a vyzývá uživatele k zadání nebo potvrzení osobních bankovních údajů. Tato zpráva může vypadat i jako email s informací o neproběhnuté platbě nebo průzkumu klientské spokojenosti. Cílem je vždy získat informace k přihlášení do internetového bankovnictví, PIN kódu platebních karet nebo další informace důvěrným informacím, které jsou pak zneužity. Phishing není cílený jen na jednu konkrétní osobu, ale je rozesílán velkému množství uživatelů a pachatelé pouze čekají, kdo své informace sdělí.

Pokud uživateli přijde tento podvodný email, tak by na něj neměl žádným způsobem reagovat, ale ihned ho smazat. Je dobré informovat i svoji banku, že tato podvodná

[32] Sociální inženýrství. *Správa sítě: slovník pojmů* [online]. ©2016 [cit. 2017-03-08]. Dostupné z: http://www.sprava-site.eu/socialni-inzenyrstvi/
[33] Pretexting. *Správa sítě: slovník pojmů* [online]. ©2016 [cit. 2017-03-08]. Dostupné z: http://www.sprava-site.eu/pretexting/

zpráva přišla, a nikdy neklikat na odkazy uvnitř emailu. Pokud tak již bylo učiněno, tak je potřeba okamžitě zablokovat kreditní karty i internetové bankovnictví. [34]

Evil Twin

Evil Twin můžeme přeložit do češtiny jako zlé dvojče. Pro kybernetický zločin je to druh specifické phishingové metody, ale na rozdíl od klasického phishingu je Evil Twin zaměřen na emailové schránky jednotlivých uživatelů. U nich se snaží získat hesla, přístupové údaje nebo infikovat operační systém daného přístroje. Jde mu o vytvoření falešné bezdrátové sítě a podvodného přístupového bodu.

V běžném životě to znamená, že se jedinec připojí k padělanému internetovému připojení na veřejném místě (např. kavárna, letiště, hotel atd.). Tvůrce tohoto útoku snadno uživatele rozpozná a zmapuje jeho činnost a zachytne důležitá osobní data a informace. U této techniky je nejvíce škodlivé to, že uživatel nemá tušení, že se stal obětí útoku a daný útok rozpozná, až když už je pozdě. To znamená až v případě, kdy mu byla způsobena nějaká újma.[35]

Pharming

Další způsob útoku, který využívá počítačové programy, které při pokusu o přihlášení do internetového bankovnictví uživatele přesměrují na podvodné internetové stránky, které jsou pouze napodobeninou skutečných. Jakmile klient zadá svoje přihlašovací jméno a heslo, program vše zaznamená a odešle. Poté se do bankovnictví může přihlásit pachatel. Pokud uživatel nemá ještě jiné zabezpečení např. pomocí SMS a nebo klientského certifikátu, tak jsou mu nepozorovaně převedeny peníze z účtu.

Na první pohled se podezřelé internetové stránky poznají podle toho, že se chovají jiným způsobem, než je zvykem. Mohou požadovat po klientech jiné údaje, než

[34] *Internetové bankovnictví* [online]. [cit. 2017-03-05]. Dostupné z: http://www.mesec.cz/bankovni-ucty/prime-bankovnictvi/internetove-bankovnictvi/pruvodce/

[35] Evil Twin. *Správa sítě: slovník pojmů* [online]. ©2016 [cit. 2017-03-08]. Dostupné z: http://www.sprava-site.eu/evil-twin/

standardně požadují. Pokud jste se i přesto přihlásili, tak by mělo následovat rychlé odhlášení a následné kontaktování vaší banky a popsání situace.[36]

Další případy hrozeb internetového bankovnictví - Vishing

Vishing v anglickém jazyce znamená voice phishing tzv. telefonický phishing. Je to podvodná manipulační technika, kdy za pomocí hlasové technologie pachatelé vylákají z lidí čísla bankovních účtů a přístupové údaje. Zločinci se vydávají za zaměstnance bank, aby u lidí vyvolali co nejmenší podezření.

Toto podvodné promyšlené jednání je velmi úspěšná kyberkriminální metoda útoku. Uživatelé se v dnešní době snaží zabezpečit svůj počítač, mobilní telefon a internetové bankovnictví různými antispamy a antivirovými programy. A tím snáze mohou podlehnout telefonnímu hovoru od falešného bankovního úředníka. Nejlépe se těmto útokům zabrání větší obezřetností při telefonních hovorech. Nejlepší metoda je komunikovat v dané bance pouze s jedním člověk, i když toto je v dnešní době velice komplikované.[37]

4.2 ANTIVIROVÉ PROGRAMY

Antivirový program je počítačový software. Je určen k identifikaci, odstranění, snížení počtu virů a jiných škodlivých softwarů (tzn. Malwarů). Malware je program, který je určen k vniknutí do počítače, aby zapříčinil jeho poškození. Při vniknutí zjistí různá data z počítače. Na trhu jich je nepřeberné množství. Úspěšnost ochrany zařízení před hrozbami závisí na tom, jaký antivirový program je používán.[38]

[36] *Phishing a pharming*. Bezpečný internet.cz [online]. [cit. 2017-02-26]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx
[37] Vishing. Správa sítě: slovník pojmů [online]. ©2016 [cit. 2017-03-08]. Dostupné z: http://www.sprava-site.eu/vishing/
[38] *Co je to anti-virový program?: PC viry* [online]. ©2008 [cit. 2017-03-05]. Dostupné z: http://pc-viry.webnode.cz/co-je-to-anti-virovy-program-/

Antivirové programy můžeme rozdělit:

1. **On – demand skenery** – pro případ, kdy systém před použitím nemůžeme spustit standardním způsobem, jelikož je již poškozen.

2. **Jednoúčelové antiviry** – jde o programy, které vznikly a jsou zaměřeny na konkrétní vir, skupinu virů. Vznikají zároveň ke zničení v aktuálním děním.

3. **Antivirové systémy** – Jde o celkovou ochranu počítače, kdy systém má ochránit uživatele před nebezpečným přijímáním přes elektronickou poštu, stažením infikovaných souborů apod.

Antivirový program hledá a kontroluje data na základě virového seznamu. Každým dnem vznikají nové hrozby v podobě nových virů a jejich mutací. Výrobci/vývojáři musí okamžitě reagovat na vývoj situace. Databáze virů je průběžně aktualizována a je uživatelům k dispozici online. Antivirový program sám automaticky kontroluje data v počítači. Uživatel ani nemusí zaznamenat, že program pracuje. Programy také nabízejí funkci skenování souborů na vyžádání, kde si každý může nastavit úroveň kontroly. Každý program musí čelit všem nástrahám dnešní doby, které jdou rychlým krokem kupředu. Proto by se každý uživatel měl mít na pozoru a nespoléhat pouze na antivirový program.[39]

[39] *CHRAŇTE SVŮJ POČÍTAČ*. Antivirové centrum [online]. [cit. 2017-03-05]. Dostupné z: https://www.antivirovecentrum.cz/antiviry.aspx

Srovnání antivirových programů

Tabulka 1: Srovnání antivirových programů

Antivirový program	Počet testů	Úspěšný	Neúspěšný	Procento úspěšnosti
ESET	103	100	3	97,1 %
Microsoft (produkty od firmy)	43	41	2	95,3 %
Norton (Symantec)	66	58	8	87,9 %
TrustPort	42	36	6	85,9 %
BitDefender	69	59	10	85,5 %
Avira	69	56	13	81,2 %
Kaspersky	105	85	20	81,0 %
Sophos	90	72	18	80,0 %
F-Secure	70	53	17	75,7 %
AVG	92	67	25	72,8 %
Avast!	96	69	27	71,9 %
Norman	94	66	28	70,2 %
McAfee	72	49	23	68,1 %

Zdroj[40]

[40] Antivirové centrum. *DLOUHODOBÉ VÝSLEDKY V TESTECH SPOLEČNOSTI VIRUS BULLETIN* [online]. © 1.2.2017 [cit. 2017-04-03]. Dostupné z: https://www.antivirovecentrum.cz/aktuality/srovnani-antiviru.aspx

PRAKTICKÁ ČÁST

5 DOTAZNÍKOVÉ ŠETŘENÍ

Tato kapitola je zaměřena na analýzu a zhodnocení výzkumu, čímž je chování uživatelů na internetu. Byl sestaven dotazník, na základě kterého bylo prováděno online šetření dané problematiky. Dotazník byl šířen mezi respondenty na sociálních sítích, emailem a také byl k dispozici na webové stránce vyplnto.cz.

5.1 METODOLOGICKÁ VÝCHODISKA

Jako základ obsahové analýzy posloužila kritéria, která byla již dřív použita a definována výzkumníky: Michal Kočí, Daniela Šikolová a Marek Waldemar.

1. Citlivost osobních údajů.
2. Zjišťování základních údajů.
3. Analýza nastavení sociálních sítí.
4. Analýza sdílených informací na sociálních sítích.
5. Analýza bezpečnosti v internetovém bankovnictví.

S výše popsanými kritérii bylo pracováno při sestavování výzkumu.

5.2 OTÁZKY A HYPOTÉZY

Dotazník byl sestavován na základě logické posloupnosti otázek, aby na sebe otázky navazovaly. Dalším kritériem bylo zaujmutí respondenta. Dotazník se skládá z 21 otázek a jedné nepovinné otevřené otázky na závěr. Celkový průměrný čas pro vyplnění byl 00.03:33, respondenti byli ochotni dotazník vyplnit a za pouhých 8 dní se dotazníkového šetření zúčastnilo 154 osob.

První a druhá otázka dotazníku jsou zaměřeny na informace ohledně věku a pohlaví respondenta. Třetí otázka je filtrační. Pokud respondenti odpoví, že nepoužívají sociální

sítě, budou přesměrováni na otázku číslo dvanáct. Také otázka číslo dvanáct je filtrační, pokud bude zodpovězeno ano, tak dotazování pokračuje otázkou číslo 13. Pokud bude odpověď na otázku „ne“, tak bude otázka číslo třináct v dotazování přeskočena.

Stejný princip posloupnosti v dotazování je zvolen od otázky číslo čtrnáct, která se ptá, zda respondent používá internetové bankovnictví. Pokud je zodpovězeno, že ano, tak dotazník pokračuje dále. Pokud je zvoleno „ne“, tak následuje otázka sedmnáct. V otázce číslo osmnáct je opět zvolena filtrace ano – ne. Při zodpovězení záporně je respondent přesměrován na otázku dvacet jedna. Poté následuje nepovinná otevřená otázka, která má zjistit, zda si daní respondenti myslí, že se na internetu chovají zodpovědně. Je jim dán prostor pro vyjádření a popsání jejich chování a názoru.

Hypotéza č. 1: Nejvíce využívají sociální sítě mladší (kolem 20 let) uživatelé internetu.

Hypotéza byla vytvořena na základě dnešního moderního trendy mladistvých v České Republice. Z důvodu, že se na sociálních sítích pohybují mnohem více než jejich rodiče a prarodiče a z tohoto důvodu jsou nejčastějšími oběťmi trestných činů na internetu.

Hypotéza č. 2: Uživatelé sdílejí na sociálních sítích důvěrné informace v domněnce, že jejich data nikdo nemůže zneužít.

Hypotéza byla definována z dlouhodobého pozorování autorky na sociálních sítích. Autorka má v přátelích na sociálních sítích zhruba 900 uživatelů. Nespočet z těchto lidí sdílí na internetu svoji aktuální polohu mimo domov, čímž prozrazují, že jejich obydlí je prázdné. Dále je na jejich profilech patrné, jak vybavená jsou jejich obydlí, proto mohou být snadno obětí loupeže. V jiných případech sdílejí fotografie svých dětí ve školním věku, které jsou poté ohroženy lidmi s různými poruchami osobnosti.

Hypotéza č. 3: Uživatelé na internetu začali být opatrní až ve chvíli, kdy se stali obětí trestného činu nebo zneužití.

Autorka hypotézy předpokládá, že uživatelé, kteří se stanou obětí na internetu, se poté začnou chovat mnohem obezřetněji. Samozřejmě se bere v potaz i to, že se respondenti nemusí přiznat, že se jim taková věc stala, protože se za to stydí.

Hypotéza č. 4: Většina uživatelů internetu má ve svém počítači antivirový program a myslí si, že je to dostatečná ochrana na internetu.

Všechny hypotézy byly tvořeny na základě poznatků z teoretické části. Bylo možno prostudovat mnoho materiálů a zpráv týkajících se používání internetu. Nesmíme opomenout i každodenní informace ohledně negativních zkušeností, kterými jsme přesyceni z médií, a nespočetným varováním, ať jsme neustále na pozoru.

5.3 VÝSLEDKY ŠETŘENÍ A PRŮZKUM SOCIÁLNÍCH SÍTÍ

Tabulka 2: Otázka č. 2

Odpověď	Počet	Lokálně %	Globálně %
21-25 let	88	57,14 %	57,14 %
26-35 let	29	18,83 %	18,83 %
36-45 let	21	13,64 %	13,64 %
16-20 let	8	5,19 %	5,19 %
46-60 let	7	4,55 %	4,55 %
61 let a více	1	0,65 %	0,65 %

Zdroj: Hrušková, K., 2017 (vlastní šetření)

Tabulka 3: Otázka č. 1

Odpověď	Počet	Lokálně %	Globálně %
Žena	101	65,58%	65,58%
Muž	53	34,42%	34,42%

Zdroj: Hrušková, K., 2017 (vlastní šetření)

V rámci vyhotovení dotazníku byly první dvě otázky shrnuty do jedné části. Otázky byly zjišťovací. Z celkového počtu 154 dotazovaných bylo 101 žen (65,58 %), což se dalo předem předkládat, kvůli jejich ochotě pomoci. Nejpočetnější skupina respondentů 88 (57,14 %) je v rozmezí 21-25 let. S velkým odstupem je druhá věková kategorie 26-35 let s pouhými 29 osobami (18,83 %).

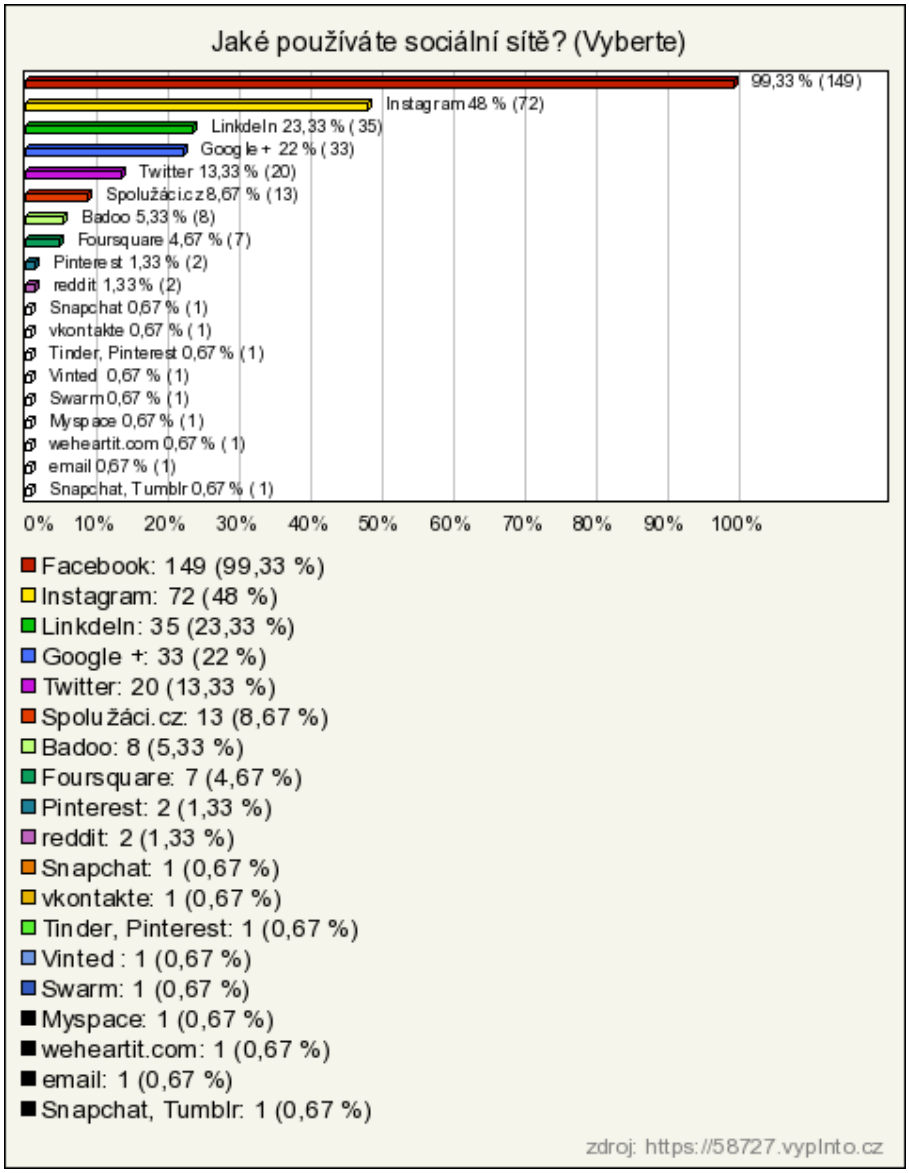
Tabulka 4: Otázka č.3

Odpověď	Počet	Lokálně %	Globálně %
ANO	150	97,4 %	97,4 %
NE	4	2,6 %	2,6 %

Zdroj: Hrušková, K., 2017 (vlastní šetření)

Další částí dotazníkového šetření jsou informace o používání sociálních sítích v otázce číslo 3. Pouze 4 (2,6 %) dotazovaných nepoužívají sociální sítě. Tím se potvrdila hypotéza č. 1, protože nejvíce respondentů bylo v rozmezí 21-25 let 57,14 %, další související skupinou je věková kategorie 16 - 20 let, těchto respondentů je 8 (5,19 %). Tyto skupiny dohromady dávají více než 60 % z celkového vzorku dotazovaných.

Graf 1: Otázka č. 4



Zdroj: Hrušková, K., 2017 (vlastní šetření)

V otázce číslo čtyři se potvrdily, již uvedené údaje v kapitole 3.1, kde se uvádí, že nejvíce rozšíření a používané sociální sítě jsou Facebook, Instagram, Twitter a Google +. Z dotazníkové šetření vyplývá fakt, že nejrozšířenější česká sociální sítě jsou spolužáci.cz i přesto ji používá pouze 13 (8,67 %) dotázaných s porovnání užíváním zahraničních sítí - Facebook 149 (99,33 %) respondentů. Celkem na otázku odpovídalo 150 respondentů a z tohoto počtu pouze jeden respondent nepoužívá sociální síť Facebook.

Tabulka 5: Otázka č. 5

Odpověď	Počet	Lokálně %	Globálně %
Několikrát za den	135	90 %	87,66 %
Jednou denně	9	6 %	5,84 %
4x do týdne	6	4 %	3,9 %

Zdroj: Hrušková, K., 2017 (vlastní šetření)

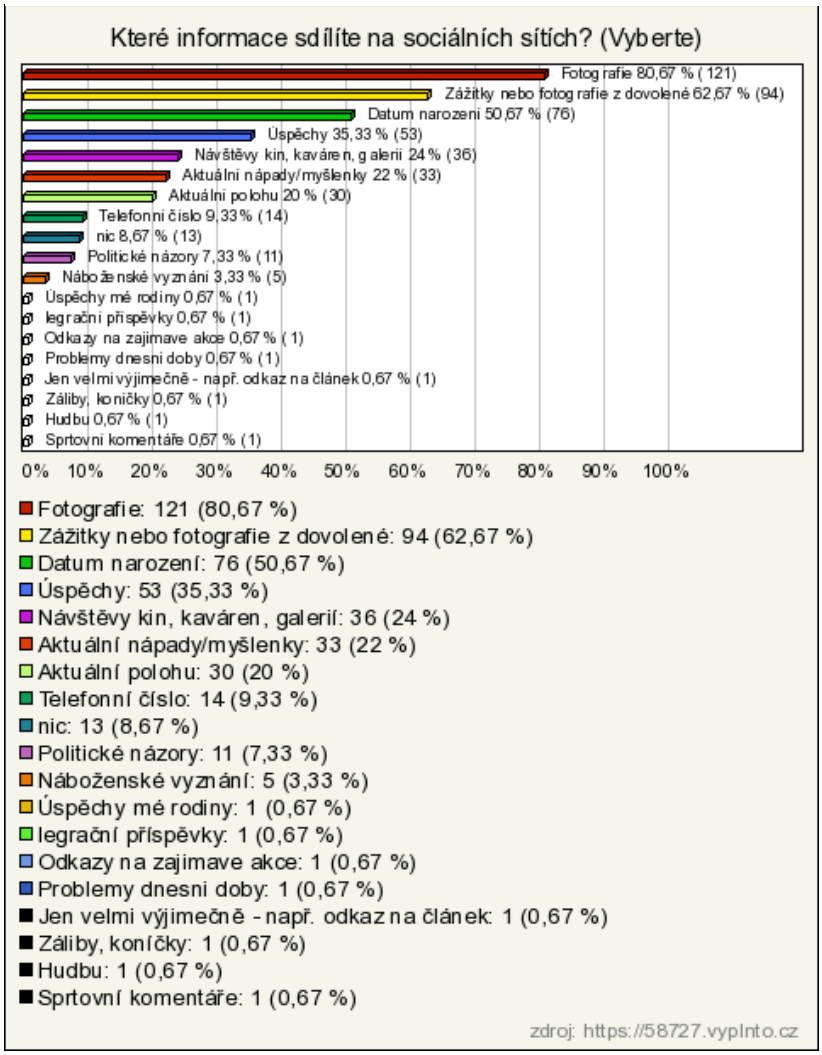
Tabulka 6: Otázka č. 7

Odpověď	Počet	Lokálně %	Globálně %
Pouze mnou schválení	93	62 %	60,39 %
Individuální nastavení	34	22,67 %	22, 08 %
Všichni uživatelé	20	13,33 %	12, 99 %
Nezáleží mi na tom	3	2 %	1, 95 %

Zdroj: Hrušková, K., 2017 (vlastní šetření)

V otázce č. 5 se výzkum zabývá, jak často uživatelé navštěvují sociální sítě a v otázce č. 7 kdo, může vidět jejich příspěvky. 135 (90 %) dotázaných používá sociální sítě několikrát denně, což je velké číslo. Pouze 13 (10 %) respondentů sítě navštěvuje jednou denně nebo několikrát do týdne. S tím souvisí otázka č. 7. Více jak polovina uživatelů má své účty zabezpečeny, tak že jejich sdílený obsah můžou vidět pouze uživatelé, které si sami schválí. Nebo mají individuální nastavení, což znamená, že mají nějakým způsobem nastaveno soukromí a sami ovládají, kdo může vidět jejich obsah na síti. Celkem 127 lidí (84,67 %) si aspoň nějakým způsobem ochraňuje sdílená data. Pouze 23 (15,33 %) z celkového počtu 150 odpovídajících má svoje profily veřejně otevřené pro všechny uživatele nebo jim nezáleží na tom, kdo jejich obsah vidí.

Graf 2: Otázka č. 6



Zdroj: Hrušková, K., 2017 (vlastní šetření)

V otázce č. 6, která byla pootevřená otázka, si z nabízených možností mohli respondenti vybrat libovolný počet odpovědí. Nebo bylo možné doplnit odpověď pro ně nejvhodnější. Z výzkumu vyplynulo, že nejvíce jsou sdíleny fotografie 121 (80,67 %) na druhém místě jsou zážitky z dovolené 94 (62,67 %) a na třetím místě je datum narození 76 (50,67 %). Níže se objevila odpověď, že 30 (20 %) dotázaných sdílí svoji aktuální polohu. V kapitole 3.2 je uvedeno, co znamená osobní údaj, a v případě, že je sdílena fotografie, datum narození a aktuální polohu, mohou nastat i případná nebezpečí, která z toho plynou. Dále stojí za zmínku, že 11 (7,33 %) lidí sdílí politické názory a 5 (3,33 %) sdílí náboženská vyznání i těchto důvodů mohou být lidé obětí

útoků. Dále 13 (8,67 %) lidí uvedlo, že na sociální sítě nedává žádné příspěvky. Po jednom respondentovi se objevily odpovědi, že lidé sdílí: sportovní komentáře, hudbu, záliby, problémy dnešní doby, odkazy na zajímavé akce, legrační příspěvky a úspěchy rodiny. Tato odpověď potvrzuje hypotézu č. 2, která říká, že uživatelé sdílí důvěrné informace.

Otázka č. 8 měla za úkol zjistit, zda se uživatelé sociální sítí osobně setkali s útoky na jejich osobu nebo jim někdo zneužil jejich osobní údaje. Kladnou odpověď zadalo 24 (16 %) osob. Ostatních 126 (84 %) odpovědělo, že ne.

Tabulka 7: Otázka č. 8

Odpověď	Počet	Lokálně %	Globálně %
NE	126	84 %	81,82 %
ANO	24	16 %	15,58 %

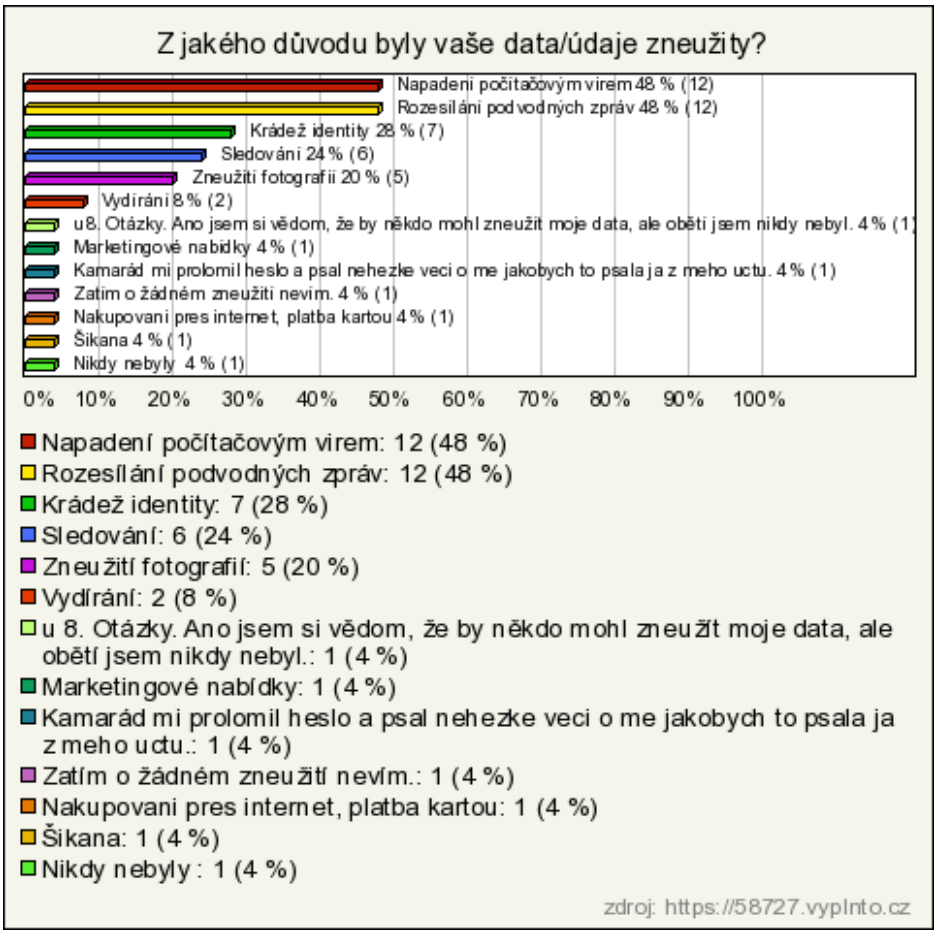
Zdroj: Hrušková, K., 2017 (vlastní šetření)

Tabulka 8: Otázka č. 10

Odpověď	Počet	Lokálně %	Globálně %
ANO	15	62,5 %	9,74 %
NE	9	37,5 %	5,84 %

Zdroj: Hrušková, K., 2017 (vlastní šetření)

Graf 3: Otázka č. 9



Zdroj: Hrušková, K., 2017 (vlastní šetření)

Otázka č. 9 (Z jakého důvodu byly vaše údaje/data zneužity?) a 10 (Změnilo se po této zkušenosti vaše chování na sociálních sítích?) jsou na sebe navazující. Na tuto otázku odpovědělo 24 respondentů, kteří u předešlé otázky zadali odpověď ano. Otázka č. 9 byla polootevřená, respondent si mohl vybrat z více odpovědí, protože respondenti nemuseli čelit pouze jedné hrozbě, případně mohli i odpovědi doplnit.

Nejvíce odpovědí bylo na napadení počítačovým virem a také na rozesílání podvodných zpráv 12 (48 %). Krádež identity přiznalo 7 (28 %), poté následuje odpověď sledování 6 (24 %), zneužití fotografií odpovědělo 6 respondentů a k vydírání se přihlásili 2 respondenti. Dále následovaly odpovědi, že odpovídající nebyli obětí, ale jsou si vědomi nebezpečí. V otázce č. 11 je dotazováno, zda těchto 24 respondentů po této zkušenosti nějakým způsobem upravilo svoje jednání na sociálních sítích.

Kladnou odpověď dalo 15 (62,5 %) respondentů, a tito pokračovali na povinnou otevřenou otázku, kde jsou dotazováni, jakým způsobem se chovají jinak.

Nejčastější odpovědí je, pravidelná změna heslo na sociálních sítích a obezřetnější chování při chování, kde jsou vystaveni virům a podvodných zprávám. Více si zabezpečují svůj účet a silným heslem a individuálním nastavením. Dále nevkládají žádné osobní údaje o sobě a přátelích. A pokud již něco sdílí, tak to není tak často, jak dříve. Jako příklad autor uvádí vybrané odpovědi dotazovaných. Vybraná odpověď:

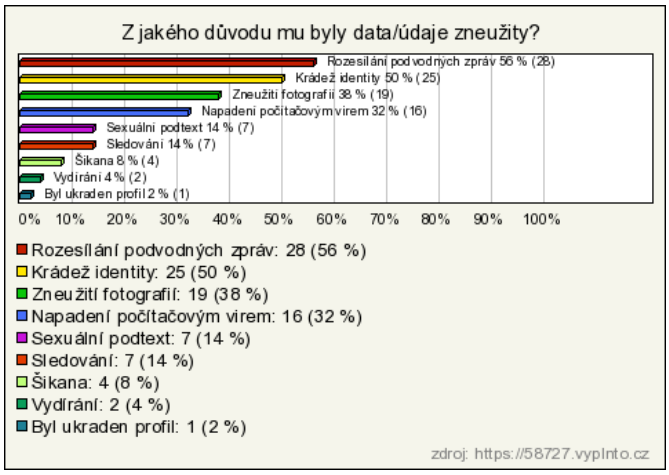
1. *„Silnejsi heslo a blokuji lidi vic i kdyz treba jen dávají moc fotek. Je to otravne. Nebo kdyz tam o sobe nic nemají-podezrele. Nechci lidi co neznám a i z lidi co znam si vybiram.“*
2. *„Nedůvěřuji všem zprávám co mi přijdou a své soukromí chráním nastavením a mám na profilu spoustu lidí, kteří mě obtěžovali svým schováním nebo obsahem a proto jsem je zablokovala, aby mě už nikdy nemohli kontaktovat.“*
3. *„Některé informace jsem ze sociálních sítí odstranil, a nastavil jsem na různéuživatele specifická práva dostupnosti osobních informací (a obsahu celkově“*
4. *„Nevkladam zadne osobni udaje, prispevky o me a mych pratelich.“*
5. *„Nezveřejňují informace tak často, vlastně už velmi málo.“*
6. *„Změna hesla, větší zabezpečení“*
7. *„Přidávám minimálně příspěvků a měním si častěji heslo.“*
8. *„Vetsi obezřetnost“*

Tabulka 9: Otázka č. 12

Odpověď	Počet	Lokálně %	Globálně %
NE	104	67,53 %	67,53 %
ANO	50	32,47 %	32,47 %

Zdroj: Hrušková, K., 2017 (vlastní šetření)

Graf 4: Otázka č. 13



Zdroj: Hrušková, K., 2017 (vlastní šetření)

Následující otázky 12 a 13 na sobě také navazují. Respondenti byli dotazováni, zda znají někoho ze svého okolí, komu byly zneužity data/osobní údaje. S odpovědí ano jsme se setkali u 50 (32,47 %) dotazovaných. Tito respondenti poté odpovídali na otázku 13, kde jsme se jich ptali z jakého důvodu. Nejvíce odpovědí bylo rozesílání podvodných zpráv 28 (32,47 %), poté následovala krádež indenty 25 (50 %), a na dalším místě bylo zneužití fotografií 19(38%) a napadení počítačovým virem 16 (32 %). Na posledních příčkách v odpovědí se umístily více závažné zkušenosti, jako jsou sexuální podtext a sledování uživatelů obě odpovědi měly po 7 (14 %) odpovědích, za nimi se umístila šikana se 4 (8 %) a poté vydírání 2 (4 %) a pouze jedna odpověď zmiňovala ukradení profilu, což jsou 2 % z celkového počtu.

5.3.1 PRŮZKUM INTERNETOVÉHO BANKOVNICTVÍ A ANTIVIRŮ

Tabulka 10: Otázka č. 14

Odpověď	Počet	Lokálně %	Globálně %
ANO	140	90,91 %	90,91 %
NE	14	9,09 %	9,09 %

Zdroj: Hrušková, K., 2017 (vlastní šetření)

Otázka č. 14 byla filtrační a zabývala se použitím internetového bankovnictví. Z celkového počtu 154 respondentů odpovědělo, že používá internetové bankovnictví 140 (90,91 %). Pouhých 14 (9,09 %) internetového bankovnictví nepoužívá.

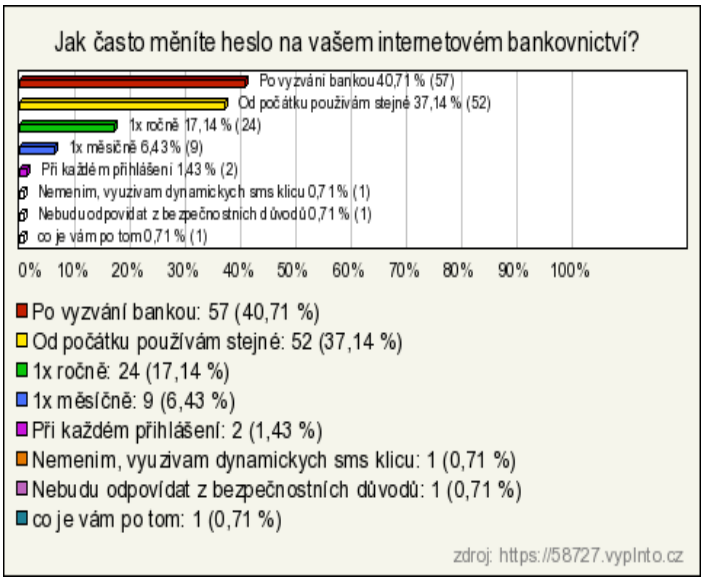
Tabulka 11: Otázka č. 15

Odpověď	Počet	Lokálně %	Globálně %
NE	135	96,43 %	87,66 %
ANO	5	3,57 %	3, 25 %

Zdroj: Hrušková, K., 2017 (vlastní šetření)

Otázka č. 15 zjišťuje, zda byly respondentům zneužity osobní údaje v rámci internetového bankovnictví. Údaje byly zneužity pouze 5 (3,57 %) dotázaným a zbývající část 135 (96,43 %) odpovědělo, že tomu tak nikdy nebylo.

Graf 5: Otázka č. 16



Zdroj: Hrušková, K., 2017 (vlastní šetření)

Otázka č. 16 pojednává o tom, zda uživatelé internetového bankovnictví mění přístupové údaje do svého internetového bankovnictví. Bohužel tyto údaje jsou zkreslené z důvodu, že každá banka používá jiné přihlášení a jiné ověřování do bankovnictví. Někteří uživatelé mohou mít debetní/ čipové karty, jiní přístup pomocí dynamický SMS a nebo pouze přihlašovací jméno a heslo. Proto je pouze tato otázka brána v potaz a není klíčová v celkovém hodnocení výzkumu.

Tabulka 12: Otázka č. 17

Odpověď	Počet	Lokálně %	Globálně %
NE	138	89,61 %	89,61 %
ANO	16	10,39 %	10,39 %

Zdroj: Hrušková, K., 2017 (vlastní šetření)

Otázka č. 17 se dotazuje, zda dotázaní mají ve svém okolí osobu, které byly zneužity údaje z internetového bankovnictví. Na tuto otázku odpovídal celkový počet respondentů, tedy 154. Odpověď ano, zvolilo 16 (10,39 %) dotázaných. Odpověď ne zvolilo 138 (89,61 %). Kladná odpověď má nižší číslo než totožná otázka, která se

zabývá sociálními sítěmi. Na sociálních sítích si uživatelé nedovedou představit riziko jejich chování. Ale pokud se jedná o jejich peníze, tak lidé bývají velice opatrní a dávají si velký pozor. I když je internetové bankovnictví mnohem lépe chráněno než sociální sítě.

Tabulka 13: Otázka č. 18

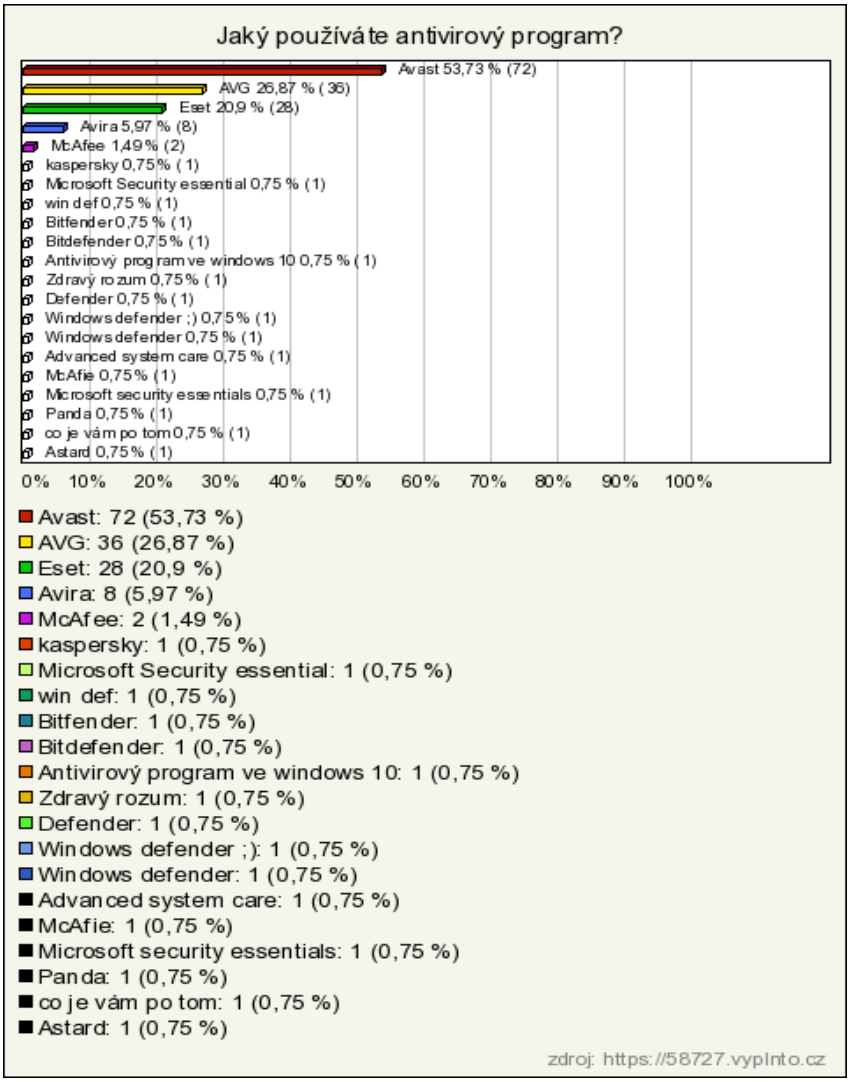
Odpověď	Počet	Lokálně %	Globálně %
ANO	134	87,01 %	87,01 %
NE	20	12, 99 %	12, 99 %

Zdroj: Hrušková, K., 2017 (vlastní šetření)

V otázce č. 18 se zjišťovalo, jestli uživatelé internetu používají i antivirové programy. Zde je jasné převaha odpovědi ano 134 (87,01 %) dotázaných program používání. Pouze 20 (12,99 %) respondentů antivirové programy nepoužívá, v této odpovědi se mohou nacházet i uživatelé operačního systému od firmy Apple (MacOS), která má větší zabezpečení svých přístrojů než ostatní formy a její uživatelé zpravidla nepoužívají žádné antivirové programy.

Na otázku č. 19 odpovídali pouze respondenti, kteří v předešlé otázce odpověděli, že používají antivirový program, tzn., počet 134. Nejvíce osob odpovědělo, že používá program Avast 72 (53,73 %), poté následuje s velkým rozdílem AVG 36 (26,87 %) a na třetím místě je Eset 28 (20,9 %). Poté následují antivirové programy s malým počtem uživatelů 5 a méně. Zajímavé je srovnání s tabulkou z kapitoly 4.2 o antivirových programech, kde je testovaná úspěšnost těchto programů. Nejlépe dopadl program Eset s 97,1 % úspěšností, na druhém místě program od firmy Microsoft 95,3 % a na třetím místě program Norton 87,9 %. V průzkumu programů se ukázalo, že antivirový program od společnosti Windows používá 5 respondentů a ve výzkumu se nenašel žádný uživatel programu Norton.

Graf 6: Otázka č. 19



Zdroj: Hrušková, K., 2017 (vlastní šetření)

Tabulka 14: Otázka č.20

Odpověď	Počet	Lokálně %	Globálně %
NE	89	57,79 %	57,79 %
ANO	65	42,21 %	42,21 %

Zdroj: Hrušková, K., 2017 (vlastní šetření)

Poslední otázka č. 20 z průzkumu byla nepovinná a respondent měl odpovědět na otázku, zda si myslím, že se chová na internetu zodpovědně a vlastními slovy popsat

důvod. Z celkového počtu 154 respondentů dobrovolně odpovědělo 81 což je 52,6 %. V odpovědích je čtrnáct (17,28 %) odpovědí pouze ano a tři odpovědi (3,7 %) ne a 3 (3,7 %) odpovědi snad ano. Ostatní respondenti se rozepsali a jejich tipy odpovědí jsou rozděleny do několika částí a některé zajímavé odpovědi budou převzaty z výzkumu a citovány.

Odpovědi, kde se respondenti vyjádřili, že se určitě chovají zodpovědně a měli různá odůvodnění. Důvody proč se chovají zodpovědně: na internetu nevystupuji, nezapojuji se do diskuzí, nikoho neurážím, využívám internet pouze k získání informací a ke stahování potřebných dat, použití internetu k účelům školy, mám pod kontrolou, co sdílím, pouze se vzdělávám. Tyto odpovědi byly ojedinělé:

1. *„Ano, nejsem hulvat, nedavam informace o tom, ze jsem pryc, kde bydlim, vybaveni bytu, datum narozeni, nesdilim radikalni nazory ci pofiderni obrazky atd.“*
2. *„Ano chovám, nic špatného tam nedělám, jen si čtu či se vzdělávám při aktuálních změnách zákonů“*
3. *„Ano, protoze ho pouzivvam jen pro ucel skoly.“*
4. *„Ano, na internetu nesdílím nic.“*
5. *„ano na nic podezřelého neklikám, nezveřejňuji choulostivé informace“*
6. *„ano - nesdílím osobní informace, bližší fotografie, nepíši moje činnosti, vzdělání, aktivity.. jsem spíše pozorovatel ostatních :)“*
7. *„ano, dávám internetu jen ty informace, které chci, aby někdo viděl (nezneužitelné informace)“*
8. *„Ano, navštěvují pouze ověřené weby s dobrým trafficem.“*
9. *„Ano, nestahuji ani nesleduji porno“*
10. *„Ano, protoze pouzivam ochranu proti spamu, sdilim jen nejnutnejsi informace“*
11. *„Individuální nastavení na sociálních sítích, náročná hesla, navštěvování podezřelých stránek, připojování pouze na známé wifi, slušné vlastní chování“*

V dalším případě, byly odpovědi velmi podobné a často se opakovaly, dotazovaní psali tyto důvody: používání antivirového programu, navštěvování pouze prověření stránek, ochrana soukromí, nesdělování důvěrných informací, řídí se pokyny banky, automaticky si neukládají hesla, nesdílí věci v aktuální čas, dbají na své soukromí, nesdělují svoje vzdělání a činnosti, nesledují porno, nenakupují přes internet, neotvírám podezřelé zprávy na sociálních sítích, sdílení jen nejnutnější informací, použití ochrany proti spamům, použití složitých hesel. Pro názornost je uvedeno několik vybraných. (Pokud odpovědi zazněli podobným způsobem, vždy je uváděna pouze jedna vybraná):

1. *„Ano, nenavštěvuji pochybné stránky, neklikám na pochybné odkazy. Při přihlášení do internetového bankovnictví vždy kontroluji adresu, zda je to skutečně stránka banky. Mám hesla, která obsahují velké, malé znaky i číslice. Asi bych je mohla ale častěji měnit“*
2. *„Ano, nesdilim kde, kdy jsem, k platbam vyuzivam vyhrazeny ucet na kterem je vzdy malo penez, pracuji v macOS- ma lepsi ochranu nez windows*
3. *Ano. Nenavštěvuji weby, na které mě prohlížeč či antivir upozorní jako potenciální riziko.“*
4. *„Ano. Nikomu neznámému nesděluji své jméno, adresu ani telefonní číslo, používám kvalitní antivir a neklikám na každou blbost, která na mě vyběhne.“*
5. *„Ano chovám, jelikož navštěvuji pouze mnou známé internetové stránky, bankovnictví otevírám přes zabezpečný prohlížeč a pokud mi antivirus oznámí, že stránka, na kterou chci vstoupit, je nějaká podezřelá, tak ji v žádném případě neotvírám“.*
6. *„Nezdieľam médiá ani informácie o sebe, o ktorých si myslím, že by mali ostať súkromné. Používam heslá, ktoré nie je možné ľahko rozlúštiť. Čo sa týka antivírusových programov, používam apple, ktorý v skutočnosti žiadny takýto program nepotrebuje. Všetko čo si stiahnem je z obchodu od applu a teda bezpečné. Nenavštevujem stránky, ktoré by mohli byť nebezpečné. To je dôvod, prečo si myslím, že moje správanie sa na internete je bezpečné. Teda aspoň do tej miery, do ktorej je to vôbec možné.“*

7. *„Nesdílím ani nikomu neposílám osobní informace, v některých ohledech, např. internetové bankovnictví, bych ale mohla být opatrnější.“*
8. *„Snažím se chovat zodpovědně, neupozorňovat na sebe, neukládat nikde hesla, nechodím na stránky, které neznám ani emaily které neznám neotvírám. Řekla bych ale, že když se nějaký hacker na někoho cíleně zaměří, tak tomu dotyčnému nepomůže stejně nic byť by měl sebelepší ochranu.“*
9. *„Ano myslím. Jsem slušně vychovaný a rozumný člověk, který sociální sítě moc neřeší a nejsou pro něho životně důležité.“*
10. *„Ano chovám. Nikdy se nezapojuji do žádných diskuzí, tím pádem nikoho a nic neurážím. Využívám internet pouze k získání informací a ke stažení potřebných dat.“*
11. *„Ano, na internetové bankovnictví využívám chráněné okno Esetu, a na sociálních sítích osobnější příspěvky jako osobní údaje či fotografie dávám k nahlédnutí pouze přátelům etc".“*
12. *„Ano, nezveřejňuji osobní informace, fotky a jiná média. Nenakupuji po internetu a dávám si pozor na to, kdo může vidět moje příspěvky.“*
13. *„Ano, nesdilim sve osobni informace a neprihlasuji se na internetove bankovnictvi na neznamych siti, ale samozrejme bezpecneji se lze vzdy chovat vice.“*
14. *„Ano. Nikomu neznámému nesděluji své jméno, adresu ani telefonní číslo, používám kvalitní antivir a neklikám na každou blbost, která na mě vyběhne.“*
15. *„protoze sem technicky znaly a umim s techniku delat (specialne se softwarem)“*
16. *„Relativně ano. Vyhýbám se pofidérnímu obsahu (pochybné stránky, odkazy, spam v e-mailu, warez), nesdílím, nepostuji o sobě zbytečně soukromé údaje - snažím se nezanechávat po sobě elektronickou stopu. Využívám možností zabezpečení soukromí.“*

Třetí skupina odpovědí byly odpovědi, kde dotazovaní napsali, že se nechovají zodpovědně. Těchto odpovědí bylo nejméně. Pokud vezmete v potaz 3 krátké odpovědi, kde respondenti uvedli ne a tyto tři níže uvedené odpovědi, tak vychází, že většina osob z výzkumu se chová zodpovědně nebo se nějakým způsobem snaží chovat rozumně na internetu. Pro úplnost uvádím zmíněné odpovědi:

1. *„Nechovám se zodpovědně, sdílím tam dost osobního života.“*
2. *„Ne. Domnívám se, že v dnešní době by bylo nejzodpovednejsi a nejbezpečnější internet vůbec nepoužívat.“*
3. *„Moc ne, jak kdy. V případě internetového bankovnictví používám výhradně firemní počítač, který je zabezpečnený jak počítače v NSA (holt jsme paranoidní a histerická firma), ale u osobních občas zajdu i na ne úplně vhodné stránky (např. weby se seriály, kde neustále skáčou reklamy a často se zde dá chytit vir).“*

Další skupina byla s neutrální odpovědí:

1. *„doufám že ano ale v dnešní době těžko říct co je zodpovědně“*
2. *„Je mi ale jasné, že zdatný hacker by se k mým informacím dostal, stále si ale myslím, že by tím moc nepomohl.“*
3. *„Když tak o tom přemýšlím, tak asi 50:50, hesla neměním a účet na Instagramu mám veřejný, oproti tomu účet na Facebooku mám přístupově hodně omezen a nesdílím osobní informace, kromě data narození, na žádných sociálních sítích.“*
4. *„Každý musí jednat s rozvahou, tak jako v reálném životě.“*
5. *„Rada se divam na serialy. Obcas na strankach co muj antivir blokuje. Vypnu ho na tu chvili a pak zase zapnu.“*
6. *„studuji informacni bezpecnost, takze se dokonale vyznam ve fungovani viru a bezpecnosti na socialnych sitich“*
7. *„Mohlo by to být asi lepší, zanechávám po sobě určité stopy :-).“*

Pro vyhodnocení této je otázky bylo nutné vzít na zřetel, že na otázku odpovědělo pouze 81 z 154 respondentů. Ale i přes tato čísla, jsou to podivuhodný výsledek. Většina uživatelů se snaží chovat na internetu, tak aby žádným způsob nezpůsobila sobě nebo svému okolí jakoukoli újmu. Každý uživatel je obezřetný jiným způsobem.

5.4 INTERPRETACE VÝSLEDKŮ

V této části práce bude následovat celkové zhodnocení výzkumu a vyhodnocení hypotéz.

Hypotéza č. 1: Nejvíce využívají sociální sítě mladší (kolem 20 let) uživatelé internetu.

Tato hypotéza se potvrdila na začátku výzkumu, v otázce číslo 3 vyšel výsledek, že nejvíce uživatelů sociálních sítí je 21-25 let (57,14 %) a poté následuje skupina 16 – 20 let (5,19 %).

Hypotéza č. 2: Uživatelé sdílejí na sociálních sítích důvěrné informace v domněnce, že jejich data nikdo nemůže zneužít.

Hypotéza je ověřena v otázce číslo 6, uživatelé sdílejí o sobě spoustu informací na sociální sítě. Mezi nejvíce sdílené věci patří fotografie, zážitky z dovolených, aktuální poloha, datum narození, telefonní číslo, politické myšlenky a náboženské vyznání. Tyto případy sdílených informací mohou vést k mnohým rizikům. Jak již bylo výše zmíněno, tak ve výzkumu se neprokázalo, že respondenti měli zkušenosti s těžkými kriminálními zločiny. Zkušenosti se špatnými praktikami měli, ale bylo jich pouze 24. Vydírání zažili 2 dotazovaní, se šikanou se setkal 1 respondent, zneužití fotografií řešilo 5 osob, sledování bylo 6 respondentů a krádež identity bylo u 7 osob.

Uživatelé si, ale musí uvědomit i další problémy, které plynou ze sdílení informací. Pokud budou uživatelé na internet nahrávat zážitky ze svojí rodinné dovolené, tak se může stát, že budou vykradeni. Pachatel si dokáže najít, informace o tom, že celá rodina je na dovolené v zahraničí. To samé platí, pokud uživatel, sdělí svoji aktuální polohu mimo domov, tak také nahrává zlodějům. Dalším problémem je sdílení

fotografií majetku uživatelů. Lidé se rádi chlubí svým majetkem, zařízením v bytě. V případě, že je uživatelský profil volně přístupný, je z nich snadný terč.

Hypotéza č. 3: Uživatelé na internetu začali být opatrní až ve chvíli, kdy se stali obětí trestného činu nebo zneužití.

Uživatelé na internetu, jsou podle svého svědomí opatrní. I když někteří si nejsou vědomi veškerých následků, které je mohou na internetu potkat. Většina dotázaných, kteří odpověděli, že byli obětí špatných praktik na internetu (otázka č. 8), sami napsali, že se pak chovali jiným způsobem (otázka č. 10). Dávají si větší pozor na podvodné jednání lidí a na podvodné zprávy, nevkládají o příspěvky o sobě a o svých přátelích, jsou více obezřetní a častěji mění hesla. Tyto odpovědi i nespočet dalších je možné vidět v poslední otázce výzkumu. Kde pouze 6 z 81 odpovídajících osob uvedlo, že se na internetu, dle svého mínění chová nezodpovědně. Je to také způsobeno, tím že byli sami obětí internetového užívání nebo někdo z jejich okolí. Uživatelovo okolí je zahrnuto v otázce č. 13, kde respondenti odpovídali na otázku, zda znají někoho komu, byly zneužity údaje. V tomto bodě vyšel výsledek, že 50 (32,47 %) respondentů někoho takového zná. V odpovědích byl vysoký počet krádeží indenty 25 (50 %), útoků se sexuálním podtextem 7 (14 %), a šikana 4 (8 %). Na předních příčkách se opět umístili odpovědi: rozesílání podvodných zpráv a napadení počítačovým virem.

S touto hypotézou souvisí také otázka č. 7, kde se řeší nastavení zabezpečení sociální sítí. Většina uživatelů 93 (62 %) uvedlo, že jejich příspěvky mohou vidět pouze jejich schválení uživatelé, většinou to jsou jejich přátelé. Pouze 34 (22,67 %) uživatelů sdělilo, že používají individuální nastavení soukromí na jejich sociálních sítích. Bohužel ve výzkumu se objevili tací, kteří mají své profily veřejně přístupné vše nebo je jim lhostejné, kdo je na jejich profilu a to 24 (15,33 %) respondentů. Pokud tito lidé na svých profilech sdílejí své osobní informace či důvěrné věci, mohou se snadno stát obětí rizik zmíněných v kapitole 3.3.

Hypotéza č. 4: Většina uživatelů internetu má ve svém počítači antivirový program a myslí si, že je to dostatečná ochrana na internetu.

Ve výzkumu byly zjištěny tyto výsledky. Antivirový program používá 134 (87,01 %) respondentů a pouze 65 (42,21 %) považuje antivirový program jako dostatečnou ochranu. V rámci zjištění jaké antivirové programy uživatelé používají, vyšlo, že nejvíce je používaný program AVAST, který v nedávné prověřování antivirových programů skončil až na 11. místě. Zatímco program, který v testu vyšel, jako nejlépe vyhovující se umístil v našem žebříku až na třetím místě pouze s 28 (20,9 %) respondenty. Tato hypotéza se tedy potvrdila pouze z části. Sami odborníci uvádí, že antivirový program není stoprocentní ochrana na internetu.

Z výzkumu také vyšlo najevo, že většina dotazovaných si je vědoma alespoň nějakého rizika, která na internetu jsou. Většina uživatelů, podle jejich rekcí se snaží na internet nedávat osobní informace, které by podle nich byly zneužitelné. Uživatelé jsou dle svého názoru zodpovědní, ale přesto, že si to o sobě myslí, tak se minimálně třetina z nich již stalo obětí nějakého útoku. Takto dobré výsledky jsou z větší části příčinou věkovou kategorií respondentů, pokud by bylo více respondentů z věkové kategorie 16 - 20 let, možná bychom dospěli k jiným číslům.

ZÁVĚR

Tato bakalářská práce je zaměřena na bezpečnost na internetu, sociálních sítích a internetovém bankovnictví a s nimi souvisejícími antivirovými programy. Toto téma je velmi aktuální a respondentům nedělalo, žádný problém odpovědět na dotazníkové šetření daného problému.

Sociální sítě jsou součástí života většiny z nás. Z výzkumu vyplývá, že pouze 4 respondenti z 154 nepoužívají sociální sítě. Většina z nich je využívá i několikrát za den, aby se s ostatními uživateli podělili o svoje zážitky a fotografie z aktuálního dění kolem sebe. Dále se uživatelé rádi dělí o své názory, náboženská vyznání a úspěchy. Uživatelé svoje příspěvky většinou sdílí se svými přáteli (62 %) nebo po pečlivém nastavení soukromí ostatními (22,67 %). Ovšem jsou tu tací, kterým nezáleží na tom, kdo si jejich příspěvky pročítá, těchto uživatelů je 24 (15,33 %) z celkového počtu 150 lidí, kteří odpovídali v dotazníkovém šetření. Daní respondenti se také přiznali, že se již stali obětí cíleného útoku na internetu. 7 osob uvedlo, že jim byla ukradena identita, 6 respondentů bylo sledováno přes sociální sítě, 2 byli vydíráni a 1 respondent byl šikanován. Po této skutečnosti si tito uživatelé dávají větší pozor, jaké informace sdílejí a lépe si zabezpečují svoje profily na sítích.

Druhou částí výzkumu, bylo zjišťováno, jakým způsobem si uživatelé chrání svůj počítač, před škodlivými programy a viry. Zde odpovídal plný počet respondentů z výzkumu, tedy 154. Z tohoto čísla pouze 134 (87,1 %) uživatelů používá antivirové programy jako ochranu na internetu. Zneklidňující je číslo, které nám říká, že 65 (42,21 %) uživatelů internetu věří, že antivirový program je dostatečná ochrana. Pokud je navíc ještě zjištěno, že nejvíce používaný antivirový program nemá nejlepší hodnocení v prověřovacích testech v porovnání s jinými programy.

V poslední otázce výzkumu byli respondenti vyzváni, aby vyjádřili svůj názor na jejich chování na internetu. Většina dotazovaných uvedla názor, že se na internetu chová zodpovědně. Jen nepatrné množství respondentů se přiznalo, že se chovají nezodpovědně nebo si připustilo myšlenku, že na internetu nemusí být nikdo v bezpečí.

SEZNAM POUŽITÝCH ZDROJŮ

Seznam použitých českých zdrojů

KRAS, P. Internet: V Kostce užití v běžném životě. Havlíčkův Brod: Fragment, 2001. ISBN 80-7200-493-X.

MCQUAIL, Denis. Úvod do teorie masové komunikace. Vyd. 2. Praha: Portál, 1999. s.31. ISBN 80-717-8714-0

PAVLÍČEK, A. Nová média a sociální sítě. 1.vyd. Praha: Oeconomica, 2010. ISBN 978-80-245-1742-1

Seznam použitých internetových zdrojů

BELLIS, M. *Who Invented Facebook?* [online]. [cit. 2017-02-04]. Dostupné z: http://inventors.about.com/od/fstartinventions/a/Facebook.htm

BENEŠOVSKÁ, M.: Historie internetu v datech. Helloworld.cz [online]. 2017 [cit. 2017-03-01]. Dostupné z: http://www.helloworld.cz/historie-internetu-v-datech/

CO JE ANTI-VIROVÝ PROGRAM?. *PC viry* [online]. 2008 [cit. 2017-03-05]. Dostupné z: http://pc-viry.webnode.cz/co-je-to-anti-virovy-program-/

CO JE STALKING A CYBERSTALKING. *E- bezpečí* [online]. 2008 [cit. 2017-02-25]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/stalking-a-kyberstalking/66-23

CO JE TO KYBERGROOMING?. *E- bezpečí* [online]. [cit. 2017-02-25]. Dostupné z: http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybergrooming.html

CO JE TO KYBERŠIKANA A JAK SE PROJEVUJE?. [online]. [cit. 2017-02-25]. Dostupné z: http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybersikana-a-jak-se-projevuje.html

DLOUHODOBÉ VÝSLEDKY V TESTECH SPOLEČNOSTI VIRUS BULLETIN. *Antivirové centrum*. [online]. 1.2.2017 [cit. 2017-04-03]. Dostupné z: https://www.antivirovecentrum.cz/aktuality/srovnani-antiviru.aspx

EVIL TWIN. *Správa sítě: slovník pojmů* [online]. 2016 [cit. 2017-03-08]. Dostupné z: http://www.sprava-site.eu/evil-twin/

FACEBOOK [online] 2017 [cit.2017-02-11] Dostupné z: https://www.facebook.com/legal/terms/update

HOAX. *Správa sítě* [online]. 2016 [cit. 2017-02-26]. Dostupné z: http://www.sprava-site.eu/hoax/

CHRAŇTE SVŮJ POČÍTAČ. *Antivirové centrum* [online]. [cit. 2017-03-05]. Dostupné z: https://www.antivirovecentrum.cz/antiviry.aspx

INSTAGRAM. *Instagram* [online] [cit.2017-02-05] Dostupné z: https://help.instagram.com/182492381886913

INTERNETOVÉ BANKOVNICTVÍ. *Měšec* [online]. [cit. 2017-03-02]. http://www.mesec.cz/bankovni-ucty/prime-bankovnictvi/internetove-bankovnictvi/pruvodce/

KOMUNIKACE PŘES INTENRET. *Jak na internet* [online]. [cit. 2017-03-04]. Dostupné z: https://www.jaknainternet.cz/page/1236/komunikace-pres-internet

KUBEŠ, R. *Sociální sítě nejsou jen Facebook. Podívejte se i na ty české* [online]. 2009 [cit. 2017-02-27]. Dostupné z: http://technet.idnes.cz/socialni-site-nejsou-jen-facebook-podivejte-se-i-na-ty-ceske-p4e-/sw_internet.aspx?c=A091017_234210_tec_reportaze_vse

KYBEPROSTOR. *Správa sítě* [online]. 2016 [cit. 2017-02-26]. Dostupné z: http://www.sprava-site.eu/kyberprostor/

KYBERKRIMINALITA. *Správa sítě* [online]. [cit. 2017-02-26]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx

KYBERSTALKING. *Správa sítě* [online]. 2006 [cit. 2017-02-25]. Dostupné z: http://www.sprava-site.eu/kyberstalking/

LETOCHOVÁ, K.: Sexting aneb Černobílá budoucnost. E- bezpečí [online]. 2013 [cit. 2017-02-26]. Dostupné z: https://www.e-bezpeci.cz/index.php/temata/sexting/601-sexting-cernobilabudoucnost

MÁŤA. *Co je instagram* [online] 2015 [cit.2017-02-05]. Dostupné z: https://www.cestujsnadno.cz/co-je-instagram

MAZANCOVÁ, M. *Sociální sítě pro začátečníky: Které vybrat?* [online]. 2011 [cit. 2016-02-04]. Dostupné z: http://www.internetprovsechny.cz/socialni-site-pro-zacatecniky-ktere-vybrat/

NOYES, D. The Top 20 Valuable Facebook Statistics. [online] 2017 [cit. 2017-02-04]. Dostupné z: https://zephoria.com/top-15-valuable-facebook-statistics/

PHILLIP, S. *A brief history of Facebook* [online]. 2007 [cit. 2017-02-04]. Dostupné z: http://inventors.about.com/od/fstartinventions/a/Facebook.htm

PHISHING A PHARMING. *Bezpečný internet.cz* [online]. [cit. 2017-02-26]. Dostupné z: http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx

PRETEXTING. *Správa sítě: slovník pojmů* [online]. 2016 [cit. 2017-03-08]. Dostupné z: http://www.sprava-site.eu/pretexting/

PŘÍME BANKOVNICTVÍ. *Měšec* [online]. [cit. 2017-03-02]. Dostupné z: http://www.mesec.cz/bankovni-ucty/prime-bankovnictvi/internetove-bankovnictvi/pruvodce/prime-bankovnictvi-2/

SMITH, C., *350+ Amazing Twitter statistics and facts (November 2016*) [online]. 2014 [cit.2016-02-04]. Dostupné z: http://expandedramblings.com/index.php/march-2013-by-the-numbers-a-few-amazing-twitter-stats/

SOCIÁLNÍ INŽENÍRSTVÍ. *Správa sítě: slovník pojmů* [online]. 2016 [cit. 2017-03-08]. Dostupné z: http://www.sprava-site.eu/socialni-inzenyrstvi/

TWITEER HELP. *The History of Twitter* [online]. [cit. 2017-02-04]. Dostupné z: http://profilerehab.com/twitter-help/history_of_twitter

VISHING. *Správa sítě: slovník pojmů* [online]. 2016 [cit. 2017-03-08]. Dostupné z: http://www.sprava-site.eu/vishing/

WARCHAR, P., *Jak vznikl Instagram? Od nuly až k Facebooku* [online] 2005 [cit.2016-02-05] Dostupné z: http://www.instagram.cz/jak-vznikl-instagram-od-nuly-az-k-facebooku/362

SEZNAM ZKRATEK

ARPA – Advanced Researcg Projects Agency

ARPANET – Advanced Researcg Projects Agency NETwork

BITNET – Because It's Time NETwork,

CD – Compact Disk

CERN – Centre Européan pour Recherche Nucléaire

CESNET – Czech Educational and Scientific NETwork

ČR – Česká republika

ČVUT – Česká vysoké učení technické

DVD – Digital Versatile Disc nebo Digital Video Disc

HTML – HyperText Markup Language

IMP - Interface Message Processor

NSE – National Stock Exchange

NSENET – National Stock Exchange NETwork

PIN – Personal Identifikation Number

SMS – Short Message Service

TAN – TransAction Number

USA – The United States of America

USB – Universal Serial Bus

WWW - World Wide Web

SEZNAM OBRÁZKŮ, TABULEK A GRAFŮ

Seznam tabulek

Seznam grafů

SEZNAM PŘÍLOH

Příloha A – Dotazník

Dobrý den,

prosím o vyplnění dotazníku k bakalářské práci. Práce se zabývá otázkou bezpečnosti a chování uživatelů na internetu.

Dotazník je určen občanům České republiky bez věkového omezení.

Děkuji za Váš čas

1. Vaše pohlaví?

- muž
- žena

2. Váš věk?

- do 15 ti let
- 16-20 let
- 21-25 let
- 26-35 let
- 36-45 let
- 46-60 let
- 61 let a více

3. Používáte sociální sítě?

- ano
- ne

4. Jaké používáte sociální sítě? (Vyberte)

- Facebook
- Twitter
- Instagram
- Myspace
- Google +
- Badoo
- LinkdeIn
- Foursquare

- Spolužáci.cz
- jiné: …..

5.Jak často navštěvujete sociální sítě?

- několikrát za den
- jednou denně
- 4x do týdně
- 1x měsíčně

6. Které informace sdílíte na sociálních sítích? (Vyberte)

- fotografie
- aktuální polohu
- zážitky z dovolené
- datum narození
- telefonní číslo
- náboženské vyznání
- aktuální nápady/myšlenky
- politické názory
- nic
- přidávám jiné příspěvky:……..

7. Kdo může vidět vaše příspěvky na sociální síti?

- všichni uživatelé
- pouze mnou schválení
- nezáleží mi na tom
- mám individuální nastavení: ……

8. Zneužil někdo vaše data/ osobní údaje ze sociálních sítí k účelům, které se vám nelíbily. Nebo jste byl obětí trestného činu?

- ano
- ne

9. Z jakého důvodu byly vaše data/údaje zneužity?

- napadení počítačovým virem
- rozesílání podvodných zpráv
- zneužití fotografií

- krádež identity
- sledování
- vydírání
- šikana
- sexuální podtext
- jiné :……

10. Změnilo se po této zkušenosti vaše chování na sociálních sítích?

- ano
- ne

11. Jak se změnilo vaše chování? (otevřená otázka)

12. Znáte někoho ve svém okolí, komu byly zneužity data/osobní ze sociálních sítí?

- ano
- ne

13. Z jakého důvodu mu byly data/údaje zneužity?

- krádež identity
- napadení počítačovým virem
- rozesílání podvodných zpráv
- zneužití fotografií
- sledování
- vydírání
- šikana
- sexuální podtext
- jiné :……

14. Používáte internetové bankovnictví?

- ano
- ne

15. Zneužil někdo vaše data/ osobní údaje z internetového bankovnictví ke krádeži či jinému chování?

- ano
- ne

16. Jak často měníte heslo na vašem internetovém bankovnictví?

- při každém přihlášení
- 1x měsíčně
- 1x ročně
- po vyzvání bankou
- Od počátku používám stejné
- jiná odpověď:

17. Znáte někoho ve svém okolí někoho komu byly zneužity data/osobní údaje z internetového bankovnictví?

-ano
- ne

18. Používáte antivirový program?

- ano
- ne

19. Jaký používáte antivirový program?

- Astard
- Avast
- AVG
- Avira
- Eset
- Panda
- Norman
- jiný:……

21. Považujete antivir jako dostatečnou ochranu na internetu?

- ano
- ne

22. Myslíte si, že se chováte zodpovědně na internetu a proč? (nepovinná otevřená otázka)

Příloha B – Datová matice

	1	2	3	4.X	5	6.I	7	8	10	11	12	14	15	16.I	16.II	16.III	16.IV	16.V	16.VI	17	18	20	21
1	2	3	1	0	1	1	2	2	0	0	1	1	2	0	0	0	4	0	0	2	1	2	0
2	1	3	1	0	1	1	2	1	1	2	1	1	2	0	0	0	4	0	0	2	1	2	0
3	1	5	1	0	1	0	2	2	0	0	2	1	2	0	0	3	0	0	0	2	1	2	66
4	2	4	1	0	1	0	2	2	0	0	2	1	2	0	0	3	0	0	0	2	1	2	0
5	1	3	1	0	1	1	1	2	0	0	2	1	2	0	0	0	0	5	0	2	2	2	0
6	2	3	1	0	1	0	2	2	0	0	2	1	2	0	0	3	0	0	0	2	1	1	0
7	1	3	1	0	1	1	4	2	0	0	1	1	2	0	0	3	0	0	0	2	2	2	0
8	1	3	1	0	1	1	4	2	0	0	1	1	2	0	0	0	0	5	0	2	2	2	0
9	2	3	1	0	1	1	2	2	0	0	2	1	2	0	0	3	0	0	0	2	1	2	0
10	2	3	1	0	1	0	4	2	0	0	2	1	2	0	0	0	0	5	0	2	1	1	2
11	2	3	1	5	1	1	2	2	0	0	2	1	2	0	0	0	0	5	0	2	2	2	0
12	1	3	1	0	1	1	4	2	0	0	2	1	2	0	0	0	0	5	0	2	1	2	49
13	1	3	1	0	1	1	2	2	0	0	2	1	2	0	0	0	0	5	0	2	1	2	0
14	2	5	1	0	1	1	2	2	0	0	2	1	2	0	0	0	4	0	0	1	1	2	28
15	2	4	1	0	1	1	4	2	0	0	1	1	2	0	0	0	4	0	0	2	1	1	52
16	1	5	1	0	1	0	2	2	0	0	2	1	2	0	0	0	0	5	0	2	1	1	6
17	2	3	1	0	1	1	1	2	0	0	2	1	2	0	0	0	0	5	0	2	2	1	0
18	1	4	1	0	1	1	2	2	0	0	1	1	2	0	0	3	0	0	0	2	1	2	0
19	1	3	1	0	1	0	4	1	1	12	1	1	2	0	0	0	4	0	0	2	1	2	63
20	1	5	1	0	1	1	3	2	0	0	2	1	2	0	0	0	4	0	0	2	1	1	0
21	1	4	1	0	2	0	2	2	0	0	2	1	1	0	0	0	4	0	0	1	2	2	23
22	1	3	1	0	1	1	4	2	0	0	2	1	2	0	0	3	0	0	0	2	1	2	0
23	1	5	1	0	1	0	4	2	0	0	2	1	2	0	0	0	0	5	0	2	1	1	19
24	1	3	1	0	1	1	2	2	0	0	1	1	2	0	0	0	0	5	0	2	2	1	0
25	1	4	1	0	1	0	1	1	2	0	2	1	1	0	0	0	4	0	0	1	1	2	0
26	1	3	1	0	1	1	2	2	0	0	2	1	2	0	0	0	4	0	0	2	1	2	42
27	2	3	1	0	1	1	2	2	0	0	1	1	2	0	0	0	0	0	3	2	1	1	0
28	1	3	1	0	1	1	2	2	0	0	2	1	2	0	2	0	0	0	0	2	1	2	44
29	1	4	1	0	1	1	2	2	0	0	2	1	2	0	0	0	0	5	0	2	1	2	22
30	2	3	1	0	1	1	2	2	0	0	2	1	2	0	0	0	0	5	0	2	1	2	-1
31	1	5	1	0	1	1	2	2	0	0	2	1	2	0	0	0	4	0	0	2	1	1	2
32	1	3	1	10	1	1	2	2	0	0	1	1	2	0	0	0	0	5	0	2	1	2	0
33	1	3	1	0	1	1	2	2	0	0	1	2	0	0	0	0	0	0	0	2	1	2	39
34	2	3	1	0	1	1	2	1	2	0	2	1	2	0	0	0	4	0	0	2	1	2	30
35	2	3	1	0	1	1	2	2	0	0	2	1	2	0	0	0	4	0	0	2	1	1	0
36	1	5	1	0	1	0	4	2	0	0	2	1	2	0	0	0	0	5	0	2	1	2	3
37	1	3	1	0	1	1	2	2	0	0	2	1	2	0	0	0	0	5	0	2	1	1	0
38	1	4	1	0	2	0	4	2	0	0	2	1	2	0	0	3	0	0	0	2	1	2	-1
39	1	3	1	0	1	1	2	2	0	0	2	1	2	0	0	0	4	0	0	2	1	1	51
40	1	3	1	0	1	1	4	2	0	0	2	1	2	0	0	0	4	0	0	2	1	1	-1
41	1	5	1	0	1	1	4	2	0	0	2	1	2	0	0	0	4	0	0	2	1	1	-1
42	2	4	1	8	1	1	4	1	1	4	1	1	2	0	0	0	4	0	0	2	1	2	47
43	1	4	1	0	1	1	2	2	0	0	2	1	2	0	0	0	4	5	0	2	1	2	-1
44	1	3	1	0	1	1	2	2	0	0	2	1	2	0	0	0	4	0	0	2	1	1	21
45	1	5	1	0	1	1	2	2	0	0	2	1	2	0	0	3	0	0	0	2	1	2	0
46	1	3	1	0	1	1	2	1	1	9	1	2	0	0	0	0	0	0	0	1	1	1	62
47	1	3	1	0	1	1	4	1	1	-1	1	1	2	0	0	3	4	0	0	2	1	1	-1
48	2	3	1	0	1	1	2	2	0	0	2	1	2	0	0	0	0	5	0	2	1	2	0
49	1	3	1	0	1	0	2	2	0	0	2	1	2	0	0	3	0	0	0	2	1	1	56
50	1	3	1	0	1	1	2	2	0	0	2	1	2	0	0	0	0	5	0	2	1	1	2

BIBLIOGRAFICKÉ ÚDAJE

Jméno autora: Klára Hrušková

Obor: Sociální a mediální komunikace

Forma studia: kombinovaná studium

Název práce: Bezpečnost a bezpečností rizika v prostředí internetu

Rok: 2017

Počet stran textu bez příloh: 48

Celkový počet stran příloh: 5

Počet titulů českých použitých zdrojů: 3

Počet internetových zdrojů: 31

Vedoucí práce: Mgr. Iskanderová Tatiana, Ph.D.